

Collaboration Endpoint software version 9.8  
JULY 2019



# Administrator guide

for Cisco Webex Boards

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/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

<b>Introduction</b> .....	<b>4</b>
User documentation and software .....	5
Webex Boards at a glance.....	6
Power On and Off .....	8
How to administer the video conferencing device .....	9
<b>Configuration</b> .....	<b>13</b>
User administration .....	14
Change the device passphrase.....	15
Restrict the access to the Settings menu.....	16
Device configuration .....	17
Add a sign in banner .....	18
Add a welcome banner.....	19
Manage the service certificates of the device .....	20
Manage the lists of trusted certificate authorities - CAs.....	21
Set up secure audit logging.....	25
Delete CUCM trust lists.....	26
Change the persistency mode.....	27
Set strong security mode .....	28
Set up an SMTP email server .....	29
Set up Intelligent Proximity for content sharing .....	30
Adjust the video quality to call rate ratio.....	35
Add corporate branding to the screen and Touch 10 user interface .....	37
Choose a ringtone and set the ringtone volume .....	39
Manage the Favorites list.....	40
Set up accessibility features.....	41
Provisioning of product specific configurations from CUCM.....	42
<b>Peripherals</b> .....	<b>44</b>
Connect an input source.....	45
Information about 4K resolution.....	47
Information about HDMI cables.....	48
Set up the Best overview feature .....	49
Connect the Touch 10 controller .....	50
Connect the ISDN Link.....	53
<b>Maintenance</b> .....	<b>54</b>
Upgrade the device software .....	55
Add option keys .....	56
Device status .....	57

Run diagnostics.....	58	UserManagement settings.....	140
Download log files.....	59	Video settings .....	142
Access the Technical support screen .....	60	Experimental settings .....	149
Create a remote support user .....	61	<b>Appendices.....</b>	<b>150</b>
Backup and restore configurations and custom elements .....	62	How to use Webex Board .....	151
CUCM provisioning of custom elements .....	63	How to use Touch 10 .....	152
TMS provisioning of custom elements.....	64	Set up remote monitoring .....	153
Revert to the previously used software image .....	65	Access call information and answer a call while using the web interface.....	154
Factory reset the video conferencing device .....	66	Place a call using the web interface .....	155
Factory reset Cisco Touch 10.....	69	Share content using the web interface.....	157
Factory reset Cisco TelePresence Touch 10.....	70	Control a far end camera.....	158
Capture user interface screenshots .....	71	Packet loss resilience - ClearPath.....	159
<b>Device settings .....</b>	<b>72</b>	Room analytics.....	160
Overview of the device settings .....	73	Customize the video conferencing device's user interface.....	162
Audio settings .....	78	Customize the video conferencing device's behavior using macros .....	164
CallHistory settings .....	80	Remove default buttons from the user interface .....	165
Cameras settings.....	81	Sending HTTP(S) requests .....	166
Conference settings .....	83	Presentation source composition .....	167
FacilityService settings.....	88	Manage startup scripts .....	169
H323 settings.....	89	Access the device's XML files .....	170
HttpClient settings .....	92	Execute API commands and configurations from the web interface .....	171
Logging settings .....	93	Connector panel .....	172
Macros settings .....	95	About Ethernet ports.....	173
Network settings.....	96	Mini-jack connector pin-out schemes.....	174
NetworkServices settings.....	104	Serial interface for maintenance for Webex Board 55S, 70S, and 85S.....	175
Peripherals settings .....	113	Serial interface for maintenance for Webex Board 55 and 70 .....	176
Phonebook settings .....	114	Open TCP Ports.....	177
Provisioning settings.....	115	HTTPFeedback address from TMS.....	178
Proximity settings.....	118	Register a device to the Cisco Webex cloud service .....	179
RoomAnalytics settings .....	119	Supported RFCs .....	180
RoomReset settings.....	120	Technical specification.....	181
RTP settings.....	121	User documentation on the Cisco web site.....	183
Security settings .....	122	Cisco contacts .....	184
SerialPort settings.....	125		
SIP settings.....	126		
Standby settings .....	130		
SystemUnit settings.....	131		
Time settings .....	132		
UserInterface settings.....	135		

## Chapter 1

# Introduction

## User documentation and software

### Products covered in this guide

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

### User documentation

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

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

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

### Documentation on the Cisco web site

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

► <https://www.cisco.com/go/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

Download software for the endpoint from the Cisco web site:

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

We recommend reading the Software release notes (CE9):

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

## Webex Boards at a glance (page 1 of 2)

The Webex Board includes a 4K camera, a capacitive touch interface, built-in microphones and speakers that integrate with a high-resolution 4K screen. The Webex Board is a powerful audio and video conferencing device, but can also be used as a wireless presentation screen and a digital whiteboard. The Webex Board helps teams collaborate in physical meeting rooms, but also securely connects to virtual meeting spaces to facilitate a continuous workflow.

The Webex Board is available in three different screen sizes:

- **Webex Board 55 and 55S** with a 55" LED screen. Designed for huddle and small spaces up to 5 people.
- **Webex Board 70 and 70S** with a 70" LED screen. Designed for small to large meetings rooms up to 8 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.

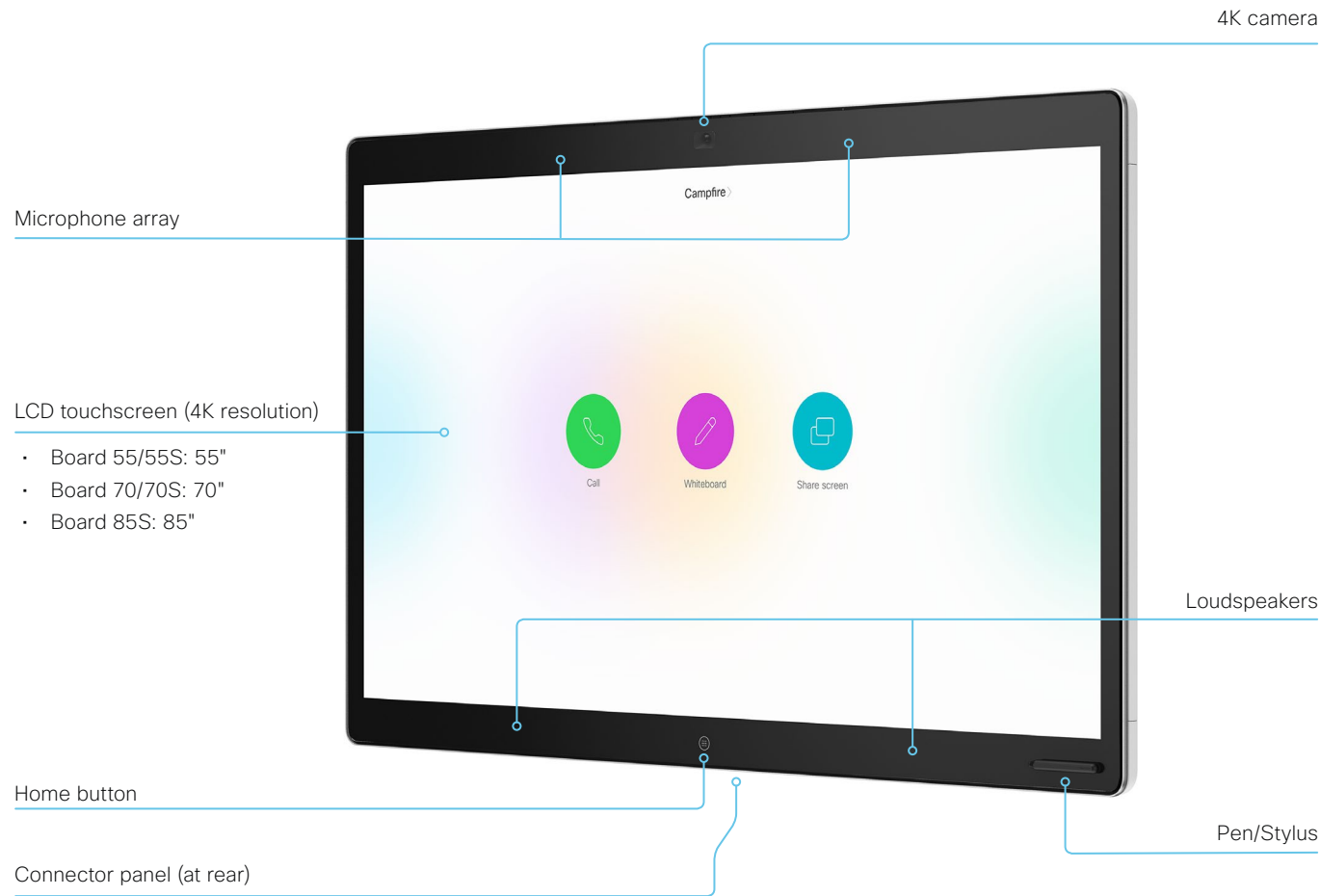
You can find more information about the Cisco Webex Board at ► <https://www.cisco.com/go/webexboard>



## Features and benefits

- **Easy sharing:** Wired or wireless content sharing.
- **Digital whiteboard:** Whiteboard-function that lets you automatically save whiteboards to a Cisco Webex Teams space or send them by email. Possibility to annotate on screen share.
- **Audio:** Built-in microphones with intelligent voice tracking. Integrated voice optimized speakers providing high-fidelity audio conferencing.
- **Best overview:** Fixed-lens camera capturing virtually the entire room.
- **Speaker tracking:** Detects and switches between active speakers, providing ideal framing.
- **High resolution:** Powerful 4K camera captures high-resolution image.
- **Continuous workflow:** Work can continue from a different location with the Webex Teams app, or from a device, such as another Webex Board.
- **Intuitive navigation:** Touch capability, simple meeting-join experience with one button to push (OBTP).
- **Security:** End to end security.
- **Flexible registration:** Can register on premises or to the cloud through Cisco Webex. The hardware is optimized to run on a cloud platform, for great experiences in shared room and spaces with easy access to host conferences.

# Webex Boards at a glance (page 2 of 2)



## Mounting options



Floor stand



Wall stand



Wall mount

## Power On and Off

### Restart and standby using the user interface

#### Restart the device

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

#### Enter standby mode

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

#### Exit standby mode

- Tap the screen of the Touch controller or the board.

#### Enter halfwake mode and clean up for the next user

- Press and hold for a few seconds the Home button on the board.

#### Exit halfwake mode

- Tap the Home button, the screen of the Touch controller, 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.

For the device to power up, you have to disconnect the power plug and connect it again.



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

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

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

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

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

### Tip

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

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

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

For example:

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

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

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

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

\* The `SerialPort > LoginRequired` setting is on only available on Board 55S, 70S, and 85S. You always have to sign in on the 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 4)

## The web interface of the device

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

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

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

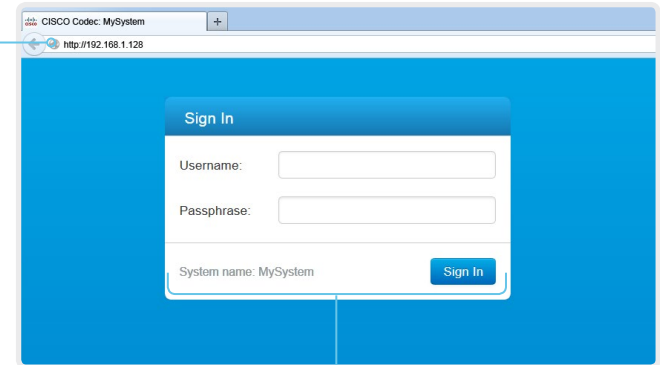
### Connect to the device

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



#### How to find the IP address

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



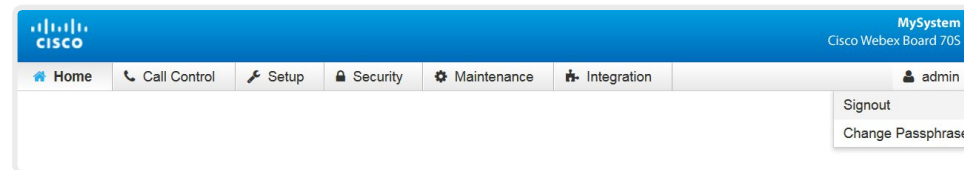
### Sign in

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



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

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



### Sign out

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

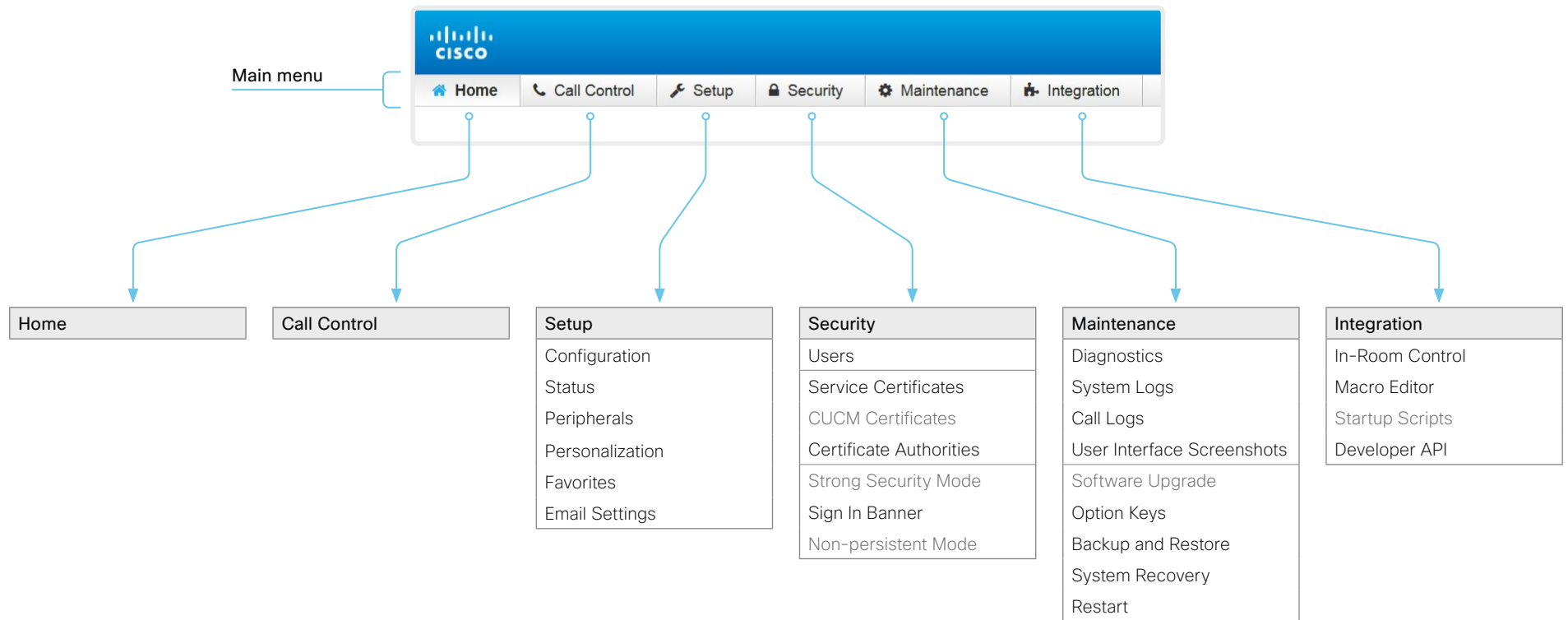
How to administer the video conferencing device (page 3 of 4)

## How the web interface is organized

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

In both cases, a user that is signed in, sees only the pages that he has access rights for.

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



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

## Settings and device information on the user interface


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

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

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

### Access Settings

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

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

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

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

In this context, the board and the Touch controller operate independently. If you unlock the settings by signing in on one of them, it has no effect on the other.

## Chapter 2

# Configuration

## User administration

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

### The default user account

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



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

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

### Create a new user account

1. Sign in to the web interface and navigate to [Security > Users](#).
2. Click [Add new user...](#)
3. Fill in the *Username*, *Passphrase* and *Repeat passphrase* input fields.  
As a default, the user has to change the passphrase when he signs in for the first time.  
Fill in the *Client Certificate DN* (Distinguished Name) field only if you use client certificates for authentication.
4. Check the appropriate *Roles* check boxes.  
If you assign the ADMIN role to a user, enter your own passphrase in the *Your passphrase* input field for verification.
5. Set the *Status* to **Active** to activate the user.
6. Click [Create User](#).  
Use the [Back](#) button to leave without making any changes.

