Administration Guide

for Cisco Webex devices running RoomOS 10.8

D15473.02
RoomOS 10.8
10-2021

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/desk-docs
- ▶ https://www.cisco.com/go/room-docs
- ▶ https://www.cisco.com/go/board-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 7
Product features at a glance.......13
Room Series at a glance.......14
Desk Series at a glance.......17
Webex Boards at a glance.......18
How to administer the video conferencing device 19
Touch controllers 24

Configuration 25
User administration.......26
Change the device passphrase 27
Restrict the access to the Settings menu.......28
Device configuration 29
Add a sign in banner 30
Add a welcome banner.......31
Manage the service certificates of the device 32
Manage the lists of trusted certificate authorities - CAs.......33
Set up secure audit logging.......37
Delete CUCM trust lists.......38
Change the persistency mode.......39
Set up an SMTP email server 40
Set up ad hoc multipoint conferences.......41
Set up Intelligent Proximity for content sharing 43
Adjust the video quality to call rate ratio.......47
Select a multi-screen background image.......49
Add corporate branding to the screen and touch controller 50
Add a virtual background 53
Add a custom wallpaper 54
Choose a ringtone and set the ringtone volume 55
Manage the Favorites list.......56
Set up accessibility features.......57
Set up the standby behavior 58
Provisioning of product specific configurations from CUCM.......59

Peripherals.................................... 61
Connecting screens or other output devices 62
Connecting input sources....... 68
Extend the number of input sources.......75
Information about displays.......76
Information about 4K resolution.......77

Information about HDMI cables....78
Set up the SpeakerTrack feature....79
Set up the Snap to Whiteboard feature.... 83
Set up the PresenterTrack feature....86
Briefing room set-up.... 90
Classroom set-up....97
Test the loudspeaker connections....105
Using extra loudspeakers and sound reinforcement....108
Bluetooth® headset....109
Connect the touch controller.... 110

Maintenance....118
Installing new software.... 119
Add option keys.... 121
Device status....122
Run diagnostics....123
Download system log files....124
Get call logs....126
Access the Technical support screen....127
Create a remote support user....128
Backup and restore configurations and custom elements....129
CUCM provisioning of custom elements....130
TMS provisioning of custom elements.... 131
Revert to the previously used software image....132
Factory reset the video conferencing device....133
Factory reset Cisco Webex Room Navigator....138
Factory reset Touch 10....139
Capture user interface screenshots....140

Device settings....141
Overview of the device settings....142
Audio settings....149
Bluetooth settings....164
Bookings settings....164
BYOD settings....165
CallHistory settings....165
Cameras settings....166
Conference settings....176
FacilityService settings....182
GPIO settings....183
H323 settings....183
HttpClient settings....186
HttpFeedback settings....187
Logging settings....188
Macros settings....190
Network settings.... 191
NetworkServices settings....201
Peripherals settings.... 211
Phonebook settings....213
Provisioning settings....214
Proximity settings....217
RoomAnalytics settings....219
RoomCleanup settings.... 220
RoomReset settings....221
RoomScheduler settings....221
RTP settings.... 222
Security settings.... 223
SerialPort settings.... 226
SIP settings....227
Standby settings....231
SystemUnit settings.... 234
Time settings.... 235
UserInteraction settings....237
UserInterface settings.... 238
UserManagement settings.... 248
Video settings....252
VoiceControl settings.... 268
WebEngine settings.... 268
Webex settings....270
WebRTC settings....271
Experimental settings....272

Physical interfaces.... 273
Power On/Off....274
Connector panel: Codec Plus.... 282
Connector panel: Codec Pro and Room Panorama.... 283
Connector panel: Room Kit.... 284
Connector panel: Room Kit Mini.... 285
Connector panel: Room 55.... 286
Connector panel: Room 55 Dual and Room 70....287
Connector panel: Room 70 G2 and Room 70 Panorama.... 288
Connector panel: Webex Desk, Desk Pro and Desk Limited Edition.... 289
Connector panel: Boards.... 290
Connector panel: Room Panorama amplifier....291

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by Cisco is under license. Other trademarks and trade names are those of their respective owners.

Appendices 292
How to use the Webex Board 293
How to use the Webex Desk, Desk Pro and Desk Limited Edition 294
How to use the touch controller 295
Using the device as a USB camera 296
Panoramic video 298
Set up remote monitoring 299
Access call information and answer a call while using the web interface 300
Place a call using the web interface 301
Share content using the web interface 303
Local layout control 304
Control a local camera 305
Control a far end camera 306
Room analytics 307
Customize the video conferencing device's user interface 308
Customize the video conferencing device's behavior using macros 310
Show or hide default buttons on the user interface 311
Use of a third-party USB input device 312
Sending HTTP(S) requests 313
Digital signage 314
Web apps 315
API-driven web views 316
Input source composition 317
Presentation source composition 319
Access the device’s XML files 321
Execute API commands and configurations from the web interface 322
Advanced customization of audio 323
About Ethernet ports 324
Mini-jack connector pin-out schemes 325
Audio inputs and outputs 326
The GPIO and 3G-SDI connectors 328
API access using the COM port 329
Serial interface for maintenance 330
The systemtools commands 334
Open TCP ports 335
HTTPFeedback address from TMS 336
Link an on-premises registered device to Cisco Webex Edge for Devices 337
Register a device to the Cisco Webex cloud service 338
Supported RFCs 339
Calculating minimum bandwidth 340
User documentation on the Cisco web site 341
Cisco contacts 342

Chapter 1

Introduction

User documentation and software

Products covered in this guide

This guide covers the following device models:

- Cisco Webex Board 55/55S, 70/70S, and 85S
- Cisco Webex Codec Plus
- Cisco Webex Codec Pro
- Cisco Webex Desk
- Cisco Webex Desk Pro
- Cisco Webex Desk Limited Edition (Desk LE)
- Cisco Webex Room Kit
- Cisco Webex Room Kit Mini
- Cisco Webex Room 55
- Cisco Webex Room 55 Dual
- Cisco Webex Room 70 Single/Dual
- Cisco Webex Room 70 Single/Dual G2
- Cisco Webex Room 70 Panorama
- Cisco Webex Room Panorama

Note that RoomOS 10 does not support Cisco TelePresence SX, DX or MX Series devices.

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 most 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/desk-docs
▶ https://www.cisco.com/go/room-docs
▶ https://www.cisco.com/go/board-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

Cisco Webex RoomOS 10 is based on Collaboration Endpoint Software 9 (CE9) and is a continuation of the same software. This means that the first release of RoomOS 10 inherits the same features as CE9.15.3 as of April 2021, with a few exceptions.

Download software for the endpoint from the Cisco web site:

▶ https://software.cisco.com/download/home

We recommend reading the Software release notes (RoomOS 10). It's the same set of release notes for all products.

▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html
▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/products-release-notes-list.html
▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-board/products-release-notes-list.html

Converting to RoomOS 10 software

Before upgrading from *CE software* to *RoomOS 10 software*, carefully consider the upgrade requirements; otherwise upgrading to RoomOS 10 software can leave you with a non-functional deployment and require you to downgrade. Read the Software release notes for full details.

Note:

- RoomOS 10 does not support ISDN Link

What’s new (page 1 of 6)

This chapter provides an overview of the new and changed device settings (configurations), and the new features and improvements compared to software version CE9.15.3.

For more details, we recommend reading the Software release notes (RoomOS 10):

- ► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html
- ► https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/products-release-notes-list.html
- ► https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-board/products-release-notes-list.html

New features and improvements in RoomOS 10.8

New products

- Cisco Webex Desk
- Cisco Microphone Array for Cisco Webex Room Panorama / Room Panorama 70

Cisco Webex Room Navigator Supports 802.1.x

(Room Navigator)

This security feature will now be supported on the Room Navigator. Support for 802.1.x enables a secure connection for customers to authenticate devices on their network. Companies that are security aware now have a way to authenticate their devices in the network.

Synchronize Software with Cisco Webex Room Navigator *(Room Navigator)*

If the software version on a Cisco Webex Room Device isn’t supported by the Cisco Webex Room Navigator, you’ll be unable to pair the device with the touch controller. Now, the Room Navigator can download supported software from the cloud to update the room device and allow successful pairing.

Local web app management

(Desk Pro, Desk Limited Edition, Webex Desk, Boards)

Now you can enable users to add and delete web apps themselves from the touch interface Settings menu on Webex Boards and Desk Series devices.

USB Microphone support for Desk and Room devices (Desk Pro, Desk Limited Edition, Webex Desk, Room Kit, Room Kit Mini, Room 55)

You can now use a USB microphone, or a USB audio interface with your Desk Pro, Room Kit, Room Kit Mini, and Room 55 device.

New layout menu *(All products)*

With the visual update to the Layout menu, you’ll now see the same layout names and icons whether you're using a Webex device or a Webex app. The new menu shows a list of stylized representations of the different layouts available.

Whiteboard shape recognition

(Desk Pro, Desk Limited Edition, Webex Desk, Boards)

Shape recognition can now understand arrows and curves. If shape recognition isn’t toggled on before drawing the shape, long pressing the shape activates it and adjusts the shape.

Complete keyboard language support turned on by default *(All products)*

The complete localized keyboard language support introduced in a previous release is now turned on by default. Keyboard language follows the language settings for the user interface and users can select the language from the device’s Settings menu.

Webex activation network test *(All products)*

During the initial setup of a device when the Startup Wizard asks for your activation code, if Webex activation fails you’ll see a Cloud Connection Test button on the interface. Tapping the button opens a screen showing the network status and result of the test.

After onboarding your device a Webex Connectivity Test option is available from the Settings menu. If you select it, the system will reach out to all of the registered Webex services and show detailed results.

Support for WPA1 removed *(Wi-Fi)* *(All products)*

WPA1 Personal and Enterprise is no longer supported.

What’s new (2 of 6)

H323 now supports AES256 encryption

(All products)

Support has been added for AES256 encryption for H323. When H323 is configured to use AES256, you should also set the H323 Encryption KeySize to Min2048bit.

Gesture recognition for raise hand

(Desk Pro, Desk Limited Edition, Webex Desk)

When the raise hand feature is already enabled, physically raising your hand in front of the device causes the raised hand indicator to show up in the meeting.

This feature requires CMS 3.2 or later.

Gesture recognition for reactions

(Desk Pro, Desk Limited Edition, Webex Desk)

On devices linked to Webex Edge for Devices, when reactions and gesture recognition are enabled, physically clapping or giving a thumbs up or down in front of the device causes the matching reaction indicator to show up in the meeting.

Cloud pairing for devices linked to Webex Edge for Devices *(All products)*

Webex Edge for Devices now allows on-premises devices to use all Webex cloud pairing options for better usability and security. Discover and connect to nearby Webex Rooms by audio (ultrasound), Wi-Fi discovery, or manually by searching for the room name.

This feature is available for devices linked to Webex Edge for Devices, and only when Webex Optimized Experience is enabled.

Direct share from Webex *(All products)*

To improve the quality of content sharing, with direct share the Webex App prefers to share content directly to the paired Webex device over the local network. In setups where direct share isn’t available, the app continues to route content share media through the cloud.

Direct share is only available for devices linked to Webex Edge for Devices.

What's new (page 3 of 6)

Configuration changes in RoomOS 10.8

New Configurations

Audio Input USBInterface [1] EchoControl Mode *(Codec Pro, Room 70 G2, Room Panorama, Room 70 Panorama)*

Audio Input USBInterface [1] Level *(Codec Pro, Room 70 G2, Room Panorama, Room 70 Panorama)*

Audio Input USBInterface [1] Mode *(Codec Pro, Room 70 G2, Room 70 Panorama)*

Audio Input USBMicrophone [1] Level *(Desk Pro, Desk Limited Edition, Room 55, Room Kit, Room Kit Mini, Webex Desk)*

Audio Output Ethernet [1..2] Mode *(Room Panorama)*

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

Conference EndToEndEncryption Identity PreferredDomain *(All products)*

Conference JoinLeaveNotifications *(All products)*

H323 Encryption AES256Support *(All products)*

Network [1] IPv4 InterfaceIdentifier *(All products)*

RoomScheduler BookingTimeout *(All products)*

Standby Halfwake Mode *(All products)*

Standby Level Networked Delay *(Webex Desk)*

Standby Level Networked Mode *(Webex Desk)*

UserInterface CustomMessage *(Boards, Webex Desk)*

UserInterface Features Call JoinGoogleMeet *(Boards, Codec Plus, Codec Pro, Desk Pro, Desk Limited Edition, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit, Room Kit Mini, Room Panorama, Room 70 Panorama)*

UserInterface Features Call VideoMute *(Desk Pro, Desk Limited Edition, Webex Desk)*

UserInterface LedControl Mode *(All products)*

UserInterface Theme Name *(All products)*

WebEngine Features LocalWebAppManagement *(Boards, Desk Pro, Desk Limited Edition, Webex Desk)*

Configurations that are removed

Audio Output Ethernet [1] Mode *(Room Panorama)*

Audio KeyClickDetector Attenuate *(All products)*

Audio KeyClickDetector Enabled *(All products)*

SIP Turn DiscoverMode *(All products)*

SIP Turn DropRflx *(All products)*

Configurations that are modified

Audio Input Microphone [2..3] Level *(Room 55, Room Kit)*
OLD: Integer (0..26)
NEW: Integer (0..24)

Audio Microphones NoiseRemoval Mode *(All products)*
OLD: Disabled/Manual
NEW: Disabled/Enabled/Manual

Audio Output Line [1..6] Level *(Codec Pro, Room 70 G2, Room Panorama, Room 70 Panorama)*
OLD: Default: 0
NEW: Default: -4

Audio USB Mode *(Room Kit Mini)*
OLD: Off/SpeakerAndMicrophone
NEW: AdditionalMicrophone/Microphone/Off/Speaker/SpeakerAndMicrophone

Audio USB Mode *(Desk Pro, Desk Limited Edition, Room 55, Room Kit)*
OLD: Off/SpeakerAndMicrophone
NEW: Microphone/Off/Speaker/SpeakerAndMicrophone

Cameras Camera [1..7] Focus Mode *(Codec Pro)*
OLD: Auto/Manual
NEW: Auto/AutoLimited/Manual

What’s new (page 4 of 6)

Configurations that are modified *(continued)*

For the following configurations: [1]

Network [1] DNS Domain Name

Network [1] DNS Server [1..3] Address

Network [1] IEEE8021X *

Network [1] IPStack

Network [1] IPv4 *

Network [1] IPv6 *

Network [1] MTU

Network [1] QoS *

Network [1] RemoteAccess Allow

Network [1] TrafficControl Mode

Network [1] VLAN Voice *

NetworkServices HTTP Proxy *

The user role was changed as follows on all products:

OLD: User role: Admin, User
NEW: User role: Admin

NetworkServices Websocket *(All products)*

OLD: Default: Off
NEW: Default: FollowHTTPService

Standby Control *(Room Panorama, Room 70 Panorama)*

OLD: Off/On
NEW: On

UserInteraction RaiseHand CMS *(All products)*

OLD: Default: True
NEW: Default: False

UserInterface CustomMessage *(All products)*

OLD: String (0, 128)
NEW: String (0, 256)

Video Input Connector [2..3] Name *(Room 55)*

OLD: Default:
NEW: Default: Connector 2: “PC 1 (HDMI)”, Connector 3: “PC 2 (HDMI)”

---

[1] <path> * means that the change applies to all configurations starting with <path>.

What’s new (page 5 of 6)

New features and improvements in RoomOS 10.3

New product

- Cisco Webex Desk Limited Edition

Administrator Guide restructuring *(All Products)*

The Cisco Webex device Administrator Guides have been reorganized with a new structure and look in this release. Instead of an individual guide per device or series, there is now one combined Administration Guide for all Cisco Webex devices running RoomOS 10.3. Additionally, some information has been moved into a new 'Physical interfaces' chapter.

It's easy to find out which devices the content on any page applies to: check the column of product labels on the left side of the page. A greyed-out label means the page does not apply to that device. Where exceptions exist to general content within a section, they are marked in the section header.

Whiteboard shape support

(Desk Pro, Desk Limited Edition, Boards)

On devices with whiteboard capability, tapping the Shapes button before you start to draw enables Shapes mode. Then, the whiteboard can recognize basic shapes like squares, circles, triangles and rectangles, and adjust the outlines as you draw them.

Share web apps in call

(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room USB, Room 55, Room 55 Dual, Room 70, Room 70 G2, Desk Pro, Desk Limited Edition, Boards)

Devices that support the web engine can now share a web view during a call. Presenters can interact with the shared web view in call, on devices that support interaction. Previewing a web view in a call prior to sharing it is not available.

Raise hand in a meeting

(Codec Pro, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70, Room 70 G2, Desk Pro, Desk Limited Edition, Boards)

During a meeting of more than two people, you can tap the new Raise Hand button on the device screen to notify the meeting host and cohosts that you have virtually raised your hand. Tapping the same button removes the notification. This feature requires CMS 3.2 or later.

In-Room booking *(All Products)*

If your Room device is linked to the cloud with Webex Edge for Devices and using the calendar service, you can now use in-room booking to extend your current meeting or book a room for a spontaneous meeting.

You can use a touch controller, Touch 10 or Room Navigator, to book an available room. If Webex Assistant is enabled, you can book the room with voice commands.

Immersive share *(Desk Pro, Desk Limited Edition)*

With Immersive Share, you can hold engaging presentations by placing yourself on top of any content on your computer. The presentation and video is sent in the content stream, so you stay in focus until you stop sharing.

Enable PII logging from touch interface *(All Products)*

You can now enable Personally Identifiable Information (PII) logging directly from the touch interface. 'PII logging mode' is available from the Settings menu under Issues and Diagnostics.

Room Analytics dashboard on web interface

(All Products)

Once you enable any Room Analytics features on your Cisco Webex Device, you'll see a Room Analytics dashboard on the device's web interface home page.

What's new (page 6 of 6)

Configuration changes in RoomOS 10.3

New Configurations

NetworkServices WifiCloud A_MPDU *(All products)*

Renamed from NetworkServices Wifi A_MPDU

RoomAnalytics ReverberationTime Interval *(All products)*

RoomAnalytics ReverberationTime Mode *(All products)*

UserInterface NameAndSiteLabels Mode *(All products)*

Video Output Webcam USBMode *(Room Kit Mini)*

Configurations that are modified

Audio KeyClickDetector Enabled *(Desk Pro)*

OLD: Default: True
NEW: Default: False

Audio Output Line [1] Channel *(Room 70 G2, Room 70 Panorama)*

OLD: Default: Left
NEW: Default: Mono

Audio Output Line [2] Channel *(Room 70 G2, Room 70 Panorama)*

OLD: Default: Right
NEW: Default: Mono

Cameras Background Enabled *(Desk Pro)*

OLD: Default: False
NEW: Default: True

Proximity Services ContentShare ToClients *(All products)*

OLD: Disabled/Enabled
NEW: Disabled

RoomReset Control *(All products)*

OLD: CameraPositionsOnly/Off/On
NEW: Off/On

Video Output Connector [1..3] CEC Mode *(Room Panorama)*

OLD: Off/On
NEW: On

Configurations that are removed

NetworkServices Wifi A_MPDU *(All products)*

Renamed to NetworkServices WifiCloud A_MPDU

Product features at a glance

Combining an unmatched video and audio experience with sophisticated design, every device in the Cisco Webex Room, Desk and Board portfolio creates a powerful collaboration solution. Rich in functionality and easily scalable, there is a Webex device for every room – from huddle spaces to boardrooms – and for personal desktops, too.

Some of the features you can expect across the Cisco Webex device portfolio include:

- Smart meetings: camera best overview, automatic framing and speaker tracking; noise reduction, join meetings easily with OBTP, Wi-Fi support, easy control with a touch controller or the Webex app.
- Smart presentations: single, dual or triple screens; wired or wireless 4k content-sharing, support for dual content sources.
- Smart rooms: automatic wakeup, people count, environmental and peripheral controls.
- Flexible registration: built for both cloud and on-premises deployment. And, you can use *Webex Edge for Devices* to link your on-premises registered devices to the Webex cloud service, and gain access to select cloud features.

The following pages contain additional details about each product, including information about features that vary from device to device.

Room Series at a glance (page 1 of 3)

Room Kit, Room Kit Mini

Cisco Webex Room Kit includes camera, codec, speakers, and microphones combined in a single device. Easy to mount, it integrates well with flat panel screens through HDMI CEC. Room Kit is designed for meeting rooms with up to seven people.

On a slightly smaller scale, **Cisco Webex Room Kit Mini** includes the same equipment and is well-suited to huddle spaces with two to five people, because of its wide 120-degree field of view. When connected to a computer, Room Kit Mini can be used as a USB camera. Room Kit Mini is also available in a bundle with Samsung Flip, thus combining the Room Kit Mini's video conferencing capabilities with the Samsung Flip's whiteboarding and content functions.

Room Kit mounted on top of a standard flat-panel display

Codec Plus, Codec Pro

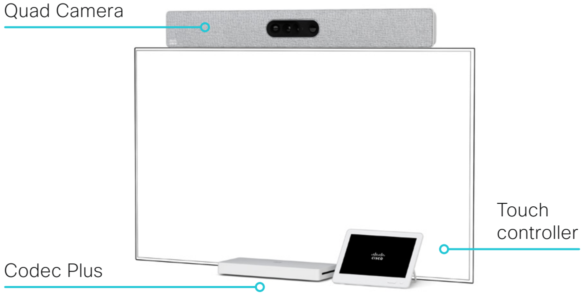
Cisco Webex Codec Plus is a powerful collaboration solution that integrates easily with flat panel screens through HDMI CEC. Codec Plus supports up to two screens, and is ideal for large, deep meeting rooms with up to 14 people.

Cisco Webex Codec Pro offers Ultra High Definition (UHD) video collaboration, and supports up to three screens. Codec Pro is excellent in very large rooms such as boardrooms and auditoriums.

Cisco offers Codec Plus and Codec Pro in Room Kit bundles combining a codec with the Cisco Quad Camera/ Precision 60 camera/PTZ-12* camera, and a Cisco touch controller user interface. Both codecs also support the SpeakerTrack 60 camera, which you can purchase separately.

---

* Codec Plus only.



Room 55

Cisco Webex Room 55 includes camera, codec, screen, speakers, and microphones - all integrated in a single device. You can choose to mount the single 55" screen on a floor stand, wheeled base, or on the wall. Perfectly designed for small to medium-sized meeting rooms, Room 55 transforms your work spaces into video collaboration hubs.

Room 55 on a floor stand

Room Series at a glance (page 2 of 3)

Room 70 G2, Room 70, Room 55 Dual

Now in its second generation, **Cisco Webex Room 70 G2** is based on the Codec Pro and comprises a quad-camera, and 70" LED single or dual 4K screen(s) with integrated speakers and microphones*. The single screen setup delivers a people-focused experience, while dual screens create compelling people- and people/content-focused experiences.

With similar functionality, the **Cisco Webex Room 70** (first generation) devices are built on the Codec Plus.

Easily scalable, and offering speaker-tracking and auto-framing capabilities, Room 70/G2 Single or Dual is an ideal all-in-one solution for large meeting rooms seating up to 14 people.

Like the Room 70 Dual (first generation) only with smaller screens, **Cisco Webex Room 55 Dual** is built on the Codec Plus, and includes a quad camera, and two 55" 4K screens with integrated speakers and microphones**. Room 55 Dual is best suited to medium or large rooms for up to 12 people.

There are three mounting kit options for each of these products: a free-standing floor stand, a wall-secured floor stand, and a wall mount kit.

Room 70 Dual G2 / Room 70 Dual on a floor stand

Room 70 Single G2 / Room 70 Sinlge on a floor stand

---

* Integrated microphones for speaker tracking only.

Room Series at a glance (page 3 of 3)

Room Panorama, Room 70 Panorama

Built for the modern C-suite, **Cisco Webex Room Panorama** transforms large meeting spaces and brings teams from around the world, face-to-face.

An all-in-one solution with the Codec Pro and Quad Camera at its core, Room Panorama features two 82-inch 8K video screens and a 65-inch 4K screen for content presentation. The camera provides panorama video, speaker-tracking, and auto-framing capabilities. The specially made integrated loudspeaker system consists of twelve main loudspeakers and four separate bass loudspeakers, driven by a sixteen channel amplifier. You won't miss a word with an integrated microphone array for accurate speaker tracking, and support for up to eight external microphones.

Cisco Webex Room 70 Panorama is a high-end collaboration system, easily scalable for medium to large conference rooms and spaces. Based on the Cisco Webex Room 70 Dual G2, Room 70 Panorama includes a powerful codec, a quad-camera, two 70-inch LED screens, and a 55-inch or 65-inch 4K screen for content presentation. Integrated loudspeakers and microphones ensure accurate speaker-tracking, and the system supports up to eight external microphones. The camera offers panorama video, speaker-tracking, and auto-framing capabilities. There are three mounting kit options: a free-standing floor stand, a wall-secured floor stand, and a wall mount kit.

Room Panorama

Room 70 Panorama,
wall mounted with 65-inch content screen above

Room 70 Panorama,
floor stand with 55-inch content screen below

Desk Series at a glance

The **Cisco Webex Desk Pro, Cisco Webex Desk Limited Edition** and **Cisco Webex Desk** devices are designed for personal desk-based collaboration, in an office or focus room that accommodates one or two people. Featuring a high resolution touchscreen, a camera with wide angle view, and an advanced audio system, the Desk Series provides an exceptional video experience as powerful as Cisco's Room Series but designed for the desktop.

With a USB-C connection for touch-redirect *(Desk Pro and Desk LE only)*, easy content sharing, and screen extension, a Desk Series device becomes your all-in-one primary monitor and collaboration device.

A Desk Pro: shown from the front, side and back

Webex Boards at a glance

Cisco Webex Boards include a 4K camera, a touch interface, and built-in microphones and speakers, all integrated with a high-resolution 4K touchscreen. Powerful audio and video conferencing devices, Webex Boards can also be used as wireless presentation screens and digital whiteboards. Collaborate easily in physical meeting rooms, and connect securely to virtual meeting spaces to facilitate a continuous workflow.

Webex Boards are available in three different screen sizes:

- **Webex Board 55 and 55S** with a 55" LED screen. Designed for huddle spaces for up to five people.
- **Webex Board 70 and 70S** with a 70" LED screen. Designed for meeting rooms for up to eight people.
- **Webex Board 85S** with a 85" LED screen. Designed for larger collaboration spaces such as auditoriums, training spaces, and classrooms.

The second generation of Webex Boards is referred to as the *S Series*, representing some minor optimizations to the hardware platform.

There are three mounting options available for Webex Boards: floor stand, wall stand, or wall mounted.

Webex Board on a floor stand

Webex Board, on a wall stand

Webex Board, wall mounted

How to administer the video conferencing device (page 1 of 5)

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

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

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

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

Tip

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

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

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

For example:

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

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

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

Access method	Notes	How to enable/disable the methods
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 · We recommend using the default baud rate, because the device may return much feedback (*SerialPort > BaudRate*) · For security reasons, you are asked to sign in by default (*SerialPort > LoginRequired*)*	*SerialPort > Mode* Restart the device for changes to take effect

* *For Boards:* The *SerialPort > LoginRequired* setting is on only available on Board 55S, 70S, and 85S. You always have to sign in on Board 55 and 70.

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

How to administer the video conferencing device (page 2 of 5)

The web interface of the device

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

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

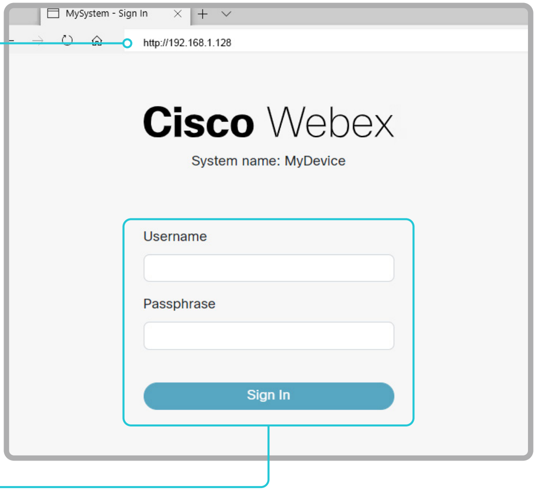
We recommend that you use the latest release of one of the major web browsers. *

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*.

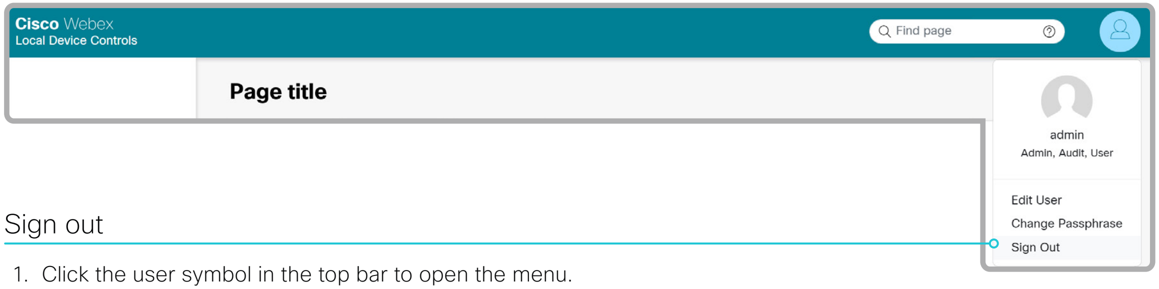

MySystem - Sign In
http://192.168.1.128
Cisco Webex
System name: MyDevice
Username
Passphrase
Sign In

Sign in

Enter user name and passphrase for the device 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.


Cisco Webex
Local Device Controls
Find page
Page title
admin
Admin, Audit, User
Edit User
Change Passphrase
Sign Out

Sign out

1. Click the user symbol in the top bar to open the menu.
2. Click *Sign Out*.

---

* Internet Explorer is not supported.

How to administer the video conferencing device (page 3 of 5)

How the web interface is organized

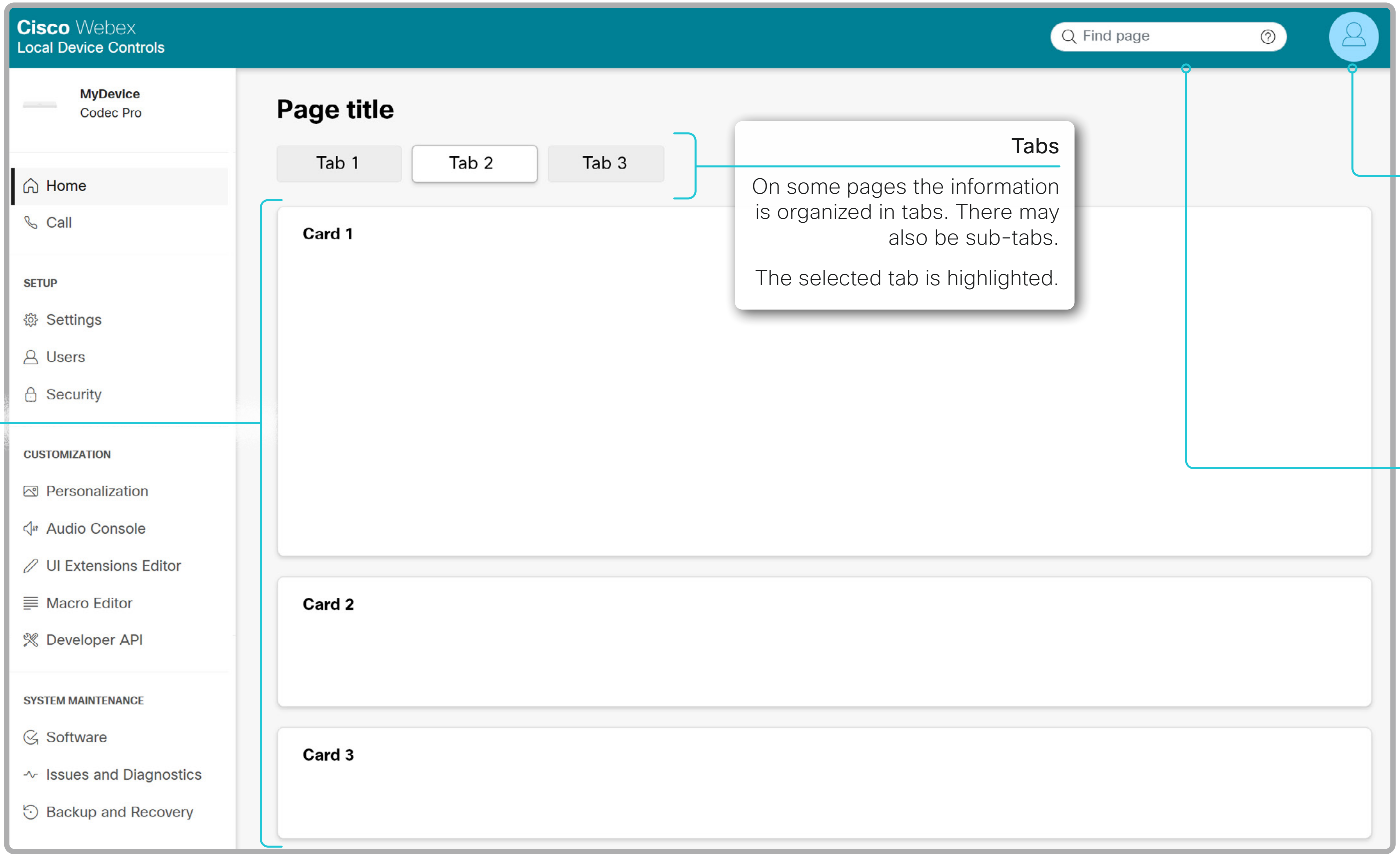
Select pages or topics from the menu at the left side. There is a search field in the top bar to help you find the page you are searching for.

Which pages are present depends on:

- Device type and service registration (Webex, Cisco UCM, VCS, Webex Edge for Devices)
- Connected peripherals and set-up
- Roles and access rights of the user that is signed in

This means that some of the menu entries shown in the illustration below may not be present on your device.

Read more about user administration, user roles and access rights in the ▶ User administration chapter.


Cisco Webex
Local Device Controls
Find page
MyDevice
Codec Pro
Home
Call
SETUP
Settings
Users
Security
CUSTOMIZATION
Personalization
Audio Console
UI Extensions Editor
Macro Editor
Developer API
SYSTEM MAINTENANCE
Software
Issues and Diagnostics
Backup and Recovery
Page title
Tab 1
Tab 2
Tab 3
Card 1
Card 2
Card 3

Device name and type

Main menu

Click an item to open a page.

Cards

The information on a page, tab, or sub-tab, may be further grouped in cards.

Tabs

On some pages the information is organized in tabs. There may also be sub-tabs.

The selected tab is highlighted.

The user menu

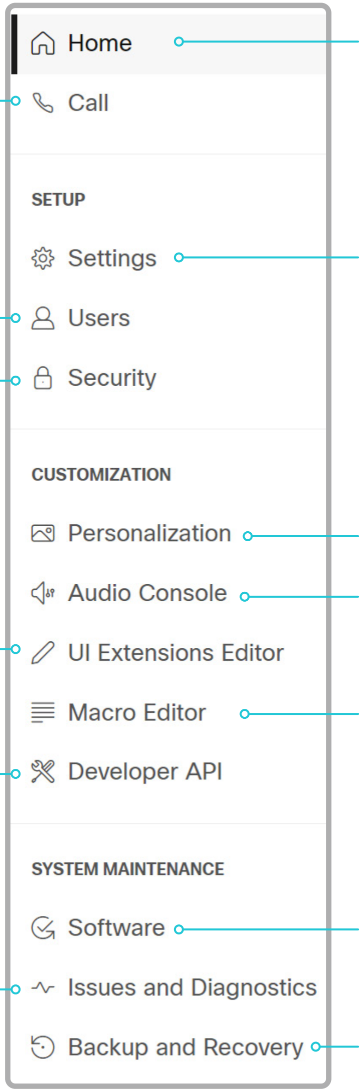
Click the symbol to show who is signed in. You can also edit the user settings, change your password, and sign out.

Search field

Use this field to search for a page. Suggestions for relevant pages appear when you start typing. When you click on one of them, the corresponding page opens.

How to administer the video conferencing device (page 4 of 5)

The main menu of the web interface



Lists general information such as IP address, MAC address, serial number, active network interface, software version, issues, registration status, utilization and environment data, and more.

Opens a page where you can set up a call from the device. You can change the camera position, mute the microphones, adjust the volume, change layouts, and check the call details.

Opens a page with access to:

- Device configurations and statuses.
- Predefined room type templates. *(Only for Codec Plus, Codec Pro, Room 55 Dual, Room 70, and Room 70 G2)*
- Details about cameras, screens, microphones, and other inputs, outputs, and peripherals.
- Setting up and enabling presenter tracking if you have a camera that supports the feature. *(Only for Codec Plus, Codec Pro, Room 55 Dual, Room 70, and Room 70 G2)*
- Setting up an SMPT server so that you can share whiteboards and annotations via email. *(Only for Webex Desk, Desk Pro, Desk Limited Edition, and Boards)*

Opens a page where you can add, edit, or delete users, or change a users passphrase. You can also create a remote support user from this page.

Opens a page where you can upload and view certificates that are required to communicate with different services and back-ends. You can also create a sign-in banner, and choose which system components to reset automatically when restarting the device.

Opens a page where you can personalize the device by adding branding elements or other background images, selecting a ringtone, and creating a local contacts list (favorites).

Opens the Audio Console, which provides a graphical interface that allows advanced customization of audio features. [1]

Opens the UI Extensions Editor, which allows you to create custom UI panels and action buttons.

Opens the Macro Editor, which allows you to create snippets of code (macros) that automates or customizes the behavior of your device. [2]

Opens a page where you can view the device's XML files, and execute commands and configurations.

Opens a page where you can install new software[3] and option keys. You can also change the product key; only change the product key if you are directed to do so by a Cisco technical support representative.

Opens a page where you can look at active diagnostics messages, download logs, and create screenshots of the user interface and on-screen messages and indicators.

Opens a page where you can backup and restore information on your device, such as branding elements, favorites list, UI extensions, macros, the sign in banner, and configurations. You can also swap to the previous software image, factory reset, restart, or shut down the device.

---

[1] The Audio Console is available only for Codec Pro, Room 70 G2, Room Panorama, and Room 70 Panorama.

[2] The former startup script feature is deprecated and removed. We recommend you to use macros instead.

[3] Not available for cloud registered devices.

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 RoomOS 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.

For Boards

If you have connected a touch controller to the board, the two devices operate independently in this context. If you unlock the settings by signing in on one of them, it has no effect on the other.

Touch controllers

Controlling your device with the external interface unit

Throughout this guide we refer to ‘touch controllers’ – external interface units you physically connect or remotely pair to video conferencing devices, in order to easily control the device by touch. Touch controllers provide instant access to everything from meetings and content to contacts and directories.

At present there are three external interface units available, all referred to interchangeably as ‘touch controllers’:

- Cisco Webex Room Navigator
- Cisco Touch 10
- Cisco TelePresence Touch 10

In addition to controlling your meeting experience on a video conferencing device, it's also possible to use touch controllers to control some room amenities like lighting, dividers, and curtains. The Room Navigator also offers environmental sensors for monitoring things like air quality and temperature.

Touch controllers can be connected directly to a device or remotely paired to it when plugged into a (PoE) network. Only one cable is needed to power the unit and network access.

See the ► Connect the touch controller chapter about how to connect a touch controller to the video conferencing device.

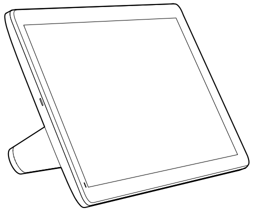
Compatibility with video conferencing devices

Room Navigator supports:

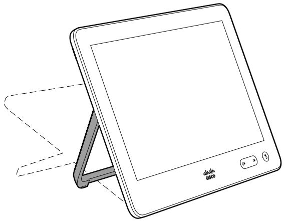
- Room Series
- Boards 55S, 70S, and 85S

Touch 10 and TelePresence Touch 10 support:

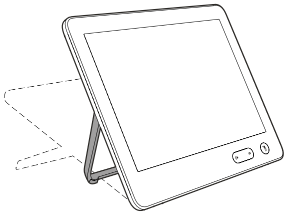
- Room Series
- Boards



Cisco Webex Room Navigator
(launched early 2021)



Cisco Touch 10
(second version, launched late 2017)



Cisco TelePresence Touch 10
(first version)

Chapter 2

Configuration

User administration

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

The default user account

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

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

Read how to set the passphrase in the ▶ Change the device passphrase chapter.

Create a new user account

1. Sign in to the web interface and go to *Users*.
2. Click *Create 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*.

   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 go to *Users*.
2. Click the appropriate user in the list.
3. Choose user roles, set the status to **Acitve** 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 *Save*.

   Use the *Back* button to leave without making any changes.

Change the passphrase

1. Sign in to the web interface and go to *Users*.
2. Click the appropriate user in the list.
3. Find the *Passphrase* card and 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 go to *Users*.
2. Click the appropriate user in the list.
3. Find the *Delete* card, 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

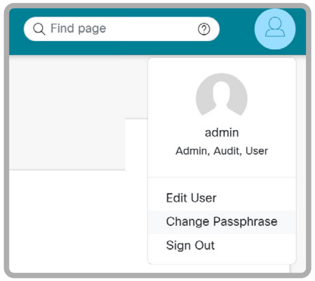
You can create many user accounts for the device.

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, and click the user symbol in the top bar to open the menu.
2. Click *Change Passphrase*.
3. Enter the current passphrase and new passphrase in the input fields, and click *Change Passphrase*.

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.

For Boards: If you are using a touch panel with your Board, you have access to the Settings menu both on the board itself and on the touch panel. In this context, the board and the touch panel operate independently. If you unlock the settings by signing in on one of them, it has no effect on the other.

Lock down the Settings menu

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
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.

Unlock the Settings menu

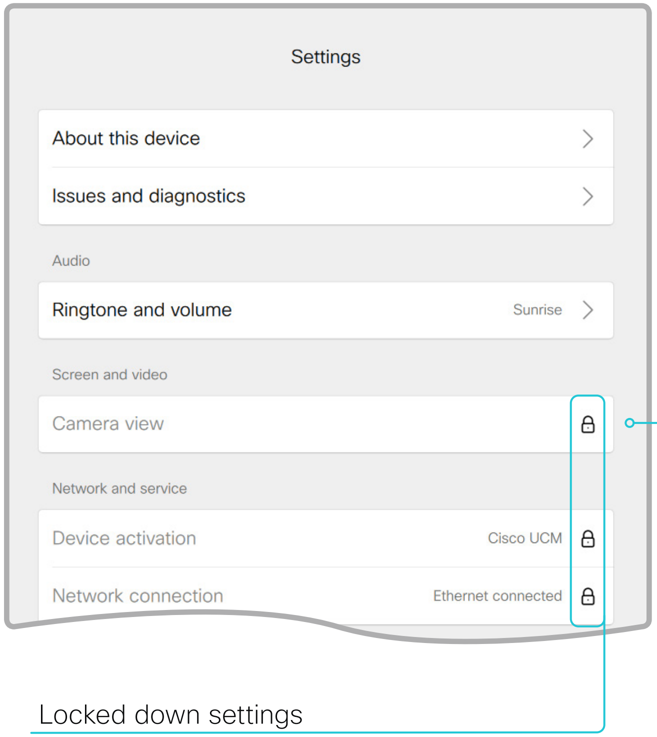
1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
2. Go to *UserInterface > SettingsMenu > Mode*, and ***select*** **Unlocked**.
3. Click *Save* for the change to take effect.

   Now all users have access to the complete Settings menu on the user interface.

The Settings menu on the user interface

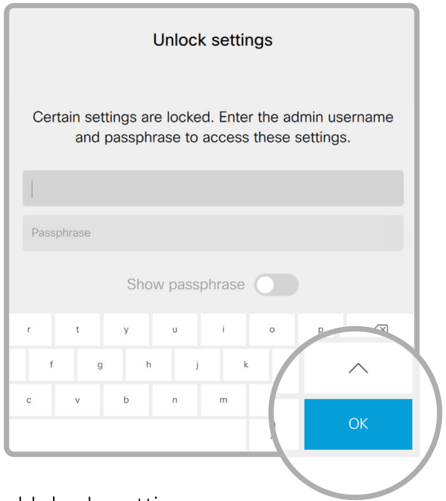
If the menu is locked down, you must sign in to access the device-critical settings.

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


Settings
About this device
Issues and diagnostics
Audio
Ringtone and volume
Sunrise
Screen and video
Camera view
Network and service
Device activation
Cisco UCM
Network connection
Ethernet connected

Locked down settings

Locked down settings are marked with a padlock.


Unlock settings
Passphrase
Show passphrase
r
t
y
u
i
o
p
f
g
h
j
k
c
v
b
n
m
OK

Certain settings are locked. Enter the admin username and passphrase to access these settings.

Unlock settings

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

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

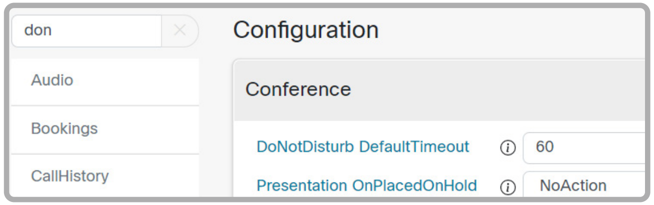
Device configuration

Sign in to the web interface, go to *Settings*, and select *Configurations*.

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.



don

Configuration

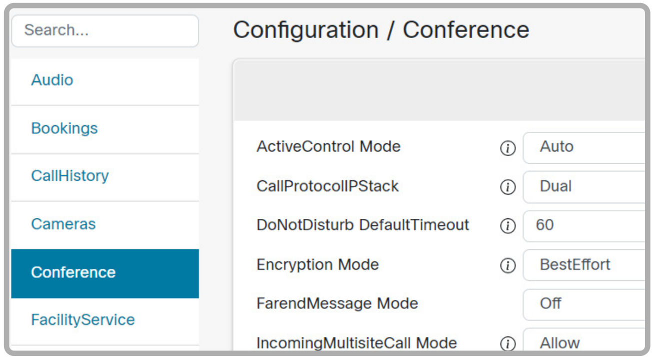
Audio
Bookings
CallHistory

Conference

DoNotDisturb DefaultTimeout: 60
Presentation OnPlacedOnHold: NoAction

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.



Search...

Configuration / Conference

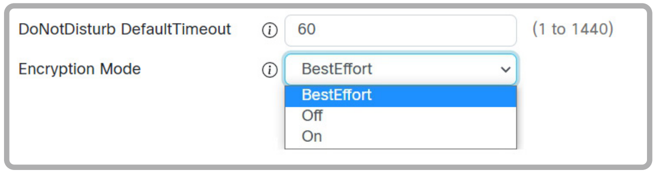
Audio
Bookings
CallHistory
Cameras
Conference
FacilityService

ActiveControl Mode: Auto
CallProtocolIPStack: Dual
DoNotDisturb DefaultTimeout: 60
Encryption Mode: BestEffort
FarendMessage Mode: Off
IncomingMultisiteCall Mode: Allow

Change a device setting

Check the value space

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

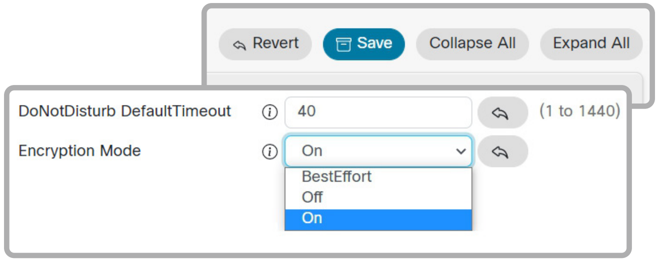


DoNotDisturb DefaultTimeout: 60 (1 to 1440)
Encryption Mode: BestEffort
BestEffort
Off
On

Change a value

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

   Use the *Revert* buttons (↶) if you don't want to make any changes.



DoNotDisturb DefaultTimeout: 40 (1 to 1440)
Encryption Mode: On
BestEffort
Off
On

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

About device settings

All device settings can be changed from the web interface.

Each device setting is described in the ▶ Device settings chapter.

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

You can read more about user administration and user roles in the ▶ User administration chapter.

Add a sign in banner

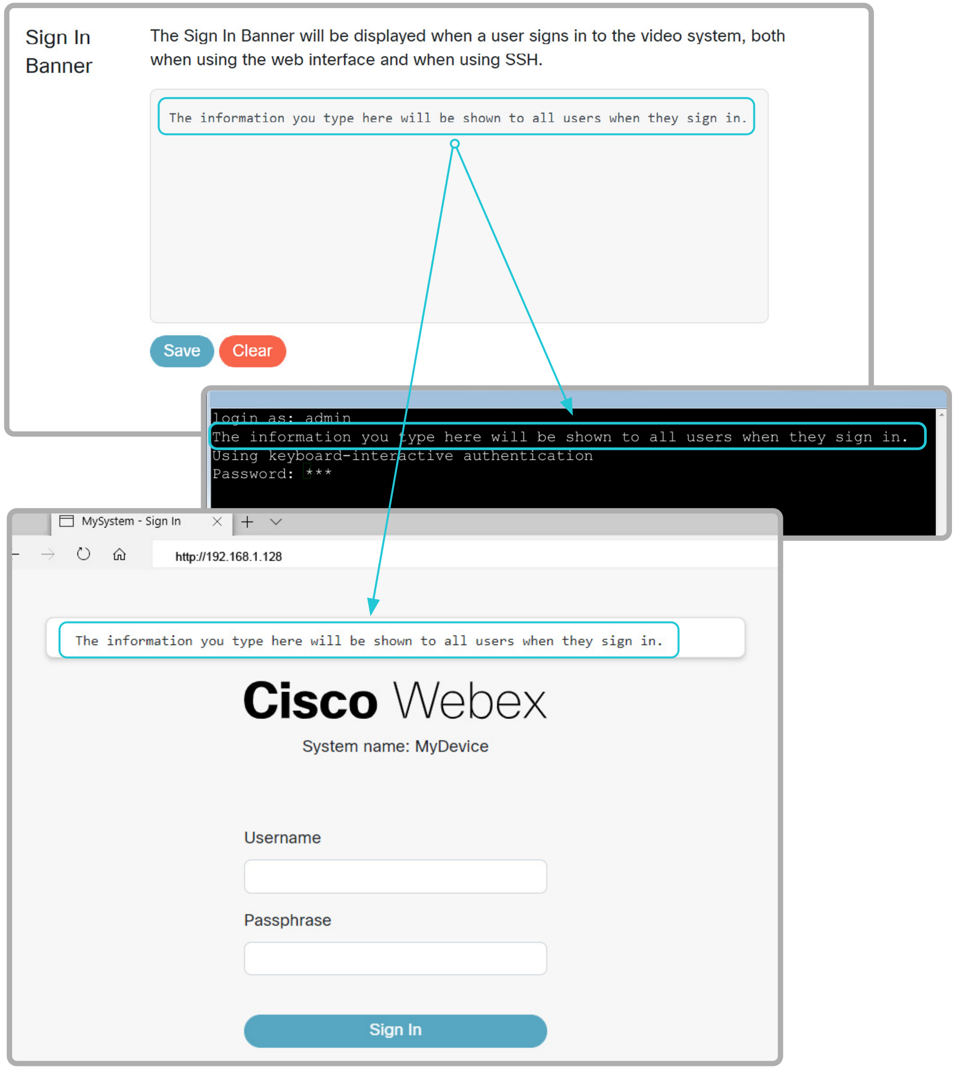
Sign in to the web interface, go to *Security*, and select *Sign-in Banner*.

Add a 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.

Delete a sign in banner

- Click *Clear* to remove a sign in banner.



Sign In Banner

The Sign In Banner will be displayed when a user signs in to the video system, both when using the web interface and when using SSH.

The information you type here will be shown to all users when they sign in.

```
login as: admin
The information you type here will be shown to all users when they sign in.
Using keyboard-interactive authentication
Password: ***
```

The information you type here will be shown to all users when they sign in.

System name: MyDevice

Username

Passphrase

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
```

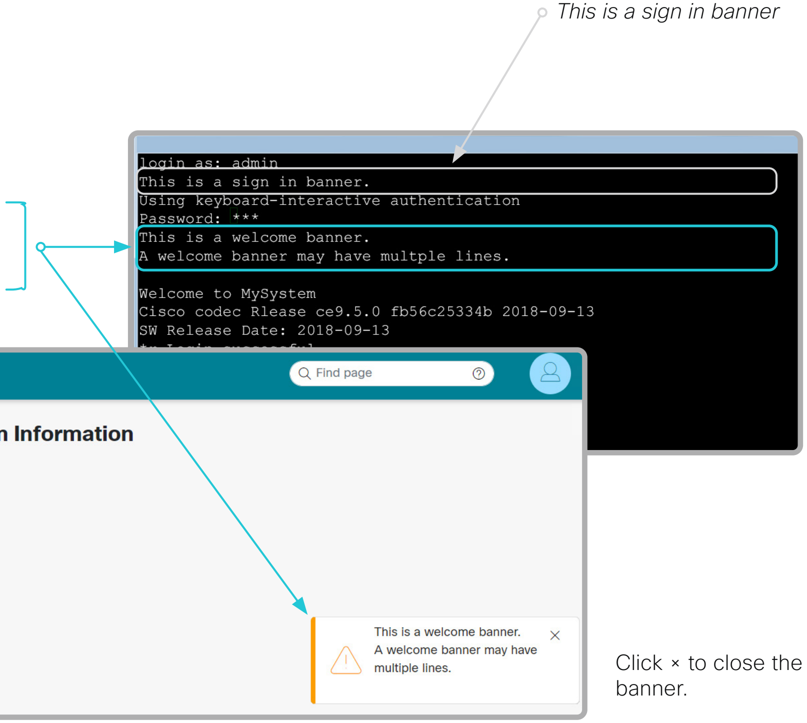
This is a multiline command. Anything you input after you issue the command, is input to the command (including line breaks). Finish the input with a separate line containing just a period ending with a line break.

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>
```



This is a sign in banner

```
login as: admin
This is a sign in banner.
Using keyboard-interactive authentication
Password: ***
This is a welcome banner.
A welcome banner may have multple lines.

Welcome to MySystem
Cisco codec Rlease ce9.5.0 fb56c25334b 2018-09-13
SW Release Date: 2018-09-13
```

System Information

This is a welcome banner.
A welcome banner may have multiple lines.

Click × to close the banner.

About welcome banner

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

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

The maximum size is: 4 kByte

Welcome banner versus sign in banner

Sign in banner:

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

Welcome banner:

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

Manage the service certificates of the device

Sign in to the web interface and go to *Security*. Select *Certificates*, and open the *Services* sub-tab.

You need the following files:

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

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

Add a certificate

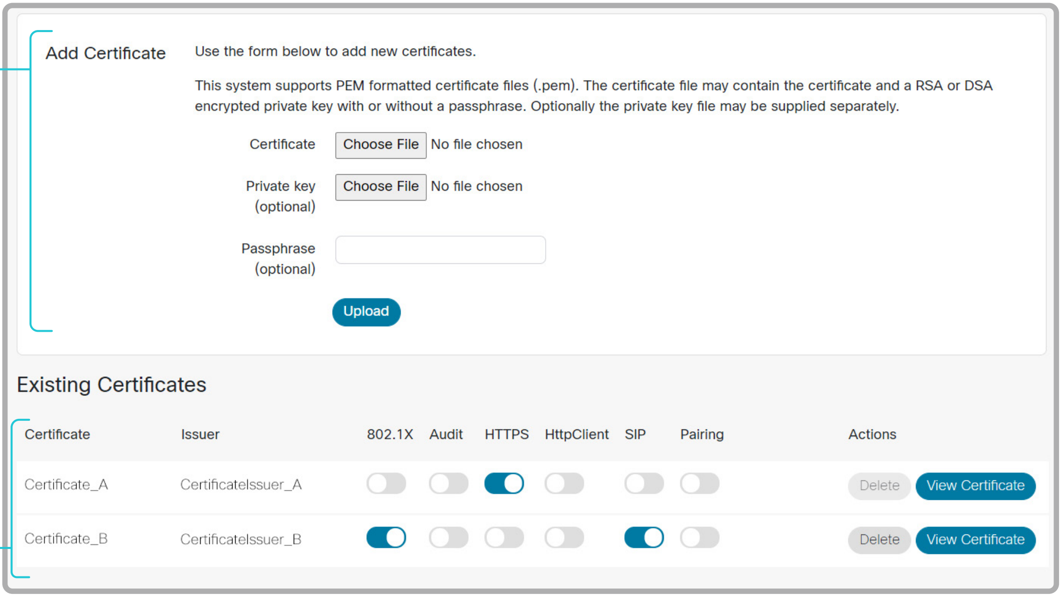
1. Browse to find the Certificate file and Private key file (optional) on your computer.
2. Fill in the *Passphrase* if required.
3. Click *Upload* to store the certificate on the device.

   Only certificates with a validity period of up to 10 years are accepted.

Enable or disable, view or delete a certificate

Use the toggle buttons to enable or disable a certificate for the different services.

Use the corresponding button to view or delete a certificate.



Add Certificate

Use the form below to add new certificates.

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

Certificate: Choose File No file chosen

Private key (optional): Choose File No file chosen

Passphrase (optional):

Upload

Existing Certificates

Certificate	Issuer	802.1X	Audit	HTTPS	HttpClient	SIP	Pairing	Actions
Certificate_A	CertificateIssuer_A	○	○	●	○	○	○	Delete View Certificate
Certificate_B	CertificateIssuer_B	●	○	○	○	●	○	Delete View Certificate

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

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, HTTP client, 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.

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

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

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

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

The CA certificate lists

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

- Sign in to the web interface, go to *Security*, and select *Certificates*. 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, such as HTTPS, SMTP ***(only Boards, Webex Desk, Desk Pro, and Desk Limited Edition)***, and 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).
- *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.

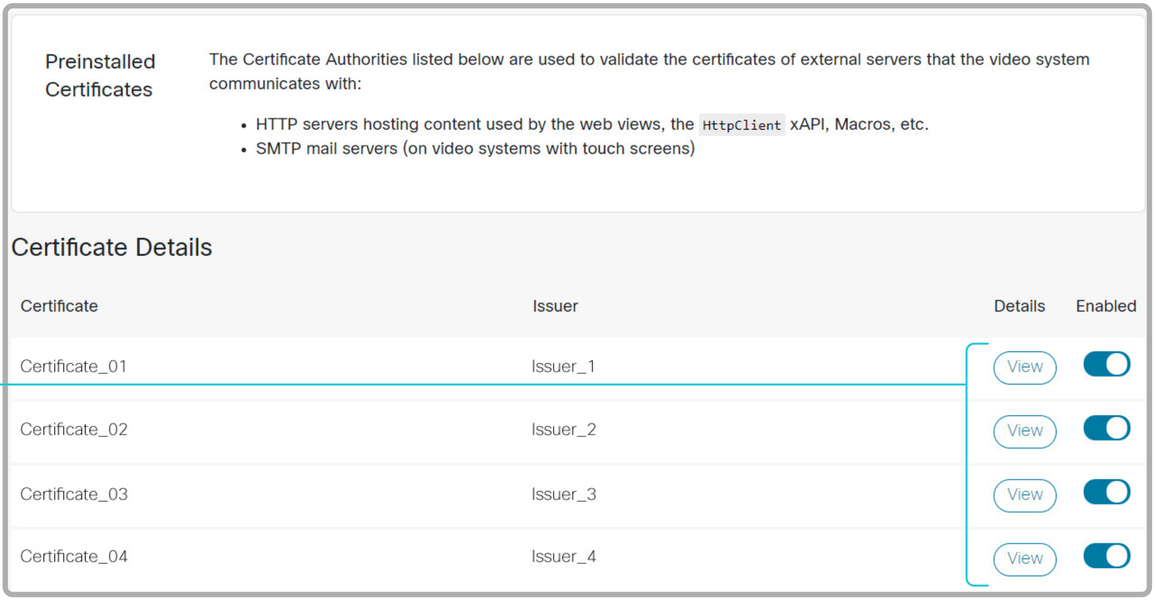
Manage pre-installed CA certificates for external servers

Sign in to the web interface and go to *Security*. Select *Certificates*, and open the *Preinstalled* sub-tab.

View, enable or disable certificates

Use the *View* button to see certificate details.

Use the toggle button to enable or disable a certificate.



Preinstalled Certificates

The Certificate Authorities listed below are used to validate the certificates of external servers that the video system communicates with:

- HTTP servers hosting content used by the web views, the `HttpClient` xAPI, Macros, etc.
- SMTP mail servers (on video systems with touch screens)

Certificate Details

Certificate	Issuer	Details	Enabled
Certificate_01	Issuer_1	View	●
Certificate_02	Issuer_2	View	●
Certificate_03	Issuer_3	View	●
Certificate_04	Issuer_4	View	●

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.

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:

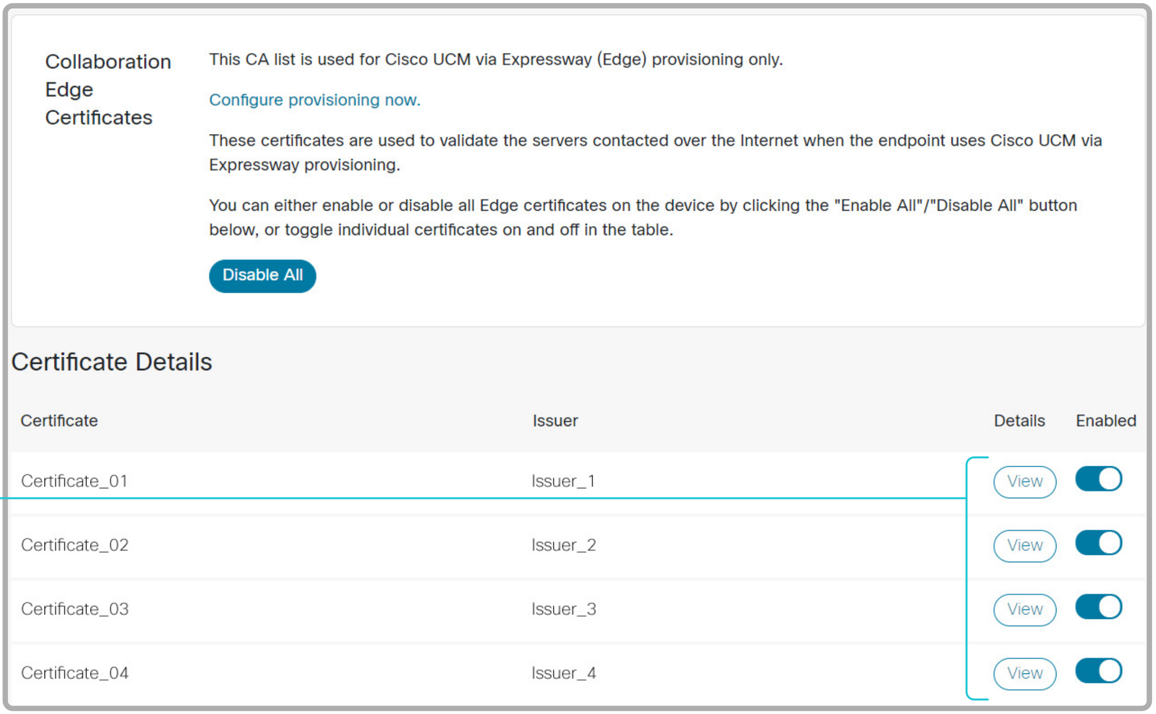
- HTTP servers that host content used by the HttpClient API or macros
- Provisioning servers
- Phone book servers
- Syslog servers (for external logging)
- SMTP mail servers *(only Boards, Webex Desk, and Desk Pro)*
- Servers and services used by the Cisco Webex cloud

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

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

Manage pre-installed CA certificates for CUCM via Expressway provisioning

Sign in to the web interface and go to *Security*. Select *Certificates*, and open the *Collaboration Edge* sub-tab.



Collaboration Edge Certificates

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

Configure provisioning now.

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

You can either enable or disable all Edge certificates on the device by clicking the "Enable All"/"Disable All" button below, or toggle individual certificates on and off in the table.

Disable All

Certificate Details

Certificate	Issuer	Details	Enabled
Certificate_01	Issuer_1	View	●
Certificate_02	Issuer_2	View	●
Certificate_03	Issuer_3	View	●
Certificate_04	Issuer_4	View	●

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

View, enable or disable certificates

Use the *View* button to see certificate details.

Use the toggle button to enable or disable a certificate.

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

Refer to the ► Upload a CA certificate to the device chapter how to update the list of trusted CA certificates.

Pre-installed CA certificates for CUCM via Expressway

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

Only Cisco Expressway infrastructure certificates are checked against this list.

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

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

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

Upload a CA certificate to the device

Sign in to the web interface and go to *Security*. Select *Certificates*, and open the *Custom* sub-tab.

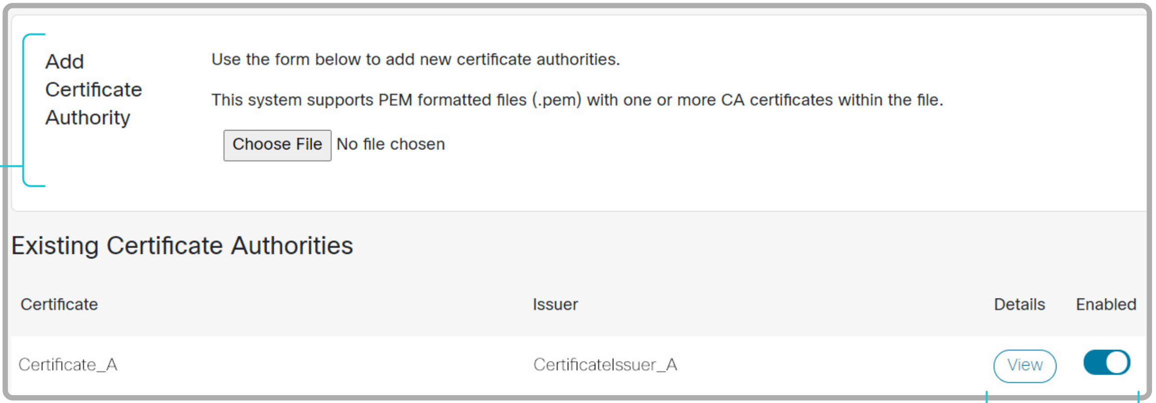
You need the following file:

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

Upload a list of CA certificates

1. Browse to find the file containing the CA certificates on your computer (file format: .PEM).
2. Click *Upload* to store the new CA certificates on the device.

   The button appears when you have chosen a file.



Add Certificate Authority

Use the form below to add new certificate authorities.

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

Choose File No file chosen

Existing Certificate Authorities

Certificate	Issuer	Details	Enabled
Certificate_A	CertificateIssuer_A	View	●

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

View, enable or disable certificates

Use the *View* button to see certificate details.

Use the toggle button to enable or disable a certificate.

⚠ 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)
- SMTP mail servers ***(only Boards and Desk Pro)***
- Cisco Expressway infrastructure
- Servers and services used by the Cisco Webex cloud

Set up secure audit logging

Sign in to the web interface, go to *Settings*, and select *Configurations*.

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

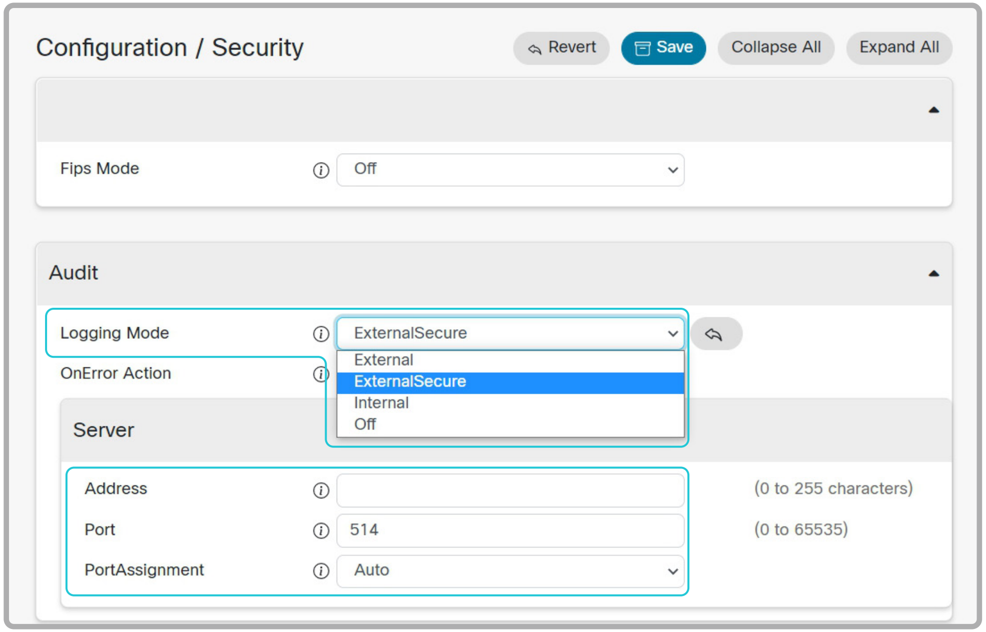
Refer to the ▶ Upload a CA certificate to the device chapter how to update the list.

1. Find the *Security > Audit > Server* settings, and enter the *Address* of the audit server.

   If you set *PortAssignment* to **Manual**, you must also enter a *Port* number for the audit server.

2. Set *Security > Audit > Logging > Mode* to **ExternalSecure**.

3. Click *Save* for the change to take effect.



Configuration / Security

Fips Mode: Off

Audit

Logging Mode: ExternalSecure

OnError Action

Server

Address: (0 to 255 characters)

Port: 514 (0 to 65535)

PortAssignment: Auto

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

This chapter is only relevant for devices that are registered to a Cisco Unified Communications Manager (CUCM).

Sign in to the web interface and go to *Security*. Select *Certificates*, and open the *Unified CM* sub-tab.

Delete the CUCM trust lists

Click *Delete CTL/ITL* to remove the trust lists.

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

In these cases, you must still delete them:

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

Overview of trust list fingerprints and certificates

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

This information may be useful for troubleshooting.

Change the persistency mode

Sign in to the web interface, go to *Security*, and select *Persistency Settings*.

Check the persistency status

The active radio buttons show the current persistency status of the device.

Alternatively, you can navigate to *Settings*, select *Statuses*, and check the *Security > 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 *Apply*.

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

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

Persistency mode

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

Generally, we recommend you NOT to change the persistency settings. Only change to **Non-persistent** mode if you have to prevent users from being able to see or traceback to any logged information from the previous session

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

- Device configuration changes
- Information about placed and reveived 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 up an SMTP email server

By setting up an SMTP server connection, the users of the video conferencing device can share their whiteboards and annotations via email with people inside or outside your organization.

It is possible to set up the server manually, but we strongly recommend you to use the setup wizard. Then you can test the connection while setting it up, and you get guidance how to upload server certificates if needed.

Enable sharing via email

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
2. Go to *NetworkServices > SMTP > Mode*. Sharing via email is only allowed if Mode is **On**.

Use the wizard to set up the server Recommended

1. Sign in to the web interface, go to *Settings*, and select *Send Whiteboard to Email*.
2. Click *Start Wizard* and enter the server address, encryption method, and port number.
3. Click *Test Connection...*.

   If everything is fine, click *OK* to continue the wizard.

   If certificates are missing, click *Reconfigure* and follow the wizard instructions to upload the required certificates to the device.
4. Enter the email address from where to send whiteboards or annotations.
5. Fill in the username and password fields if the SMTP server requires authentication and the encryption method is TLS or STARTTLS.
6. Select *Verify and Save* to finish the server setup wizard.

   Provided that *NetworkServices > SMTP > Mode* is **On**, the device is now ready to send whiteboards and annotations by email.

If you choose *Manual Configuration* instead of starting the wizard, fill in the same fields as described above and select *Verify and Save*.

Set up the server from the configurations page

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
2. Go to *NetworkServices > SMTP* and set the *Server*, *Security* (encryption method), *Port*, *From*, *Username*, and *Password* settings.
3. If required, upload CA certificates to the device as described in the ► Upload a CA certificate to the device chapter.

Encryption methods and certificates

You must choose an encryption method that the email server supports.

Both the TLS and STARTTLS encryption methods require a server certificate. The device doesn't allow connections where the certificate of the SMTP server cannot be validated. Ignoring the certificate check is not an option.

Most often the server certificate can be validated using the CA list that is *pre-installed* on the device. If not, you have to upload the required certificates to the device yourself. Certificates that you upload yourself are added to the list of *Custom* certificates.

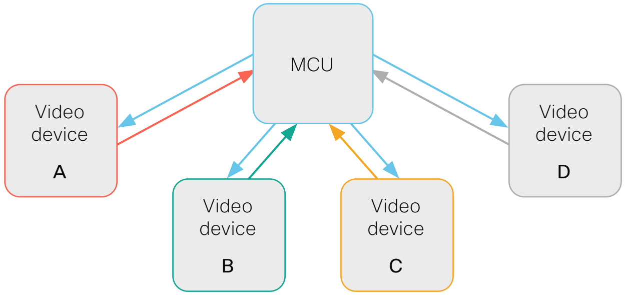
Read more about CA lists in the ► Manage the lists of trusted certificate authorities - CAs chapter.

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

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

Centralized conference infrastructure

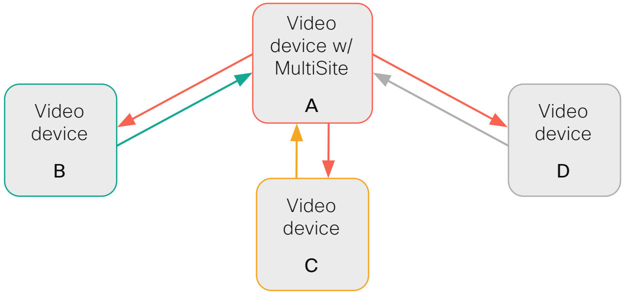
Most solutions are based on a centralized conference infrastructure, i.e. an MCU (multipoint control unit) [1].



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

Local conference resources - MultiSite

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



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

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

The maximum number of participants supported by MultiSite is:

- Codec Pro, Room 70 G2, Room Panorama, Room 70 Panorama, Webex Desk, Desk Pro, Desk Limited Edition: Five participants (yourself included)
- Other products: Four participants (yourself included)

Multipoint configuration

Use the *Conference > Multipoint > Mode* setting to decide how to handle multipoint conferences. This setting takes the following values:

- Auto
- CUCMMediaResourceGroupList
- MultiSite
- Off

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

---

[1] MCU - multipoint control unit, also called video-conferencing gateway or bridge.

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

Conference Multipoint Mode setting	MultiSite option key	Remote device type [2]	Add participant behavior	
Off	N/A	MCU	Direct Remote Add	· 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.
		Video device	Plus one audio	· You can add one extra participant on audio-only. · You cannot add more participants on video.
CUCM-MediaResource-GroupList	N/A	Video device	Consultative Add	· 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 particiant 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.
MultiSite [3]	Yes	N/A	Local MultiSite [4]	· There is an *Add* button in the UI, and you can call the next participant directly. · You can keep adding participants until you reach the maximum number for the device.
	No	N/A	Plus one audio	· You can add one extra participant on audio-only. · You cannot add more participants on video.
Auto	Yes	MCU	Direct Remote Add	· 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.
		Video device	Local MultiSite without cascading [5]	· There is an *Add* button in the UI, and you can call the next participant directly. · 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.
	No	MCU	Direct Remote Add	· 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.
		Video device	Plus one audio	· You can add one extra participant on audio-only. · You cannot add more participants on video.

---

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

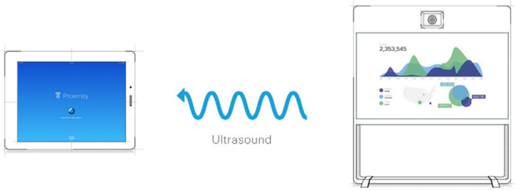
[3] MultiSite is disabled automatically in a conference that is using multi stream. This means that you cannot add any new participants to the conference using the Add button in the UI (neither video nor audio-only participants).

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

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

Cisco Proximity allows users to share content from their lap tops and control the video conferencing device from their mobile device when they are 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.



Number of Proximity connections

The maximum number of simultaneous Proximity connections is:

- 30

The client warns new users if the maximum number of connections has been reached.

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)

Wireless share from a laptop:

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

Place calls and control the video conferencing device

Wireless share from a mobile device

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 2 of 4)

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 Panorama, Room 70 Panorama, Room 55, Room 55 Dual, Room Kit, Room Kit Mini, and Room Kit Plus:

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

Webex Desk, Desk Pro and Desk Limited Edition:

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

Codec Plus and Codec Pro:

- 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

Webex Desk, Desk Pro and Desk Limited Edition:

You can always use a headset with these devices because:

- The devices have a dedicated headset output, on which we never emit ultrasound.

Room 70, Room 70 G2, Room Panorama, Room 70 Panorama, Room 55 Dual, Room Kit Plus, Codec Plus, Codec Pro, and Boards:

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

Room 55, Room Kit, and Room Kit Mini:

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

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

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

Enable Proximity services

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.

2. Go to *Proximity > Mode* to switch Proximity **On**.

   Proximity is Off by default on the following products: Codec Plus, Codec Pro, Webex Desk, Desk Pro, and Desk Limited Edition. For other products Proximity is On by default.

   When Proximity in On, the video conferencing device sends ultrasound pairing messages.

3. Enable the services you want to allow. *Wireless share from a desktop client* is enabled by default.

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

   Place calls and control the video conferencing device:

   - Go to *Proximity > Services > CallControl* 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

Default behavior

Codec Plus and Codec Pro: The Proximity feature is switched **Off** by default, because the use of third-party speakers may need additional testing for Proximity to work as expected. In rare cases the ultrasound may cause audio artifacts. If so, consider to decrease the maximum ultrasound volume with the *Audio > Ultrasound > MaxVolume* setting.

Desk Pro and Desk Limited Edition: The Proximity feature is switched **Off** by default, because the Desk products are often deployed in open offices with several devices close to each other. In such environments, pairing could be unstable. In general, Proximity should be switched **On** only on one device per room.

Other products: The Proximity feature is switched **On** by default.

Ultrasound

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.

Recommendation

In general, Cisco recommends - for the best user experience - that Proximity always is switched **On**.

However, for Codec Plus, Codec Pro, Webex Desk, Desk Pro, and Desk Limited Edition, it is important that you verify that Proximity is suitable in your environment and setup before you switch it 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 4 of 4)

Room considerations

Room acoustics

- Rooms with hard surfaces may cause challenges due to severe audio reflections. Acoustical treatment of meeting rooms is always highly recommended for the best meeting experience as well as Intelligent Proximity performance.
- Cisco recommends only one video 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

Note that for Desk Pro and Desk Limited Edition, the mobile devices in the room can only receive and view content when the Desk device is in a call.

Basic troubleshooting

Cannot detect devices with Proximity clients

- Check if the video conferencing device is in standby mode. Ultrasound is not transmitted if the speakers (for example a TV in standby mode) are turned off. *(only Codec Plus and Codec Pro)*
- Check the speaker volume. The volume control on a speaker itself (not the volume controlled with the remote control or touch controller) affects the ultrasound volume. If the volume is too low, the listening devices cannot detect the ultrasound pairing messages. *(only Codec Plus and Codec Pro)*
- Some Windows laptops are not able to record sound in the ultrasound frequency range (20 kHz-22 kHz). This can be due to frequency limitations with the sound card, sound driver or the internal microphone of the particular device. Refer to the Support forum for more information.
- Check *Settings > Issues and diagnostics* on the user interface, or *Maintenance > Diagnostics* on the web interface of the video conferencing device. If there are no ultrasound related Issues listed ("Unable to verify the ultrasound signal"), ultrasound pairing messages are emitted by the video conferencing device as they should. Refer to the Proximity *Support forum* for further assistance with the client detection issues.

Audio artifacts

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

Cannot share content from a laptop

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

Additional resources

Cisco Proximity site:
► https://proximity.cisco.com

Support forum:
► https://www.cisco.com/go/proximity-support

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

Video input quality settings

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

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

Optimal definition profile

The optimal definition profile should reflect the lighting conditions in the video conferencing room and the quality of the camera (video input source). The better the lighting conditions and the better the quality of the camera, the higher the optimal definition 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 pages. The resolution and frame rate must be supported by both the calling and called devices.

Threshold for sending video at 60 fps

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

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

Allowing video at 60 fps

(Applies to: Room Kit, Room Kit Mini, and Room 55)

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.

Sign in to the web interface, go to *Settings*, and select *Configurations*.

1. ***Applies to all prodcuts and connectors except Connector 1 (integrated camera) of Boards, Webex Desk, Desk Pro, Desk Limited Edition, Room Kit, Room Kit Mini, and Room 55.***

   Go to *Video > Input > Connector n > Quality* and set the video quality parameter to **Motion**.

2. Go to *Video > Input > Connector n > OptimalDefinition > Profile* and choose the preferred optimal definition profile.

3. Go to *Video > Input > Connector n > OptimalDefinition > Threshold60fps* to set the threshold below which the maximum transmitted frame rate will be 30 fps.

4. ***Applies to Room Kit, Room Kit Mini, and Room 55.***

   Go to *Cameras > Camera > Framerate* and choose whether or not to allow video at 60 fps.

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

Boards, Codec Pro, Codec Plus, Webex Desk, Desk Pro, Desk Limited Edition, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama (non-panoramic mode), and Room Panorama (non-panoramic mode)

Resolutions and frame rate [w×h@fps] obtained for different optimal definition profiles and call rates

Call rate [kbps]	H.264, max 30 fps, max 128 kbps audio bit rate			H.264, max 60 fps, max 128 kbps audio bit rate		
	Normal	*Medium*	*High*	*Normal*	*Medium*	*High*
128	320×180@30	320×180@30	512×288@30	320×180@30	512×288@20	512×288@30
256	512×288@30	640×360@30	768×448@30	512×288@30	640×360@30	512×288@60
384	640×360@30	768×448@30	768×448@30	640×360@30	512×288@60	640×360@30
512	768x448@30	1024x576@30	1024x576@30	512×288@60	640×360@60	768×448@60
768	1024×576@30	1280×720@30	1280×720@30	640×360@60	768×448@60	1024x576@60
1152	1280×720@30	1280×720@30	1280×720@30	768x448@60	1024x576@60	1280×720@60
1472	1280×720@30	1280×720@30	1920×1080@30	1024×576@60	1024x576@60	1280×720@60
1920	1280x720@30	1920x1080@30	1920x1080@30	1024×576@60	1280x720@60	1280x720@60
2560	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
3072	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
4000	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1920x1080@60	1920x1080@60
6000	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60

Codec Pro, Codec Plus, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama (non-panoramic mode), and Room Panorama (non-panoramic mode)

Resolutions and frame rate [w×h@fps] obtained for different optimal definition profiles and call rates

Call rate [kbps]	H.265, max 30 fps, max 128 kbps audio bit rate			H.265, maximum 60 fps, max 128 kbps audio bit rate		
	Normal	*Medium*	*High*	*Normal*	*Medium*	*High*
128	512×288@30	512×288@30	640×360@30	512×288@30	512×288@30	512×288@60
256	640×360@30	768×448@30	768×448@30	640×360@30	512×288@60	640×360@60
384	768×448@30	1024×576@30	1280×720@30	640×360@60	768×448@60	768×448@60
512	1024x576@30	1280x720@30	1280x720@30	640×360@60	768×448@60	1024×576@60
768	1280×720@30	1280×720@30	1920×1080@30	768×448@60	1024×576@60	1280×720@60
1152	1280×720@30	1920×1080@30	1920×1080@30	1024x576@60	1280×720@60	1280×720@60
1472	1280×720@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1280×720@60
1920	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1280x720@60	1920x1080@60
2560	1920x1080@30	1920x1080@30	1920x1080@30	1280x720@60	1920x1080@60	1920x1080@60
3072	1920x1080@30	1920x1080@30	1920x1080@30	1920x1080@60	1920x1080@60	1920x1080@60
4000	1920x1080@30	1920x1080@30	1920x1080@30	1920x1080@60	1920x1080@60	1920x1080@60
6000	1920×1080@30	1920×1080@30	1920×1080@30	1920×1080@60	1920×1080@60	1920×1080@60

Select a multi-screen background image

You can select to use a multi-screen background image for Room Panorama, Room 70 Panorama, and the dual screen versions of Room 70 and Room 70 G2. A multi-screen background image is an image that spans all the screens, and it is shown when the system is in the awake state.

The default behavior is to use a:

- 2-screen background image for Room 70 Dual and Room 70 G2 Dual
- 3-screen background image for Room Panorama and Room 70 Panorama

  For Room 70 Panorama, the content screen can be either above or below the main screens.

We recommend you NOT to use the Branding feature if you are using a multi-screen background image.

You must use the *UserInterface WallpaperBundle* API commands if you want to turn off the multi-screen background image feature or change to a different background image. You cannot do this from the touch controller or the web interface.

Check which multi-screen background images you can choose between:

```
xCommand UserInterface WallpaperBundle List
```

Change to another background image:

```
xCommand UserInterface WallpaperBundle Set Name:
"Name"
```

Turn off the multi-screen background image feature:

```
xCommand UserInterface WallpaperBundle Clear
```

16:27
BoardRoom
No ongoing meetings
Cisco Webex

Add corporate branding to the screen and touch controller (page 1 of 3)

Sign in to the web interface, go to *Personalization*, and select *Branding*.

From this page you can add your own branding elements to the video conferencing device:

- Background brand image
- Logo
- Custom message

The elements are shown when the device is in the halfwake or awake states.

The Branding feature, as described in this chapter, allows you to customize the screen appearance without compromising the overall Cisco user experience. It also applies to the touch controller for those devices that have that.

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.

Branding and Custom wall paper

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.

Branding and Multi-screen background image

(Room 70 Dual, Room 70 Dual G2, Room 70 Panorama and Room Panorama)

We recommend you not to use the Branding feature if you are using a multi-screen background image.

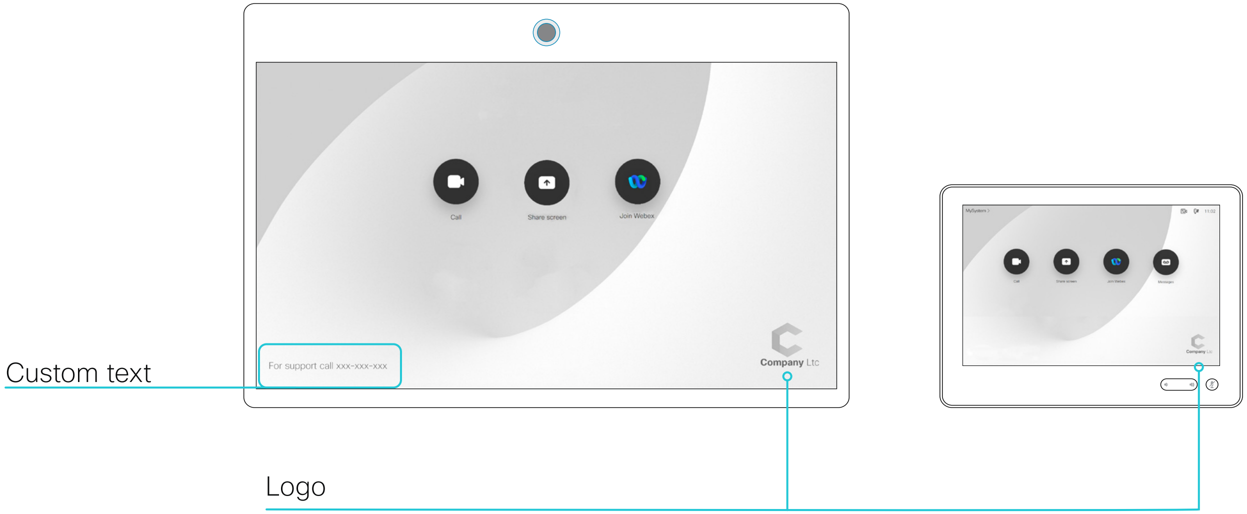
Add corporate branding to the screen and touch controller (page 2 of 3)

Branding in the awake state

In the awake state you can:

- Add a logo in the bottom right corner (screen and touch controller)
- Add custom text in the bottom left corner (*Not available for Boards)*

  The custom text is only on the screen, not on the touch controller

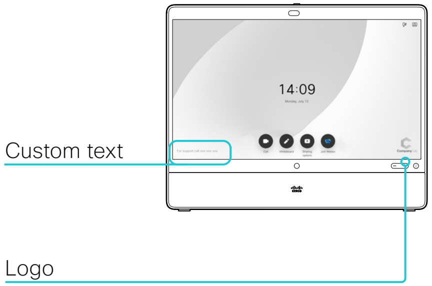

Call
Share screen
Join Webex
For support call xxx-xxx-xxx
Company Ltd
Custom text

Logo

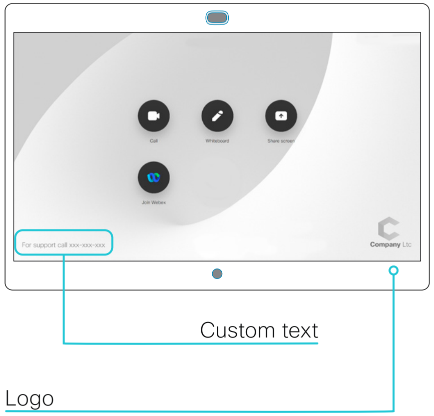
We recommend:

- 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)

Webex Desk, Desk Pro, and Desk Limited Edition


14:09
Custom text
Logo

Boards


Call
Whiteboard
Share screen
Join Webex
For support call xxx-xxx-xxx
Company Ltd
Custom text
Logo

Add corporate branding to the screen and touch controller (page 3 of 3)

Branding in the halfwake state

In halfwake state you can:

- Add a custom background (screen and touch controller)
- Add a logo in the bottom right corner (screen and touch controller

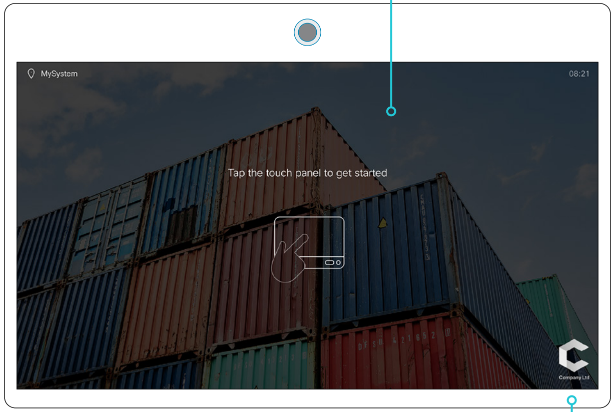
Instructions how to start using the device

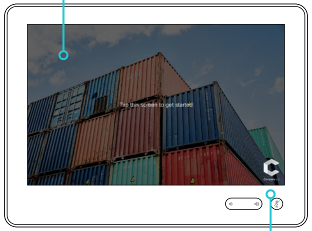
Use the *UserInterface > OSD > HalfwakeMessage* setting if you want to customize or remove the message at the center of the screen (only on screen, not on touch controller). This is the message that informs the user how to start using the device.

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.

Custom background

- 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: 3840 × 2160 pixels


MySystem
08:21
Tap the touch panel to get started
Company Ltd

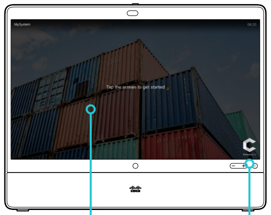

Tap the screen to get started

Logo

We recommend:

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

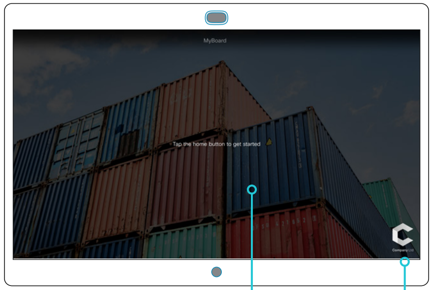
Webex Desk, Desk Pro, and Desk Limited Edition


MySystem
Tap the screen to get started

Custom background

Logo

Boards

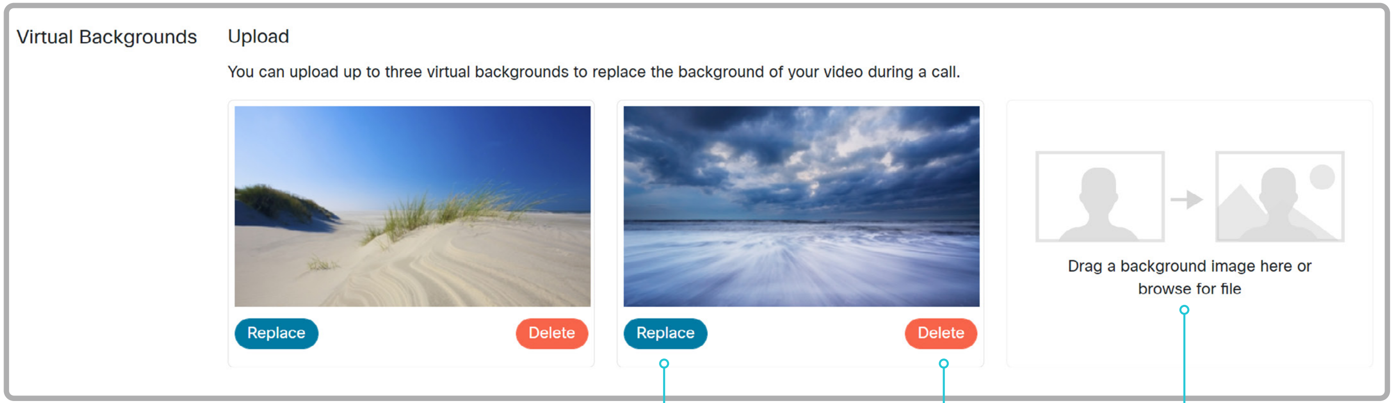

MyBoard
Tap the home button to get started

Custom background

Logo

Add a virtual background

Sign in to the web interface, go to *Personalization*, and select *Virtual Backgrounds*.



Virtual Backgrounds

Upload

You can upload up to three virtual backgrounds to replace the background of your video during a call.

Replace the background image

Replace allows you to replace the virtual background with a new file.

Delete the background image

Delete fully removes the virtual background from the device.

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

Upload a background image

Browse to select a new virtual background or select the file from your file system and drag it into the web interface.

Supported file formats: BMP, GIF (no animation), JPEG, PNG

Maximum file size: 4 MB

About a virtual background

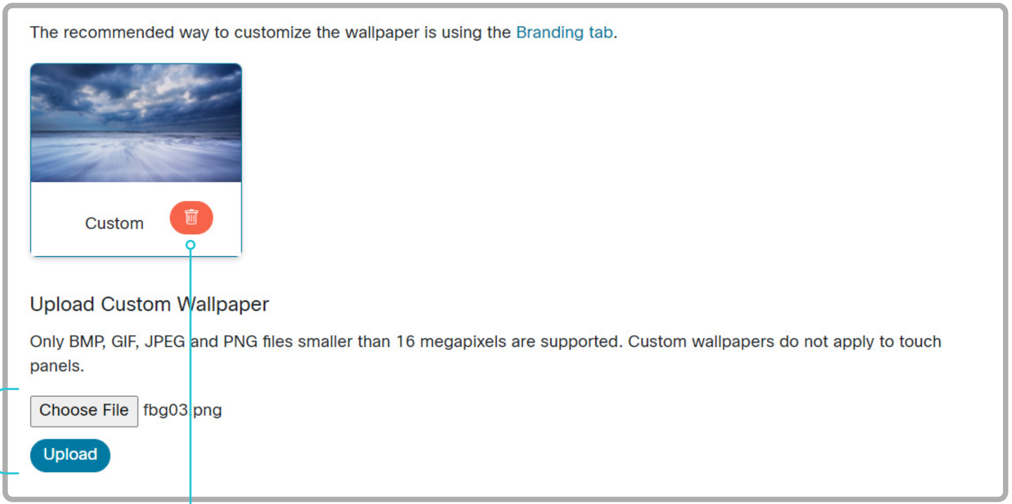
If you want to use a custom image as the background while you are in a call, you may upload and use up to three *virtual backgrounds*.

It is also possible to connect a computer and use the computer display as your background.

Virtual backgrounds, also called *video backgrounds*, can be selected from the user interface. Tap the **Selfview** icon to open the background options. See the user guide for more details.

Add a custom wallpaper

Sign in to the web interface, go to *Personalization*, and select *Custom Wallpaper*.



The recommended way to customize the wallpaper is using the Branding tab.

Upload Custom Wallpaper

Only BMP, GIF, JPEG and PNG files smaller than 16 megapixels are supported. Custom wallpapers do not apply to touch panels.

Upload a custom wallpaper

Overwrites an 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 (no animation), 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 loosing functionality such as One Button To Push and the list of upcoming meetings. Also, the device doesn't go automatically into halfwake state when using a custom wallpaper.

See the ▶ Add corporate branding to the screen and touch controller chapter.

Branding and Custom wall paper

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

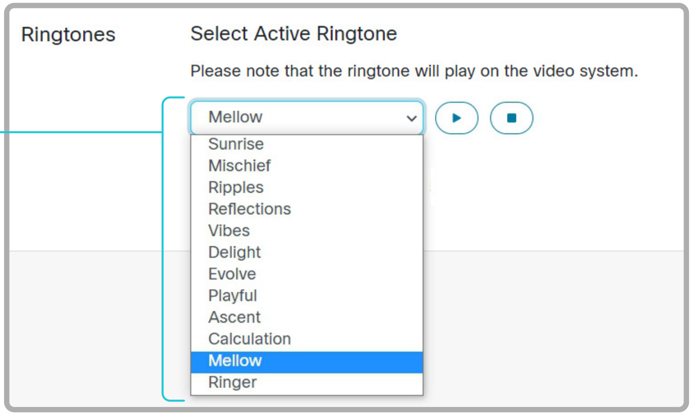
If your device is set up with branding elements you must click *Enable* before you can add a custom wallpaper.

Choose a ringtone and set the ringtone volume

Sign in to the web interface, go to *Personalization*, and select *Ringtones*.

Change the ringtone

1. Choose a ringtone from the drop-down list.
2. Click *Save* to make it the active ringtone.



Ringtones

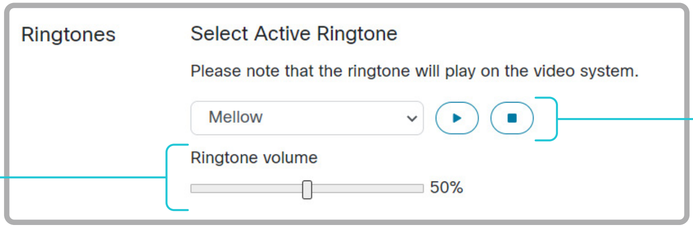
Select Active Ringtone

Please note that the ringtone will play on the video system.

Mellow

Set the ringtone volume

Use the slide bar to adjust the ringtone volume.



Ringtones

Select Active Ringtone

Please note that the ringtone will play on the video system.

Mellow

Ringtone volume 50%

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, go to *Personalization*, and select *Contacts*.

Import or export contacts from file

Click *Export* to save the local contacts in a file; and click *Import* to bring in contacts from a file.

The current local contacts are discarded when you import new contacts from a file.

Add or edit a contact

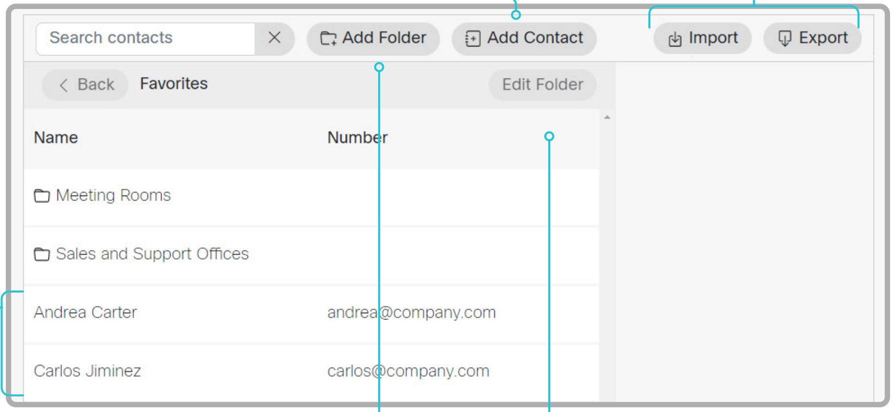
1. Click *Add Contact* to make a new local contact, or click a contact's name followed by *Edit Contact*.
2. Fill in or update the form that pops up.

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

   Click *Add Contact Method* and fill in the new input fields if you want to store more than one contact method for the contact (for example video address, telephone and mobile number).
3. Click *Save* to store the local contact.

Delete a contact

1. Click a contacts name followed by *Edit Contact*.
2. Click *Delete* to remove the local contact.



Name	Number
Meeting Rooms	
Sales and Support Offices	
Andrea Carter	andrea@company.com
Carlos Jiminez	carlos@company.com

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

For Boards this only applies to a paired touch controller, not to the board itself.

Add a contact in the Favorites list

1. Select *Call* on the home screen.
2. Select the contact you want to add.
3. ***Only for Webex Desk, Desk Pro, and Desk Limited Edition.***

   Select the three dots that appear under the *Call* button on the contact card.
4. Select *Mark as favorite* ***(Webex Desk, Desk Pro, and Desk Limited Edition)*** or *Add to favorites* ***(other products)***.

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. ***Only for Webex Desk, Desk Pro, and Desk Limited Edition.***

   Select the three dots that appear under the *Call* button on the contact card.
5. Select *Unmark as favorite* ***(Webex Desk, Desk Pro, and Desk Limited Edition)*** or *Remove favorite* ***(other products)***.

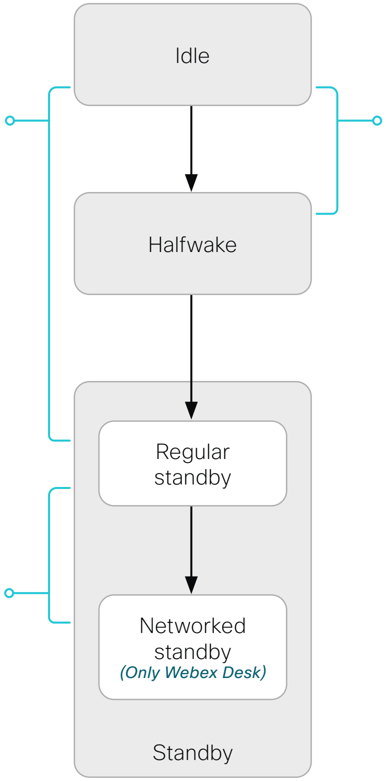
Set up accessibility features

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, go to *Settings*, and select *Configurations*.
2. Go to *UserInterface > Accessibility > IncomingCallNotification* and select **AmplifiedVisuals**.
3. Click *Save*.

Set up the standby behavior



By default, a device will enter standby after *y* minutes. The default delay depends on the product.

You can set the preferred delay or switch off standby using these settings:

- *Standby Control:* Off/On
- *Standby Delay:* Integer (1..480)

The device will never enter standby mode automatically if the *Standby Control* is **Off**. If the *Standby Control* is **On**, the device will enter standby mode when the *Standby Delay* has timed out.

Note that the *Standby Delay* also includes the halfwake period.

By default, a device will enter half-wake mode after 2 minutes (not configurable) when there is no activity, no active web apps or sessions. Halfwake mode will be displayed for *x* minutes, where *x = Standby Delay - 2.*

Example: *Standby Delay:* **5**

> The halfwake screen will be displayed for 3 minutes, and then the device will go into standby mode.

In order to skip the halfwake stage, use the following setting:

- *Standby Halfwake Mode:* **Manual**

By default, a device will enter networked standby 2 minutes after it enters regular standby.

You can set the preferred delay or switch off the automatic transition to networked standby using these settings:

- *Standby Level Networked Mode:* Off/On
- *Standby Level Networked Delay:* Integer (1..1440)

The device will never enter networked standby level if the *Standby Level Networked Control* is **Off**. If the *Standby Level Networked Control* is **On**, the device will enter networked standby when the *Standby Level Networked Delay* has timed out.

If the delay is set to 0, the device will go directly to networked standby, skipping the regular standby stage.

Halfwake mode

The halfwake mode is a stage between idle and standby. A device remains in halfwake mode until activity is detected or until it goes into standby mode.

The halfwake mode may show a darkened screen with text or it may be configured to show branding information, including web pages or digital signage.

Standby levels

There are several levels of standby mode, each providing different power consumption profiles.

Regular standby *(All products)*

This is the first stage of standby. The display is off.

Networked standby *(Only Webex Desk)*

This is the second stage of standby, which reduces power consumption further than the regular standby level.

In addition to turning off the display, we will clock down the CPU/GPU and power down some modules on lower level.

The device is still accessible through the network, and it will wake up when receiving a call.

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

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

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

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

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

Configuration control modes

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

These are the various configuration control modes:

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

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

Pull configurations from the device on-demand

Administrators can use the *Pull xConfig. from Device* option in CUCM to pull configuration changes from the devices on-demand at any time.

This option is enabled only if the device is registered.

Supported CE software versions

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

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

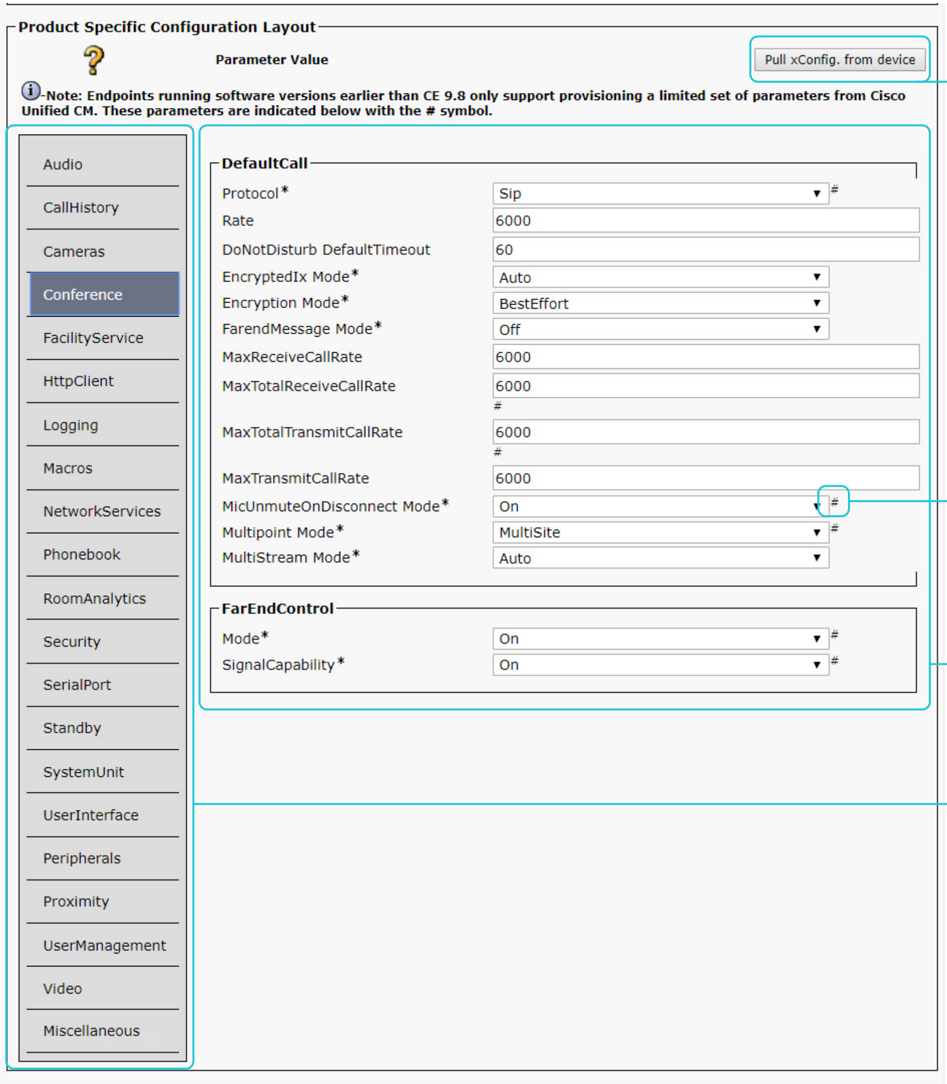
The full set of parameters functions only if you upgrade the device to CE9.8 or higher.

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

Set up provisioning from CUCM

1. Sign in to CUCM, navigate to *Device > Phone*, and find your device.
2. Find the *Product Specific Configuration Layout* section (see illustration).
3. Click the *Miscellaneous* category and find the *Configuration Control Mode* setting.

   Choose your preferred mode: Unified CM, Endpoint, or Unified CM and Endpoint (see the description on the previous page).
4. Click the *Pull xConfig. from Device* button if you want to load the current configuration from the device.
5. Select a category and set a value for the configurations you want to change.
6. Finally, click *Save* and *Apply Config*, just like you do in earlier CUCM versions.


Product Specific Configuration Layout
Parameter Value
Pull xConfig. from device
Audio
CallHistory
Cameras
Conference
FacilityService
HttpClient
Logging
Macros
NetworkServices
Phonebook
RoomAnalytics
Security
SerialPort
Standby
SystemUnit
UserInterface
Peripherals
Proximity
UserManagement
Video
Miscellaneous

Note: Endpoints running software versions earlier than CE 9.8 only support provisioning a limited set of parameters from Cisco Unified CM. These parameters are indicated below with the # symbol.

DefaultCall

Protocol* Sip #
Rate 6000
DoNotDisturb DefaultTimeout 60
EncryptedIx Mode* Auto
Encryption Mode* BestEffort
FarendMessage Mode* Off
MaxReceiveCallRate 6000
MaxTotalReceiveCallRate 6000 #
MaxTotalTransmitCallRate 6000 #
MaxTransmitCallRate 6000
MicUnmuteOnDisconnect Mode* On #
Multipoint Mode* MultiSite #
MultiStream Mode* Auto

FarEndControl

Mode* On #
SignalCapability* On #

Pull configurations from the device on-demand

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

Settings marked with a hash,

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

Settings or parameters

The settings that belong to the selected category.

Categories

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

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

Chapter 3

Peripherals

Connecting screens or other output devices (page 1 of 6)

The *number of video outputs* depends on the product. Typically, the outputs are used for screens or other types of displays. Codec Pro and Room 70 G2 also support connecting a recorder.

The integrated devices has one or more *internal screens* in addition to connectors that are available for *external screens*. The kits and codecs have connectors only for *external screens*.

The device distributes the layout (people and content) on all available monitors. Refer to the article Webex Rooms | Video Stream Layouts on Webex Help Center for information about how layouts appear depending on your device and the number of screens in your setup.

Logical connectors

A logical output is assigned to each output connector, and also to internal screens that are not connected to a physical connector on the connector panel of the device.

The logical outputs are added in parentheses in the table below: Connector 1, Connector 2, etc.

These are the names that are used in the configuration and status paths, and also in API commands.

Maximum resolution

Note that you need Premium HDMI cables to support high resolutions and frame rates.

Audio support

Note that audio is not supported on all outputs.

Product	Number of video outputs	In use for internal screens	Available for external screens and other output devices		
			Connectors	**Maximum resolution**	**Audio support**
Boards	1	Internal (Connector 1)	None		
Codec Plus	2	None	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	3840 × 2160 at 60 fps	If the connected camera has loudspeakers (Quad Camera) there is no audio on the HDMI outputs. Otherwise there is audio on HDMI 1.
Codec Pro	3	None	HDMI 1 (Connector 1) HDMI 2 (Connector 2) HDMI 3 (Connector 3)	3840 × 2160 at 60 fps	If the connected camera has loudspeakers (Quad Camera) there is no audio on the HDMI outputs. If all connectors are set to Auto and no Quad Camera is connected, the device will try HDMI 1, then HDMI 2, and finally HDMI 3 and play the audio on the first available screen. See full description of the Audio Output HDMI [n] Mode in the Device Settings section.
Webex Desk	1	Internal (Connector 1)	None		
Desk Pro	1	Internal (Connector 1)	None		
Desk Limited Edition	1	Internal (Connector 1)	None		
Room Kit	2	None	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	3840 × 2160 at 60 fps	No audio on the HDMI outputs.
Room Kit Mini	1	None	HDMI (Connector 1)	3840 × 2160 at 60 fps	No audio on the HDMI output.
Room 55	2	Internal (Connector 1)	HDMI (Connector 2)	3840 × 2160 at 60 fps	No audio on the HDMI output.
Room 55 Dual / Room 70 Dual	2	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	None		Audio only on the integrated screens.

Connecting screens or other output devices (page 2 of 6)

Product	Number of video outputs	In use for internal screens	Available for external screens and other output devices		
			Connectors	Maximum resolution	Audio support
Room 70 Single	2	HDMI 1 (Connector 1)	HDMI 2 (Connector 2)		Audio only on the integrated screens. If required, an external speaker can be connected to the audio line output connector.
Room 70 Dual G2	3	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	HDMI 3 (Connector 3)		As default, audio only on the integrated screens.
Room 70 Single G2	3	HDMI 1 (Connector 1)	HDMI 2 (Connector 2) HDMI 3 (Connector 3)		As default, audio only on the integrated screen.
Room 70 Panorama	3	HDMI 1 (Connector 1) HDMI 2 (Connector 2) HDMI 3 (Connector 3)	None		
Room Panorama	3	HDMI 1 (Connector 1) HDMI 2 (Connector 2) HDMI 3 (Connector 3)	None		

Connecting screens or other output devices (page 3 of 6)

Automatic setup

(Not relevant for devices with only one video output; and not relevant for Room 70 Panorama and Room Panorama which have a pre-defined behavior of all screens)

By default the number of screens is auto-detected, and the role of each screen - whether it is intended to be the first, second, or third screen - is automatically set according to the physical connections.

Sign in to the web interface, go to *Settings*, and select *Configurations*, to find the settings referred below.

Examples

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

- *Video > Monitors*: **Triple**
- *Video > Output > Connector 1 > MonitorRole*: **First**
- *Video > Output > Connector 2 > MonitorRole*: **Second**
- *Video > Output > Connector 3 > MonitorRole*: **Third**

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

- *Video > Monitors*: **Dual**
- *Video > Output > Connector 1 > MonitorRole*: **First** [1]
- *Video > Output > Connector 2 > MonitorRole*: **Second** [1]

When do you need manual setup

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

- Dedicate a screen to only show presentations
- Use one of the outputs for a recorder *(available for: Codec Pro and Room 70 G2)*
- Replicate the same layout on more than one screen
- Show the on-screen messages and indicators (OSD) on another screen than the video output with the lowest number *(not available for Room 55)*
- Set the resolution manually, e.g. if the device fails to detect the native resolution and refresh rate of a screen

---

[1] Room 55 doesn't have explicit MonitorRole settings. The internal screen (Connector 1) always assumes the monitor role **First**, and an external screen connected to the HMDI output (Connector 2) always assumes the monitor role **Second**.

Connecting screens or other output devices (page 4 of 6)

Manual setup

(Not relevant for devices with only one video output; and not relevant for Room 70 Panorama and Room Panorama which have a pre-defined behavior of all screens)

The automatic setup works well for common scenarios with one or mutiple screens. For more complex scenarios, you may need manual configuration.

Sign in to the web interface, go to *Settings*, and select *Configurations*, to find the settings referred below

Set a role for each screen

Define a role for each screen with the *Video > Output > Connector n > MonitorRole* setting. [1]

The monitor role decides which layout (people and content) will appear on the screen that is connected to this output.

Screens with the same monitor role get the same layout; screens with different monitor roles get different layouts.

You must choose monitor roles that match your screen setup.

Set the number of screens

Set the number of screens with *different* layouts in your setup with the *Video > Monitors* setting.

Most often the number of different layouts are the same as the number of physical screens, but not always. If exactly the same layout shall be repeated on more that one screen, the number of different layouts is less.

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

The other options allow you to fix a single, dual, or triple screen setup; and to reserve one screen for content.

Choose on which screen to display messages and indicators

Define on which screen to display the messages and indicators on-screen with the *UserInterface > OSD > Output* setting. [2]

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

Set the screen resolution and refresh rate

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

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

Examples

Two screens in total, and the second screen is dedicated to only show presentations:

- *Video > Monitors*: **DualPresentationOnly**
- *Video > Output > Connector 1 > MonitorRole*: **Auto** [1]
- *Video > Output > Connector 2 > MonitorRole*: **Auto**
- *UserInterface > OSD > Output*: **1** or **Auto** [2, 3]

Three screens in total[4], and the third screen is dedicated to only show presentations:

- *Video > Monitors*: **TriplePresentationOnly**
- *Video > Output > Connector 1 > MonitorRole*: **Auto**
- *Video > Output > Connector 2 > MonitorRole*: **Auto**
- *Video > Output > Connector 3 > MonitorRole*: **Auto**
- *UserInterface > OSD > Output*: **1**

Two screens in total, and a recording device[4] is attached to Connector 3 (HDMI). OSD is on the screen on Connector 2:

- *Video > Monitors*: **Auto**
- *Video > Output > Connector 1 > MonitorRole*: **Auto**
- *Video > Output > Connector 2 > MonitorRole*: **Auto**
- *Video > Output > Connector 3 > MonitorRole*: **Recorder**
- *UserInterface > OSD > Output*: **2**

---

[1] Room 55 doesn't have explicit MonitorRole settings. The internal screen (Connector 1) always assumes the monitor role **First**, and an external screen connected to the HMDI output (Connector 2) always assumes the monitor role **Second**.

[2] Room 55 doesn't have the OSD Output setting. OSD is always displayed on the internal screen.

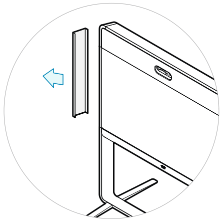
[3] Set to **1** for Codec Pro and Room 70 G2; **Auto** for other devices.

[4] Only Codec Pro and Room 70 G2 support three outputs.

Connecting screens or other output devices (page 5 of 6)

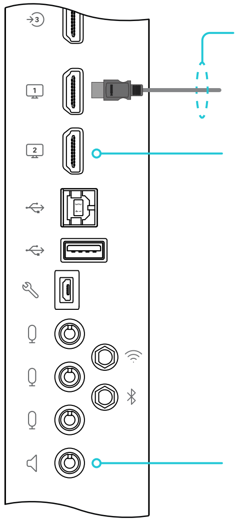
Output connectors

⚠ Always switch off power when you connect and disconnect screens and peripherals.



Remove the left side cover to get access to the connector panel and power switch for these devices. The cover is fastened with magnets.

Room 70 Single



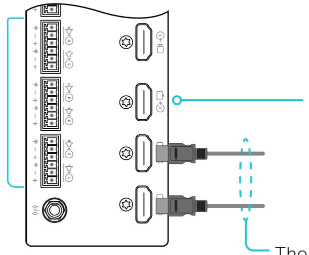
This connector is used for the integrated screen. Do not disconnect!

HDMI output for external screen (Output Connector 2)

Audio Line Output (minijack)

Codec connector panel

Room 70 Dual G2



Audio Line outputs (Euroblock, 3.5 mm)

HDMI output for external screen (Output Connector 3)

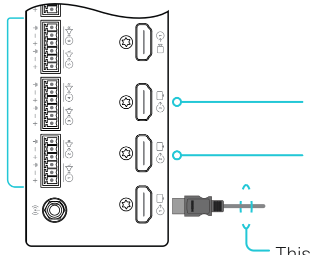
These connectors are used for the integrated screens. Do not disconnect!

Codec connector panel

Room 55 Dual and Room 70 Dual

Both HDMI outputs (Output Connector 1 and 2) is used for the integrated screens. Do not disconnect!

Room 70 Single G2



Audio Line outputs (Euroblock, 3.5 mm)

HDMI output for external screen (Output Connector 3)

HDMI output for external screen (Output Connector 2)

This connector is used for the integrated screen. Do not disconnect!

Codec connector panel

⚠ Do not disconnect the integrated screens for Room 55 Dual, Room 70 and Room 70 G2.

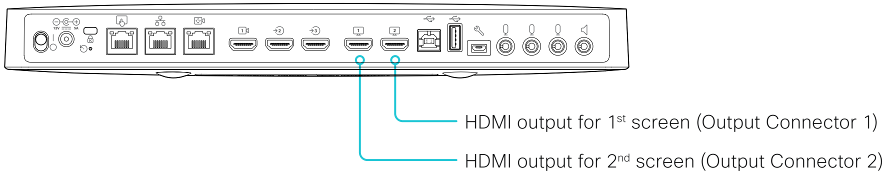
The integrated screen connections make use of multichannel audio, which drives the speaker system of the devices. Inserting third party equipment is likely to break the audio chain, causing the device to fail from an audio perspective.

Connecting screens or other output devices (page 6 of 6)

Output connectors

⚠ Always switch off power when you connect and disconnect screens and peripherals.

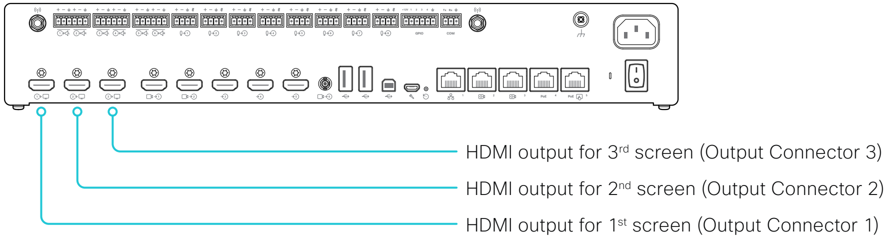
Codec Plus



HDMI output for 1st screen (Output Connector 1)

HDMI output for 2nd screen (Output Connector 2)

Codec Pro

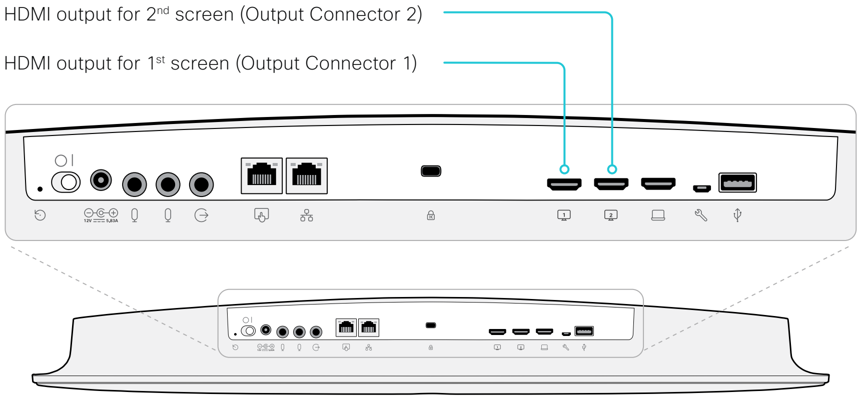


HDMI output for 3rd screen (Output Connector 3)

HDMI output for 2nd screen (Output Connector 2)

HDMI output for 1st screen (Output Connector 1)

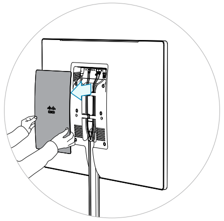
Room Kit



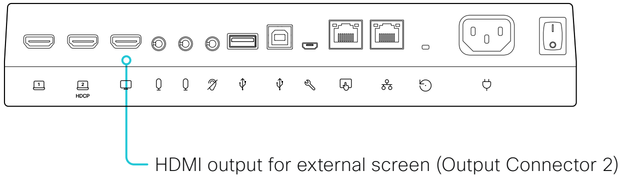
HDMI output for 2nd screen (Output Connector 2)

HDMI output for 1st screen (Output Connector 1)

Room 55

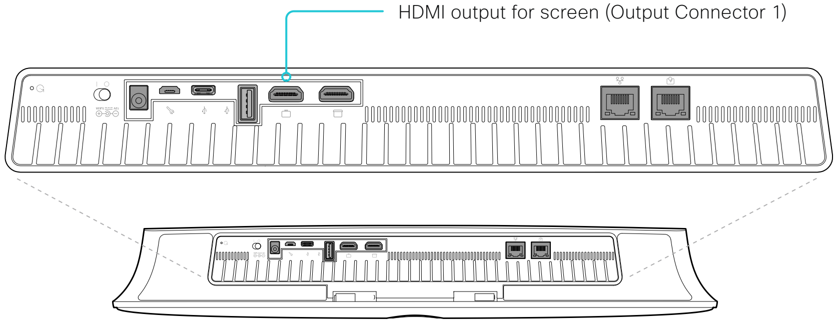


Remove the rear cover to get access to the connector panel and power switch.



HDMI output for external screen (Output Connector 2)

Room Kit Mini



HDMI output for screen (Output Connector 1)

Connecting input sources (page 1 of 7)

Sign in to the web interface, go to *Settings*, and select *Configurations*, to find the settings referred in this chapter.

The *number of video inputs* depends on the product. Typically, the video inputs are used for cameras and computers. and other content sources, but you can also connect other types of video and content sources.

When you connect a computer or content source to an input, you can share content locally or with conference participants.

The integrated devices has *internal cameras* in addition to connectors that are available for *external* content sources. The kits and codecs have connectors only for *external* cameras and other content sources.

Logical connectors

A logical input is assigned to each input connector, and also to internal cameras that are not connected to a physical connector on the connector panel of the device.

The logical inputs are added in parentheses in the table on the next pages: Connector 1, Connector 2, etc.

These are the names that are used in the configuration and status paths, and also in API commands.

About video and content quality

When encoding and transmitting video there is a trade-off between high resolution and high frame rate. For some video sources it is more important to transmit a high frame rate than high resolution and vice versa.

Use the *Video > Input > Connector n > Quality* setting to optimize quality with respect to motion (high frame rate) or sharpness (high resolution).

Typically, you should choose **Motion** for regular video inputs and when there is a lot of motion in the picture. Choose **Sharpness** when you want the highest quality of detailed images and graphics.

ⓘ If a Quad Camera, SpeakerTrack 60 camera, or Precision 60 camera is detected by the device this setting is automatically set to **Motion**. If a user changes this setting manually, it will be set back to **Motion** after a restart or a camera reconnect.

The default value is **Motion** for connectors that are most often used for cameras, and **Sharpness** for connectors that are most often used for presentation sources. Refer to the table.

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.

Product	Quality default setting
Boards	Connector 2: Sharpness
Codec Plus	Connector 1: Motion Connector 2: Sharpness Connector 3: Sharpness
Codec Pro	Connector 1: Motion Connector 2: Motion Connector 3: Sharpness Connector 4: Sharpness Connector 5: Sharpness Connector 6: Motion
Webex Desk / Desk Pro / Desk Limited Edition	Connector 2: Sharpness Connector 3: Sharpness
Room Kit	Connector 2: Sharpness
Room Kit Mini	Connector 2: Sharpness
Room 55	Connector 2: Sharpness Connector 3: Sharpness
Room 55 Dual / Room 70	Connector 1: Motion Connector 2: Sharpness Connector 3: Sharpness
Room 70 G2	Connector 1: Motion Connector 2: Motion Connector 3: Sharpness Connector 4: Sharpness Connector 5: Sharpness Connector 6: Motion
Room Panorama / Room 70 Panorama	Connector 1: Motion Connector 2: Motion Connector 3: Sharpness Connector 4: Sharpness Connector 5: Sharpness Connector 6: Motion

Connecting input sources (page 2 of 7)

HDCP support

(Applies to: Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama)

You can configure one of the input connectors to support HDCP (High-bandwidth Digital Content Protection), which means that the device is authorized to display HDCP protected content.

This only applies to specifc connectors, refer to the table below.

Use this setting to enable HDCP on this input:

- *Video > Input > Connector n > HDCP > Mode*

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

Connect external microphones

(Applies to: Room Kit and Room 55)

These devices support one or two external microphones in addition to their built-in microphone. We recommend the Cisco Table Microphone or the Cisco TelePresence Ceiling Microphone.

Note that Microphone 1 is the integrated microphone.

Connecting cameras

(Applies to: Codec Plus, Codec Pro)

Always use Connector 1 when you connect the Quad Camera to the device. This is required for correct playback of audio through the loudspeakers in the camera.

For details about connecting cameras, refer to the installation guides for the Room Series products online.

Connect a computer or other content source

You can connect one or more content sources, for example computers, to a device in order to share content locally or with conference participants. The number of external input sources and the maximum resolution they support is in the table below.

Note that you need a High Speed HDMI 1.4b cable to support the higher resolutions and frame rates.

Input connector overview

Product	Number of video inputs	Reserved for internal camera	External input sources	Maximum resolution	HDCP support	Comments
Boards	2	Internal (Connector 1)	HDMI 2 (Connector 2)	Connector 2: 3840 × 2160 at 30 fps or 1080p at 60 fps	Not available	
Codec Plus	3	N/A	HDMI 1 (Connector 1) HDMI 2 (Connector 2) HDMI 3 (Connector 3)		HDMI 2 (Connector 2)	Quad Camera: Always use Connector 1 SpeakerTrack 60: Use Connector 1 and Connector 2 Camera Control: Through the auxiliary Ethernet port If you connect more than one camera you need an Ethernet switch to allow for camera control on all cameras.

Connecting input sources (page 3 of 7)

Product	Number of video inputs	Reserved for internal camera	External input sources	Maximum resolution	HDCP support	Comments
Codec Pro	6	N/A	HDMI 1 (Connector 1) HDMI 2 (Connector 2) HDMI 3 (Connector 3) HDMI 4 (Connector 4) HDMI 5 (Connector 5) SDI (Connector 6)	Connector 1: 1080p60 Connector 2: 1080p60 Connector 3: 4Kp30 Connector 4: 4Kp30 Connector 5: 4Kp30	HDMI 5 (Connector 5)	Quad Camera: Always use Connector 1 SpeakerTrack 60: Use Connector 1 and Connector 2 Camera Control: Through the auxiliary Ethernet ports If you have more cameras than available auxiliary Ethernet ports you need an Ethernet switch to allow for camera control of all cameras.
Desk Pro	3	Internal (Connector 1)	USB-C (Connector 2) HDMI (Connector 3)	Connector 2: 3840 × 2160 at 60 fps Connector 3: 3840 × 2160 at 60 fps	Not available	USB-C: For screen extension, content sharing, and touch forwarding capabilities on supported operating systems. The USB-C also allows the use of camera, microphone, and speakers with any software client (USB-camera mode); as well as, providing laptop charging (60 W maximum). HDMI: For screen extension and content sharing.
Webex Desk / Desk Limited Edition	3	Internal (Connector 1)	USB-C (Connector 2) HDMI (Connector 3)	Connector 2: 1920 × 1080 at 60 fps Connector 3: 1920 × 1080 at 60 fps	Not available	USB-C: For screen extension and content sharing on supported operating systems. Desk Limited Edition also has touch forwarding capabilities. The USB-C also allows the use of camera, microphone, and speakers with any software client (USB-camera mode). HDMI: For screen extension and content sharing.
Room Kit	2	Internal (Connector 1)	HDMI 2 (Connector 2)	Connector 2: 3840 × 2160 at 30 fps	Not available	
Room Kit Mini	2	Internal (Connector 1)	HDMI 2 (Connector 2)	Connector 2: 3840 × 2160 at 30 fps	Not available	
Room 55	3	Internal (Connector 1)	HDMI 1 (Connector 2) HDMI 2 (Connector 3	Connector 2: 3840 × 2160 at 30 fps Connector 3: 3840 × 2160 at 30 fps	HDMI 2 (Connector 3)	

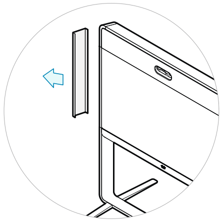
Connecting input sources (page 4 of 7)

Product	Number of video inputs	Reserved for internal camera	External input sources	Maximum resolution	HDCP support	Comments
Room 55 Dual / Room 70	3	HDMI 1 (Connector 1)	HDMI 2 (Connector 2) HDMI 3 (Connector 3)		HDMI 2 (Connector 2)	Camera Control: Through the auxiliary Ethernet port If you connect extra cameras you need an Ethernet switch to allow for camera control on all cameras.
Room 70 G2	6	HDMI 1 (Connector 1)	HDMI 2 (Connector 2) HDMI 3 (Connector 3) HDMI 4 (Connector 4) HDMI 5 (Connector 5) SDI (Connector 6)	Connector 1: 1080p60 Connector 2: 1080p60 Connector 3: 4Kp30 Connector 4: 4Kp30 Connector 5: 4Kp30	HDMI 5 (Connector 5)	Camera Control: Through the auxiliary Ethernet ports If you have more cameras than available auxiliary Ethernet ports you need an Ethernet switch to allow for camera control of all cameras.
Room 70 Panorama	6	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	HDMI 3 (Connector 3) HDMI 4 (Connector 4) HDMI 5 (Connector 5) SDI (Connector 6	Connector 1: 1080p60 Connector 2: 1080p60 Connector 3: 4Kp30 Connector 4: 4Kp30 Connector 5: 4Kp30	HDMI 5 (Connector 5)	Camera control is through Ethernet port 2.
Room Panorama	6	HDMI 1 (Connector 1) HDMI 2 (Connector 2)	HDMI 3 (Connector 3) HDMI 4 (Connector 4) HDMI 5 (Connector 5) SDI (Connector 6	Connector 1: 1080p60 Connector 2: 1080p60 Connector 3: 4Kp30 Connector 4: 4Kp30 Connector 5: 4Kp30	HDMI 5 (Connector 5)	Camera control is through Ethernet port 2.

Connecting input sources (page 5 of 7)

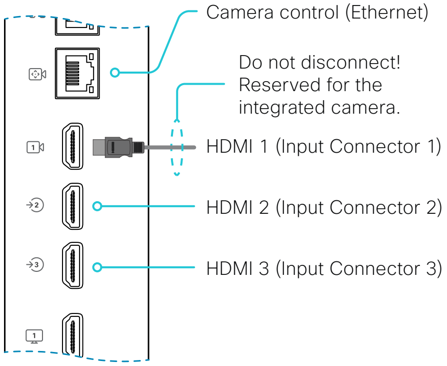
Input connectors

⚠ Always switch off power when you connect and disconnect peripherals.



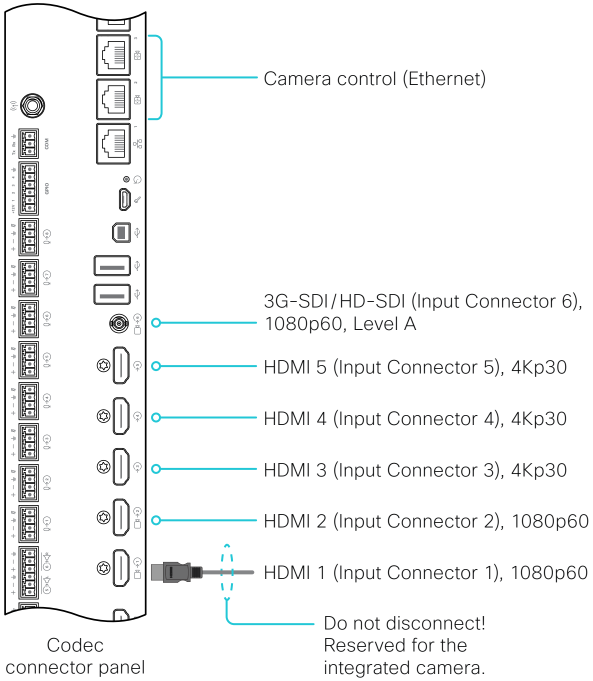
Remove the left side cover to get access to the connector panel and power switch for these devices. The cover is fastened with magnets.

Room 55 Dual and Room 70


Camera control (Ethernet)
Do not disconnect! Reserved for the integrated camera.
HDMI 1 (Input Connector 1)
HDMI 2 (Input Connector 2)
HDMI 3 (Input Connector 3)

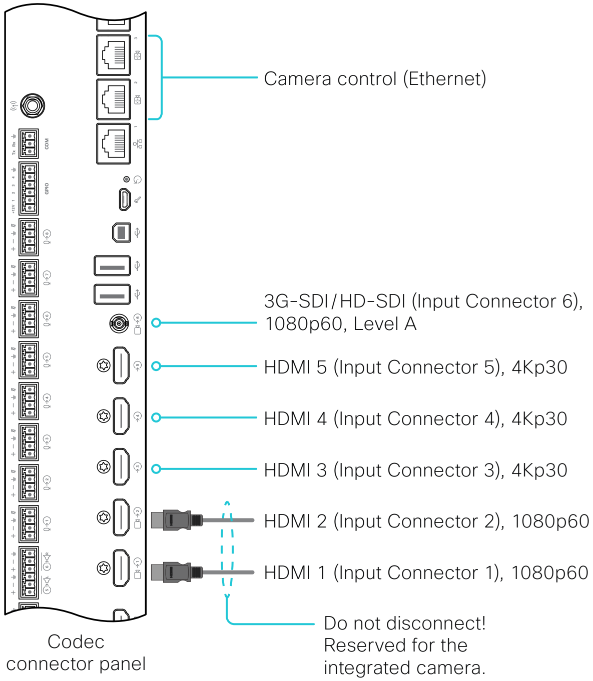
Codec connector panel

Room 70 G2


Camera control (Ethernet)
3G-SDI/HD-SDI (Input Connector 6), 1080p60, Level A
HDMI 5 (Input Connector 5), 4Kp30
HDMI 4 (Input Connector 4), 4Kp30
HDMI 3 (Input Connector 3), 4Kp30
HDMI 2 (Input Connector 2), 1080p60
HDMI 1 (Input Connector 1), 1080p60
Do not disconnect! Reserved for the integrated camera.

Codec connector panel

Room 70 Panorama


Camera control (Ethernet)
3G-SDI/HD-SDI (Input Connector 6), 1080p60, Level A
HDMI 5 (Input Connector 5), 4Kp30
HDMI 4 (Input Connector 4), 4Kp30
HDMI 3 (Input Connector 3), 4Kp30
HDMI 2 (Input Connector 2), 1080p60
HDMI 1 (Input Connector 1), 1080p60
Do not disconnect! Reserved for the integrated camera.

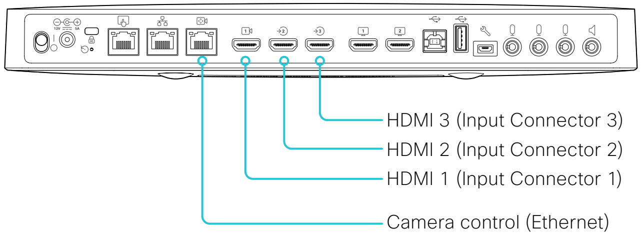
Codec connector panel

Connecting input sources (page 6 of 7)

Input connectors

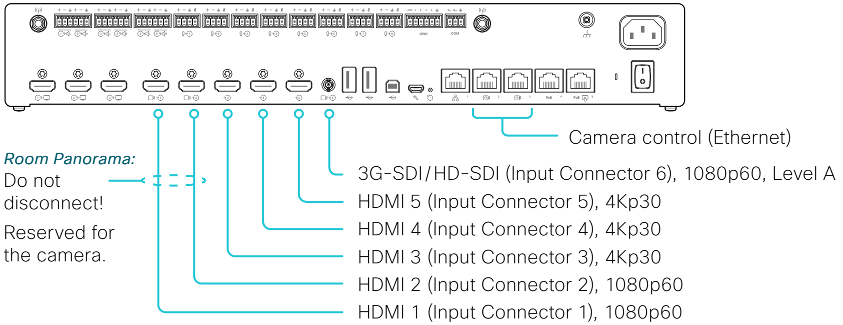
⚠ Always switch off power when you connect and disconnect peripherals.

Codec Plus



HDMI 3 (Input Connector 3)
HDMI 2 (Input Connector 2)
HDMI 1 (Input Connector 1)
Camera control (Ethernet)

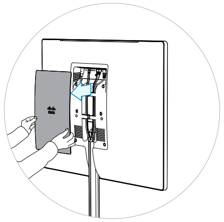
Codec Pro and Room Panorama



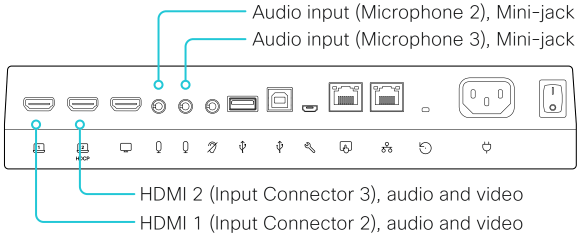
Camera control (Ethernet)
3G-SDI/HD-SDI (Input Connector 6), 1080p60, Level A
HDMI 5 (Input Connector 5), 4Kp30
HDMI 4 (Input Connector 4), 4Kp30
HDMI 3 (Input Connector 3), 4Kp30
HDMI 2 (Input Connector 2), 1080p60
HDMI 1 (Input Connector 1), 1080p60

Room Panorama:
Do not disconnect!
Reserved for the camera.

Room 55

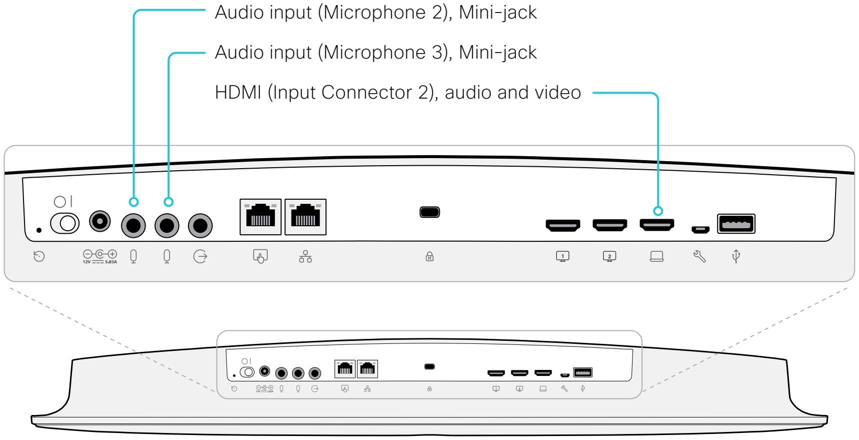


Remove the rear cover to get access to the connector panel and power switch.



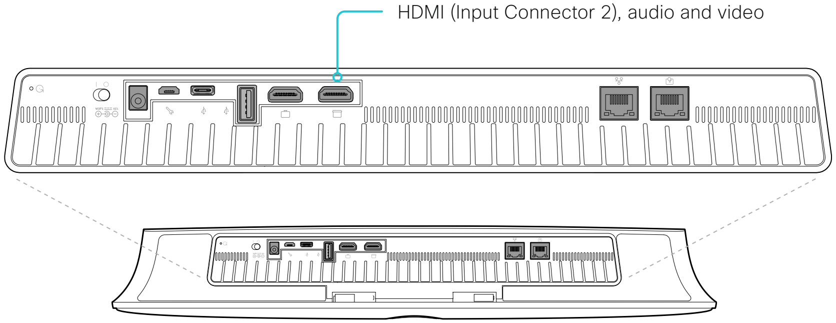
Audio input (Microphone 2), Mini-jack
Audio input (Microphone 3), Mini-jack
HDMI 2 (Input Connector 3), audio and video
HDMI 1 (Input Connector 2), audio and video

Room Kit



Audio input (Microphone 2), Mini-jack
Audio input (Microphone 3), Mini-jack
HDMI (Input Connector 2), audio and video

Room Kit Mini



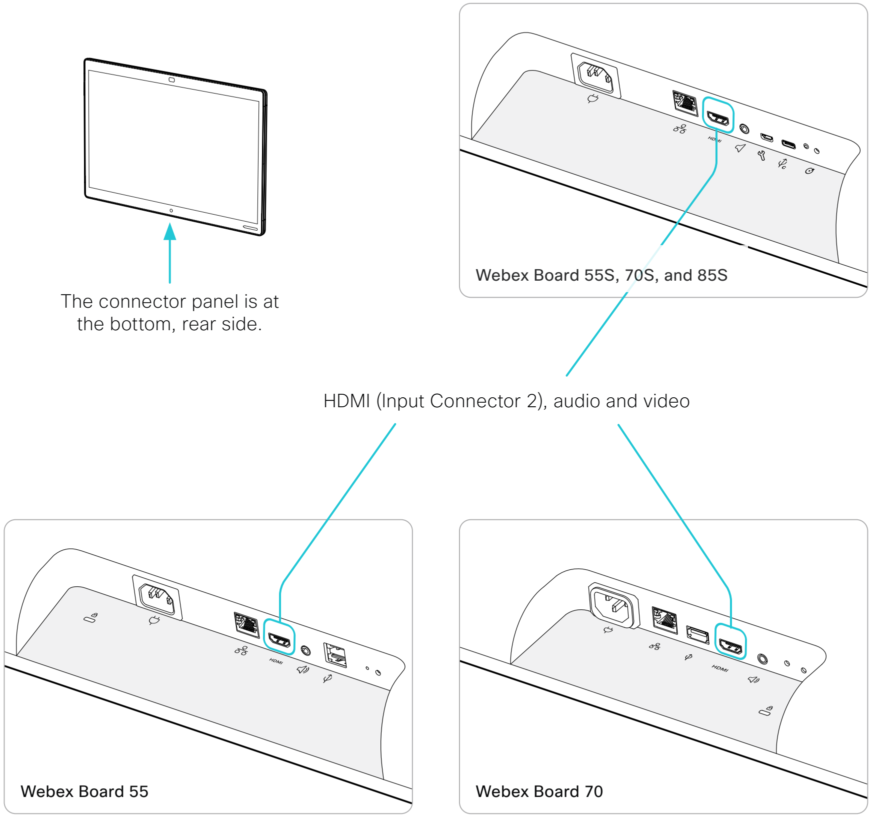
HDMI (Input Connector 2), audio and video

Connecting input sources (page 7 of 7)

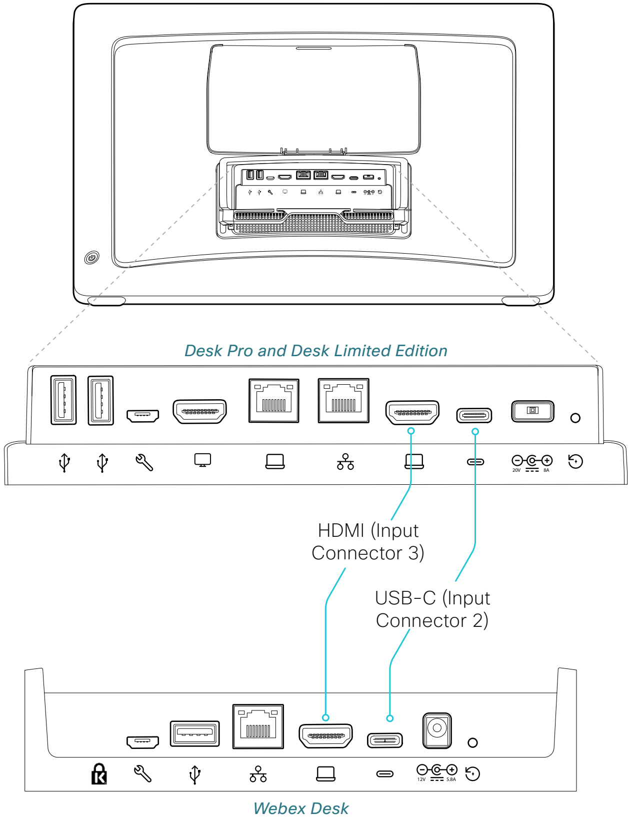
Input connectors

⚠ Always switch off when you connect and disconnect peripherals.

Webex Boards


The connector panel is at the bottom, rear side.
Webex Board 55S, 70S, and 85S
HDMI (Input Connector 2), audio and video
Webex Board 55
Webex Board 70

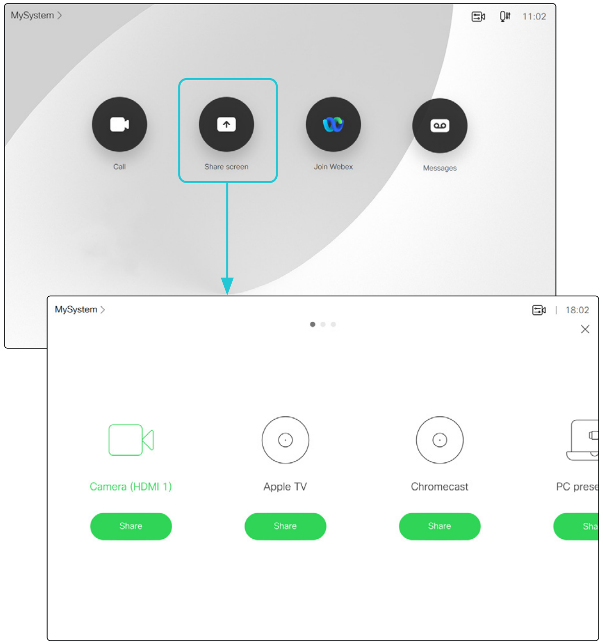
Webex Desk, Desk Pro and Desk Limited Edition


Desk Pro and Desk Limited Edition
HDMI (Input Connector 3)
USB-C (Input Connector 2)
Webex Desk

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.


MySystem >
11:02
Call
Share screen
Join Webex
Messages
MySystem >
18:02
Camera (HDMI 1)
Share
Apple TV
Share
Chromecast
Share
PC prese
Sha

User interface with multiple external input sources (example)

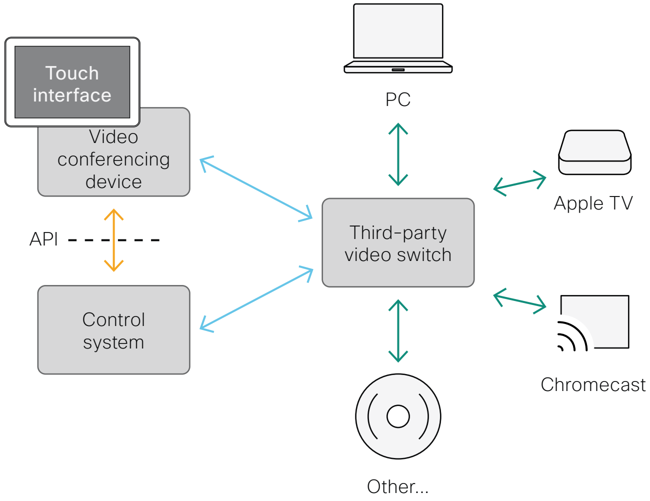
Consult the *Customization guide* for full details about how to extend the user interface, and how to use the device's API to set it up. Go to:

- ▶ https://www.cisco.com/go/in-room-control-docs

Architecture

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

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


Touch interface
Video conferencing device
API
Control system
PC
Third-party video switch
Apple TV
Chromecast
Other...