### Edit an existing user account

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

#### Change the user privileges

1. Sign in to the web interface and navigate to [Security > Users](#).
2. Click the appropriate user in the list.
3. Choose user roles, set the status to **Active** or **Inactive**, and decide if the user has to change the passphrase on the next sign in.  
Fill in the *Client Certificate DN* (Distinguished Name) field only if you use certificate login on HTTPS.
4. Click [Edit User](#) to save the changes.  
Use the [Back](#) button to leave without making any changes.

#### Change the passphrase

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

#### Delete the user account

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

### User roles

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

These are the *user roles*:

**ADMIN:** A user with this role can create new users, change most settings, make calls, and search the contact lists. The user cannot upload audit certificates and change the security audit settings.

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

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

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

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

## Change the device passphrase

You need to know the device passphrase in order to:

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

### The default user account

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



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

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

### Other user accounts

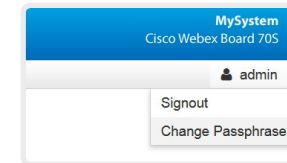
You can create many user accounts for the device.

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

## Change your passphrase

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

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



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

## Change another user's passphrase

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

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

## Restrict the access to the Settings menu

By default, any user has access to the Settings menu on the user interface (both on the board and the Touch controller).

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

### Lock down the Settings menu

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

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

### Unlock the Settings menu

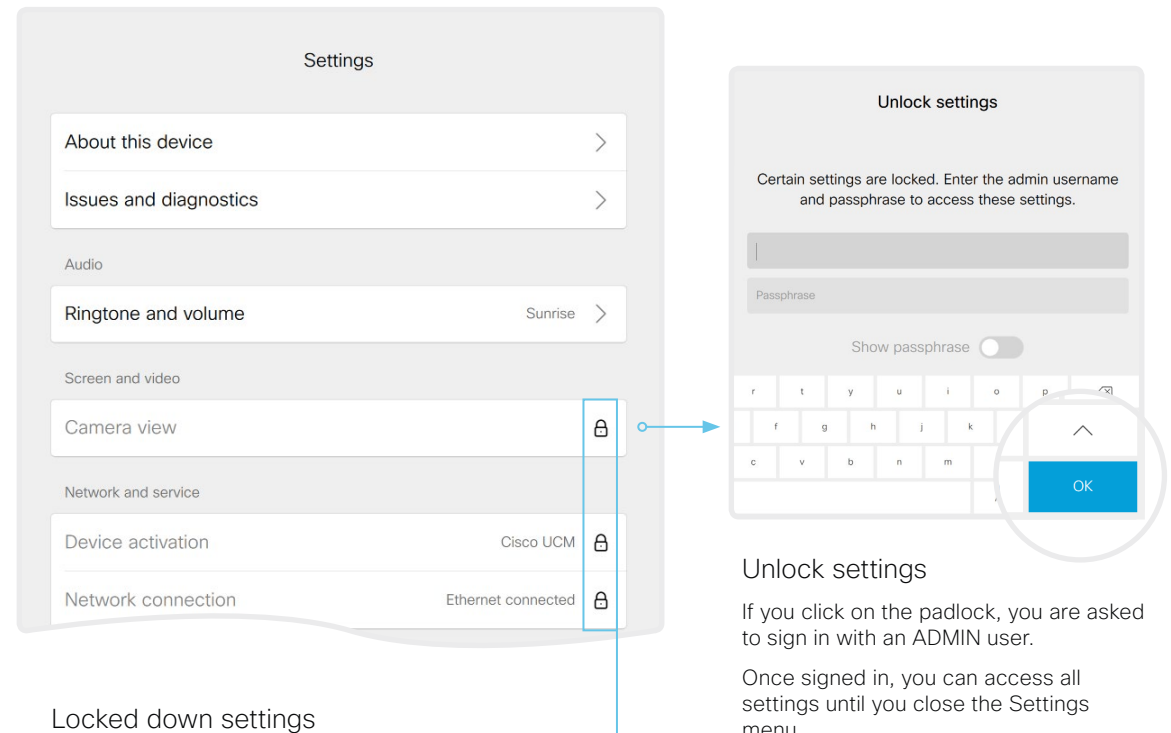
1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Go to [UserInterface > SettingsMenu > Mode](#), and select **Unlocked**.
3. Click [Save](#) for the change to take effect.

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

### The Settings menu on the user interface

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

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



#### Locked down settings

Locked down settings are marked with a padlock.

#### Unlock settings

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

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

In this context, the board and the Touch controller operate independently. If you unlock the settings by signing in on one of them, it has no effect on the other.



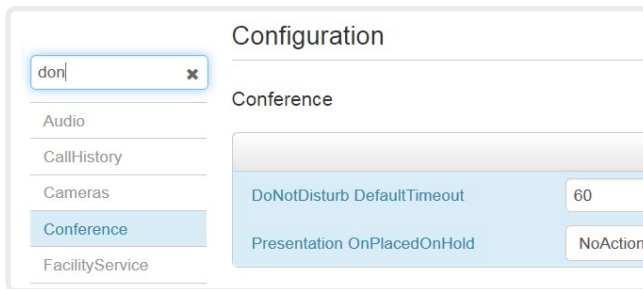
## Device configuration

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

### Find a device setting

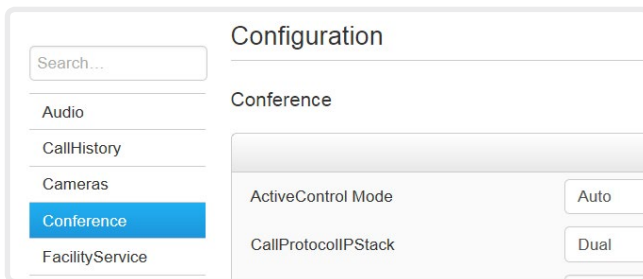
#### Search for settings

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



#### Select a category and navigate to settings

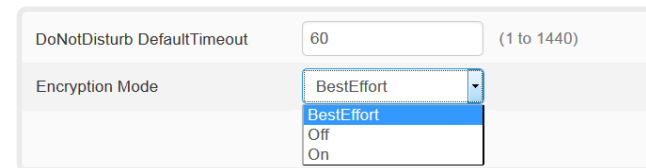
The device settings are grouped in categories. Choose a category in the left pane to show the associated settings.



### Change a device setting

#### Check the value space

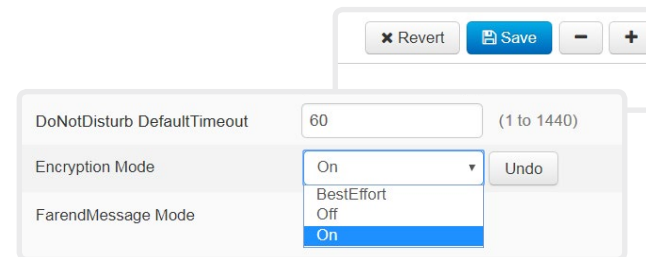
A settings's value space is specified either by text following the input field or in a drop-down list that opens when you click the arrow.



#### Change a value

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

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



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

### About device settings

All device settings can be changed from the web interface.

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

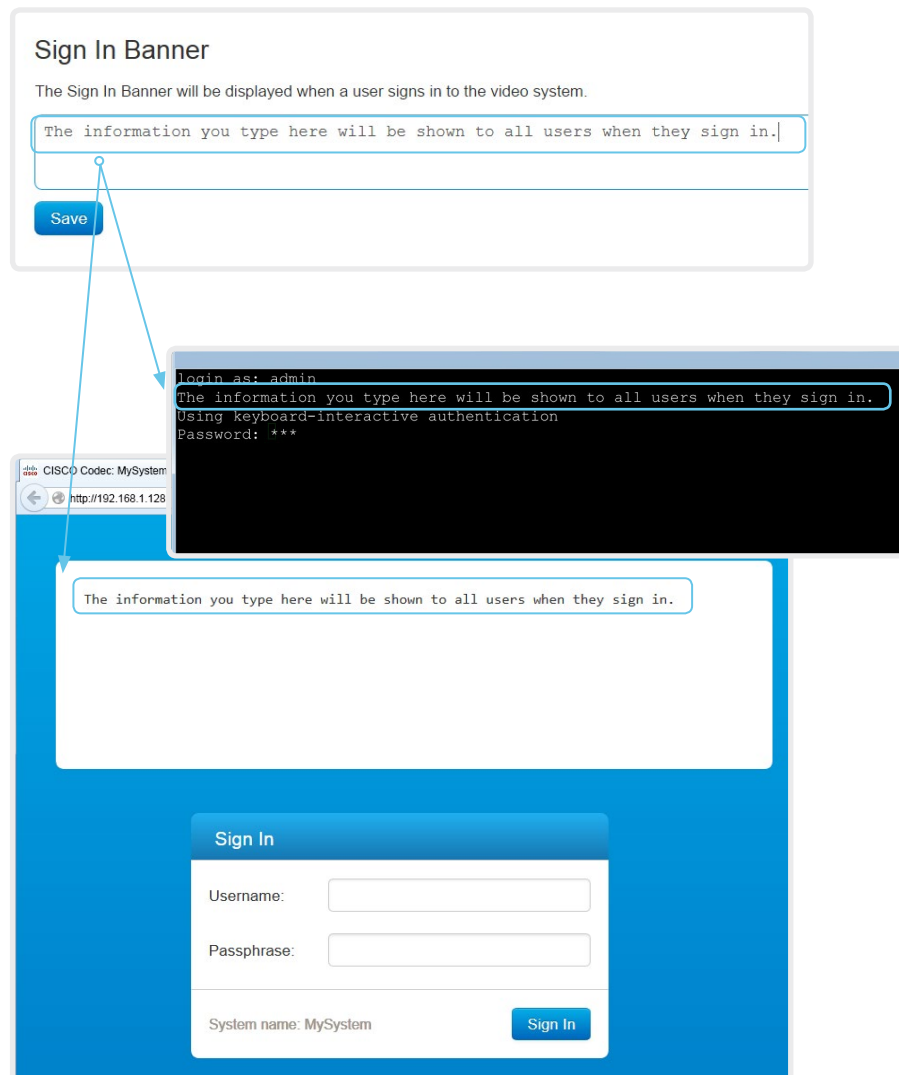
Different settings may require different user credentials. In order to be sure that an administrator is able to change all device settings, an administrator user must possess all user roles.

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

## Add a sign in banner

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

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



### About sign in banner

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

The maximum size is: 4kByte

### Welcome banner versus sign in banner

Sign in banner:

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

Welcome banner:

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

## Add a welcome banner

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

### API commands

```
xCommand SystemUnit WelcomeBanner Set
```

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

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

```
xCommand SystemUnit WelcomeBanner Clear
```

```
xCommand SystemUnit WelcomeBanner Get
```

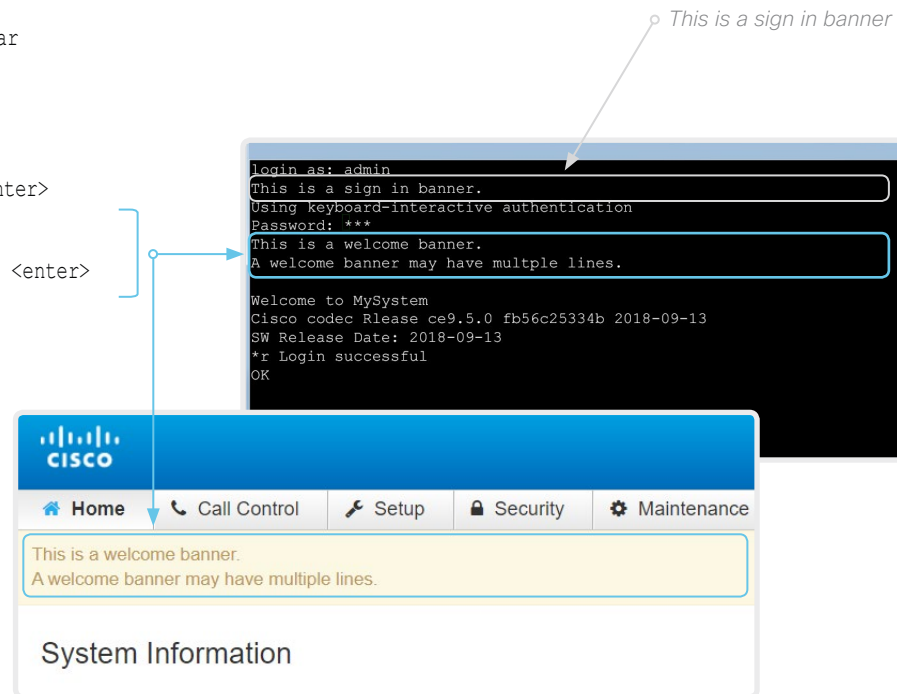
### Example

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

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

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

```
. <enter>
```



### About welcome banner

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

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

The maximum size is: 4 kByte

### Welcome banner versus sign in banner

Sign in banner:

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

Welcome banner:

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

## Manage the service certificates of the device

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

You need the following files:

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

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

### About the service certificates of the device

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

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

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

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

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

If authentication fails, the connection will not be established.

Enable or disable, view or delete a certificate

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

Use the corresponding button to view or delete a certificate.

**Service Certificates**

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

**Add Certificate**

Certificate  No file selected.

Private key (optional)  No file selected.

Passphrase (optional)

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

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

### Add a certificate

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

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

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

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

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

### The CA certificate lists

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

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

These are the CA lists:

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

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

## Manage pre-installed CA certificates for external servers

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

**Certificate Authorities**

Custom Preinstalled Collaboration Edge

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

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

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

### View or disable certificates

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



As an alternative to using the pre-installed certificates, you can append the 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 are 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
- SMTP mail servers

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

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

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

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

**Certificate Authorities**

Custom Preinstalled Collaboration Edge

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

[Configure provisioning now.](#)

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

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

### View or disable certificates

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

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

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

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

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

Only Cisco Expressway infrastructure certificates are checked against this list.

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

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

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

## Upload a CA certificate to the device

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

You need the following file:

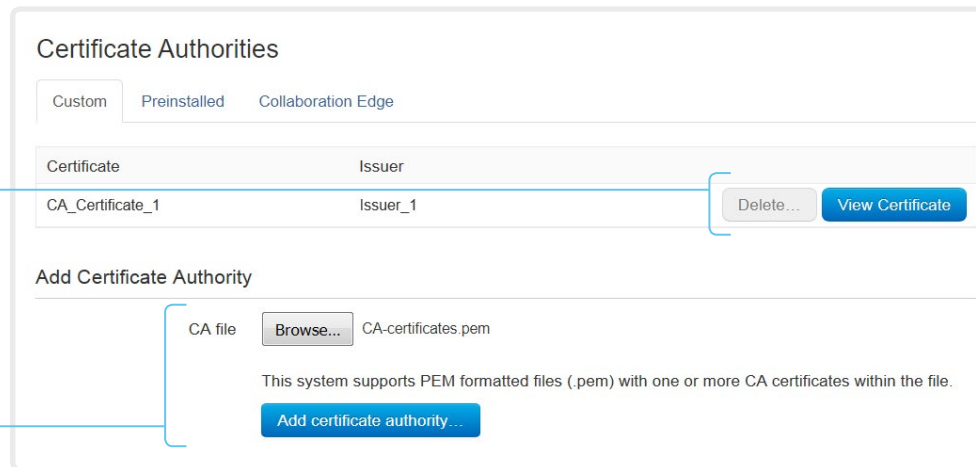
- CA certificate list (file format: .PEM).

### View or delete a certificate

Use the corresponding button to view or delete a certificate.

### Upload a list of CA certificates

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



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



Previously stored certificates are not deleted automatically.

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

### About the custom list of trusted CA certificates

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

If not covered by the lists of pre-installed CA certificates, they can be used for HTTP servers, SMTP servers, and Cisco Expressway infrastructure as well.



## Set up secure audit logging

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



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

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

1. Open the *Security* category.
2. Find the *Audit > Server* settings, and enter the *Address* of the audit server.  
If you set *PortAssignment* to **Manual**, you must also enter a *Port* number for the audit server.
3. Set *Audit > Logging > Mode* to **ExternalSecure**.
4. Click *Save* for the change to take effect.

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

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

Buttons for 'Revert', 'Save', and 'Undo' are visible next to the settings.

### 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 custom CA list.

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


## Delete CUCM trust lists

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

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

### Delete the CUCM trust lists

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

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

In these cases, you must still delete them:

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

### Overview of trust list fingerprints and certificates

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

This information may be useful for troubleshooting.

### More information about trust lists

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

## Change the persistency mode

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

### Check the persistency status

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

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

### Change the persistency settings

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

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

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



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

### Persistency mode

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

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

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

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



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

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

## Set strong security mode

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

### Set strong security mode

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

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

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

### Return to normal mode

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

The device restarts automatically.

### Strong Security Mode

Strong Security Mode is **not** enabled.

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

It will introduce the following:

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

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

### Strong Security Mode

Strong Security Mode is enabled.

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

### About strong security mode

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

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

## Set up 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 and navigate to [Setup > Configuration](#).
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 and navigate to [Setup > Email Settings](#).
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 [Continue to uploading step](#) and follow the wizard instructions to upload the required certificates to the device.
4. Enter the email address from where the whiteboards or annotations will be sent.
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.

### Set up the server manually

1. Sign in to the web interface and navigate to [Setup > Configuration](#).
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 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 Intelligent Proximity for content sharing (page 1 of 5)

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

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



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

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

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

### Proximity services

*Place calls and control the video conferencing device:*

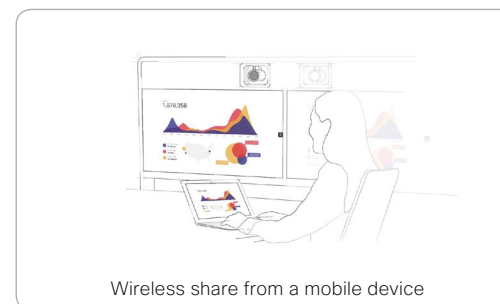
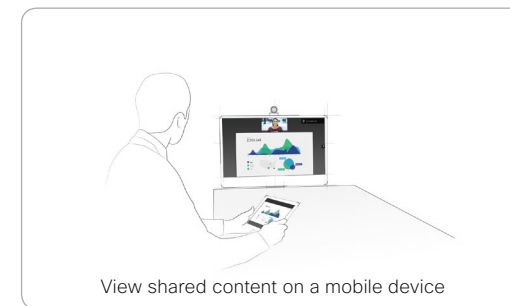
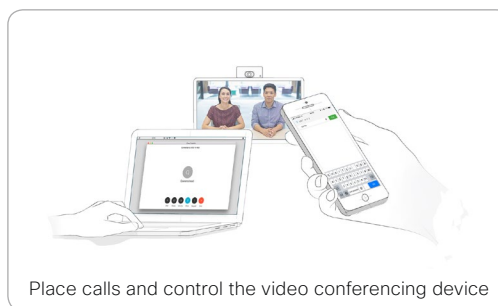
- Dial, mute, adjust volume, hang up
- Available on laptops (OS X and Windows), smartphones and tablets (iOS and Android)

*View shared content on a mobile device:*

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

*Wireless share from a laptop:*

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



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

### Install a Cisco Proximity client

#### Where to find the clients

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

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

#### End-user license agreement

Read the end-user license agreement carefully, ► [https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN\\_.html](https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html)

#### Supported operating systems

- iOS 7 and above
  - Android 4.0 and above
  - Mac OS X 10.9 and above
  - Windows 7 and above
- The tile based interface introduced with Windows 8 is not supported.

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

### Ultrasound emission

Cisco video conferencing devices emit ultrasound as part of the Proximity feature.

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

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

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

*Room 70, Room 70 G2, Room 55, Room 55 Dual, Room Kit, Room Kit Mini, Room Kit Plus, SX10N and MX Series:*

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

*DX70 and DX80:*

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

*Boards:*

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

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

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

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

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

### Headsets

*DX70, DX80, and SX10N:*

You can always use a headset with these devices because:

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

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

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

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

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

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



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

### Enable Proximity services

1. Sign in to the web interface and navigate to [Setup > Configuration](#).
2. Go to [Proximity > Mode](#). Check that Proximity is **On** (default), so that the video conferencing device sends ultrasound pairing messages.

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

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

*Place calls and control the video conferencing device:*

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

*View shared content on a mobile device:*

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

*Wireless share from a desktop client:*

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

### The Proximity indicator



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

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

### About Proximity

The Proximity feature is switched **On** by default.

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

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

Cisco recommends – for the best user experience – that Proximity always is switched **On**\*

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

---

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

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

### Room considerations

#### Room acoustics

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

### About privacy

In the Cisco Privacy statement and the Cisco Proximity Supplement you find information about data collection in the clients and privacy concerns that needs to be considered when deploying this feature in the organization. Refer to:

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

### Basic troubleshooting

#### Cannot detect devices with Proximity clients

- Some Windows laptops are not able to record sound in the ultrasound frequency range (20kHz-22kHz). This can be due to frequency limitations with the sound card, sound driver or the internal microphone of the particular device. Refer to the Support forum for more information.
- Check *Settings > Issues and diagnostics* on the user interface, or *Maintenance > Diagnostics* on the web interface of the video conferencing device. If there are no ultrasound related issues listed ("Unable to verify the ultrasound signal"), ultrasound pairing messages are emitted by the video conferencing device as they should. Refer to the Proximity *Support forum* for further assistance with the client detection issues.

#### Audio artifacts

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

#### Cannot share content from a laptop

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

### Additional resources

Cisco Proximity site:

► <https://proximity.cisco.com>

Support forum:

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

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

### Video input quality settings

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

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

### Optimal definition profile

The optimal definition profile should reflect the lighting conditions in the video conferencing room and the quality of the camera (video input source). The better the lighting conditions and the better the quality of the camera, the higher the profile should be used.

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

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

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

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

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

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

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

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

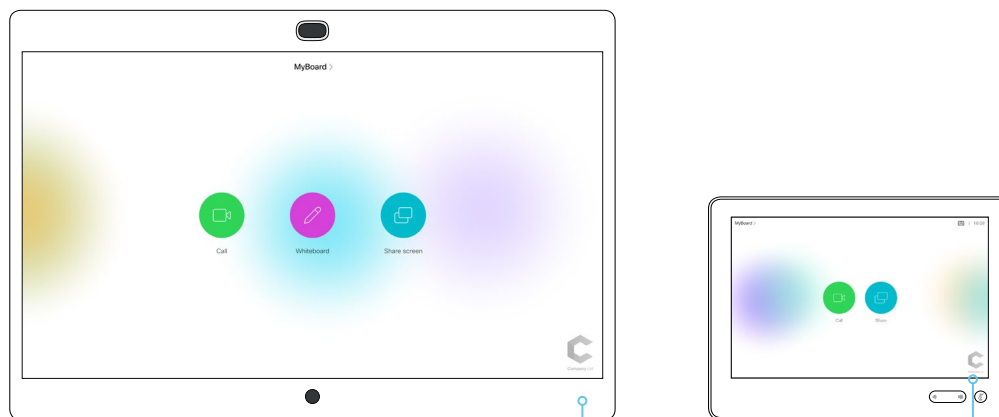
Sign in to the web interface and navigate to [Setup > Personalization](#), and open the [Branding](#) tab.

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

### Branding in the awake state

In the awake state you can:

- Add a logo in the bottom right corner (screen and Touch 10)



#### Logo

We recommend:

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

### About Branding

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

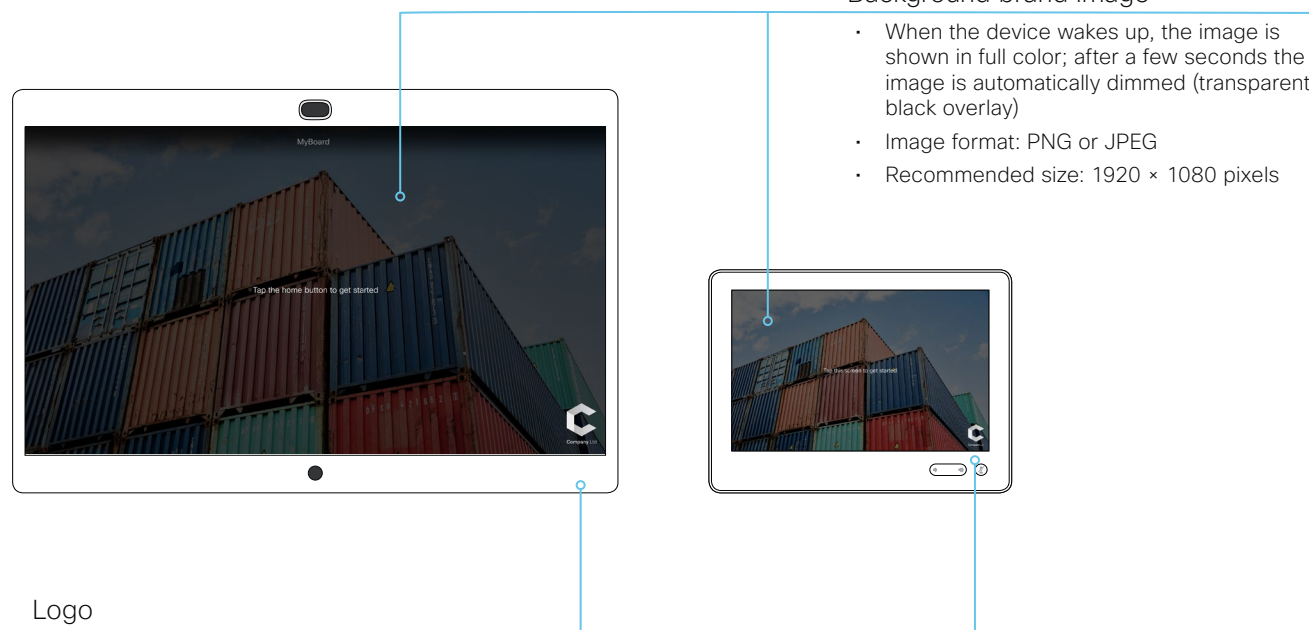
## Add corporate branding to the screen and Touch 10 user interface (page 2 of 2)

### Branding in the halfwake state

In halfwake state you can:

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

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



#### Background brand image

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

#### Logo

We recommend:

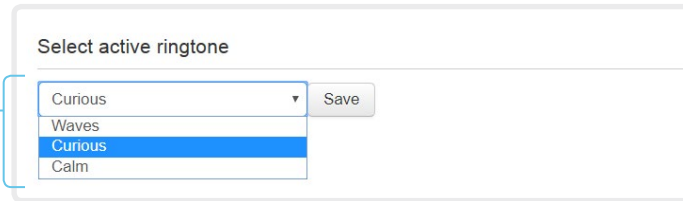
- A white logo (so that it goes well with the dark background brand image)
- PNG-format with transparent background
- Minimum 272×272 pixels

## Choose a ringtone and set the ringtone volume

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

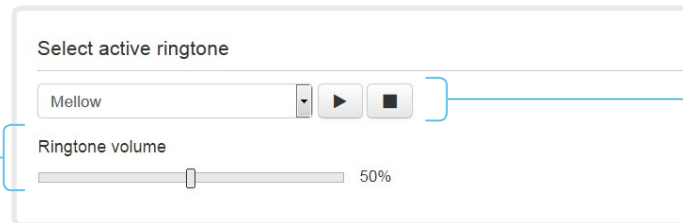
### Change the ringtone

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



### Set the ringtone volume

Use the slide bar to adjust the ringtone volume.



### Play back the ringtone

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

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

### About ringtones

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

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

## Manage the Favorites list

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

### Import/Export contacts from file

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

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

### Add or edit a contact

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

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

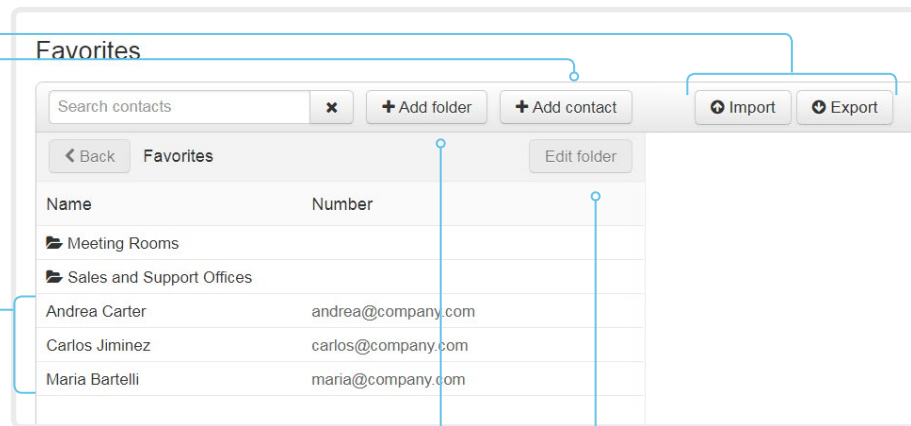
Choose a folder in the folder drop down list in order to store the contact in a sub-folder.

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

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

### Delete a contact

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



### Add or edit a sub-folder

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

### Delete a sub-folder

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

## Manage Favorites using the device's user interface

For Boards this only applies to a paired Touch 10, 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. Select [Add to favorites](#).

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

### Remove a contact from the Favorites list

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



## Set up accessibility features

### Flashing screen for incoming calls

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

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

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

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

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

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

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

### Configuration control modes

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

These are the various configuration control modes:

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

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

### Pull configurations from the device on-demand

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

This option is enabled only if the device is registered.

### Supported CE software versions

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

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

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

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

### Set up provisioning from CUCM

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

Pull configurations from the device on-demand

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

Settings marked with a hash, #

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

Settings or parameters

The settings that belong to the selected category.

Categories

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

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

## Chapter 3

# Peripherals

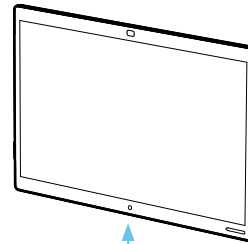
## Connect an input source (page 1 of 2)

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

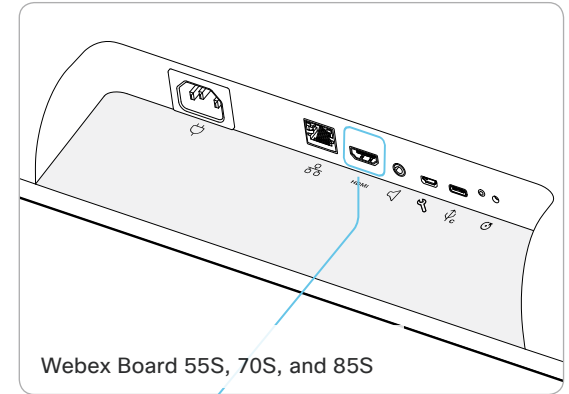
### Connect a computer or other content source

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

The HDMI input supports resolutions up to 3840 × 2160 at 30 fps; and up to 1080p at 60 fps. You need a High Speed HDMI 1.4b cable to support the high resolutions and frame rates.

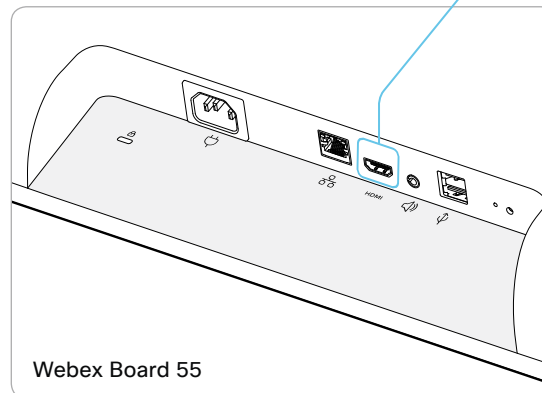


The connector panel is at the bottom, rear side.

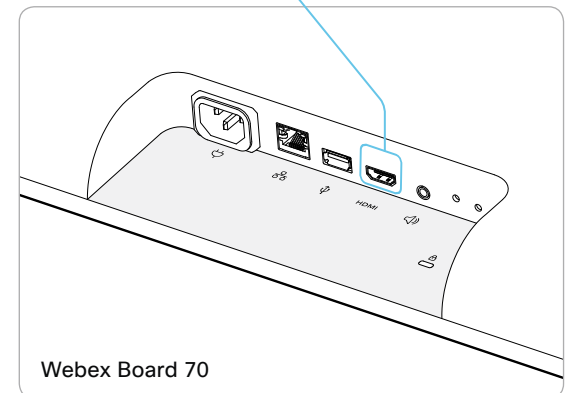


Webex Board 55S, 70S, and 85S

Input Connector 2  
HDMI input (audio and video) for  
computer or other content source



Webex Board 55



Webex Board 70

## Connect an input source (page 2 of 2)

### Set type and name for an input source

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

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

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

Note that Input Connector 1 is the integrated camera.