---

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

Information about displays

Display recommendations

As a technology leader in video conferencing, Webex has created a certification program to further ensure premium meeting experiences with third party displays.

Webex Certifications are done using rigorous analysis and test specifications. These define a standard point of reference for performance that faithfully reproduces the engineering intent.

The Webex Rooms devices are designed to optimize picture quality, minimize the camera-to-screen delay, implement robust standby handling, and implement other measures for an optimal experience.

Webex Rooms certified displays

Cisco recommends using the following displays for the best experience and verified compatibility. These displays are certified to achieve this optimal performance automatically when they are connected to a Webex Room device.

Vendor	Series	Tested version
Samsung	QMR	2123.0, 2151.0
Samsung	QBR	2123.0, 2151.0
Samsung	Flip 2.0	1080.7

Webex Rooms compatible displays

Cisco has tested the following displays for the experience and verified compatibility. They fulfill basic requirements for experience and compatibility.

Vendor	Series	Tested version
Panasonic	EQ1	1.50 Cu
LG	UH5F-H	03.02.00
LG	UL3G	03.12.80

Other displays

When not using a certified display, it is important that you configure the display is to give the best possible experience.

In the default display configuration, the delay through most displays is often very high (>100 ms). This can be 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, such as *Motion Flow*, *Natural Motion*, or any other video processing that introduces delay.
- Deactivate advanced audio processing, such as *Virtual Surround* effects and *Dynamic Compression*, which will cause malfunctions in acoustic echo cancellation.
- Change to a different HDMI input.

In order to achieve automatic input switching and standby control, the Consumer Electronics Control (CEC) function of the display may need to be enabled manually.

This function is then utilized as follows:

- The active video input on a display may be changed by the user through the manufacturer's user interface. Therefore, when a call is placed, the video conferencing device queries the active video input source and switches this source back to itself, if necessary.
- If the video conferencing device goes into standby without being the active input source, the display will not be set to standby.

Information about 4K resolution

Connecting a computer

If an error occurs when you connect a computer, a message will show on the screen or touch controller.

The default preferred resolution on the video input connector is 1080p60 (1920_1080_60).

4K resolution

(Applies to: All products except Webex Desk)

If you want to use 4K resolution with the computer, sign in to the web interface, go to *Settings*, and select *Configurations*. Go to *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.

Connecting an external display

(Applies to: All products except Boards, Webex Desk, Desk Pro, Desk Limited Edition, Room 70 Panorama, and Room Panorama)

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

If you need to adjust the settings for the external display at a later stage, sign in to the web interface, go to *Settings*, and select *Configurations*. Go to *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 lists of Webex Room certified and compatible displays. Refer to the ▶ Information about displays chapter.

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 connectors (input and/or output) are configured correctly.

Check that the connected external device has support for 4K and that it is configured correctly.

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:

- Presentation sources
- External cameras *(not supported by Boards, Webex Desk, Desk Pro, and Desk Limited Edition)*
- External displays *(not supported by Boards, Webex Desk, Desk Pro, and Desk Limited Edition)*

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

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).

HDMI cables for external cameras and displays

(Applies to: All products except Boards, Webex Desk, Desk Pro, and Desk Limited Edition)

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.

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

---

[*] Our 4K multihead cables (CAB-HDMI-MUL4K-9M and CAB-HDMI-MUL4K-2M) are compatible with devices in the Board, Desk, and Room series. The cables have connectors HDMI type A ↔ USB-C, Mini display port, and HDMI type A.

Our 1080p multihead cable (CAB-HDMI-MULT-9M) is not compatible with these devices..

Set up the SpeakerTrack feature (page 1 of 4)

Speaker tracking features

Speaker tracking abilities depend on the camera of the device.

Best overview

Digital face detection and automatic camera framing are used to assess the situation and compose the *best overview* containing all the people in the room. If people are moving around in the room or additional participants enter the room, the system will adapt and automatically adjust to include all persons in the frame.

Webex Desk, Desk Pro, Desk Limited Edition, and Room Kit Mini are limited to the best overview; however, the other devices described on this page also employ audio tracking. This is used to locate the active speaker in a room in support of creating closeups and group framing.

Closeups

Not supported by Webex Desk, Desk Pro, Desk Limited Edition, or Room Kit Mini.

When closeup is enabled, audio tracking is used to find and zoom in on the active speaker to the exclusion of other participants. If you want to ensure that everyone in the room is always in the camera frame, turn off the closeup functionality.

If you wish to focus solely on the speaker, note that there are some limitations. Depending on the maximum zoom factor of the camera and the distance at which the speaker is located away from the camera, it might not be possible to create a framing for the speaker alone.

Group framing

Not supported by the SpeakerTrack 60 camera, Webex Desk, Desk Pro, Desk Limited Edition, or Room Kit Mini.

Here, the system strives to create a more natural user experience by creating frames that include, not only the active speaker, but also the participants in close proximity to him/her.

This has the additional positive effect of reducing the total number of switches. For example, if another person within the frame starts to speak, the camera will most likely not need to reframe.

View limits

Not supported by the SpeakerTrack 60 camera, Webex Desk, Desk Pro, Desk Limited Edition, Room Kit Mini, or the Room Panorama / Room 70 Panorama in panoramic video scenarios.

The *view limits* feature provides the ability to limit the field of view and exclude parts of the room through the user interface.

Products that support speaker tracking

The following Cisco products support speaker tracking[1]:

- Room Kit
- Room Kit Mini [2]
- Codec Plus with Quad Camera (Room Kit Plus) or SpeakerTrack 60 camera
- Codec Pro with Quad Camera (Room Kit Pro) or SpeakerTrack 60 camera
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2
- Room Panorama [3]
- Room 70 Panorama [3]
- Webex Desk [2]
- Desk Pro [2]
- Desk Limited Edition [2]

---

[1] A head-tracking algorithm enables speaker tracking to work when people are wearing masks. Note that the SpeakerTrack 60 camera doesn't support this algorithm.

[2] The full speaker tracking feature is not supported; only best overview. For these products, the *Cameras > SpeakerTrack > Mode* setting applies to turning on and off the best overview.

[3] In panoramic video scenarios, the 2-camera panoramic view cannot be switched off. In this case, speaker tracking is not enabled. In all other scenarios, speaker tracking works and can be configured as described in this chapter.

Set up the SpeakerTrack feature (page 2 of 4)

Camera specifics

Built-in camera that supports speaker tracking

(i.e., Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama, and Boards)

- The camera supports best overview and closeup.
- Group framing is supported by all built-in cameras.

Cisco Quad Camera

(an option for Codec Plus and Codec Pro)

- The camera supports best overview, closeup, and group framing.
- Finding a good group framing is prioritized over making a closeup of only the active speaker.
- The camera has a lower maximum zoom factor than the SpeakerTrack 60 camera and therefore cannot zoom in so closely on speakers far away from the camera.
- Certain room conditions such as lighting and acoustics, can significantly impact the Quad camera's ability to detect every person present. Speaker tracking functionality works best under optimal room conditions in combination with a seating area that is a maximum of 8 m / 26 ft deep and up to 5 m / 16 ft wide, in relation to the camera's position. Sub-optimal room conditions or a camera distance greater than 8 m / 26 ft will cause performance to degrade. Participants seated outside the horizontal field of view (83°) will not be detected.

Cisco TelePresence SpeakerTrack 60 Camera

(an option for Codec Plus and Codec Pro)

- The dual camera assembly consists of two cameras that support best overview and closeup.
- Group framing is not supported. When a change of speaker is detected, the video conferencing device will switch automatically between the two cameras to always show the optimal camera frame.
- SpeakerTrack 60 works best when the room's seating area is a maximum of 9 m / 30 ft deep and 5 m / 16 ft wide, in relation to the camera's position. Participants seated outside the horizontal field of view (80°) will not be detected. Room conditions such as lighting, also impact the camera's ability to detect people.

Cameras limited to best overview

(i.e., Room Kit Mini, Webex Desk, Desk Pro, and Desk Limited Edition)

- Best overview is supported.
- Group framing and closeup are not supported.

Set up the SpeakerTrack feature (page 3 of 4)

Sign in to the web interface, go to *Settings*, and select *Configurations*, to find the settings referred.

Configure speaker tracking

Speaker tracking

Cameras > SpeakerTrack > Mode

This setting is to turn speaker tracking on/off. [4]

Auto: Speaker tracking is enabled by default. Users can switch the mode on or off instantly from the camera control panel in the user interface, or for Boards, from the *Settings > Advanced Settings* panel on the Board itself.

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

Closeup

Cameras > SpeakerTrack > Closeup

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

Turn on/off the closeup feature.

Auto: The behavior depends on the device type. Boards will strive to keep everyone in the room in the camera frame at all times. The other devices will zoom in on the person speaking.

Off: The device will keep everyone in the room in the camera frame at all times.

On: The device will zoom in on the active speaker.

Whiteboard mode

Supported by the Room Kit, Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, and Room 70 G2.

Cameras > SpeakerTrack > Whiteboard mode

Refer to the ► Set up the Snap to Whiteboard feature chapter for details.

---

[4] For Webex Desk, Desk Pro, Desk Limited Edition, and Room Kit Mini, this setting applies to turning on and off the best overview.

Set up the SpeakerTrack feature (page 4 of 4)

Tracking mode

Applies to Codec Plus and Codec Pro, when these devices are using a SpeakerTrack 60 camera.

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

Cameras > SpeakerTrack > TrackingMode

Auto: This is the default setting.

Conservative: The device reacts slower to detected changes and delays switching the camera view.

Speaker track connector detection

Applies to Codec Plus and Codec Pro, when these devices are using a SpeakerTrack 60 camera.

In most cases the device detects automatically which inputs the left and right camera of the Speaker Track 60 are connected to. You should only set the connector detection mode to Manual if that's not the case.

Cameras > SpeakerTrack > ConnectorDetection > Mode

Auto: The device will automatically detect the video input.

Manual: Manually configure the video input for each individual camera. You should choose manual configuration in situations where the video conferencing device does not receive Extended Display Identification Data (EDID) information from the cameras.

If the connector detection mode is set to Manual, you must specify which video input connectors the left and right cameras are connected to.

Cameras > SpeakerTrack > ConnectorDetection > CameraRight

Cameras > SpeakerTrack > ConnectorDetection > CameraLeft

Set the number of the video input connectors that the left and right camera of the SpeakerTrack 60 are connected to.

Settings that are overidden by the speaker track functionality

Applies to Codec Plus and Codec Pro, when these devices are using a SpeakerTrack 60 camera.

These settings are changed automatically when speaker tracking is on:

- *Video > Input > Connector n > Quality*

  These settings are always forced to **Motion** for the connectors where the dual cameras are connected. If both settings are already set to **Motion**, there is no change.

- *Video > Input > Connector n > OptimalDefinition > Threshold60fps*

  These settings will stay untouched if they are already equal for the connectors where the dual cameras are connected. If they are not equal, the lowest threshold among the two is preferred.

- *Video > Input > Connector n > OptimalDefinition > Profile*

  These settings will stay untouched if they are already equal for the connectors where the dual cameras are connected. If they are not equal, the preferred setting is the first value in the list, (**Normal**, **Medium**, **High**) that one of the two settings has.

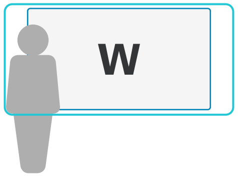
The settings above are restored to their previous values when speaker tracking is turned off. This is regardless of whether you have used the user interface or the *Cameras > SpeakerTrack > Mode* setting to turn off speaker tracking.

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

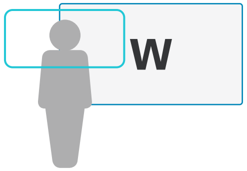
The Snap to Whiteboard feature extends the speaker tracking functionality, thus you need a camera that supports SpeakerTrack:

- Room Kit
- Codec Plus with Quad Camera (Room Kit Plus) or SpeakerTrack 60 camera
- Codec Pro with Quad Camera (Room Kit Pro) or SpeakerTrack 60 camera
- Room 55
- Room 55 Dual
- Room 70
- Room 70 G2

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

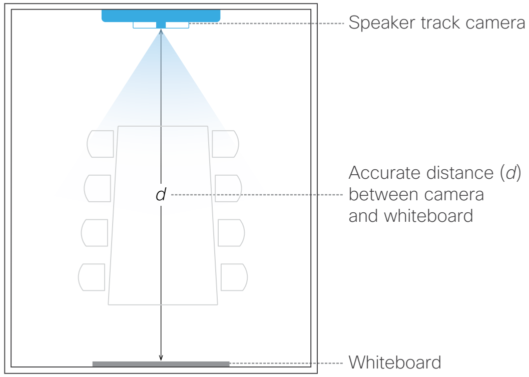


Without the Snap to Whiteboard extension, the camera captures only the person.



Preparations

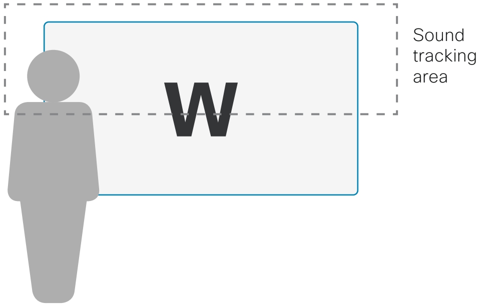
Whiteboard position



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

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

Speaker position



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

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

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

The Snap to Whiteboard wizard is only available when:

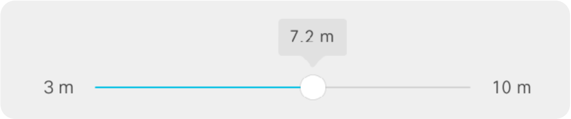
- *Cameras > SpeakerTrack > Mode* is **Auto**.

Define the whiteboard area

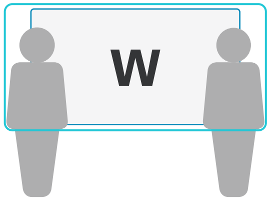
Use the wizard on the touch controller to define the whiteboard area.

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

   Sign in with ADMIN credentials if the *Settings* menu is passphrase protected on your device.
3. Tap *Configure* or *Reconfigure* to start the wizard (depends whether you configure the feature for the first time or not).
4. Follow the instructions in the wizard - use the back button ← if you want to redo a step, and the next button → to move to the next step:
   - Move the slider to set the distance between the camera and the whiteboard. It is important that the distance is measured accurately.



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



   - If you have a Codec Plus or Codec Pro with a SpeakerTrack 60 camera: Fine tune both cameras (pan, tilt, zoom) to show the same view.
   - Stand next to the whiteboard and start speaking.

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

Troubleshooting

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

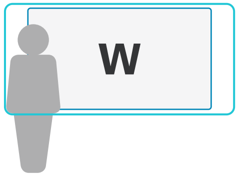
- Check that the whiteboard is placed across the room from the camera.
- Check that the distance between the camera and whiteboard is measured accurately.
- The person who is speaking must be close to the whiteboard. Furthermore, the person must stand upright so that the sound comes from the upper half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

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

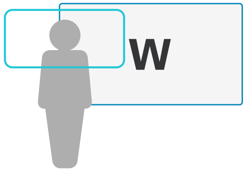
Enable and disable Snap to Whiteboard

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

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



Camera view when Snap to Whiteboard is *enabled*



Camera view when Snap to Whiteboard is *disabled*

From the touch controller

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

   Sign in with ADMIN credentials if the *Settings* menu is protected by a passphrase on your device.
3. Set the toggle switch to:

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

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

From the web interface

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
2. Find the *Cameras > SpeakerTrack > Whiteboard > Mode* setting.

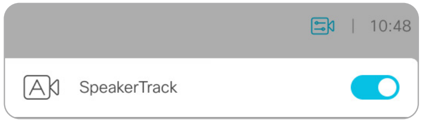
   On: Snap to Whiteboard is enabled, and the camera will capture both the person that speaks and the whiteboard he or she is standing next to.

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

How to switch on speaker tracking

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

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



Set up the PresenterTrack feature (page 1 of 4)

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

The following cameras and video conferencing devices support PresenterTrack:

- Codec Plus with Precision 60 or SpeakerTrack 60 camera
- Codec Pro with Precision 60 or SpeakerTrack 60 camera
- Room 55 Dual with Precision 60 as external camera
- Room 70 with Precision 60 as external camera
- Room 70 G2 with Precision 60 as external camera

Capabilities and limitations

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

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

Considerations before placing the camera

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

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

Stage area

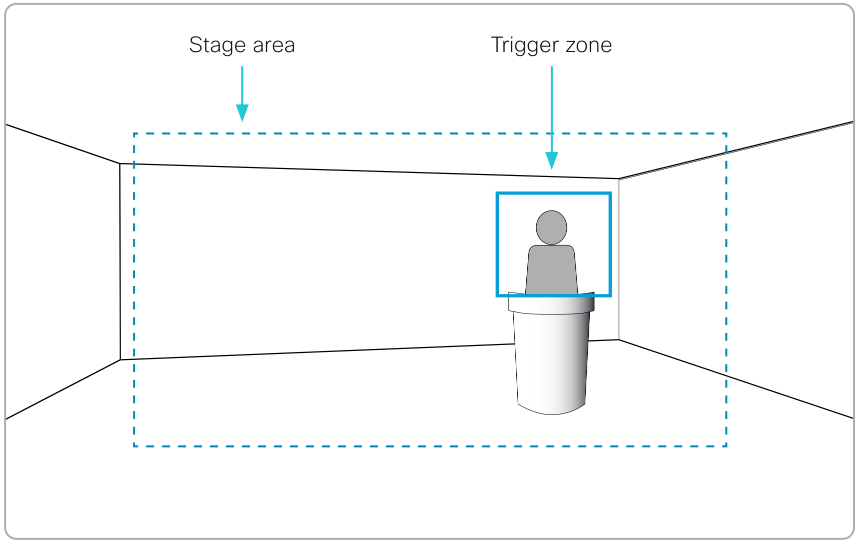
The stage area is the zoomed-out overview image.

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

Trigger zone

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

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



Set up the PresenterTrack feature (page 2 of 4)

Set up and test PresenterTrack

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

1. Sign in to the web interface and go to *Settings*. Select *Audio and Video*, and open the *Presenter Track* sub-tab.
2. Toggle on *Enable PresenterTrack* and click *Configure* to open the configuration page.

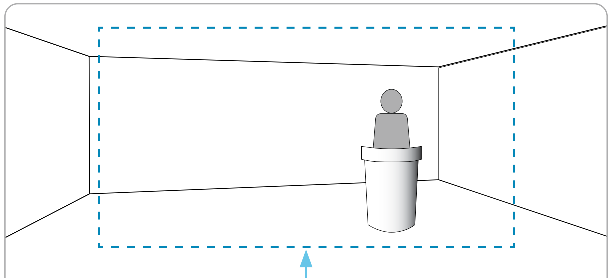
   Opening this page deactivates standby and presenter tracking, enables the self-view in full screen, and shows the trigger zone rectangle on the screen of the device.

   ⚠ Don't leave this web page without clicking *Done*, otherwise the trigger zone rectangle stays visible on the screen of the device.

   Alternatively, you can remove the rectangle by tapping the *Camera icon* on the touch controller and choose a camera position from the list.

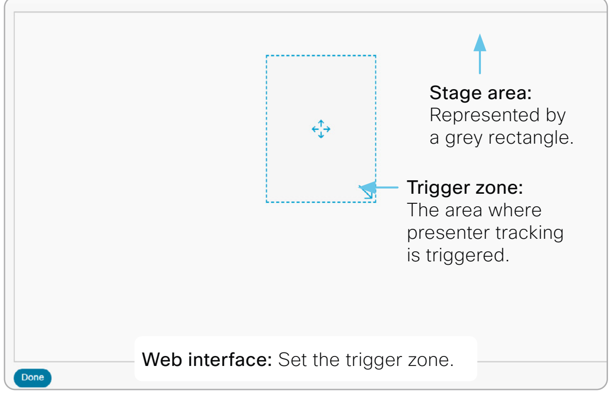
3. Choose a camera from the *Camera source* drop down list and use the camera controls (zoom, pan, tilt) on the touch controller to define the stage area.

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

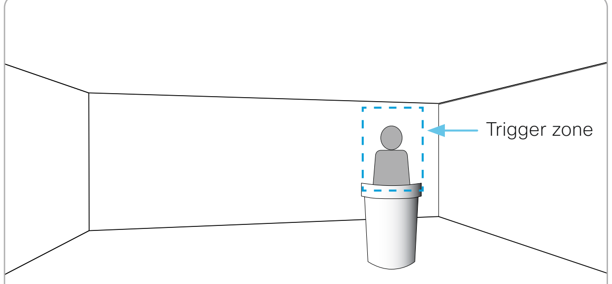


Stage area: The zoomed-out overview image. Large enough for the presenter to move around. When the presenter leaves the stage area the tracking stops.

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


Stage area: Represented by a grey rectangle.
Trigger zone: The area where presenter tracking is triggered.
Done

Web interface: Set the trigger zone.



Video conferencing device screen: See the video from the room when you set the trigger zone.

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

5. Click *Done*.

Set up a polygonal trigger zone

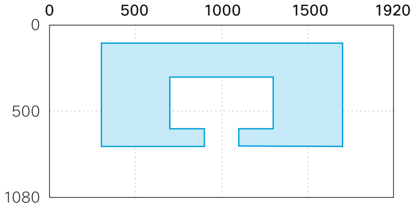
You can set up only rectangular trigger zones from the *Presenter Track* web page.

If you want to define a more advanced polygonal trigger zone, you must go to *Settings*, select *Configurations*, and find the *Cameras > PresenterTrack > TriggerZone* setting.

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

Example:

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



The coordinates of the vertices are:

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

The corresponding setting value is:

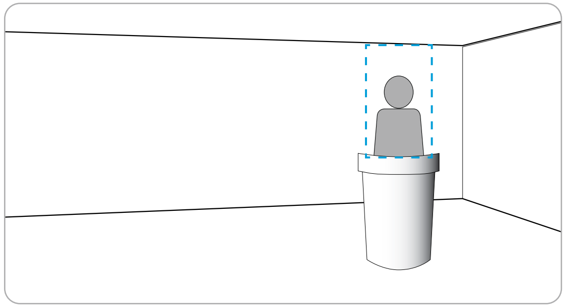
Cameras > PresenterTrack > TriggerZone: 300,100,1700,100,1700,700,1100,700, 1100,600,1300,600,1300,300,700,300, 700,600,900,600,900,700,300,700

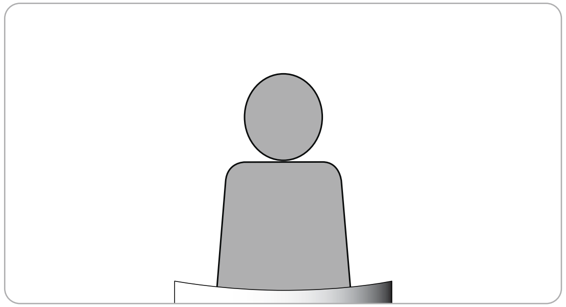
Set up the PresenterTrack feature (page 3 of 4)

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

   This activates presenter tracking.

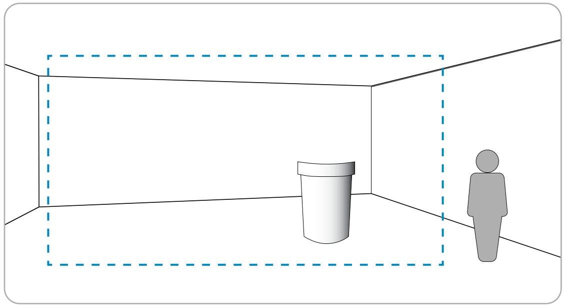
7. Position yourself in the trigger zone and see that the camera zooms in on you.





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

9. Check that presenter tracking stops when you leave the stage.



If something fails, go back to step 3, 4 and 5 to adjust the size and location of the stage area and the trigger zone.

For more troubleshooting help, you can switch on PresenterTrack *Diagnostics Mode*, as described on the next page.

Temporarily activate or deactivate PresenterTrack

During a meeting, you can use the touch controller to temporarily activate or deactivate presenter tracking.

1. Tap the *Camera* icon in the status bar.
2. Select *Presenter* in the list of camera positions to activate presenter tracking.

   Deselect *Presenter* in the list of camera positions to deactivate presenter tracking.

If presenter tracking has been deactivated, the presenter must enter the trigger zone again in order for tracking to start.

Set up the PresenterTrack feature (page 4 of 4)

Diagnostics mode

The PresenterTrack diagnostics mode may be a helpful tool when troubleshooting an issue. In order to set the device in diagnostics mode, you have to use the xAPI of the device.

Sign in to the xAPI and run the following command:

- `xCommand Cameras PresenterTrack Set Mode: Diagnostic`

In this mode, you see the stage area (the zoomed-out overview image) on the screen, and an overlay with the following indicators::

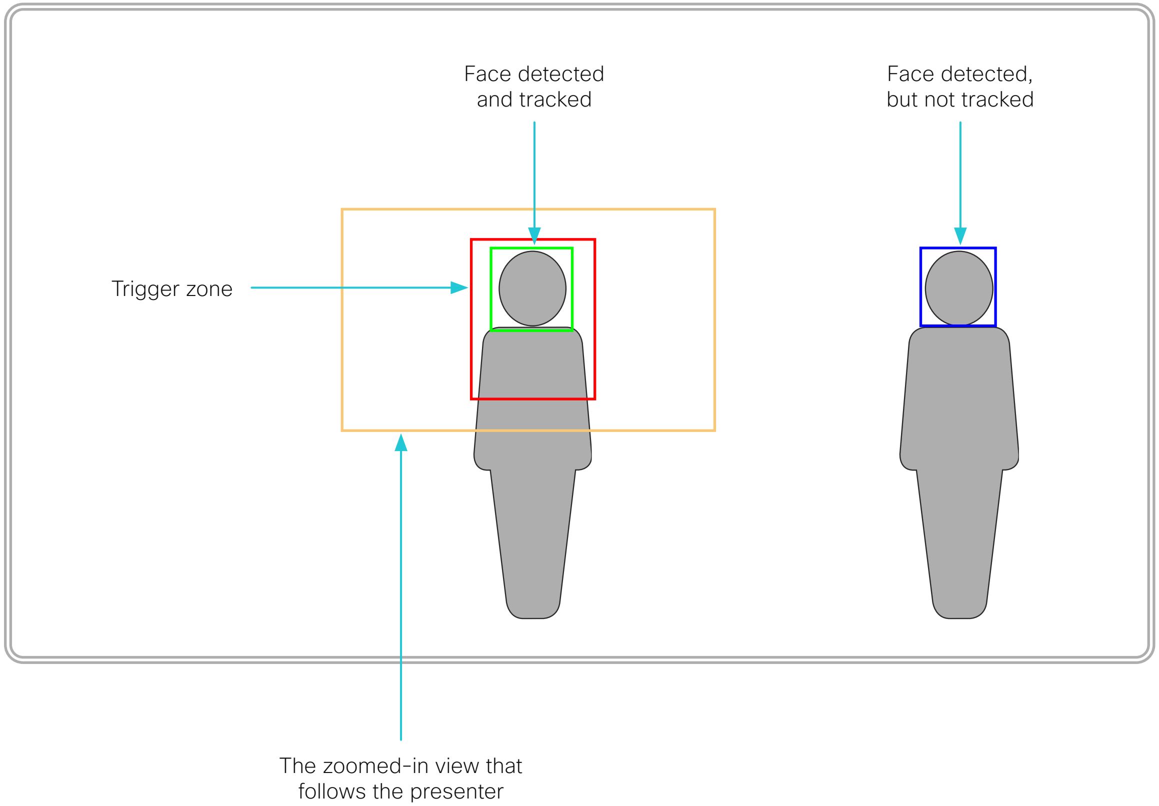
☐ RED frame: The trigger zone.

☐ YELLOW frame: The zoomed-in view of the presenter.

☐ GREEN frame: A face that is detected and tracked.

🟩🟥 GREEN or RED blinking filled frame: Face detections. Green color indicates a high confidence, red color indicates a low confidence.

☐ BLUE: A face is detected but the face is not tracked.


Face detected and tracked
Face detected, but not tracked
Trigger zone
The zoomed-in view that follows the presenter

Briefing room set-up (page 1 of 7)

The *Briefing room* set-up makes it easy to set up, manage, and use a room to deliver training and education sessions to groups of people.

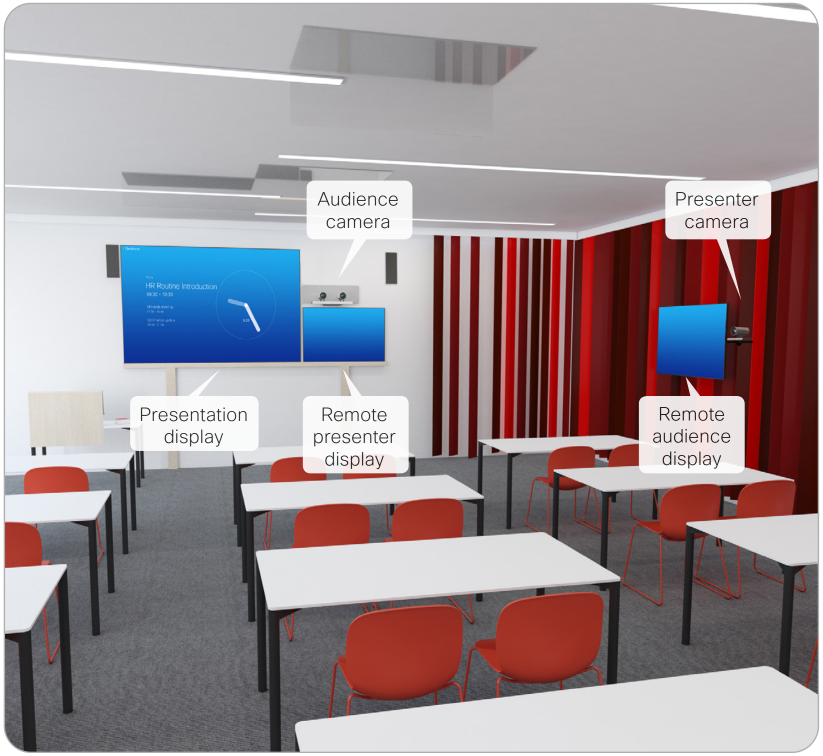
The *Briefing room* set-up has the following predefined room modes that accommodate different scenarios::

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

The *Briefing room* set-up is available as a room type template. When you set up a room using a template, a set of configurations is pushed automatically to the device. It is important that the room is set up correctly, and that the cameras and screens are connected exactly as specified. Otherwise the configurations will not match the room.

Required equipment

- One of the following devices:
  - Codec Pro
  - Room 70 G2
- Three displays (Presentation display, Remote presenter display, and Remote audience display)
- Two cameras (Audience camera and Presenter camera)
- Microphones
- Speakers
- Touch controller



Briefing room set-up [*]

Classroom versus Briefing Room set-up

The *Classroom* set-up is more flexible than the *Briefing room* set-up in the number of screens and how the layout is distributed on the screens. Also, more products support *Classroom*.

Classroom

- Supported products: Codec Plus, Codec Pro, Room 55 Dual, Room 70, and Room 70 G2
- You can use any number of screens that the device supports, typically two or three. Use the video monitor settings to configure the distribution of layouts on the screens, if the default behavior does not fulfill your requirements.

Briefing room

- Supported products: Codec Pro and Room 70 G2
- The set-up requires three screens, and the layouts on the screens are preconfigured (and fixed) to match that particular scenario.

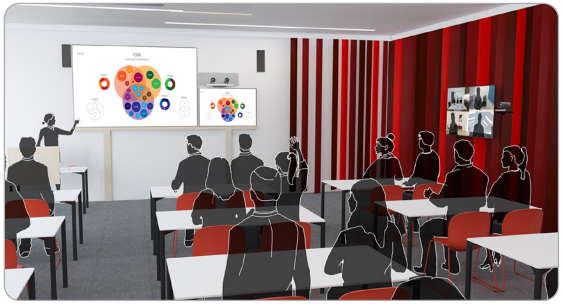
---

[*] The illustration shows a codec with Speaker Track 60 camera as audience camera. The same principle applies also to the supported integrated devices, and other supported codec and camera combinations.

Briefing room set-up (page 2 of 7)

Room modes*

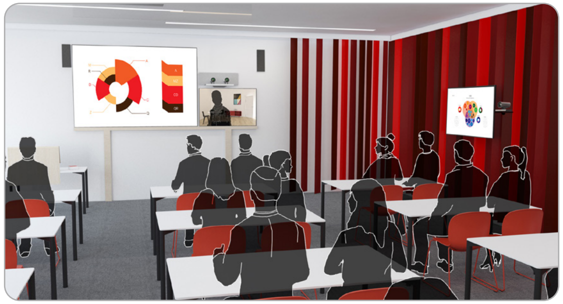
Local Presenter mode



The presenter is in the room. This mode also covers the case when someone in the local audience asks a question (Q&A).

If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* detects a presenter in the room.

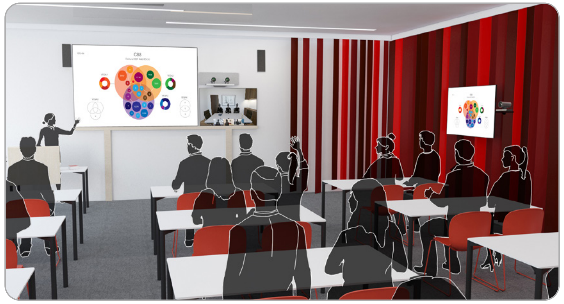
Remote Presenter mode



The presenter is calling in.

If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* doesn't detect a presenter in the room.

Discussion mode



For discussions between different sites. A local presenter is in the room.

Always use the touch controller to activate this mode.

	Local Presenter mode	**Remote Presenter mode**	**Discussion mode**
Video sent to the far end	Sends video from the *Presenter camera* Q&A: Sends split-screen video from the *Presenter camera* and the person asking the question (*Audience camera*)	Sends video from the *Audience camera*	Sends video from the *Audience camera*
Remote presenter display	Shows the presentation	Shows the presenter that is calling in, and other remote sites (you can decide the layout locally)	Shows the remote sites that are part of the discussion (you can decide the layout locally)
Presentation display	Shows the presentation	Shows the presentation	Shows the presentation
Remote audience display	Shows the remote participants that are calling in from different sites	Shows the presentation	Shows the presentation

If there is no presentation, nothing will be shown on the corresponding screens (gray).

---

* The illustrations show a codec with Speaker Track 60 camera as audience camera. The same principle applies also to the supported integrated devices, and other supported codec and camera combinations.

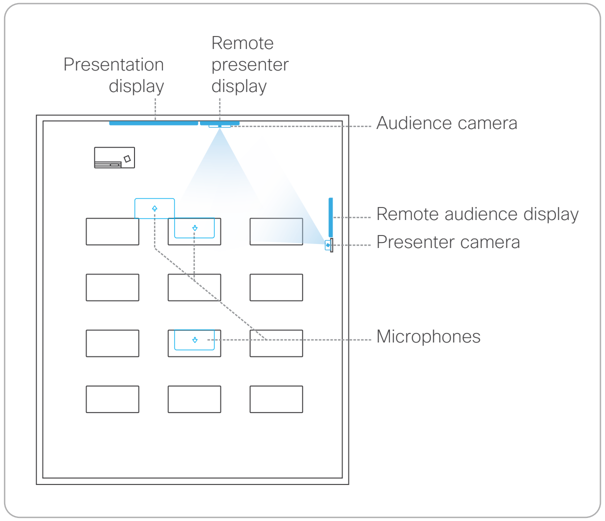
Briefing room set-up (page 3 of 7)

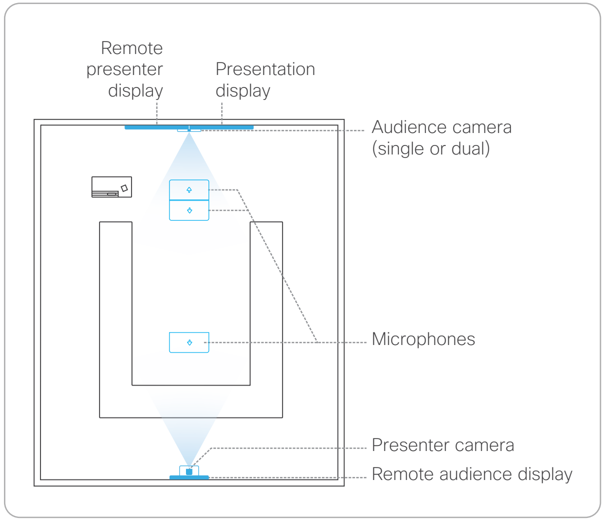
Room arrangement examples

These illustrations show examples of how to arrange screens, cameras and microphones, and where to place people for the best experience.

Recommendation

- *Remote presenter display:* 1st screen, placed at front. For integrated devices, this is its (left) screen.
- *Presentation display:* 2nd screen, placed at front. For integrated devices with two screens, this is its right screen.
- *Remote audience display:* 3rd screen, placed on the side or at the back, so that the local presenter can see the remote audience.
- *Audience camera:* Use the integrated camera for video conferencing devices that have that. For other devices, we recommend the Cisco Quad Camera or Cisco TelePresence SpeakerTrack 60 camera. We recommend a camera with speaker tracking, but it is also possible to use a camera without speaker tracking capabilities.
- *Presenter camera:* Cisco TelePresence Precision 60 with presenter tracking enabled.
- *Microphones:* We recommend the Cisco TelePresence Ceiling Microphone for good coverage of the room. Also other microphone solutions can be used.
- *Speakers:* Use the integrated speakers for video conferencing devices that have that. For other devices, we recommend good quality stereo speakers placed next to the *Presentation display* at the front of the room.

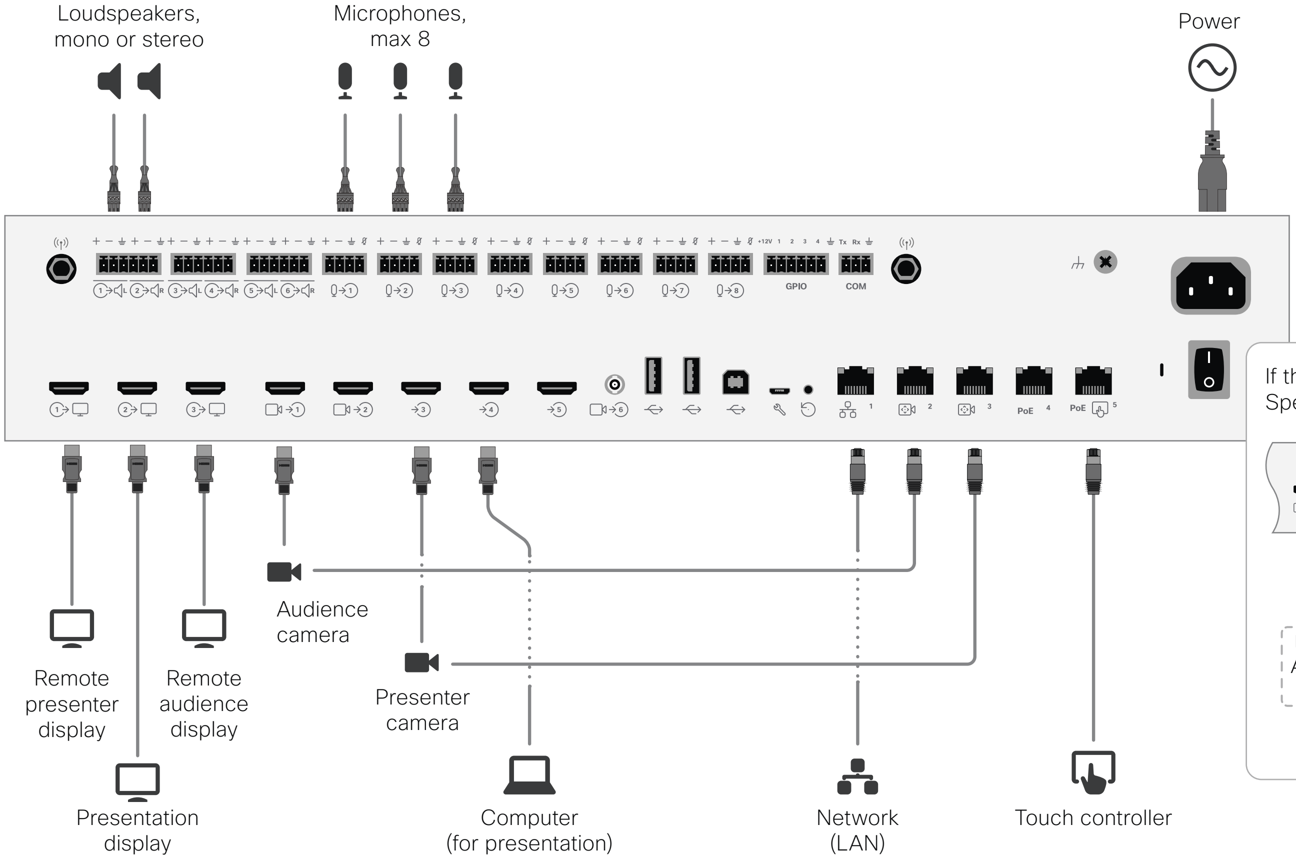

Presentation display
Remote presenter display
Audience camera
Remote audience display
Presenter camera
Microphones


Remote presenter display
Presentation display
Audience camera (single or dual)
Microphones
Presenter camera
Remote audience display

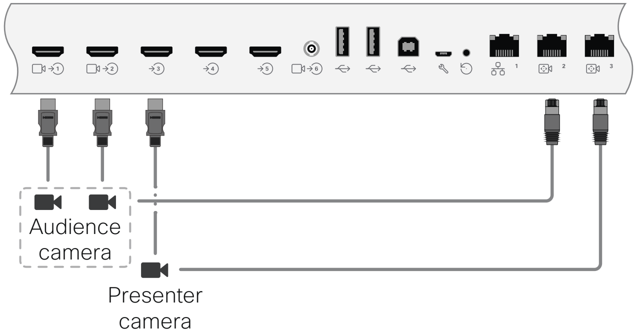
Briefing room set-up (page 4 of 7)

Codec Pro: Connect cables

⚠ Connect the cameras to the device as shown in the illustrations. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Briefing* room type template, match your actual set-up.


Loudspeakers, mono or stereo
Microphones, max 8
Power
GPIO
COM
PoE
Remote presenter display
Remote audience display
Audience camera
Presenter camera
Presentation display
Computer (for presentation)
Network (LAN)
Touch controller

If the *Audience Camera* is a Cisco TelePresence SpeakerTrack 60 camera, then it uses two HDMI inputs.

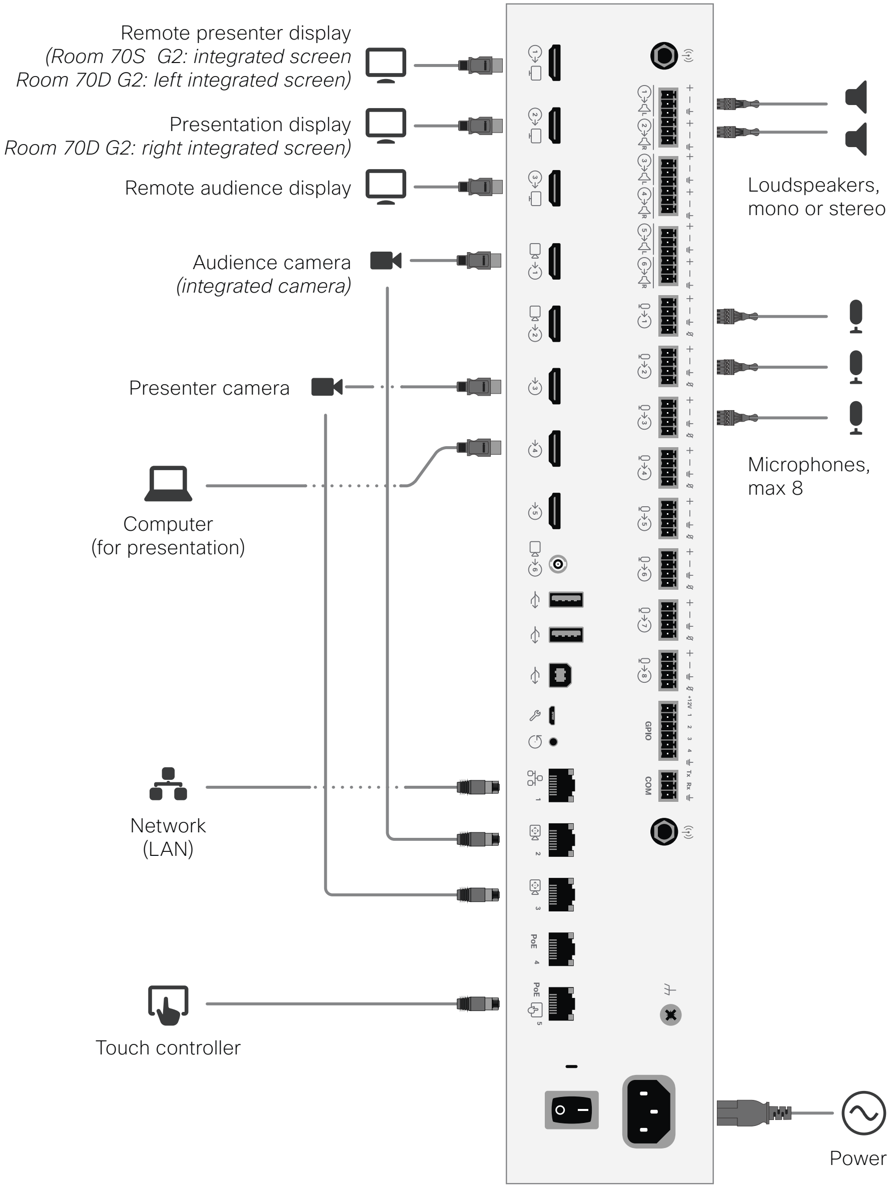

Audience camera
Presenter camera

Briefing room set-up (page 5 of 7)

Room 70 G2: Connect cables

⚠ Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Briefing* room type template, match your actual set-up.

Keep all preconnected cables, including the cables for the integrated camera and screens, as delivered from the factory. **You only have to connect the external screens and cameras.**


Remote presenter display
(Room 70S G2: integrated screen
Room 70D G2: left integrated screen)
Presentation display
Room 70D G2: right integrated screen)
Remote audience display
Audience camera
(integrated camera)
Presenter camera
Computer
(for presentation)
Network
(LAN)
Touch controller
Loudspeakers,
mono or stereo
Microphones,
max 8
Power

Briefing room set-up (page 6 of 7)

Configure the device

We recommend you to be in the same room when setting up the Briefing room. Otherwise you are not able to set up PresenterTrack properly.

1. Connect cameras and screens as described on the previous page.
2. Use the touch controller to stop sharing the video from the *Presenter camera*. It is important that video from the *Presenter camera* is not displayed on any screen while setting up Briefing room.
3. Sign in to the web interface, go to *Settings*, and select *Configurations*.
4. Go to *Video > Input > Connector 3*, and set the following:
    - *InputSourceType*: camera
    - *PresentationSelection*: Manual
    - *Quality*: Motion
    - *Visibility*: Never
    - *CameraControl Mode*: On

    Click *Save* for the changes to take effect.
5. Set up PresenterTrack for the *Presenter camera*, see the ▶ Set up the PresenterTrack feature chapter.

    This feature enables the camera to follow a presenter that is moving about on stage.
6. Go to *Settings*, and select *Configurations*. Find *Cameras > PresenterTrack > PresenterDetectedStatus* and choose whether to enable (default) or disable automatic switching between *Local Presenter* and *Remote Presenter* modes.

    Click *Save* for the changes to take effect.
7. Go to *Settings*, and select *Room Types*. Click the *Briefing* thumbnail to push the corresponding configuration to the device.

Switching between room modes

Switching between room modes (*Local Presenter, Remote Presenter, Discussions*), which implies that camera input sources, and remote and local screen layouts, are changed, can be done in two ways:

- Automatically, based on who is speaking and whether a local presenter is present on stage.

    Automatic switching is only between the *Local Presenter* and *Remote Presenter* modes. The room mode doesn't change automatically if the current mode is *Discussion*.

    Automatic swtiching is supported only when the PresenterTrack feature enabled (*Cameras > PresenterTrack > Enabled* set to True).
- Manually, using the buttons on the touch controller.

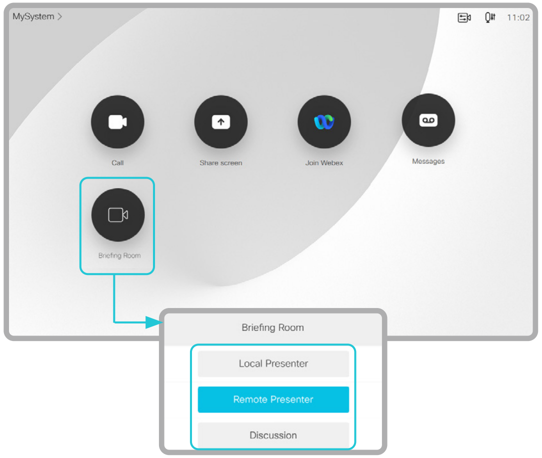
Automatic switching implies:

- The device switches to the *Local Presenter* mode when a person is detected in the PresenterTrack trigger zone.
- The device switches to the *Remote Presenter* mode when the local presenter, who is tracked, leaves the stage.
- If someone in the local audience asks a question when the device is in *Local Presenter* mode, the device sends split-screen video showing both the presenter and the person asking the question. This requires a SpeakerTrack 60 or Quad Camera as *Audience camera*, and that speaker tracking is switched on.

Switch between room modes manually

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

1. Tap *Briefing Room* on the touch controller.
2. Tap the mode you want to change to: *Local Presenter, Remote Presenter*, or *Discussion*. The current mode is highlighted.



Briefing room set-up (page 7 of 7)

Limitations

Not supported functionality when using *Briefing Room*:

- MultiSite (embedded multipoint switch)
- Content sharing to Proximity clients
- Directional audio
- Snap to Whiteboard
- Active control (selection of layouts from CMS)

Classroom set-up (page 1 of 8)

The *Classroom* set-up makes it easy to set up, manage, and use a room to deliver training and education sessions to groups of people.

The *Classroom* set-up is available as a room type template. When you set up a room using a template, a set of configurations is pushed automatically to the device. It is important that the room is set up correctly, and that the cameras are connected exactly as specified. Otherwise the configurations will not match the room.

Required equipment

- One of the following devices:
  - Codec Plus
  - Codec Pro
  - Room 55 Dual
  - Room 70
  - Room 70 G2
- One or more screens (configurable)
- Two cameras (Audience camera and Presenter camera)
- Microphones
- Speakers
- Touch controller

Limitations

Not supported functionality when using Classroom:

- MultiSite (embedded multipoint switch)
- Content sharing to Proximity clients
- Directional audio
- Snap to Whiteboard
- Active control (selection of layouts from CMS)

Room modes

The *Classroom* set-up has the following predefined room modes that accommodate different scenarios: Local Presenter, Remote Presenter, and Discussion.

Local Presenter mode

- The presenter is in the room. This mode also covers the case when someone in the local audience asks a question (Q&A).
- If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* detects a presenter in the room.
- Sends video from the *Presenter camera* to the far end. In the Q&A case: Sends split-screen video from the *Presenter camera* and the person asking the question (*Audience camera*) to the far end.

Remote Presenter mode

- The presenter is calling in.
- If automatic switching is enabled (default), the device switches to this mode when the *Presenter camera* doesn't detect a presenter in the room.
- Sends video from the *Audience camera* to the far end.

Discussion mode

- For discussions between different sites. A local presenter is in the room.
- Always use the touch controller to activate this mode.
- Sends video from the *Audience camera* to the far end.

Classroom versus Briefing Room set-up

The *Classroom* set-up is more flexible than the *Briefing room* set-up in the number of screens and how the layout is distributed on the screens. Also, more products support *Classroom*.

Classroom

- Supported products: Codec Plus, Codec Pro, Room 55 Dual, Room 70, and Room 70 G2
- You can use any number of screens that the device supports, typically two or three. Use the video monitor settings to configure the distribution of layouts on the screens, if the default behavior does not fulfill your requirements.

Briefing room

- Supported products: Codec Pro and Room 70 G2
- The set-up requires three screens, and the layouts on the screens are preconfigured (and fixed) to match that particular scenario.

Classroom set-up (page 2 of 8)

Room arrangement examples

These illustrations show examples of how to arrange screens, cameras and microphones, and where to place people for the best experience.

Recommendation

Audience camera:

- Use the integrated camera for video conferencing devices that have that. For other devices, we recommend the Cisco Quad Camera or Cisco TelePresence SpeakerTrack 60 camera. We recommend a camera with speaker tracking, but it is also possible to use a camera without speaker tracking capabilities.

Presenter camera:

- Cisco TelePresence Precision 60 with presenter tracking enabled.

Microphones:

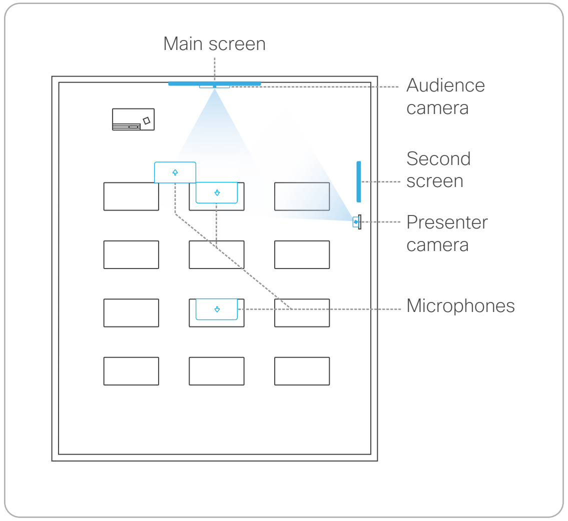
- We recommend the Cisco TelePresence Ceiling Microphone for good coverage of the room. Also other microphone solutions can be used.

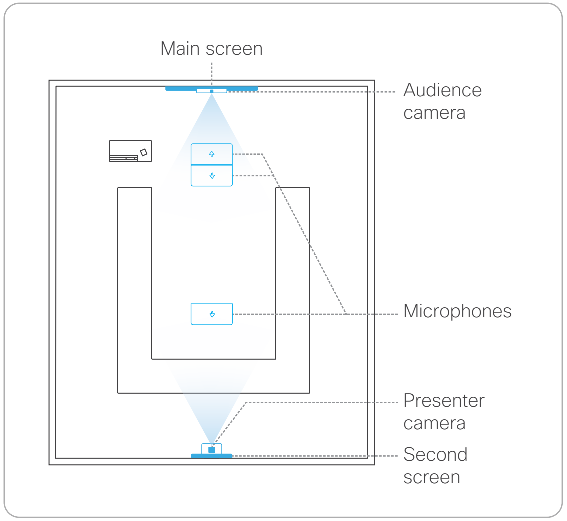
Speakers:

- Use the integrated speakers for video conferencing devices that have that. For other devices, we recommend good quality stereo speakers placed next to the main screen at the front of the room.

Screens:

- You can use one or more screens (the maximum number of screens depends on your type of device).
- For most set-ups, we recommend that you use two screens or more. Place the main screen at the front of the room. Place a second screen on the side or at the back, so that the local presenter can see the remote audience.

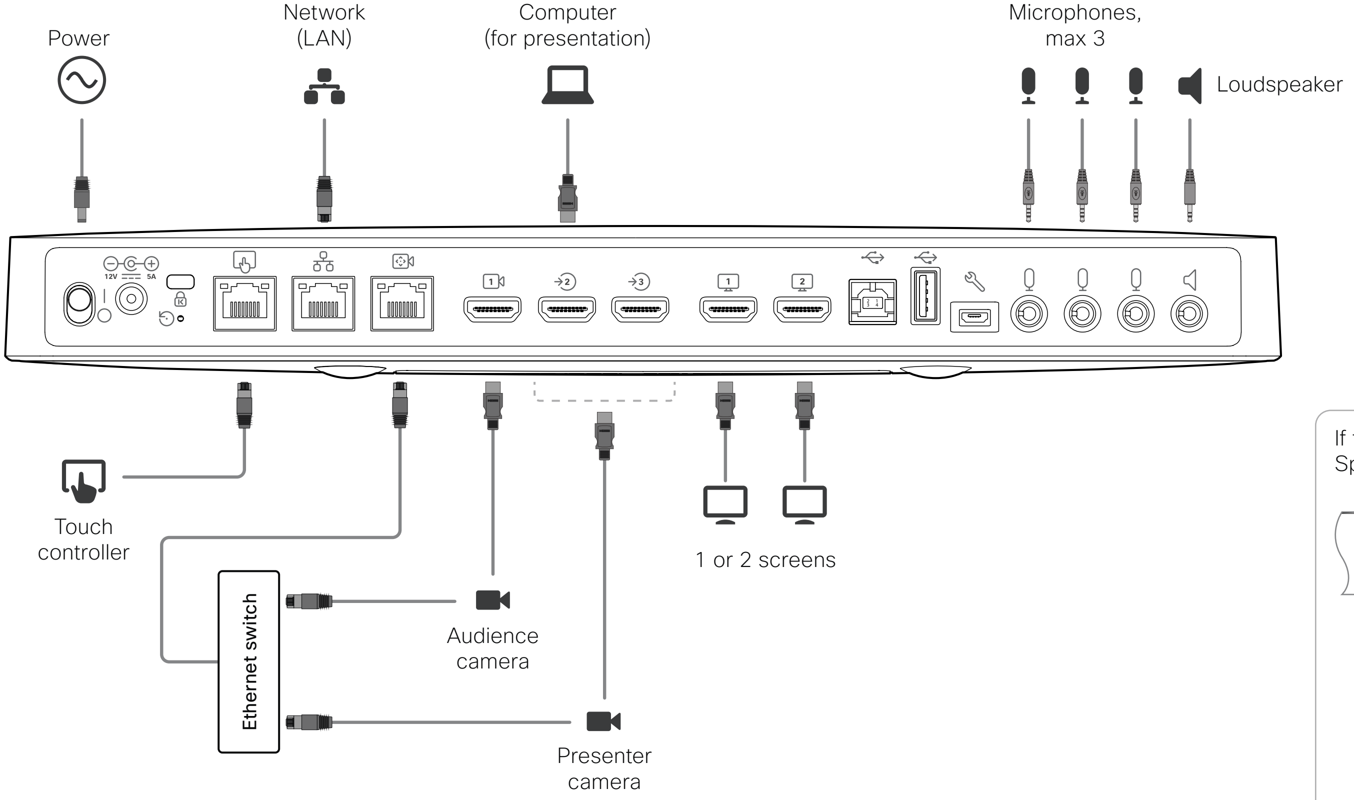




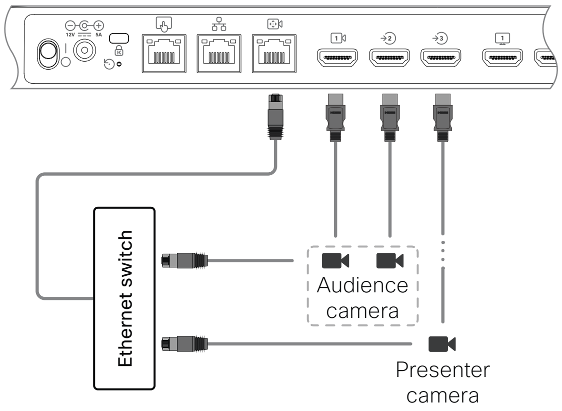
Classroom set-up (page 3 of 8)

Codec Plus: Connect cables

⚠ Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Classroom* room type template, match your actual set-up.


Power
Network (LAN)
Computer (for presentation)
Microphones, max 3
Loudspeaker
Touch controller
Ethernet switch
Audience camera
Presenter camera
1 or 2 screens

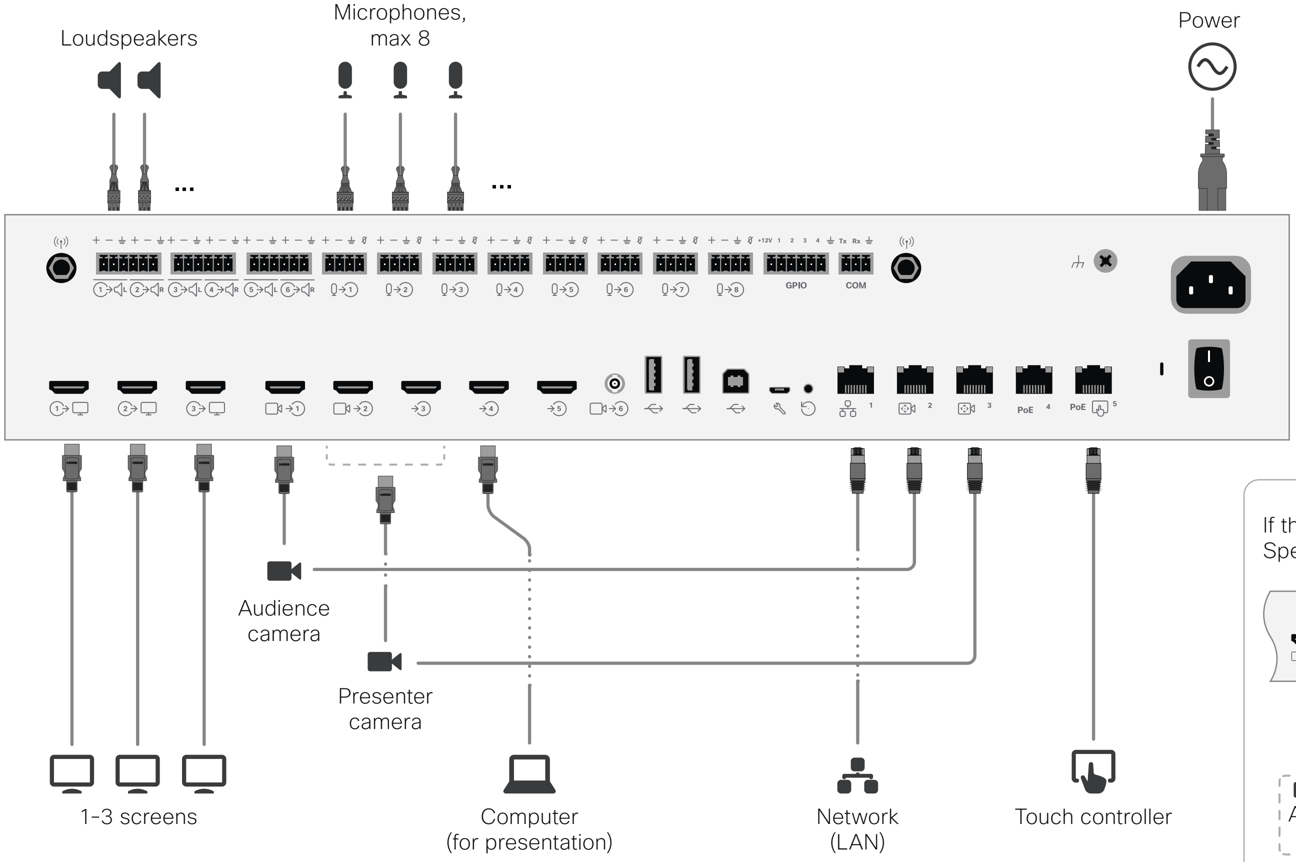
If the *Audience Camera* is a Cisco TelePresence SpeakerTrack 60 camera, then it uses two HDMI inputs.


Ethernet switch
Audience camera
Presenter camera

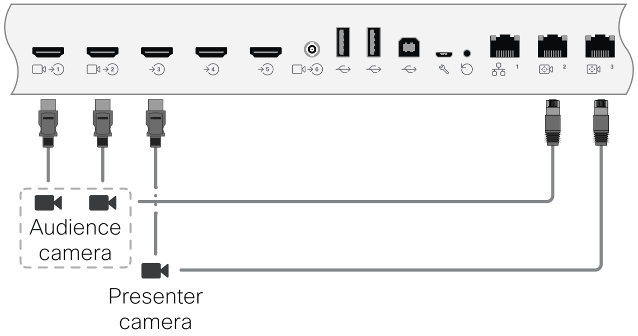
Classroom set-up (page 4 of 8)

Codec Pro: Connect cables

⚠ Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Classroom* room type template, match your actual set-up.


Loudspeakers
Microphones, max 8
Power
GPIO
COM
PoE
PoE
Audience camera
Presenter camera
1-3 screens
Computer (for presentation)
Network (LAN)
Touch controller

If the *Audience Camera* is a Cisco TelePresence SpeakerTrack 60 camera, then it uses two HDMI inputs.

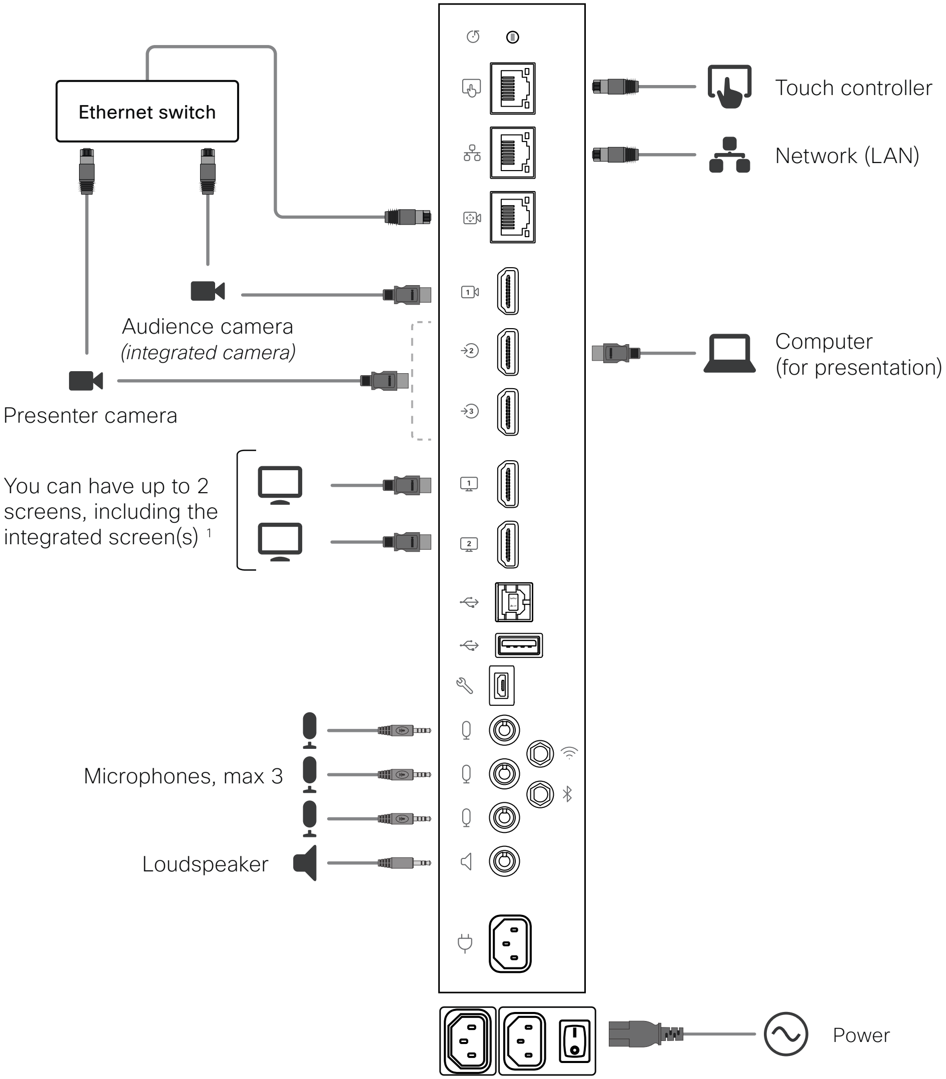

Audience camera
Presenter camera

Classroom set-up (page 5 of 8)

Room 55 Dual and Room 70: Connect cables

⚠ Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Classroom* room type template, match your actual set-up.

Keep all preconnected cables, including the cables for the integrated camera and screens, as delivered from the factory. **You only have to connect the external screens and cameras.**


Ethernet switch
Touch controller
Network (LAN)
Audience camera
(integrated camera)
Presenter camera
Computer
(for presentation)
You can have up to 2 screens, including the integrated screen(s) 1
Microphones, max 3
Loudspeaker
Power

---

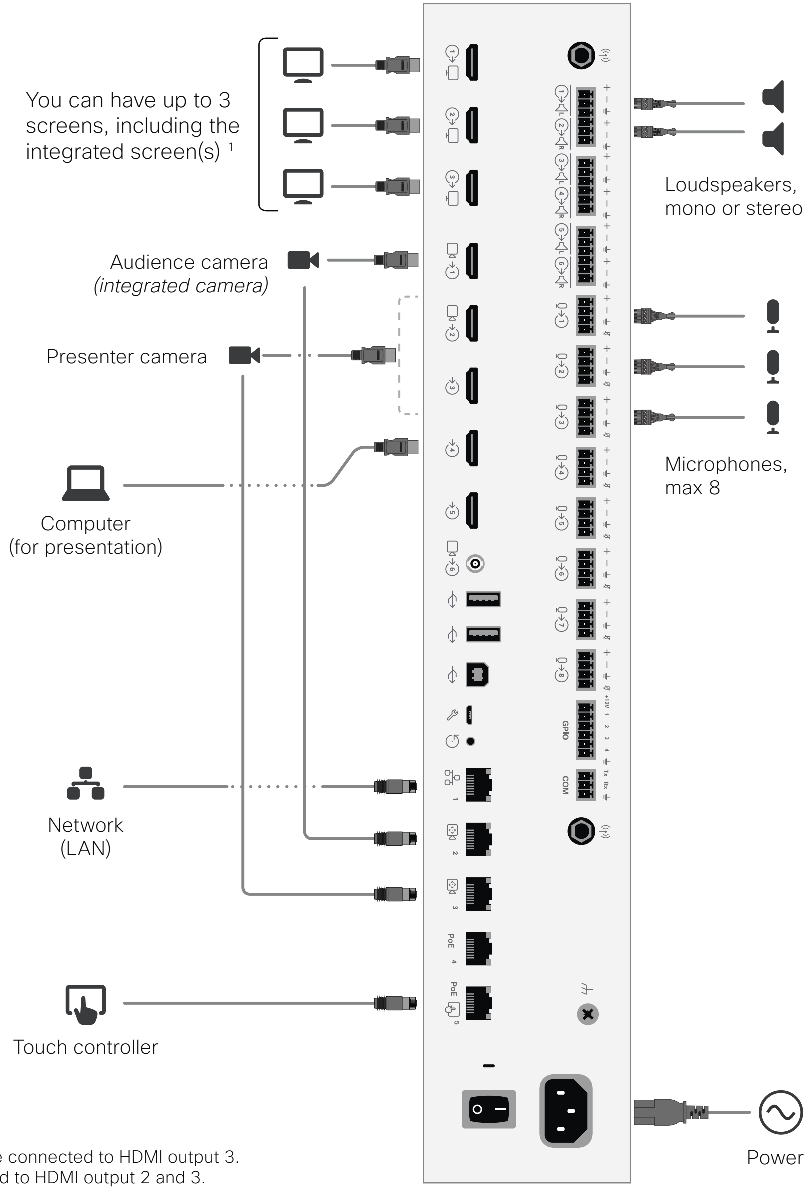
[1] *Room 55 Dual and Room 70 Dual:* HDMI outputs 1 and 2 are for the integrated screens of the device. External screens are not supported.
Room 70 Single: HDMI output 1 is for the integrated screen of the device. An external screen may be connected to HDMI output 2.

Classroom set-up (page 6 of 8)

Room 70 G2: Connect cables

Connect the cameras to the device as shown in the illustration. Following the illustration ensures that the configurations that are automatically pushed to the device when selecting the *Classroom* room type template, match your actual set-up.

Keep all preconnected cables, including the cables for the integrated camera and screens, as delivered from the factory. **You only have to connect the external screens and cameras.**


You can have up to 3 screens, including the integrated screen(s) [1]
Audience camera
(integrated camera)
Presenter camera
Computer
(for presentation)
Network
(LAN)
Touch controller
Loudspeakers, mono or stereo
Microphones, max 8
Power
GPIO
COM
PoE

---

[1] *Room 70 Dual G2:* HDMI outputs 1 and 2 are for the integrated screens of the device. An external screen may be connected to HDMI output 3.
Room 70 Single G2: HDMI output 1 is for the integrated screen of the device. External screens may be connected to HDMI output 2 and 3.

Classroom set-up (page 7 of 8)

Configure the device

We recommend you to be in the same room when setting up the Classroom. Otherwise you are not able to set up PresenterTrack properly.

1. Connect cameras and screens as described on the previous pages.
2. Use the touch controller to stop sharing the video from the *Presenter camera*. It is important that video from the *Presenter camera* is not displayed on any screen while setting up Classroom.
3. Sign in to the web interface, go to *Settings*, and select *Configurations*.
4. Go to *Video > Input > Connector n*, and set the following (*n* is the number of the Connector where the *Presenter Camera* is connected):
    - *InputSourceType*: camera
    - *PresentationSelection*: Manual
    - *Quality*: Motion
    - *Visibility*: Never
    - *CameraControl Mode*: On

    Click *Save* for the changes to take effect.
5. Set up PresenterTrack for the *Presenter camera*, see the ▶ Set up the PresenterTrack feature chapter.

    This feature enables the camera to follow a presenter that is moving about on stage.
6. Go to *Settings*, and select *Configurations*. Find *Cameras > PresenterTrack > PresenterDetectedStatus* and choose whether to enable (default) or disable automatic switching between *Local Presenter* and *Remote Presenter* modes.

    Click *Save* for the changes to take effect.

    Read more about switching between modes on the next page.
7. If the default screen and layout behavior does not suit your set-up, you must configure the screens and layouts using the following settings:
    - *Video > Monitors*: Defines the number of different layouts in your room set-up.
    - *Video > Output > Connector n > MonitorRole*: Defines which layout each screen gets. Screens with different monitor roles get different layouts.

    Refer to the chapter about connecting monitors for details.
8. Go to *Settings*, and select *Room Types*. Click the *Classroom* thumbnail to push the corresponding configuration to the device.

Classroom set-up (page 8 of 8)

Switching between room modes

Switching between room modes (*Local Presenter, Remote Presenter, Discussions*), which implies that camera input sources, and remote and local screen layouts, are changed, can be done in two ways:

- Automatically, based on who is speaking and whether a local presenter is present on stage.

  Automatic switching is only between the *Local Presenter* and *Remote Presenter* modes. The room mode doesn't change automatically if the current mode is *Discussion*.