### About video and content quality

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

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

The default value is **Sharpness** for Connector 2.

## Information about 4K resolution

### Connecting a computer

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

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

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

### Checklist

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

Check that the video conferencing device's input connector is configured correctly.


Check that the device (computer) 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.

 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).

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

---

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



## Set up the Best overview feature

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

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

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

### Configure Best overview

Use the [Cameras > SpeakerTrack](#) settings to configure best overview.

[Cameras > SpeakerTrack > Mode](#)

**Auto:** Best overview is enabled in general. The device will detect people in the room and automatically select the best camera framing. Users can switch Best overview on or off instantly in the [Settings > Advanced Settings](#) panel on the Board.

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

## Connect the Touch 10 controller (page 1 of 3)

Touch 10 must be paired to the video conferencing device via the network (LAN). This is referred to as remote pairing.

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

Connect Touch 10 and the video conferencing device to network wall sockets or to a network switch as illustrated.

#### Touch 10 set-up

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

When the *Select a room system* screen appears, note the following:

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

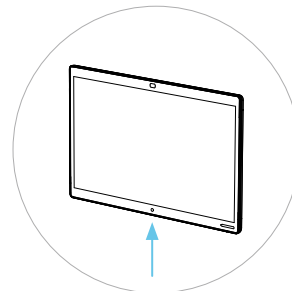
Note that the following must be fulfilled for a device to show up in the list:

- The device and Touch 10 must be on the same subnet.
- The device must have been restarted within the last 10 minutes. If the device does not appear in the list, try restarting it.
- If the device does not appear in the list of available devices, enter its IP address or hostname in the input field. Tap *Connect*.
- You have to log in with username and passphrase for the pairing process to commence. Tap *Login*.

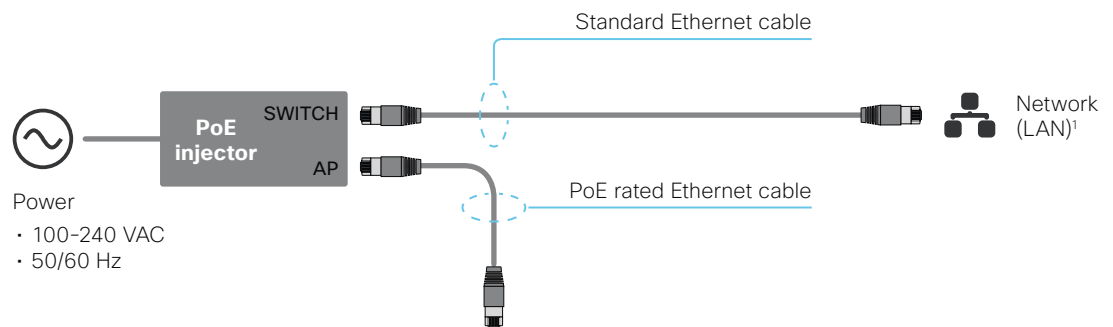
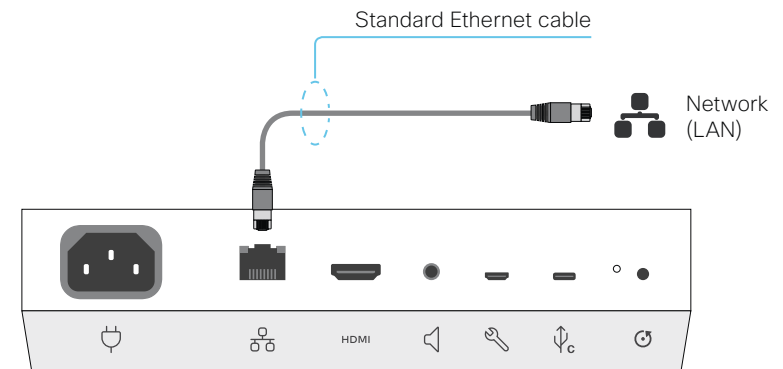
A user with the USER role is sufficient; you do not need the ADMIN role to perform this task.

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

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

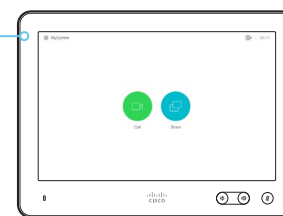


The connector panel is at the bottom, rear side.



#### Contact information

The video conferencing device's name or address is displayed in the status bar when Touch 10 is successfully paired to the device.



The Ethernet connector is at the rear of Touch 10.

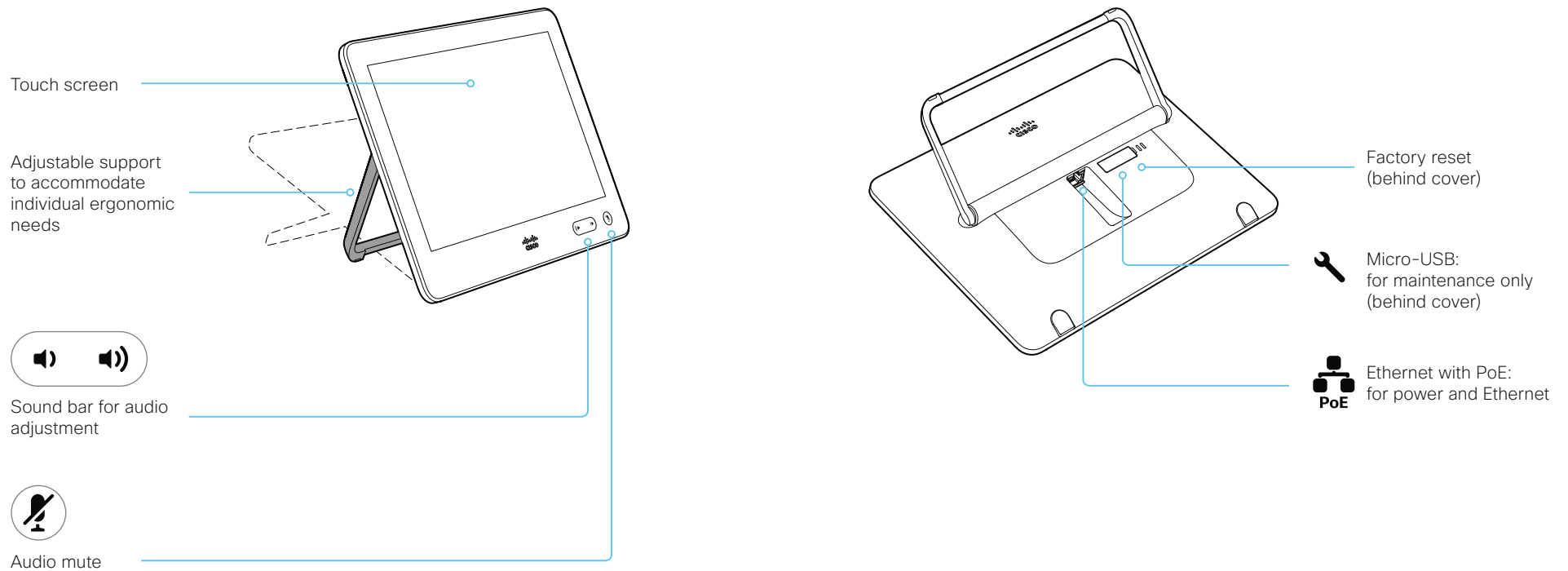
<sup>1</sup> If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

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

## Connect the Touch 10 controller (page 2 of 3)

### Cisco Touch 10 physical interface

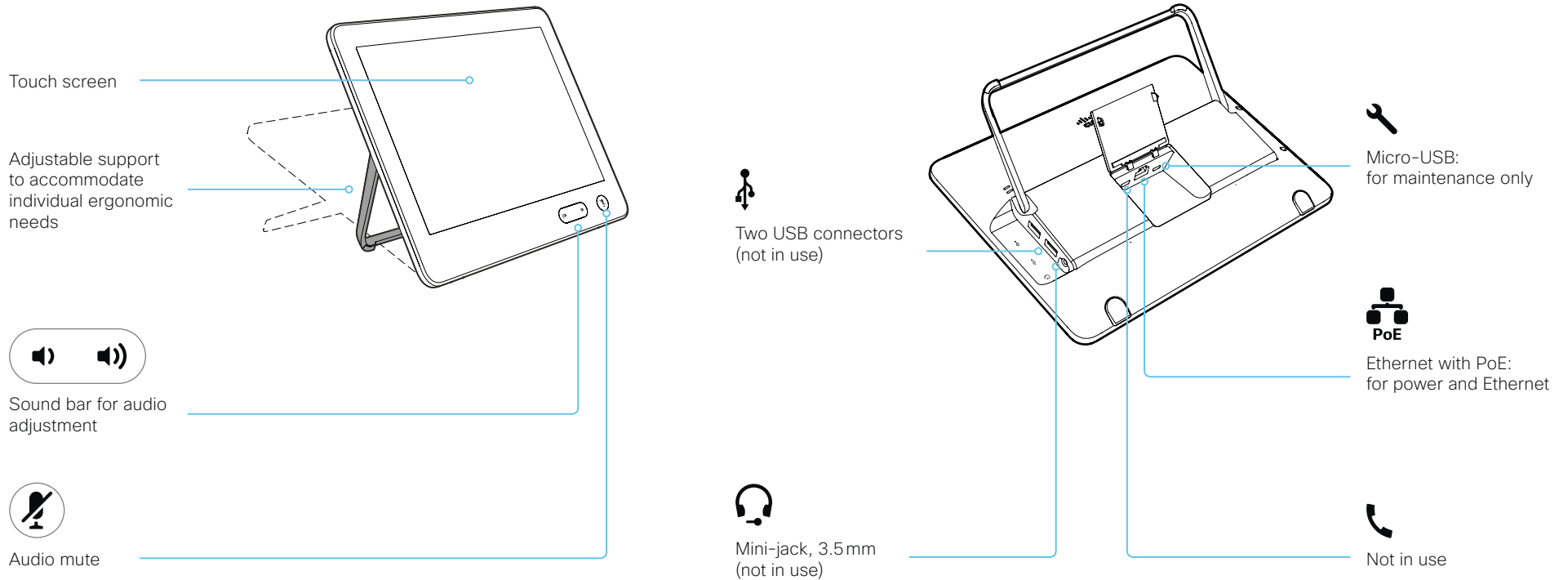
This is the new version of the Touch 10 controller launched late 2017. It has the same functionality as the previous version, but has a slightly different physical interface. The new device is identified by the logo on front, and fewer connectors at the back.



## Connect the Touch 10 controller (page 3 of 3)

### Cisco TelePresence Touch 10 physical interface

See next page for a newer version of the Touch 10 controller.



## Connect the ISDN Link

The ISDN Link enables a video conferencing device to use ISDN lines for connectivity, and enables both video calls and telephone calls over the PSTN (Public Switched Telephone Network).

ISDN Link support ISDN BRI, ISDN PRI and V.35. ISDN can be used in addition to regular IP connectivity for SIP or H.323 calls, or without any IP infrastructure.

ISDN Link is managed from the video conferencing device's web interface. Sign in to the web interface and navigate to [Setup > Peripherals](#).

Requirements and limitations:

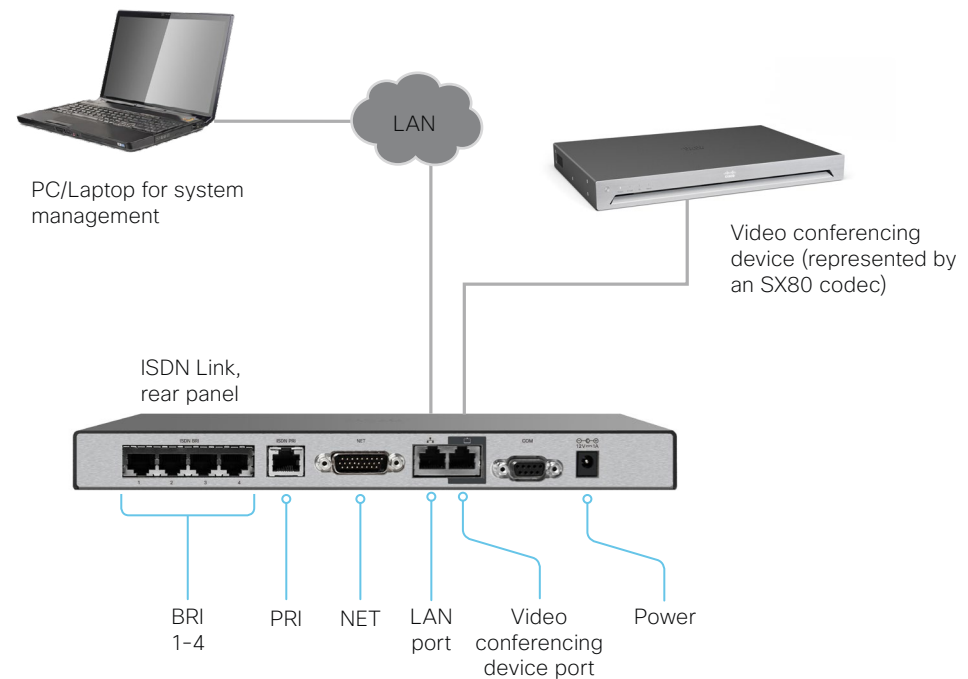
- The video conferencing system must be connected to a Touch controller
- The ISDN Link must be running IL1.1.7 software or later
- The video conferencing device must have IPv6 enabled in the web interface or API in order to communicate with the ISDN Link
- Observe the network topology in the ISDN Link Installation Guide in order to guarantee a successful installation
- The video conferencing device and ISDN Link must be on the same subnet. If the endpoint or ISDN Link are assigned new IP addresses they will only remain paired as long as they are kept in the same subnet.
- Video conferencing devices that are registered to the Cisco Webex cloud service are not able to use ISDN Link.

### Setup and configuration

More information about ISDN Link (Release Notes, Installation Guide, Administrator Guide, API Guide, Compliance and Safety guide) is found here: <https://www.cisco.com/go/isdnlink-docs>

Setup with LAN and direct connection between the video conferencing device and ISDN Link

This is the recommended setup. But there are other options, so see the user documentation for additional examples: <https://www.cisco.com/go/isdnlink-docs>



## Chapter 4

# Maintenance

## Upgrade the device software

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

### Download new software

Each software version has a unique file name. Go to the Cisco Download Software web page, and select your product:

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

The format of the file name is:

“cmterm-s53200ce9\_8\_x-yyy.k3.cop.sgn”

where "x" represents the dot dot release number, and "yyy" represents a unique identifier of the software.

### Install new software

Download the appropriate software package and store it on your computer. This is a .cop.sgn file. Don't change the file name.

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

The software version will be detected and shown.

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

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

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

### Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (CE9).

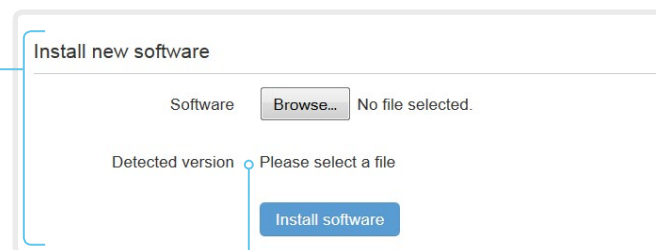
Go to: ► <https://www.cisco.com/c/en/us/support/collaboration-endpoints/spark-board/tsd-products-support-series-home.html>

### Software download

Go to the Cisco Download Software web page, and select your product: ► <https://software.cisco.com/download/home>

The Webex Boards and Room series can be upgraded from the web interface using COP files.

The SX, MX and DX series can be upgraded from the web interface using PKG files



### Check new software version

When you have selected a file, the software version is shown here

## Add option keys

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

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

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

### The device's serial number

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

### Add an option key

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

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

Serial number .....

Option key

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

[Add option key](#)

## About option keys

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

Each device has unique option keys.

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



## Device status

### Device information overview

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

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

### Detailed device status

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

### Search for a status entry

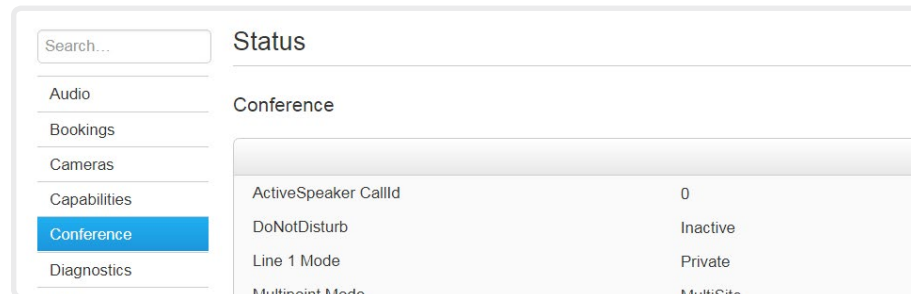
Enter as many letters as needed in the search field. All entries that contain these letters are shown in the right pane. Entries that have these letters in their value space are also shown.



Status	
<b>Audio</b>	
Ultrasound Volume	70
Volume	48

### Select a category and navigate to the correct status

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



Status	
<b>Conference</b>	
ActiveSpeaker CallId	0
DoNotDisturb	Inactive
Line 1 Mode	Private

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

## Run diagnostics

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

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

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

### Run diagnostics

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

### Leave standby mode

Click [Wake up the system](#) to wake up a device that is in standby mode.

**Diagnostics** Wake up the system Re-run diagnostics

Diagnostics help identify issues that may cause the system to fail or not work as expected.

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

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

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

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

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

## Download log files

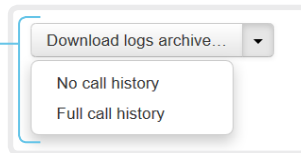
Sign in to the web interface and navigate to [Maintenance > System Logs](#).

### Download all log files

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

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

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



### Open/save one log file

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

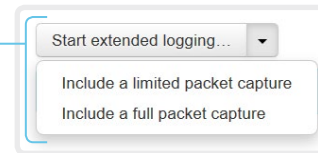
### Start extended logging

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

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

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

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



### Refresh a log file list

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



## About log files

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

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

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

### Extended logging mode

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

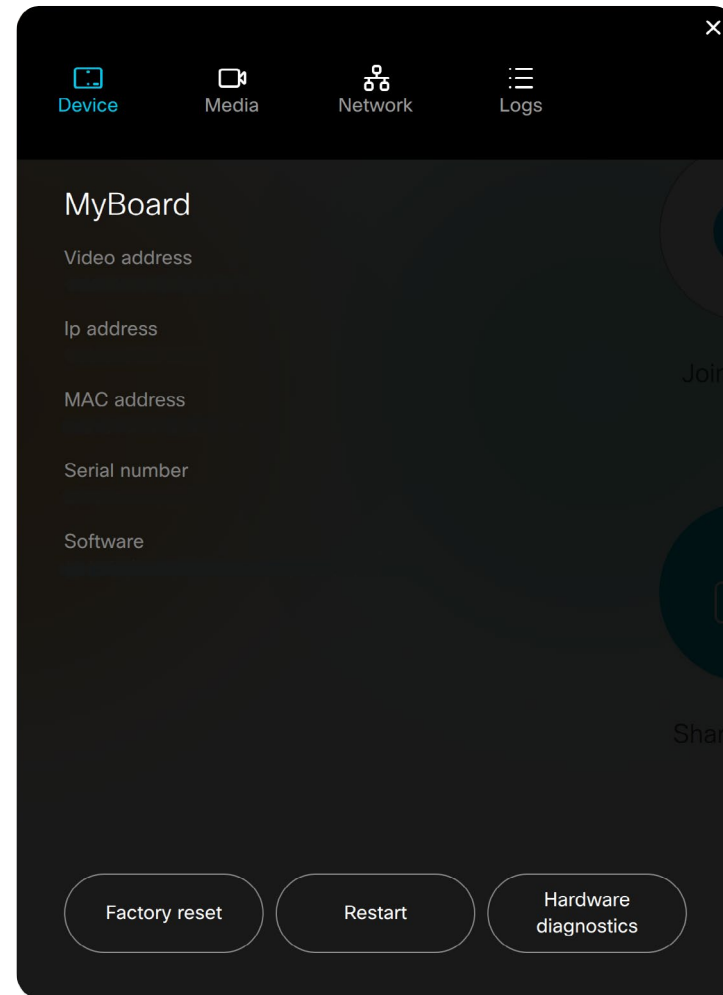
Extended logging uses more of the device's resources, and may cause the device to under-perform. Only use extended logging mode when you are troubleshooting an issue.

## 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 informatiton
- Media statistics
- Network information and diagnostics
- Hardware diagnostics (microphone levels, touch screen, best overview, and camera)
- Logs
- Restart the board
- Factory reset



## Create a remote support user

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

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

### Create remote support user

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

4. Cisco TAC will generate a *password*.

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

The system does not have an active Remote Support User.

[Create user](#) [Delete user](#)

**This user is valid until**  
2018-10-05 16:50:18

**Token**

```
bgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5z1+b
TQek1PaSpsQJNEMfzThgbvK4J7pgOyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
e9CpAoRNq+mZMqEG1lsswKPZ7HYulvyVTH/XuPzU7Nues
9pwzLc8BFgBt1xV0fKeoeOmMX+it1Ecamln4lnXlScgOt
yPSXiFWLdKAJsQHJQH20PCxxYcnEUYNpAoJiD39edLy4
etY+/SATwBIiohrqF9JLW9FfNEF+IyDlwUmYkPoEirBj7
N3Zvpivlv1Z7+NUalQW9qWTj4Ag==
```

The system has an active Remote Support User.

[Create user](#) [Delete user](#)

### Delete remote support user

Click [Delete user](#).

### About the remote support user

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

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

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

## Backup and restore configurations and custom elements

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

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

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

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

### Create a backup file

1. Open the [Create backup](#) tab.
2. Select the elements you want to include in the backup file.  
Elements that currently don't exist on the device are greyed out.
3. Select which settings - if any - you want to include in the backup file. Note the following:
  - As default, all settings are included in the backup file.
  - You can remove one or more settings manually by deleting them from the list on the web page.
  - If you want to remove all settings that are specific to one device, click [Remove system-specific configurations](#).  
This is useful if you are going to restore the backup bundle on other devices.
4. Click [Download backup](#) to store the elements in a zip-file on your computer.

### Restore a backup file

1. Choose the [Restore backup](#) tab.
2. Click [Browse...](#) and find the backup file you want to restore.  
All settings and elements in the backup file will be applied.
3. Click [Upload file](#) to apply the backup.  
Some settings may require that you restart the device before they take effect.

### Additional information

#### Restoring macros

If a backup file that contains macros is restored on a device the following applies:

- The macro runtime is started or restarted.
- The macros are automatically activated (started).

#### Restoring branding images

If a backup bundle contains branding images, the *UserInterface Wallpaper* setting is automatically set to **Auto**.

This means that the branding images will automatically be displayed, possibly replacing a custom wallpaper.

#### The backup file

The backup file is a zip-file that contains several files. It is important that the files are at the top level within the zip-file, and not include in a folder.


## CUCM provisioning of custom elements

A backup file, as described in the ► [Backup and restore configurations and custom elements](#) chapter, can be used as a *customization template* for multiple devices.

The customization template (backup file) may be hosted on either:

- the CUCM TFTP file service, or
- a custom web server that can be reached by the devices on HTTP or HTTPS.

When a device get information from CUCM (Cisco Unified Communications Manager) about the name and location of a customization template, the device will contact the server, download the file, and restore the custom elements.

 Configurations will not be restored on the device, even if they are part of the backup file that you use as a customization template.

Upload a customization template to the TFTP file server

1. Sign in to *Cisco Unified OS Administration*.
2. Navigate to *Software Upgrades > TFTP File Management*.
3. Click *Upload File*. Enter the name and path of the customization template in the input field.
4. Click *Upload File*.

Add customization provisioning information for each device

1. Sign in to *Cisco Unified CM Administration*.
2. Navigate to *Device > Phone*.
3. Fill in the **Customization Provisioning** fields in the product specific configuration section of the relevant devices:
  - *Customization File*: The customization template file name (for example: backup.zip) \*
  - *Customization Hash Type*: **SHA512**
  - *Customization Hash*: The SHA512 checksum for the customization template.

If these fields are not present, you must install a newer Device Package on CUCM.

4. Click *Save* and *Apply Config* to push the configuration to the devices.

\* If not using the TFTP Service, you must enter the complete URI for the customization template: <hostname>:<portnumber>/<path-and-filename>

For example:

- http://host:6970/backup.zip, or
- https://host:6971/backup.zip

### SHA512 checksum

**Tip!** You can find the SHA512 checksum of a file by restoring it to a device using its web interface.

1. Sign in to the web interface and navigate to *Maintenance > Backup and Restore*.
2. Choose the *Restore backup* tab.
3. Click *Browse...* and find the file you want to calculate the checksum for.

Then you can see the SHA512 checksum at the bottom of the page.

### CUCM documentation

► <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html>

## TMS provisioning of custom elements

A backup file, as described in the [► Backup and restore configurations and custom elements](#) chapter, can be used as a *customization template* for multiple devices.

The backup file must be hosted on a custom web server that can be reached by the devices on HTTP or HTTPS.

When a device get information from TMS (TelePresence Management Suite) about the name and location of the backup file, the device will contact the server, download the file, and restore the custom elements.

### Create and apply a configuration template

1. Create a configurations template.
2. Add a custom command containing the following XML string in the configuration template:

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

where

*web-server-address*: The URI to the backup file (for example, <http://host/backup.zip>).

*checksum*: The SHA512 checksum of the backup file.

*origin*: **Provisioning**\*

3. Select the devices you want to push the configuration template to, and click [Set on systems](#).

Read the [► Cisco TMS administrator guide](#) for details how to create TMS configurations templates and make custom commands.

### SHA512 checksum

**Tip!** You can find the SHA512 checksum of a file by restoring it to a device using its web interface.

1. Sign in to the web interface and navigate to [Maintenance > Backup and Restore](#).
2. Choose the [Restore backup](#) tab.
3. Click [Browse...](#) and find the file you want to calculate the checksum for.

Then you can see the SHA512 checksum at the bottom of the page.

---

\* If not setting this parameter to **Provisioning**, also configurations that are part of the backup file will be pushed to the device. If the backup file contains configurations that are specific to one device, for example static IP addresses, device name, and contact information, you may end up with devices that you cannot reach.



## Revert to the previously used software image

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

We recommend you to back up the log files, configurations, and custom elements of the device before you swap to the previously used software image.

### Back up log files, configurations and custom elements

1. Select the *Backup* tab.
2. Click [Download logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download backup](#) and follow the instructions to save the backup bundle on your computer.

### Revert to the previously used software image

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

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

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

### About the previously used software image

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

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

## Factory reset the video conferencing device (page 1 of 3)

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



It is not possible to undo a factory reset.

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

We recommend that you use the web interface or user interface to factory reset the device. If these interfaces are not available, use the reset pin-hole.

A factory reset implies:

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

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

**We recommend that you back up the log files, configurations, and custom elements of the device before you perform a factory reset; otherwise these data will be lost.**

## Factory reset the video conferencing device (page 2 of 3)

### Factory reset using the web interface

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

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

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

When the device has been successfully reset to factory settings, the *Setup assistant* starts with the *Welcome* screen.

### Factory reset from the Technical support screen

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, configurations, and custom elements

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

1. Select the *Backup* tab.
2. Click [Download logs](#) and follow the instructions to save the log files on your computer.
3. Click [Download backup](#) and follow the instructions to save the backup bundle on your computer.

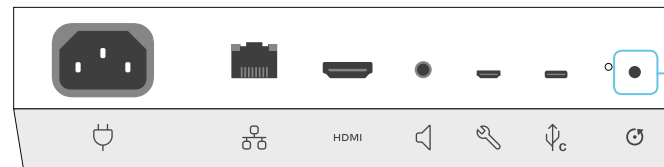
## Factory reset the video conferencing device (page 3 of 3)

### Factory reset using the reset button

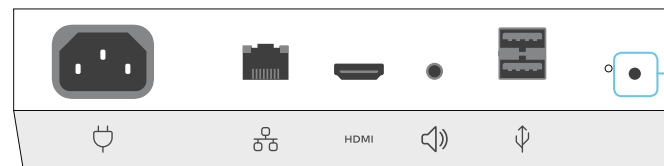
We recommend that you back up the log files and configuration of the device before you continue with the factory reset.

1. Locate the reset button (pin hole) 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 device reverts to the default factory settings. When finished, the device restarts automatically. This may take a few minutes.

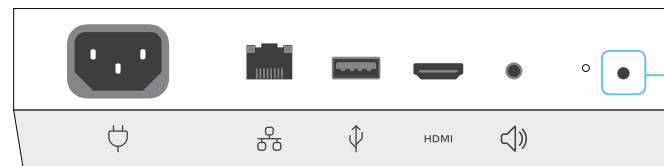
When the device has been successfully reset to factory settings, the Setup assistant starts with the *Welcome* screen.



Webex Board 55S, 70S, and 85S



Webex Board 55



Webex Board 70

**Reset button**

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


## Factory reset Cisco Touch 10

**This chapter applies to the new Touch 10 controller that was launched late 2017 (Cisco Touch 10).** This device is identified by the logo on front, and fewer connectors at the back.

See the next page for the older version.

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

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

 It is not possible to undo a factory reset.

1. Open the small cover at the rear to find the reset button.
2. Press and hold the reset button until the mute button at the front starts blinking (approximately 5 seconds). Then release the button.

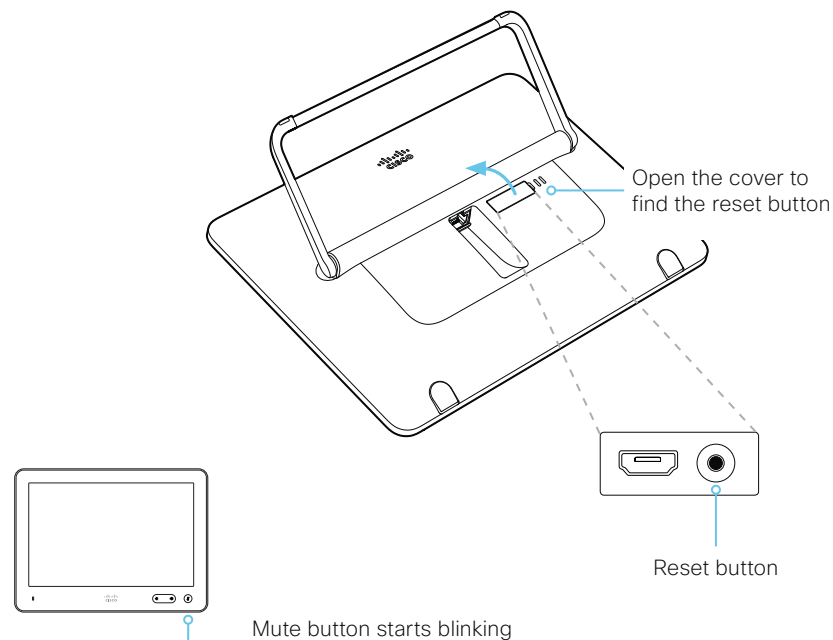
Touch 10 automatically reverts to the default factory settings and restarts.

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

### About pairing and how to connect Touch 10 to the video conferencing device

In order to use the Touch 10 controller, it must be paired to the video conferencing device via LAN (remote pairing).

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



## Factory reset Cisco TelePresence Touch 10

**This chapter applies to the first Touch 10 controller (Cisco TelePresence Touch 10).** This device has no logo on front.

See the previous page for the newer version that was launched late 2017.

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

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

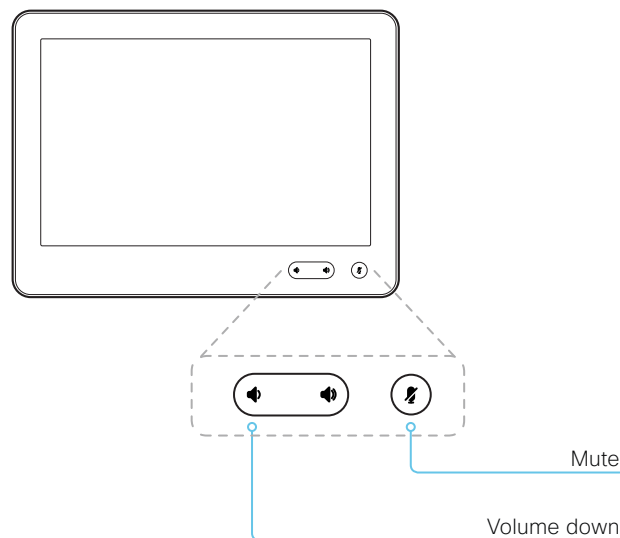


It is not possible to undo a factory reset.