  Automatic swtiching is supported only when the PresenterTrack feature enabled (*Cameras > PresenterTrack > Enabled* set to **True**).
- Manually, using the buttons on the touch controller.

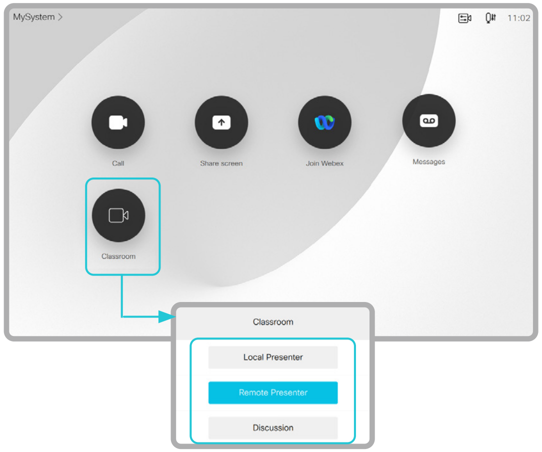
Automatic switching implies:

- The device switches to the *Local Presenter* mode when a person is detected in the PresenterTrack trigger zone.
- The device switches to the *Remote Presenter* mode when the local presenter, who is tracked, leaves the stage.
- If someone in the local audience asks a question when the device is in *Local Presenter* mode, the device sends split-screen video showing both the presenter and the person asking the question. This behavior requires a SpeakerTrack 60 or Quad Camera as *Audience camera*, and that speaker tracking is switched on.

Switch between room modes manually

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

1. Tap *Classroom* on the touch controller.
2. Tap the mode you want to change to: *Local Presenter*, *Remote Presenter*, or *Discussion*. The current mode is highlighted.



Test the loudspeaker connections (page 1 of 3)

It is crucial for the conferencing experience that the device's loudspeakers are correctly connected to the codec.

Correct cabling ensures that sound meant to be coming from the right loudspeakers actually comes from the right speakers, and the sound meant to be coming from the left loudspeakers comes from the left speakers. If the speaker cables are incorrectly connected this will not happen.

You must be in the same room as the video conferencing device when you test the loudspeaker connections. If the speaker test reveals any issues, you must reconnect the cables.

Room 55 Dual, Room 70, Room 70 G2, and Room 70 Panorama

We have provided a speaker check tool that you can run to verify that the loudspeakers are correctly connected. The speaker in the camera module is also included in the test.

Sign in to the web interface and go to *Developer API*.

Run the loudspeaker check

1. Enter the following command in the *Execute Commands and Configurations* text area: [*]

   ```
   xCommand Audio SpeakerCheck
      MeasurementLength: <number of
   seconds>
      Volume: <test-signal volume>
   ```

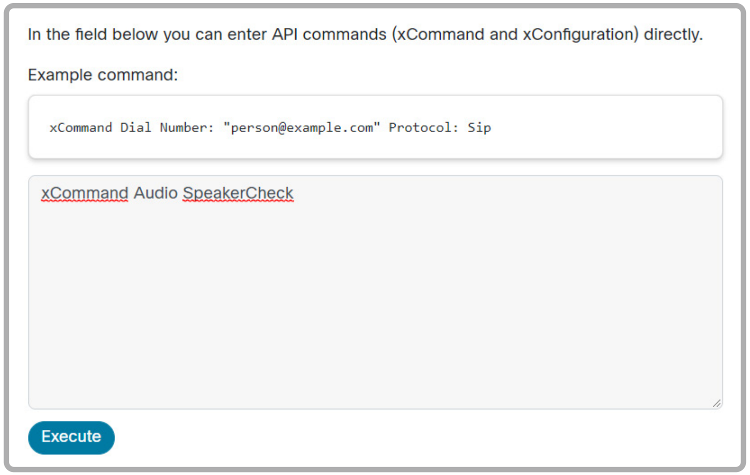
   If you leave out the `MeasurementLength` and `Volume` parameters, the test signal is emitted for 1 second from each speaker, and the volume is 1.

2. Click *Execute*.

   The speaker check will now run, and a test signal will be emitted from each speaker, in sequence from left to right.

3. Listen for the test signals.

   If one or more speakers do not make a sound, or the sequence is not strictly from left to right, you have to reconnect the loudspeaker cables and run the speaker check again.



In the field below you can enter API commands (xCommand and xConfiguration) directly.

Example command:

```
xCommand Dial Number: "person@example.com" Protocol: Sip
```

```
xCommand Audio SpeakerCheck
```

---

[*] Syntax and semantics are explained in the API guide for the device.

Test the loudspeaker connections (page 2 of 3)

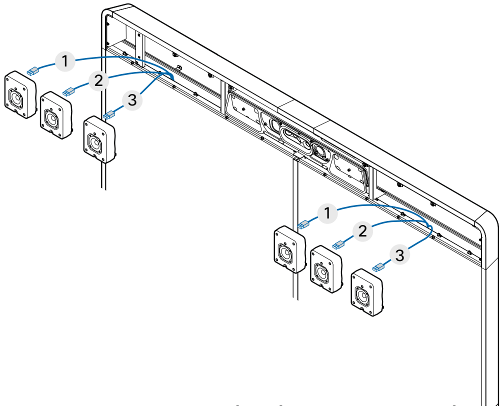
How to reconnect cables

Check the *Installation Guide* for the product for all details.

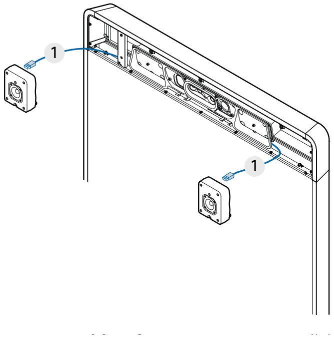
1. Remove the device's upper textile grille. It snaps to magnets.
2. Unscrew the screw that fastens the loudspeaker (Torx T20). Then, release the speaker gently from its peg.
3. Disconnect the cable that is connected incorrectly, and connect the correct cable.

   The cables are marked with a number. Check the illustrations to see which cable should be connected to which loudspeaker.

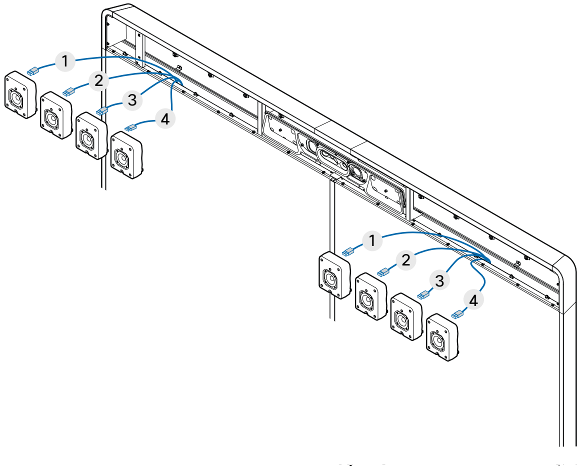
Room 55 Dual



Room 70 Single and Room 70 Single G2



Room 70 Dual, Room 70 Dual G2, Room 70 Panorama



Test the loudspeaker connections (page 3 of 3)

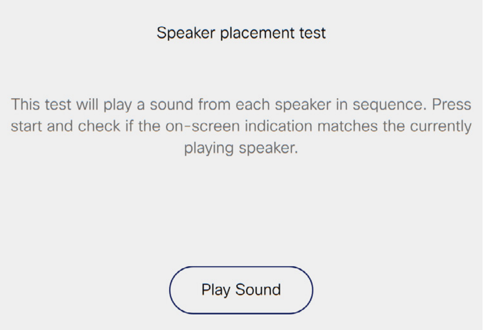
Room Panorama

The loudspeaker test is included in the Room Panorama setup assistant. This is described in the Getting Started guide for the product.

You can also start the test manually from the touch controller.

When you perform the loudspeaker test, a sound plays from each loudspeaker in sequence.

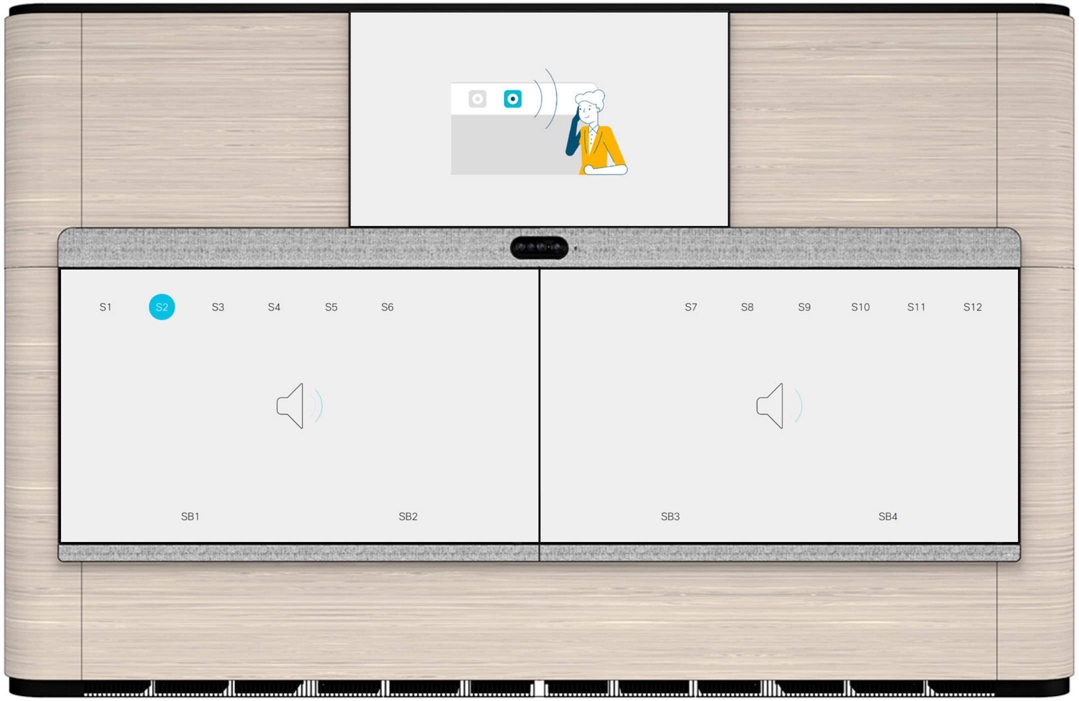
1. Tap *Settings > Issues and diagnostics > Manual speaker check > Play Sound* to start the test.



Speaker placement test

This test will play a sound from each speaker in sequence. Press start and check if the on-screen indication matches the currently playing speaker.

2. Tap *Next* to listen to the next loudspeaker, or *Previous* to go back and listen to the previous loudspeaker again.



While running the test the graphics on the screens show a number close to the position of each loudspeaker. The number close to the loudspeaker that is supposed to play is marked with blue color.

- S1-S12: The loudspeakers above the screens (behind the speaker grille)
- SB1-SB4: The subwoofers below the screens (behind the cosmetic panels)

If the loudspeakers and subwoofers are connected correctly, you will hear that the sound is played from the speaker in the position that is marked with blue.

If the loudspeakers play out of order, or a loudspeaker doesn't play at all, you must check the cabling. Read the Getting Started guide to find how to fix the problem.

Using extra loudspeakers and sound reinforcement

When using the device with local sound reinforcement, extra loudspeakers are strongly recommended to ensure that people in the room get the good auditory experience.

The Audio Console, found on the web interface for the device, is the recommended tool for setting up local reinforcement. See the *Using Extra Loudspeakers and Sound Reinforcement* guide for a comprehensive description and best practices for the solution. Go to:

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

Bluetooth® headset

The following Bluetooth profiles are supported:

- HFP (Hands-Free Profile)
- A2DP (Advanced Audio Distribution Profile)
- The headset must support both HFP and A2DP or HFP-only. Headsets with A2DP-only is not supported.

A Bluetooth headset is supported directly with the embedded Bluetooth radio or using a USB Bluetooth dongle. Multiple headsets can be paired to the video conferencing device, but only one can be connected at a time.

The range is up to 10 m (30 ft). If you move outside the range when in a call, the audio will switch to the speakers on the video conferencing device.

Most headsets have built in volume controls. When in a call, the volume of the headset and video conferencing device is synchronized. When not in a call, the volume buttons on the headset and video conferencing device operates independently.

Supported Bluetooth features:

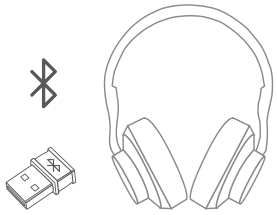
- Answer an incoming call
- Hold and Resume a call
- Reject an incoming call
- Hang up a call
- Volume up and down
- Some headsets have mute control. This operates independently from the mute control on the video conferencing device.

USB Bluetooth dongle

- When using a USB Bluetooth dongle the headset is detected as a USB headset.
- There will be no synchronization of headset volume and video conferencing device volume when using a dongle.
- We have tested Cisco 700 USB Adapter, Jabra Link 360, Jabra Link 370, Plantronics BT300 and Plantronics BT600; though others might work as well.

Pairing a Bluetooth headset

1. Activate Bluetooth pairing on the headset. Refer to the instruction manual for the headset if in doubt.
2. Select the device name or address at the top of the user interface. Select *Settings*, followed by *Bluetooth*. If Bluetooth is disabled, turn it on. Bluetooth is enabled by default.
3. The video conferencing device will scan for Bluetooth devices. Upon successful discovery the Bluetooth headset should be displayed in the device list.
4. Select the device and pairing begins. It may take a few seconds for the pairing to complete.
5. If the pairing is successful the video conferencing device will now list the headset as connected. The pairing is now completed.



You may use Bluetooth pairing directly to the video conferencing device, or use a USB dongle

Switch between devices

You can switch between the speaker on the video conferencing device and the devices that are connected via Bluetooth or USB.

Select the icon (☎ / 🎧 / 🎧 / 🔊 / ᛒ) in the status bar of the user interface, and choose from the available devices.

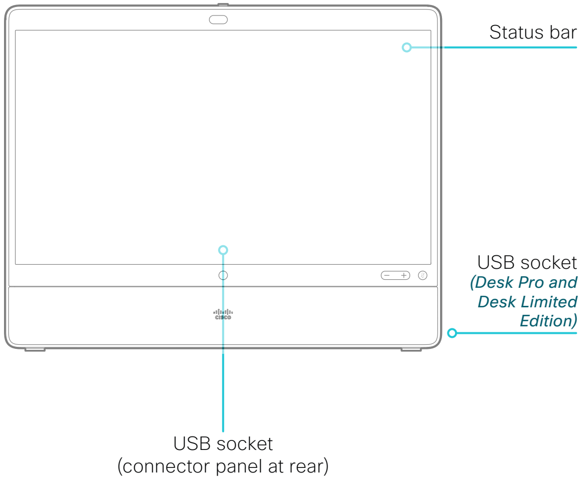
🔊 Speakers

🎧 Analog headset

🎧 USB headset

☎ USB handset

ᛒ Bluetooth device


Status bar
USB socket *(Desk Pro and Desk Limited Edition)*
USB socket
(connector panel at rear)

Connect the touch controller (page 1 of 8)

Depending on the type of video conferencing device, the touch controller[*] can be connected in the following ways:

- Directly to the video conferencing device *(not supported by Boards)*
- Paired to the device via the network (LAN). The is referred to as remote pairing.

Connecting the touch controller directly to the video conferencing device

Applies to: All products except Boards

Room Panorama: The Room Panorama installation has an Ethernet switch that is mounted under the table, or close to the table. Connect the touch controller to this switch, and not directly to the codec.

Room Panorama supports up to two touch controllers.

Other products: Connect the touch controller to the video conferencing device's dedicated touch controller port (RJ-45) as illustrated on the next pages.

Note that the Room Kit does not provide Power over Ethernet (PoE), so you need a mid-span PoE injector to power the touch controller.

Touch controller set-up

The touch controller is powered over Ethernet (PoE). Once connected, the set-up procedure begins. Follow the instructions on screen.

If the touch controller 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. The touch controller restarts after the upgrade.

Connecting the touch controller to the video conferencing device via the network (LAN)

Connect the touch controller and the video conferencing device to network wall sockets or to a network switch as illustrated.

Touch controller set-up

Once the touch controller 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 controller 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 the touch controller needs software upgrade, new software will be downloaded from the device and installed on the unit automatically as part of the set-up procedure. The touch controller restarts after the upgrade.

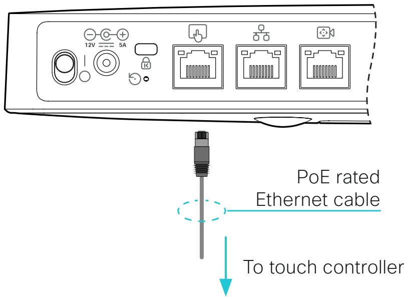
---

[*] Supported touch controllers: Touch 10 (shown in illustrations) and Room Navigator. However, Board 55 and 70 (not S Series) support only Touch 10.

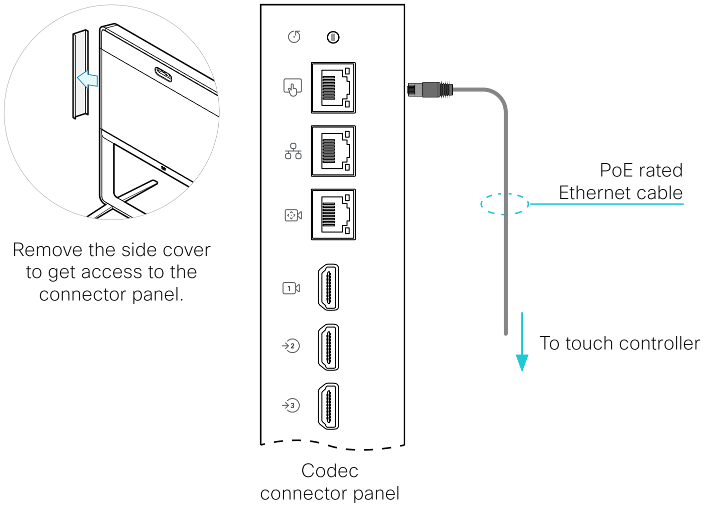
Connect the touch controller (page 2 of 8)

Connecting the touch controller directly to the video conferencing device

Codec Plus

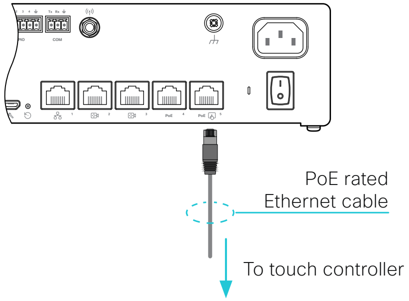

PoE rated Ethernet cable
To touch controller

Room 55 Dual and Room 70

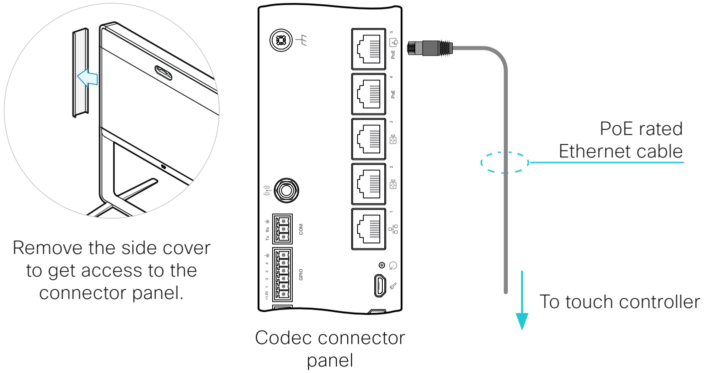

PoE rated Ethernet cable
To touch controller
Codec connector panel

Remove the side cover to get access to the connector panel.

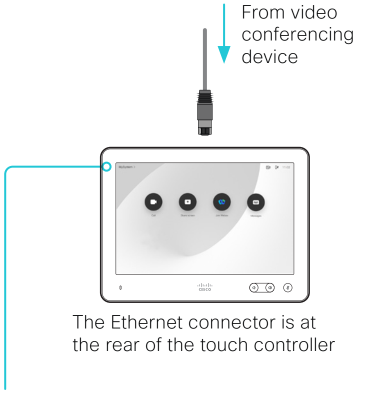
Codec Pro


PoE rated Ethernet cable
To touch controller

Room 70 G2 and Room 70 Panorama


PoE rated Ethernet cable
To touch controller
Codec connector panel

Remove the side cover to get access to the connector panel.


From video conferencing device

The Ethernet connector is at the rear of the touch controller

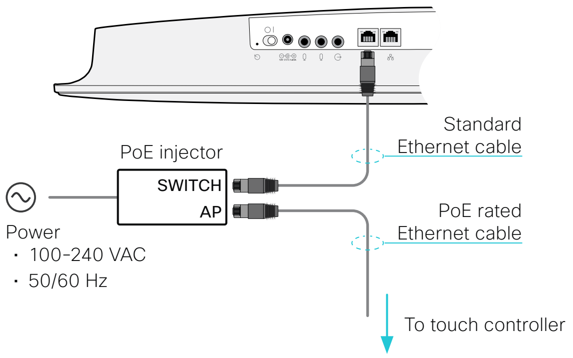
Contact information

The video conferencing device's name or address is displayed in the status bar when the touch controller is successfully connected to the device.

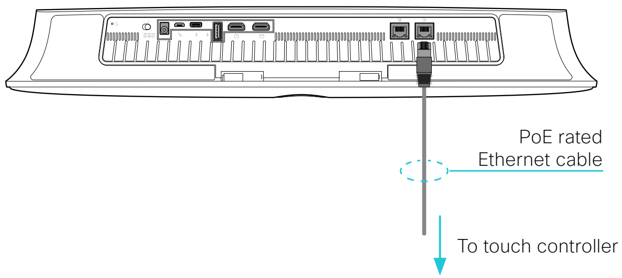
Connect the touch controller (page 3 of 8)

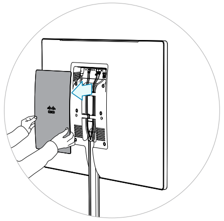
Connecting the touch controller directly to the video conferencing device

Room Kit


Standard
Ethernet cable
PoE injector
SWITCH
AP
Power
• 100-240 VAC
• 50/60 Hz
PoE rated
Ethernet cable
To touch controller

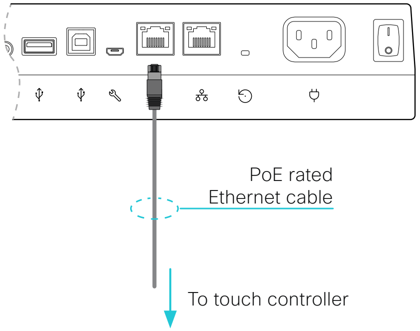
Room Kit Mini


PoE rated
Ethernet cable
To touch controller

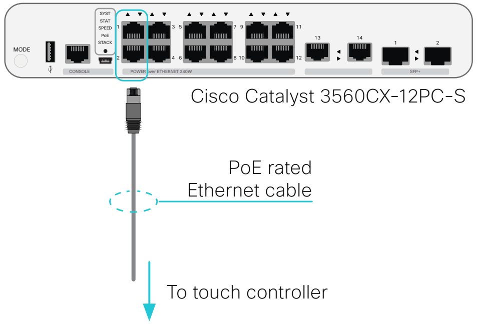


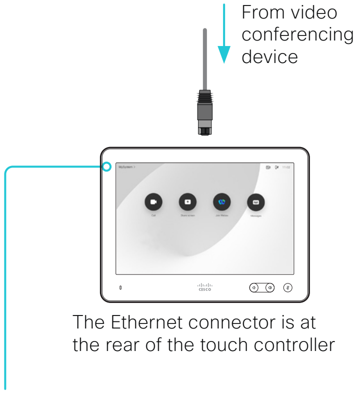
Remove the rear cover to get access to the connector panel and power switch.

Room 55


PoE rated
Ethernet cable
To touch controller

Room Panorama


Cisco Catalyst 3560CX-12PC-S
PoE rated
Ethernet cable
To touch controller


From video
conferencing
device
The Ethernet connector is at
the rear of the touch controller

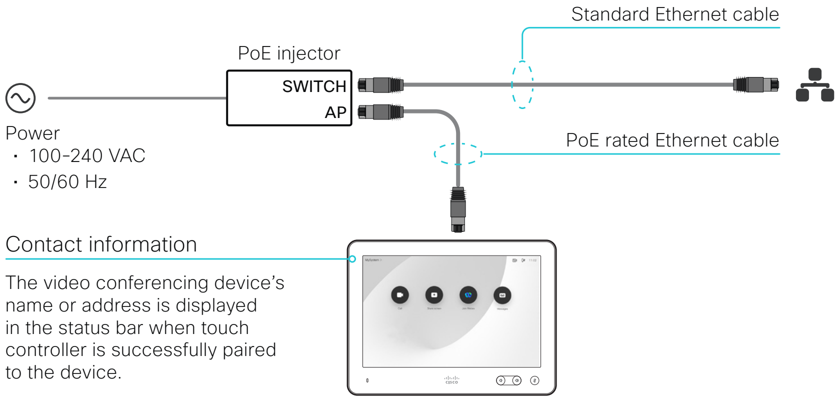
Contact information

The video conferencing device's name or address is displayed in the status bar when the touch controller is successfully connected to the device.

Connect the touch controller (page 4 of 8)

Connecting the touch controller to the video conferencing device via the network (LAN)

Touch controller


Standard Ethernet cable
PoE injector
SWITCH
AP
Power
• 100-240 VAC
• 50/60 Hz
PoE rated Ethernet cable
Contact information

The video conferencing device's name or address is displayed in the status bar when touch controller is successfully paired to the device.

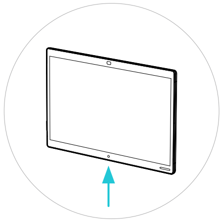
The Ethernet connector is at the rear of touch controller.

Network (LAN)

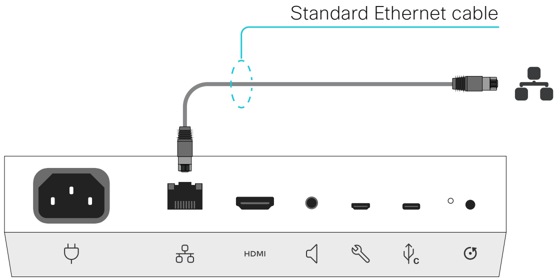
If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; The touch controller should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

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

Boards



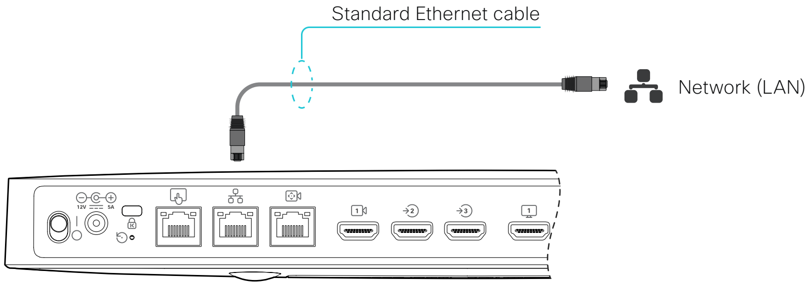
The connector panel is at the bottom, rear side.


Standard Ethernet cable
Network (LAN)
HDMI

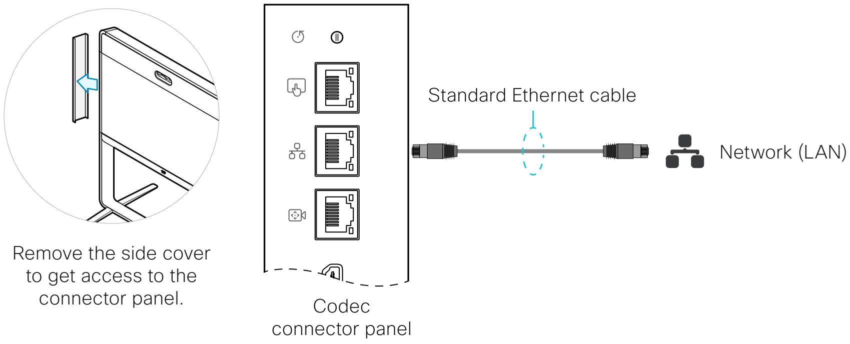
Connect the touch controller (page 5 of 8)

Connecting the touch controller to the video conferencing device via the network (LAN)

Codec Plus

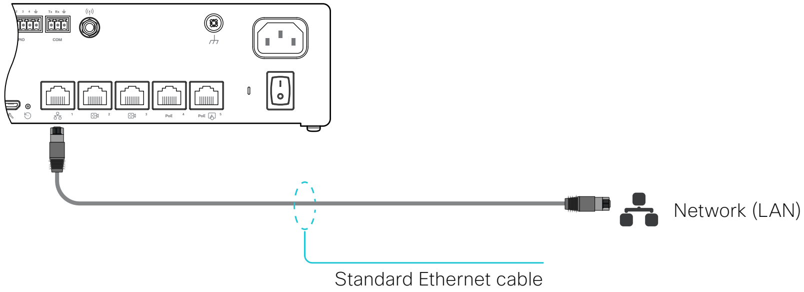

Standard Ethernet cable
Network (LAN)

Room 55 Dual and Room 70

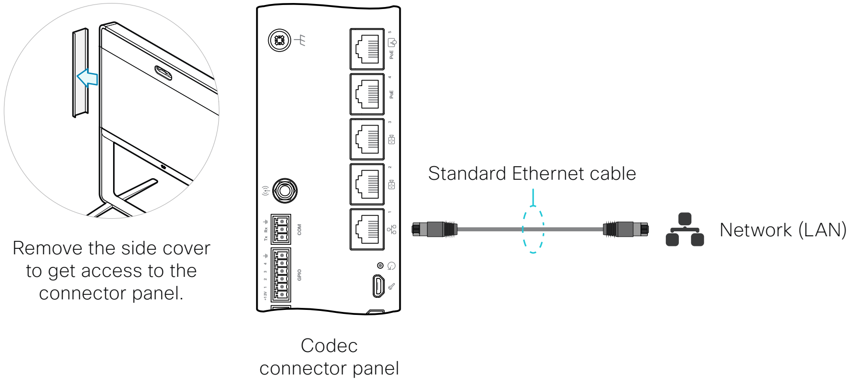

Standard Ethernet cable
Network (LAN)
Codec connector panel

Remove the side cover to get access to the connector panel.

Codec Pro and Room Panorama


Network (LAN)
Standard Ethernet cable

Room 70 G2 and Room 70 Panorama

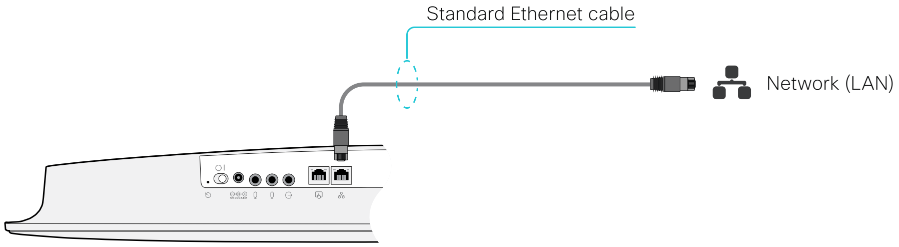

Standard Ethernet cable
Network (LAN)
Codec connector panel

Remove the side cover to get access to the connector panel.

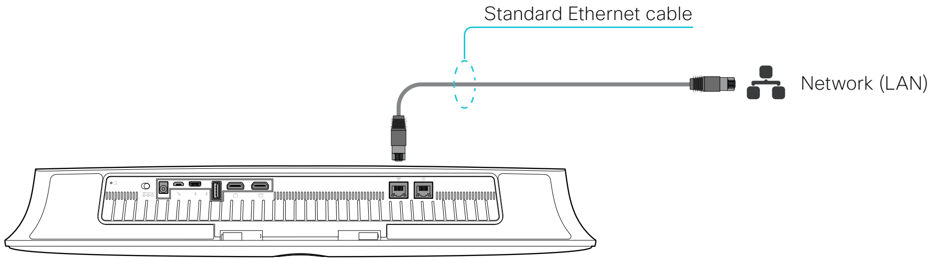
Connect the touch controller (page 6 of 8)

Connecting the touch controller to the video conferencing device via the network (LAN)

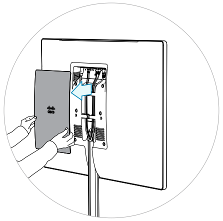
Room Kit


Standard Ethernet cable
Network (LAN)

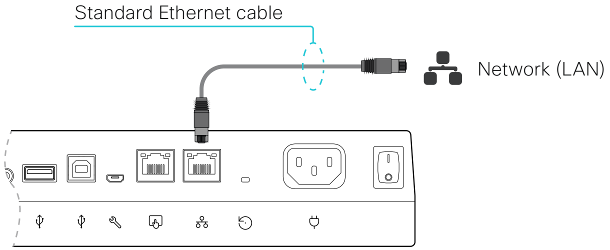
Room Kit Mini


Standard Ethernet cable
Network (LAN)

Room 55



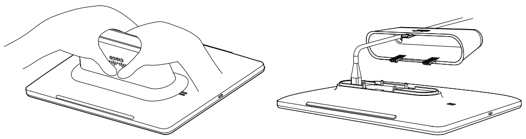
Remove the rear cover to get access to the connector panel and power switch.


Standard Ethernet cable
Network (LAN)

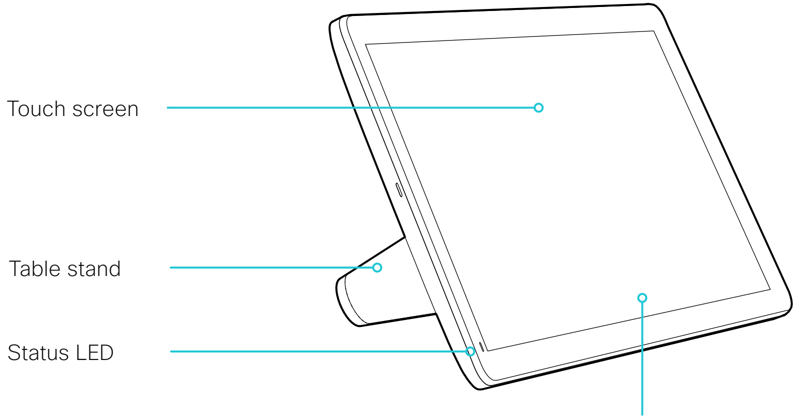
Connect the touch controller (page 7 of 8)

Cisco Webex Room Navigator physical interface

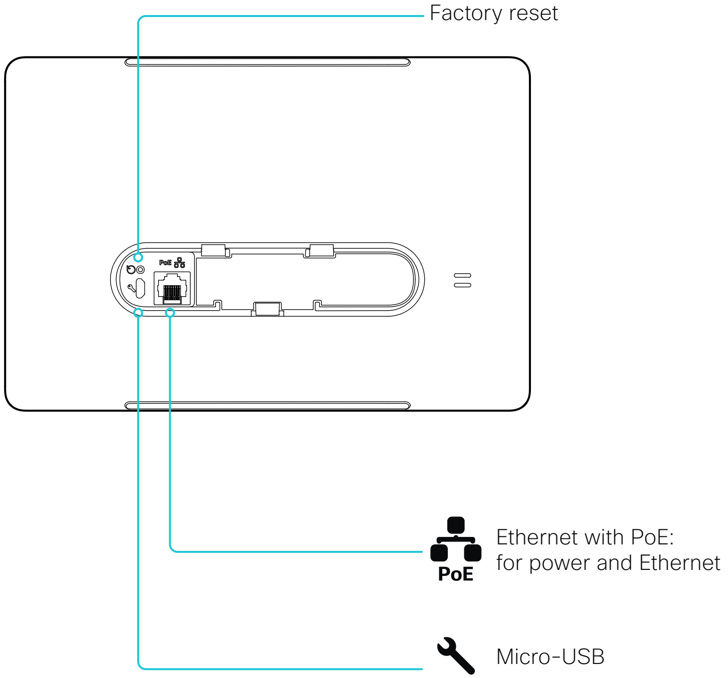
This touch controller was launched early 2021. It has the same functionality as the Touch 10, but also offers environmental sensors for monitoring things like air quality and temperature.



Remove the table stand to access the connector panel. Press firmly and pivot.


Touch screen
Table stand
Status LED

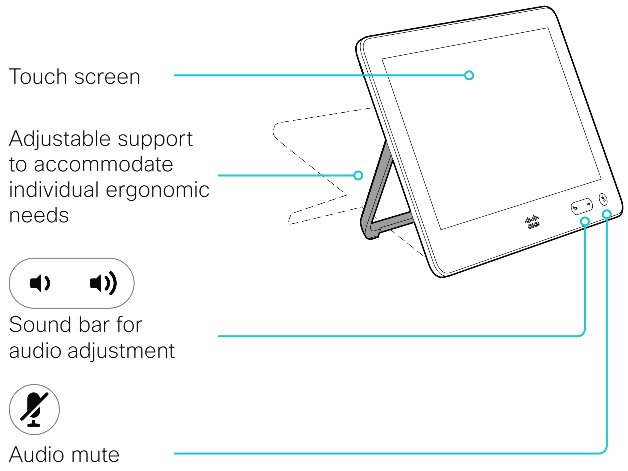
The sound bar and the audio mute is accessible from the user interface.

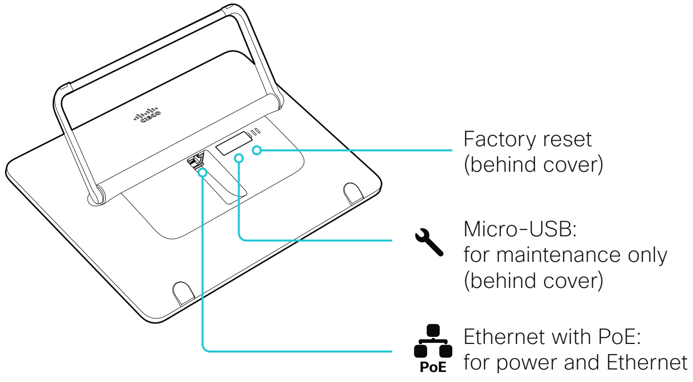

Factory reset
PoE
Ethernet with PoE: for power and Ethernet
Micro-USB

Connect the touch controller (page 8 of 8)

Cisco Touch 10 physical interface

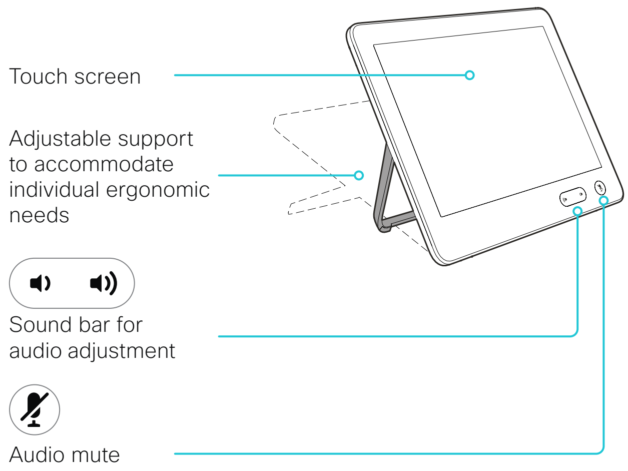
This is the second version of the Touch 10 controller (launched late 2017). It has the same functionality as the first version, but has a slightly different physical interface. The new device is identified by the logo on front, and fewer connectors at the back.

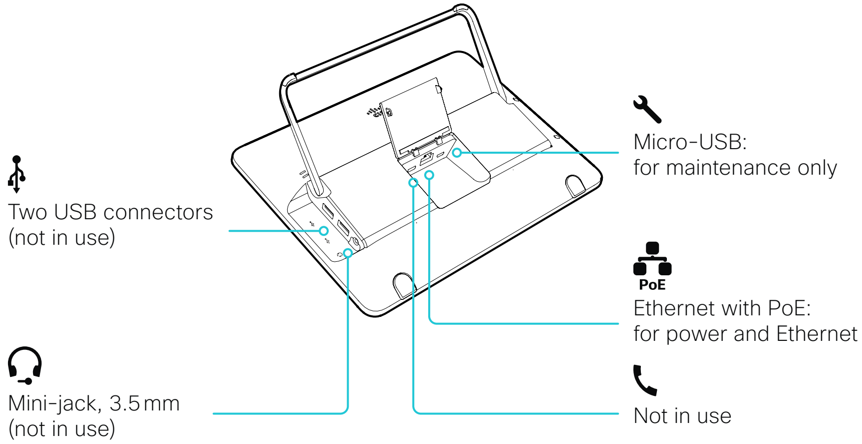

Touch screen
Adjustable support to accommodate individual ergonomic needs
Sound bar for audio adjustment
Audio mute


Factory reset (behind cover)
Micro-USB: for maintenance only (behind cover)
Ethernet with PoE: for power and Ethernet
PoE

Cisco TelePresence Touch 10 physical interface

This is the first version of the Touch 10 controller.


Touch screen
Adjustable support to accommodate individual ergonomic needs
Sound bar for audio adjustment
Audio mute


Micro-USB: for maintenance only
Two USB connectors (not in use)
PoE
Ethernet with PoE: for power and Ethernet
Mini-jack, 3.5 mm (not in use)
Not in use

Chapter 4

Maintenance

Installing new software (page 1 of 2)

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-s53200ce10_x_y_z.k3.cop.sgn" or "cmterm-s53200ce10_x_y_z.k3.cop.sha512"
  (for Boards, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, and Room 70)
- "cmterm-s53300ce10_x_y_z.k3.cop.sgn" or "cmterm-s53300ce10_x_y_z.k3.cop.sha512"
  (for Codec Pro, Desk Pro, Desk Limited Edition, Room 70 G2, Room 70 Panorama, and Room Panorama)
- "cmterm-s53300ce10_z_y_z-l4t.k3.cop.sha512"
  (for Webex Desk)

where "x" is the minor release number, "y" is the patch number and "z" is the build number.

Cloud-managed software upgrade

If your device is linked to Webex Edge for Devices, you can choose to upgrade the software from the Webex cloud service. Then the device is upgraded automatically as soon as a new RoomOS software version is available from the cloud.

Refer to the ▶ Cloud-Managed Software Upgrade for Webex Edge for Devices (https://help.webex.com/naspqfz/) article on Webex Help Center for details.

File formats for software images

About PKG files and COP files

The software images for the video device and the peripherals are in separate PKG files.

Therefore, you must use the COP file when upgrading these devices. The COP file contains the required PKG files for the video device and the peripherals, and a *loads* file that lists the content of the COP file.

Upgrading from CUCM

Use the COP file when upgrading a device. [*]

When upgrading these devices, you must specify the software using the *loads* file. You cannot use only the PKG file of the video device, because then the peripherals won't be upgraded.

Upgrading from TMS or from the web interface of the device

Use the COP file when upgrading a device. Don't use only the PKG file for the video device, since it doesn't contain the software images for the peripherals.

Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (RoomOS 10). It's one set of release notes that covers all products. Go to:

- ▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/products-release-notes-list.html
- ▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-room-kit-series/products-release-notes-list.html
- ▶ https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-board/products-release-notes-list.html

Upgrading to or downgrading from CE9.13 or later

Be aware that upgrading and downgrading can result in a loss of settings in certain circumstances.

When upgrading to or downgrading from CE9.13 or later, any settings not appearing in the version you are installing will be deleted. If you later try to go back to the previous software version, those removed settings will be assigned default values.

---

[*] For CUCM 14 and later, use the files with extension .sha512. For older CUCM versions, use the files with extension .sgn.

Installing new software (page 2 of 2)

Sign in to the web interface, go to *Software*, and select *Software Upgrade*.

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.

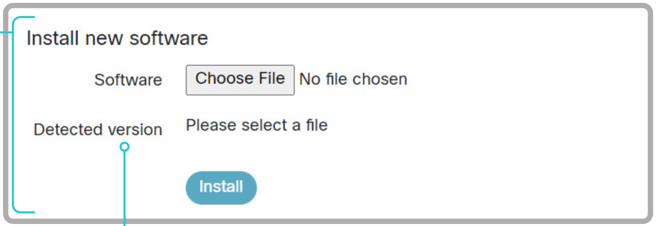
1. Click *Choose File.* and find the .cop.sgn file that contains the new software.

   The software version will be detected and shown.

2. Click *Install* 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.



Install new software

Software: Choose File No file chosen

Detected version: Please select a file

Check new software version

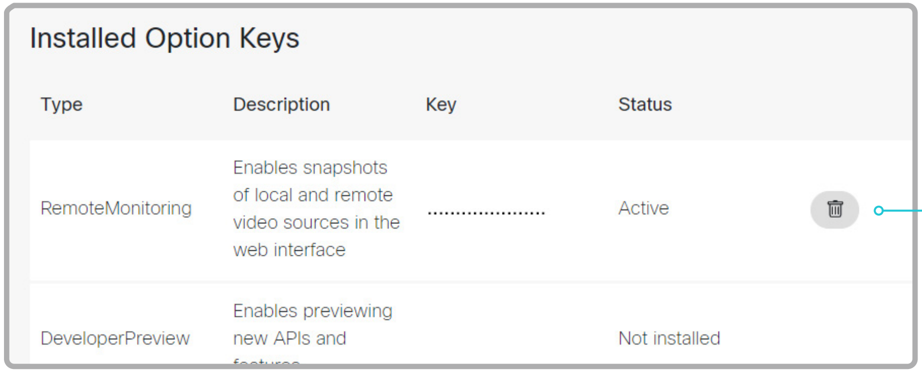
When you have selected a file, the software version is shown here

Add option keys

Sign in to the web interface, go to *Software*, and select *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.

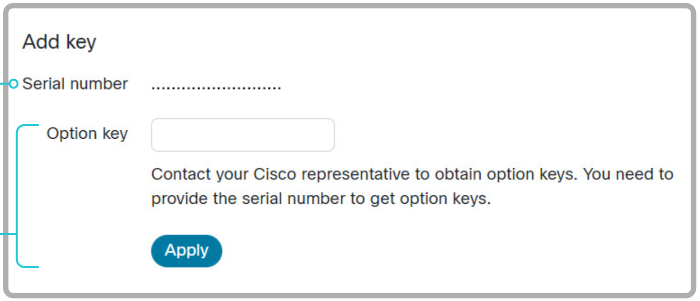


Installed Option Keys

Type	Description	Key	Status
RemoteMonitoring	Enables snapshots of local and remote video sources in the web interface	....	Active
DeveloperPreview	Enables previewing new APIs and		Not installed

Uninstall an option key

Click the delete button to uninstall an option key.



Add key

Serial number ....

Option key

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

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 *Apply* to add the 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 and select *Home*.

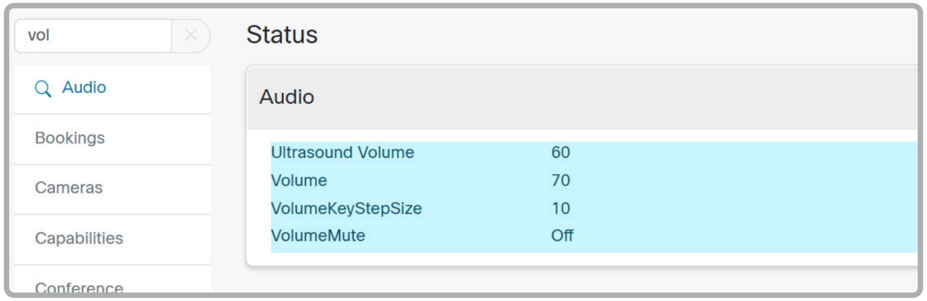
This is the *System Information* page, which shows general information such as IP address, MAC address, serial number, active network interface, software version, issues, registration status, and more.

Detailed device status

Sign in to the web interface, go to *Settings*, and select *Statuses*, 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.



vol

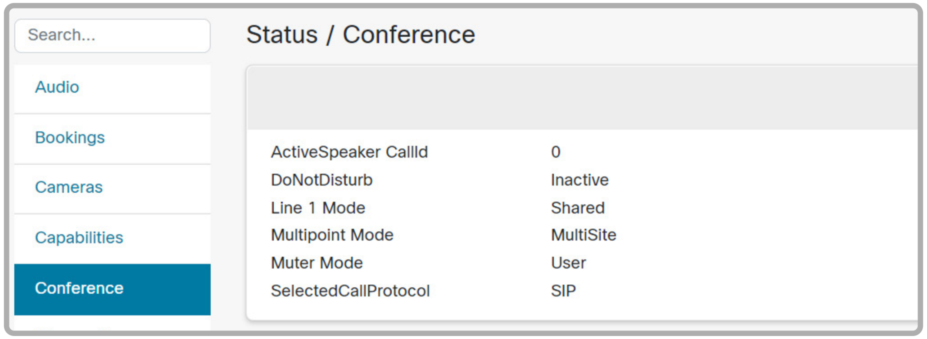
Status

Audio

Ultrasound Volume	60
Volume	70
VolumeKeyStepSize	10
VolumeMute	Off

Select a category and navigate to the correct status

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



Status / Conference

ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Shared
Multipoint Mode	MultiSite
Muter Mode	User
SelectedCallProtocol	SIP

---

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

Run diagnostics

Sign in to the web interface, go to *Issues and Diagnostics*, and select *Issues*.

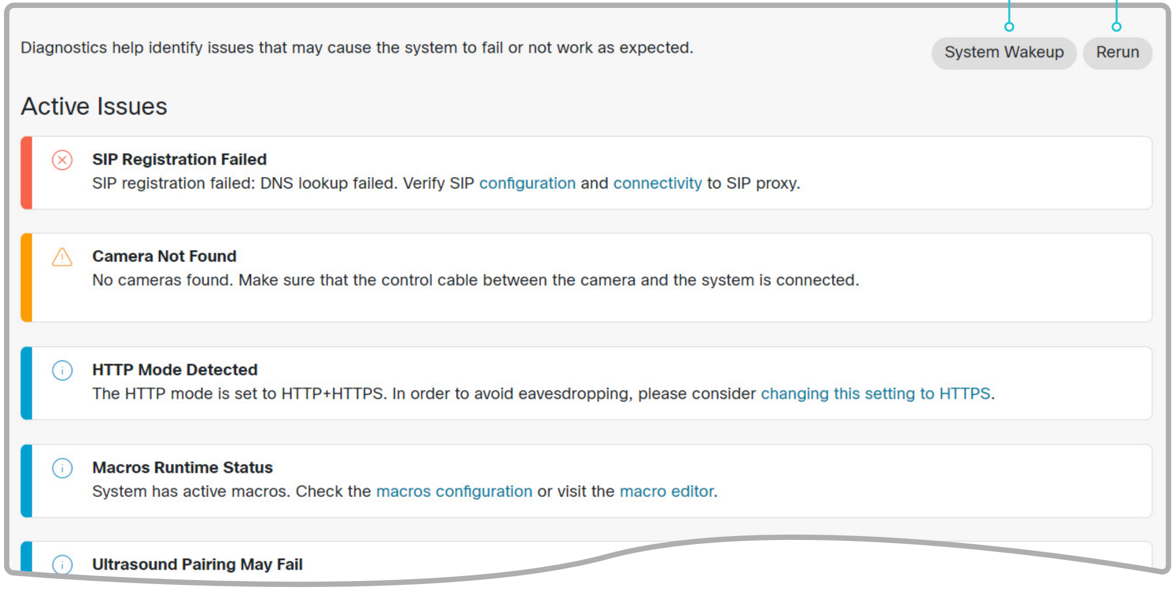
A list of active issues[*] are shown. Errors and critical issues are clearly marked in red color; warnings are yellow.

Run diagnostics

Click *Rerun* to ensure that the list is up to date.

Leave standby mode

Click *System Wakeup* to wake up a device that is in standby mode.



Diagnostics help identify issues that may cause the system to fail or not work as expected.

Active Issues

SIP Registration Failed
SIP registration failed: DNS lookup failed. Verify SIP configuration and connectivity to SIP proxy.

Camera Not Found
No cameras found. Make sure that the control cable between the camera and the system is connected.

HTTP Mode Detected
The HTTP mode is set to HTTP+HTTPS. In order to avoid eavesdropping, please consider changing this setting to HTTPS.

Macros Runtime Status
System has active macros. Check the macros configuration or visit the macro editor.

Ultrasound Pairing May Fail

---

[*] The issues shown in the illustration serve as examples. Your device will show other information.

Download system log files (page 1 of 2)

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

Current logs and historical logs

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. Network traffic may also be captured in this mode.

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.

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

Personal identifiable information *(PII)* in logs

You can choose whether to include PII in the logs or not. In some cases PII is replaced by a *Removed for privacy* note rather than the full entry being removed.

Set up logs from the user interface

You have a few options to set up logs from the device's user interface. Go to *Settings > Issues and diagnostics* and find these toggle buttons:

- *Extended logging:* If toggled on, a full capture of network traffic will be included in the logs. PII information will also be included.
- *PII logging:* If toggled on, PII will be included in the logs, even if Extended logging is not turned on.

Sending logs to the Webex cloud

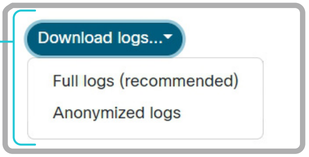
If your device is registered to the Webex cloud service or linked to Webex Edge for Devices, you can also upload the logs to the cloud by tapping *Settings > Issues and diagnostics > Send logs*.

Download system log files (page 2 of 2)

Set up and download logs from the web interface

Sign in to the web interface, go to *Issues and Diagnostics*, and select *System Logs*.

Download all log files


Download logs...
Full logs (recommended)
Anonymized logs

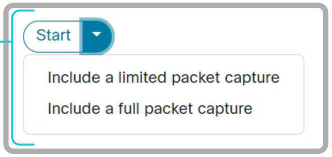
Find the *System Logs* card, and click *Download logs...*.

Choose whether to download *Full logs* or *Anonymized logs*.

Follow the instructions to save the file.

Personal identifiable information (PII) are replaced by a *Removed for privacy* note in the anonymized logs. Attaching anonymized logs to support cases may increase the time needed to resolve your issue.

Start extended logging


Start
Include a limited packet capture
Include a full packet capture

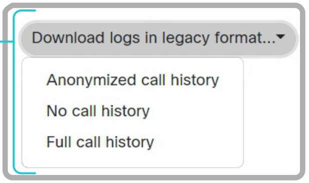
Find the *Extended Logging* card, and click *Start*.

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

Click *Stop* 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.

Download all log files *(legacy format)* Not recommended


Download logs in legacy format...
Anonymized call history
No call history
Full call history

Find the *System Logs* card, and click *Download logs in legacy format...*.

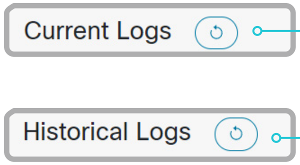
Choose whether to include the full call history (non-anonymous caller/callee), an anonymized call history, or no call history at all, in the log files.

Follow the instructions to save the file.

Open or save a log file

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

Click a *historical log file* and follow the instructions to save the file on your computer.


Current Logs
Historical Logs

Refresh a log file list

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

Log file format

We introduced a new log file format for on-premises registered devices in CE9.15. The new format aligns with the format used for cloud registered devices.

We recommend you to download logs using the new file format, rather than using the legacy format.

Get call logs

Sign in to the web interface, go to *Issues and Diagnostics*, and select *Call Logs*. From the list that appears, select a call to see its details.

The details include information about the remote number, direction of the originating call, protocol, call rate, encryption type, and duration; as well as, information relating to the disconnection of a call.

The **Disconnect cause type** field is used to describe why the call was disconnected. There are many possible values, and these can be changed downstream. Some examples include: OtherLocal, LocalDisconnect, UnknownRemoteSite, LocalBusy, LocalReject, InsufficientSecurity, OtherRemote, RemoteDisconnect, RemoteBusy, RemoteRejected, RemoteNoAnswer, CallForwarded, and NetworkRejected.

The **disconnection cause** field can provide additional information as a suppliment to the **disconnect cause type**.

The **disconnect cause code** is defined by SIP and Q.850.

Occurrence type provides further information relating to whether the call was placed, received, missed, rejected, if the remote end never answered the call, or if the call answered on another device.

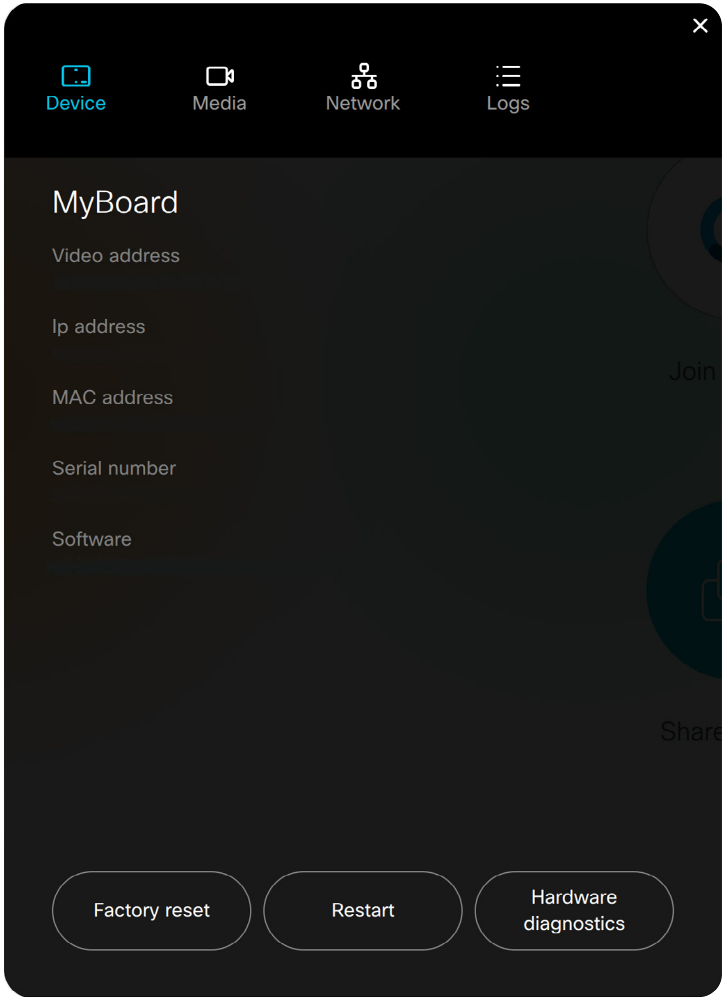
The **Is acknowledged** field shows whether or not a missed call has been acknowledged by a user.

Access the Technical support screen

You can access the *Technical support screen* by holding the screen with one finger and tapping the *Home button* three times.

From the *Technical support screen* you can access:

- Device information
- Media statistics
- Network information and diagnostics
- Hardware diagnostics (microphone levels, touch screen, best overview, and camera)
- Logs
- Restart the board
- Factory reset


Device
Media
Network
Logs
MyBoard
Video address
Ip address
MAC address
Serial number
Software
Join
Share
Factory reset
Restart
Hardware diagnostics

Create a remote support user

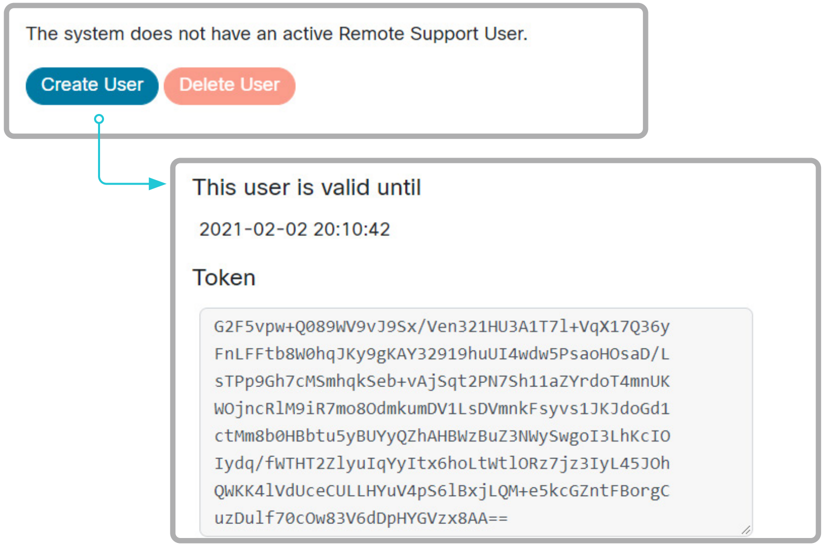
Sign in to the web interface and, go to *Users*.

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

Create remote support user

1. Find the *Remote Support User* card, and click *Create User*.
2. Open a case with Cisco TAC.
3. Copy the text in the *Token* field and send it to Cisco TAC.
4. Cisco TAC will generate a *password*.

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



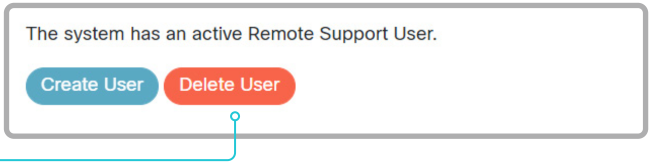
The system does not have an active Remote Support User.

This user is valid until

2021-02-02 20:10:42

Token

```
G2F5vpw+Q089WV9vJ9Sx/Ven321HU3A1T7l+VqX17Q36y
FnLFFtb8W0hqJKy9gKAY32919huUI4wdw5PsaoHOsaD/L
sTPp9Gh7cMSmhqkSeb+vAjSqt2PN7Sh11aZYrdoT4mnUK
WOjncRlM9iR7mo8OdmkumDV1LsDVmnkFsyvs1JKJdoGd1
ctMm8b0HBbtu5yBUYyQZhAHBWzBuZ3NWySwgoI3LhKcIO
Iydq/fWTHT2ZlyuIqYyItx6hoLtWtlORz7jz3IyL45JOh
QWKK4lVdUceCULLHYuV4pS6lBxjLQM+e5kcGZntFBorgC
uzDulf70cOw83V6dDpHYGVzx8AA==
```



The system has an active Remote Support User.

Delete remote support user

Click *Delete User*.

About the remote support user

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

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

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

Backup and restore configurations and custom elements

Sign in to the web interface and go to *Backup and Recovery*.

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. Select *Backup*.
2. Select the elements you want to include in the backup file.
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* to store the elements in a zip-file on your computer.

Restore a backup file

1. Select *Restore*.
2. Click *Choose File* and find the backup file you want to restore.

   All settings and elements in the backup file will be applied.
3. Click *Upload* 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
    - *Cutomization 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.

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, go to *Backup and Recovery*, and select *Restore*.
2. Click *Choose File* and find the file you want to calculate the checksum for.

    Then you can see the SHA512 checksum at the bottom of the page.

CUCM documentation

▶ https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

---

[*] 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

TMS provisioning of custom elements

A backup file, as described in the ▶ Backup and restore configurations and custom elements chapter, can be used as a *customization template* for multiple devices.

The backup file must be hosted on a custom web server that can be reached by the devices on HTTP or HTTPS.

When a device get information from TMS (TelePresence Management Suite) about the name and location of the backup file, the device will contact the server, download the file, and restore the custom elements.

Create and apply a configuration template

1. Create a configurations template.
2. Add a custom command containing the following XML string in the configuration template:

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

   where

   `web-server-address`: The URI to the backup file (for example, http://host/backup.zip).

   `checksum`: The SHA512 checksum of the backup file.

   `origin`: **Provisioning** [*]

3. Select the devices you want to push the configuration template to, and click *Set on systems*.

Read the ▶ Cisco TMS administrator guide for details how to create TMS configurations templates and make custom commands.

SHA512 checksum

Tip! You can find the SHA512 checksum of a file by restoring it to a device using its web interface.

1. Sign in to the web interface, go to *Backup and Recovery*, and select *Restore*.
2. Click *Choose File* and find the file you want to calculate the checksum for.

   Then you can see the SHA512 checksum at the bottom of the page.

---

[*] If not setting this parameter to **Provisioning**, also configurations that are part of the backup file will be pushed to the device. If the backup file contains configurations that are specific to one device, for example static IP addresses, device name, and contact information, you may and up with devices that you cannot reach.

Revert to the previously used software image

Sign in to the web interface, go to *Backup and Recovery*, and select *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

1. Go to *Issues and Diagnostics* and select *System Logs*.
2. Click *Download logs* and follow the instructions to save the log files on your computer.

Back up configurations and custom elements

1. Go to *Backup and Recovery* and select *Backup*.
2. Click *Download* and follow the instructions to save the backup bundle on your computer.

Revert to the previously used software image

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

1. Select *System Recovery*.
2. Find the *Software Recovery Swap* card and click *Swap software*.
3. Click *Confirm* to continue, or *Cancel* if you have changed your mind.

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

About the previously used software image

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

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

Factory reset the video conferencing device (page 1 of 5)

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 *(not available for Boards)*, 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 5)

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, go to *Backup and Recovery*, and select *System Recovery*.

1. Find the *Factory Reset* card, and read the provided information carefully.
2. Click *Reset to Factory Defaults*.
3. Click *Factory Reset* 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 Technical support screen

Applies to: Boards

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

1. To access the *Technical support screen*, hold down one finger on the board's screen, and press the home button three times.
2. Select *Factory reset*.
3. Select *Reset* to confirm your choice, or *Cancel* if you have changed your mind.
4. Wait while the device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

   When the device has been successfully reset to factory settings, the *Setup assistant* starts with the *Welcome* screen.

Factory reset from the user interface

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

1. Select the device name or address at the top of the user interface.
2. Select *Settings*.
3. Select *Factory reset*.
4. Select *Reset* to confirm your choice, or *Back* if you have changed your mind.
5. Wait while the device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

   When the device has been successfully reset to factory settings, the *Setup assistant* starts with the *Welcome* screen.

Back up log files

1. Go to *Issues and Diagnostics* and select *System Logs*.
2. Click *Download logs* and follow the instructions to save the log files on your computer.

Back up configurations and custom elements

1. Go to *Backup and Recovery* and select *Backup*.
2. Click *Download* and follow the instructions to save the backup bundle on your computer.

Factory reset the video conferencing device (page 3 of 5)

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.

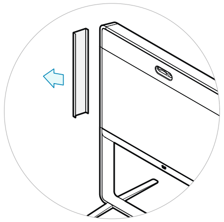
1. Use a paper clip (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.
2. Wait while the device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

   When the device has been successfully reset to factory settings, the Setup assistant starts with the *Welcome* screen.

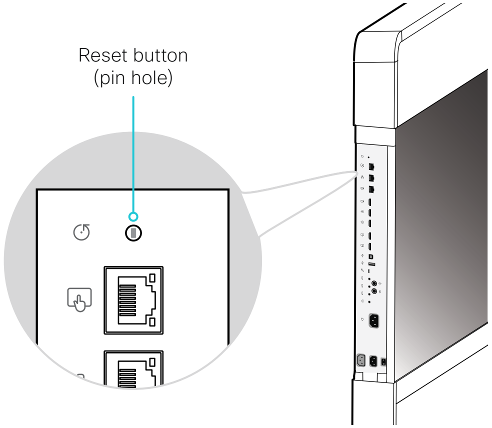
ⓘ See the illustrations to find the recessed reset button for the different products.

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

Room 55 Dual and Room 70

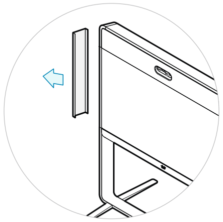


Remove the left side cover of the device to get access to the codec connector panel. The cover snaps to magnets.

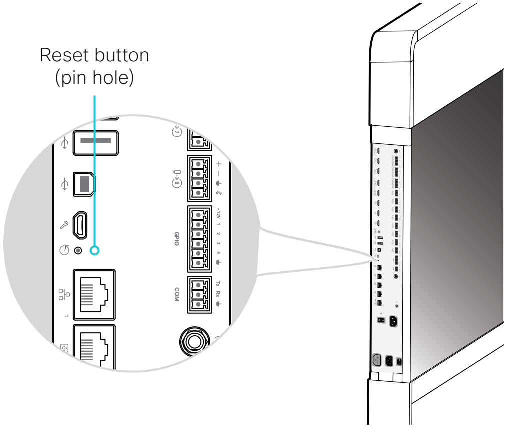


Reset button
(pin hole)

Room 70 G2 and Room 70 Panorama



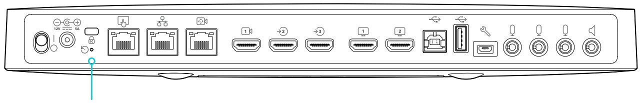
Remove the left side cover of the device to get access to the codec connector panel. The cover snaps to magnets.



Reset button
(pin hole)

Factory reset the video conferencing device (page 4 of 5)

Codec Plus

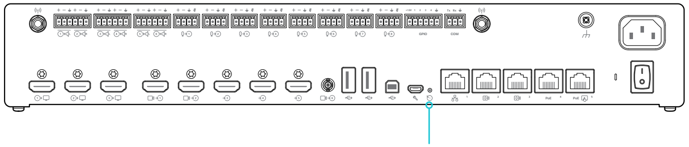


Reset button
(pin hole)

Codec Pro and Room Panorama

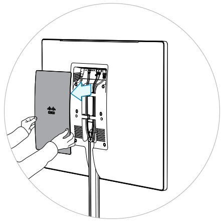
For Room Panorama:

- Use the handle at the bottom of the deco grille, and pull down the left monitor to get access to the codec.



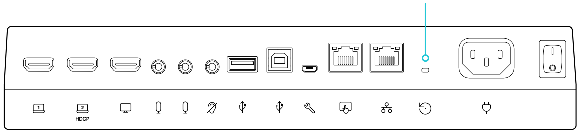
Reset button
(pin hole)

Room 55



Remove the rear cover to get access to the connector panel.

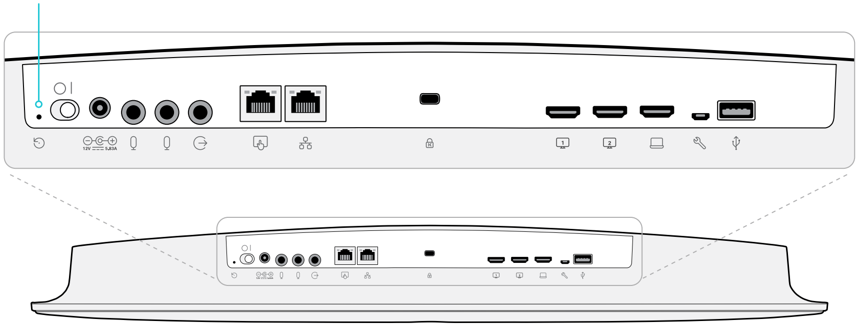
Reset button
(pin hole)



Room Kit

Tilt the unit forward to get access to the connector panel.

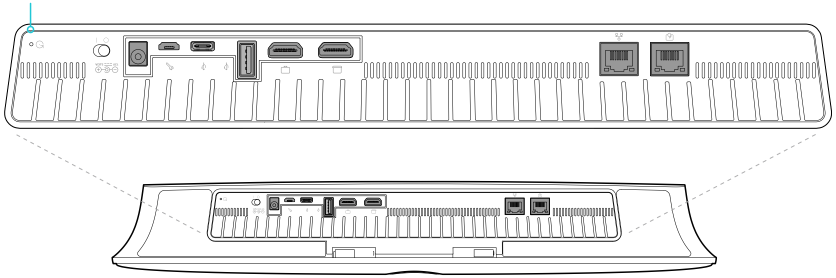
Reset button
(pin hole)



Room Kit Mini

Tilt the unit forward to get access to the connector panel.

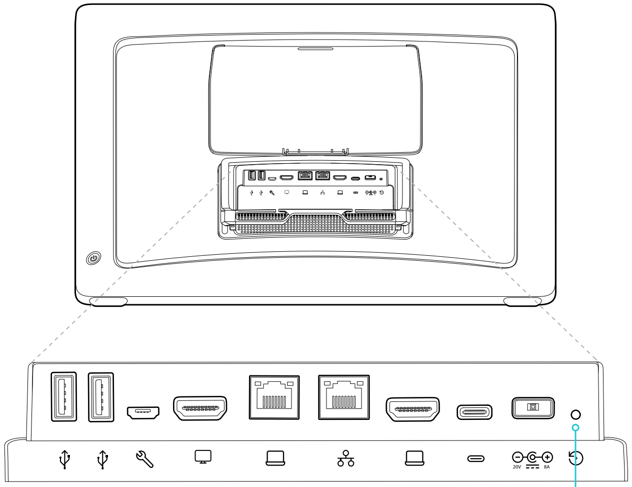
Reset button
(pin hole)



Factory reset the video conferencing device (page 5 of 5)

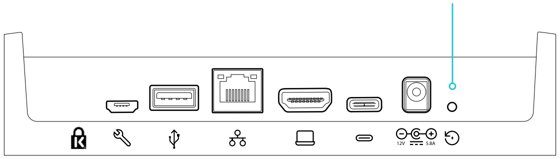
Webex Desk, Desk Pro, and Desk Limited Edition

Flip the cover on the back of the device to get access to the connector panel.



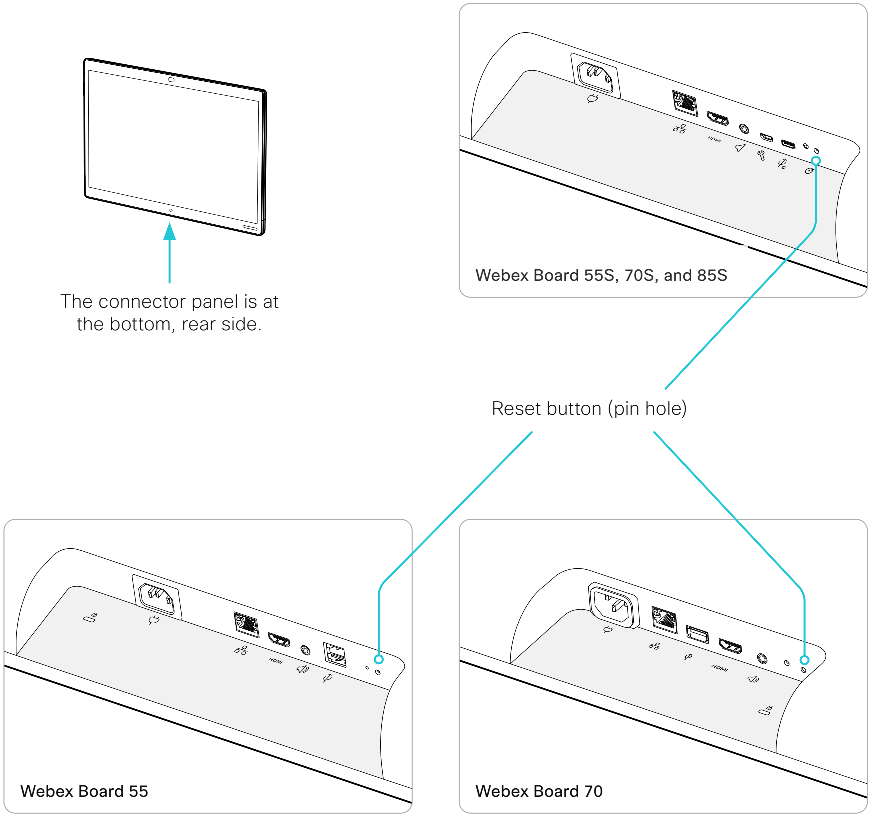
Desk Pro and Desk Limited Edition

Reset button (pin hole)



Webex Desk

Webex Boards


The connector panel is at the bottom, rear side.
Webex Board 55S, 70S, and 85S
Reset button (pin hole)
Webex Board 55
Webex Board 70

Factory reset Cisco Webex Room Navigator

In an error situation it may be required to factory reset the touch controller to recover connectivity.