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

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

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



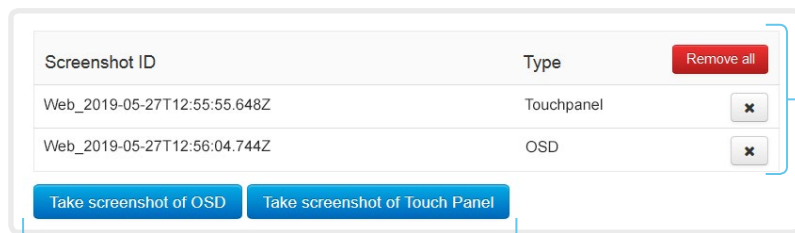
### About pairing and how to connect Touch 10 to the video conferencing device

In order to use the Touch 10 controller, it must be paired to the video conferencing device via LAN (remote pairing).

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

## Capture user interface screenshots

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



### Capture a screenshot

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

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

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

### Delete screenshots

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

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

### About user interface screenshots

You can capture screenshots both of a Touch controller that is connected to the device, and of the main screen with menus, indicators and messages (also know as *on-screen display*).

## Chapter 5

# Device settings



## Overview of the device settings

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

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

### How to find the IP address

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

<b>Audio settings</b> .....	<b>78</b>
Audio DefaultVolume.....	78
Audio KeyClickDetector Attenuate.....	78
Audio KeyClickDetector Enabled .....	78
Audio SoundsAndAlerts RingTone .....	78
Audio SoundsAndAlerts RingVolume.....	78
Audio Ultrasound MaxVolume.....	79
Audio Ultrasound Mode .....	79
<b>CallHistory settings</b> .....	<b>80</b>
CallHistory Mode.....	80
<b>Cameras settings</b> .....	<b>81</b>
Cameras Camera [n] Backlight DefaultMode .....	81
Cameras Camera [n] Brightness DefaultLevel .....	81
Cameras Camera [n] Brightness Mode .....	81
Cameras Camera [n] Focus Mode .....	81
Cameras Camera [n] Gamma Level .....	82
Cameras Camera [n] Gamma Mode.....	82
Cameras SpeakerTrack Mode.....	82
<b>Conference settings</b> .....	<b>83</b>
Conference ActiveControl Mode .....	83
Conference AutoAnswer Delay.....	83
Conference AutoAnswer Mode .....	83
Conference AutoAnswer Mute .....	83
Conference CallProtocolIPStack.....	83
Conference DefaultCall Protocol .....	84
Conference DefaultCall Rate.....	84
Conference DoNotDisturb DefaultTimeout .....	84
Conference Encryption Mode.....	84
Conference FarEndControl Mode.....	84
Conference FarEndControl SignalCapability.....	85
Conference FarEndMessage Mode .....	85
Conference IncomingMultisiteCall Mode.....	86
Conference MaxReceiveCallRate .....	85
Conference MaxTotalReceiveCallRate.....	85
Conference MaxTotalTransmitCallRate .....	86

Conference MaxTransmitCallRate.....	85	<b>Macros settings .....</b>	<b>95</b>
Conference MicUnmuteOnDisconnect Mode.....	86	Macros AutoStart.....	95
Conference Multipoint Mode.....	86	Macros Mode.....	95
Conference Presentation OnPlacedOnHold.....	87	<b>Network settings.....</b>	<b>96</b>
Conference Presentation RelayQuality.....	87	Network [n] DNS DNSSEC Mode.....	96
Conference VideoBandwidth Mode.....	87	Network [n] DNS Domain Name.....	96
<b>FacilityService settings.....</b>	<b>88</b>	Network [n] DNS Server [m] Address.....	96
FacilityService Service [n] CallType.....	88	Network [n] IEEE8021X AnonymousIdentity.....	97
FacilityService Service [n] Name.....	88	Network [n] IEEE8021X Eap Md5.....	98
FacilityService Service [n] Number.....	88	Network [n] IEEE8021X Eap Peap.....	98
FacilityService Service [n] Type.....	88	Network [n] IEEE8021X Eap Tls.....	98
<b>H323 settings.....</b>	<b>89</b>	Network [n] IEEE8021X Eap Tls.....	98
H323 Authentication LoginName.....	89	Network [n] IEEE8021X Identity.....	97
H323 Authentication Mode.....	89	Network [n] IEEE8021X Mode.....	96
H323 Authentication Password.....	89	Network [n] IEEE8021X Password.....	97
H323 CallSetup Mode.....	89	Network [n] IEEE8021X TlsVerify.....	97
H323 Encryption KeySize.....	90	Network [n] IEEE8021X UseClientCertificate.....	97
H323 Gatekeeper Address.....	90	Network [n] IPStack.....	98
H323 H323Alias E164.....	90	Network [n] IPv4 Address.....	99
H323 H323Alias ID.....	90	Network [n] IPv4 Assignment.....	99
H323 NAT Address.....	91	Network [n] IPv4 Gateway.....	99
H323 NAT Mode.....	90	Network [n] IPv4 SubnetMask.....	99
H323 PortAllocation.....	91	Network [n] IPv6 Address.....	100
<b>HttpClient settings.....</b>	<b>92</b>	Network [n] IPv6 Assignment.....	99
HttpClient AllowHTTP.....	92	Network [n] IPv6 DHCPOptions.....	100
HttpClient AllowInsecureHTTPS.....	92	Network [n] IPv6 Gateway.....	100
HttpClient Mode.....	92	Network [n] MTU.....	100
<b>Logging settings.....</b>	<b>93</b>	Network [n] QoS Diffserv Audio.....	101
Logging Debug Wifi.....	93	Network [n] QoS Diffserv Data.....	101
Logging External Mode.....	93	Network [n] QoS Diffserv ICMPv6.....	102
Logging External Protocol.....	93	Network [n] QoS Diffserv NTP.....	102
Logging External Server Address.....	93	Network [n] QoS Diffserv Signalling.....	101
Logging External Server Port.....	93	Network [n] QoS Diffserv Video.....	101
Logging Internal Mode.....	94	Network [n] QoS Mode.....	100
Logging Mode.....	94	Network [n] RemoteAccess Allow.....	102
		Network [n] Speed.....	102

Network [n] TrafficControl Mode .....	103	NetworkServices UPnP Mode .....	110
Network [n] VLAN Voice Mode .....	103	NetworkServices UPnP Timeout .....	111
Network [n] VLAN Voice VlanId .....	103	NetworkServices Websocket .....	111
<b>NetworkServices settings .....</b>	<b>104</b>	NetworkServices WelcomeText .....	111
NetworkServices CDP Mode .....	104	NetworkServices Wifi Allowed .....	111
NetworkServices H323 Mode .....	104	NetworkServices Wifi Enabled .....	111
NetworkServices HTTP Mode .....	104	NetworkServices XMLAPI Mode .....	112
NetworkServices HTTP Proxy LoginName .....	104	<b>Peripherals settings .....</b>	<b>113</b>
NetworkServices HTTP Proxy Mode .....	105	Peripherals Profile Cameras .....	113
NetworkServices HTTP Proxy PACUrl .....	105	Peripherals Profile ControlSystems .....	113
NetworkServices HTTP Proxy Password .....	105	<b>Phonebook settings .....</b>	<b>114</b>
NetworkServices HTTP Proxy Url .....	105	Phonebook Server [n] ID .....	114
NetworkServices HTTPS OCSP Mode .....	105	Phonebook Server [n] Pagination .....	114
NetworkServices HTTPS OCSP URL .....	105	Phonebook Server [n] Type .....	114
NetworkServices HTTPS Server MinimumTLSVersion .....	106	Phonebook Server [n] URL .....	114
NetworkServices HTTPS StrictTransportSecurity .....	106	<b>Provisioning settings .....</b>	<b>115</b>
NetworkServices HTTPS VerifyClientCertificate .....	106	Provisioning Connectivity .....	115
NetworkServices HTTPS VerifyServerCertificate .....	106	Provisioning ExternalManager Address .....	115
NetworkServices NTP Mode .....	106	Provisioning ExternalManager AlternateAddress .....	115
NetworkServices NTP Server [n] Address .....	107	Provisioning ExternalManager Domain .....	116
NetworkServices NTP Server [n] Key .....	107	Provisioning ExternalManager Path .....	116
NetworkServices NTP Server [n] KeyAlgorithm .....	107	Provisioning ExternalManager Protocol .....	115
NetworkServices NTP Server [n] KeyId .....	107	Provisioning LoginName .....	116
NetworkServices SIP Mode .....	107	Provisioning Mode .....	116
NetworkServices SMTP From .....	108	Provisioning Password .....	117
NetworkServices SMTP Mode .....	108	<b>Proximity settings .....</b>	<b>118</b>
NetworkServices SMTP Password .....	108	Proximity Mode .....	118
NetworkServices SMTP Port .....	108	Proximity Services CallControl .....	118
NetworkServices SMTP Security .....	109	Proximity Services ContentShare FromClients .....	118
NetworkServices SMTP Server .....	108	Proximity Services ContentShare ToClients .....	118
NetworkServices SMTP Username .....	108	<b>RoomAnalytics settings .....</b>	<b>119</b>
NetworkServices SNMP CommunityName .....	109	RoomAnalytics AmbientNoiseEstimation Mode .....	119
NetworkServices SNMP Host [n] Address .....	109	RoomAnalytics PeopleCountOutOfCall .....	119
NetworkServices SNMP Mode .....	109	RoomAnalytics PeoplePresenceDetector .....	119
NetworkServices SNMP SystemContact .....	109	<b>RoomReset settings .....</b>	<b>120</b>
NetworkServices SNMP SystemLocation .....	110	RoomReset Control .....	120
NetworkServices SSH AllowPublicKey .....	110		
NetworkServices SSH HostKeyAlgorithm .....	110		
NetworkServices SSH Mode .....	110		

<b>RTP settings</b> .....	<b>121</b>	SIP Turn DropRflx.....	128
RTP Ports Range Start.....	121	SIP Turn Password.....	129
RTP Ports Range Stop.....	121	SIP Turn Server.....	129
RTP Video Ports Range Start.....	121	SIP Turn UserName.....	129
RTP Video Ports Range Stop.....	121	SIP Type.....	129
<b>Security settings</b> .....	<b>122</b>	SIP URI.....	129
Security Audit Logging Mode.....	122	<b>Standby settings</b> .....	<b>130</b>
Security Audit OnError Action.....	122	Standby Control.....	130
Security Audit Server Address.....	122	Standby Delay.....	130
Security Audit Server Port.....	122	Standby WakeupOnMotionDetection.....	130
Security Audit Server PortAssignment.....	123	<b>SystemUnit settings</b> .....	<b>131</b>
Security Session FailedLoginsLockoutTime.....	123	SystemUnit CrashReporting Advanced.....	131
Security Session InactivityTimeout.....	123	SystemUnit CrashReporting Mode.....	131
Security Session MaxFailedLogins.....	123	SystemUnit CrashReporting Url.....	131
Security Session MaxSessionsPerUser.....	123	SystemUnit Name.....	131
Security Session MaxTotalSessions.....	123	<b>Time settings</b> .....	<b>132</b>
Security Session ShowLastLogon.....	124	Time DateFormat.....	132
<b>SerialPort settings</b> .....	<b>125</b>	Time TimeFormat.....	132
SerialPort BaudRate.....	125	Time Zone.....	133
SerialPort LoginRequired.....	125	<b>UserInterface settings</b> .....	<b>135</b>
SerialPort Mode.....	125	UserInterface Accessibility IncomingCallNotification.....	135
<b>SIP settings</b> .....	<b>126</b>	UserInterface Branding AwakeBranding Colors.....	135
SIP ANAT.....	126	UserInterface ContactInfo Type.....	135
SIP Authentication Password.....	126	UserInterface Features Call End.....	136
SIP Authentication UserName.....	126	UserInterface Features Call MidCallControls.....	136
SIP DefaultTransport.....	126	UserInterface Features Call Start.....	136
SIP DisplayName.....	126	UserInterface Features Call VideoMute.....	136
SIP Ice DefaultCandidate.....	127	UserInterface Features HideAll.....	136
SIP Ice Mode.....	127	UserInterface Features Share Start.....	136
SIP Line.....	127	UserInterface Features Whiteboard Start.....	137
SIP ListenPort.....	127	UserInterface KeyTones Mode.....	135
SIP Mailbox.....	127	UserInterface Language.....	137
SIP MinimumTLSVersion.....	128	UserInterface OSD EncryptionIndicator.....	137
SIP PreferredIPSignaling.....	128	UserInterface OSD Output.....	137
SIP Proxy [n] Address.....	128	UserInterface Phonebook Mode.....	138
SIP TlsVerify.....	128	UserInterface Security Mode.....	138
SIP Turn DiscoverMode.....	128	UserInterface SettingsMenu Mode.....	138

UserInterface SettingsMenu Visibility .....	138	Video Selfview Default PIPPosition.....	148
UserInterface SoundEffects Mode.....	139	Video Selfview OnCall Duration.....	148
UserInterface Wallpaper .....	139	Video Selfview OnCall Mode .....	148
<b>UserManagement settings.....</b>	<b>140</b>	<b>Experimental settings .....</b>	<b>149</b>
UserManagement LDAP Admin Filter .....	140		
UserManagement LDAP Admin Group .....	140		
UserManagement LDAP Attribute.....	140		
UserManagement LDAP BaseDN .....	140		
UserManagement LDAP Encryption .....	140		
UserManagement LDAP MinimumTLSVersion.....	141		
UserManagement LDAP Mode .....	141		
UserManagement LDAP Server Address .....	141		
UserManagement LDAP Server Port.....	141		
UserManagement LDAP VerifyServerCertificate.....	141		
<b>Video settings.....</b>	<b>142</b>		
Video ActiveSpeaker DefaultPIPPosition .....	142		
Video DefaultLayoutFamily Remote .....	142		
Video DefaultMainSource .....	142		
Video Input Connector [n] CameraControl Camerald .....	143		
Video Input Connector [n] CameraControl Mode .....	143		
Video Input Connector [n] CEC Mode.....	143		
Video Input Connector [n] InputSourceType .....	143		
Video Input Connector [n] Name.....	143		
Video Input Connector [n] OptimalDefinition Profile.....	144		
Video Input Connector [n] PreferredResolution .....	144		
Video Input Connector [n] PresentationSelection .....	145		
Video Input Connector [n] Quality .....	145		
Video Input Connector [n] RGBQuantizationRange.....	145		
Video Input Connector [n] Visibility .....	146		
Video Output Connector [n] Resolution .....	146		
Video Presentation DefaultPIPPosition .....	146		
Video Presentation DefaultSource.....	146		
Video Presentation Priority .....	147		
Video Selfview Default FullscreenMode .....	147		
Video Selfview Default Mode.....	147		
Video Selfview Default OnMonitorRole.....	147		

## Audio settings

### Audio DefaultVolume

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

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 70

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 KeyClickDetector Attenuate

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb the other participants. If the participant types on the keyboard and speaks at the same time the microphone signal will not be attenuated. Requires that the Audio KeyClickDetector Enabled setting is set to On.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: True

Value space: False/True

False: The attenuation of the microphone signal is disabled.

True: The device attenuates the microphone signal if clicking noise from keyboards is detected. If voice or voice + keyboard clicks are detected the microphone signal is not attenuated.

### Audio KeyClickDetector Enabled

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb other participants. To enable attenuation on the microphone signal, set the Audio KeyClickDetector Attenuate to On.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: True

Value space: False/True

False: The key click detection is disabled.

True: The device will detect clicking noise from keyboards.

### Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Waves

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

Select a ringtone from the list.

### Audio SoundsAndAlerts RingVolume

Define the ring volume for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

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

## Audio Ultrasound Mode

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN, INTEGRATOR

Default value: Static

Value space: Dynamic/Static

Dynamic: The device adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Audio Ultrasound Volume MaxVolume setting.

Static: Use only if advised by Cisco.

## Audio Ultrasound MaxVolume

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message.

Requires user role: ADMIN, INTEGRATOR

Default value: Webex Board 55S/70S/85S: 90 Webex Board 55: 58 Webex Board 70: 70

Value space: Webex Board 55S/70S/85S: Integer (0..90) Webex Board 55: Integer (0..58)  
Webex Board 70: Integer (0..70)

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

## CallHistory settings

### CallHistory Mode

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

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

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

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



## Cameras settings

### Cameras Camera [n] Backlight DefaultMode

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

### Cameras Camera [n] Brightness Mode

n: 1..1

Define the camera brightness mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

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

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

### Cameras Camera [n] Brightness DefaultLevel

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: 20

Value space: Integer (1..31)

The brightness level.

### Cameras Camera [n] Focus Mode

n: 1..1

Define the camera focus mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: The camera will do single shot auto focusing once a call is connected and when the view has changed.

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

## Cameras Camera [n] Gamma Mode

n: 1..1

This setting enables gamma corrections. Gamma describes the nonlinear relationship between image pixels and monitor brightness.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: Auto is the default and the recommended setting.

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

## Cameras Camera [n] Gamma Level

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (0..7)

Define the gamma level.

## Cameras SpeakerTrack Mode

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

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Off

Auto: Best overview is switched on. The device will detect people in the room and automatically select the best camera framing. Users can switch best overview on or off instantly in the camera control panel on the Touch controller, but the feature is switched back on after each call so that the device is ready for the next user.

Off: Best overview is switched off.

## Conference settings

### Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server or Cisco Meeting Server using the video conferencing device's interfaces. Each user can see the participant list, change video layout, disconnect participants, etc. from the interface. The active control feature is enabled by default, provided that it is supported by the infrastructure (Cisco Unified Communications Manager (CUCM) version 9.1.2 or newer, Cisco TelePresence Video Communication Server (VCS) version X8.1 or newer, Cisco Media Server (CMS) version 2.1 or newer). Change this setting if you want to disable the active control features.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off

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

### Conference AutoAnswer Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

- Off: You can answer incoming calls manually by tapping Answer on the Touch controller.
- On: The device automatically answers incoming calls, except if you are already in a call. You can answer or decline incoming calls manually when you are already engaged in a call.

### Conference AutoAnswer Mute

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

- Off: The incoming call will not be muted.
- On: The incoming call will be muted when automatically answered.

### Conference AutoAnswer Delay

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..50)

- The auto answer delay (seconds).

### Conference CallProtocolIPStack

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

Requires user role: ADMIN

Default value: Dual

Value space: Dual/IPv4/IPv6

- Dual: Enables both IPv4 and IPv6 for the call protocol.
- IPv4: When set to IPv4, the call protocol will use IPv4.
- IPv6: When set to IPv6, the call protocol will use IPv6.

## Conference DefaultCall Protocol

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

Requires user role: ADMIN

Default value: Auto

Value space: Auto/H320/H323/Sip/Spark

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

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

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

Sip: All calls are set up as SIP calls.

Spark: Reserved for Webex registered devices. Do not use.

## Conference DefaultCall Rate

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

Requires user role: ADMIN, INTEGRATOR

Default value: 10000

Value space: Integer (64..10000)

The default call rate (kbps).

## Conference DoNotDisturb DefaultTimeout

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

Requires user role: ADMIN, INTEGRATOR

Default value: 60

Value space: Integer (1..1440)

The number of minutes (maximum 1440 minutes = 24 hours) before the Do Not Disturb session times out automatically.

## Conference Encryption Mode

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

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

Requires user role: ADMIN

Default value: BestEffort

Value space: Off/On/BestEffort

Off: The device will not use encryption.

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

BestEffort: The device will use encryption whenever possible.

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

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

## Conference FarEndControl Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

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

## Conference FarEndControl SignalCapability

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

## Conference FarEndMessage Mode

Toggle whether it is allowed to send data between two devices in a point-to-point call, for use with control systems or macros. Works with SIP calls only. This setting will enable/disable the use of the xCommand Call FarEndMessage Send command.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: It is not possible to send messages between two devices.

On: It is possible to send messages between two devices in a point-to-point call.

## Conference MaxReceiveCallRate

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

Requires user role: ADMIN

Default value: 10000

Value space: Integer (64..10000)

The maximum receive call rate (kbps).

## Conference MaxTransmitCallRate

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum transmitt call rate (kbps).

## Conference MaxTotalReceiveCallRate

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

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

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

Requires user role: ADMIN

Default value: 10000

Value space: Integer (64..10000)

The maximum receive call rate (kbps).

## Conference MaxTotalTransmitCallRate

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

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

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum transmit call rate (kbps).

## Conference MicUnmuteOnDisconnect Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

On: Unmute the microphones after the call is disconnected.

## Conference Multipoint Mode

Define how the device handles multiparty video conferences (ad hoc conferences).

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

The CUCM conference bridge allows you to set up conferences with many participants. The MultiSite feature allows up to four participants (yourself included).

The MultiSite feature is optional and may not be available on all devices.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/CUCMMediaResourceGroupList/MultiSite/Off

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

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

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

Off: Multiparty conferences are not allowed.

## Conference IncomingMultisiteCall Mode

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

Requires user role: ADMIN

Default value: Allow

Value space: Allow/Deny

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

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

## Conference Presentation OnPlacedOnHold

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

Requires user role: ADMIN

Default value: NoAction

Value space: NoAction/Stop

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

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

## Conference Presentation RelayQuality

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

Requires user role: ADMIN

Default value: Sharpness

Value space: Motion/Sharpness

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

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

## Conference VideoBandwidth Mode

Define the conference video bandwidth mode.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

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

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

## FacilityService settings

### FacilityService Service [n] Type

n: 1..5

Up to five different facility services can be supported simultaneously. With this setting you can select what kind of services they are. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Helpdesk

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

Catering: Select this option for catering services.

Concierge: Select this option for concierge services.

Emergency: Select this option for emergency services.

Helpdesk: Select this option for helpdesk services.

Security: Select this option for security services.

Transportation: Select this option for transportation services.

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

### FacilityService Service [n] Name

n: 1..5

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

Requires user role: ADMIN, INTEGRATOR

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

Value space: String (0, 1024)

The name of the facility service.

### FacilityService Service [n] Number

n: 1..5

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

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 1024)

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

### FacilityService Service [n] CallType

n: 1..5

Define the call type for each facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Video

Value space: Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.



## H323 settings

### H323 Authentication Mode

Define the authentication mode for the H.323 profile.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

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

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

### H323 Authentication LoginName

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication login name.

### H323 Authentication Password

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication password.

### H323 CallSetup Mode

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

Requires user role: ADMIN

Default value: Gatekeeper

Value space: Direct/Gatekeeper

Direct: You can only make an H.323 call by dialing an IP address directly.

Gatekeeper: The device uses a Gatekeeper to make an H.323 call. When choosing this option, the H323 Gatekeeper Address must also be configured.

## H323 Encryption KeySize

Define the minimum or maximum key size for the Diffie-Hellman key exchange method, which is used when establishing the Advanced Encryption Standard (AES) encryption key.

Requires user role: ADMIN

Default value: Min1024bit

Value space: Max1024bit/Min1024bit/Min2048bit

Max1024bit: The maximum size is 1024 bit.

Min1024bit: The minimum size is 1024 bit.

Min2048bit: The minimum size is 2048 bit.

## H323 Gatekeeper Address

Define the IP address of the Gatekeeper. Requires H323 CallSetup Mode to be set to Gatekeeper.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

## H323 H323Alias E164

The H.323 Alias E.164 defines the address of the device, according to the numbering plan implemented in the H.323 Gatekeeper. The E.164 alias is equivalent to a telephone number, sometimes combined with access codes.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 30)

The H.323 Alias E.164 address. Valid characters are 0-9, \* and #.

## H323 H323Alias ID

Define the H.323 Alias ID, which is used to address the device on a H.323 Gatekeeper and will be displayed in the call lists.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 49)

The H.323 Alias ID. Example: "firstname.lastname@company.com", "My H.323 Alias ID"

## H323 NAT Mode

The firewall traversal technology creates a secure path through the firewall barrier, and enables proper exchange of audio/video data when connected to an external video conferencing device (when the IP traffic goes through a NAT router). NOTE: NAT does not work in conjunction with gatekeepers.

Requires user role: ADMIN

Default value: Off

Value space: Auto/Off/On

Auto: The device will determine if the H323 NAT Address or the real IP address should be used in signaling. This makes it possible to place calls to devices on the LAN as well as devices on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.

Off: The device will signal the real IP address.

On: The device will signal the configured H323 NAT Address instead of its real IP address in Q.931 and H.245. The NAT server address will be shown in the startup-menu as: "My IP Address: 10.0.2.1". If the H323 NAT Address is wrong or not set, H.323 calls cannot be set up.

## H323 NAT Address

Define the external/global IP address to the router with NAT support. Packets sent to the router will then be routed to the video conferencing device. Note that NAT cannot be used when registered to a gatekeeper.

In the router, the following ports must be routed to the video conferencing device's IP address:

- \* Port 1720
- \* Port 5555-6555
- \* Port 2326-2487

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

## H323 PortAllocation

This setting affects the H.245 port numbers used for H.323 call signaling.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

**Dynamic:** The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

**Static:** When set to Static the ports are given within a static predefined range [5555-6555].

## HttpClient settings

### HttpClient Mode

Allow or prohibit communication with an external HTTP(S) server using HTTP(S) requests and responses.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The video conferencing device cannot communicate with an external HTTP(S) server.

On: The video conferencing device is allowed to communicate with an external HTTP(S) server.

### HttpClient AllowHTTP

The HttpClient Mode setting is used to allow or prohibit communication with an external HTTP(S) server. The Mode setting does not distinguish between HTTP and HTTPS. You must use the HttpClient AllowHTTP setting to further allow or prohibit the use of HTTP.

Requires user role: ADMIN

Default value: True

Value space: False/True

False: The video conferencing device can communicate only over HTTPS.

True: The video conferencing device can communicate over both HTTPS and HTTP.

### HttpClient AllowInsecureHTTPS

You can choose whether or not to allow the video conferencing device to communicate with a server over HTTPS without checking the server's certificate first.

Even if the device is allowed to skip the certificate validation process, it doesn't automatically do it. You must specifically set the AllowInsecureHTTPS parameter in each xCommand HttpClient command for data to be exchanged with the server without certificate validation.

Requires user role: ADMIN

Default value: False

Value space: False/True

False: The device always checks that the HTTPS server has a valid certificate. No communication with the server takes place if the certificate validation fails.

True: The device is allowed to skip the certificate validation process before communicating with the server.

## Logging settings

### Logging Debug Wifi

When this option is enabled, the device logs more information about the set-up and maintenance of the Wi-Fi connection between the device and the access point. This may be useful when you are troubleshooting Wi-Fi connection issues. We recommend that this setting is Off if the Wi-Fi connection is working as expected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Logging only basic Wi-Fi information.

On: Logging a large amount of information about the Wi-Fi connection.

### Logging External Mode

Determine whether or not to store the device logs on a remote syslog server. This setting has no effect if the Logging Mode setting is set to Off.

You must enter the address of the remote server in the Logging External Server Address setting. Unless otherwise specified in the Logging External Server Port setting, the standard syslog port is used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Device logs will not be stored on the remote syslog server.

On: Device logs will be stored on the remote syslog server.

### Logging External Protocol

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

Requires user role: ADMIN

Default value: SyslogTLS

Value space: Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

### Logging External Server Address

The address of the remote syslog server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

### Logging External Server Port

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

Requires user role: ADMIN

Default value: 514

Value space: Integer (0..65535)

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

## Logging Internal Mode

Determine whether or not to store the system logs on the device (local files). These are the files that you get when you download the log bundles from the device. This setting has no effect if the Logging Mode setting is set to Off.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: System logs will not be stored on the device.

On: System logs will be stored on the device.

## Logging Mode

Define the logging mode for the device (syslog service). When disabled, the syslog service does not start, and most of the systema and audit logs are not generated. The Historical Logs and Call Logs are not affected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the system logging service.

On: Enable the system logging service.

## Macros settings

### Macros Mode

Macros allow you to write snippets of JavaScript code that can automate parts of your video conferencing device, thus creating custom behavior. Use of macros is disabled by default, but the first time you open the Macro Editor you will be asked whether to enable use of macros on the device. Use this setting when you want to manually enable, or to permanently disable the use of macros on the device. You can disable the use of macros within the Macro Editor. But this will not permanently disable macros from running, because every time the device is reset the macros will be re-enabled automatically.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Permanently disable the use of macros on this device.

On: Enable the use of macros on this device.

### Macros AutoStart

All the macros run in a single process on the video conferencing device, called the macro runtime. It should be running by default, but you can choose to stop and start it manually. If you restart the device, the runtime will automatically start again if auto start is enabled.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The macro runtime will not start automatically after a restart of the device.

On: The macro runtime will start automatically after a restart of the device.

## Network settings

### Network [n] DNS DNSSEC Mode

n: 1..1

Domain Name System Security extensions (DNSSEC) is a set of extensions to DNS. It is used to authenticate DNS replies for zones that are signed. It will still allow unsigned zones.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable Domain Name System Security Extensions.

On: Enable Domain Name System Security Extensions.

### Network [n] DNS Domain Name

n: 1..1

The DNS Domain Name is the default domain name suffix which is added to unqualified names.

Example: If the DNS Domain Name is "company.com" and the name to lookup is "MyVideoSystem", this will result in the DNS lookup "MyVideoSystem.company.com".

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The DNS domain name.

### Network [n] DNS Server [m] Address

n: 1..1

m: 1..3

Define the network addresses for DNS servers. Up to three addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

### Network [n] IEEE8021X Mode

n: 1..1

The device can be connected to an IEEE 802.1X LAN network, with a port-based network access control that is used to provide authenticated network access for Ethernet networks.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: The 802.1X authentication is disabled.

On: The 802.1X authentication is enabled.



## Network [n] IEEE8021X TlsVerify

n: 1..1

Verification of the server-side certificate of an IEEE802.1x connection against the certificates in the local CA-list when TLS is used. The CA-list must be uploaded to the video conferencing device. This can be done from the web interface.

This setting takes effect only when Network [1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: When set to Off, TLS connections are allowed without verifying the server-side X.509 certificate against the local CA-list. This should typically be selected if no CA-list has been uploaded to the device.

On: When set to On, the server-side X.509 certificate will be validated against the local CA-list for all TLS connections. Only servers with a valid certificate will be allowed.

## Network [n] IEEE8021X UseClientCertificate

n: 1..1

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video conferencing device. This can be done from the web interface.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: When set to Off client-side authentication is not used (only server-side).

On: When set to On the client (video conferencing device) will perform a mutual authentication TLS handshake with the server.

## Network [n] IEEE8021X Identity

n: 1..1

Define the username for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The username for 802.1X authentication.

## Network [n] IEEE8021X Password

n: 1..1

Define the password for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 50)

The password for 802.1X authentication.

## Network [n] IEEE8021X AnonymousIdentity

n: 1..1

The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The 802.1X Anonymous ID string.

## Network [n] IEEE8021X Eap Md5

n: 1..1

Define the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled.

## Network [n] IEEE8021X Eap Ttls

n: 1..1

Define the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled.

## Network [n] IEEE8021X Eap Tls

n: 1..1

Enable or disable the use of EAP-TLS (Transport Layer Security) for IEEE802.1x connections. The EAP-TLS protocol, defined in RFC 5216, is considered one of the most secure EAP standards. LAN clients are authenticated using client certificates.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled.

## Network [n] IEEE8021X Eap Peap

n: 1..1

Define the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled.

## Network [n] IPStack

n: 1..1

Select if the device should use IPv4, IPv6, or dual IP stack, on the network interface. NOTE: After changing this setting you may have to wait up to 30 seconds before it takes effect.

Requires user role: ADMIN, USER

Default value: Dual

Value space: Dual/IPv4/IPv6

Dual: When set to Dual, the network interface can operate on both IP versions at the same time, and can have both an IPv4 and an IPv6 address at the same time.

IPv4: When set to IPv4, the device will use IPv4 on the network interface.

IPv6: When set to IPv6, the device will use IPv6 on the network interface.

## Network [n] IPv4 Assignment

n: 1..1

Define how the device will obtain its IPv4 address, subnet mask and gateway address. When using DHCP for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

Requires user role: ADMIN, USER

Default value: DHCP

Value space: Static/DHCP

Static: The addresses must be configured manually using the Network IPv4 Address, Network IPv4 Gateway and Network IPv4 SubnetMask settings (static addresses).

DHCP: The device addresses are automatically assigned by the DHCP server.