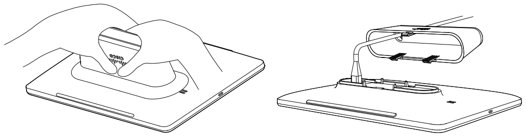
When factory resetting the touch controller the pairing information is lost, and the touch controller itself (not the video conferencing device) is reverted to factory defaults.

It is not possible to undo a factory reset.

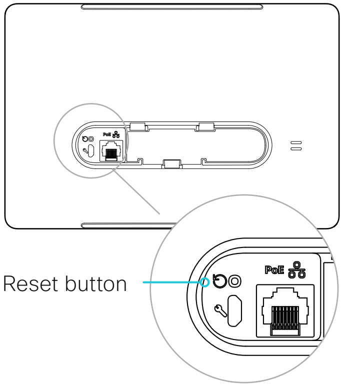
1. Remove the foot to find the reset button (pin hole) on the connector panel.
2. Use a paper clip (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.
3. Wait while the Room Navigator reverts to the default factory settings. When finished, the Room Navigator restarts automatically. This may take a few minutes.

   If the Room Navigator is directly connected to the video conferencing device, it receives a new configuration automatically from the device.

   If the Room Navigator 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.



Press firmly and pivot to remove the table stand.



About pairing and how to connect the Room Navigator to the video conferencing device

There are two ways to connect a Room Navigator to the video conferencing device:

- Connect the Room Navigator directly to the video conferencing device (local pairing) *(not available for Boards)*
- Pair the Room Navigator to the video conferencing device via LAN (remote pairing)

Read about pairing and how to connect the Room Navigator to the video conferencing device in the ▶ Connect the touch controller chapter.

Factory reset Touch 10

In an error situation it may be required to factory reset the touch controller to recover connectivity.

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

⚠ It is not possible to undo a factory reset.

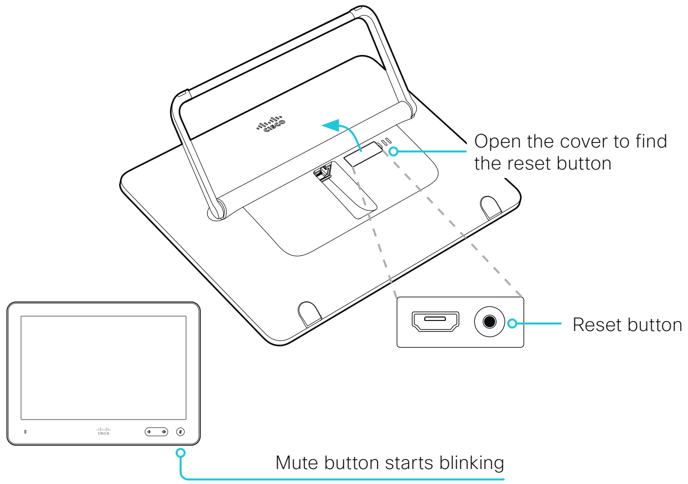
Cisco Touch 10

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.


Open the cover to find the reset button
Reset button
Mute button starts blinking

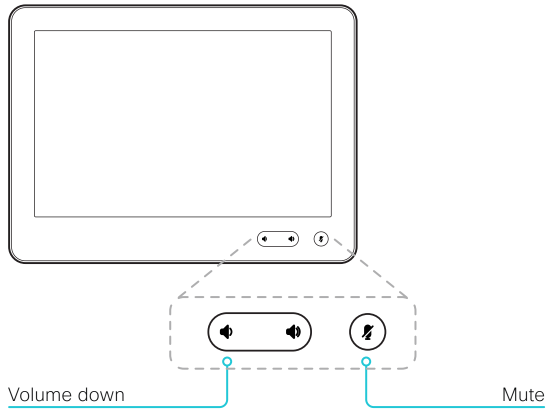
Cisco TelePresence Touch 10

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.



Two Touch 10 versions

There are two versions of the Touch 10. They look almost the same and has the same functionality.

- *Cisco TelePresence Touch 10*: This is the first version. It has no logo on front.
- *Cisco Touch 10*: This version was launched late 2017. It is identified by the logo on front, and fewer connectors at the back.

About pairing and how to connect the Touch 10 to the video conferencing device

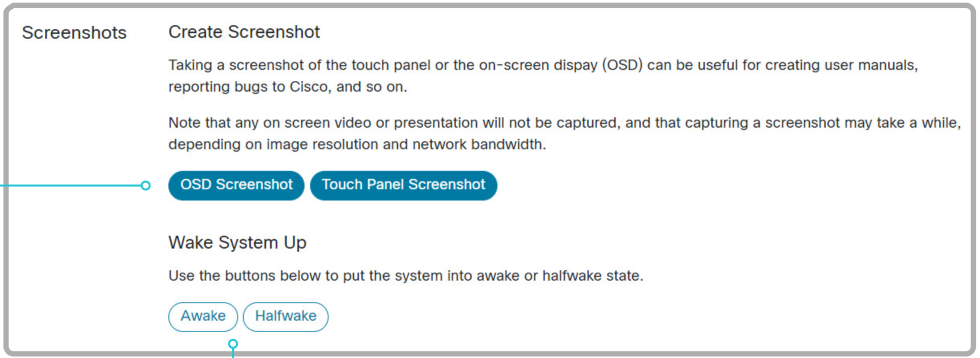
There are two ways to connect a Touch 10 to the video conferencing device:

- Connect the Touch 10 directly to the video conferencing device (local pairing) *(not available for Boards)*
- Pair the Touch 10 to the video conferencing device via LAN (remote pairing)

Read about pairing and how to connect the Touch 10 to the video conferencing device in the ▶ Connect the touch controller chapter.

Capture user interface screenshots

Sign in to the web interface, go to *Issues and Diagnostics*, and select *User Interface Screenshots*.



Screenshots

Create Screenshot

Taking a screenshot of the touch panel or the on-screen dispay (OSD) can be useful for creating user manuals, reporting bugs to Cisco, and so on.

Note that any on screen video or presentation will not be captured, and that capturing a screenshot may take a while, depending on image resolution and network bandwidth.

Wake System Up

Use the buttons below to put the system into awake or halfwake state.

Capture a screenshot

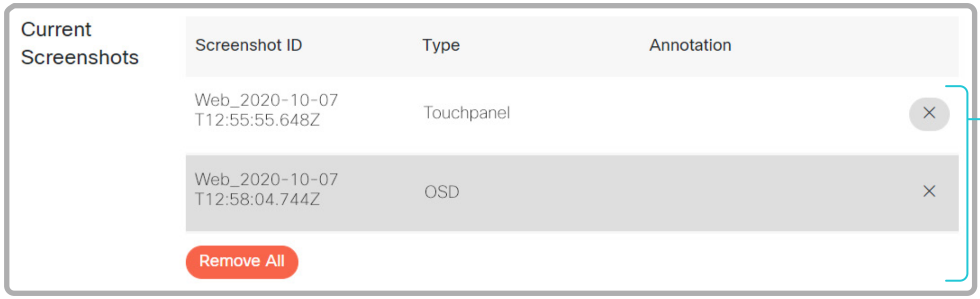
Click *Touch Panel Screenshot* to capture a screenshot of the touch controller, or click *OSD screenshot* to capture a screenshot of the main screen (on screen display).

The screenshot appears below the *Current Screenshots* card. It may take up to 30 seconds before the screenshot is ready.

All captured screenshots are listed in the *Current Screenshots* card. Click the screenshot ID to display the image.

Wake up the device

Use these buttons to wake up the device from standby.



Current Screenshots

Screenshot ID	Type	Annotation
Web_2020-10-07 T12:55:55.648Z	Touchpanel	
Web_2020-10-07 T12:58:04.744Z	OSD	

Delete screenshots

If you want to delete all screenshots, click *Remove All*.

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

About user interface screenshots

You can capture screenshots both of a touch controller that is connected to a video conferencing device, and of the main screen with menus, indicators and messages (also know as *on-screen display*).

For Webex Desk, Desk Pro and Desk Limited Edition:

- Only OSD screenshots are available.

Chapter 5

Device settings

Overview of the device settings

In the following pages you find a complete list of the device settings. They can be configured from the web interface.

Open a web browser, enter the IP address of the device, and sign in. Go to *Settings*, and select *Configurations*.

ⓘ

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.. 149
Audio DefaultVolume.. 149
Audio Input ARC [n] Mode.. 149
Audio Input HDMI [n] Level.. 150
Audio Input HDMI [n] Mode.. 150
Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo.. 150
Audio Input MicrophoneMode.. 153
Audio Input Microphone [n] Channel.. 150
Audio Input Microphone [n] EchoControl Dereverberation.. 151
Audio Input Microphone [n] EchoControl Mode.. 151
Audio Input Microphone [n] EchoControl NoiseReduction.. 151
Audio Input Microphone [n] Equalizer ID.. 151
Audio Input Microphone [n] Equalizer Mode.. 152
Audio Input Microphone [n] Level.. 152
Audio Input Microphone [n] Mode.. 152
Audio Input Microphone [n] MuteOverride.. 152
Audio Input Microphone [n] PhantomPower.. 153
Audio Input Microphone [n] VideoAssociation MuteOnInactiveVideo.. 153
Audio Input Microphone [n] VideoAssociation VideoInputSource.. 153
Audio Input USBC [n] Level.. 154
Audio Input USBC [n] Mode.. 154
Audio Input USBC [n] VideoAssociation MuteOnInactiveVideo.. 154
Audio Input USBInterface [n] EchoControl Mode.. 154
Audio Input USBInterface [n] Level.. 155
Audio Input USBInterface [n] Mode.. 155
Audio Input USBMicrophone [n] Level.. 155
Audio Input WebView[n] Mode.. 155
Audio Microphones AGC.. 156
Audio Microphones Mute Enabled.. 156
Audio Microphones NoiseRemoval Mode.. 156
Audio Microphones PhantomPower.. 156
Audio Output ARC [n] Delay DelayMs.. 157
Audio Output ARC [n] Delay Mode.. 157
Audio Output ARC [n] Mode.. 157
Audio Output ConnectorSetup.. 158
Audio Output Ethernet [n] Mode.. 158
Audio Output HDMI [n] Delay DelayMs.. 159
Audio Output HDMI [n] Delay Mode.. 159
Audio Output HDMI [n] Level.. 159
Audio Output HDMI [n] Mode.. 159
Audio Output InternalSpeaker Mode.. 160
Audio Output Line [n] Channel.. 160
Audio Output Line [n] Delay DelayMs.. 160

Audio Output Line [n] Delay Mode 160
Audio Output Line [n] Equalizer ID 161
Audio Output Line [n] Equalizer Mode 161
Audio Output Line [n] Level 161
Audio Output Line [n] Mode 161
Audio Output Line [n] OutputType 162
Audio Output USBInterface [n] Mode 162
Audio SoundsAndAlerts RingTone 162
Audio SoundsAndAlerts RingVolume 162
Audio Ultrasound MaxVolume 163
Audio Ultrasound Mode 163
Audio USB Mode 163

Bluetooth settings 164
Bluetooth Allowed 164
Bluetooth Enabled 164

Bookings settings 164
Bookings ProtocolPriority 164

BYOD settings 165
BYOD HidForwarding Enabled 165
BYOD TouchForwarding Enabled 165

CallHistory settings 165
CallHistory Mode 165

Cameras settings 166
Cameras Background Enabled 166
Cameras Background UserImagesAllowed 166
Cameras Camera Brightness DefaultLevel 168
Cameras Camera Brightness Mode 167
Cameras Camera ExposureCompensation Level 168
Cameras Camera Framerate 171
Cameras Camera [n] AssignedSerialNumber 166
Cameras Camera [n] Backlight DefaultMode 167
Cameras Camera [n] Brightness Algorithm 167
Cameras Camera [n] Brightness DefaultLevel 168
Cameras Camera [n] Brightness Mode 167
Cameras Camera [n] Flip 168
Cameras Camera [n] Focus Mode 169
Cameras Camera [n] Gamma Level 170
Cameras Camera [n] Gamma Mode 169
Cameras Camera [n] Mirror 170
Cameras Camera [n] MotorMoveDetection 171
Cameras Camera [n] Whitebalance Level 171
Cameras Camera [n] Whitebalance Mode 171
Cameras PowerLine Frequency 172
Cameras PresenterTrack CameraPosition Pan 172
Cameras PresenterTrack CameraPosition Tilt 172
Cameras PresenterTrack CameraPosition Zoom 172
Cameras PresenterTrack Connector 172
Cameras PresenterTrack Enabled 173
Cameras PresenterTrack PresenterDetectedStatus 173
Cameras PresenterTrack TriggerZone 173
Cameras SpeakerTrack Closeup 174
Cameras SpeakerTrack ConnectorDetection CameraLeft 175
Cameras SpeakerTrack ConnectorDetection CameraRight 175
Cameras SpeakerTrack ConnectorDetection Mode 175
Cameras SpeakerTrack Mode 174
Cameras SpeakerTrack TrackingMode 174
Cameras SpeakerTrack Whiteboard Mode 175

Conference settings 176
Conference ActiveControl Mode 176
Conference AutoAnswer Delay 176
Conference AutoAnswer Mode 176
Conference AutoAnswer Mute 176
Conference CallProtocolIPStack 176
Conference DefaultCall Protocol 177
Conference DefaultCall Rate 177
Conference DoNotDisturb DefaultTimeout 177
Conference Encryption Mode 177
Conference EndToEndEncryption Identity PreferredDomain 178
Conference EndToEndEncryption Mode 178
Conference FarEndControl Mode 178
Conference FarEndControl SignalCapability 178
Conference FarEndMessage Mode 178
Conference IncomingMultisiteCall Mode 181
Conference JoinLeaveNotifications 179
Conference MaxReceiveCallRate 179
Conference MaxTotalReceiveCallRate 179
Conference MaxTotalTransmitCallRate 180
Conference MaxTransmitCallRate 179
Conference MicUnmuteOnDisconnect Mode 180
Conference Multipoint Mode 180
Conference MultiStream Mode 181
Conference Presentation OnPlacedOnHold 181
Conference Presentation RelayQuality 181

FacilityService settings 182
FacilityService Service [n] CallType 182
FacilityService Service [n] Name 182
FacilityService Service [n] Number 182
FacilityService Service [n] Type 182

GPIO settings 183
GPIO Pin [n] Mode 183

H323 settings 183
H323 Authentication LoginName 183
H323 Authentication Mode 183
H323 Authentication Password 184
H323 CallSetup Mode 184
H323 Encryption AES256Support 184
H323 Encryption KeySize 184
H323 Gatekeeper Address 184
H323 H323Alias E164 185
H323 H323Alias ID 185
H323 NAT Address 186
H323 NAT Mode 185
H323 PortAllocation 186

HttpClient settings 186
HttpClient AllowHTTP 186
HttpClient AllowInsecureHTTPS 187
HttpClient Mode 186
HttpClient UseHttpProxy 187

HttpFeedback settings 187
HttpFeedback TlsVerify 187
HttpFeedback UseHttpProxy 188

Logging settings 188
Logging CloudUpload Mode 188
Logging Debug Wifi 188
Logging External Mode 189
Logging External Protocol 189
Logging External Server Address 189
Logging External Server Port 189
Logging External TlsVerify 189
Logging Internal Mode 190
Logging Mode 190

Macros settings 190
Macros AutoStart 190
Macros Mode 190
Macros UnresponsiveTimeout 191
Macros XAPI Transport 191

Network settings 191
Network [n] DNS DNSSEC Mode 191
Network [n] DNS Domain Name 191
Network [n] DNS Server [m] Address 192
Network [n] IEEE8021X AnonymousIdentity 193
Network [n] IEEE8021X Eap Md5 193
Network [n] IEEE8021X Eap Peap 194
Network [n] IEEE8021X Eap Tls 194
Network [n] IEEE8021X Eap Ttls 194
Network [n] IEEE8021X Identity 193
Network [n] IEEE8021X Mode 192
Network [n] IEEE8021X Password 193
Network [n] IEEE8021X TlsVerify 192
Network [n] IEEE8021X UseClientCertificate 192
Network [n] IPStack 194
Network [n] IPv4 Address 195
Network [n] IPv4 Assignment 195
Network [n] IPv4 Gateway 195
Network [n] IPv4 InterfaceIdentifier 195
Network [n] IPv4 SubnetMask 196
Network [n] IPv6 Address 197
Network [n] IPv6 Assignment 196
Network [n] IPv6 DHCPOptions 197
Network [n] IPv6 Gateway 197
Network [n] IPv6 InterfaceIdentifier 197
Network [n] MTU 198
Network [n] QoS Diffserv Audio 198
Network [n] QoS Diffserv Data 199
Network [n] QoS Diffserv ICMPv6 199
Network [n] QoS Diffserv NTP 199
Network [n] QoS Diffserv Signalling 199
Network [n] QoS Diffserv Video 198
Network [n] QoS Mode 198
Network [n] RemoteAccess Allow 200
Network [n] Speed 200

Network [n] TrafficControl Mode 200
Network [n] VLAN Voice Mode 200
Network [n] VLAN Voice VlanId 201

NetworkServices settings 201
NetworkServices CDP Mode 201
NetworkServices H323 Mode 201
NetworkServices HTTP Mode 202
NetworkServices HTTP Proxy LoginName 202
NetworkServices HTTP Proxy Mode 202
NetworkServices HTTP Proxy PACUrl 202
NetworkServices HTTP Proxy Password 203
NetworkServices HTTP Proxy Url 203
NetworkServices HTTPS OCSP Mode 203
NetworkServices HTTPS OCSP URL 203
NetworkServices HTTPS Server MinimumTLSVersion 203
NetworkServices HTTPS StrictTransportSecurity 203
NetworkServices HTTPS VerifyClientCertificate 204
NetworkServices NTP Mode 204
NetworkServices NTP Server [n] Address 204
NetworkServices NTP Server [n] Key 204
NetworkServices NTP Server [n] KeyAlgorithn 205
NetworkServices NTP Server [n] KeyId 205
NetworkServices SIP Mode 205
NetworkServices SMTP From 206
NetworkServices SMTP Mode 205
NetworkServices SMTP Password 206
NetworkServices SMTP Port 206
NetworkServices SMTP Security 207
NetworkServices SMTP Server 206
NetworkServices SMTP Username 206
NetworkServices SNMP CommunityName 207
NetworkServices SNMP Mode 207
NetworkServices SNMP SystemContact 207
NetworkServices SNMP SystemLocation 208
NetworkServices SSH AllowPublicKey 208
NetworkServices SSH HostKeyAlgorithm 208
NetworkServices SSH Mode 208
NetworkServices UPnP Mode 209
NetworkServices UPnP Timeout 209
NetworkServices Websocket 209
NetworkServices WelcomeText 209
NetworkServices Wifi Allowed 210
NetworkServices WifiCloud A_MPDU 210
NetworkServices Wifi Enabled 210
NetworkServices XMLAPI Mode 210

Peripherals settings 211
Peripherals InputDevice Mode 211
Peripherals Pairing CiscoTouchPanels EmcResilience 211
Peripherals Pairing CiscoTouchPanels RemotePairing 211
Peripherals Profile Cameras 211
Peripherals Profile Cameras 212
Peripherals Profile ControlSystems 212
Peripherals Profile NetworkSwitches 212
Peripherals Profile TouchPanels 212

Phonebook settings 213
Phonebook Server [n] ID 213
Phonebook Server [n] Pagination 213
Phonebook Server [n] TlsVerify 213
Phonebook Server [n] Type 214
Phonebook Server [n] URL 214

Provisioning settings 214
Provisioning Connectivity 214
Provisioning CUCM CallManagementRecords CallDiagnostics 214
Provisioning ExternalManager Address 215
Provisioning ExternalManager AlternateAddress 215
Provisioning ExternalManager Domain 215
Provisioning ExternalManager Path 215
Provisioning ExternalManager Protocol 215
Provisioning LoginName 216
Provisioning Mode 216
Provisioning Password 216
Provisioning TlsVerify 216
Provisioning WebexEdge 217

Proximity settings 217
Proximity AlternatePort Enabled 217
Proximity Mode 218
Proximity Services CallControl 218
Proximity Services ContentShare FromClients 218
Proximity Services ContentShare ToClients 218

RoomAnalytics settings 219
RoomAnalytics AmbientNoiseEstimation Interval 219
RoomAnalytics AmbientNoiseEstimation Mode 219

RoomAnalytics PeopleCountOutOfCall 219
RoomAnalytics PeoplePresenceDetector....219
RoomAnalytics ReverberationTime Interval 220
RoomAnalytics ReverberationTime Mode.... 220

RoomCleanup settings.... 220
RoomCleanup AutoRun ContentType WebData.... 220
RoomCleanup AutoRun ContentType Whiteboards 220
RoomCleanup AutoRun HourOfDay 220

RoomReset settings.... 221
RoomReset Control....221

RoomScheduler settings.... 221
RoomScheduler BookingTimeout 221
RoomScheduler Enabled 221

RTP settings.... 222
RTP Ports Range Start 222
RTP Ports Range Stop 222
RTP Video Ports Range Start.... 222
RTP Video Ports Range Stop 222

Security settings 223
Security Audit Logging Mode 223
Security Audit OnError Action 223
Security Audit Server Address 223
Security Audit Server Port 224
Security Audit Server PortAssignment....224
Security Fips Mode 224
Security Session FailedLoginsLockoutTime 224
Security Session InactivityTimeout 225
Security Session MaxFailedLogins 225
Security Session MaxSessionsPerUser....225
Security Session MaxTotalSessions 225
Security Session ShowLastLogon 225

SerialPort settings 226
SerialPort BaudRate.... 226
SerialPort LoginRequired 226
SerialPort Mode 226

SIP settings.... 227
SIP ANAT....227
SIP Authentication Password....227
SIP Authentication UserName 227
SIP DefaultTransport 227
SIP DisplayName....227
SIP Ice DefaultCandidate 228
SIP Ice Mode.... 228
SIP Line 228
SIP ListenPort 228
SIP Mailbox 229
SIP MinimumTLSVersion 229
SIP PreferredIPSignaling.... 229
SIP Proxy [n] Address.... 229
SIP TlsVerify 229
SIP Turn Password 230
SIP Turn Server 230
SIP Turn UserName.... 230
SIP Type 230
SIP URI 230

Standby settings 231
Standby BootAction 231
Standby Control 231
Standby Delay....231
Standby Halfwake Mode 232
Standby Level Networked Delay....231
Standby Level Networked Mode 232
Standby Signage Audio 232
Standby Signage InteractionMode.... 232
Standby Signage Mode 233
Standby Signage RefreshInterval.... 233
Standby Signage Url 233
Standby StandbyAction 233
Standby WakeupAction.... 234
Standby WakeupOnMotionDetection.... 234

SystemUnit settings 234
SystemUnit CrashReporting Advanced 234
SystemUnit CrashReporting Mode 235
SystemUnit CrashReporting Url.... 235
SystemUnit CustomDeviceId 235
SystemUnit Name 234

Time settings 235
Time DateFormat 235
Time TimeFormat.... 235
Time Zone.... 236

UserInteraction settings.......237
UserInteraction RaiseHand CMS.......237

UserInterface settings.......238
UserInterface Accessibility IncomingCallNotification.......238
UserInterface Assistant Mode.......238
UserInterface Assistant ProactiveMeetingJoin.......238
UserInterface Bookings Visibility Title.......238
UserInterface Branding AwakeBranding Colors.......239
UserInterface ContactInfo Type.......239
UserInterface CustomMessage.......239
UserInterface Diagnostics Notifications.......239
UserInterface Features Call End.......240
UserInterface Features Call JoinGoogleMeet.......240
UserInterface Features Call JoinWebex.......240
UserInterface Features Call Keypad.......240
UserInterface Features Call MidCallControls.......241
UserInterface Features Call MusicMode.......241
UserInterface Features Call Start.......241
UserInterface Features Call VideoMute.......241
UserInterface Features HideAll.......242
UserInterface Features Share Start.......242
UserInterface Features Whiteboard Start.......242
UserInterface KeyTones Mode.......239
UserInterface Language.......242
UserInterface LedControl Mode.......243
UserInterface NameAndSiteLabels Mode.......243
UserInterface OSD EncryptionIndicator.......243
UserInterface OSD HalfwakeMessage.......243
UserInterface OSD Mode.......244
UserInterface OSD Output.......244
UserInterface Phonebook Mode.......245
UserInterface Proximity Notifications.......245
UserInterface Security Mode.......245
UserInterface SettingsMenu Mode.......245
UserInterface SettingsMenu Visibility.......246
UserInterface SoundEffects Mode.......246
UserInterface Theme Name.......246
UserInterface UsbPromotion.......247
UserInterface Wallpaper.......246
UserInterface WebcamOnlyMode.......247
UserInterface Whiteboard ActivityIndicators.......247
UserInterface Whiteboard DefaultTheme.......247

UserManagement settings.......248
UserManagement LDAP Admin Filter.......248
UserManagement LDAP Admin Group.......248
UserManagement LDAP Attribute.......248
UserManagement LDAP BaseDN.......248
UserManagement LDAP Encryption.......248
UserManagement LDAP MinimumTLSVersion.......249
UserManagement LDAP Mode.......249
UserManagement LDAP Server Address.......249
UserManagement LDAP Server Port.......250
UserManagement LDAP VerifyServerCertificate.......250
UserManagement PasswordPolicy Complexity MinimumDigits.......250
UserManagement PasswordPolicy Complexity MinimumLength.......250
UserManagement PasswordPolicy Complexity MinimumLowercase.......251
UserManagement PasswordPolicy Complexity MinimumSpecial.......251
UserManagement PasswordPolicy Complexity MinimumUppercase.......251
UserManagement PasswordPolicy MaxLifetime.......251
UserManagement PasswordPolicy ReuseLimit.......252

Video settings.......252
Video ActiveSpeaker DefaultPIPPosition.......252
Video DefaultLayoutFamily Local.......253
Video DefaultLayoutFamily LocalContent.......253
Video DefaultLayoutFamily Remote.......254
Video DefaultMainSource.......254
Video Input Connector [n] CameraControl CameraId.......254
Video Input Connector [n] CameraControl Mode.......255
Video Input Connector [n] CEC Mode.......255
Video Input Connector [n] HDCP Mode.......256
Video Input Connector [n] InputSourceType.......256
Video Input Connector [n] Name.......257
Video Input Connector [n] OptimalDefinition Profile.......257
Video Input Connector [n] OptimalDefinition Threshold60fps.......258
Video Input Connector [n] PreferredResolution.......258
Video Input Connector [n] PresentationSelection.......259
Video Input Connector [n] Quality.......259
Video Input Connector [n] RGBQuantizationRange.......260
Video Input Connector [n] Visibility.......260
Video Monitors.......261
Video Output Connector [n] Brightness.......261
Video Output Connector [n] BrightnessMode.......261
Video Output Connector [n] CEC Mode.......262
Video Output Connector [n] Location HorizontalOffset.......262

Video Output Connector [n] Location VerticalOffset........ 263
Video Output Connector [n] MonitorRole........ 263
Video Output Connector [n] Resolution........ 264
Video Output Connector [n] RGBQuantizationRange........ 264
Video Output Connector [n] Whitebalance Level........ 265
Video Output Webcam USBMode........ 265
Video Presentation DefaultPIPPosition........ 265
Video Presentation DefaultSource........ 265
Video Presentation Priority........ 266
Video Selfview Default FullscreenMode........ 266
Video Selfview Default Mode........ 266
Video Selfview Default OnMonitorRole........ 266
Video Selfview Default PIPPosition........ 267
Video Selfview OnCall Duration........ 267
Video Selfview OnCall Mode........ 267

VoiceControl settings........ 268
VoiceControl Wakeword Mode........ 268

WebEngine settings........ 268
WebEngine Features LocalWebAppManagement........ 268
WebEngine Features SipUrlHandler........ 269
WebEngine Features WebGL........ 268
WebEngine MinimumTLSVersion........ 269
WebEngine Mode........ 269
WebEngine RemoteDebugging........ 269
WebEngine UseHttpProxy........ 269

Webex settings........ 270
Webex CloudProximity GuestShare........ 270
Webex CloudProximity Mode........ 270
Webex CloudUpgrades Mode........ 270
Webex Meetings JoinProtocol........ 271

WebRTC settings........ 271
WebRTC EndCallTimeout........ 271
WebRTC InteractionMode........ 271

Experimental settings........ 272

Software version:

- RoomOS 10.8.2

Products covered:

- CodecPro
- CodecPlus
- Room70G2
- Room70/Room55D
- Room55
- RoomKit
- RoomKitMini
- RoomPanorama/Room70Panorama
- DeskPro/DeskLE
- WebexDesk
- Boards

Audio settings

Audio DefaultVolume

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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.

Default value:

50 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk]*

70 *[Boards]*

Value space:

Integer (0..100)

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

Audio Input ARC [n] Mode

Applies to: CodecPlus CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Each HDMI output has an associated audio return channel (ARC). You can use the ARC to send audio from a screen or TV, which is connected to the HDMI ouput, to the video conferencing device. You can decide for each HDMI output connector (n) separately, whether or not to allow audio transmission.

Default value:

On

Value space:

Off/On

Off: Disable the ARC channel of HDMI output n (audio is not sent to the video conferencing device).

On: Enable the ARC channel of HDMI output n (audio is sent to the video conferencing device).

n: Unique ID that identifies the ARC input.

Range: 1..1 *[CodecPlus]*

Range: 1..3 *[CodecPro]*

Range: 3..3 for Room 70 Dual G2; 2..3 for Room 70 Single G2 *[Room70G2]*

Range: 3..3 *[RoomPanorama/Room70Panorama]*

Audio Input HDMI [n] Level

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Set the gain on the HDMI input connector. The gain can be tuned in steps of 1 dB.

Default value:

0

Value space:

Integer (-24..0)

Range: Select the gain in decibel (dB).

n: Unique ID that identifies the HDMI input.

Range: 2..3 *[CodecPlus Room70/Room55D]*

Range: 1..5 *[CodecPro]*

Range: 1..1 *[RoomKit RoomKitMini DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[Room55]*

Range: 2..5 *[Room70G2 RoomPanorama/Room70Panorama]*

Audio Input HDMI [n] Mode

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define if the audio on the HDMI input connector shall be enabled.

Default value:

On

Value space:

Off/On

Off: Disable audio on the HDMI input.

On: Enable audio on the HDMI input.

n: Unique ID that identifies the HDMI input.

Range: 2..3 *[CodecPlus Room70/Room55D]*

Range: 1..5 *[CodecPro]*

Range: 1..1 *[RoomKit RoomKitMini DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[Room55]*

Range: 2..5 *[Room70G2 RoomPanorama/Room70Panorama]*

Audio Input HDMI [n] VideoAssociation MuteOnInactiveVideo

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama WebexDesk

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

On *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D WebexDesk]*

HDMI *[1,2]*: Off HDMI [3,4,5]: On [CodecPro]

HDMI *[2]*: Off HDMI [3,4,5]: On [Room70G2 RoomPanorama/Room70Panorama]

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.

n: Unique ID that identifies the HDMI input.

Range: 2..3 *[CodecPlus Room70/Room55D]*

Range: 1..5 *[CodecPro]*

Range: 1..2 *[Room55]*

Range: 2..5 *[Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..1 *[RoomKit RoomKitMini WebexDesk]*

Audio Input Microphone [n] Channel

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define whether the signal on the microphone input is a mono signal or part of a multichannel signal.

Default value:

Mono

Value space:

Left/Mono/Right

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

Mono: The microphone input signal is a mono signal.

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

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input Microphone [n] EchoControl Mode

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

On

Value space:

Off/On

Off: Turn off the echo control. Recommended if external echo cancellation or playback equipment is used.

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

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..3 *[RoomKit Room55]*

Audio Input Microphone [n] EchoControl Dereverberation

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Off

Value space:

Off/On

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..3 *[RoomKit Room55]*

Audio Input Microphone [n] EchoControl NoiseReduction

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

On

Value space:

Off/On

Off: Turn off the noise reduction.

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

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..3 *[RoomKit Room55]*

Audio Input Microphone [n] Equalizer ID

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

1

Value space:

Integer (1..8)

Set the equalizer ID.

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input Microphone [n] Equalizer Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Off

Value space:

Off/On

Off: No equalizer.

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

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input Microphone [n] Level

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Set the gain on the Microphone input connector. The gain should be adjusted to suit the output level of the connected audio source. The gain can be tuned in steps of 1 dB.

If the gain is set too high, the audio signal will be clipped. If the gain is set too low, the audio signal-to-noise ratio will be degraded; however, this is usually preferable to clipping.

Note that unprocessed speech signals typically contain significant level variations, making it very important to allow for sufficient signal headroom.

The maximum input level with 0 dB gain differs depending on the product: -18 dBu (Room Kit, Codec Plus, Room 55, Room 70, Room 55 Dual), 24 dBu (Codec Pro, Room 70 G2).

Example: If your microphone has a maximum output level of -44 dBu, and it is connected to a Codec Pro, then you should set the gain to 24 dBu - (-44 dBu) = 68 dB.

Default value:

14 *[RoomKit CodecPlus Room55 Room70/Room55D]*

58 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Value space:

Integer (0..24) *[RoomKit CodecPlus Room55 Room70/Room55D]*

Integer (0..70) *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: Select the gain in decibel (dB).

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..3 *[RoomKit Room55]*

Audio Input Microphone [n] Mode

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Disable or enable audio on the microphone connector.

Room Kit, Room 55: Microphone [1] is the device's internal microphone.

Default value:

On

Value space:

Off/On

Off: Disable the audio input microphone connector.

On: Enable the audio input microphone connector.

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[RoomKit CodecPlus Room55 Room70/Room55D]*

Audio Input Microphone [n] MuteOverride

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

This setting is only for the analog microphone inputs on Codec Pro.

Configure the microphone input to override the main mute state of the system (i.e., the one controlled with the ordinary mute button(s)).

This allows for the microphone input to be unmuted and used as a line input for transmitting presentation sounds, etc. during active video input.

Note that the microphone may still be muted if it is associated with an inactive video input and is set to mute on inactive video input.

As an example, if one needs to present audio from an analog source, some of the microphone inputs need to be repurposed as line inputs.

Without MuteOverride, the sound from these presentation sources will go silent if the presenter mutes the microphone(s) during playback of the presentation.

Default value:

Off

Value space:

Off/On

Off: Do not override the mute setting.

On: Override the mute setting.

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input Microphone [n] PhantomPower

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define whether or not to have phantom power (48 V +/- 1 V) on the microphone input.

Default value:

On

Value space:

Off/On

Off: Disable the phantom power on the microphone input. Use this when connecting to equipment that do not need phantom power, such as external mixers.

On: Enable the phantom power on the microphone input. Use this when connecting directly to microphones that require phantom power, including the Cisco Table Microphone and Cisco Ceiling Microphone.

n: Unique ID that identifies the microphone input.

Range: 1..8 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Audio Input Microphone [n] VideoAssociation MuteOnInactiveVideo

Applies to: CodecPro

Requires user role: ADMIN, INTEGRATOR

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

Default value:

On

Value space:

Off/On

Off: No video source is associated.

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

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input Microphone [n] VideoAssociation VideoInputSource

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

1

Value space:

1/2/3/4/5/6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

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

n: Unique ID that identifies the microphone input.

Range: 1..8

Audio Input MicrophoneMode

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

If the microphone mode is Focused, the microphones can be combined to focus sound sensitivity. As a result, the noise in the room is suppressed, and you can be heard better when sitting right in front of the device. The voice of people not sitting right in front of the device will be suppressed.

If the microphone mode is Wide, the device behaves like any other device. The voice of people sitting beside you will be heard, and also more noise from the room.

We recommend that you use Focused mode when you are the only speaker. Use Wide mode when several speakers are in front of the device.

Default value:

Focused *[DeskPro/DeskLE WebexDesk]*

Value space:

Focused/Wide

Focused: Focused sound sensitivity, suppressing sound from sources that are not right in front of the device.

Wide: Default microphone operation with normal sound sensitivity.

Audio Input USBC [n] Level

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Set the USB-C audio level.

Default value:

0

Value space:

Integer (-24..0)

The audio level, between -24 and 0 decibels.

n: Unique ID that identifies the USBC input.

Range: 1..1

Audio Input USBC [n] Mode

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Set the USB-C audio mode.

Default value:

On

Value space:

Off/On

On: Allow audio from the USB-C.

Off: Do not allow any audio from the USB-C.

n: Unique ID that identifies the USBC input.

Range: 1..1

Audio Input USBC [n] VideoAssociation MuteOnInactiveVideo

Applies to: WebexDesk

Requires user role: ADMIN, INTEGRATOR

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.

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 USBC input source.

On: Audio is played, locally and to far end, only when the connected presentation source is shown on-screen.

n: Unique ID that identifies the USBC input.

Range: 1..1

Audio Input USBInterface [n] EchoControl Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

On

Value space:

Off/On

Off: Turn off the echo control. Recommended if external echo cancellation or playback equipment is used.

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

n: Unique ID that identifies the USB interface.

Range: 1..1

Audio Input USBInterface [n] Level

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Set the gain on the USB connector to fit the output level of the specific USB device that is connected. The output levels of USB devices may vary.

The gain can be tuned in steps of 1 dB.

Default value:

5

Value space:

Integer (0..24)

Set the gain in decibel (dB).

n: Unique ID that identifies the USB interface.

Range: 1..1

Audio Input USBInterface [n] Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Disable or enable audio input on the USB connector.

Default value:

On

Value space:

Off/On

Off: Disable audio input on the USB connector.

On: Enable audio input on the USB connector.

n: Unique ID that identifies the USB interface.

Range: 1..1

Audio Input USBMicrophone [n] Level

Applies to: RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Set the gain on the USB connector to fit the output level of the specific USB microphone that is connected. The output levels of USB microphones may vary.

The gain can be tuned in steps of 1 dB.

Default value:

5

Value space:

Integer (0..24)

Set the gain in decibel (dB).

n: Unique ID that identifies the USB interface.

Range: 1..1

Audio Input WebView[n] Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Set the WebView mode.

Default value:

On

Value space:

Off/On

On: Allow audio from the web browser.

Off: Do not allow any audio to be played from the web browser.

n: Unique ID that identifies the WebView input.

Range: 1..1

Audio Microphones AGC

Applies to: RoomKit CodecPlus

Requires user role: ADMIN, INTEGRATOR, USER

Enable or disable Automatic Gain Control (AGC) on the microphones.

Default value:

On

Value space:

Off/On

Off: Disable AGC. Use this when connecting to equipment where AGC is already applied to the microphone signal, like external mixers or DSPs.

On: Enable Automatic Gain Control.

Audio Microphones NoiseRemoval Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Show or hide the buttons on the user interface that allow users to turn background noise removal on and off. The setting also determines whether you can turn it on and off using API commands.

If the device is registered to the Webex cloud and in Personal Mode, the Enabled and Manual behavior is different from the description below. If noise removal is turned on, it stays on; if it's turned off, it stays off. This applies both after a call and after a device restart.

Default value:

Manual

Value space:

Disabled/Enabled/Manual

Disabled: The noise removal function is turned off and can't be turned on by the user or by sending API commands.

Enabled: You can turn noise removal on and off using buttons on the user interface or by sending API commands. Noise removal is turned on by default and returns to this state when a call ends or you restart the device.

Manual: You can turn noise removal on and off using buttons on the user interface or by sending API commands. Noise removal is turned off by default and returns to this state when a call ends or you restart the device.

Audio Microphones Mute Enabled

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define the microphone mute behavior on the device.

Default value:

True

Value space:

True/InCallOnly

True: Muting of audio is always available. In general, the microphone mute LED will not be lit outside of call, but you can still mute using the API commands.

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

Audio Microphones PhantomPower

Applies to: RoomKit CodecPlus Room55

Requires user role: ADMIN

Define whether or not to have phantom power (11 V +/- 1 V) on the microphone input.

Default value:

On

Value space:

Off/On

Off: Disable the phantom power on the microphone input. Use this when connecting to equipment that do not need phantom power, such as external mixers.

On: Enable the phantom power on the microphone input. Use this when connecting directly to microphones that require phantom power, including the Cisco Table Microphone and Cisco Ceiling Microphone.

Audio Output ARC [n] Delay DelayMs

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

0

Value space:

Integer (0..290)

The delay in milliseconds.

n: Unique ID that identifies the audio ARC output.

Range: 1..1

Audio Output ARC [n] Delay Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

You may add extra delay to an audio ARC output with the Audio Output ARC [n] Delay DelayMs setting. The extra delay added is either a fixed number of milliseconds, or a number of milliseconds relative to the detected delay on or reported by an external monitor.

Default value:

RelativeToHDMI *[CodecPro]*

Fixed *[Room70G2 RoomPanorama/Room70Panorama]*

Value space:

Fixed/RelativeToHDMI

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

RelativeToHDMI: Any extra delay (DelayMs) added to the output, will be relative to the detected delay on or reported by an external monitor. The actual delay is detected-delay + DelayMs. The Audio Output Connectors ARC [n] DelayMs status reports the actual delay.

n: Unique ID that identifies the audio ARC output.

Range: 1..1

Audio Output ARC [n] Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Choose whether or not to enable the audio return channel (ARC) on the HDMI [n] input connector. The ARC output must be enabled if you want audio playback through the Quad Camera.

On Room 70 G2, the Quad Camera is a part of the integrated loudspeaker system. We recommend to leave the ARC output enabled. If you want to disable the complete integrated loudspeaker system, use the Audio Output InternalSpeaker Mode setting.

Default value:

On

Value space:

Off/On

Off: Disable the ARC output on the HDMI input.

On: Enable the ARC output on the HDMI input.

n: Unique ID that identifies the audio ARC output.

Range: 1..1

Audio Output ConnectorSetup

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

You can choose whether to set up the audio inputs and outputs manually, or to let the video conferencing device do it automatically based on the type of camera you have and which screens are connected.

In Auto mode, you cannot add, update, delete or connect audio inputs and outputs manually. Therefore the following API commands do not have any effect: xCommand Audio Setup *, xCommand Audio LocalInput *, and xCommand Audio LocalOutput *.

When going from Manual to Auto mode: The existing Audio setup is cleared (xCommand Audio Setup Clear), and the input and output groups are set up according to product defaults. The Audio Output HDMI [n] Mode and Audio Output ARC [1] Mode settings are set to their default value. For Codec Pro automatic delay measurement is enabled.

When going from Auto to Manual mode: The HDMI and ARC output connectors are connected to the default groups. The Audio Output HDMI [n] Mode and Audio Output ARC [1] Mode settings are not changed. For Codec Pro delay measurement is stopped.

Default value:

Auto

Value space:

Auto/Manual

Auto: For Code Pro, the video conferencing device will play audio either through the camera, or through a screen that is connected to one of the HDMI outputs. The video conferencing device chooses to play the audio on the first available device in the following list:

1. A Quad Camera that has camera control connected to one of the camera control connectors of the video conferencing device (Ethernet 2 or 3), and HDMI connected to the camera input of the video conferencing device (HDMI 1 input). Additionally, the Audio Output ARC [1] Mode and Video Input Connector [1] CEC Mode settings must be On. The audio return channel (ARC) on the HDMI 1 input is used to play audio through the camera.

2. A screen that is connected to the HDMI 1 output, provided that the Audio Output HDMI [1] Mode setting is On.

3. A screen that is connected to the HDMI 2 output, provided that the Audio Output HDMI [2] Mode setting is On.

4. A screen that is connected to the HDMI 3 output, provided that the Audio Output HDMI [3] Mode setting is On.

When audio is played out through the Quad Camera, the video conferencing device will measure the delay between a screen and the camera, so that it can synchronize the audio on the camera with the video on screen (lip-synchronization). In order to measure the delay, the video conferencing device sends a signal to the screen, and the screen sends the signal back to the video conferencing device using the audio return channel. The first screen in the list above that supports CEC (Consumer Electronics Control), and has the Video Output Connector [n] CEC Mode set to On, is used for the delay measurements.

When audio is played out through a screen, additional lip-synchronization delay is the responsibility of the screen. The video conferencing device will not add any delay.

For Room 70 G2, the video conferencing device will play audio through its integrated loudspeaker system, provided that Audio Output ARC [1] Mode and Audio Output InternalSpeaker Mode is On, and Audio Output HDMI [n] Mode is On for the integrated screen(s). Automatic delay measurement is not necessary, because the relationship between the integrated loudspeaker system and screen(s) is known.

Manual: You must set up the audio inputs and outputs manually using the Audio Console application or the API (xCommand Audio LocalInput *, and xCommand Audio LocalOutput *).

For Room 70 G2, external screen(s) may be used for audio output if the connectors are explicitly added using the Audio Console application or the API (xCommand Audio LocalOutput *). In that case, the external screens will play a stereo down mix of the audio that is played on the built-in loudspeaker system. Ultrasound signals will not play through external screens or line outputs; only through the integrated loudspeaker system.

Audio Output Ethernet [n] Mode

Applies to: RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

This setting applies only to Room Panorama; not to Room 70 Panorama.

Ethernet [1]: For future use.

Ethernet [2]: Enable or disable audio output through the Ethernet connection to the DNAM IV amplifier.

We recommend you use the embedded Room Panorama audio system, which requires this setting to be On. If you switch it Off, the Room Panorama loudspeakers will not be used, and you will need to connect external loudspeakers to the codec.

Default value:

On

Value space:

Off/On

Off: The Ethernet connection is disabled.

On: The Ethernet connection is enabled.

n: Unique ID that identifies the Ethernet connection.

Range: 1..2

Audio Output HDMI [n] Delay DelayMs

Applies to: CodecPro

Requires user role: ADMIN, INTEGRATOR

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

Default value:

0

Value space:

Integer (0..290)

The delay in milliseconds.

n: Unique ID that identifies the audio line output.

Range: 1..3

Audio Output HDMI [n] Delay Mode

Applies to: CodecPro

Requires user role: ADMIN, INTEGRATOR

You may add extra delay to an audio hdmi output with the Audio Output HDMI [n] Delay DelayMs setting. The extra delay added is either a fixed number of milliseconds, or a number of milliseconds relative to the detected delay on or reported by an external monitor.

Default value:

Fixed

Value space:

Fixed/RelativeToHDMI

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

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

n: Unique ID that identifies the audio line output.

Range: 1..3

Audio Output HDMI [n] Level

Applies to: Room70G2

Requires user role: ADMIN, INTEGRATOR

Set the gain on the HDMI input connector. The gain can be tuned in steps of 1 dB.

Default value:

0

Value space:

Integer (-24..0)

Range: Select the gain in decibel (dB).

n: Unique ID that identifies the HDMI output.

Range: 1..3 *[Room70G2 RoomPanorama/Room70Panorama]*

Audio Output HDMI [n] Mode

Applies to: CodecPlus CodecPro Room70G2

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Room 70 Dual G2: HDMI 1,2: On HDMI 3: Off
Room 70 Single G2: HDMI 1: On HDMI 2,3: Off *[Room70G2 RoomPanorama/Room70Panorama]*
On *[CodecPlus CodecPro]*

Value space:

Off/On

Off: The connector will not be used for audio out.

On: The connector can be used for audio out. For Codec Pro and Room 70 G2 it depends on the Audio Output ConnectorSetup setting.

n: Unique ID that identifies the HDMI output.

Range: 1..1 *[CodecPlus]*
Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Audio Output InternalSpeaker Mode

Applies to: RoomKit CodecPlus Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define whether or not to use the camera's integrated speakers. Codec Plus must be connected to a Quad Camera for this setting to apply.

For Room 70 G2, the Audio Output HDMI [n] Mode settings for the integrated monitor(s) must be set to On in order to play any audio on the integrated speakers. For Room 70 G2, also the Audio Output ARC 1 Mode setting must be On.

For all products except Codec Plus, you can limit the use of the integrated speakers to play only ultrasound.

Default value:

On

Value space:

Off/On/UltrasoundOnly *[RoomKit Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Off/On *[CodecPlus]*

Off: Disable the device's integrated speakers.

On: Enable the device's integrated speakers.

UltrasoundOnly: Enable the device's integrated speakers only for ultrasound.

Audio Output Line [n] Channel

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Line *[1,3,5]*: Left Line [2,4,6]: Right [CodecPro Room70G2]

Room Panorama: Line *[1,3,5]*: Left Line [2,4,6]: Right

Room 70 Panorama: Line *[1,2]*: Mono Line [3,5]: Left Line [4,6]: Right [RoomPanorama/Room70Panorama]

Value space:

Left/Mono/Right

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

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

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

n: Unique ID that identifies the audio line output.

Range: 1..6

Audio Output Line [n] Delay DelayMs

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

0

Value space:

Integer (0..290)

The delay in milliseconds.

n: Unique ID that identifies the audio line output.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Audio Output Line [n] Delay Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Fixed *[Room70G2 RoomPanorama/Room70Panorama]*

RelativeToHDMI *[CodecPro]*

Value space:

Fixed/RelativeToHDMI

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

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

n: Unique ID that identifies the audio line output.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Audio Output Line [n] Equalizer ID

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

1

Value space:

Integer (1..8)

Set the equalizer ID.

n: Unique ID that identifies the audio line output.

Range: 1..6

Audio Output Line [n] Equalizer Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Default value:

Off

Value space:

Off/On

Off: No equalizer.

On: Enable the equalizer for the audio line output.

n: Unique ID that identifies the audio line output.

Range: 1..6

Audio Output Line [n] Level

Applies to: CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Set the gain on the Line output connector. The gain should be adjusted to fit the audio input level of the connected device. The gain can be tuned in steps of 1 dB.

The maximum output level with 0 dB gain differs depending on the product: 8 dBu (Room 70, Room 55 Dual), 18 dBu (Codec Pro, Room 70 G2).

Example: If the audio device that is connected to a Codec Pro has max input level 10 dBu, then you should set the gain to 10 dBu - 18 dBu = -8 dB.

Default value:

-4 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

0 *[Room70/Room55D]*

Value space:

Integer (-24..0)

Range: Select the gain in decibel (dB).

n: Unique ID that identifies the audio line output.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..1 *[Room70/Room55D]*

Audio Output Line [n] Mode

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the mode for the audio line output.

Default value:

On

Value space:

Off/On

Off: Disable the audio line output.

On: Enable the audio line output.

n: Unique ID that identifies the audio line output.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..1 *[RoomKit CodecPlus Room55 Room70/Room55D]*

Audio Output Line [n] OutputType

Applies to: RoomKit CodecPlus Room55 Room70/Room55D

Requires user role: ADMIN, INTEGRATOR

The output type should be set to match the connected device.

Default value:

Loudspeaker *[RoomKit CodecPlus Room55]*

LineOut *[Room70/Room55D]*

Value space:

LineOut/Loudspeaker/Microphone/Recorder/Subwoofer *[RoomKit]*

LineOut/Loudspeaker/Microphone/Recorder *[CodecPlus Room55 Room70/Room55D]*

Loudspeaker: Use Loudspeaker if a loudspeaker is connected to the line output. In this mode, the output level on that connector follows the master volume control and the output signal includes all system sounds (ringtones, webex assistant, etc.).

Microphone: In this mode, the sound picked up by the connected microphones will be sent to the line output. System sounds and sounds from far-end sources are not included.

Recorder: Use Recorder if a recorder is connected to the line output. In this mode, the output level is fixed and system sounds are not included. The sound from local presentation sources, the local microphones, and any far end sources are included.

Subwoofer: Use Subwoofer if a subwoofer is connected to the line output. In this mode, the bass is sent to line output and the rest of the audio range is played on the internal speaker.

LineOut: Use LineOut for other devices. In this mode, the output level is fixed and system sounds are not included. The sound from local presentation sources and far end sources are included.

n: Unique ID that identifies the audio line output.

Range: 1..1

Audio Output USBInterface [n] Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Disable or enable audio output on the USB connector.

Default value:

On

Value space:

Off/On

Off: Disable audio output on the USB connector.

On: Enable audio output on the USB connector.

n: Unique ID that identifies the USB interface.

Range: 1..1

Audio SoundsAndAlerts RingTone

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Define which ringtone to use for incoming calls.

Default value:

Sunrise *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk]*

Waves *[Boards]*

Value space:

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

Select a ringtone from the list.

Audio SoundsAndAlerts RingVolume

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Define the ring volume for incoming calls.

Default value:

50 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Default value:

Dynamic *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk]*

Static *[Boards]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

70

Value space:

Integer (0..90) *[CodecPlus CodecPro]*

Integer (0..70) *[RoomKit RoomKitMini Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Select a value in the specified range. If set to 0, ultrasound pairing messages are not emitted.

Audio USB Mode

Applies to: RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Enable or disable the audio channels on the USB connector.

Default value:

SpeakerAndMicrophone

Value space:

Microphone/Off/Speaker/SpeakerAndMicrophone *[RoomKit Room55 DeskPro/DeskLE WebexDesk]*

AdditionalMicrophone/Microphone/Off/Speaker/SpeakerAndMicrophone *[RoomKitMini]*

AdditionalMicrophone: Both the video conferencing device's built-in microphone and an external audio input device (microphone) will be used. The USB audio output channel is disabled.

Microphone: Only the external USB microphone will be used; other microphones are disabled. The USB audio output channel is also disabled.

Off: No audio will flow over USB but signaling is still enabled. This allows for using a USB device as a mute or volume controller.

Speaker: The USB audio output channel will be connected (speaker). Other speakers are disabled. The USB audio input channel is also disabled.

SpeakerAndMicrophone: Both the input (microphone) and output (speaker) channels of a USB audio device will be connected. Other microphones and speakers are disabled.

Bluetooth settings

Bluetooth Allowed

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN

The device has a built-in Bluetooth® module. As a default, the user can turn it on or off using the user interface. With this setting, the administrator can disable Bluetooth configuration, so that it cannot be set up from the user interface.

Default value:

True

Value space:

False/True

False: Bluetooth is switched off by the administrator, and the user cannot turn it on from the user interface.

True: Bluetooth is allowed. The user can turn it on or off from the user interface.

Bluetooth Enabled

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN

Provided that Bluetooth® connections are allowed (see the Bluetooth Allowed setting), you can use this setting to enable and disable Bluetooth. The video conferencing device supports the HFP (Hands-Free Profile) and A2DP (Advanced Audio Distribution Profile) profiles. Headsets that only supports A2DP cannot be used.

Default value:

False

Value space:

False/True

False: Bluetooth is disabled, and no Bluetooth devices can pair with the video conferencing device.

True: Bluetooth is enabled, and you can pair and use a Bluetooth headset.

Bookings settings

Bookings ProtocolPriority

Applies to: All products

Requires user role: ADMIN

Video devices can join Microsoft Teams meetings either using SIP via a Cloud Video Interop (CVI) gateway, which is a service that is provided in the Webex cloud, or by running the Microsoft Teams meeting web app (WebRTC).

Joining Microsoft Teams meetings relies on a calendar service and is available for devices that are registered to an on-premises service and linked to Webex Edge for Devices, and for devices that are registered to the Webex cloud service.

Default value:

Auto

Value space:

Auto/WebRTC

Auto: The device will join the Microsoft Teams meeting via SIP/CVI if there is a CVI address in the meeting invite. Otherwise it will use WebRTC.

WebRTC: The device will always use WebRTC for Microsoft Teams meetings.

BYOD settings

BYOD HidForwarding Enabled

Applies to: DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

If you use an external mouse or keyboard for your laptop (wired USB or USB dongle), you can connect them to the video conferencing device's USB port instead of directly to the laptop.

Default value:

False

Value space:

False/True

False: You must connect the external mouse or keyboard directly to your laptop.

True: You can connect the external mouse or keyboard for your laptop to the video conferencing device.

BYOD TouchForwarding Enabled

Applies to: DeskPro/DeskLE Boards

Requires user role: ADMIN, INTEGRATOR

Use this setting to enable or disable the touch redirect feature. Touch redirect enables you to control your laptop from the touch screen of the borad or video device. You must connect the laptop to the device with an HDMI cable (wired sharing) and a USB-C cable. You can use either a USB-C to USB-C cable or a USB-C to USB-A cable from the device to the laptop.

This feature is not available on the first generation of boards (Webex Board 55 and 70, not S-series).

Default value:

True

Value space:

False/True

False: Touch redirect is disabled.

True: Touch redirect is enabled.

CallHistory settings

CallHistory Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Specify 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.

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 Background Enabled

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, USER

Enable or disable the Camera Background feature.

The Camera Background feature allows for a virtual background (i.e., images or effects) to be shown as the background in the camera view, instead of the real surroundings. This configuration must be enabled to allow the Cameras Background Set command to take effect.

Default value:

True

Value space:

False/True

True: Enable the Camera Background feature.

False: Disable the Camera Background feature.

Cameras Background UserImagesAllowed

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN

Enable or disable the ability for users to use custom images as virtual background during meetings or calls.

The Cameras Background Enabled setting must also be enabled for this feature to be accessible.

Default value:

False

Value space:

False/True

True: Enable the use of custom images as virtual backgrounds.

False: Disable the use of custom images as virtual backgrounds.

Cameras Camera [n] AssignedSerialNumber

Applies to: CodecPlus CodecPro Room70/Room55D

Requires user role: ADMIN, INTEGRATOR

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

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

Typical situations where the video conferencing device does not receive EDID information are: when you connect a Cisco TelePresence Precision 60 camera using 3G-SDI, or when you use an HDMI repeater that does not pass on EDID information.

Default value:

" "

Value space:

String (0, 20)

The camera's serial number.

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Backlight DefaultMode

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Not applicable for the Cisco Quad Camera and the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions.

Default value:

Off

Value space:

Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Brightness Algorithm

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Specify the camera brightness algorithm.

Default value:

Auto

Value space:

Auto/Average/FaceOptimized

Auto: The camera brightness algorithm is automatically set by the device.

Average: The traditional brightness algorithm is applied. This uses the entire image area to calculate brightness.

FaceOptimized: Brightness is calculated by weighing the areas where people are detected. This includes automatic backlight compensation.

n: Unique ID that identifies the camera.

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Cameras Camera [n] Brightness Mode

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the camera brightness mode.

Not applicable for the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions.

Default value:

Auto

Value space:

Auto/Manual

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

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera Brightness Mode

Applies to: RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define the camera brightness mode.

Default value:

Auto

Value space:

Auto/Manual

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

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

Cameras Camera [n] Brightness DefaultLevel

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

Not applicable for the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions.

Default value:

20

Value space:

Integer (1..31)

The brightness level.

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera Brightness DefaultLevel

Applies to: RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

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

Default value:

20

Value space:

Integer (1..31)

The brightness level.

Cameras Camera ExposureCompensation Level

Applies to: DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Adjust for over- or under-exposure in camera images by setting an ExposureCompensation Level. Automatic exposure still runs, but this setting changes the target brightness.

Default value:

0

Value space:

Integer (-3..3)

A positive number increases brightness in the captured image; a negative number darkens it.

Cameras Camera [n] Flip

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

This feature is not supported by the Quad Camera, the PTZ-12 camera, and the integrated cameras of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama.

Default value:

Auto

Value space:

Auto/Off/On *[CodecPro]*

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

Off: Display the image on screen the normal way.

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Focus Mode

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the camera focus mode.

Default value:

Auto

Value space:

Auto/AutoLimited/Manual *[CodecPlus CodecPro]*

Auto/Manual *[Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Auto: The auto focus works differently for different products. For Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama,

and when using the Cisco Quad Camera with a codec (Codec Plus or Codec Pro), the camera will do single shot auto focusing once a call is connected, and when the view has changed.

When using a Cisco TelePresence Precision 60 camera with a codec (Codec Plus or Codec Pro), the camera will do continuous auto focusing. It will run auto focus once a call is connected,

after pan, tilt, or zoom, and generally when the camera identifies a change in the scene.

AutoLimited: This mode only applies when using a Cisco TelePresence Precision 60 camera with a Codec Plus or Codec Pro. In most cases this mode will operate the same way as auto focus.

In some cases, auto-limited will reduce the focus hunting that may occur.

Problematic scenes have large areas with no or low contrast (e.g., a painted wall with no details, oa partly empty whiteboard). There's a slightly higher chance of background focus with this mode, compared to auto focus.

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Gamma Mode

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

This setting enables gamma corrections. Gamma describes the nonlinear relationship between image pixels and monitor brightness.

It's not applicable for the Cisco Quad Camera and the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions. Also, this feature is not supported by the PTZ-12 camera.

Default value:

Auto

Value space:

Auto/Manual

Auto: Auto is the default and the recommended setting.

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Gamma Level

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

It's not applicable for the Cisco Quad Camera and the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions. Also, this feature is not supported by the PTZ-12 camera.

Default value:

0

Value space:

Integer (0..7)

Define the gamma level.

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Mirror

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

This setting is not applicable for the Cisco Quad Camera and the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. Also, this feature is not supported by the PTZ-12 camera.

Default value:

Auto *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Value space:

Auto/Off/On *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

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

Off: Display the image as other people see you.

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] MotorMoveDetection

Applies to: CodecPro

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

Off

Value space:

Off/On

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

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Cameras Camera [n] Whitebalance Mode

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the camera white balance mode.

It's not applicable for the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions.

Default value:

Auto

Value space:

Auto/Manual

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

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

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera [n] Whitebalance Level

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

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

It's not applicable for the integrated camera of Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, and Room Panorama. These cameras automatically adjust themselves based on the room lighting conditions. Also, the Whitebalance Level setting has no effect for the PTZ-12 camera, which is using Sony's One Push mode when the Whitebalance Mode is set to manual.

Default value:

1

Value space:

Integer (1..16)

The white balance level.

n: Unique ID that identifies the camera.

Range: 1..7 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Cameras Camera Framerate

Applies to: RoomKit RoomKitMini Room55

Requires user role: ADMIN

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.

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

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

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.

The Cisco 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.

Default value:

Auto

Value space:

50Hz/60Hz/Auto

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

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

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

Cameras PresenterTrack CameraPosition Pan

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the pan position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

0

Value space:

Integer (-65535..65535)

The pan position.

Cameras PresenterTrack CameraPosition Tilt

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the tilt position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

0

Value space:

Integer (-65535..65535)

The tilt position.

Cameras PresenterTrack CameraPosition Zoom

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the zoom position that the presenter tracking camera will move to when the feature is activated. Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

0

Value space:

Integer (-65535..65535)

The zoom position.

Cameras PresenterTrack Connector

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define which video input connector the presenter tracking camera is connected to. Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

1 *[CodecPlus Room70/Room55D]*

1 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Value space:

Integer (1..6) *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Integer (1..3) *[CodecPlus Room70/Room55D]*

The video input connector.

Cameras PresenterTrack Enabled

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define whether or not the PresenterTrack feature is available for use. Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

False

Value space:

False/True

False: The PresenterTrack feature is disabled.

True: The PresenterTrack feature is available for use.

Cameras PresenterTrack PresenterDetectedStatus

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define whether to enable or disable automatic switching between the Remote Presenter and Local Presenter modes in the Briefing room and Classroom scenarios (Room Type templates). Automatic switching implies that the device switches to Local Presenter mode when a person is detected in the PresenterTrack trigger zone, and that the device switches back to the Remote Presenter mode when the local presenter leaves the stage.

If this setting is enabled, the Cameras PresenterTrack PresenterDetected status will be updated when a new person enters the trigger zone.

Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking. Briefing room is not supported by Codec Plus, Room 70, and Room 55 Dual.

Default value:

Enabled

Value space:

Disabled/Enabled

Disabled: No automatic switching between modes.

Enabled: Automatic switching between the Local Presenter and Remote Presenter modes.

Cameras PresenterTrack TriggerZone

Applies to: CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the trigger zone, which corresponds to the area where a person's face must be detected for presenter tracking to start.

The format is a string of x and y coordinate pairs: "x1,y1,...xn,yn", where the range of x is (0,1920) and y is (0,1080). Two coordinate pairs define the upper left and lower right corner of a rectangular trigger zone. More than two coordinate pairs define the vertices of a polygonal trigger zone.

Only the Precision 60 and SpeakerTrack 60 cameras support presenter tracking.

Default value:

""

Value space:

String (0..255)

The coordinates for the trigger zone.

Cameras SpeakerTrack Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

This setting applies only when using a camera with support for speaker tracking or best overview.

Cisco Quad Camera: Speaker tracking uses automatic camera framing to select the best camera view based on where people are in the room. The Quad Camera uses an audio tracking technique that finds and captures a close-up of the active speaker.

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

Video conferencing devices with a built-in speakertrack camera (Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama, Boards): Speaker tracking uses automatic camera framing to select the best camera view based on where people are in the room. The camera uses an audio tracking technique that finds and captures a close-up of the active speaker.

Video conferencing devices with a camera that supports Best overview, but not speaker tracking (Room Kit Mini, Webex Desk, Desk Pro, Desk Limited Edition): Best overview uses automatic camera framing to select the best camera view based on where people are in the room.

Default value:

Auto

Value space:

Auto/Off

Auto: Speaker tracking (not supported on Room Kit Mini) and best overview is switched on. The device will detect people in the room and automatically select the best camera framing. Users can switch the feature on or off instantly in the camera control panel on the touch controller, but the feature is switched back on after each call so that the device is ready for the next user.

Off: Speaker tracking (not supported on Room Kit Mini, Webex Desk, Desk Pro, or Desk Limited Edition) and best overview is switched off. If you have a Cisco TelePresence SpeakerTrack 60 Camera assembly the two cameras will operate as individual cameras.

Cameras SpeakerTrack Closeup

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama Boards

Requires user role: ADMIN, INTEGRATOR, USER

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

When the closeup functionality is turned on, the device will detect that a person is speaking and select the best framing to cover that person. This is called a closeup and may not include all the persons in the room. If you want all the persons in the room to be in the picture at all times you can turn off the closeup functionality.

Default value:

Auto

Value space:

Auto/Off/On

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

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

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

Cameras SpeakerTrack TrackingMode

Applies to: CodecPlus CodecPro

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

Auto

Value space:

Auto/Conservative

Auto: This is the normal tracking mode.

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

Cameras SpeakerTrack ConnectorDetection Mode

Applies to: CodecPlus CodecPro

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

Auto

Value space:

Auto/Manual

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

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

Cameras SpeakerTrack ConnectorDetection CameraLeft

Applies to: CodecPlus CodecPro

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

1

Value space:

Integer (1..5) *[CodecPro]*

Integer (1..3) *[CodecPlus]*

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

Cameras SpeakerTrack ConnectorDetection CameraRight

Applies to: CodecPlus CodecPro

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

2

Value space:

Integer (1..5) *[CodecPro]*

Integer (1..3) *[CodecPlus]*

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

Cameras SpeakerTrack Whiteboard Mode

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR, USER

The Snap to Whiteboard feature extends the speaker tracking functionality, thus you need a camera that supports speaker tracking. When a presenter is standing next to the whiteboard, the camera will capture both the presenter and the whiteboard if the Snap to Whiteboard feature is enabled. If the feature is disabled, only the presenter will be captured. The Snap to Whiteboard feature is set up from the touch controller or web interface.

Default value:

Off

Value space:

Off/On

Off: The Snap to Whiteboard feature is disabled.

On: The Snap to Whiteboard feature is enabled.

Conference settings

Conference ActiveControl Mode

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..50)

The auto answer delay (seconds).

Conference CallProtocolIPStack

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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

Default value:

6000 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk]*

10000 *[Boards]*

16000 *[RoomPanorama/Room70Panorama]*

Value space:

Integer (64..6000) *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk]*

Integer (64..10000) *[Boards]*

Integer (64..20000) *[RoomPanorama/Room70Panorama]*

The default call rate (kbps).

Conference DoNotDisturb DefaultTimeout

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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 EndToEndEncryption Identity PreferredDomain

Applies to: All products

Requires user role: ADMIN

This is only available on devices registered to the Webex cloud service or linked to Webex Edge for devices.

This configuration is made when the admin sets the device's preferred domain from Control Hub. It is only necessary if the organization has more than one domain.

The device uses this domain when it requests a certificate from the Webex CA. The domain then identifies the device.

This configuration is not applicable when the device has an active, externally-issued certificate to identify itself.

Default value:

""

Value space:

String (0..255)

Conference EndToEndEncryption Mode

Applies to: All products

Requires user role: ADMIN

This is only available on devices registered to the Webex cloud service or linked to Webex Edge for devices.

Enables the End-to-End Encryption (E2EE) meeting option for the device.

Default value:

Off

Value space:

Off/On

On: Enable the use of E2EE for the device.

Off: Disable the use of E2EE for the device.

Conference FarEndControl Mode

Applies to: All products

Requires user role: ADMIN

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).

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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.

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 JoinLeaveNotifications

Applies to: All products

Requires user role: ADMIN

Specify when to show notifications of people entering or exiting meetings.

Default value:

Auto

Value space:

Always/Auto/Never

Always: Always show all notifications.

Auto: Show notifications only for the first 25 joining participants.

Never: Never show notifications.

Conference MaxReceiveCallRate

Applies to: All products

Requires user role: ADMIN

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.

Default value:

6000 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk]*

10000 *[Boards]*

20000 *[RoomPanorama/Room70Panorama]*

10000 *[Boards]*

Value space:

Integer (64..6000) *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk]*

Integer (64..20000) *[RoomPanorama/Room70Panorama]*

Integer (64..10000) *[Boards]*

The maximum receive call rate (kbps).

Conference MaxTransmitCallRate

Applies to: All products

Requires user role: ADMIN

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.

Default value:

6000 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk Boards]*

20000 *[RoomPanorama/Room70Panorama]*

Value space:

Integer (64..6000) *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk Boards]*

Integer (64..20000) *[RoomPanorama/Room70Panorama]*

The maximum transmitt call rate (kbps).

Conference MaxTotalReceiveCallRate

Applies to: All products

Requires user role: ADMIN

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.

Default value:

6000 *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D WebexDesk]*

10000 *[Boards]*

15000 *[CodecPro Room70G2 DeskPro/DeskLE]*

20000 *[RoomPanorama/Room70Panorama]*

Value space:

Integer (64..6000) *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D WebexDesk]*

Integer (64..10000) *[Boards]*

Integer (64..15000) *[CodecPro Room70G2 DeskPro/DeskLE]*

Integer (64..20000) *[RoomPanorama/Room70Panorama]*

The maximum receive call rate (kbps).

Conference MaxTotalTransmitCallRate

Applies to: All products

Requires user role: ADMIN

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.

Default value:

6000 *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D WebexDesk Boards]*

15000 *[CodecPro Room70G2 DeskPro/DeskLE]*

20000 *[RoomPanorama/Room70Panorama]*

Value space:

Integer (64..6000) *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D WebexDesk Boards]*

Integer (64..15000) *[CodecPro Room70G2 DeskPro/DeskLE]*

Integer (64..20000) *[RoomPanorama/Room70Panorama]*

The maximum transmit call rate (kbps).

Conference MicUnmuteOnDisconnect Mode

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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).

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

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN

The device supports multistream video for conferences.

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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.

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.

FacilityService settings

FacilityService Service [n] Type

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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.

n: Unique ID that identifies the service.

Range: 1..5

FacilityService Service [n] Name

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

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

Value space:

String (0, 1024)

The name of the facility service.

n: Unique ID that identifies the service.

Range: 1..5

FacilityService Service [n] Number

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

""

Value space:

String (0, 1024)

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

n: Unique ID that identifies the service.

Range: 1..5

FacilityService Service [n] CallType

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

Video

Value space:

Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.

n: Unique ID that identifies the service.

Range: 1..5

GPIO settings

GPIO Pin [n] Mode

Applies to: CodecPro Room70G2 RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

The four GPIO pins are configured individually. The actual measured pin state (Low/High) can be retrieved by the GPIO Pin [1..4] State status.

The default state for a pin in output mode is High (+12 V).

NOTE: A pin defined to output mode can be set to force line Low actively. If set to High, the line will be high only when it is not connected to an external device that pulls the line low.

Default value:

InputNoAction

Value space:

InputAcceptAllCalls/InputDisconnectAllCalls/InputMuteMicrophones/InputNoAction/OutputAllCallsEncrypted/OutputInCall/OutputManualState/OutputMicrophonesMuted/OutputPresentationOn/OutputStandbyActive

InputAcceptAllCalls: When the pin transitions from High to Low on an incoming call, the call will be accepted (the Call Accept command is issued automatically).

InputDisconnectAllCalls: When the pin transitions from High to Low during a call, call(s) will be disconnected (the Call Disconnect command is issued automatically).

InputMuteMicrophones: When the pin transitions from High to Low during a call, the microphones will be muted. When the pin transitions from Low to High during a call, the microphones will be unmuted (the Audio Mute and Audio Unmute commands are issued automatically).

InputNoAction: The pin state does not trigger any action. The pin state can be read with the GPIO Pin [1..4] State status.

OutputAllCallsEncrypted: The pin is set Low when all calls are encrypted, and High when one or more calls are not encrypted.

OutputInCall: The pin is set Low when in call, and High when not in call.

OutputManualState: The pin state can be set to High or Low by the GPIO ManualState Set PinX command. It is set to +12 V or 0 V, respectively.

OutputMicrophonesMuted: The pin is set Low when the microphones are muted, and High when they are not muted.

OutputPresentationOn: The pin is set Low when a presentation is active, and High when a presentation is not active.

OutputStandbyActive: The pin is set Low when the device is in standby mode, and High when the device is not in standby mode.

n: GPIO pin number.

Range: 1..4

H323 settings

H323 Authentication Mode

Applies to: All products

Requires user role: ADMIN

Define the authenticatin mode for the H.323 profile.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0, 50)

The authentication login name.

H323 Authentication Password

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0, 50)

The authentication password.

H323 CallSetup Mode

Applies to: All products

Requires user role: ADMIN

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.

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 AES256Support

Applies to: All products

Requires user role: ADMIN

The device always supports 128-bit AES encryption keys for the media transport. You can configure the device to also support 256-bit keys. When using 256-bit keys the minimum key size for the Diffie-Hellman key exchange method should be 2048 bit (refer to the H323 Encryption KeySize setting).

Default value:

Off

Value space:

Off/On

Off: The device only supports 128-bit AES encryption keys.

On: The device supports both 128-bit and 256-bit AES encryption keys.

H323 Encryption KeySize

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

Define the IP address of the Gatekeeper. Requires H323 CallSetup Mode to be set to Gatekeeper.

Default value:

""

Value space:

String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

H323 H323Alias E164

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0, 30)

The H.323 Alias E.164 address. Valid characters are 0-9, * and #.

H323 H323Alias ID

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

The H323 NAT Mode is intended to be used if your device is on a private network and is not registered to a gatekeeper. H323 NAT Mode can then be used to reach devices on a public network.

NAT is not supported for IPv6.

NOTE: The H323 NAT Mode and H323 NAT Address settings will be ignored if the video conferencing devices is registered to a gatekeeper. We recommend the use of a gatekeeper with firewall traversal capabilities, rather than using the H323 NAT Mode.

Default value:

Off

Value space:

Auto/Off/On

Auto: Auto mode works only if you have specified the NAT address in the H323 NAT Address setting.

NAT is turned On if the device is not registered to a gatekeeper, the local address of the device is private, the address you are calling (remote) is public, and both the local and remote addresses are IPv4. Otherwise, NAT is turned Off.

This means that you can place calls to devices on your private network as well as to external devices (outside your private network). For calls on your private network, the H323 NAT Address is not used (but must be present). For calls to the public network, the H323 NAT Address is used.

Off: NAT is turned off, and the H323 NAT Address setting will be ignored. In this case you will not be able to set up a call to a device that is outside of your private network unless you use a gatekeeper.

On: NAT is always turned on. You must specify the NAT address in the H323 NAT Address setting. The device will always signal the H323 NAT Address instead of its private IP address in Q.931 and H.245. If the H323 NAT Address is wrong or not set, H.323 calls cannot be set up.

H323 NAT Address

Applies to: All products

Requires user role: ADMIN

Define the external/global IP address of the router with NAT support. This address will be exposed when setting up a call to devices outside your private network. Refer to the H323 NAT Mode setting for details when the NAT Address is used.

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

Default value:

" "

Value space:

String (0, 64)

An IPv4 address. It's most often a public IP address, refer to RFC 1918, but it could also be another private address (e.g. in a larger company network).

H323 PortAllocation

Applies to: All products

Requires user role: ADMIN

This setting affects the H.245 port numbers used for H.323 call signaling.

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

Applies to: All products

Requires user role: ADMIN

Allow or prohibit communication with an external HTTP(S) server using HTTP(S) requests and responses.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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.

HttpClient UseHttpProxy

Applies to: All products

Requires user role: ADMIN

There are several UseHttpProxy settings that specify if a service shall communicate via an HTTP proxy or not. The HttpClient UseHttpProxy setting applies to macros and arbitrary HTTP(S) requests using the HttpClient commands.

For this setting to have any effect, a proxy server for HTTP, HTTPS, and WebSocket traffic must be set up using the NetworkServices HTTP Proxy settings.

Default value:

On

Value space:

Off/On

Off: Set up communication directly with the server (not using a proxy).

On: Set up communication via proxy.

HttpFeedback settings

HttpFeedback TlsVerify

Applies to: All products

Requires user role: ADMIN

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.

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.

HttpFeedback UseHttpProxy

Applies to: All products

Requires user role: ADMIN

There are several UseHttpProxy settings that specify if a service shall communicate via an HTTP proxy or not. The HttpFeedback UseHttpProxy setting applies to feedback sent from the video device.

For this setting to have any effect, a proxy server for HTTP, HTTPS, and WebSocket traffic must be set up using the NetworkServices HTTP Proxy settings.

Default value:

On

Value space:

Off/On

Off: Set up communication directly with the server (not using a proxy).

On: Set up communication via proxy.

Logging settings

Logging CloudUpload Mode

Applies to: All products

Requires user role: ADMIN

Specify whether or not logs from the device can be uploaded to the Webex cloud service. The device logs will be filtered for personally-identifiable information before they are sent to the cloud.

When enabled, the log upload can be initiated from the device itself or from Control Hub. The device will display a "Send logs" button on the user interface, and there will be a "Manage Logs" section on the Devices page in Control Hub.

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.

Default value:

Off

Value space:

Off/On

Off: Logs from the device can not be uploaded to the Webex cloud.

On: Logs from the device can be uploaded to the Webex cloud.

Logging Debug Wifi

Applies to: All products

Requires user role: ADMIN

When this option in 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.

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

Applies to: All products

Requires user role: ADMIN

Specify 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.

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

Applies to: All products

Requires user role: ADMIN

Specify 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.

Default value:

SyslogTLS

Value space:

Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

Logging External Server Address

Applies to: All products

Requires user role: ADMIN

Specify the address of the remote syslog server.

Default value:

" "

Value space:

String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Logging External Server Port

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

Specify 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.

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

Applies to: All products

Requires user role: ADMIN

Define the logging mode for the device (syslog service). When disabled, the syslog service does not start, and most of the systema and audit logs are not generated. The Historical Logs and Call Logs are not affected.

Default value:

On

Value space:

Off/On

Off: Disable the system logging service.

On: Enable the system logging service.

Macros settings

Macros Mode

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

5 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

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

Applies to: All products

Requires user role: ADMIN

Set the xAPI transport method used in the macro system.

Default value:

WebSocket

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

Off

Value space:

Off/On

Off: Disable Domain Name System Security Extensions.

On: Enable Domain Name System Security Extensions.

n: Index that identifies the network.

Range: 1..1

Network [n] DNS Domain Name

Applies to: All products

Requires user role: ADMIN

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".

Default value:

""

Value space:

String (0, 64)

The DNS domain name.

n: Index that identifies the network.

Range: 1..1

Network [n] DNS Server [m] Address

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address or IPv6 address.

n: Index that identifies the network.

Range: 1..1

m: Index that identifies the DNS server. **Maximum three DNS servers are allowed.**

Range: 1..3

Network [n] IEEE8021X Mode

Applies to: All products

Requires user role: ADMIN

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.

Default value:

Off

Value space:

Off/On

Off: The 802.1X authentication is disabled.

On: The 802.1X authentication is enabled.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X TlsVerify

Applies to: All products

Requires user role: ADMIN

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).

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X UseClientCertificate

Applies to: All products

Requires user role: ADMIN

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.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Identity

Applies to: All products

Requires user role: ADMIN

Define the username for 802.1X authentication.

Default value:

" "

Value space:

String (0, 64)

The username for 802.1X authentication.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Password

Applies to: All products

Requires user role: ADMIN

Define the password for 802.1X authentication.

Default value:

" "

Value space:

String (0, 50)

The password for 802.1X authentication.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X AnonymousIdentity

Applies to: All products

Requires user role: ADMIN

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.

Default value:

" "

Value space:

String (0, 64)

The 802.1X Anonymous ID string.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Eap Md5

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Eap Ttls

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Eap Tls

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled.

n: Index that identifies the network.

Range: 1..1

Network [n] IEEE8021X Eap Peap

Applies to: All products

Requires user role: ADMIN

Define the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Default value:

On

Value space:

Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled.

n: Index that identifies the network.

Range: 1..1

Network [n] IPStack

Applies to: All products

Requires user role: ADMIN

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.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv4 Assignment

Applies to: All products

Requires user role: ADMIN

Define how the device will obtain its IPv4 address, subnet mask and gateway address.

The client identifier, which is used in the DHCP requests, is different for different products: MAC address (Touch 10), "01" followed by the MAC address (Room Kit, Room Kit Mini, Room 55, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama, Boards, Codec Plus, and Codec Pro), and DHCP Unique Identifier (DUID) as specified in RFC 4361 (other products, including Room Navigator).

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv4 Address

Applies to: All products

Requires user role: ADMIN

Define the static IPv4 network address for the device. Applicable only when Network IPv4 Assignment is set to Static.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv4 Gateway

Applies to: All products

Requires user role: ADMIN

Define the IPv4 network gateway address. Applicable only when the Network IPv4 Assignment is set to Static.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv4 InterfaceIdentifier

Applies to: All products

Requires user role: ADMIN

Select which identifier to use for IPv4 DHCP.

Default value:

Auto

Value space:

Auto/MAC/Opaque

MAC: The device will send “01” followed by the MAC address of the device as identifier.

Opaque: The device will use an RFC4361-based DHCP Unique Identifier (DUID); DUID-LL, based on the link-layer address with no timestamp.

Auto: The use of MAC or Opaque as identifier depends on the product. MAC address (Touch 10), "01" followed by the MAC address (Room Kit, Room Kit Mini, Room 55, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama, Boards, Codec Plus, and Codec Pro), and DHCP Unique Identifier (DUID) as specified in RFC 4361 (other products, including Room Navigator).

n: Index that identifies the network.

Range: 1..1

Network [n] IPv4 SubnetMask

Applies to: All products

Requires user role: ADMIN

Define the IPv4 network subnet mask. Applicable only when the Network IPv4 Assignment is set to Static.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv6 Assignment

Applies to: All products

Requires user role: ADMIN

Define how the device will obtain its IPv6 address, subnet mask and gateway address.

The client identifier, which is used in the DHCP requests, is different for different products: MAC address (Touch 10), "01" followed by the MAC address (Room Kit, Room Kit Mini, Room 55, Room 70, Room 70 G2, Room 70 Panorama, Room Panorama, Boards, Codec Plus, and Codec Pro), and DHCP Unique Identifier (DUID) as specified in RFC 4361 (other products, including Room Navigator).

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv6 Address

Applies to: All products

Requires user role: ADMIN

Define the static IPv6 network address for the device. Applicable only when the Network IPv6 Assignment is set to Static.

Default value:

""

Value space:

String (0, 64)

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

n: Index that identifies the network.

Range: 1..1

Network [n] IPv6 Gateway

Applies to: All products

Requires user role: ADMIN

Define the IPv6 network gateway address. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Default value:

""

Value space:

String (0, 64)

A valid IPv6 address.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv6 DHCPOptions

Applies to: All products

Requires user role: ADMIN

Retrieve a set of DHCP options, for example NTP and DNS server addresses, from a DHCPv6 server.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] IPv6 InterfaceIdentifier

Applies to: All products

Requires user role: ADMIN

Define the IPv6 interface identifier for the device. The interface identifier you choose, either MAC or Opaque, will determine the method that is used for generating part of the the IPv6 address. This is applicable to both link-local IPv6 addresses and Stateless Address Autoconfiguration (SLAAC) addresses.

The address contains a 64-bit prefix and a 64-bit interface identifier generated by the device. With MAC, an EUI-64 based interface identifier is generated, as described in RFC-2373.

With Opaque, a random 64-bit interface identifier is generated as described in RFC-7217 on the first boot of the device, and this is used forever, or until factory reset.

Default value:

MAC

Value space:

MAC/Opaque

MAC: Select MAC as the Interface Identifier method.

Opaque: Select Opaque as the Interface Identifier method.

n: Index that identifies the network.

Range: 1..1

Network [n] MTU

Applies to: All products

Requires user role: ADMIN

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.

Default value:

1500

Value space:

Integer (576..1500)

Set a value for the MTU (bytes).

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Mode

Applies to: All products

Requires user role: ADMIN

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.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv Audio

Applies to: All products

Requires user role: ADMIN

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.

Default value:

46

Value space:

Integer (0..63)

Set the priority of the audio packets in the IP network. 0 means "best-effort".

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv Video

Applies to: All products

Requires user role: ADMIN

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets of the presentation channel (shared content) are also in the Video packet category. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use AF41 for Video. AF41 equals the decimal value 34.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Default value:

34

Value space:

Integer (0..63)

Set the priority of the video packets in the IP network. 0 means "best-effort".

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv Data

Applies to: All products

Requires user role: ADMIN

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.

Default value:

34

Value space:

Integer (0..63)

Set the priority of the data packets in the IP network. 0 means "best-effort".

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv Signalling

Applies to: All products

Requires user role: ADMIN

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.

Default value:

24

Value space:

Integer (0..63)

Set the priority of the signalling packets in the IP network. 0 means "best-effort".

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv ICMPv6

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..63)

Set the priority of the ICMPv6 packets in the IP network. 0 means "best effort".

n: Index that identifies the network.

Range: 1..1

Network [n] QoS Diffserv NTP

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..63)

Set the priority of the NTP packets in the IP network. 0 means "best-effort".

n: Index that identifies the network.

Range: 1..1

Network [n] RemoteAccess Allow

Applies to: All products

Requires user role: ADMIN

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.

Default value:

" "

Value space:

String (0..255)

A valid IPv4 address or IPv6 address.

n: Index that identifies the network.

Range: 1..1

Network [n] Speed

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] TrafficControl Mode

Applies to: All products

Requires user role: ADMIN

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

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.

n: Index that identifies the network.

Range: 1..1

Network [n] VLAN Voice Mode

Applies to: All products

Requires user role: ADMIN

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.

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.

n: Index that identifies the network.

Range: 1..1

Network [n] VLAN Voice VlanId

Applies to: All products

Requires user role: ADMIN

Define the VLAN voice ID. This setting will only take effect if Network VLAN Voice Mode is set to Manual.

Default value:

1

Value space:

Integer (1..4094)

Set the VLAN voice ID.

n: Index that identifies the network.

Range: 1..1

NetworkServices settings

NetworkServices CDP Mode

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

NetworkServices H323 Mode

Applies to: All products

Requires user role: ADMIN

Define whether the device should be able to place and receive H.323 calls or not.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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. We support the following HTTP authentication schemes: Digest using the MD5 algorithm, and the Basic HTTP authentication scheme.

Default value:

" "

Value space:

String (0, 80)

The authentication login name.

NetworkServices HTTP Proxy Mode

Applies to: All products

Requires user role: ADMIN

You can configure a proxy server for HTTP, HTTPS, and WebSocket traffic. The HTTP proxy can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

If NetworkServices HTTP Proxy Mode is not turned Off, you can further specify which services shall use the proxy in the HttpClient UseHttpProxy, HttpFeedback UseHttpProxy, and WebEngine UseHttpProxy settings.

Communication with the Cisco Webex cloud will always go via the proxy if NetworkServices HTTP Proxy Mode is not turned Off.

Regardless of the Proxy Mode, the device will never communicate with CUCM, MRA (CUCM via Expressway), or TMS via proxy.

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 PACUrl

Applies to: All products

Requires user role: ADMIN

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

Default value:

" "

Value space:

String (0..255)

The URL of the PAC (Proxy Auto Configuration) script.

NetworkServices HTTP Proxy Password

Applies to: All products

Requires user role: ADMIN

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. We support the following HTTP authentication schemes: Digest using the MD5 algorithm, and the Basic HTTP authentication scheme.

Default value:

""

Value space:

String (0, 64)

The authentication password.

NetworkServices HTTP Proxy Url

Applies to: All products

Requires user role: ADMIN

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Default value:

""

Value space:

String (0..255)

The URL of the HTTP proxy server.

NetworkServices HTTPS OCSP Mode

Applies to: All products

Requires user role: ADMIN

When a client certificate is used as login credentials to the web user interface and xConfiguration NetworkServices HTTPS VerifyClientCertificate is enabled, an Online Certificate Status Protocol (OCSP) responder service can be used to verify the client certificate's revocation status.

If Mode is set to On, the web UI examines the client certificate for an OCSP URL and contacts the host to check the client's certificate validity status.

Default value:

Off

Value space:

Off/On

Off/On: Disable/enable OSCP client certificate verification.

NetworkServices HTTPS OCSP URL

Applies to: All products

Requires user role: ADMIN

Specify the URL of the OCSP server that will be used to check the client's certificate validity status.

Default value:

""

Value space:

String (0..255)

A valid URL.

NetworkServices HTTPS Server MinimumTLSVersion

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

"0.tandberg.pool.ntp.org"

Value space:

String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

n: Unique ID for the NTP server.

Range: 1..3

NetworkServices NTP Server [n] Key

Applies to: All products

Requires user role: ADMIN

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 setting to supply the key. Prefix the key with "HEX:".

Default value:

""

Value space:

String (0, 2045)

The key, which is part of the ID/key pair that the NTP source uses.

n: Unique ID for the NTP server.

Range: 1..3

NetworkServices NTP Server [n] KeyId

Applies to: All products

Requires user role: ADMIN

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] KeyId settings for the ID.

Default value:

" "

Value space:

String (0, 10)

The ID, which is part of the ID/key pair that the NTP source uses.

n: Unique ID for the NTP server.

Range: 1..3

NetworkServices NTP Server [n] KeyAlgorithn

Applies to: All products

Requires user role: ADMIN

Choose the authentication hash function that the NTP server uses, and that the video conferencing device must use to authenticate the time messages.

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).

n: Unique ID for the NTP server.

Range: 1..3

NetworkServices SIP Mode

Applies to: All products

Requires user role: ADMIN

Define whether the device should be able to place and receive SIP calls or not.

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 SMTP Mode

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

You can set up the device to use SMTP (Simple Mail Transfer Protocol) for sending email from the device to a mail server for relaying. This is required if you want to allow users to send their whiteboards and presentations via email to people inside or outside their organization.

If the device is set up for encrypted communication (see the NetworkServices SMTP Security setting), the device only allows connections where the SMTP server's certificate is validated. There is no option for ignoring the certificate check.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

Off

Value space:

Off/On

Off: Disable SMTP (and email) support.

On: Enable SMTP support for sending email.

NetworkServices SMTP Server

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

This is the address of the SMTP server.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

""

Value space:

String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SMTP Port

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

This port is used for outgoing emails from the device to the SMTP server.

Set a port number based on the encryption setting (NetworkServices SMTP Security) and the requirements of the SMTP server. Do not use the default value.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

0

Value space:

Integer (0..65535)

The port used for outgoing emails from the device.

NetworkServices SMTP Username

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

This is the username part of the credentials that are used to authenticate the device with the SMTP server. This setting may be required by the SMTP server.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

""

Value space:

String (0, 80)

A valid username.

NetworkServices SMTP Password

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

This is the password part of the credentials that are used to authenticate the device with the SMTP server. This setting may be required by the SMTP server.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

""

Value space:

String (0, 64)

A valid password.

NetworkServices SMTP From

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

When sending an email message from this device, this is the name of the mailbox that the message is sent from.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

""

Value space:

String (0, 255)

An email address that meets the requirements of the SMTP server.

NetworkServices SMTP Security

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

Choose if and how to secure the communication between the device and the SMTP server.

This setting is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

StartTls

Value space:

None/StartTls/Tls

None: Connect to the SMTP server without encryption.

StartTls: Initially connect to the SMTP server without encryption, and then send a STARTTLS command to upgrade to an encrypted connection (TLS).

Tls: Connect to the SMTP server over TLS (Transport Layer Security).

NetworkServices SNMP Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

SNMP (Simple Network Management Protocol) is used by network management systems to monitor and manage network devices. The video conferencing device exposes the following object identifiers (OIDs), so that management systems can read and write basic parameters: SNMPv2-MIB::sysDescr (read), SNMPv2-MIB::sysObjectID (read), DISMAN-EVENT-MIB::sysUpTimeInstance (read), SNMPv2-MIB::sysContact (read/write), SNMPv2-MIB::sysName (read/write), SNMPv2-MIB::sysLocation (read/write), and SNMPv2-MIB::sysServices (read).

Note, Webex devices will stop supporting SNMP, and this configuration will be removed in a future release.

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 CommunityName

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Note, Webex devices will stop supporting SNMP, and this configuration will be removed in a future release.

Default value:

""

Value space:

String (0, 50)

The SNMP community name.

NetworkServices SNMP SystemContact

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define contact information that SNMP servers can use.

Note, Webex devices will stop supporting SNMP, and this configuration will be removed in a future release.

Default value:

""

Value space:

String (0, 50)

String that describes the contact information for the video device.

NetworkServices SNMP SystemLocation

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define location information that SNMP servers can use.

Note, Webex devices will stop supporting SNMP, and this configuration will be removed in a future release.

Default value:

""

Value space:

String (0, 50)

String that describes the location of the video device.

NetworkServices SSH Mode

Applies to: All products

Requires user role: ADMIN

The SSH (or Secure Shell) protocol can provide secure encrypted communication between the video conferencing device and your local computer.

Default value:

On

Value space:

Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

NetworkServices SSH HostKeyAlgorithm

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

Secure Shell (SSH) public key authentication can be used to access the device.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

600

Value space:

Integer (0..3600)

Range: Select a value between 0 and 3600 seconds.

NetworkServices Websocket

Applies to: All products

Requires user role: ADMIN

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).

Default value:

FollowHTTPService

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

Applies to: All products

Requires user role: ADMIN

Choose which information the user should see when logging on to the device through SSH.

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

Applies to: All products

Requires user role: ADMIN, USER

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: WPA2 Personal mode (AES), WPA2 with EAP-TLS, WPA2 with EAP-TTLS, WPA2 with EAP-FAST, WPA2 with PEAP (with EAP-MSCHAPv2 or 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.

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 WifiCloud A_MPDU

Applies to: All products

Requires user role: ADMIN

This config is to improve real-time media performance. When Aggregate MAC Protocol Data Unit (A-MPDU) is On, MAC Protocol Data frames are grouped and sent together. The receiver acknowledges reception of the group, rather than acknowledging every individual frame. This optimizes bandwidth but can lead to delays in data delivery. This is bad for data which requires a real-time delivery priority, such as video call data.

Default value:

Off

Value space:

Off/On

Off: Disable A-MPDU so that data is not grouped and sent together but is sent immediately to preserve real-time delivery priority.

On: Enable A-MPDU so that MAC Protocol Data frames are grouped and sent together.

NetworkServices Wifi Enabled

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

True

Value space:

False/True

False: Wi-Fi is disabled.

True: Wi-Fi is enabled.

NetworkServices XMLAPI Mode

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: The XML API is disabled.

On: The XML API is enabled.

Peripherals settings

Peripherals InputDevice Mode

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN

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.

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

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN

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.

Default value:

Off

Value space:

Off/On

Off: The EMC resilience is disabled.

On: The EMC resilience is enabled.

Peripherals Pairing CiscoTouchPanels RemotePairing

Applies to: All products

Requires user role: ADMIN

In order to use a touch controller (Cisco Webex Room Navigator or Cisco Touch 10) as user interface for the video conferencing device, the touch controller must be paired to the device. When the touch controller is paired via the network (LAN), this is referred to as remote pairing. Remote pairing is allowed by default; you must switch this setting Off if you want to prevent remote pairing.

Board 55/70 does not support the Room Navigator.

Default value:

On

Value space:

Off/On

Off: Remote pairing of the touch controller is not allowed.

On: Remote pairing of the touch controller is allowed.

Peripherals Profile Cameras

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define the number of external 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.

Default value:

Minimum1 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

0 *[DeskPro/DeskLE WebexDesk]*

Value space:

NotSet/Minimum1/0/1/2/3/4/5/6/7 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

0 *[DeskPro/DeskLE WebexDesk]*

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 Cameras

Applies to: Boards

Requires user role: ADMIN, INTEGRATOR

Define the number of external cameras that are expected to be connected to the 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.

Default value:

0

Value space:

0

0: The number of cameras that are expected to be connected to the device.

Peripherals Profile ControlSystems

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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

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

Default value:

NotSet

Value space:

1/NotSet *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama WebexDesk]*

NotSet *[DeskPro/DeskLE Boards]*

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 NetworkSwitches

Applies to: RoomPanorama/Room70Panorama

Requires user role: ADMIN, INTEGRATOR

Define the number of network switches that are expected to be connected to the device. This information is used by the device's diagnostics service. If the number of connected network switches does not match this setting, the diagnostics service will report it as an inconsistency.

Default value:

Room Panorama: 2; Room 70 Panorama: NotSet

Value space:

1/2/Minimum1/NotSet

NotSet: No network switch is connected.

Minimum1: At least one network switch should be connected to the device.

1-2: Specify the number of network switches that are expected to be connected to the device.

Peripherals Profile TouchPanels

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

Minimum1 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

0 *[DeskPro/DeskLE WebexDesk]*

Value space:

NotSet/Minimum1/0/1/2/3/4/5 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

0 *[DeskPro/DeskLE WebexDesk]*

NotSet: No touch controller check is performed.

Minimum1: At least one Cisco touch controller should be connected to the device.

0-5: Select the number of Cisco touch controllers that are expected to be connected to the device. The number of Cisco touch controllers that are officially supported are: 0 for Webex Desk and Desk Pro/Desk Limited Edition, 2 for Room Panorama and Room 70 Panorama, and 1 for the other products.

Phonebook settings

Phonebook Server [n] ID

Applies to: All products

Requires user role: ADMIN

Define a name for the external phone book.

Default value:

" "

Value space:

String (0, 64)

The name for the external phone book.

n: Unique ID that identifies the phonebook server.

Range: 1..1

Phonebook Server [n] Pagination

Applies to: All products

Requires user role: ADMIN

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.

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.

n: Unique ID that identifies the phonebook server.

Range: 1..1

Phonebook Server [n] TlsVerify

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

Select the phonebook server type.

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.

n: Unique ID that identifies the phonebook server.

Range: 1..1

Phonebook Server [n] URL

Applies to: All products

Requires user role: ADMIN

Define the address (URL) to the external phone book server.

Default value:

""

Value space:

String (0..255)

A valid address (URL) to the phone book server.

n: Unique ID that identifies the phonebook server.

Range: 1..1

Provisioning settings

Provisioning Connectivity

Applies to: All products

Requires user role: ADMIN, USER

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

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 CUCM CallManagementRecords CallDiagnostics

Applies to: All products

Requires user role: ADMIN, USER

Enable devices to send call statistics to CUCM which will then be populated in CUCM's Call Management Records The call statistics are sent to CUCM upon termination of a call.

Default value:

Enabled

Value space:

Disabled/Enabled

Enabled: Enables support for CUCM Call Management Records.

Disabled: Disables support for CUCM Call Management Records.

Provisioning ExternalManager Address

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager AlternateAddress

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

""

Value space:

String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager Protocol

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

HTTP

Value space:

HTTPS/HTTP

HTTPS: Send requests via HTTPS.

HTTP: Send requests via HTTP.

Provisioning ExternalManager Path

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

""

Value space:

String (0..255)

A valid path to the external manager or provisioning system.

Provisioning ExternalManager Domain

Applies to: All products

Requires user role: ADMIN, USER

Define the SIP domain for the VCS provisioning server.

Default value:

""

Value space:

String (0, 64)

A valid domain name.

Provisioning Mode

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

Auto

Value space:

Off/Auto/CUCM/Edge/Webex/WebexCalling/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. In order to register to the Webex cloud service, the encryption option key must be installed on the device.

WebexCalling: Not available in this release.

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

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

" "

Value space:

String (0, 80)

A valid username.

Provisioning Password

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

" "

Value space:

String (0, 64)

A valid password.

Provisioning TlsVerify

Applies to: All products

Requires user role: ADMIN, USER

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).

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

Applies to: All products

Requires user role: ADMIN, USER

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

On *[RoomKit RoomKitMini Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama Boards]*

Off *[CodecPlus CodecPro DeskPro/DeskLE WebexDesk]*

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

Applies to: All products

Requires user role: ADMIN, USER

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.

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

Applies to: All products

Requires user role: ADMIN, USER

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.

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

Applies to: All products

Requires user role: ADMIN, USER

This is no longer applicable.

Default value:

Disabled

Value space:

Disabled

RoomAnalytics settings

RoomAnalytics AmbientNoiseEstimation Interval

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Set the interval at which the ambient noise estimation is run, if enabled. The xConfiguration RoomAnalytics AmbientNoiseEstimation Mode can be used to enable or disable ambient noise estimations.

Default value:

10

Value space:

Integer (10..60)

Set the interval, in seconds, for how often the ambient noise estimation is run.

RoomAnalytics AmbientNoiseEstimation Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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.

Codec Plus, Codec Pro: Applies only when the device has a Cisco Quad Camera connected.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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.

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.

RoomAnalytics ReverberationTime Interval

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Defines how often the RT60 will be measured and reported to the RoomAnalytics status. The interval is in seconds.

The RoomAnalytics ReverberationTime Mode configuration must be enabled to set the interval.

Default value:

1800

Value space:

Integer (60..3600)

Interval in seconds.

RoomAnalytics ReverberationTime Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Reverberation time is a measure of how fast a sound will "fade away" or decay in a room.

This is highly related to the perception of the acoustic quality of a room.

The Cisco Webex devices are capable of measuring the reverberation time, RT60, directly from the acoustic echo canceller.

As opposed to traditional reverberation time measurement where it is required to emit a noise or impulse signal in the room, the Cisco device will measure RT60 as a “silent measurement”.

Due to the silent measurement behavior, the RT60 values will be indicative and not strictly correct according to the ISO 3382-2 standard.

The measurements will measure the RT60 values for each octave band from 125 Hz to 4 kHz.

Default value:

Off

Value space:

Off/On

On: activate the silent RT60 measurements.

Off: deactivate the silent RT60 measurements.

RoomCleanup settings

RoomCleanup AutoRun ContentType WebData

Applies to: All products

Requires user role: ADMIN

Enable or disable the daily room cleanup of web data. Use xConfiguration RoomCleanup AutoRun HourOfDay to set the time of day.

Default value:

Daily

Value space:

Daily/Off

Daily: Enable the daily clearing of web data.

Off: Disable the daily clearing of web data.

RoomCleanup AutoRun ContentType Whiteboards

Applies to: All products

Requires user role: ADMIN

Enable or disable the daily room cleanup of whiteboards. Use xConfiguration RoomCleanup AutoRun HourOfDay to set the time of day.

Default value:

Daily

Value space:

Daily/Off

Daily: Enable the daily clearing of whiteboards.

Off: Disable the daily clearing of whiteboards.

RoomCleanup AutoRun HourOfDay

Applies to: All products

Requires user role: ADMIN

Set the hour of the day when room cleanup will be performed each day.

Default value:

0

Value space:

Integer (0..23)

The hour of the day at which the room cleanup will occur.

RoomReset settings

RoomReset Control

Applies to: All products

Requires user role: ADMIN

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
```

Default value:

On

Value space:

Off/On

Off: No RoomReset events will be sent.

On: The room reset control is enabled and RoomReset events will be sent.

RoomScheduler settings

RoomScheduler BookingTimeout

Applies to: All products

Requires user role: ADMIN

The scheduler will provide immediate feedback to a user when they book a room or a device; however, the calendar service can take some time to confirm the booking.

If it takes too long to get the confirmation and this time exceeds the value set here, the booking will be cleared, and the device or room will be shown as available.

Default value:

60

Value space:

Integer (60..300)

The number of seconds to wait for a confirmation.

RoomScheduler Enabled

Applies to: All products

Requires user role: ADMIN

The room scheduling feature allows you to book a room directly from the touch controller that is in the meeting room. You can also extend an ongoing meeting if the room is still available. You can also use the Webex Assistant (voice-driven virtual assistant) to book or extend a meeting.

The room scheduling feature requires that the device is registered to the Webex cloud service or linked to Webex Edge for devices. In addition, the room must be set up with a calendar service that allows booking.

The room scheduling feature is not supported on personal mode devices.

Default value:

False

Value space:

False/True

False: The room scheduling feature is not available.

True: The room scheduling feature is available if the prerequisites listed above are met.

RTP settings

RTP Ports Range Start

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: AUDIT

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.

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

Applies to: All products

Requires user role: AUDIT

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.

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

Applies to: All products

Requires user role: AUDIT

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.

Default value:

""

Value space:

String (0..255)

A valid IPv4 address, IPv6 address, or DNS name.

Security Audit Server Port

Applies to: All products

Requires user role: AUDIT

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.

Default value:

514

Value space:

Integer (0..65535)

Set the audit server port.

Security Audit Server PortAssignment

Applies to: All products

Requires user role: AUDIT

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

60

Value space:

Integer (0..10000)

Set the lockout time (minutes).

Security Session InactivityTimeout

Applies to: All products

Requires user role: ADMIN

Define how long the device will accept inactivity from the user before automatically logging out from a web or SSH session.

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

Default value:

0

Value space:

Integer (0..10000)

Set the inactivity timeout (minutes). Specifying 0 will result in a time out of 1 hour. The maximum timeout length is 12 hours.

Security Session MaxFailedLogins

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..10)

Set the maximum number of failed login attempts per user.

Security Session MaxSessionsPerUser

Applies to: All products

Requires user role: ADMIN

The maximum number of simultaneous sessions per user is 20 sessions.

Default value:

20

Value space:

Integer (1..20)

Set the maximum number of simultaneous sessions per user.

Security Session MaxTotalSessions

Applies to: All products

Requires user role: ADMIN

The maximum number of simultaneous sessions in total is 20 sessions.

Default value:

20

Value space:

Integer (1..20)

Set the maximum number of simultaneous sessions in total.

Security Session ShowLastLogon

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Enable/disable the serial port. If the device has more than one serial port, this setting applies to all of them.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

Default value:

On

Value space:

Off/On

Off: Serial communication is disabled.

On: Serial communication is enabled.

SerialPort BaudRate

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Set the baud rate (data transmission rate) for the serial port. A new baud rate takes effect after a device reboot.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

This setting does not have any effect on a dedicated maintenance port (micro USB). The maintenance port always uses the default baud rate.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

Default value:

115200

Value space:

115200 *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk Boards]*

9600/19200/38400/57600/115200 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Choose a baud rate from the list (bits per second).

SerialPort LoginRequired

Applies to: All products

Requires user role: ADMIN

Define if login shall be required when connecting to a serial port. If the device has more than one serial port, this setting applies to all of them.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

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

Applies to: All products

Requires user role: ADMIN

ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Default value:

Off

Value space:

Off/On

Off: Disable ANAT.

On: Enable ANAT.

SIP Authentication UserName

Applies to: All products

Requires user role: ADMIN

This is the username part of the credentials used to authenticate towards the SIP proxy.

Default value:

" "

Value space:

String (0, 128)

A valid username.

SIP Authentication Password

Applies to: All products

Requires user role: ADMIN

This is the password part of the credentials used to authenticate towards the SIP proxy.

Default value:

" "

Value space:

String (0, 128)

A valid password.

SIP DefaultTransport

Applies to: All products

Requires user role: ADMIN

Select the transport protocol to be used over the LAN.

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

Applies to: All products

Requires user role: ADMIN

When configured the incoming call will report the display name instead of the SIP URI.

Default value:

" "

Value space:

String (0, 550)

The name to be displayed instead of the SIP URI.

SIP Ice DefaultCandidate

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Note that STUN also, regardless of the SIP Ice Mode, is used as a keep-alive mechanism to refresh NAT bindings.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama WebexDesk]*

Auto *[DeskPro/DeskLE Boards]*

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

Applies to: All products

Requires user role: ADMIN

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox.

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

IPv4

Value space:

IPv4/IPv6

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

SIP Proxy [n] Address

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

n: Index that identifies the proxy (maximum 4 proxys can be defined).

Range: 1..4

SIP TlsVerify

Applies to: All products

Requires user role: ADMIN

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.

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 Server

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

Define the username needed for accessing the TURN server.

Default value:

""

Value space:

String (0, 128)

A valid username.

SIP Turn Password

Applies to: All products

Requires user role: ADMIN

Define the password needed for accessing the TURN server.

Default value:

""

Value space:

String (0, 128)

A valid password.

SIP Type

Applies to: All products

Requires user role: ADMIN

Enables SIP extensions and special behavior for a vendor or provider.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

""

Value space:

String (0..255)

An address (URI) that is compliant with the SIP URI syntax.

Standby settings

Standby BootAction

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Define the camera position after a restart of the video conferencing device.

Default value:

DefaultCameraPosition *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama WebexDesk]*

RestoreCameraPosition *[DeskPro/DeskLE Boards]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define whether the device should go into standby mode or not.

Default value:

On

Value space:

Off/On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk Boards]*

On *[RoomPanorama/Room70Panorama]*

Off: The device will not enter standby mode.

On: The device will enter standby mode when the Standby Delay has timed out.

Standby Delay

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

10 *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk]*

4 *[Boards]*

Value space:

Integer (1..480)

Set the standby delay (minutes).

Standby Level Networked Delay

Applies to: WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define how long (in minutes) the device shall be in the "Display Off" level of standby mode before it goes into the "Networked" level of standby mode.

If the delay is set to 0, the device will go directly to Networked Standby, skipping the "Display Off" level.

Default value:

2

Value space:

Integer (0..1440)

Set the standby level networked delay (minutes).

Standby Level Networked Mode

Applies to: WebexDesk

Requires user role: ADMIN, INTEGRATOR

Disable/enable the automatic transition to networked standby mode.

Networked standby mode is a deeper level of standby which reduces power consumption further than the traditional standby mode.

The device will into the "Networked" level of standby mode after it has been in Standby, at the "DisplayOff" level, for x minutes, as defined in the Standby Level Networked Delay setting.

The Standby Control setting must be set to On for standby mode to be automatically initiated; however; you can trigger it manually with the Standby Activate command.

If Standby Level Networked Mode is On, the device will then enter networked standby mode after the Standby Level Networked Delay has timed out.

Default value:

On

Value space:

Off/On

On: The device will enter networked standby mode when the Standby Level Networked Delay has timed out.

Off: The device will not enter networked standby mode.

Standby Halfwake Mode

Applies to: All products

Requires user role: ADMIN

Disable/Enable the automatic halfwake mode.

By default, the device goes into halfwake mode after 2 minutes of inactivity.

It remains in halfwake mode until activity is detected or until it goes into standby mode.

If enabled in the Standby Control setting and regardless of Standby Halfwake Mode setting,

the device will go into standby after x minutes of inactivity, where x is defined by the Standby Delay setting.

Default value:

Auto

Value space:

Auto/Manual

Auto: By default, the device will go into halfwake mode after 2 minutes of inactivity. It will remain in halfwake mode until it enters Active mode or Standby mode, if enabled.

Manual: The automatic halfwake mode is disabled. It can only be triggered manually with xCommand Standby Halfwake.

Standby Signage Audio

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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 InteractionMode

Applies to: RoomKitMini DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN, INTEGRATOR

By default, a user cannot interact with a digital signage web page. You can use this setting to enable the ability to interact with the web page.

The Interactive mode is not available for Room Kit Mini in general, only when Room Kit Mini is used with Samsung Flip (Webex on Flip).

Default value:

NonInteractive

Value space:

Interactive/NonInteractive

Interactive: It's possible to interact with the web page.

NonInteractive: It's not possible to interact with the web page.

Standby Signage Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Content from a URL (a web page) can replace the traditional halfwake background image and information.

This feature is called digital signage. Users can interact with the web page if the device has an interactive screen, for example click on a link or enter text in a form.

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.

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 halfwake mode, provided that also the WebEngine Mode setting is On.

Standby Signage RefreshInterval

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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 halfwake mode.

If the URL fails, the device retains normal halfwake mode and a diagnostics message is issued.

Default value:

" "

Value space:

String (0, 2000)

The URL of the web page.

Standby StandbyAction

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

Define the camera position when going into standby mode.

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

Applies to: Room70/Room55D All products

Requires user role: ADMIN, INTEGRATOR, USER

Define the camera position when leaving standby mode.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

On *[RoomKit RoomKitMini Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Off *[CodecPlus CodecPro]*

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

" "

Value space:

String (0, 50)

Define the device name.

SystemUnit CrashReporting Advanced

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

"acr.cisco.com"

Value space:

String (0..255)

The URL to the Cisco Automatic Crash Report tool (ACR).

SystemUnit CustomDeviceId

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

The SystemUnit CustomDeviceId provides a place for you to store custom information about a unit. This can be useful, for example, in aiding to track devices in a provisioning setup).

Default value:

""

Value space:

String (0..255)

Time settings

Time TimeFormat

Applies to: All products

Requires user role: ADMIN, USER

Define the time format.

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

Applies to: All products

Requires user role: ADMIN, USER

Define the date format.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Define the time zone for the geographical location of the device. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Default value:

Etc/UTC

Value space:

Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Nuuk, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Porto_Velho, America/Puerto_Rico, America/Punta_Arenas, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Atyrau, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Famagusta, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qostanay, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yangon, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/

Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Saratov, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Samoa, UTC, Universal, W-SU, WET, Zulu

Select a time zone from the list.

UserInteraction settings

UserInteraction RaiseHand CMS

Applies to: All products

Requires user role: ADMIN, USER

This setting controls the availability of the raise hand feature for CMS meetings. If CMS supports the raise hand feature and this setting is set to True, then the raise hand button will be present in the user interface on the device.

Default value:

False

Value space:

False/True

False: The raise hand button will not be present.

True: The raise hand button will be present if CMS supports the feature.

UserInterface settings

UserInterface Accessibility IncomingCallNotification

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

You can enable an incoming call notification with amplified visuals. The screen and touch controller 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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

On

Value space:

Off/On

Off: Webex Assistant is switched off.

On: Webex Assistant can be used if it is supported by the infrastructure.

UserInterface Assistant ProactiveMeetingJoin

Applies to: All products

Requires user role: ADMIN

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.

Default value:

True

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 Bookings Visibility Title

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

Sets the meeting details to private. "Scheduled meeting" will be displayed as the title of the meeting.

Default value:

Auto

Value space:

Auto/Hidden

Auto: The title of the meeting is public and will be displayed on the user interface.

Hidden: The title of the meeting will be hidden and "Scheduled meeting" will be displayed on the user interface.

UserInterface Branding AwakeBranding Colors

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

Auto

Value space:

Auto/Native

Auto: The opacity of the logo is reduced.

Native: The logo has full colors.

UserInterface ContactInfo Type

Applies to: All products

Requires user role: ADMIN

Choose which type of contact information to show in the user interface.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

A custom message can be displayed, in the lower left side of the screen, in awake mode.

Default value:

" "

Value space:

String (0, 256)

Add a custom message. Add an empty string to remove a custom message.

UserInterface Diagnostics Notifications

Applies to: All products

Requires user role: ADMIN

Hide or show diagnostics notifications on the user interface.

Default value:

Auto

Value space:

Auto/Hidden

Auto: The diagnostics notifications will be displayed on the user interface.

Hidden: The diagnostics notifications will not be displayed on the user interface.

UserInterface KeyTones Mode

Applies to: All products

Requires user role: ADMIN, USER

You can configure the device to make a keyboard click sound effect (key tone) when typing text or numbers.

Default value:

Off *[DeskPro/DeskLE WebexDesk Boards]*

On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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 Keypad

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose whether or not to remove the default in-call Keypad button from the user interface. This button opens a keypad, which for example can be used for DTMF input.

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 JoinGoogleMeet

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE Boards

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the GoogleMeet button on the user interface.

The button allows users to dial into Google Meet meetings using just the meeting code generated by the Google invite.

This is only available on devices registered to the Webex cloud service or linked to Webex Edge for devices.

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 JoinWebex

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the default Join Webex button on 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.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the default Hold, Transfer, and Resume in-call buttons on the user interface.

The setting removes only the buttons, not their functionality as such.

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 MusicMode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the toggle button for Music Mode on the user interface.

Default value:

Hidden

Value space:

Auto/Hidden

Auto: Shows the toggle button for Music Mode in the user interface if this feature is supported in the ongoing call.

Hidden: The toggle button for Music Mode is never shown in the user interface.

UserInterface Features Call Start

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the default Call button (including the directory, favorites, and recent calls lists)

and the default in-call Add participant button on the user interface. The setting removes only the buttons, not their functionality as such.

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

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN, INTEGRATOR

Choose to show or hide the default "Turn video off" button on the user interface.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Choose to hide all the buttons on the user interface.

The setting removes only the buttons, not their functionality.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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 still share content using Cisco Proximity or Cisco Webex apps.

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 Features Whiteboard Start

Applies to: DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN, INTEGRATOR

Choose whether or not to remove the default Whiteboard button from the user interface. The setting removes only the button, not its functionality as such. This setting only applies to Cisco Webex registered devices.

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 Language

Applies to: All products

Requires user role: ADMIN, USER

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

Default value:

English

Value space:

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

Select a language from the list.

UserInterface LedControl Mode

Applies to: All products

Requires user role: ADMIN

You can configure the LED lights on a Room Scheduler.

Default value:

Auto

Value space:

Auto/Manual/Off

Auto: Use the default system settings for Room Scheduler

(i.e., Green – available, Red – in use, Yellow – meeting starting soon).

Manual: Set the color manually using xCommand UserInterface LedControl Color Set Color with value options of Green, Red, Yellow, and Off.

Off: Turn off the LED lights.

UserInterface NameAndSiteLabels Mode

Applies to: All products

Requires user role: ADMIN

You can configure a device to hide all name and site labels for remote participants in a meeting.

Default value:

Auto

Value space:

Auto/Hidden

Auto: Show name and site labels.

Hidden: Hide name and site labels.

UserInterface OSD EncryptionIndicator

Applies to: All products

Requires user role: ADMIN

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a locked padlock.

Default value:

Auto

Value space:

Auto/AlwaysOn/AlwaysOff

Auto: If the call is encrypted, a "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. No encryption indicator icon is shown.

AlwaysOn: The “Call is encrypted” notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

AlwaysOff: The encryption indicator is never displayed on screen.

UserInterface OSD HalfwakeMessage

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

A custom message can be displayed in the middle of the main screen when the device is in the halfwake 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.

Default value:

""

Value space:

String (0, 128)

The custom message. An empty string: Restore the default message. A space only: There will be no message at all.

UserInterface OSD Mode

Applies to: All products

Requires user role: ADMIN

You can configure a device to output a clean video stream. This is referred to as broadcast mode. In this mode the indicators, notifications, and controls are removed. This mode is primarily for broadcasting and recording services where you only want to pass on the video to your viewers.

Default value:

Auto

Value space:

Auto/Unobstructed

Auto: Indicators, notifications, and controls are included in the video stream (normal mode).

Unobstructed: Indicators, notifications, and controls are removed from the video stream (broadcast mode). Name labels are not removed.

UserInterface OSD Output

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Default value:

1 *[CodecPro Room55 Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Auto *[RoomKit RoomKitMini CodecPlus Room70/Room55D]*

Value space:

1 *[Room55 DeskPro/DeskLE WebexDesk Boards]*

Auto/1/2 *[RoomKit CodecPlus Room70/Room55D]*

Auto/1/2/3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Auto *[RoomKitMini]*

Auto: For devices with integrated screen, the on-screen information and indicators are sent to the integrated screen. If the device has two integrated screens, the left monitor is used.

For devices without integrated screens, the device detects when a monitor is connected to a video output, and sends the on-screen information and indicators to the first monitor you connect. If you have a multi-monitor setup, and all monitors are connected before switching on the device, the on-screen information and indicators are sent to the video output with the lowest number, starting with Output Connector 1 (HDMI 1).

1..n: The device sends the on-screen information and indicators to the specified output. Choose n to send the on-screen information and indicators to the device's Output Connector n.

For devices with integrated screens, the lowest numbers refer to the integrated screens.

UserInterface Phonebook Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

ReadWrite

Value space:

ReadOnly/ReadWrite

ReadOnly: You neither can add a contact to the Favorites list, edit a contact in the Favorites list, nor edit any contact from the Directory or Favorites list before calling.

ReadWrite: You are able to add a contact to the Favorites list, edit a contact in the Favorites list, and edit a contact from the Directory or Favorites list before calling.

UserInterface Proximity Notifications

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Configure the display of proximity notifications on the user interface.

Default value:

Auto

Value space:

Auto/Off/On

Auto: Allow the system to automatically determine when to display proximity notifications.

Off: Proximity notifications will not be shown on the user interface.

On: All proximity notifications will be shown on the user interface.

UserInterface Security Mode

Applies to: All products

Requires user role: ADMIN

This setting allows you to prevent important device information from being exposed in the user interface (drop down menu and Settings panel), for example the contact information and IP addresses of the video conferencing device, touch controller, and UCM/VCS registrars. It is important to note that such information is not hidden when navigating further into the Settings panel.

If you want to fully prevent that people without administrator rights can see the contact information, IP addresses, MAC address, serial number, and software version, you must also set the UserInterface SettingsMenu Mode to Locked, and of course have a passphrase for all user accounts with administrator rights.

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

Applies to: All products

Requires user role: ADMIN

The Settings panel in the user interface (touch controller 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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN, USER

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).

Default value:

On

Value space:

Off/On

Off: There are no sound effects.

On: The sound effects are switched on.

UserInterface Theme Name

Applies to: All products

Requires user role: ADMIN, USER

Change the theme on the user interface.

Note, this config may change or be replaced in the future.

Default value:

Auto

Value space:

Auto/Light/Night

Auto: Use the default settings, letting the system decide what is best.

Light: Use the "Light" background theme.

Night: Use the "Night" background theme.

UserInterface Wallpaper

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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. Additionally,

the endpoint does not go automatically into halfwake state, as it would do otherwise after 2 minutes without any activity.

Default value:

Auto

Value space:

Auto/Custom/None

Auto: Use the default wallpaper.

None: There is no background image on the screen.

Custom: Use the custom wallpaper as background image on the screen.

If no custom wallpaper is uploaded to the device, the setting will revert to the default value.

UserInterface UsbPromotion

Applies to: RoomKitMini

Requires user role: ADMIN

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

Default value:

Off

Value space:

Off/On

Off: The USB camera information text is not shown.

On: The USB camera information text is shown.

UserInterface WebcamOnlyMode

Applies to: RoomKitMini

Requires user role: ADMIN

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.

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.

UserInterface Whiteboard ActivityIndicators

Applies to: All products

Requires user role: ADMIN

Activity indicators let you see who is drawing and annotating in a call.

The avatars of the participants or the initials of the device are displayed when someone is interacting with the whiteboard, so you can follow who is drawing or annotating.

Applies only to cloud-registered devices.

Default value:

On

Value space:

Off/On

On: Enables activity indicators.

Off: Disables activity indicators.

UserInterface Whiteboard DefaultTheme

Applies to: All products

Requires user role: ADMIN

Change the whiteboard default theme to be black or white.

Default value:

Light

Value space:

Dark/Light

Dark: The default appearance of the whiteboard is black. It is also black when someone shares a whiteboard with you.

Light: The default appearance of the whiteboard is white. It is also white when someone shares a whiteboard with you.

UserManagement settings

UserManagement LDAP Admin Filter

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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

Default value:

""

Value space:

String (0..255)

The attribute name.

UserManagement LDAP BaseDN

Applies to: All products

Requires user role: ADMIN

The distinguishing name of the entry at which to start a search (base).

Default value:

""

Value space:

String (0..255)

The distinguishing name of the base. Example: "DC=company, DC=com"

UserManagement LDAP Encryption

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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

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

Applies to: All products

Requires user role: ADMIN

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))"

Default value:

Off

Value space:

Off/On

Off: LDAP authentication is not allowed.

On: LDAP authentication is allowed.

UserManagement LDAP Server Address

Applies to: All products

Requires user role: ADMIN

Set the IP address or hostname of the LDAP server.

Default value:

""

Value space:

String (0..255)

A valid IPv4 address, IPv6 address or hostname.

UserManagement LDAP Server Port

Applies to: All products

Requires user role: ADMIN

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).

Default value:

0

Value space:

Integer (0..65535)

The LDAP server port number.

UserManagement LDAP VerifyServerCertificate

Applies to: All products

Requires user role: ADMIN

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.

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

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..4)

The minimum number of numerical characters. 0 means no restrictions.

UserManagement PasswordPolicy Complexity MinimumLength

Applies to: All products

Requires user role: ADMIN

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.

Default value:

8

Value space:

Integer (0..256)

The minimum number of characters. 0 means no restrictions.

UserManagement PasswordPolicy Complexity MinimumLowercase

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..4)

The minimum number of lower-case characters. 0 means no restrictions.

UserManagement PasswordPolicy Complexity MinimumSpecial

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..4)

The minimum number of special characters. 0 means no restrictions.

UserManagement PasswordPolicy Complexity MinimumUppercase

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..4)

The minimum number of upper-case characters. 0 means no restrictions.

UserManagement PasswordPolicy MaxLifetime

Applies to: All products

Requires user role: ADMIN

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.

Default value:

0

Value space:

Integer (0..7300)

The minimum number of days. 0 means no restrictions.

UserManagement PasswordPolicy ReuseLimit

Applies to: All products

Requires user role: ADMIN

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.

Default value:

12

Value space:

Integer (0..24)

The minimum number of passwords. 0 means no restrictions.

Video settings

Video ActiveSpeaker DefaultPIPPosition

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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

Applies to: All products

Requires user role: ADMIN

Select which video layout family to use locally. This setting applies only when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

Default value:

Auto

Value space:

Auto/Equal/Overlay/Prominent/Prominent_L/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 Grid layout family will be used as the local layout. Participants are shown in a grid of equal sized videos. If there is shared content it will appear beside the grid.

Overlay: The Overlay layout family will be used as the local layout. The active speaker will be shown in full screen, with the other participants in thumbnails overlaid across the bottom. If there is content it will appear in full screen with the active speaker in a thumbnail overlaid at the top. Transitions between active speakers are voice switched.

Prominent: The Stack layout family will be used as the local layout. The active speaker, or shared content, will be a large picture, while the other participants will be small pictures across the top. Transitions between active speakers are voice switched.

Prominent_L: The Prominent layout family will be used as the local layout. The active speaker is shown in the upper left part of the screen, and other participants are ranged across the bottom and beside on the right.

Single: The Focus layout family will be used as the local layout. 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 LocalContent

Applies to: All products

Requires user role: ADMIN

Select which video layout family to switch to by default locally, when content sharing starts. This setting applies only when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

Default value:

Auto

Value space:

Auto/Equal/Overlay/Prominent/Prominent_L/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 Grid layout family will be used as the local layout. Participants are shown in a grid of equal sized videos. Shared content will appear beside the grid.

Overlay: The Overlay layout family will be used as the local layout. Shared content will appear in full screen with the active speaker in a thumbnail overlaid at the top.

Prominent: The Stack layout family will be used as the local layout. The shared content will be a large picture, and participants will be small pictures across the top.

Prominent_L: The Prominent layout family will be used as the local layout. Content is shown in the upper left part of the screen, and participants are ranged across the bottom and beside on the right.

Single: The Focus layout family will be used as the local layout. The shared content will be shown in full screen. Participants are not shown.

Video DefaultLayoutFamily Remote

Applies to: All products

Requires user role: ADMIN

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.

Default value:

Auto

Value space:

Auto/Equal/Prominent/Prominent_L/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 Grid layout family will be used as the local layout. Participants are shown in a grid of equal sized videos. If there is shared content it will appear beside the grid.

Overlay: The Overlay layout family will be used as the local layout. The active speaker will be shown in full screen, with the other participants in thumbnails overlaid across the bottom. If there is content it will appear in full screen with the active speaker in a thumbnail overlaid at the top. Transitions between active speakers are voice switched.

Prominent: The Stack layout family will be used as the local layout. The active speaker, or shared content, will be a large picture, while the other participants will be small pictures across the top. Transitions between active speakers are voice switched.

Prominent_L: The Prominent layout family will be used as the local layout. The active speaker is shown in the upper left part of the screen, and other participants are ranged across the bottom and beside on the right.

Single: The Focus layout family will be used as the local layout. 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

Applies to: All products

Requires user role: ADMIN, USER

Define the default input source for main video in calls. The main video is played on this source when you switch on or restart the video conferencing device. Use the Video Input SetMainVideoSource command to change to another source while the device is running.

Default value:

1

Value space:

1/2/3/4/5/6 *[CodecPro]*

1/2/3/4 *[Room70G2 RoomPanorama/Room70Panorama]*

1 *[RoomKitMini Boards]*

1/2/3 *[RoomKit CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

The default source for main video.

Video Input Connector [n] CameraControl CameraId

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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

For devices with more than one camera you can use the xStatus Camera API command to see the IDs of the different cameras.

Default value:

Connector n: n *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

1 *[RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk Boards]*

Value space:

1/2/3/4/5/6/7 *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

1 *[RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk Boards]*

For devices with more than one camera, select the ID of the camera. For devices with one camera the value is fixed and cannot be changed.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] CameraControl Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define whether the camera on this video input connector can be controlled or not. Some connectors cannot be controlled (Off is the only available value).

Default value:

On *[CodecPlus Room70/Room55D]*

Connector 1,2,3,4,5: On Connector 6: Off *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: On Connector 2,3: Off *[Room55 DeskPro/DeskLE WebexDesk]*

Connector 1: On Connector 2: Off *[RoomKit RoomKitMini Boards]*

Value space:

Off/On *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: Off/On Connector 2,3: Off *[Room55 DeskPro/DeskLE WebexDesk]*

Connector 1: Off/On Connector 2: Off *[RoomKit RoomKitMini Boards]*

Off: Disable camera control.

On: Enable camera control.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] CEC Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

The video input (HDMI) supports Consumer Electronics Control (CEC). When this setting is enabled, information about the connected device (for example device type and device name) is available in the video conferencing device status (Video Input Connector[n] ConnectedDevice CEC [n]), provided that the connected device also supports CEC.

If you have Cisco Quad Camera, do not switch off CEC on that connector because then there will be no sound on the speakers on the camera. CEC is required for HDMI ARC (Audio Return Channel), which is the channel used for sending audio from the video conferencing device to the camera.

Default value:

On

Value space:

Off/On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Connector 1: On Other connectors: Off/On *[Room70/Room55D]*

Off: CEC is disabled.

On: CEC is enabled.

n: Unique ID that identifies the video input connector.

Range: 1..5 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..3 *[Room55 DeskPro/DeskLE WebexDesk]*

Range: 2..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] HDCP Mode

Applies to: CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/ Room70Panorama

Requires user role: ADMIN, INTEGRATOR

One of the video conferencing device's HDMI inputs can be configured to support HDCP protected content (High-bandwidth Digital Content Protection, version 1.4). This allows customers to re-purpose a video conferencing device's screen by connecting devices such as a Google ChromeCast, an AppleTV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the input connector is configured to support HDCP, it is reserved for this type of content. This means that you can't share any content from this specific connector while in a call, regardless of what is connected, nor can you take web snapshots of this source.

The screens, on which the protected content is displayed, must support HDCP. For Codec Plus, Room 70 (Single and Dual), and Room 55 Dual, the protected content is always displayed on the screen that is connected to output connector 1; for Codec Pro, Room 70 G2 (Single and Dual), Room Panorama, and Room 70 Panorama, the protected content is displayed on screens connected to output connector 1 and 2; and for Room 55, the protected content is displayed on the integrated screen. The integrated screens of devices in the Room Series support HDCP.

Default value:

Off

Value space:

Connector 1,3: Off, Connector 2: Off/On *[CodecPlus Room70/Room55D]*

Connector 1,2,3,4: Off, Connector 5: Off/On *[CodecPro Room70G2 RoomPanorama/ Room70Panorama]*

Connector 2: Off, Connector 3: Off/On *[Room55]*

Off: Disable support for HDCP protected content on this video input connector.

On: Enable support for HDCP protected content this video input connector.

n: Unique ID that identifies the video input connector.

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 1..5 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 2..3 *[Room55]*

Video Input Connector [n] InputSourceType

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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

If the device has an integrated camera, Connector 1 refers to the integrated camera.

Default value:

Connector 1,2,6: camera Connector 3,4,5: PC *[CodecPro Room70G2 RoomPanorama/ Room70Panorama]*

Connector 1: camera Other connectors: PC *[CodecPlus Room55 Room70/Room55D DeskPro/ DeskLE WebexDesk]*

Connector 1: camera Connector 2: PC *[RoomKit RoomKitMini Boards]*

Value space:

PC/camera/document_camera/mediaplayer/whiteboard/other *[CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: camera Connector 2: PC/camera/document_camera/mediaplayer/ whiteboard/other *[RoomKit RoomKitMini Boards]*

Connector 1: camera Other connectors: PC/camera/document_camera/mediaplayer/ whiteboard/other *[Room55 DeskPro/DeskLE WebexDesk]*

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.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] Name

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define a name for the video input connector.

Default value:

Connector 1: "Camera 1" Connector 2: "Camera 2" Connector 3: "PC 1 (HDMI)" Connector 4: "PC 2 (HDMI)" Connector 5: "PC 3 (HDMI)" Connector 6: "Camera 3 (SDI)" *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: "Camera" Connector 2: "PC 1 (HDMI)" Connector 3: "PC 2 (HDMI)" *[CodecPlus Room70/Room55D]*

Connector 1: "Camera" Connector 2: "PC 1 (HDMI)" Connector 3: "PC 2 (HDMI)" *[Room55]*

Connector 1: "Camera" Connector 2: "PC" *[RoomKit RoomKitMini Boards]*

Connector 1: "Camera" Connector 2: "PC (USB-C)" Connector 3: "PC (HDMI)" *[DeskPro/DeskLE WebexDesk]*

Value space:

String (0, 50)

Name for the video input connector.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] OptimalDefinition Profile

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Use the Video Input Connector [n] OptimalDefinition Threshold60fps setting to set the lowest resolution where 60 fps is allowed. Below this threshold, 30 fps is the maximum frame rate.

Default value:

Medium *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama WebexDesk Boards]*

Connector 1: Medium Connector 2, 3: High *[DeskPro/DeskLE]*

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.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] OptimalDefinition Threshold60fps

Applies to: All products

Requires user role: ADMIN

For each video input, this setting tells the device the lowest resolution where it can transmit 60 fps. For all resolutions lower than this value, the maximum transmitted frame rate would be 30 fps. Above this resolution 60fps is possible, if the available bandwidth is adequate.

Default value:

1920_1080 *[RoomKitMini CodecPlus CodecPro Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Never *[RoomKit Room55]*

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.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Video Input Connector [n] PreferredResolution

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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 larger formats than 1920_1080_60 use much more data, and requires a presentation cable (or adapter) that is qualified for at least HDMI 1.4b data rates.

Default value:

1920_1080_60 *[CodecPro Room70G2 RoomPanorama/Room70Panorama WebexDesk]*

For Desk Pro: 3840_2160_60

For Desk Limited Edition: 1920_1080_60 *[DeskPro/DeskLE]*

1920_1080_60 *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D Boards]*

Value space:

Connector 1,2: 1920_1080_60 Connector 3,4,5: 1920_1080_60/2560_1440_60/3840_2160_30 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: 1920_1080_60 Connector 2,3 : 1920_1080_60/2560_1440_60/3840_2160_30 *[CodecPlus Room70/Room55D]*

1920_1080_60/2560_1440_60/3840_2160_30 *[RoomKit RoomKitMini Room55 Boards]*

For Desk Pro: 1920_1080_60/2560_1440_60/3840_2160_30/3840_2160_60

For Desk Limited: 1920_1080_60 *[DeskPro/DeskLE]*

1920_1080_60 *[WebexDesk]*

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.

3840_2160_60: The resolution is 3840 x 2160, and the refresh rate is 60 Hz.

n: Unique ID that identifies the video input connector.

Range: 1..5 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 2..3 *[Room55 DeskPro/DeskLE WebexDesk]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] PresentationSelection

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

For devices with more than one camera: Any input source can be used as a presentation source; normally, the main camera will not be used as a presentation source.

For devices with an integrated camera: The integrated camera is not available as a presentation source.

Default value:

Connector 1,2,6: Manual Connector 3,4,5: OnConnect *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: Manual Other connectors: OnConnect *[CodecPlus Room70/Room55D]*

Desktop *[DeskPro/DeskLE WebexDesk]*

OnConnect *[RoomKit RoomKitMini Room55]*

AutoShare *[Boards]*

Value space:

AutoShare/Desktop/Manual/OnConnect *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

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.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..2 *[RoomKit RoomKitMini Boards]*

Range: 2..3 *[Room55 DeskPro/DeskLE WebexDesk]*

Video Input Connector [n] Quality

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

When encoding and transmitting video there is a trade-off between high resolution and high frame rate. For some video sources it is more important to transmit high frame rate than high resolution and vice versa. This setting specifies whether to give priority to high frame rate or to high resolution.

If a Quad Camera, SpeakerTrack 60 camera, or Precision 60 camera is detected by the device this setting is automatically set to Motion. If a user changes this setting manually, it will be set back to Motion after a restart or a camera reconnect.

Default value:

Connector 1,2,6: Motion Connector 3,4,5: Sharpness *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: Motion Connector 2,3: Sharpness *[CodecPlus Room70/Room55D]*

Sharpness *[RoomKit RoomKitMini Room55 DeskPro/DeskLE WebexDesk Boards]*

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 motion in the picture.

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

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..2 *[RoomKit RoomKitMini Boards]*

Range: 2..3 *[Room55 DeskPro/DeskLE WebexDesk]*

Video Input Connector [n] RGBQuantizationRange

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

The devices connected to the video input should follow the rules for RGB video quantization range defined in CTA-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.

Default value:

Auto *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk Boards]*

Value space:

Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on video format according to CTA-861-F. 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 CTA-861-F.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CTA-861-F.

n: Unique ID that identifies the video input connector.

Range: 1..5 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 2..3 *[Room55 DeskPro/DeskLE WebexDesk]*

Range: 1..3 *[CodecPlus Room70/Room55D]*

Range: 2..2 *[RoomKit RoomKitMini Boards]*

Video Input Connector [n] Visibility

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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

For devices with an integrated camera: Connector 1 is the device's integrated camera and is not available as a presentation source.

Default value:

Connector 1: Never Other connectors: IfSignal *[CodecPro Room70G2 DeskPro/DeskLE WebexDesk]*

Connector 1: Never Connector 2: Never Other connectors: IFSignal *[RoomPanorama/Room70Panorama]*

Connector 1: Never Other connectors: Always *[CodecPlus Room55 Room70/Room55D]*

Connector 1: Never Connector 2: Always *[RoomKit RoomKitMini]*

Connector 1: Never Connector 2: IfSignal *[Boards]*

Value space:

Always/IfSignal/Never *[CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama]*

Connector 1: Never Connector 2: Always/IfSignal/Never *[RoomKit RoomKitMini Boards]*

Connector 1: Never Other connectors: Always/IfSignal/Never *[DeskPro/DeskLE WebexDesk]*

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: Yhe 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.

n: Unique ID that identifies the video input connector.

Range: 1..6 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Range: 1..2 *[RoomKit RoomKitMini Boards]*

Video Monitors

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, INTEGRATOR

A monitor role is assigned to each screen using the Video Output Connector [n] MonitorRole setting. The monitor role decides which layout (call participants and presentation) will appear on the screen that is connected to this output. Screens with the same monitor role will get the same layout; screens with different monitor roles will have different layouts.

The monitor layout mode that is set in the Video Monitors setting should reflect the number of different layouts you want in your room setup. Note that some screens can be reserved for presentations.

Default value:

Auto *[RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE WebexDesk]*

Value space:

Auto/Single/Dual/DualPresentationOnly *[RoomKit CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

Auto/Single/Dual/DualPresentationOnly/TriplePresentationOnly/Triple *[CodecPro Room70G2]*

Auto/TriplePresentationOnly *[RoomPanorama/Room70Panorama]*

Auto: The number of screens connected to the device is automatically detected, and the layout is distributed on the screens according to the monitor role.

Single: The layout is shown on the device's screen. If the device has more than one screen, the same layout is shown on all screens.

Dual: The layout is distributed on screens with monitor role First and Second. If a presentation is part of the layout, all participants in the call are shown on screens with monitor role First, and the presentation is shown on screens with monitor role Second.

DualPresentationOnly: All participants in the call are shown on screens with monitor role First. If a presentation is part of the layout, the presentation is shown on screens with monitor role Second.

Triple: The layout is distributed on screens with monitor role First, Second and Third. Screens with monitor role Second are used first, then First, and finally Third. If a presentation is part of the layout, all participants in the call are shown on screens with monitor role First and Second, and the presentation is shown on the screen with monitor role Third.

TriplePresentationOnly: All participants in the call are distributed on screens with monitor role First and Second. Screens with monitor role Second are used first, then First. If a presentation is part of the layout, the presentation is shown on the screen with monitor role Third.

Video Output Connector [n] Brightness

Applies to: Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, USER

Define the brightness level for the device's integrated screen.

Default value:

80

Value space:

Integer (0..100)

Range: The value must be between 0 and 100.

n: Unique ID that identifies the video output connector.

Range: 1..1

Video Output Connector [n] BrightnessMode

Applies to: DeskPro/DeskLE

Requires user role: ADMIN, USER

Configure to allow for automatic or manual control of the brightness level on the main display.

Default value:

Auto

Value space:

Auto/Manual

Auto: Allow for the brightness level of the display to be set automatically by the device.

Manual: Allow for the brightness level of the display to be set manually by the user.

n: Unique ID that identifies the video output connector.

Range: 1..1

Video Output Connector [n] CEC Mode

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

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).

Default value:

On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 DeskPro/DeskLE]*

Off *[Room70/Room55D Room70G2]*

Room Panorama: On ; Room 70 Panorama: Connector 1: Off, Connector 2: Off, Connector 3: On *[RoomPanorama/Room70Panorama]*

Value space:

Off/On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE]*

Room Panorama: On;

Room 70 Panorama: Off/On *[RoomPanorama/Room70Panorama]*

Off: CEC is disabled.

On: CEC is enabled.

n: Unique ID that identifies the video output connector.

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..1 *[RoomKitMini]*

Range: 2..2 *[Room55 DeskPro/DeskLE]*

Range: 2..2 for Room 70 Single; not available for Room 70 Dual *[Room70/Room55D]*

Range: 1..2 *[RoomKit CodecPlus]*

Video Output Connector [n] Location HorizontalOffset

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = "0" and VerticalOffset = "0" indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

For Room 55, Desk Pro and Desk Limited Edition, the integrated screen (Connector 1) has HorizontalOffset = "0" and VerticalOffset = "0" (implicit, not configurable).

Example: You have two screens side by side. The left screen is on Connector 1 and the right screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "1", VerticalOffset = "0"

Example: You have two screens, one below the other. The upper screen is on Connector 1 and the lower screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "0", VerticalOffset = "-1"

Default value:

Connector 1: "-1" Connector 2: "0" Connector 3: "1" *[CodecPro Room70G2]*

Connector 1: "0" Connector 2: "1" Connector 3: "0.5" *[RoomPanorama/Room70Panorama]*

Connector 1: "0" Connector 2: "1" *[RoomKit CodecPlus Room70/Room55D]*

Connector 2: "1" *[Room55 DeskPro/DeskLE]*

Value space:

String (1, 12)

The string represents a decimal number between -100.0 and 100.0 (these numbers included). Input strings that complies with the std::stof function in the C++ <string> library are accepted. This means that you can use either decimal notation or E-notation, for example "12", "12.0", "1.2e1", "1.2E1", "-0.12", "-12e-2". Leading whitespace characters are discarded, and the decimal point is "."

n: Unique ID that identifies the video output connector.

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..2 *[RoomKit CodecPlus Room70/Room55D]*

Range: 2..2 *[Room55 DeskPro/DeskLE]*

Video Output Connector [n] Location VerticalOffset

Applies to: RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = "0" and VerticalOffset = "0" indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

For Room 55, Desk Pro, and Desk Limited Edition, the integrated screen (Connector 1) has HorizontalOffset = "0" and VerticalOffset = "0" (implicit, not configurable).

Example: You have two screens side by side. The left screen is on Connector 1 and the right screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "1", VerticalOffset = "0"

Example: You have two screens with one below the other. The upper screen is on Connector 1 and the lower screen on Connector 2. Then the following settings will apply:

Video Output Connector 1 Location: HorizontalOffset = "0", VerticalOffset = "0"

Video Output Connector 2 Location: HorizontalOffset = "0", VerticalOffset = "-1"

Default value:

Connector n: "0" *[RoomKit CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE]*

Connector 1, 2: "0" Connector 3: "-1" *[RoomPanorama/Room70Panorama]*

Value space:

String (1, 12)

The string represents a decimal number between -100.0 and 100.0 (these numbers included). Input strings that complies with the std::stof function in the C++ <string> library are accepted. This means that you can use either decimal notation or E-notation, for example "12", "12.0", "1.2e1", "1.2E1", "-0.12", "-12e-2". Leading whitespace characters are discarded, and the decimal point is ".".

n: Unique ID that identifies the video output connector.

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 1..2 *[RoomKit CodecPlus Room70/Room55D]*

Range: 2..2 *[Room55 DeskPro/DeskLE]*

Video Output Connector [n] MonitorRole

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

The monitor role describes which video streams will be shown on the screen connected to this video output. Together the Video Monitors setting and the MonitorRole settings for all outputs define which layout (video streams) will be shown on each screen.

This setting is not applicable for Room Kit Mini, since it supports only one screen.

Default value:

Auto *[RoomKit CodecPlus CodecPro Room55 Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE]*

Dual: Connector 1,2: Auto; Single: Connector 1: Auto Connector 2: PresentationOnly *[Room70/Room55D]*

Value space:

Auto/First/Second/PresentationOnly *[RoomKit CodecPlus Room55 Room70/Room55D DeskPro/DeskLE]*

Auto/First/Second/Third/PresentationOnly/Recorder *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Auto: The device will detect when a screen is connected, and a monitor role (First, Second, Third) that corresponds with the Video Monitors setting will be assigned automatically.

First/Second/Third: Define the role of the screen in a multi-screen setup. In a single-screen setup, there is no difference between First, Second and Third.

PresentationOnly: Show presentation video stream if active, and nothing else. Screens/outputs with this monitor role are ignored by the Video Monitors setting.

Recorder: Show all participants, including the local main video (self-view). If active, also show the presentation. Screens/outputs with this monitor role are ignored by the Video Monitors setting.

n: Unique ID that identifies the video output connector.

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 2..2 *[Room55 DeskPro/DeskLE]*

Range: 1..2 *[RoomKit CodecPlus Room70/Room55D]*

Range: 1..1 *[RoomKitMini]*

Video Output Connector [n] Resolution

Applies to: All products

Requires user role: ADMIN, INTEGRATOR, USER

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.

Default value:

3840_2160_60 *[DeskPro/DeskLE Boards]*

1920_1080_60 *[WebexDesk]*

Connector 1: 3840_2160_60 Connector 2: Auto *[Room55]*

Auto *[RoomKit RoomKitMini CodecPlus CodecPro Room70/Room55D Room70G2]*

Connector 1, 2: Auto; Connector 3: 3840_2160_30 *[RoomPanorama/Room70Panorama]*

Value space:

Connector 1,2: Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60 Connector 3: Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30 *[CodecPro Room70G2]*

Connector 1,2: Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60 Connector 3: 3840_2160_30 *[RoomPanorama/Room70Panorama]*

3840_2160_60 *[Boards]*

Connector 1: 3840_2160_60 Connector 2: Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60 *[Room55 DeskPro/DeskLE]*

1920_1080_50 *[WebexDesk]*

Auto/1920_1080_50/1920_1080_60/1920_1200_50/1920_1200_60/2560_1440_60/3840_2160_30/3840_2160_60 *[RoomKit RoomKitMini CodecPlus Room70/Room55D]*

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

1280_720_50: The resolution is 1280 x 720, and the refresh rate is 50 Hz.

1280_720_60: The resolution is 1280 x 720, and the refresh rate is 60 Hz.

1920_1080_50: The resolution is 1920 x 1080, and the refresh rate is 50 Hz.

1920_1080_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

1920_1200_50: The resolution is 1920 x 1200, and the refresh rate is 50 Hz.

1920_1200_60: The resolution is 1920 x 1200, and the refresh rate is 60 Hz.

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.

n: Unique ID that identifies the video output connector.

Range: 1..1 *[RoomKitMini WebexDesk Boards]*

Range: 1..2 *[RoomKit CodecPlus Room55 Room70/Room55D DeskPro/DeskLE]*

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Video Output Connector [n] RGBQuantizationRange

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE

Requires user role: ADMIN, INTEGRATOR

Displays connected to an HDMI output should follow the rules for RGB video quantization range defined in CTA-861. Unfortunately some displays 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 expect full quantization range.

Default value:

Full *[RoomKit RoomKitMini CodecPro Room55 Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE]*

Connector 1: Auto, Connector 2: Full *[CodecPlus Room70/Room55D]*

Value space:

Auto/Full/Limited

Auto: If the display signals support for "Selectable RGB Quantization Range" in the EDID, then the AVI InfoFrame will signal Full Range in the RGB Quantization Range bits (Q0, Q1). Otherwise Limited Range will be signaled in the AVI InfoFrame for CE video formats and Full Range for IT video formats.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CTA-861-F.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CTA-861-F.

n: Unique ID that identifies the video output connector.

Range: 1..1 *[RoomKitMini]*

Range: 1..2 *[RoomKit CodecPlus Room70/Room55D]*

Range: 1..3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

Range: 2..2 *[Room55 DeskPro/DeskLE]*

Video Output Webcam USBMode

Applies to: RoomKitMini WebexDesk

Requires user role: ADMIN, INTEGRATOR

Specify whether to enter USB mode (i.e., do-not-disturb) when you connect video or when you start streaming video.

Default value:

OnStreaming

Value space:

OnConnect/OnStreaming

OnConnect: Go into USB mode when you connect video.

OnStreaming: Go into USB mode when you start streaming video.

Video Output Connector [n] Whitebalance Level

Applies to: Room55 DeskPro/DeskLE WebexDesk

Requires user role: ADMIN, USER

The integrated screen's color temperature (white balance) is adjustable from 4000 K (warm) to 9000 K (cool).

Default value:

6500

Value space:

Integer (4000..9000)

The color temperature in Kelvin.

n: Unique ID that identifies the video output connector.

Range: 1..1

Video Presentation DefaultPIPPosition

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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

Applies to: All products

Requires user role: ADMIN, USER

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.

Default value:

3 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

2 *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk Boards]*

Value space:

1/2/3/4/5 *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

1/2/3 *[CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk]*

1/2 *[RoomKit RoomKitMini Boards]*

The video input source to use as default presentation source.

Video Presentation Priority

Applies to: All products

Requires user role: ADMIN

Specify how to distribute the bandwidth between the presentation channel and the main video channel.

Default value:

Equal

Value space:

Equal/High/Low *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk Boards]*

Equal *[RoomPanorama/Room70Panorama]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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).

For Webex Desk, Desk Pro, and Desk Limited Edition, if you use the user interface to turn full screen self-view off, it will come back as a PiP if you use the user interface to turn it on again.

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Define if the main video source (self-view) shall be displayed on screen after a call, and also after video has been turned off and on again during 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.

Default value:

Current

Value space:

Off/Current/On

Off: Self-view is switched off when leaving a call, and also after video is turned on during 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. Similar after turning on video during a call.

On: Self-view is switched on when leaving a call, and also after video is turned on during a call.

Video Selfview Default OnMonitorRole

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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).

Default value:

Current

Value space:

Current/First/Second *[RoomKit RoomKitMini CodecPlus Room55 Room70/Room55D DeskPro/DeskLE WebexDesk Boards]*

Current/First/Second/Third *[CodecPro Room70G2 RoomPanorama/Room70Panorama]*

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 monitor role First.

Second: The self-view picture will be shown on outputs with monitor role Second.

Third: The self-view picture will be shown on outputs with monitor role Third.

Video Selfview Default PIPPosition

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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).

Default value:

Current *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 DeskPro/DeskLE WebexDesk]*

LowerRight *[RoomPanorama/Room70Panorama]*

Current *[Boards]*

Value space:

Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the self-view PiP will be kept unchanged when leaving a call.

UpperLeft: The self-view PiP will appear in the upper left corner of the screen.

UpperCenter: The self-view PiP will appear in the upper center position.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear in the center left position.

CentreRight: The self-view PiP will appear in the center right position.

LowerLeft: The self-view PiP will appear in the lower left corner of the screen.

LowerRight: The self-view PiP will appear in the lower right corner of the screen.

Video Selfview OnCall Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

Default value:

On *[RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE]*

Off *[WebexDesk Boards]*

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

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

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.

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.

VoiceControl settings

VoiceControl Wakeword Mode

Applies to: All products

Requires user role: ADMIN, INTEGRATOR

Use this setting to enable or disable the wakeword (e.g., "Ok Webex") that is used by the Webex Assistant. The Webex Assistant allows you to use the device hands free, and by using the wakeword you can initiate tasks, such as placing a call and starting a presentation.

Use the UserInterface Assistant Mode setting to switch on the Webex Assistant.

Default value:

On

Value space:

Off/On

Off: Disable the use of a wakeword.

On: Enable the use of a wakeword.

WebEngine settings

WebEngine Features LocalWebAppManagement

Applies to: DeskPro/DeskLE WebexDesk Boards

Requires user role: ADMIN

Decides whether to show a list of installed web apps in the Settings menu on the user interface of the device, and whether the user can manage the web apps (add, edit, or delete) from this menu.

Only web apps that are set up directly on the device, from the device's local web interface, or by using the API can be managed from the Settings menu (locally managed); web apps that are set up from Control Hub (externally managed) are shown in the list, but the user can never manage them.

Default value:

Off

Value space:

Allowed/NotAllowed/Off

Allowed: A user can add, edit, and delete locally managed web apps from the Settings menu on the user interface of the device.

NotAllowed: The list of installed web apps is shown in the Settings menu, but the user cannot manage them.

Off: There is no entry for listing or managing web apps in the Settings menu.

WebEngine Features WebGL

Applies to: All products

Requires user role: ADMIN

WebGL (Web Graphics Library) is a Javascript API for rendering interactive 2D and 3D graphics within the web browser without using plug-ins.

WebGL is an experimental feature and might change in the future.

Default value:

Off

Value space:

Off/On

On: WebGL is enabled.

Off: WebGL is disabled.

WebEngine Features SipUrlHandler

Applies to: RoomKit DeskPro/DeskLE Boards

Requires user role: ADMIN

This configuration allows you to start SIP calls directly from web view based features (e.g., web app, digital signage). The user selects a button labeled with SIP:yourSipUrl to initiate a call, and the call is then placed by the device.

Default value:

Off

Value space:

Off/On

Off: Starting SIP calls from a web view is disabled.

On: Starting SIP calls from a web view is enabled.

WebEngine MinimumTLSVersion

Applies to: All products

Requires user role: ADMIN

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

Default value:

TLSv1.1

Value space:

TLSv1.0/TLSv1.1/TLSv1.2

TLSv1.0: Support of TLS version 1.0 or higher.

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

WebEngine Mode

Applies to: All products

Requires user role: ADMIN

The web engine is a prerequisite for features that use the device's web view, for example digital signage and web apps.

Default value:

Off

Value space:

Off/On

Off: The web engine is disabled.

On: The web engine is enabled.

WebEngine RemoteDebugging

Applies to: All products

Requires user role: ADMIN

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.

Default value:

Off

Value space:

Off/On

Off: Remote debugging is switched off.

On: Remote debugging is switched on.

WebEngine UseHttpProxy

Applies to: All products

Requires user role: ADMIN

There are several UseHttpProxy settings that specify if a service shall communicate via an HTTP proxy or not. The WebEngine UseHttpProxy setting applies all web view based features, such as digital signage, API-driven web views, and web apps.

For this setting to have any effect, a proxy server for HTTP, HTTPS, and WebSocket traffic must be set up using the NetworkServices HTTP Proxy settings.

Default value:

On

Value space:

Off/On

Off: Set up communication directly with the server (not using a proxy).

On: Set up communication via proxy.

Webex settings

Webex CloudProximity GuestShare

Applies to: All products

Requires user role: ADMIN

This setting allows you to turn off the guest share feature via devices.webex.com.

Default value:

Auto

Value space:

Auto/Off

Auto: Allow the system to automatically determine whether or not to allow guest sharing. This is enabled by default currently.

Off: Turn off the guest share feature.

Webex CloudProximity Mode

Applies to: All products

Requires user role: ADMIN

Devices registered to an on-premises call manager and linked to Webex Edge for Devices support both on-premises and cloud proximity mode for handling pairing mechanisms like ultrasound, Wi-Fi discovery, and guest sharing. This setting allows you to define which of the two proximity modes to use.

Default value:

Off

Value space:

Off/On

Off: The linked device uses on-premises proximity mode.

On: The linked device uses cloud proximity mode.

Webex CloudUpgrades Mode

Applies to: All products

Requires user role: ADMIN

On devices that are registered to an on-premises service and linked to Webex Edge for Devices, you can choose whether to upgrade the software from the on-premises provisioning service or from the Webex cloud service (cloud-managed software upgrade).

With cloud-managed software upgrade the device is upgraded automatically when a new RoomOS software version is available, that is at the same time as cloud registered devices are upgraded. You get the latest updates and bug fixes faster without having to upgrade the device manually.

Default value:

Off

Value space:

Off/On

Off: The device software is not upgraded from the cloud. You must use an on-premises provisioning service, such as CUCM, or rely on manual upgrades.

On: The device software is automatically upgraded when a new software version is available in the cloud.

Webex Meetings JoinProtocol

Applies to: All products

Requires user role: ADMIN

Devices that are registered to an on-premises service and linked to Webex Edge for Devices may use the Webex cloud service for calling into Webex meetings. Calling via Webex gives you the full set of native Webex Meetings in-call features, such as advanced mute, cohost, transfer host, and face recognition, to name a few.

These are the cases when Webex Meetings call routing may be used: When using the Join Webex button, when using the Webex Assistant to join a Personal Room meeting (PMR), and when using the Call button or the Dial API command with a URI with one of the following domains: @webex.com, @*.webex.com, and @meet.ciscospark.com. Other calls will use to the default protocol.

Also, native Webex Meetings call routing requires that the device is enabled for cloud-managed software upgrade, configuration from Control Hub is enabled, and the Conference Multipoint Mode is set to Auto.

Room Panorama and Room 70 Panorama are not supported in CE 9.15.0.

Default value:

SIP

Value space:

SIP/Webex

SIP: The call protocol is SIP.

Webex: The call protocol is Webex, provided that the requirements above are met. Otherwise, it is SIP.

WebRTC settings

WebRTC EndCallTimeout

Applies to: RoomKit RoomKitMini CodecPlus CodecPro Room55 Room70/Room55D Room70G2 RoomPanorama/Room70Panorama DeskPro/DeskLE Boards

Requires user role: ADMIN

You can extend the period between pressing End call in a WebRTC meeting and the closing of the web view.

In normal operation, you do not need to change this setting, but it can be useful for troubleshooting.

WebRTC is only available for devices that are registered to an on-premises service and linked to Webex Edge for Devices,

and for devices that are registered to the Webex cloud service.

Default value:

2

Value space:

Integer (0..600)

The period in seconds.

WebRTC InteractionMode

Applies to: RoomKitMini DeskPro/DeskLE Boards

Requires user role: ADMIN

When in a WebRTC meeting, you can use the device's call controls or the WebRTC app's native controls.

WebRTC is only available for devices that are registered to an on-premises service and linked to Webex Edge for Devices,

and for devices that are registered to the Webex cloud service.

Default value:

NonInteractive

Value space:

Interactive/NonInteractive

Interactive: You can use the WebRTC app's native controls directly from the device's touch screen. This will give you access to the native WebRTC features.

NonInteractive: The WebRTC app's native controls are not available; you can only use the normal call controls of the device.

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.

Chapter 6

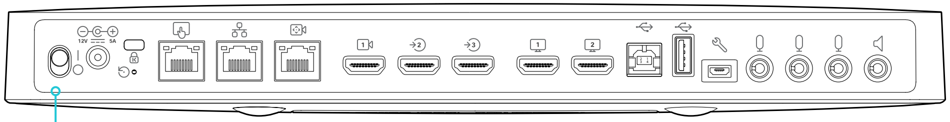
Physical interfaces

Power On/Off (page 1 of 8)

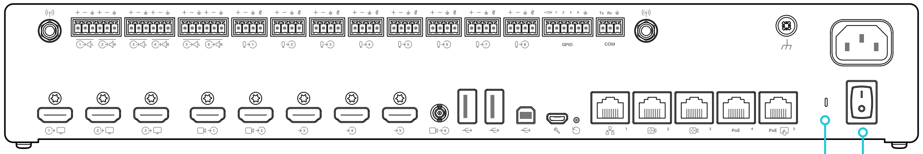
Codec Plus, Codec Pro

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

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



Power switch on the Codec Plus[*]. The LED is on top of the device.



The codec has two identical status LEDs: one at the back, and one on the front of the device.

Power switch on the Codec Pro[*].

LED behavior

In idle mode (screens are awake):

Steady light.

In standby mode (screens are off):

Steady light.

The device needs attention (e.g. missed call or no network connection):

The LED repeatedly flashes twice.

During startup (boot):

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

---

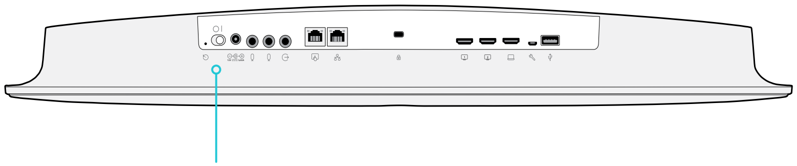
[*] Configuration changes might be lost if you shut down the device using the power switch just a few seconds after saving the changes.

Power On/Off (page 2 of 8)

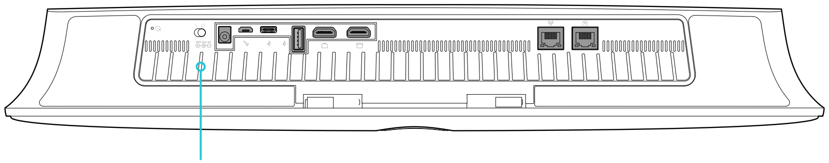
Room Kit, Room Kit Mini

The main On/Off switch is located on the back of the Room Kit/Room Kit Mini. Switch it to the On position. It may take a few minutes to start up. The system LED lights steadily when the device is ready for use.

Keep in mind that once the device is mounted on top of a screen, the power switch may be difficult to access.



Power switch on the Room Kit*. The LEDs are on the front of the device.



Power switch on the Room Kit Mini*. The LEDs are on the front of the device.

LED behavior

System LED

In idle mode (screens are awake):

Steady light.

In standby mode (screens are off):

Steady light.

The device needs attention (e.g. missed call or 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:

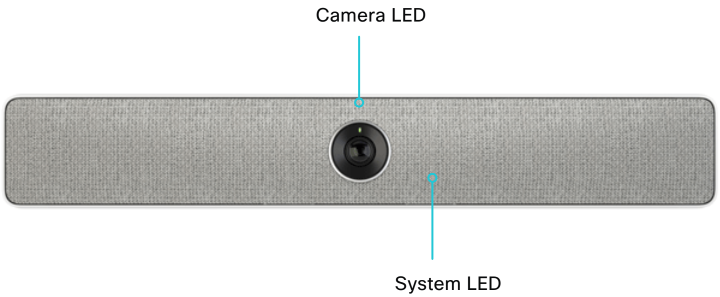
The LED flashes.

In call:

Steady light.

Selfview on:

Steady light.



---

[*] Configuration changes might be lost if you shut down the device using the power switch just a few seconds after saving the changes.

Power On/Off (page 3 of 8)

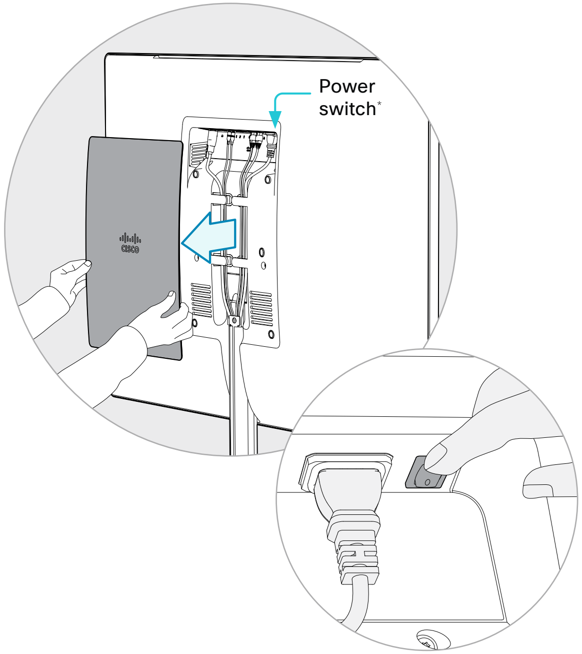
Room 55

When Room 55 is mounted to a wall, you cannot access the power switch. Ensure that Room 55 is mounted with the power switch in the *On* position so that once it's plugged in, it will automatically power-on.

Before unplugging the device, shut it down via the web interface: *Maintenance > Restart > Shutdown device.*

You may experience problems if you unplug the device before shutting it down properly. If this happens, try restarting the video system using the web interface to restore normal behaviour.

On a floor stand or wheel base mounted Room 55, remove the cover on the back to get access to the connectors.The power switch is next to the power connecter.



LED behavior

System LED

The system LED is to the right of the camera. The normal LED color is white. A red light indicates hardware failure.

In idle mode (screens are awake):

LED is off.

In standby mode (screens are off):

Steady light.

The device needs attention
(e.g. missed call or 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

The camera LED is just above the camera lens.

Incoming call:

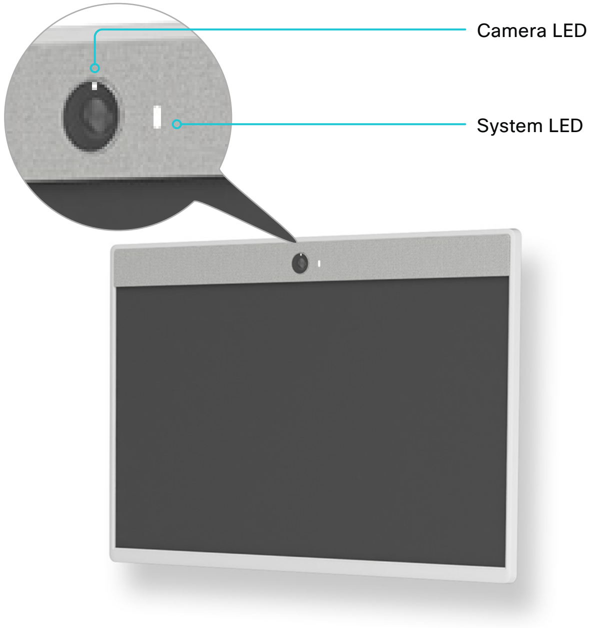
The LED flashes.

In call:

Steady light.

Selfview on:

Steady light.



---

[*] Configuration changes might be lost if you shut down the device using the power switch or by unplugging it just a few seconds after saving the changes.

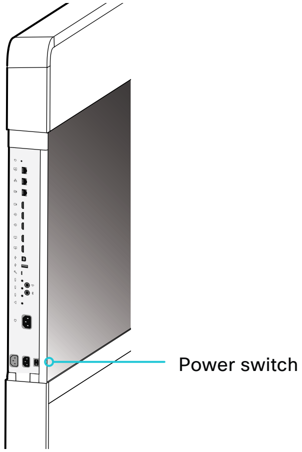
Power On/Off (page 4 of 8)

Room 70 Single/Dual G2, Room 70 Single/Dual, Room 55 Dual, Room 70 Panorama

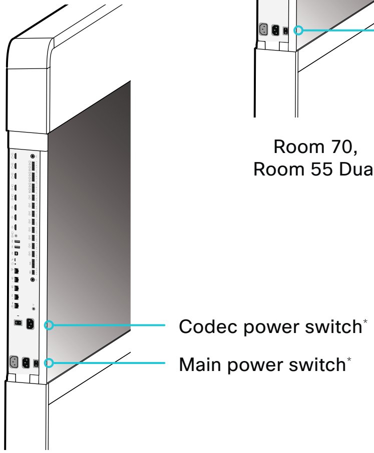
The power switch is behind the left side cover, in the same place for all mounting options.

To access the switch, remove the left side cover. It snaps in/out of place with magnets. The power switch is next to the main power connector below the codec.

(Room 70 G2 Single/Dual, Room 70 Panorama) Also make sure that the codec power switch is on.



Room 70,
Room 55 Dual



Room 70 G2,
Room 70 Panorama

LED behavior

System LED

The system LED is behind the fabric to the right of the camera. The normal LED color is white. A red light indicates hardware failure.

In idle mode (screens are awake):

LED is off.

In standby mode (screens are off):

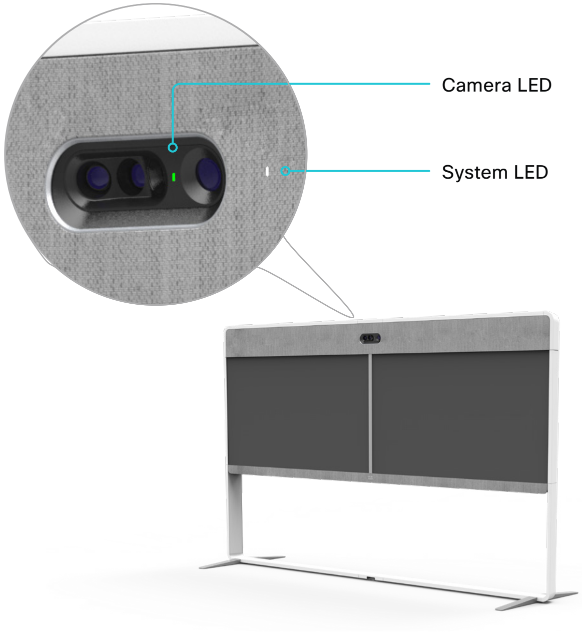
Steady light.

The device needs attention (e.g. missed call or 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

The camera LED is just above the camera lenses.

Incoming call:

The LED flashes.

In call:

Steady light.

Selfview on:

Steady light.

---

[*] Configuration changes might be lost if you shut down the device using the power switch just a few seconds after saving the changes.

Power On/Off (page 5 of 8)

Room Panorama (page 1 of 2)

Multiple components connected to wall sockets

Room Panorama consists of many components. Each component has a power cord that is connected directly to a wall socket.*

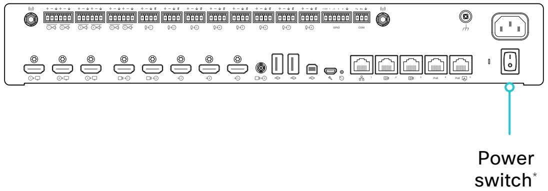
There are socket outlets on both sides of the system. Use the handles at the bottom of the deco grilles, and pull down the left and right screens to get access to all the outlets.

Only a few components have a power switch. To fully turn off power for the complete system, pull out the plugs from the wall socket outlets.

The codec power switch

The codec is behind the left screen. Using the handle at the bottom of the deco grille, pull down the left screen to get access to the codec.

- The power switch is set to On as part of the installation.



The camera power switch

The camera has a power switch that is set to On as part of the installation.

You don't have easy access to this switch when the system is assembled.

The 24 V PSU power switch

This PSU is in the left cavity behind the left screen.

- Using the handle at the bottom of the deco grille, pull down the left screen to get access to the PSU.
- The power switch is set to On as part of the installation.

The screen power buttons

The screens should automatically power up when connected to power. If they don't, use the remote control or the power button to switch them on.

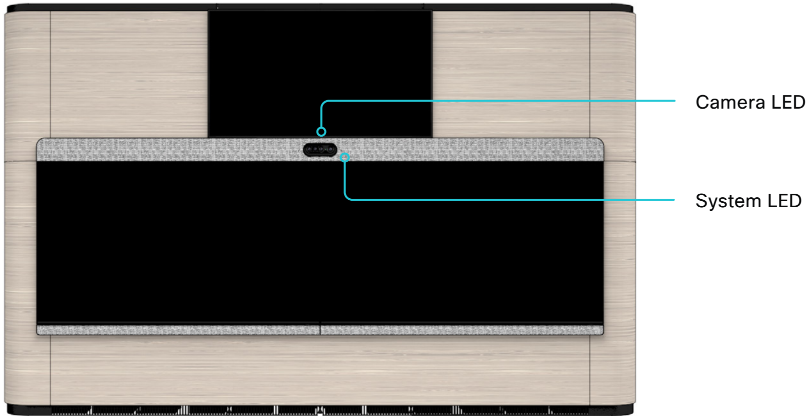
- Main screens: power button below the logo (lower right)
- Content screen: power button (lower center)

---

* Configuration changes might be lost if you shut down the device using the power switch just a few seconds after saving the changes.

Power On/Off (page 6 of 8)

Room Panorama (page 2 of 2)



Pull down the left screen to see the amplifier and codec. Both units are mounted with the connector panel facing upward.

System LED

In idle mode (screens are awake):

LED is off.

In standby mode (screens are off):

Steady light.

During startup (boot):

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

The LED goes off before the whole system (all peripherals) is ready for use.

Camera LED

Incoming call:

The LED flashes.

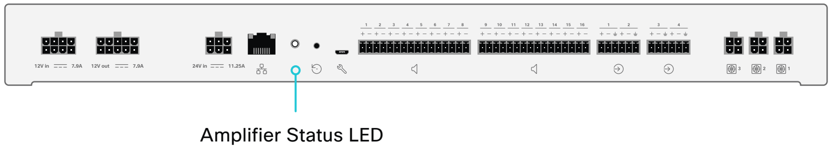
In call:

Steady light.

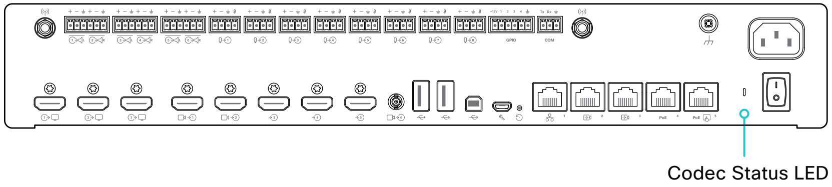
Selfview on:

Steady light.

Amplifier: Cisco Natural Audio Module IV



Codec: Cisco Webex Codec Pro



Amplifier status LED

During startup (boot):

Steady light.

The device is not connected to a codec (un-paired):

Blinking fast.

The device is connected to a codec:

Steady light.

The codec is in standby mode:

Blinking slowly.

Codec Status LED

In idle mode (screens are awake):

Steady light.

In standby mode (screens are off):

Steady light.

The device needs attention (e.g. missed call or no network connection):

The LED repeatedly flashes twice.

During startup (boot):

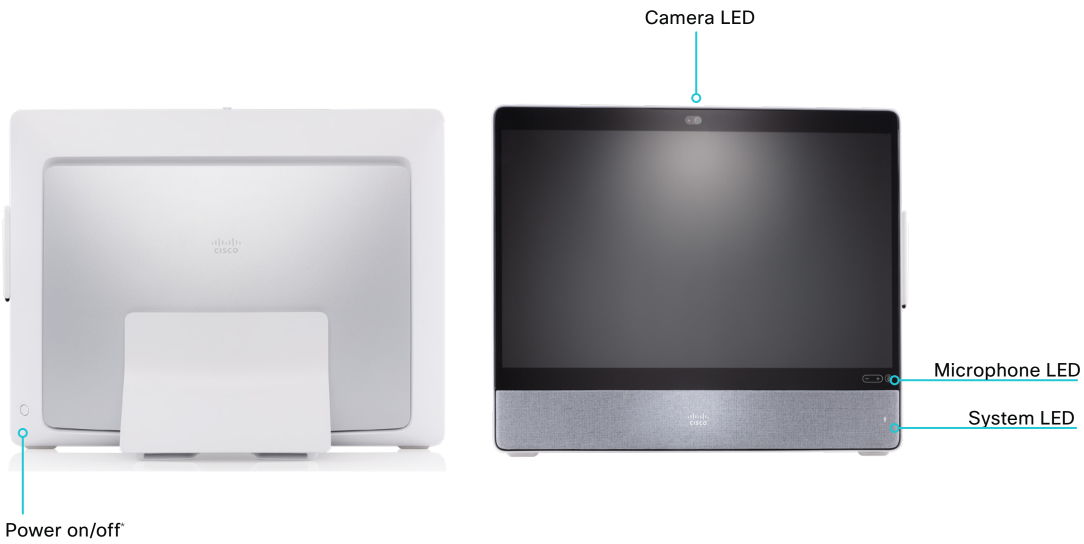
The LED flashes. It turns steady when the device is ready for use.

Power On/Off (page 7 of 8)

Webex Desk, Desk Pro, and Desk Limited Edition

The power button with LED indicator is on the back, as shown below.

To switch the device on, press the power button once. To switch it off, press the power button once. It takes at least 10 seconds before the device turns off.



LED behavior

System LED

In idle mode (screen is active):
The LED is off.

In standby mode (screen is off):
Steady light.

Missed call:
The LED is off.

No network connection:
The LED repeatedly flashes twice.

During startup (boot):
The LED flashes.

Camera LED

The camera LED is on the top of the screen, just above the camera lens.

Incoming call:
The LED flashes.

In call:
Steady light.

Selfview on:
Steady light.

During startup (boot):
The LED is lit for a short while.

Microphone LED

In call, the microphone is on:
Steady green.

In call, the microphone is off:
Steady red.

---

[*] Configuration changes might be lost if you shut down the device using the power button just a few seconds after saving the changes.

Power On/Off (page 8 of 8)

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.

Enter and exit standby mode

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

To exit standby mode, tap the touch controller.

Or, tap the screen *(Webex Desk, Desk Pro, Desk Limited Edition, and Boards)*.

Halfwake mode and clean up for the next user

Applies to: Boards

- To enter halfwake mode, press the Home button on the board and hold it for a few seconds
- To exit halfwake mode, tap the Home button, the touch controller screen, or the board itself.

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

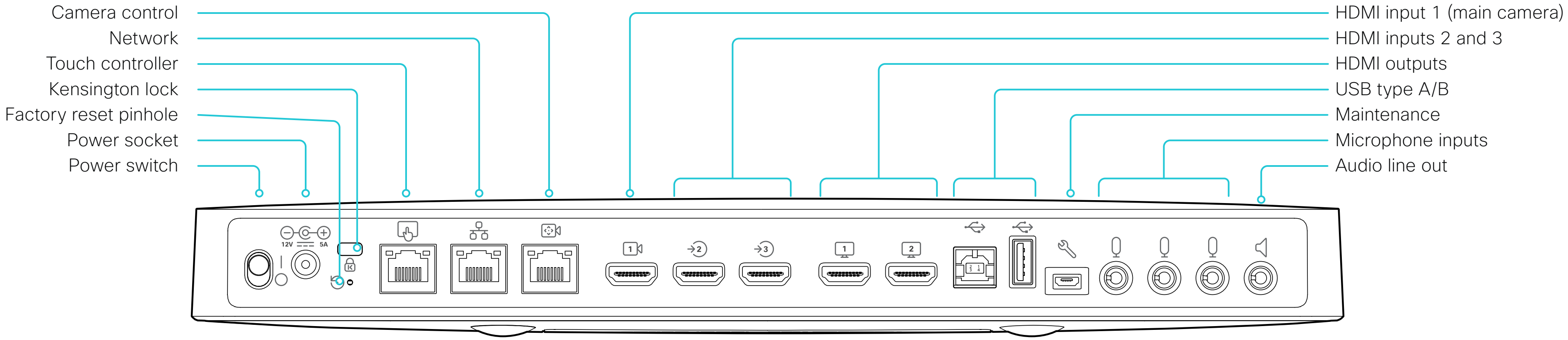
Click *Shutdown device...* and confirm your choice.

ⓘ You cannot power the device on again remotely.

To power up the device after a remote shutdown:

- Disconnect the power plug and connect it again. *(Room Kit, Room Kit Mini, and Boards)*
- Turn the power switch Off and then On. *(Codec Pro, Room 70 G2, Room 70, Room 55 Dual, Room Panorama, Room 70 Panorama, Webex Desk, Desk Pro, and Desk Limited Edition)*
- Turn the power switch Off and then On, or disconnect the power plug and plug it in again. *(Room 55)*

Connector panel: Codec Plus



Power

Always use the provided power supply:

- DC output: 5 A, 12 V
- AC input: 100-240 V, 50-60 Hz, max 1.2 A

The device powers up automatically, as long as the power switch is in its On position.

Factory reset pinhole

Use the pinhole as a last resort. We recommend to perform a factory reset from the Touch user interface or the web interface.

Kensington lock

The Kensington lock may be used to prevent the device from being moved and to prevent theft.

Touch controller

The touch controller is powered over Ethernet (PoE), which is provided through this socket.

Network

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

HDMI inputs

HDMI 1: HDMI version 1.4b, resolutions up to 1920 × 1080 at 60 fps. Most often used for the main camera. You must always use the HDMI 1 for a Quad camera.

HDMI 2 and 3: HDMI version 1.4b, resolutions up to 3840 × 2160 at 30 fps / 1920 × 1080 at 60 fps. Used for different types of input sources, like computers, cameras, or external playback devices (audio and video). You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable. The second HDMI input connector allows display of HDCP (High-bandwidth Digital Content Protection) encrypted content.

HDMI outputs

HDMI version 2.0, resolutions up to 3840 × 2160 at 60 fps. Use output 1 for the main monitor and output 2 for the optional second monitor. You need Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables.

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

Camera control

Camera control (pan, tilt, zoom) for the camera. If you connect an extra camera you need an Ethernet switch to allow for camera control on both cameras.

USB

USB 2.0 type A/B.

Maintenance

Micro USB connector for serial communication with the device.

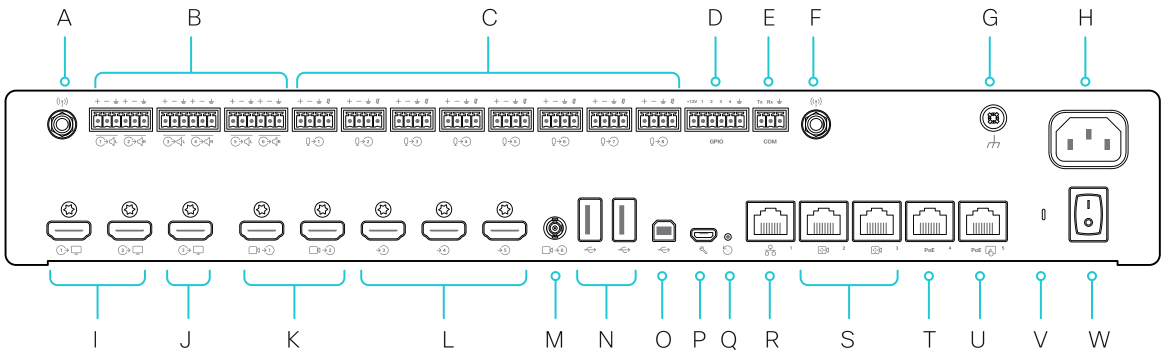
Microphones

Three 3.5 mm mini-jack, 4-pin connectors for external microphones: Cisco Table Microphone 20 or Cisco TelePresence Ceiling Microphone.

Audio line out

3.5 mm mini-jack, 3-pin connector. To be used with active loudspeakers (built-in amplifier).

Connector panel: Codec Pro and Room Panorama



A. Antenna connector (2)

2.4GHz and 5GHz antennas for use with wireless networks or Bluetooth connections.

B. Line outputs (6)

Balanced line level outputs. 3 or 6 pin Euroblock connectors.

C. Microphone/line inputs (8)

8 microphones, 48V phantom powered, each with separate echo cancellers and noise reduction; all microphones can be set for balanced line level. 4 pin Euroblock connectors.

D. Programmable GPIO port. 6 pin Euroblock connector.

E. COM port. 3 pin Euroblock connector.

F. Antenna connector, see A

G. Ground. Protective earth.

H. Main power input

Always use the provided power supply. AC input: 100-240 V, 50-60 Hz, max 1.3 – 0.6 A

I. HDMI outputs (3)

Audio and video. HDMI version 2.0, resolutions up to 3840 × 2160 at 60 fps. Use Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables. There is no audio on the HDMI outputs if the connected camera has loudspeakers (Quad Camera). Otherwise, there is audio out from this connector.

HDMI 1: Main monitor

HDMI 2 and HDMI 3: Optional second and third monitor

J. HDMI output, see I

K. HDMI inputs (5)

Audio and video. HDMI version 1.4b, resolutions up to 3840 × 2160 at 30 fps / 1920 × 1080 at 60 fps. Use a High-Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable.

HDMI 1 and HDMI 2: Use as main camera inputs. Quad camera always connects to HDMI 1.

HDMI 3 to HDMI 5: Use for different types of input sources, like computers, cameras, or external playback devices (audio and video). HDMI 5 input connector allows display of HDCP (High-bandwidth Digital Content Protection) encrypted content.

L. HDMI inputs, see K

M. 3G-SDI/HD-SDI input

Video. Resolutions up to 1920 × 1080 at 60 fps. HD-BNC: 1080p60, Level A 10-bit data native color encoding 4:2:2 YCbCr, 75 Ω.

N. USB connectors (2), 2.0 type A

O. USB connector, 2.0 type B

P. Maintenance

Micro USB connector for serial communication with device.

Q. Factory reset pinhole

Use the pinhole as a last resort. Perform a factory reset from the touch controller or the web interface.

R. Network

RJ-45: Ethernet interface, 1Gb Ethernet interface.

S. Camera control (2)

RJ-45: Camera control (pan, tilt, zoom). Connecting an extra camera requires an Ethernet switch for control on both cameras.

T. Ethernet PoE

RJ-45: Internal network port for PoE devices.

U. Touch controller

RJ-45: Dedicated PoE port for the touch controller.

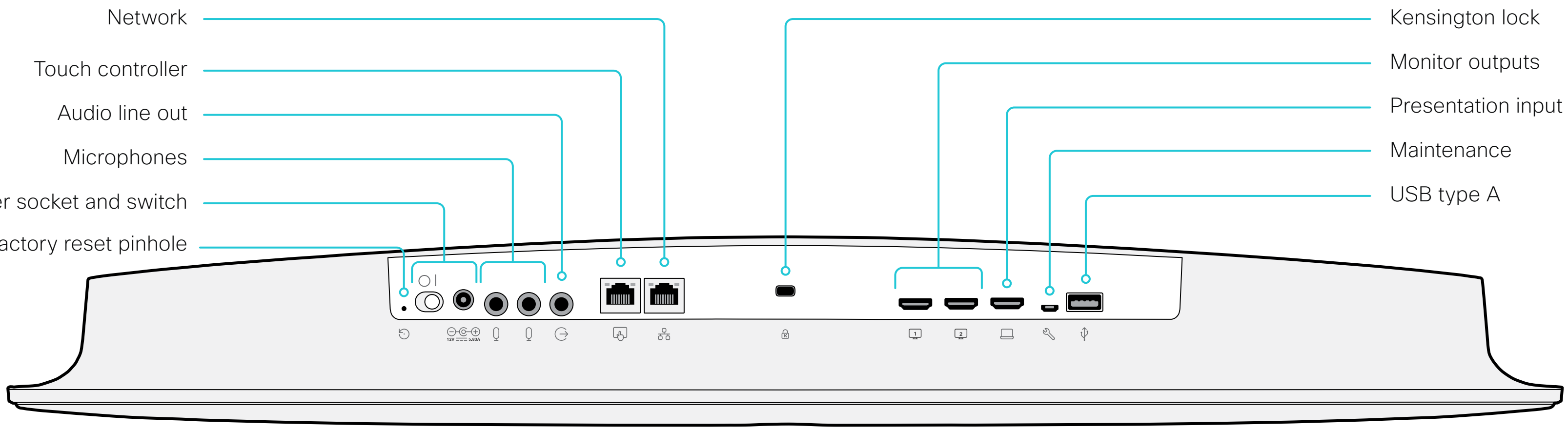
V. Status LED

Mirrors the front status LED.

W. Power On/Off

The device powers up automatically, as long as the power switch is in its On position.

Connector panel: Room Kit



Network

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

Touch controller

The touch controller is powered over Ethernet, which is not provided through this socket. Therefore, you need a mid-span power injector between the touch controller and the video conferencing device, see the ► Connect the touch controller chapter.

Audio line out

3.5 mm mini-jack, 3-pin connector. To be used with active loudspeakers (built-in amplifier) or with a self-powered subwoofer (refer to the *Audio Output Line OutputType* setting).

Microphones

Two 3.5 mm mini-jack, 4-pin connectors for external microphones: Cisco Table Microphone 20 or Cisco TelePresence Ceiling Microphone.

Power

Always use the provided power supply:

- DC output: 5.83 A, 12 V
- AC input: 100-240 V, 50-60 Hz, max 1.2 A

The device powers up automatically, as long as the power switch is in its On position.

Factory reset pinhole

Use the pinhole as a last resort. We recommend to perform a factory reset from the touch controller or the web interface.

Monitor outputs

HDMI version 2.0, resolutions up to 3840 × 2160 at 60 fps. Use output 1 for the main monitor and output 2 for the optional second monitor. There is no audio on these outputs. 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 × 2160 at 30 fps. Used for different types of input sources, like computers or external playback devices (audio and video). You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable.

Maintenance

Micro USB connector for serial communication with the device.

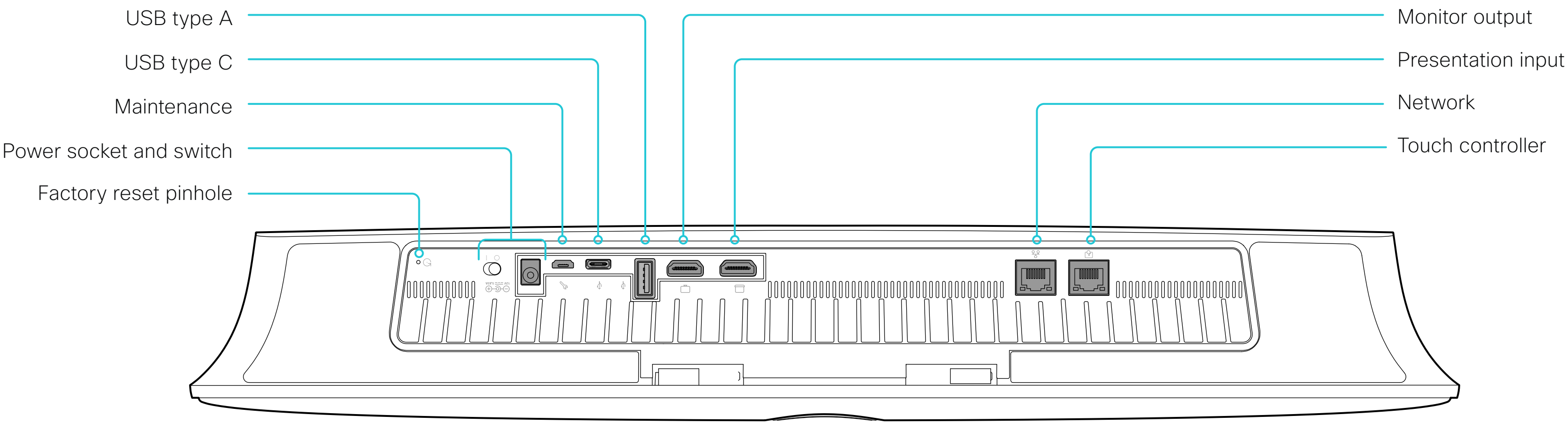
USB

USB 2.0 type A.

Kensington lock

The Kensington lock may be used to prevent the device from being moved and to prevent theft.

Connector panel: Room Kit Mini



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 × 2160 at 60 fps. 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 × 2160 at 30 fps 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.

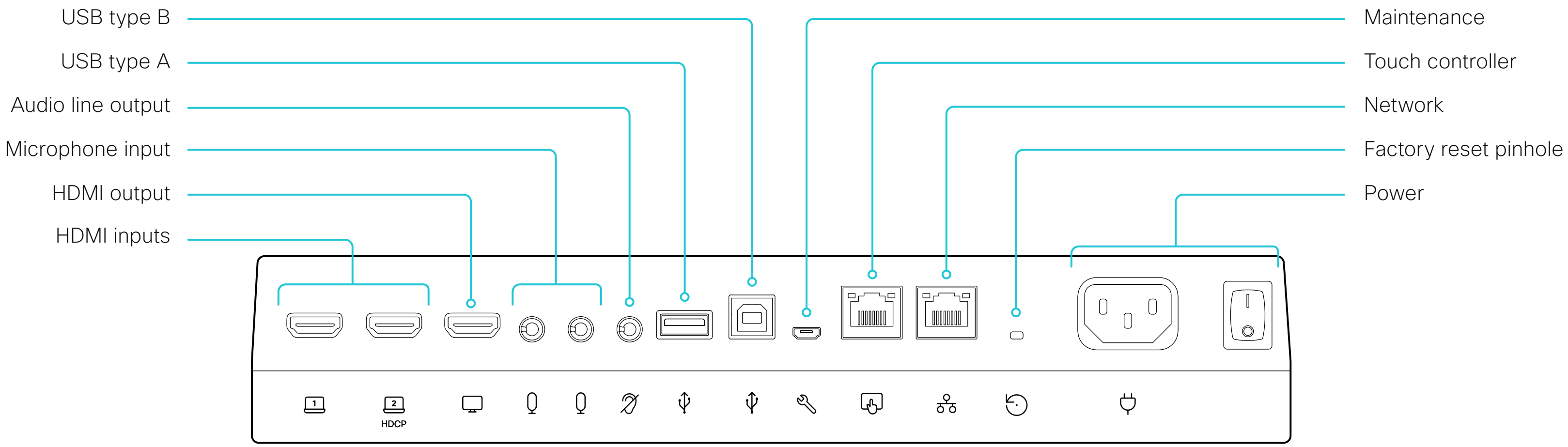
Network

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

Touch controller

The touch controller is powered over Ethernet, which is provided through this socket.

Connector panel: Room 55



HDMI inputs

HDMI version 1.4b, resolutions up to 3840 × 2160 at 30fps. Used for different types of input sources, like computers, or external playback devices (audio and video). You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable.

The second HDMI input allows display of HDCP (High-bandwidth Digital Content Protection) encrypted content.

HDMI output

HDMI version 2.0, resolutions up to 3840 × 2160 at 60fps. Used for an optional second display (only video). You need Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables.

Microphones

Two 3.5 mm mini-jack, 4-pin connectors for external microphones: Cisco Table Microphone 20 or Cisco TelePresence Ceiling Microphone.

Audio line out

3.5 mm mini-jack, 3-pin connector. For example to be used with an audio induction loop system.

USB

- USB 2.0 type A
- USB 2.0 type B

Maintenance

Micro USB connector for serial communication with the device.

Touch controller

The touch controller is powered over Ethernet, which is provided through this socket. See the ► Connect the touch controller chapter for more details.

Network

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

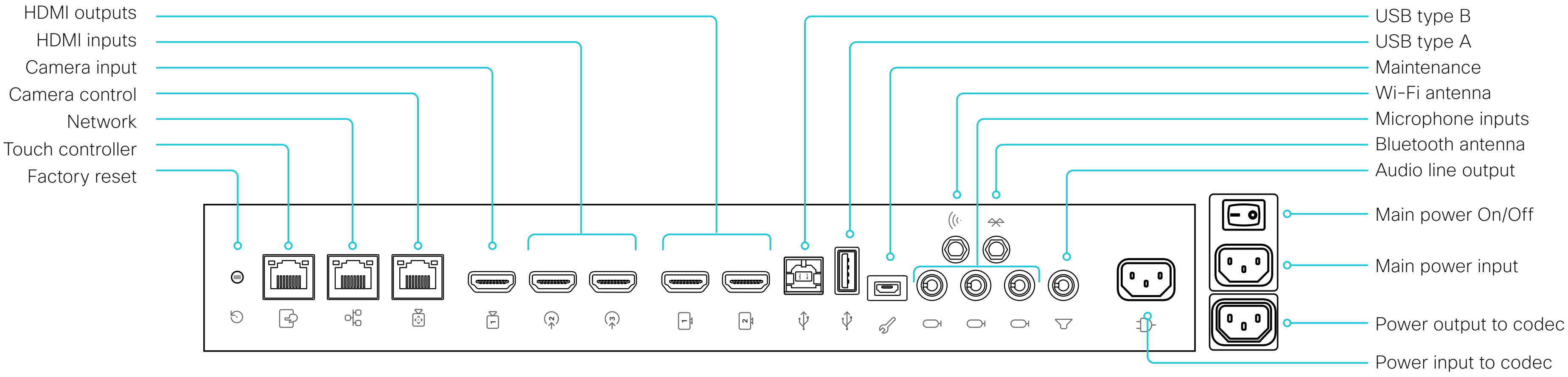
Factory reset pinhole

Use the pinhole as a last resort. We recommend to perform a factory reset from the touch controller or the web interface.

Power

100-240 VAC, 1.8-0.8 A, 50/60 Hz
The device powers up automatically, as long as the power switch is in its On position.

Connector panel: Room 55 Dual and Room 70


HDMI outputs
HDMI inputs
Camera input
Camera control
Network
Touch controller
Factory reset
USB type B
USB type A
Maintenance
Wi-Fi antenna
Microphone inputs
Bluetooth antenna
Audio line output
Main power On/Off
Main power input
Power output to codec
Power input to codec

Factory reset

Pinhole for factory reset. We recommend to perform a factory reset from the Touch user interface or the web interface.

Touch controller

The touch controller is powered over Ethernet (PoE), which is provided through this socket.

Network

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

Camera control

Camera control (pan, tilt, zoom) for the integrated camera.

Camera input

This HDMI input is reserved for the integrated camera.

HDMI inputs with audio

HDMI version 1.4b, resolutions up to 3840 × 2160 at 30 fps. For computer, extra camera, or external playback devices. You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable. The second HDMI input connector allows display of HDCP (High-bandwidth Digital Content Protection) encrypted content.

HDMI outputs with 4K resolution

HDMI version 2.0, resolutions up to 3840 × 2160 at 60 fps. Output 1 is reserved for the internal screen for single screen devices. Both outputs are reserved for the internal screens for dual screen devices. You need Premium HDMI cables to support the high resolutions and frame rates. We recommend Cisco qualified display cables. There is no audio on HDMI output connector 2 on a single screen device.

Audio line output

3.5 mm mini-jack, 3-pin connector.

Microphones

Three 3.5 mm mini-jack, 4-pin connectors for external microphones: Cisco Table Microphone 20 or Cisco TelePresence Ceiling Microphone.

USB connectors

- USB 2.0 type B
- USB 2.0 type A, reserved for internal use
- Micro USB socket for maintenance

Antenna connectors

- Wi-Fi antenna for wireless network connection
- Bluetooth antenna (for future use)

Power

- Reserved for power input to codec
- Reserved for power output to codec
- Main power input (100-240 VAC, 3.5-2.0 A, 50/60 Hz)
- Main power On/Off

Connector panel: Room 70 G2 and Room 70 Panorama

A. Antenna connector (2)

2.4GHz and 5GHz antennas for use with wireless networks or Bluetooth connections.

B. Line outputs (6)

Balanced line level outputs. Euroblock, 3.5 mm.

C. Microphone/line inputs (8)

8 microphones, 48V phantom powered, each with separate echo cancellers and noise reduction; all microphones can be set for balanced line level. Euroblock, 3.5 mm..

D. Programmable GPIO port. 3.5 mm Euroblock connector.

E. COM port. 3.5 mm Euroblock connector.

F. Antenna connector, see A

G. Ground. Protective earth.

H. Power input

Power input to codec and power on/off switch.

I. Main power input

Main power input (100-240 VAC, 5.5-2.5 A, 50/60 Hz) and power on/off switch.

J. HDMI outputs (2).

Audio and video. Connectors 1 and 2, 4Kp60.

K. HDMI output (1)

Audio and video. Connector 3, 4Kp30.

L. Camera inputs (2)

HDMI, connector 1-2, 1080p60.

M. HDMI inputs (3)

Audio and video. Connector 3-5, 4Kp30. Connector 5 supports HDCP.

N. Camera input

3G-SDI / HD-SDI. Connector 6, 1080p60, Level A only, HD-BNC, 75 Ω.

O. USB connectors (2), 2.0 type A.

P. USB connector, 2.0 type B.

Q. Maintenance

Micro USB connector for serial communication with device.

R. Factory reset pinhole

Use the pinhole as a last resort. Perform a factory reset from the touch controller or the web interface.

S. Network

RJ-45: Ethernet interface, 1Gb Ethernet interface.

T. Camera control (2)

RJ-45: Camera control (pan, tilt, zoom). Connecting an extra camera requires an Ethernet switch for control on both cameras.

U. Ethernet PoE

RJ-45: Internal network port for PoE devices.

V. Touch controller

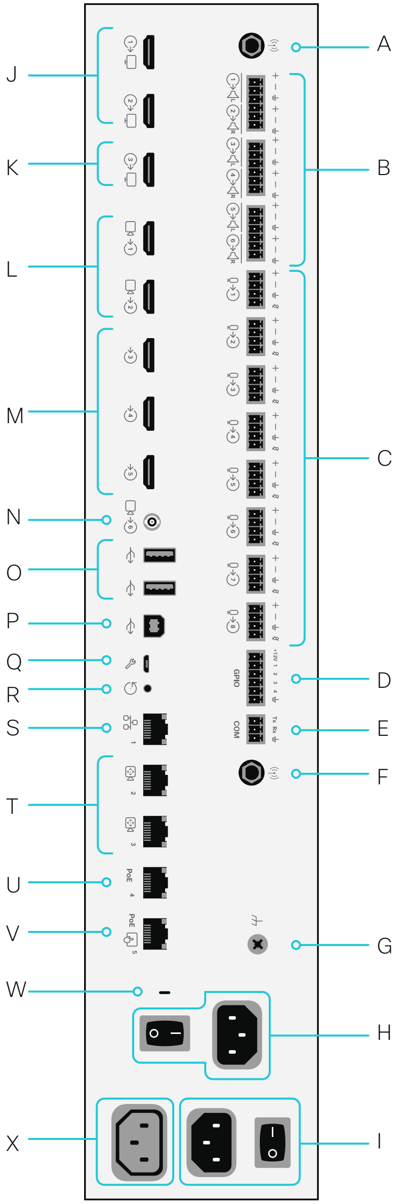
RJ-45: Dedicated PoE port for the touch controller.

W. Status LED

Mirrors the front status LED.

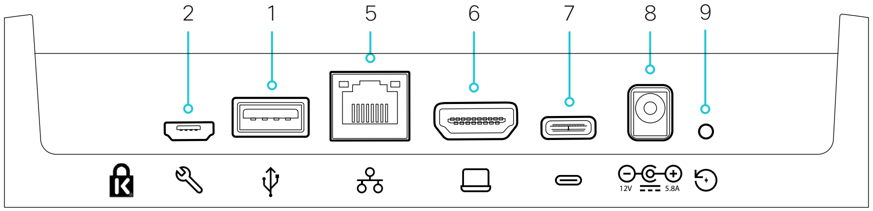
X. Power ouput

Codec power output.

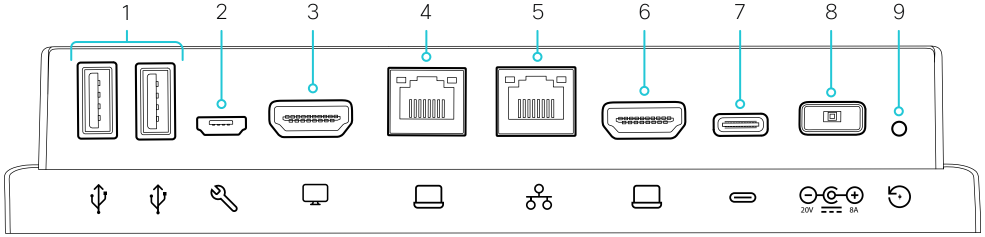


Connector panel: Webex Desk, Desk Pro and Desk Limited Edition

1. USB
   - USB 2.0 type A
2. Maintenance (micro USB)
   - For serial communication with the device
3. HDMI out: for future use *(Only Desk Pro and Desk Limited Edition)*
4. Network for PC *(Only Desk Pro and Desk Limited Edition)*
   - Ethernet interface, 10 Mb / 100 Mb / 1 Gb Ethernet LAN interface (RJ45)
5. Network
   - Ethernet interface, 10 Mb / 100 Mb / 1 Gb Ethernet LAN interface (RJ45)
6. HDMI input
   - HDMI 2.0 type A input. Supports formats up to:
     - 3840 × 2160 at 60 fps (4kp60) *(Desk Pro)*
     - 1920 × 1080 at 60 fps (1080p60) *(Webex Desk and Desk Limited Edition)*
   - Screen extension and content sharing
7. USB-C
   - Supports formats up to the following, using Alternate Mode Display Port:
     - 3840 × 2160 at 60 fps (4kp60) *(Desk Pro)*
     - 1920 × 1080 at 60 fps (1080p60) *(Webex Desk and Desk Limited Edition)*
   - Screen extension and content sharing
   - Touch forwarding capabilities on supported operating systems *(Only Desk Pro and Desk Limited Edition)*
   - Use the camera, microphone and speakers with any software client (USB-camera mode)
   - Laptop charging (60 W maximum) *(Only Desk Pro)*
8. Power
   - Rated:
     - 200 W maximum *(Desk Pro and Desk Limited Edition)*
     - 70 W maximum *(Webex Desk)*
   - Standby power consumption:
     - 15 W; regular standby *(Desk Pro and Desk Limited Edition)*
     - 7.5 W; networked standby *(Webex Desk)*



Main connector panel at the back
(Webex Desk)

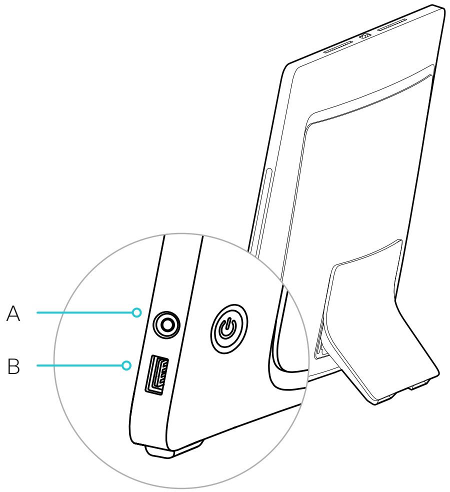


Main connector panel at the back
(Desk Pro and Desk Limited Edition)

9. Factory reset pinhole
   - Use the pinhole as last resort. If possible, we recommend that you reset the device from the user interface or the web interface.

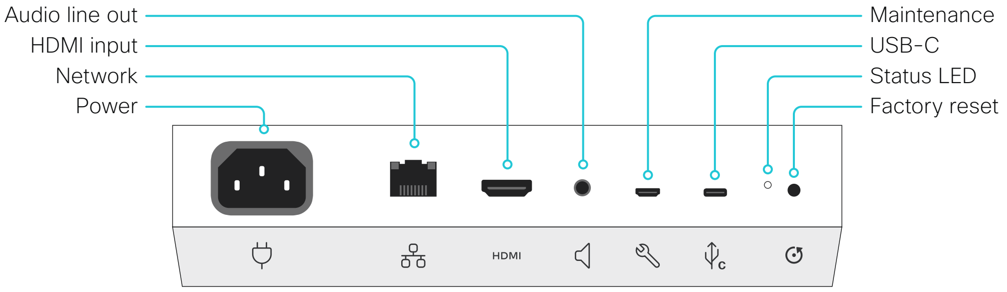
A. Analog audio output *(Only Desk Pro and Desk Limited Edition)*
   - 3.5 mm stereo mini-jack (3-pin)
   - For headphones

B. USB, audio input and output *(Only Desk Pro and Desk Limited Edition)*
   - USB 2.0 type A
   - For USB headset

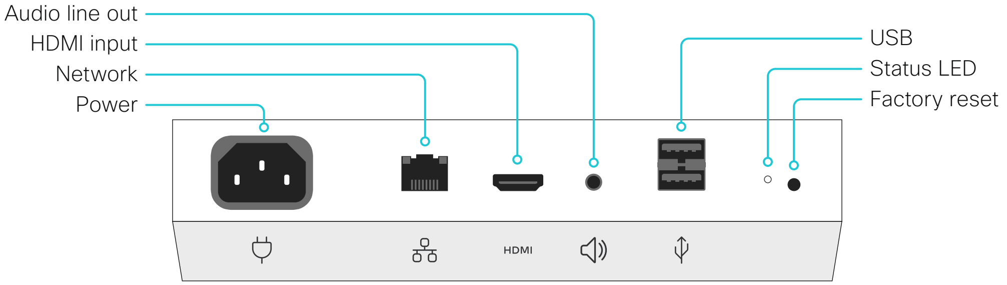


Audio connectors on the right side
(Desk Pro and Desk Limited Edition)

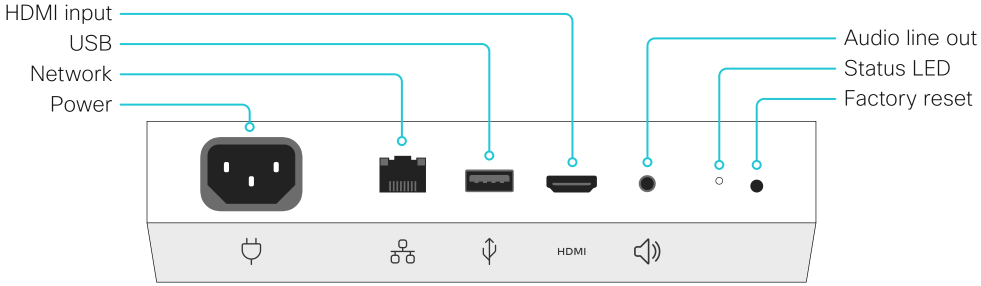
Connector panel: Boards


Audio line out
HDMI input
Network
Power
Maintenance
USB-C
Status LED
Factory reset
HDMI
C

Board 55S, 70S, and 85S [1]


Audio line out
HDMI input
Network
Power
USB
Status LED
Factory reset
HDMI

Board 55


HDMI input
USB
Network
Power
Audio line out
Status LED
Factory reset
HDMI

Board 70

Power

- Board 55S: 100-240 VAC, 3.0-1.5 A, 50/60 Hz
- Board 70S: 100-240 VAC, 3.5-2.0 A, 50/60 Hz
- Board 85S: 100-240 VAC, 4.6-2.0 A, 50/60 Hz
- Board 55, 70: 100-240 VAC, 3.5 A max, 50/60 Hz

Network

- Ethernet interface, 10 Mb / 100 Mb / 1 Gb Ethernet LAN interface (RJ45). [2]

HDMI input

- HDMI version 1.4b, resolutions up to 3840 × 2160 at 30 fps. For computer or external playback devices. You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates. We recommend a Cisco qualified presentation cable.

Audio line output

- 3.5 mm mini-jack, 3-pin connector.

USB

- Board 55: Two USB 2.0 type A for maintenance
- Board 70: One USB 2.0 type A for maintenance
- Board 55S, 70S, and 85S: Micro USB for maintenance
- Board 55S, 70S, and 85S: USB-C

Factory reset

- Pinhole for factory reset. If possible, we recommend that you reset the board from the touch user interface or the web interface.

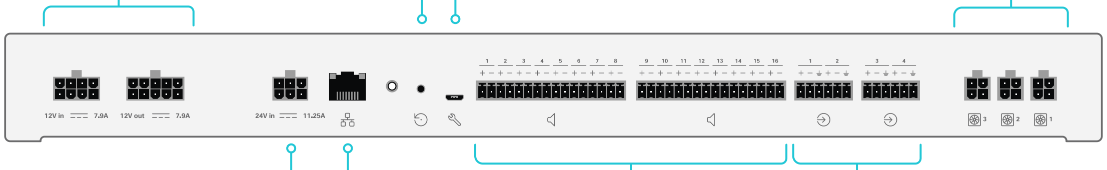
---

[1] The second generation Webex Board family (*S Series*) has some minor hardware platform optimizations.

[2] All models also support Wi-Fi.

Connector panel: Room Panorama amplifier

The Cisco Natural Audio Module IV is an essential component of Room Panorama. It is a 16 channel audio power amplifier with Ethernet and analog inputs.



12V Power input and output

This is a passthrough current limited power connection for the Cisco Quad Camera in a Cisco Room Panorama system.

Factory reset

- Pinhole

Maintenance

- Micro USB

Fan outputs

There are three fan output ports to control the fans in a Cisco Room Panorama system.

Amplifier power input

This is the DC power supply input for the amplifier.

- 24VDC, 11.25A

Ethernet

The Ethernet port is used for audio streaming from a Cisco Codec Pro and for control and software upgrades.

- 1000BASE-T

Speaker outputs

Each speaker output channel is a bridged/differential amplifier output. The + and – connections should be connected to a single speaker only, and not connected to another speaker output or to ground.

Bridged differential output on 3.5 mm Euroblock connectors.

- Max 25 W / 8 ohm at 0.1% THD per channel.
- < 0.1% THD at all levels below clipping.
- 106 dB SNR.
- Max 200 W total output power.

Analog inputs / Line inputs

Each analog input is a differential analog line input. For best performance it should be connected to balanced analog line output signals. However it can be used with unbalanced sources, in that case the – terminal should be connected to ground.

Differential input on 3.5 mm Euroblock connectors.

- Max 24 dBu input level.
- 106 dB SNR.

Chapter 7

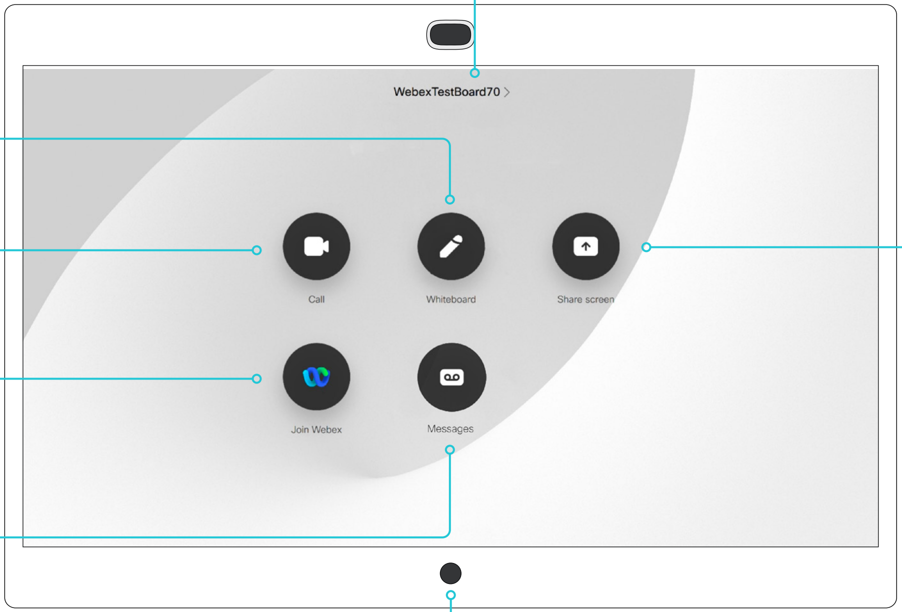
Appendices

How to use the Webex Board

The Webex Board and and its use are described in full detail in the *User guide*.

You can control volume in a call or video presentation. Tap the lower part of the screen and use the slider to adjust the volume.

If you have a touch controller connected to the board, additional features are available on the touch controller.



Tap the device name or address to access *Settings*. Here you can find: *Device Information, Advanced Settings, Network settings, Device activation, Ringtone, Restart* and *Factory reset*.

Tap *Whiteboard* to start a new whiteboard or to access the list of existing whiteboards.

Tap *Call* to make a call.

Tap *Share screen* to view sharing options.

Tap *Join Webex* to join a Webex meeting.

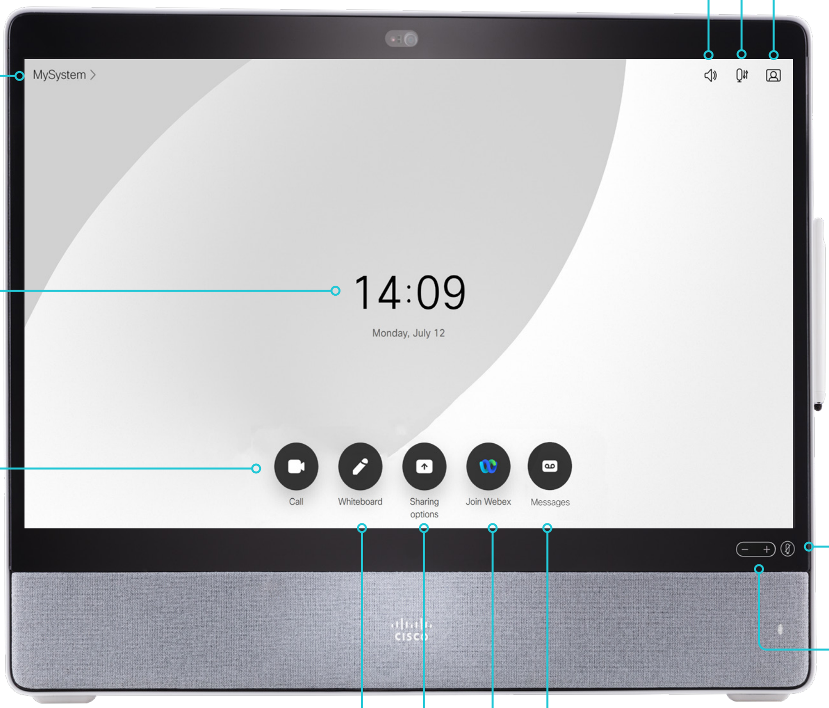
Tap *Messages* to call your voice mail (if available).

Tap the *Home button* to return to the homescreen. Press and hold the button to put the board to standby mode.

How to use the Webex Desk, Desk Pro and Desk Limited Edition

The video conferencing device and its use are described in full detail in the User guide for the device.

Not all features are available on all products; therefore the touch buttons shown here may or may not be present on your device.



Here you can find:

- Do not disturb
- Forward calls
- Settings menu
- Standby

Select audio output (if you have a headset connected)

Turn on audio features such as noise removal and music mode

Self view

Time of day

Stylus *(only Desk Pro and Desk Limited Edition)*

Make calls from your directory or call history, or by using the dial pad

Mute your microphone

Adjust volume

Whiteboarding

Call your voice mail (if available).

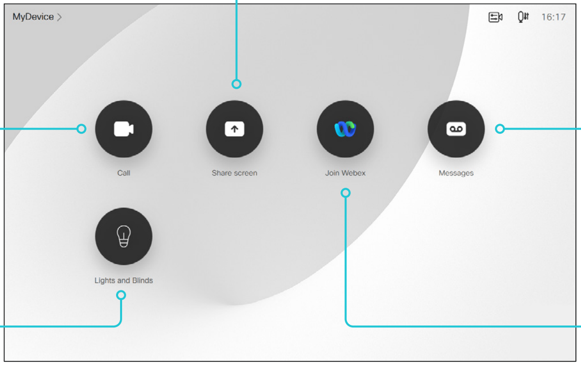
Share computer screen in and outside calls

Join Webex meetings

How to use the touch controller

The touch controller and its use are described in full detail in the User guide for the video conferencing device.

Not all features are available on all products; therefore the touch buttons shown here may or may not be present on your device.



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

Tap the device name or address to access *System Information, Settings, Restart* and *Factory reset*. You can also activate *Call forwarding, Standby,* and *Do not disturb* modes.

Tap *Call* to make a call, and to invoke the *Favorites, Directory* and *Recents* contact lists.

Entry point for user interface extensions (your device may have zero or more such buttons with different text and icons).

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

Tap the *Audio settings* icon turn on audio features such as noise removal and music mode.

Time of day.

Tap *Messages* to call your voice mail (if available).

Tap *Join Webex* to join a Webex meeting.

Volume controls and mute

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 Mute button to mute and unmute microphones.

Room Navigator:

- The volume control is on the touch screen
- The mute button is shown only when in a call

Touch 10:

- The volume controls and mute button are below the touch screen

Using the device as a USB camera (page 1 of 2)

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
- The screen of the device *(Webex Desk, Desk Pro and Desk Limited Edition)*
  If any, the screen that is connected to the device *(Room Kit Mini)*
- 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

Applies to: Room Kit Mini

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 controller, or to remove elements that are irrelevant when not registered to a call service.

Video resoution

Supported video resolutions:

- 720p
- 1080p

Minimum requirements

Minimum USB version:

- USB 2.0

Minimum computer operating system:

- Windows 7
- OS X 10.6

---

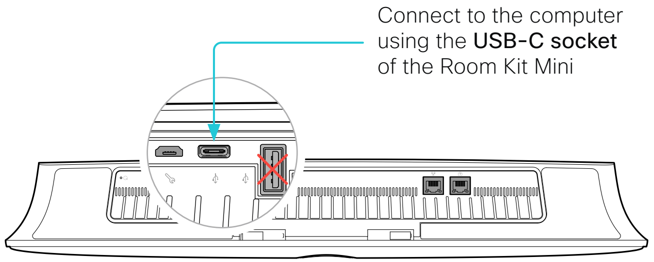
* For example Microsoft Teams, Skype for business, Slack, or Zoom. Cisco successfully tested these clients before product launch. Compatibility between different software versions will not be tested regularly.

Using the device as a USB camera (page 2 of 2)

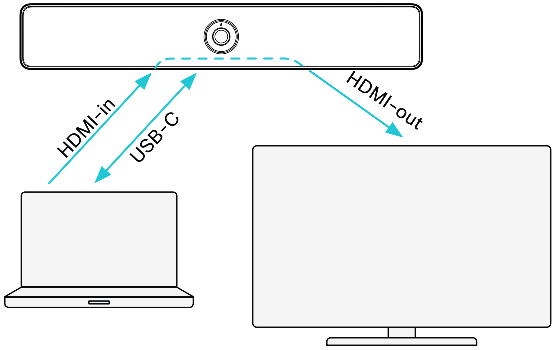
Connect to USB-C

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).

Room Kit Mini



Connect to the computer using the **USB-C socket** of the Room Kit Mini



USB-C:

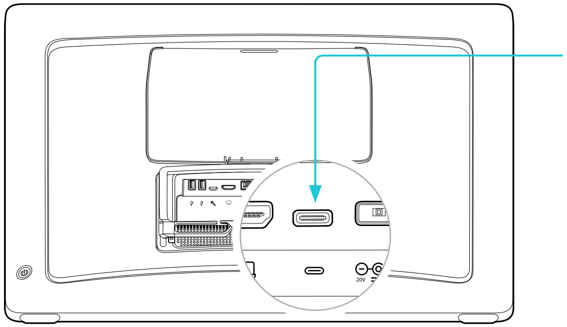
- Video and audio from the camera and microphone of the video conferencing device to the computer client
- Audio from computer client to the loudspeakers of the video conferencing device

HDMI-in and HDMI-out:

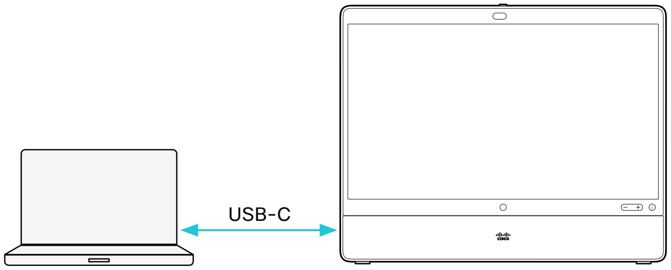
- Video from the computer client (far end), via the video conferencing device, to the screen

You can control the camera and volume from the user interface of the device. Other functionality is controlled by the third-party client on your computer.

Webex Desk, Desk Pro and Desk Limited Edition



Connect to the computer to the **USB-C socket**



USB-C:

- Video and audio from the camera and microphone of the video device to the computer client
- Video and audio from the computer client (far end) to the speakers and screen of the video device

Panoramic video

In Panoramic video we are using two of the camera's telelenses simultaneously to create a wide camera view.

Panoramic video is *always* used in the supported scenarios. It's not a feature that you can switch off, neither permanently nor temporarily.

Supported scenarios

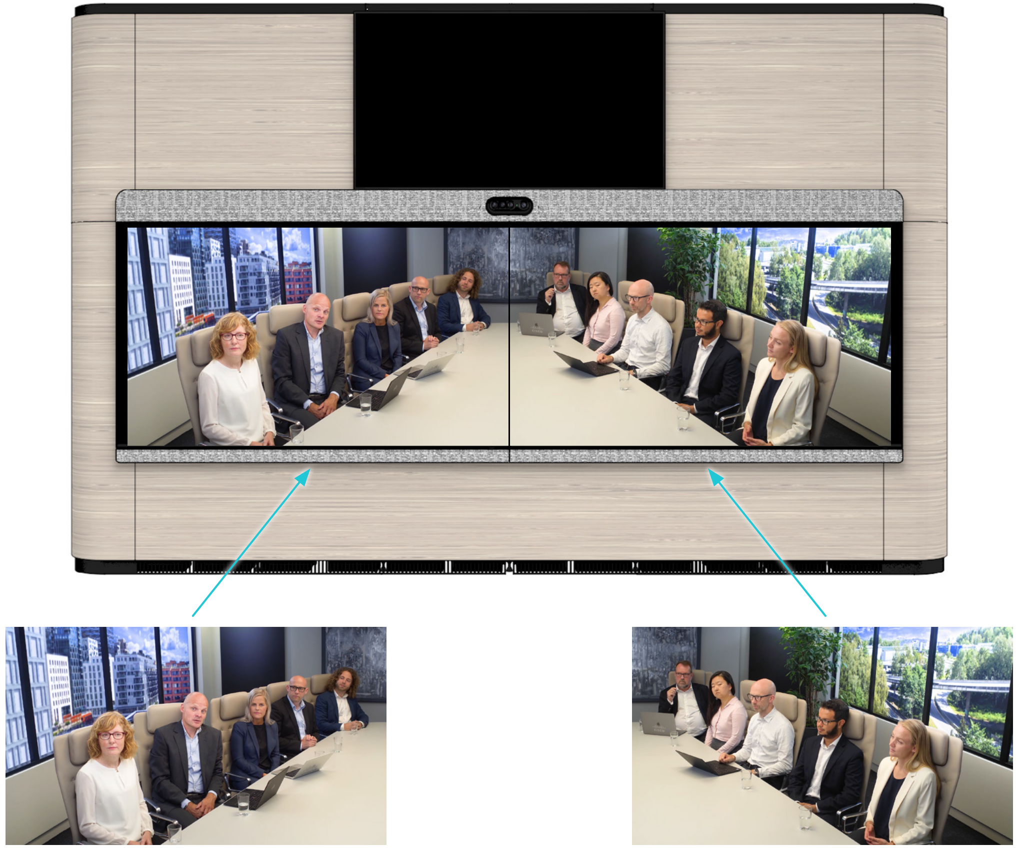
Panoramic video is used in the following scenarios:

- Point-to-point calls between two devices that support Panoramic video
- CMS meeting between two devices that support Panoramic video

More scenarios will be available in later software releases.

Devices that support Panoramic video

- Cisco Webex Room Panorama
- Cisco Webex Room 70 Panorama



Video captured by the right telelense

Video captured by the left telelense

Video from the camera's right and left telelenses are stitched together to create the wide panorama view.

Set up remote monitoring

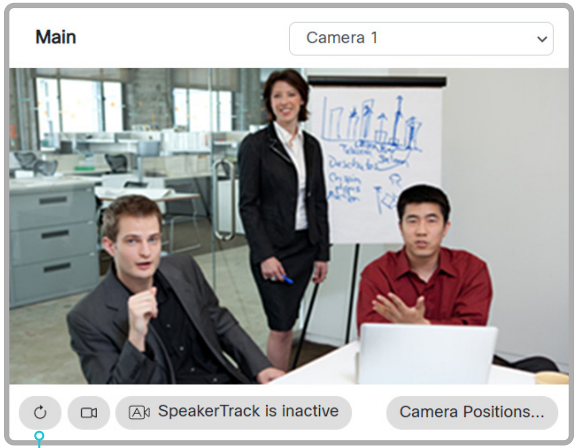
Requirement:

- *RemoteMonitoring* option

Remote monitoring is useful when you want to control the device from another location.

Snapshots from input sources appear in the web interface, so you can check the camera view and control the camera without being in the room.

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



Automatically refresh snapshots

Check whether or not the device has the *RemoteMonitoring* option

1. Sign in to the web interface, go to *Software*, and select *Option Keys*.
2. Check if *RemoteMonitoring* is on the list of *Installed Option Keys*.

   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

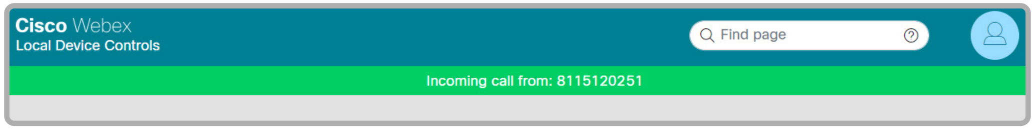
When in call, you may also see snapshots from the far end camera. It does not matter whether or not the far end device has the *RemoteMonitoring* option.

Far end snapshots are not displayed if the call is encrypted.

Access call information and answer a call while using the web interface

A green banner at the top of the web page 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 green banner.



Incoming call from: 8115120251

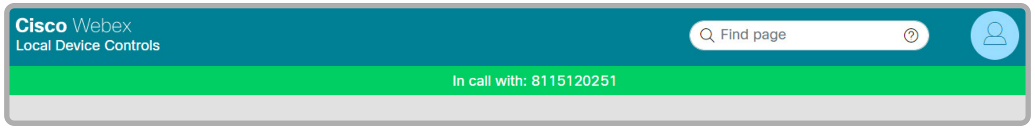
Notification of an incoming call

Click the *green banner* to open the *Call* page, where you can accept or decline the call.

Control the call

Relevant control buttons are present on the *Call* page. Use the buttons to:

- ⓘ Show call details
- ⏸ Put the call on hold
- ☎ Answer the call
- ☎ Disconnect the call



In call with: 8115120251

The device is in a call

The *green banner shows if the device is in a call.* It will also show if the device has multiple active calls.

Place a call using the web interface (page 1 of 2)

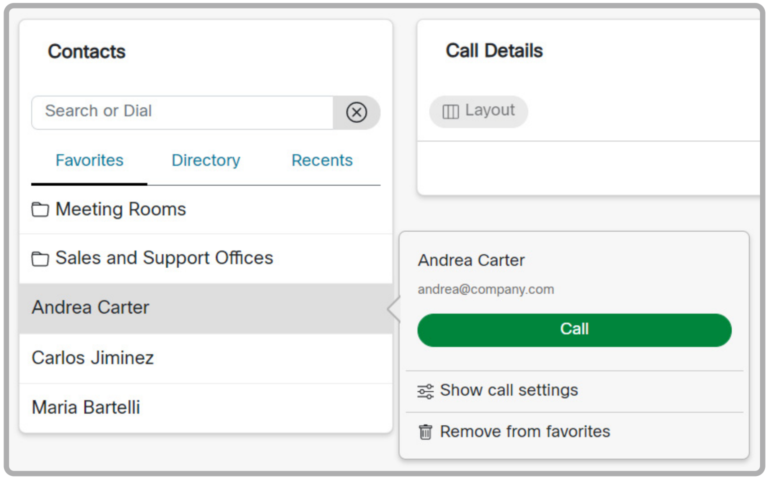
Sign in to the web interface and go to *Call*.

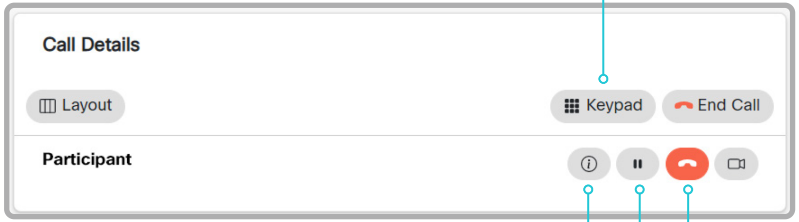
Place a call

ⓘ 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.


Contacts
Search or Dial
Favorites
Directory
Recents
Meeting Rooms
Sales and Support Offices
Andrea Carter
Carlos Jiminez
Maria Bartelli
Call Details
Layout
Andrea Carter
andrea@company.com
Call
Show call settings
Remove from favorites


Call Details
Layout
Keypad
End Call
Participant

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 *End Call*. 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 shown as you type.

Place a call using the web interface (page 2 of 2)

Sign in to the web interface and go to *Call*.

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 or five participants, yourself included, can join the video call (conference), see the table.

Video conferencing device	**Maximum number of participants in a MultiSite call**
Boards, Codec Plus, Room Kit, Room Kit Mini, Room 55, Room 55 Dual, Room 70	4
Codec Pro, Webex Desk, Desk Pro, Desk Limited Edition, Room 70 G2, Room 70 Panorama, Room Panorama	5

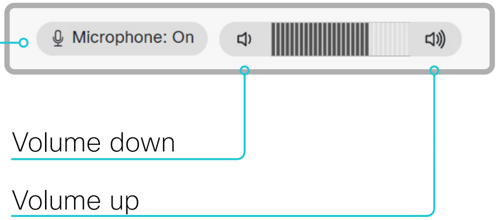
Follow the same procedure to call the next conference participant as you did when calling the first participant.

Adjust the volume

Mute the microphone

Click *Microphone: On* to mute the microphone. Then the text changes to *Microphone: Off*.

Click *Microphone: Off* to unmute.



Share content using the web interface

Sign in to the web interface and go to *Call*.

Share content

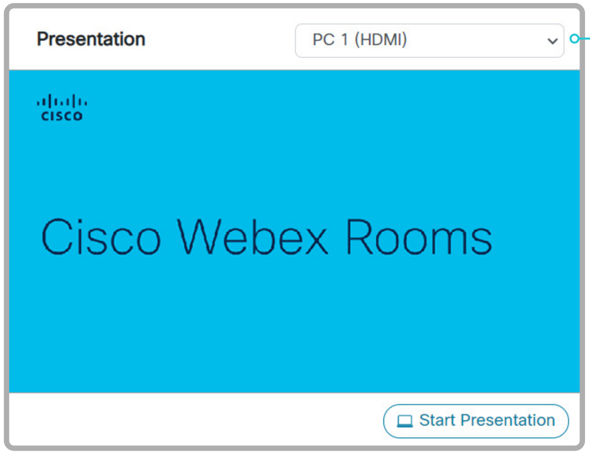
1. Choose which content source to share in the *Presentation* source drop down list.

   Products that support only one input source, have only one entry in the drop down list.

2. Click *Start Presentation*. Then the text changes to *Stop Presentation*.

Stop content sharing:

Click the *Stop Presentation* button that is present while sharing.



Presentation source drop down list

Choose which input source to share, from the drop down list.

Snapshot area

Shows snapshots of the selected presentation source.

Only available on devices that have the *Remote Monitoring* option.

About content sharing

You can connect a presentation source to a video input on your device. Most often a PC is used as presentation source, but other options may be available depending on your device setup.

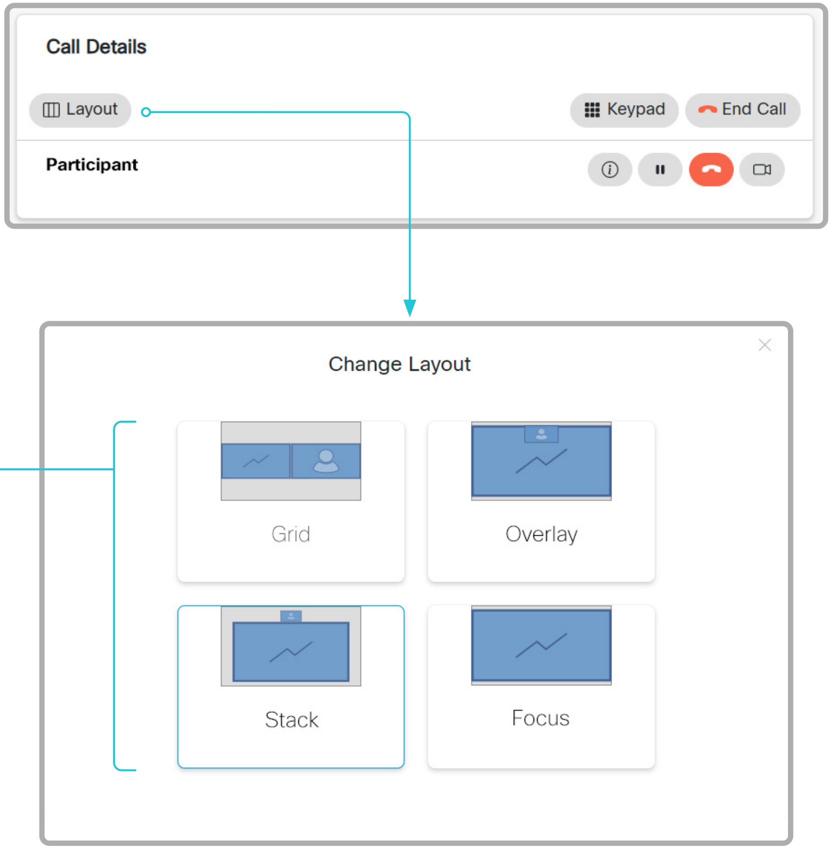
While in a call you can share content with the other participants in the call (far end).

If you are not in a call, the content is shown locally.

Local layout control

Sign in to the web interface and go to *Call*.

Note: Local layout control is not available in Panoramic video scenarios.



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.

About layouts

The term layout is used to describe the various ways presentations and videos can appear on the screens. Different types of meetings may require different layouts.

The number of call or conference participants are reflected in the available choices.

Note: The set of layouts are currently being renamed. For a short period, you might see a mix of both the old and new names in use.

Old name	New name
Equal	Grid
Overlay	Overlay
Prominent	Stack
Single	Focus

---

[*] Changing the participant layout from the web interface is not supported when calling a conference bridge, even if it is supported on the video conferencing device itself.

Control a local camera

Sign in to the web interface and go to *Call*.

Prerequisites for manual camera control

- The *Video > Input > Connector n > CameraControl > Mode* setting is switched **On** .
- The camera has pan, tilt or zoom functionality.
- Best overview / Speaker tracking is switched off.
- Panoramic video is not in use.

Snapshot area

Shows snapshots of the selected camera (main input source).

Only available on devices that have the *Remote Monitoring* option.

Automatically refresh snapshots

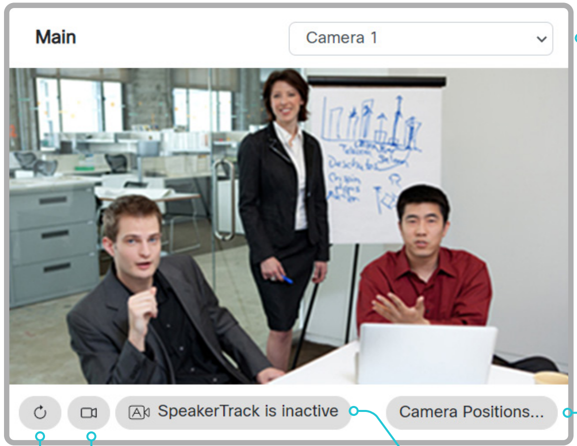
Move the camera using the pan/tilt/zoom controls

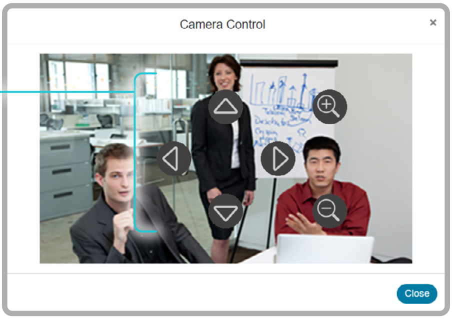
Camera control is not available when speaker tracking / best overview is switched on.

1. If applicable, choose which camera to control in the *Main* source drop down list.
2. Click the camera icon to open the camera control window.

   Video snapshots from the room are only displayed for devices that have the *Remote Monitoring* option.
3. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and − to zoom in and out.

   Only relevant controls appear in the window.
4. Click *Close* to close the window.





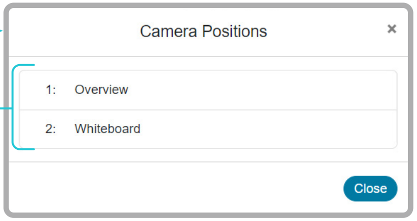
Main source drop down list

Choose which camera to control from the drop down list.

Products that support only one camera don't have a drop down list.

Best overview / Speaker tracking

Click to toggle the feature on and off.



Move the camera to a preset position

1. If applicalbe, choose which camera to control in the *Main* source drop down list.
2. Click *Camera Positions...* to open a list of available presets.

   If no presets are defined, the button is disabled and named *No presets*.
3. Click a preset's name to move the camera to the preset position.
4. Click *Close* to close the window.

ⓘ You cannot use the web interface to define a preset; you should use the user interface of the device.

When you select a preset, speaker tracking / best overview will be switched off automatically.

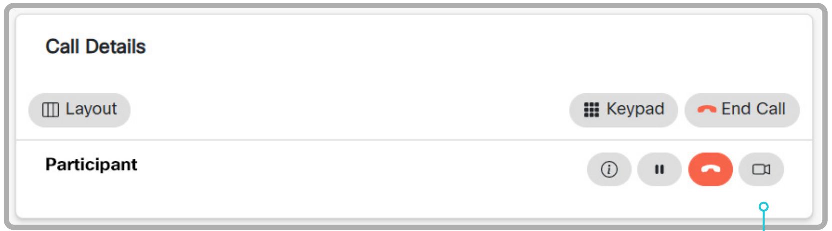
Control a far end camera

Sign in to the web interface and go to *Call*.

Prerequisites

While in a call, you can control the remote participant's camera (far end) provided that:

- Panoramic video is *not* in use.
- 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.

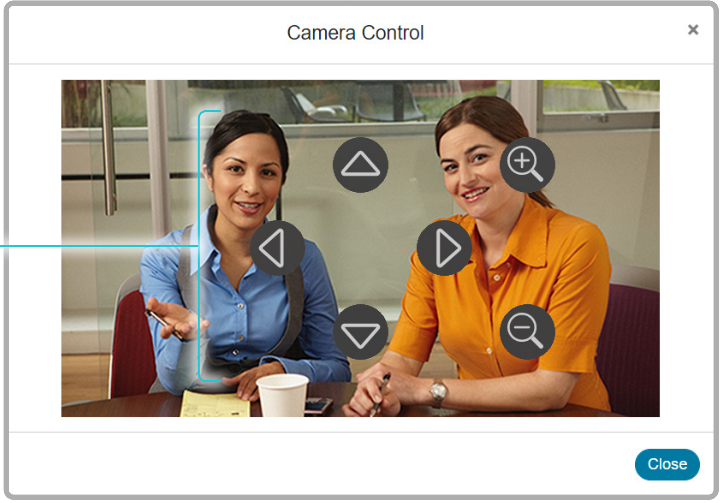


Control the remote participant's camera

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.



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.

To find the settings referred below, sign in to the web interface, go to *Settings*, and select *Configurations*.

To find a status, sign in to the web interface, go to *Settings*, and select *Statuses*.

Ambient noise reporting

The devices can report the stationary ambient noise level in the room. The reported value is an A-weighted decibel value (dBA), which reflects the response of the human ear. All signal processing related to this feature is local, the only data transmitted is the calculated noise level.

This value can be used to detect abnormal changes to the noise level. Such changes may be caused by noise that can be an annoyance for people working in the room. Facility management can then quickly intervene to troubleshoot the issue.

You can turn the ambient noise detection on or off from the web interface. Use the *RoomAnalytics > AmbientNoiseEstimation > Mode* setting.

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. Use the *RoomAnalytics > PeoplePresenceDetector* setting.

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 retrive 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.

Use the *RoomAnalytics > PeopleCountOutOfCall* setting.

For Codec Pro and Codec Plus

- People count in call requires the use of a Quad Camera or SpeakerTrack 60 camera.
- People count outside of call requires a Quad Camera.

Status

You may see the status at a given moment of people’s presence and people count. Look at the *RoomAnalytics* status.

Diagnostics

You can see the live people counter on-screen by enabling the SpeakerTrack Diagnostics mode from the user interface. 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*.

For Boards:

If you have connected a touch controller you can use the procedure described above.

Alternatively, you can open the *Technical support screen* on the board itself (hold down one finger on the board's screen, and press the home button three times). Then click *Hardware diagnostics* under the Device tab, and turn on *BestOverview debug*.

Call history command

After a call the average people count value can be extracted from the Call History command.

- `xCommand CallHistory Get DetailLevel: Full`

The Call History command is available from the API (Application Programming Interface). Refer to the API Reference Guide, which covers all product, for details. Go to:

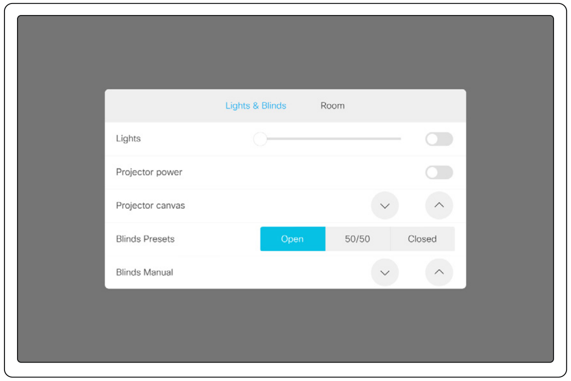
- ▶ https://www.cisco.com/go/room-docs
- ▶ https://www.cisco.com/go/board-docs
- ▶ https://www.cisco.com/go/desk-docs

Boards
Codec Plus
Codec Pro
Desk, Desk LE, Desk Pro
Room Kit
Room Kit Mini
Room 55
Room 55 Dual
Room 70
Room 70 G2
Room 70 Panorama
Room Panorama

Customize the video conferencing device's user interface (page 1 of 2)

You can customize the user interface to allow control of peripherals in a meeting room, for example lights and blinds, or to modify the video conferencing device’s behavior by triggering macros.

This allows for the powerful combination of a control system’s functionality and the video conferencing device's user-friendly touch user interface.



Example in-room control panel

Consult the *Customization guide* for full details about how to design custom user interface panels, action buttons, and web apps using the UI Extensions editor, and how to use the video conferencing device’s API to program the controls and actions. Go to:

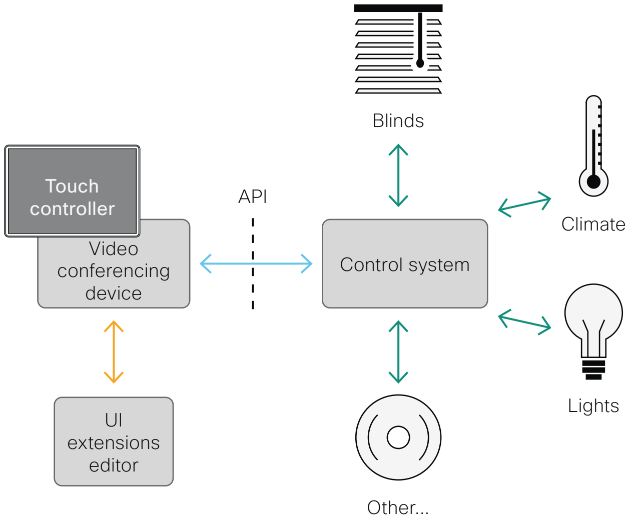
► https://www.cisco.com/go/in-room-control-docs

In-room control architecture

You need a Cisco video conferencing device with a touch interface (touch controller or integrated touch screen), 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.

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.



In-room control schematics

Product support

These devices support custom user interface panels and action buttons:

- Devices that has a touch controller.
- Devices with an integrated touch screen.

These products support web apps:

- Devices with an integrated touch screen.

For Boards:

- If you have not connected a touch controller to the board, the custom panels and action buttons are on the board itself.
- If you have connected a touch controller to the board, all the custom panels and action buttons are on the touch controller.
- Web apps are always on the board.

Customize the video conferencing device's 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, web apps, 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 go to *UI Extensions Editor*.

- The editor opens directly in the device's web interface.

  You can create and push a new panel, action button, or web app to the device, and see the result immediately on its user interface.

Preview function

The editor also provides a preview function, which allows you to see how the custom interfaces will appear on the user interface.

- Click 👁 to start the preview.

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 user interface.

Therefore, you can use the preview function to test your integrations without having a real 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.

Customize the video conferencing device's behavior using macros

With macros, you can create your own snippets of code that run on the device. The language is JavaScript / ECMAScript 6 with support for features such as arrow functions, promises and classes.

The macro framework allows an integrator to write scripts that tailor a device's behavior to suite an individual customer's requirements. The integrators can, for example, implement their own features or variations of features, automate specific configurations or re-configurations, and create custom tests and monitoring functions.

By combining the use of macros and creation of a custom user interface panel (UI extension), you can amend the user interface 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, go to *Settings*, and select *Configurations*.

- 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 go to *Macro Editor*.

This opens the Macro Editor, w**hich is embedded in the web interface of the device.** We don't offer a stand-alone editor.

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

Show or hide default buttons on 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 show or hide buttons on the user interface. The configurations are available both from the web interface of the device, and in the API.

- *UserInterface > Features > Call > Start*: Show or hide the default *Call* button (including the directory, favorites, and recent calls lists). Also affects the *Add* participant button while in a call. [1]
- *UserInterface > Features > Call > JoinWebex*: Show or hide the default button for joining a Webex meeting.
- *UserInterface > Features > Call > JoinGoogleMeet*: Show or hide the button for joining a Google Meet meeting. [2]
- *UserInterface > Features > Share > Start*: Removes the default user interface for sharing and previewing content, both in call and out of call.
- *UserInterface > Features > Whiteboard > Start*: Removes the default button for starting a whiteboard. ***(Only Boards, Webex Desk, Desk Pro, and Desk Limited Edition)***
- *UserInterface > Features > Call > VideoMute*: Removes the default *Turn video off* button.
- *UserInterface > Features > Call > End*: Removes the *End Call* button.
- *UserInterface > Features > Call > MidCallControls*: Removes the *Hold*, *Resume*, and *Transfer* in-call buttons. [1]
- *UserInterface > Features > Call > MusicMode*: Removes the toggle button that enables Music mode on the device. Music mode is useful when the microphones should capture music.
- *UserInterface > Features > Call > Keypad*: Removes the in-call *Keypad* button, which opens a keypad that can be used for DTMF input.
- *UserInterface > Features > HideAll*: Removes all the default buttons. Custom buttons are not removed.

ⓘ 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

---

[1] ***Boards:*** The *Add* participant, *Hold*, *Resume*, and *Transfer* buttons are not available on the Board itself, only on a connected touch controller.

[2] The button allows users to dial into Google Meet meetings using just the meeting code, generated by the Google invite. This is only available on devices registered to the Webex cloud service or linked to Webex Edge for devices.

Use of a third-party USB input device

You can use a third-party USB input device to control certain functions on the 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 video conferencing device's user interface, wherever convenient. It is not meant to replace the user interface.

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 interface. For example, in operating rooms in a hospital.

Functional Overview

Pressing a button on the USB input device, generates an event in the API. Macros or third-party control devices can listen for such events, and respond to them. This behavior is similar to the behavior of custom UI buttons (UI extensions). It is also possible to listen for the events using webhooks, directly in an SSH session.

There isn't a library of actions readily available to select actions from. You must define and implement the actions to be taken as response to the events yourself. For example:

- Increase the volume of the video conferencing device when the Volume Up key is pressed.
- Put the video conferencing device in standby mode when the Sleep key is pressed.

Configurations, Events, and Status

The support for third-party USB input devices is disabled by default. Enable it explicitly by setting the *Peripherals > InputDevice > Mode* to **On**.

Pressing and releasing a button generates a Pressed and a Released event:

```
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Pressed
** end
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Released
** end
```

To listen for events, you must register feedback from the InputDevice events:

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

When the video conferencing device detects the third-party input device, the input device is listed in the video conferencing device's *UserInterface > Peripherals > ConnectedDevice* status. The input device may be reported as multiple devices.

Required Equipment

- A device from the Cisco Webex Room, Board, or Desk Series.
- A third-party input device that advertises itself as a USB keyboard, for example a Bluetooth remote control with a USB dongle.

Further Information

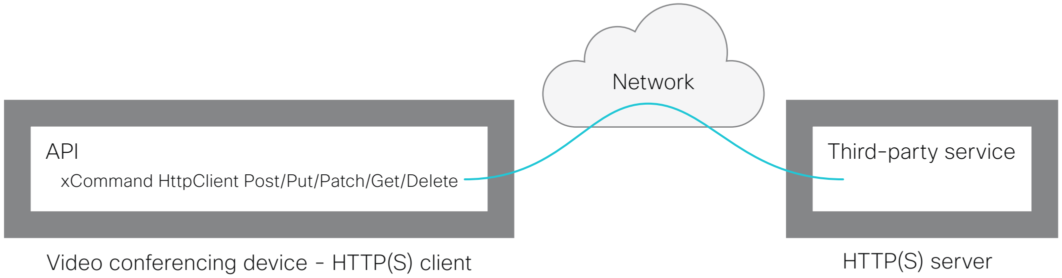
Find more information about the use of a third-party input device in the *Customization guide*. Go to:

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

Cisco support (TAC) doesn't support debugging of third-party code, including macros. Please check the ► Cisco Collaboration Developer community if you need help with macros and third-party code.

Customization

Sending HTTP(S) requests


Network
API
xCommand HttpClient Post/Put/Patch/Get/Delete
Third-party service
Video conferencing device – HTTP(S) client
HTTP(S) server

The HTTP(S) request feature makes it possible to send arbitrary HTTP(S) requests from a video conferencing device to an HTTP(S) server. Furthermore, the device receives the response that the server sends back. The device supports the **Post**, **Put**, **Patch**, **Get**, and **Delete** methods.

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

Security measures:

- The HTTP(S) request feature is disabled by default. A system administrator must explicitly enable the feature by setting *HttpClient > Mode* to **On**.
- The system administrator can prevent the use of HTTP by setting *HttpClient > AllowHTTP* to **False**.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent HTTP(S) requests is limited.

List of Allowed HTTP(S) servers

The system administrator can use these commands to set up and maintain a list of up to ten allowed HTTP(S) servers (hosts):

- `xCommand HttpClient Allow Hostname Add Expression: <Regular expression that matches the host name or IP address of the HTTP(S) server>`
- `xCommand HttpClient Allow Hostname Clear`
- `xCommand HttpClient Allow Hostname List`
- `xCommand HttpClient Allow Hostname Remove Id: <id of an entry in the list>`

If the list is not empty, you can send HTTP(S) requests only to the servers in the list. If the list is empty, you can send the requests to any HTTP(S) server.

The check against the list of allowed servers is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

HTTPS without certificate validation

When sending requests over HTTPS, the video conferencing device checks the certificate of the HTTPS server by default. If the HTTPS server certificate is not found to be valid, you get an error message. The device doesn't send any data to that server.

We recommend using HTTPS with certificate validation. If certificate validation is not possible, the system administrator can set *HttpClient > AllowInsecureHTTPS* to **On**. This allows the use of HTTPS without validating the certificate of the server.

Sending HTTP(S) requests

Once the HTTP(S) request feature is enabled, you can use the following commands to send requests to an HTTP(S) server:

```
xCommand HttpClient <Method>
  [AllowInsecureHTTPS: <True/False>]
  [Header: <Header text>]
  [ResponseSizeLimit: <Maximum response size>]
  [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

Further information

Find more information about HTTP(S) Post requests in the *Customization guide*. Go to:

▶ https://www.cisco.com/go/in-room-control-docs

Web view based features

Digital signage

Digital signage allows you to show custom content (a web page) on a device when it's in half-wake state. Digital signage is a way to display advertising content and promote your brand, but also to show visitor and internal employee information, dashboards, or calendars.

The content replaces the traditional half-wake background image and information, and is always shown on full screen. Only one web window or tab is supported. If a web page tries to open a page in a new window or tab, it replaces the current page.

Data, such as cache, cookies, and local storage, is NOT automatically cleared when the device restarts. You must use the delete storage command to delete the data.

- `xCommand WebEngine DeleteStorage [Type: WebApps]`

If a web page is not supported, the device goes directly to normal half-wake mode.

Interactive mode

Applies to: Boards, Webex Desk, Desk Pro, and Desk Limited Edition

Users can interact with the content on the screen, for example click on a link or enter text in a form.

Set up digital signage

1. Sign in to the web interface, go to *Settings*, and select *Configurations*.
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

- If supported, decide whether to allow interaction with the web page.

  Standby > Signage > InteractiveMode

- 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.

Using a proxy

You can set up the device to use an HTTP proxy for web view based features.

NetworkServices > HTTP Proxy

Additionally, this setting must be **On:**

WebEngine > UseHttpProxy

Web view based features

Web apps

A web app is a web page or application that a user can access from the home screen of the device. The web app is available only when not in a call.

A web app launches in full screen, and times out after 15 minutes if not being used. The web app may be interactive.

Data, such as cache, cookies, and local storage, is automatically cleared when the session ends.

You must use the *UI Extensions editor*, which is available from the web interface of the device, to create web apps. The editor also lets you configure the label and icon to be used on the Home screen. By default, the web page's icon is used, but you can choose another icon instead.

Icon details:

- Formats: .ico, .png, .jpg. svg, or .gif
- Icon size: Minimum 60×60 pixels, maximum 1200×1200 pixels

Typical apps may be Office 365, Trello, Wikipedia, YouTube or company internal web pages and tools.

Further information

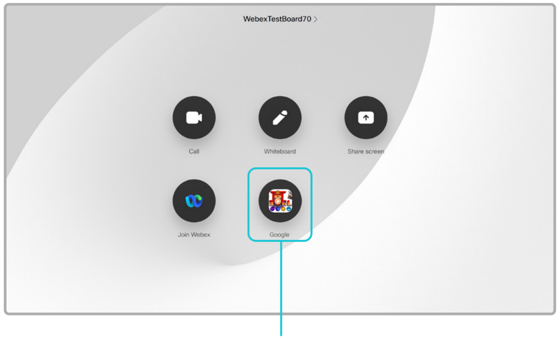
Find more information about how to create web apps in the *Customization guide*. Go to:

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

Create a web app

1. Sign in[*] to the web interface, go to *Settings*, and select *Configurations*.
2. Set *WebEngine > Mode* to **On** to enable the web engine.
3. Go to *UI Extensions Editor*, and the editor opens directly in the device's web interface.
4. Click *New* and select the Web App *Add* button.
5. Fill in the web app properties in the right side bar:
    - Id: Unique identifier of the app.
    - Name: The label of the button on the Home screen.
    - Web app URL: The web app URL.
    - Web app icon URL (optional): The icon for the button on the Home screen.
6. Click the export button in the top bar to upload the configuration to the device.

   Now you can see the button for the new web app on the Home screen.



Web app button with label and icon

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.

Using a proxy

You can set up the device to use an HTTP proxy for web view based features.

NetworkServices > HTTP Proxy

Additionally, this setting must be **On:**

WebEngine > UseHttpProxy

---

[*] 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.

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.

Using a proxy

You can set up the device to use an HTTP proxy for web view based features.

NetworkServices > HTTP Proxy

Additionally, this setting must be **On:**

WebEngine > UseHttpProxy

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 maxmium number of *different* input sources depends on the device:

Video conferencing device	Maximum number of different input sources
Room Kit, Room Kit Mini	2
Codec Plus, Room 55, Room 55 Dual, Room 70, Webex Desk, Desk Pro, Desk Limited Edition	3
Codec Pro, Room 70 G2, Room Panorama*, Room 70 Panorama*	4

Source composition

Composition layout

You can choose between three layouts:

- Grid
- Stack
- 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.

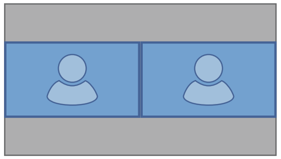
Change compositions and layouts on demand

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.

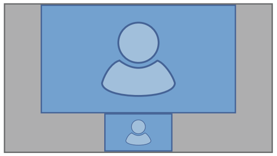
Layouts

Grid



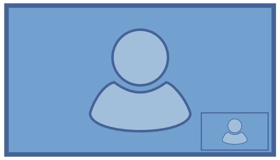
Number of sources: 2

Stack

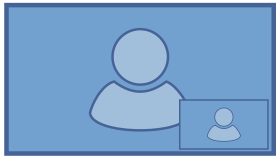


Number of sources: 2

Picture-in-Picture *(PIP)*



Lower right corner



Lower right corner, large PIP

---

* *Room 70 Panorama and Room Panorama:* These devices use two input sources for the main camera.

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.

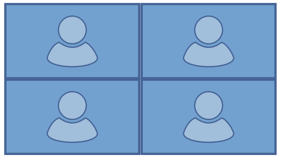
You see the difference between the Grid (`Layout: Equal`) PIP (`Layout: PIP`), and Stack (`Layout: Prominent`) layouts in the examples.

You can modify the PIP position to one of the corners. The size of the PIP can be normal (auto) or large.

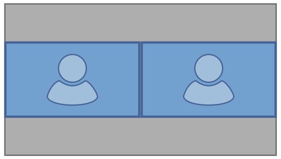
Refer to the API-guide for more details.

Examples

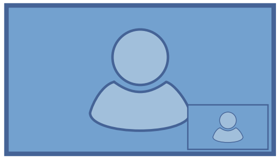
`xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 ConnectorId: 3 ConnectorId: 4 Layout: Equal`



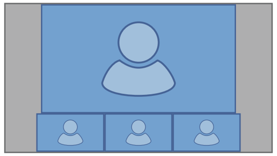
`xCommand Video Input SetMainVideoSource ConnectorId: 1 ConnectorId: 2 Layout: Equal`



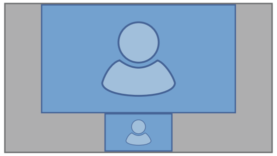
`xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 Layout: PIP PIPPosition: LowerRight PIPSize: Large`



`xCommand Video Input SetMainVideoSource SourceId: 1 SourceId: 2 SourceId: 3 SourceId: 4 Layout: Prominent`



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



Presentation source composition (page 1 of 2)

You can use the device's API to combine up to four presentation sources in a single video stream. *

The maxmium number of *different* presentation sources depends on the device:

Video conferencing device	**Maximum number of different presentation sources**
Room Kit, Room Kit Mini, Board	2
Codec Plus, Room 55, Room 55 Dual, Room 70, Webex Desk, Desk Pro, Desk Limited Edition	3
Codec Pro, Room 70 G2, Room Panorama*, Room 70 Panorama*	4

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:

- Grid
- Stack

You can change the number of sources at any time, both in call and outside of call. The image sizes cannot be modified.

The order in which the sources appear on the screen depends on the order they have in the command; starting from upper left, ending at bottom right.

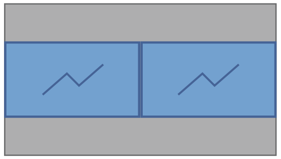
Change compositions and layouts on demand

Presentation source composition is only available using API commands; we don't provide a dedicated user interface for it.

To be able to easily change compositions and layouts on demand, we recommend that you use macros and create a custom user interface panel (UI extension) for it.

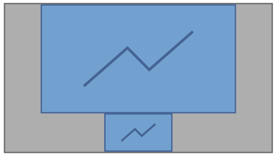
Layouts

Grid



Number of sources: 2

Stack



Number of sources: 2

---

* *Room 70 Panorama and Room Panorama:* These devices use two input sources for the main camera.

Presentation source composition (page 2 of 2)

API command

```
xCommand Presentation Start
    ConnectorId: <1..n>
    PresentationSource: <None, 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.

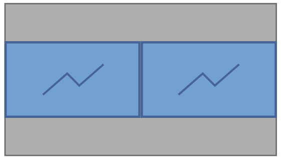
If you select `PresentationSource: None`, a black frame is inserted. *

You see the difference between the Grid (`Layout: Equal`) and Stack (`Layout: Prominent`) layouts in the examples.

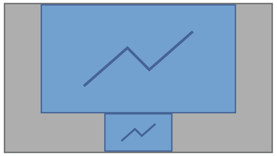
Refer to the API-guide for more details.

Examples

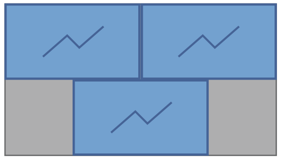
```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```



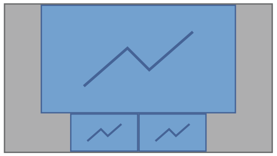
```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```



```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 ConnectorId: 3 Layout: Equal
```



```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 PresentationSource: 3 Layout: Prominent
```



---

* *Boards:* `None` is not available.

Access the device’s XML files

Sign in to the web interface and go to *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.

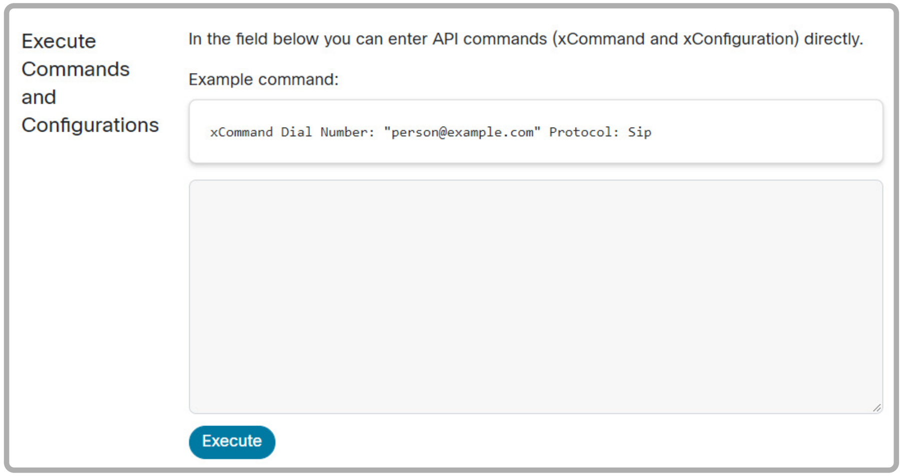
Execute API commands and configurations from the web interface

Sign in to the web interface and go to *Developer API*.

Commands (xCommand) and configurations (xConfiguration) can be executed from the web interface. Syntax and semantics are explained in the API guide for the device.

Execute API commands and configurations

1. Enter a command (xCommand or xConfiguration), or a sequence of commands, in the text area.
2. Click *Execute* to issue the command(s).



Execute Commands and Configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

Example command:

```
xCommand Dial Number: "person@example.com" Protocol: Sip
```

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.

Advanced customization of audio

Sign in to the web interface and go to *Audio Console*.

This opens the Audio Console utility, which is embedded in the web interface of the device.

The Audio Console provides a graphical interface to advanced customizable audio features. It lets you define how to connect audio inputs to outputs, using simple drag and drop techniques.

The main features of the Audio Console are:

- Configure the audio system of the codec
- Change the default mixing, routing and equalizers
- Set various input and output connector properties
- Configure advanced features such as local reinforcement

See the *Customization guide* for details about the Audio Console. Go to:

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

We also recommend you to read the ► Using extra loudspeakers and sound reinforcement chapter for more information about a good auditory experience.

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 controllers, 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, such as the touch controller.

Product	Number of auxiliary network ports	Number of auxiliary network ports with PoE
Room Kit	1	0
Room Kit Mini	1	1 (☝)
Room 55	1	1 (☝)
Room 70[1] / Room 55 Dual[1]	2	1 (☝)
Room 70 G2[1]	4	2 (☝ , PoE)
Room 70 Panorama[1] / Room Panorama[1]	4	2 (☝ , PoE)
Codec Plus	2	1 (☝)
Codec Pro	4	2 (☝ , PoE)
Boards	0	0
Webex Desk	0	0
Desk Pro / Desk Limited Edition[2]	1	0

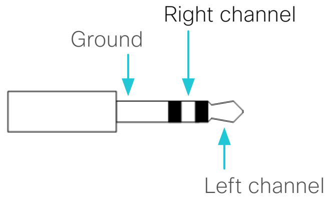
---

[1] One or more of the auxiliary ports on this product is reserved for internal use.

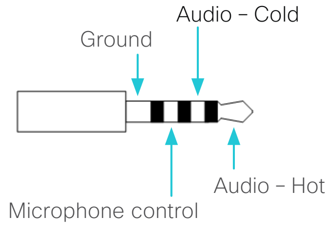
[2] The auxiliary port on this product is a network expansion port. You can connect a computer or other device to this port and get access to the same network/LAN as the video conferencing device itself. This port is not used for peripheral devices, and you don't get a local IP address from the codec.

Mini-jack connector pin-out schemes

3.5 mm mini-jack, 3-pin *(line-out)*



3.5 mm mini-jack, 4-pin *(microphone)*



Audio connectors (mini-jack) *		
	Microphone	**Line-out**
Connector pin out	Tip = Hot Ring 1 = Cold Ring 2 = Mic. control Shield = GND	Tip = Left channel Ring = Right channel Shield = GND
Signal type	Balanced	Unbalanced
Connector (codec)	Mini-jack 3.5 mm, 4-conductor	Mini-jack 3.5 mm, 3-conductor
Input impedance	900 Ohm/leg	N/A
Output impedance	N/A	470 Ohm
Maximum input level	-18.3 dBu ±2 dB	N/A
Maximum output level	N/A	8.2 dBu ±2 dB
Phantom power	10 V ± 0.5 V	N/A
Phantom power resistor pin ”tip”	1.0 kOhm	N/A
Phantom power resistor pin ”ring 1”	1.0 kOhm	N/A
Frequency response	20 Hz-20 kHz ±1 dB	20 Hz-20 kHz ±1 dB
Signal to Noise Ratio	-95 dB	-100 dB

---

* *Boards, Desk Pro, and Desk Limited Edition:* These devices have a mini-jack socket only for line-out.

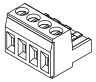
Webex Desk don't have any mini-jack connector.

Audio inputs and outputs (page 1 of 2)

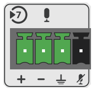
Audio inputs

The audio inputs can be used as both microphone and line inputs, because you can adjust the gain and switch on or off phantom power on each input individually. Use the following settings:

- *Audio > Input > Microphone [n] > Level*: Adjust the gain on the input connector to suit the connected audio source. The gain can be tuned from 0 to 70 dB in steps of 1 dB. The maximum input level with 0 dB gain is 24 dBu.
- *Audio > Input > Microphone [n] > PhantomPower*: In the default configuration, there is phantom power on the input (48 V ± 1 V). This required for some microphones, such as the Cisco table and ceiling microphones. You can switch off the phantom power when connecting to equipment that don't need it, such as external mixers.

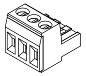


The audio inputs are configured for the use of Euroblock connectors with up to 4 ports.



If you use a Euroblock with 3 ports make sure it is inserted in the leftmost position possible. That is, port 4 (microphone mute) is not used.

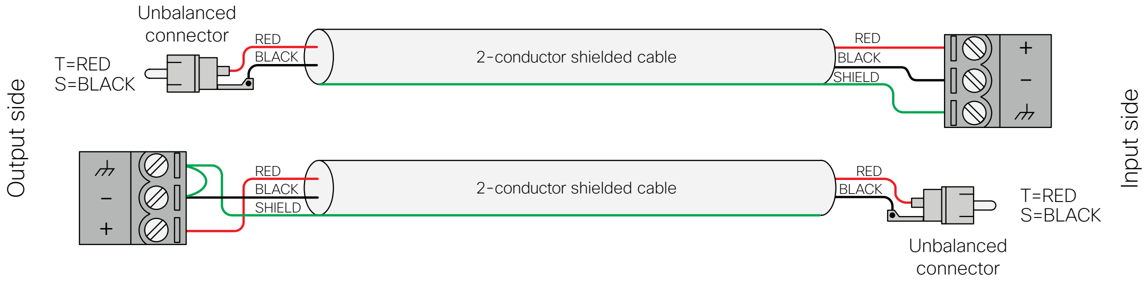
Audio outputs



The audio outputs are configured for the use of Euroblock connectors with 3 ports.

Connecting to unbalanced connectors

These illustrations show best practice when connecting the video conferencing device to unbalanced connectors.


Output side
Unbalanced connector
T=RED
S=BLACK
RED
BLACK
2-conductor shielded cable
RED
BLACK
SHIELD
+
–
Input side
RED
BLACK
SHIELD
2-conductor shielded cable
RED
BLACK
–
+
T=RED
S=BLACK
Unbalanced connector

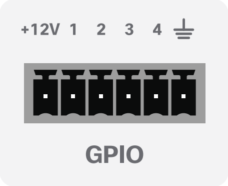
Audio inputs and outputs (page 2 of 2)

Audio input/output specification		
	Microphone/Line Input	**Line Output**
Connector type	• Balanced input • 3.5 mm pitch Phoenix/Euroblock type male header	• Impedance-balanced output • 3.5 mm pitch Phoenix/Euroblock type male header
Phantom Power	• 48 V, 6.8 kohm impedance / 7 mA max current per leg. • Independently switchable.	N/A
Input Impedance	• 2.5 kohm per leg	N/A
Output Impedance	N/A	• 200 ohm per leg
Recommended Load Impedance	N/A	• > 600 ohm
Signal Level	• 0 dB input gain: 24 dBu max. (1 kHz, +/-1 dB) • Input gain independently adjustable from 0 dB to + 70dB in 1 dB steps	• 0 dB output gain: 18 dBu max. (1 kHz, +/-1 dB) • Output gain independently adjustable from 0 to -24 dB in 1 dB steps
Frequency Response	• 20 Hz–20 kHz: +0/-1 dB	• 20 Hz–20 kHz: +0/-0.5 dB
Total Harmonic Distortion + Noise (THD+N)	• 0 dB input gain, 22 dBu signal level: < 0.005% (20 Hz-20 kHz, 22 kHz BW) • 46 dB input gain, -24 dBu signal level: < 0.01% (20 Hz-20 kHz, 22 kHz BW)	• 0 dB output gain, 17 dBu signal level: < 0.005% (20 Hz-20 kHz, 22 kHz BW)
Equivalent Input Noise (EIN)	• 46 dB input gain, Rs=150 ohm: < -124 dBu (20 Hz-20 kHz A-weighted)	N/A
Dynamic Range	• 0 dB input gain, Rs=150 ohm: > 107 dB (20 Hz-20 kHz, 22 kHz BW) • 46 dB input gain, Rs=150 ohm: > 102 dB (20 Hz-20 kHz, 22 kHz BW)	• 0 dB output gain: > 109 dB (20 Hz-20 kHz un-weighted)
Crosstalk	• 0 dB input gain, 23 dBu signal level, 10 kHz: < -110 dB • 46 dB input gain, -23 dBu signal level, 10 kHz: < -110 dB	• 0 dB output gain, 17 dBu signal level 10 kHz: < -100 dB

The GPIO and 3G-SDI connectors

GPIO connector

The device has one 6-pin Euroblock GPIO (General Purpose Input/Output) port with GND, +12V, and 4 GPIO pins.



You can configure the mode for the four GPIO pins individually. A pin can be configured to trigger an action (input) or to report some status of the device (output). For example:

- Mute the microphones (input), or report whether the microphones are muted (output).
- Accept or disconnect a call (input), or report whether the device is in a call (output).

Operating principles

The +12V pin provides +12V_{DC}, and it is capable of sourcing up to 500mA.

The GND pin is a common ground for all pins in the GPIO connector.

When used as input, a GPIO pin detects state as follows:

- Low state for voltages 0-1V_{DC}
- High state for voltages 2-12V_{DC}

When used as output, a GPIO pin is set as follows:

- Low state will drive a pin low, i.e. to GND
- High state will set a pin to open-drain with internal pull-up, i.e. it will set the pin to 12V unless an external connection drives it low

Commands and configurations

To set the mode of a pin:

Read the description of the setting for more details about the pre-defined input and output modes:

- *GPIO > Pin [n] > Mode*
  `(xConfiguration GPIO Pin [n] Mode)`

To retrieve the state of a pin:

- *GPIO > Pin [n] > State*
  `(xStatus GPIO Pin [n] State)`

To set the state of a pin that is in manual mode:

- `xCommand GPIO ManualState Set`

For more information about the API commands, see the API guide for RoomOS software. Go to ► https://www.cisco.com/go/room-docs

3G-SDI connector

The Codec Pro has one 3G-SDI input connector.

The connector is HD-BNC, supporting resolutions up to 1080p60. The 3G-SDI signal is Level A, 75 Ω, 10-bit data native color encoding 4:2:2 YCbCr.

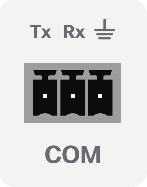
Use the 3G-SDI connector if you want to place a camera far away from the codec - for example, in bigger rooms where you want to have a camera in the back.

Since the total coaxial cable length can be up to 100m, it allows extra flexibility when building or setting up a video conferencing room.

API access using the COM port

The device has a COM port that you can use to access the device's API over a serial connection. [*]

It is a 3 pin Euroblock, with Tx (transmit), Rx (receive), and GND pins.



Serial communication is enabled by default. Use the following configuration if you want to disable it:

SerialPort > Mode

For security reasons, you are asked to sign in before using the serial interface. Use the following setting if you want to switch off the sign in prompt:

SerialPort > LoginRequired

The device can give very much feedback, so we recommend keeping the connection at the highest baud rate possible. In some situations, such as when using long cables, a lower rate may be used to avoid bit errors. Use the following setting if you want to adjust the baud rate.

SerialPort > BaudRate

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

The parameters for the serial connection are:

- Baud rate: 9600, 19200, 38400, 57600, or 115200 bps
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

The same set of configurations and parameters are used for the micro-USB maintenance port, except for the baud rate. The baud rate for the maintenance port is always 115200 bps.

---

[*] Don't use the COM port for maintenance; use the micro-USB port instead.

Serial interface for maintenance (page 1 of 4)

Use the micro USB connector for direct communication with the device[1]. 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[2].

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

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

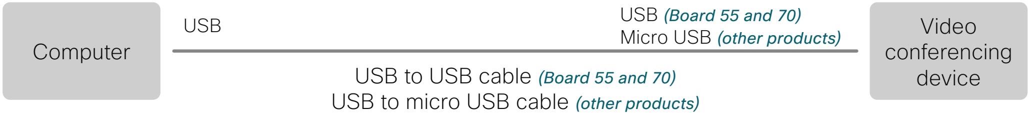
For security reasons, you are asked to sign in before using the serial interface. Use the following setting to change the behavior:

SerialPort > LoginRequired

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

Codec Pro, Room 70 G2, Room 70 Panorama, and Room Panorama

- The *SerialPort > BaudRate* setting has no effect on the maintenance port. The maintenance port always uses the default baud rate.


Computer
USB
USB *(Board 55 and 70)*
Micro USB *(other products)*
Video conferencing device
USB to USB cable *(Board 55 and 70)*
USB to micro USB cable *(other products)*

ⓘ See the illustrations on the following pages to find the micro USB maintenance port the different products.

Webex Board 55S, 70S, and 85S:

1. Connect a USB cable from a computer to the micro-USB port on the board.

   You will see two USB to Serial Port devices on your computer. The names depend on the operating system of the computer. On Linux, you typically see `/dev/ttyUSB0` for the camera and `/dev/ttyUSB1` for main.

   These ports are connected to the native serial interface (UART) on the two CPUs. They show everything printed by the system to this port, including logs from bootloaders.

2. Sign in with admin credentials when you get the sign-in prompt after bootup is completed. You can only sign in to the main CPU, not to the camera CPU.

   After signing in, you have access to the API of the board.

   If your board has been factory reset, the sign-in is *admin* with an empty password.

Webex Board 55 and 70:

1. Connect a USB cable from your computer to the USB-A port on the board. On Webex Board 55, use the USB port closest to the panel.

2. Power up the board. You will see the virtual serial port on the computer. Its name depends on the operating system of the computer. On Linux, you typically see `/dev/ttyACM0`.

   NOTE: If you power up the board before you connect the computer, the computer can't see the board

3. Sign in with admin credentials when you get the sign-in prompt. After signing in, you have access to the API of the board.

   If your board has been factory reset, the sign-in is *admin* with an empty password.

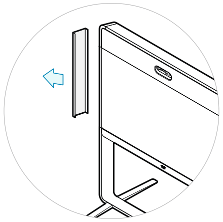
---

[1] The micro-USB port is for maintenance. If you want to access the device's API over a serial connection, refer to the API guide for details.

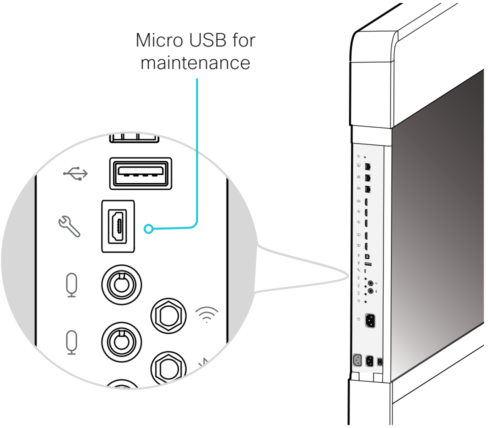
[2] You need a CP210x USB to UART Bridge Virtual COM Port (VCP) driver, see ▶ http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers

Serial interface for maintenance (page 2 of 4)

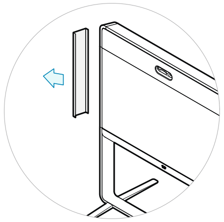
Room 55 Dual and Room 70



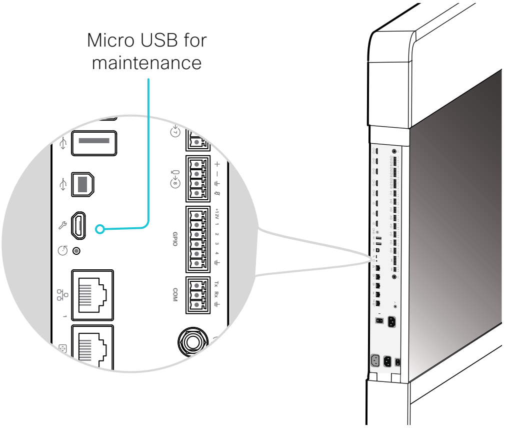
Remove the left side cover of the device to get access to the codec connector panel. The cover snaps to magnets.



Room 70 G2 and Room 70 Panorama



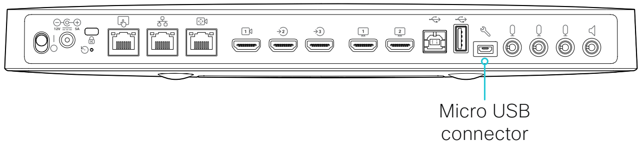
Remove the left side cover of the device to get access to the codec connector panel. The cover snaps to magnets.



Boards
Codec Plus
Codec Pro
Desk, Desk LE, Desk Pro
Room Kit
Room Kit Mini
Room 55
Room 55 Dual
Room 70
Room 70 G2
Room 70 Panorama
Room Panorama

Serial interface for maintenance (page 3 of 4)

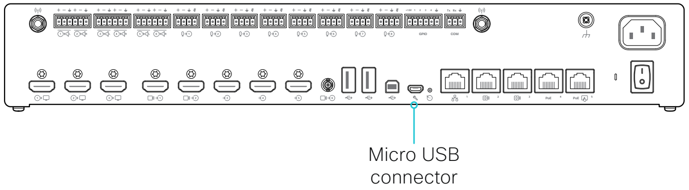
Codec Plus


Micro USB connector

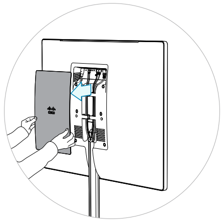
Codec Pro and Room Panorama

For Room Panorama:

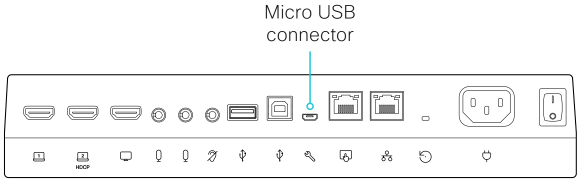
- Use the handle at the bottom of the deco grille, and pull down the left monitor to get access to the codec.


Micro USB connector

Room 55

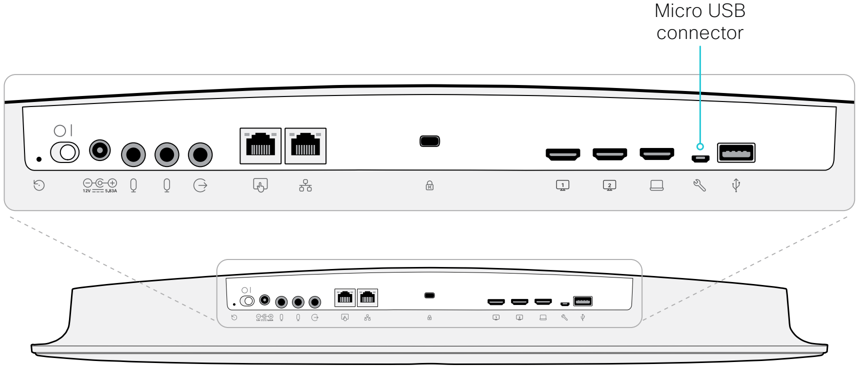


Remove the rear cover to get access to the connector panel.


Micro USB connector

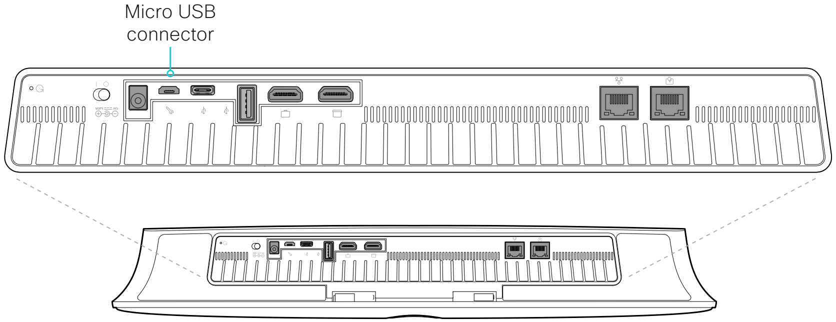
Room Kit

Tilt the unit forward to get access to the connector panel.


Micro USB connector

Room Kit Mini

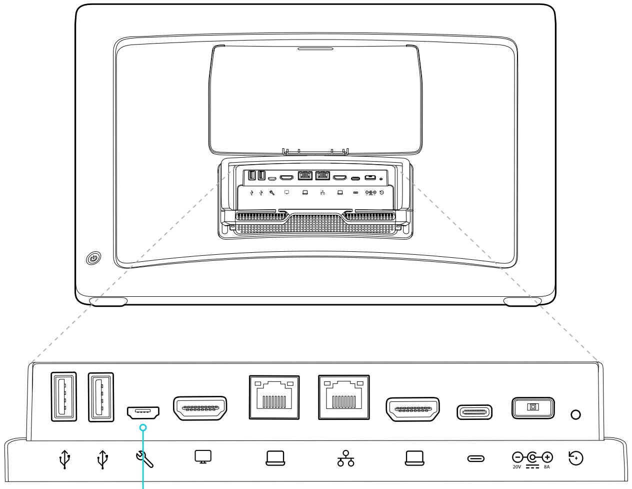
Tilt the unit forward to get access to the connector panel.


Micro USB connector

Serial interface for maintenance (page 4 of 4)

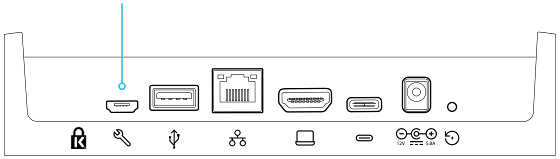
Desk Pro and Desk Limited Edition

Flip the cover on the back of the device to get access to the connector panel.



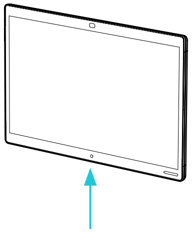
Desk Pro and Desk Limited Edition

Micro USB connector

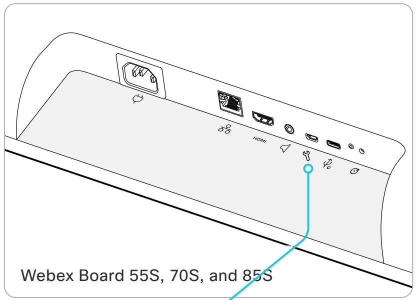


Webex Desk

Webex Boards



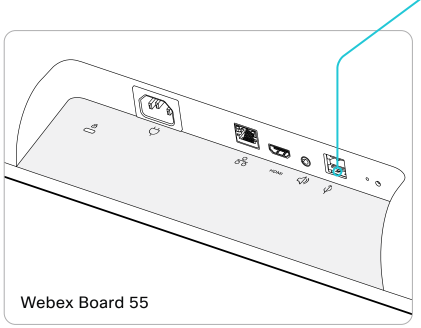
The connector panel is at the bottom, rear side.



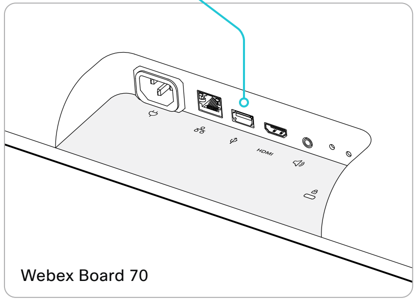
Webex Board 55S, 70S, and 85S

Micro USB connector

USB connector



Webex Board 55



Webex Board 70

The systemtools commands

The systemtools commands are used for administrative control of the device and are only available from a command line interface. Systemtools should not be used to program the device.

To get an overview of the supported commands type "systemtools ?".

Example:

```
systemtools ?
selectsw
whoami
license
network
ntp
ps
securitystatus
bootlogo
idefixversion
touch
```

To see the usage of the commands add a question mark after the command.

Example:

```
systemtools network ?
usage: network ping <hostname> | traceroute
<hostname> | netstat | addrs | ifconfig |
ifstats <ifname>
```

`systemtools bootlogo`

Shows the current bootlogo setting.

`systemtools bootlogo off`

Disables display of the Cisco boot screen when the video device is booting. The command is persistent over a factory reset.

`systemtools bootlogo on`

Reverts back to showing the Cisco boot screen when the video device is rebooting. The command is persistent over a factory reset.

`systemtools idefixversion`

(not for Webex Desk, Desk Pro, and Desk Limited Edition)

Returns the software version a connected Touch 10 should have.

`systemtools license list`

Lists all the licenses for the device.

`systemtools license show <name>`

Shows the content of a license file, defined by the name.

<name>: The name of the license file.

`systemtools network ping <hostname>`

Network debug command.

<hostname>: The IP-address or URL of the host.

`systemtools network traceroute <hostname>`

Network debug command.

<hostname>: The IP-address or URL of the host.

`systemtools network netstat`

Network debug command.

`systemtools network addrs`

Shows the device's IP-addresses.

`systemtools network ifconfig`

Network debug command.

`systemtools network ifstats <ifname>`

Network debug command. Prints out network interface statistics.

<ifname>: The name of the interface.

`systemtools ntp`

Shows the NTP status.

`systemtools ps`

Lists all running processes.

`systemtools securitystatus`

Shows the security status for the device.

`systemtools selectsw`

Select which of the available software images to use. Changing the software image will restart the device.

No argument given: Lists the version of the available software images, and shows which one is active.

image name: Swap to the software with this name.

`systemtools touch start`

(only for Desk Pro, Desk Limited Edition, and Boards)

Debug command for testing the touch screen.

`systemtools touch stop`

(only for Desk Pro, Desk Limited Edition, and Boards)

Debug command for testing the touch screen.

`systemtools touch forever`

(only for Desk Pro, Desk Limited Edition, and Boards)

Debug command for testing the touch screen.

`systemtools whoami`

Lists the name and id of the signed in user, and the user roles held by this user.

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.

You can configure the the device settings from the web interface of the device. Open a web browser, enter the IP address of the device, and sign in. Go to *Settings*, and select *Configurations*.

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

Applies to all except Webex Desk, Desk Pro, and Desk Limited Edition

You can close the port by setting remote pairing for the touch controller to **Off**.

`Peripherals Pairing CiscoTouchPanels RemotePairing: Off / On`

TCP 4045: Remote pairing version information

Applies to all except Webex Desk, Desk Pro, and Desk Limited Edition

You can close the port by setting remote pairing for the touch controller to **Off**.

`Peripherals Pairing CiscoTouchPanels RemotePairing: Off / On`

TCP 4047: Remote pairing session connection

Applies to all except Webex Desk, Desk Pro and Desk Limited Edition

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 controller to **Off**.

`Peripherals Pairing CiscoTouchPanels RemotePairing: Off / On`

TCP 4051: Remote pairing port *(Deprecated)*

You can close the port by setting remote pairing for the touch controller to Off.

`Peripherals Pairing CiscoTouchPanels RemotePairing: Off / On`

TCP 4062: Remote pairing port

You can close the port by setting remote pairing for the touch controller to Off.

`Peripherals Pairing CiscoTouchPanels RemotePairing: Off / On`

TCP 4190: UPnP port

You can close the ports by setting the SIP listen ports to **Off**.

`NetworkServices UPnP Mode: Off`

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`

Ephemeral IP ports

Ephemeral IP port range: 32768 - 60999

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

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[1], and media services remain on-premises. You can manage the cloud services and get device diagnostics in Webex Control Hub.

More detailed information

To find more details about how to link a device to Webex Edge for Devices, supported features, prerequisites, and limitations, read the ▶ Webex Edge for Devices (https://help.webex.com/cy2l2z/) **article on Webex Help Center.**

Set-up

We recommend that you register the device to the on-premises service first; then you link it to the Webex Edge.

Find details in the *Webex Edge for Devices* article referenced to the left.

Features

Find a comprehensive list of features and functionality in the *Webex Edge for Devices* article referenced to the left. Some of them are:

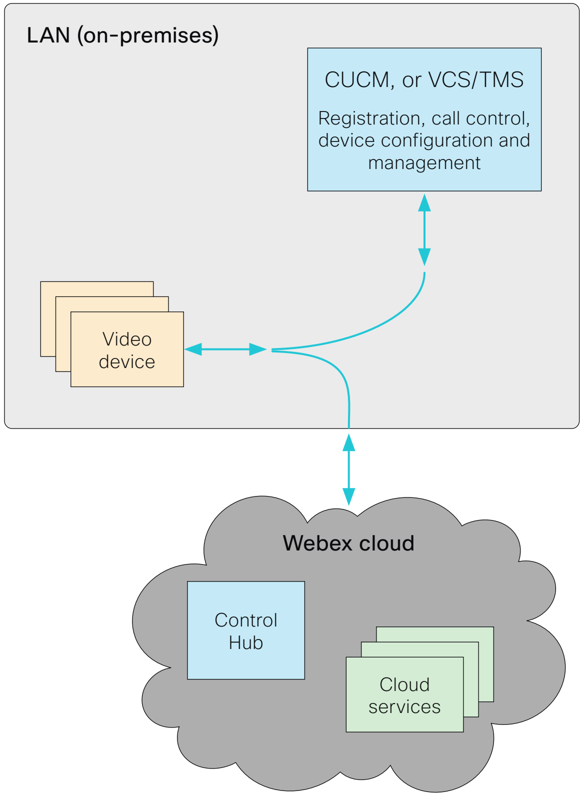
- Online/Offline connection status in Control Hub
- Device diagnostics with the ability to set administrator alerts
- Device historical analytics available directly in Control Hub
- Access to device settings from Control Hub
- Cloud xAPI access
- Real time media metrics when joining Webex calls
- Manage logs from Control Hub
- Hybrid calendar through Control Hub [2]
- Webex Assistant (voice-driven virtual assistant)

The *Webex Edge for Devices* article referenced above has an updated list of all available features and limitations.

Prerequisites

Find a comprehensive list of prerequsites and limitations in the *Webex Edge for Devices* article referenced to the left. Some of them are:

- Encrypted version of RoomOS or CE software
- If registered to CUCM: CUCM version 12.5su1, or 11.5.x with the latest device pack
- Control Hub administrator access
- Cisco Webex Device Connector (to set up the link to Webex Egde)
- A cloud services license (Cisco Collaboration Flex Plan)



---

[1] You can configure the device to use the Webex cloud service for calling into Webex meetings. For details, read the ▶ Webex Optimized Experience for Webex Edge for Device (https://help.webex.com/c31fqg/) article on Webex Help Center.

[2] TMS based bookings will be ignored.

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.

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.

Create an activation code

To register a device to Cisco Webex, you need an activation code.

Devices in shared mode:

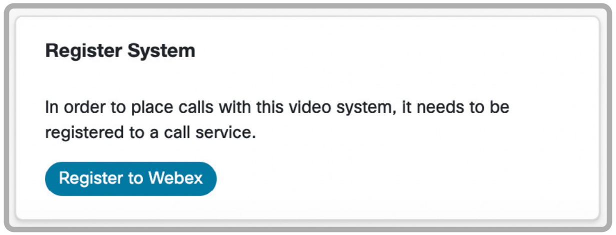
> An administrator has to create an activation code on Control Hub.
>
> To learn how to create an activation code for devices in shared mod, see ► Create a Workspace and Add Services for a Cisco Webex Room Device or a Cisco Webex Board (https://help.webex.com/1mqb9cb/).

Devices in personal mode:

> From *Cisco Webex Settings (https://settings.webex.com)*, you can get your activation code without having to be an administrator.
>
> To learn how to create an activation code for devices in personal mode, see ► Set Up a Webex Board, Room or Desk Device as a Personal Device (https://help.webex.com/n3alqtv/).

1. Sign in to the web interface and go to *Home*. Find the *Register System* card.

   This card is only available if the device is not registered to a service already.



Register System

In order to place calls with this video system, it needs to be registered to a call service.

2. Click *Register to Webex*.
3. A pop-up appears and you can enter the activation code.

   Format:
   - *xxxx-xxxx-xxxx-xxxx*, or
   - *xxxxxxxxxxxxxxxx*
4. 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).

RoomOS software supports a range of RFCs, including the following:

- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3263 Locating SIP Servers
- RFC 3361 DHCP Option for SIP Servers
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
- RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
- RFC 4582 The Binary Floor Control Protocol

  draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5321 Simple Mail Transfer Protocol *(Boards, Webex Desk, Desk Pro, and Desk Limited Edition)*
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

Calculating minimum bandwidth

The minimum bandwidth requirements are specified in the technical specifications. When dual-stream is used, the available bandwidth is split into two streams.

To calculate the minimum bandwidth for a desired resolution in dual-stream, double the minimum bit rate (bps) for that resolution (e.g., 720p30).

For example, if there is a minimum bandwidth of 768 kbps for the resolution 720p30. Then, the dual-stream minimum bandwidth will be 768 × 2, or 1536 kbps.

User documentation on the Cisco web site

Use the following short-links to find the documentation for the product series running RoomOS software.

Room Series:

▶ https://www.cisco.com/go/room-docs

Desk Series:

▶ https://www.cisco.com/go/desk-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/c/en/us/support/collaboration-endpoints

The documents are organized in the following categories - some documents are not available for all products:

Install and Upgrade > Install and Upgrade Guides

- *Installation guides:* How to install the product
- *Getting started guide:* Initial configurations required to get the device up and running
- *RCSI guide:* Regulatory compliance and safety information

Maintain and Operate > Maintain and Operate Guides

- *Getting started guide:* Initial configurations required to get the device up and running
- *Administrator guide:* Information required to administer your product
- *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

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. Some features are not available for all types of products.

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 > 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.