## Network [n] IPv4 Address

n: 1..1

Define the static IPv4 network address for the device. Applicable only when Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

## Network [n] IPv4 Gateway

n: 1..1

Define the IPv4 network gateway address. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

## Network [n] IPv4 SubnetMask

n: 1..1

Define the IPv4 network subnet mask. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

## Network [n] IPv6 Assignment

n: 1..1

Define how the device will obtain its IPv6 address and the default gateway address.

When using DHCPv6 for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

Requires user role: ADMIN, USER

Default value: Autoconf

Value space: Static/DHCPv6/Autoconf

Static: The device and gateway IP addresses must be configured manually using the Network IPv6 Address and Network IPv6 Gateway settings. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

DHCPv6: All IPv6 addresses, including options, will be obtained from a DHCPv6 server. See RFC 3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC 4862 for a detailed description. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

## Network [n] IPv6 Address

n: 1..1

Define the static IPv6 network address for the device. Applicable only when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

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

## Network [n] IPv6 Gateway

n: 1..1

Define the IPv6 network gateway address. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv6 address.

## Network [n] IPv6 DHCPOptions

n: 1..1

Retrieve a set of DHCP options, for example NTP and DNS server addresses, from a DHCPv6 server.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: Disable the retrieval of DHCP options from a DHCPv6 server.

On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

## Network [n] MTU

n: 1..1

Define the Ethernet MTU (Maximum Transmission Unit) size. The MTU size must be supported by your network infrastructure. The minimum size is 576 for IPv4 and 1280 for IPv6.

Requires user role: ADMIN, USER

Default value: 1500

Value space: Integer (576..1500)

Set a value for the MTU (bytes).

## Network [n] QoS Mode

n: 1..1

The QoS (Quality of Service) is a method which handles the priority of audio, video and data in the network. The QoS settings must be supported by the infrastructure. DiffServ (Differentiated Services) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying, managing network traffic and providing QoS priorities on modern IP networks.

Requires user role: ADMIN, USER

Default value: Diffserv

Value space: Off/Diffserv

Off: No QoS method is used.

Diffserv: When you set the QoS Mode to DiffServ, the Network QoS DiffServ Audio, Network QoS DiffServ Video, Network QoS DiffServ Data, Network QoS DiffServ Signalling, Network QoS DiffServ ICMPv6 and Network QoS DiffServ NTP settings are used to prioritize packets.

## Network [n] QoS Diffserv Audio

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Audio packets should have in the IP network.

The priority for the packets ranges from 0 to 63 – the higher the number, the higher the priority. The recommended class for Audio is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the audio packets in the IP network – the higher the number, the higher the priority. 0 means "best effort".

## Network [n] QoS Diffserv Video

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets on the presentation channel (shared content) are also in the Video packet category. The priority for the packets ranges from 0 to 63 – the higher the number, the higher the priority. The recommended class for Video is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the video packets in the IP network – the higher the number, the higher the priority. 0 means "best effort".

## Network [n] QoS Diffserv Data

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Data packets should have in the IP network.

The priority for the packets ranges from 0 to 63 – the higher the number, the higher the priority. The recommended value for Data is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the data packets in the IP network – the higher the number, the higher the priority. 0 means "best effort".

## Network [n] QoS Diffserv Signalling

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority Signalling packets that are deemed critical (time-sensitive) for the real-time operation should have in the IP network.

The priority for the packets ranges from 0 to 63 – the higher the number, the higher the priority. The recommended class for Signalling is CS3, which equals the decimal value 24. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the signalling packets in the IP network – the higher the number, the higher the priority. 0 means "best effort".

## Network [n] QoS Diffserv ICMPv6

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority ICMPv6 packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for ICMPv6 is 0, which means best effort. If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the ICMPv6 packets in the IP network - the higher the number, the higher the priority. 0 means "best effort".

## Network [n] QoS Diffserv NTP

n: 1..1

This setting will only take effect if Network QoS Mode is set to Diffserv.

Define which priority NTP packets should have in the IP network.

The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for NTP is 0, which means "best effort". If in doubt, contact your network administrator.

The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the NTP packets in the IP network - the higher the number, the higher the priority. 0 means "best effort".

## Network [n] RemoteAccess Allow

n: 1..1

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the device from SSH/HTTP/HTTPS. Multiple IP addresses are separated by a white space.

A network mask (IP range) is specified by <ip address>/N, where N is 1-32 for IPv4, and N is 1-128 for IPv6. The /N is a common indication of a network mask where the first N bits are set. Thus 192.168.0.0/24 would match any address starting with 192.168.0, since these are the first 24 bits in the address.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

A valid IPv4 address or IPv6 address.

## Network [n] Speed

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/10half/10full/100half/100full/1000full

Auto: Auto-negotiate link speed.

10half: Force link to 10 Mbps half-duplex.

10full: Force link to 10 Mbps full-duplex.

100half: Force link to 100 Mbps half-duplex.

100full: Force link to 100 Mbps full-duplex.

1000full: Force link to 1 Gbps full-duplex.

## Network [n] TrafficControl Mode

n: 1..1

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: Transmit video packets at link speed.

On: Transmit video packets at maximum 20 Mbps. Can be used to smooth out bursts in the outgoing network traffic.

## Network [n] VLAN Voice Mode

n: 1..1

Define the VLAN voice mode. The VLAN Voice Mode will be set to Auto automatically if you have Cisco UCM (Cisco Unified Communications Manager) as provisioning infrastructure. Note that Auto mode will NOT work if the NetworkServices CDP Mode setting is Off.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/Manual/Off

Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled.

Manual: The VLAN ID is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.

Off: VLAN is not enabled.

## Network [n] VLAN Voice VlanId

n: 1..1

Define the VLAN voice ID. This setting will only take effect if Network VLAN Voice Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: 1

Value space: Integer (1..4094)

Set the VLAN voice ID.

## NetworkServices settings

### NetworkServices CDP Mode

Enable or disable the CDP (Cisco Discovery Protocol) daemon. Enabling CDP will make the device report certain statistics and device identifiers to a CDP-enabled switch. If CDP is disabled, the Network VLAN Voice Mode: Auto setting will not work.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

### NetworkServices H323 Mode

Define whether the device should be able to place and receive H.323 calls or not.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable the possibility to place and receive H.323 calls.

On: Enable the possibility to place and receive H.323 calls.

### NetworkServices HTTP Mode

Define whether or not to allow access to the device using the HTTP or HTTPS (HTTP Secure) protocols. Note that the device's web interface use HTTP or HTTPS. If this setting is switched Off, you cannot use the web interface.

For additional security (encryption and decryption of requests and pages that are returned by the web server), allow only HTTPS.

Note: The default value is HTTP+HTTPS for devices that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the device has not been factory reset after the upgrade.

Requires user role: ADMIN

Default value: HTTPS (changed from HTTP+HTTPS to HTTPS in CE9.4)

Value space: Off/HTTP+HTTPS/HTTPS

Off: Access to the device not allowed via HTTP or HTTPS.

HTTP+HTTPS: Access to the device allowed via both HTTP and HTTPS.

HTTPS: Access to the device allowed via HTTPS, but not via HTTP.

### NetworkServices HTTP Proxy LoginName

This is the username part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 80)

The authentication login name.



## NetworkServices HTTP Proxy Password

This is the password part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The authentication password.

## NetworkServices HTTP Proxy Mode

The HTTP proxy for Cisco Webex can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

Requires user role: ADMIN, USER

Default value: Off

Value space: Manual/Off/PACUrl/WPAD

Manual: Enter the address of the proxy server in the NetworkServices HTTP Proxy URL setting. Optionally, also add the HTTP proxy login name and password in the NetworkServices HTTP Proxy LoginName/Password settings.

Off: The HTTP proxy mode is turned off.

PACUrl: The HTTP proxy is auto-configured. You must enter the URL for the PAC (Proxy Auto Configuration) script in the NetworkServices HTTP Proxy PACUrl setting.

WPAD: With WPAD (Web Proxy Auto Discovery) the HTTP proxy is fully automated and auto-configured.

## NetworkServices HTTP Proxy Url

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

The URL of the HTTP proxy server.

## NetworkServices HTTP Proxy PACUrl

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

The URL of the PAC (Proxy Auto Configuration) script.

## NetworkServices HTTPS OCSP Mode

Define the support for OCSP (Online Certificate Status Protocol) responder services. The OCSP feature allows users to enable OCSP instead of certificate revocation lists (CRLs) to check the certificate status.

For any outgoing HTTPS connection, the OCSP responder is queried of the status. If the corresponding certificate has been revoked, then the HTTPS connection will not be used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable OCSP support.

On: Enable OCSP support.

## NetworkServices HTTPS OCSP URL

Define the URL of the OCSP responder (server) that will be used to check the certificate status.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid URL.

## NetworkServices HTTPS Server MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.1

Value space: TLSv1.1/TLSv1.2

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

## NetworkServices HTTPS StrictTransportSecurity

The HTTP Strict Transport Security header lets a web site inform the browser that it should never load the site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

## NetworkServices HTTPS VerifyServerCertificate

When the video conferencing device connects to an external HTTPS server (like a phone book server or an external manager), this server will present a certificate to the device to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify server certificates.

On: Requires the device to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the device in advance.

## NetworkServices HTTPS VerifyClientCertificate

When the video conferencing device connects to an HTTPS client (like a web browser), the client can be asked to present a certificate to the video conferencing device to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify client certificates.

On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the device in advance.

## NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the device's time and date to a reference time server. The time server will be queried regularly for time updates.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Manual/Off

Auto: The device will use an NTP server for time reference. As default, the server address will be obtained from the network's DHCP server. If a DHCP server is not used, or if the DHCP server does not provide an NTP server address, the NTP server address that is specified in the NetworkServices NTP Server [n] Address setting will be used.

Manual: The device will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The device will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

## NetworkServices NTP Server [n] Address

n: 1..3

The address of the NTP server that will be used when NetworkServices NTP Mode is set to Manual, and when NetworkServices NTP Mode is set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN

Default value: "0.tandberg.pool.ntp.org"

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

## NetworkServices NTP Server [n] Key

n: 1..3

To make sure that the NTP information comes from a trusted source, the video conferencing device must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 2045)

The key, which is part of the ID/key pair that the NTP source uses.

## NetworkServices NTP Server [n] KeyId

n: 1..3

To make sure that the NTP information comes from a trusted source, the video conferencing device must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 10)

The ID, which is part of the ID/key pair that the NTP source uses.

## NetworkServices NTP Server [n] KeyAlgorithm

n: 1..3

Choose the authentication hash function that the NTP server uses, and that the video conferencing device must use to authenticate the time messages.

Requires user role: ADMIN

Default value: ""

Value space: None/SHA1/SHA256

None: The NTP server doesn't use a hash function.

SHA1: The NTP server uses the SHA-1 hash function.

SHA256: The NTP server uses the SHA-256 hash function (from the SHA-2 family of hash functions).

## NetworkServices SIP Mode

Define whether the device should be able to place and receive SIP calls or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the possibility to place and receive SIP calls.

On: Enable the possibility to place and receive SIP calls.

## NetworkServices SMTP Mode

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.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable SMTP (and email) support.

On: Enable SMTP support for sending email.

## NetworkServices SMTP Server

This is the address of the SMTP server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

## NetworkServices SMTP Port

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.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..65535)

The port used for outgoing emails from the device.

## NetworkServices SMTP Username

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.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

A valid username.

## NetworkServices SMTP Password

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.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid password.

## NetworkServices SMTP From

When sending an email message from this device, this is the name of the mailbox that the message is sent from.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

An email address that meets the requirements of the SMTP server.

## NetworkServices SMTP Security

Choose if and how to secure the communication between the device and the SMTP server.

Requires user role: ADMIN

Default value: None

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

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed devices, which describe the device configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Requires user role: ADMIN, INTEGRATOR

Default value: ReadOnly

Value space: Off/ReadOnly/ReadWrite

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

ReadWrite: Enable the SNMP network service for both queries and commands.

## NetworkServices SNMP Host [n] Address

n: 1..3

Define the address of up to three SNMP Managers.

The device's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), for example about device location and device contact. SNMP traps are not supported.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

## NetworkServices SNMP CommunityName

Define the name of the Network Services SNMP Community. SNMP Community names are used to authenticate SNMP requests. SNMP requests must have a password (case sensitive) in order to receive a response from the SNMP Agent in the device. The default password is "public". If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE: The SNMP Community password is case sensitive.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

The SNMP community name.

## NetworkServices SNMP SystemContact

Define the name of the Network Services SNMP System Contact.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

The name of the SNMP system contact.

## NetworkServices SNMP SystemLocation

Define the name of the Network Services SNMP System Location.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

The name of the SNMP system location.

## NetworkServices SSH Mode

The SSH (or Secure Shell) protocol can provide secure encrypted communication between the video conferencing device and your local computer.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

## NetworkServices SSH HostKeyAlgorithm

Choose the cryptographic algorithm that shall be used for the SSH host key. Choices are RSA (Rivest-Shamir-Adleman) with 2048 bits keysize, ECDSA (Elliptic Curve Digital Signature Algorithm) with NIST curve P-384, and EdDSA (Edwards-curve Digital Signature Algorithm) with ed25519 signature schema.

Requires user role: ADMIN

Default value: RSA

Value space: ECDSA/RSA/ed25519

ECDSA: Use the ECDSA algorithm (nist-384p).

RSA: Use the RSA algorithm (2048 bits).

ed25519: Use the ed25519 algorithm.

## NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the device.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH public key is not allowed.

On: The SSH public key is allowed.

## NetworkServices UPnP Mode

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video conferencing device has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video conferencing device. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting.

When UPnP is enabled, the device advertises its presence on the network. The advertisement permits a Touch controller to discover video conferencing devices automatically, and you do not need to manually enter the device's IP address in order to pair the Touch controller.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: UPnP is disabled. The video conferencing device does not advertise its presence, and you have to enter the device's IP address manually in order to pair a Touch controller to the device.

On: UPnP is enabled. The video conferencing device advertises its presence until the timeout period expires.

## NetworkServices UPnP Timeout

Define for how many seconds UPnP shall stay enabled after the device is switched on or restarted. The NetworkServices UPnP Mode setting must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: 600

Value space: Integer (0..3600)

Range: Select a value between 0 and 3600 seconds.

## NetworkServices Websocket

It is possible to interact with the API of the device over the WebSocket protocol, both the insecure and secure versions (ws and wss). A WebSocket is tied to HTTP, so that also HTTP or HTTPS must be enabled before you can use WebSockets (see the NetworkServices HTTP Mode setting).

Requires user role: ADMIN

Default value: Off

Value space: FollowHTTPSService/Off

FollowHTTPSService: Communication over the WebSocket protocol is allowed when HTTP or HTTPS is enabled.

Off: Communication over the WebSocket protocol is not allowed.

## NetworkServices WelcomeText

Choose which information the user should see when logging on to the device through SSH.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The welcome text is: Login successful

On: The welcome text is: Welcome to <system name>; Software version; Software release date; Login successful.

## NetworkServices Wifi Allowed

Devices that have a built-in Wi-Fi adapter, can connect to the network either via Ethernet or Wi-Fi. Both Ethernet and Wi-Fi are allowed by default, and the user can choose which one to use from the user interface. With this setting, the administrator can disable Wi-Fi configuration, so that it cannot be set up from the user interface.

The devices support the following standards: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac. The device supports the following security protocols: WPA-PSK (AES), WPA2-PSK (AES), EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, EAP-MSCHAPv2, EAP-GTC, and open networks (not secured).

If the PID (Product ID), found on the rating label at the rear of the device, contains the letters NR (No Radio) the device does not support Wi-Fi.

Requires user role: ADMIN, USER

Default value: True

Value space: False/True

False: Wi-Fi cannot be used. You must connect to the network via Ethernet.

True: Both Ethernet and Wi-Fi are allowed.

## NetworkServices Wifi Enabled

Provided that the device is allowed to connect to the network via Wi-Fi (see the NetworkServices WIFI Allowed setting), you can use this setting to enable and disable Wi-Fi.

You cannot use Ethernet and Wi-Fi at the same time. If you try to configure Wi-Fi while an Ethernet cable is connected, you must unplug the Ethernet cable to proceed. If you connect an Ethernet cable while connected to Wi-Fi, Ethernet will take precedence. If you unplug the Ethernet cable, the device will automatically connect to the last connected Wi-Fi network, if available.

Requires user role: ADMIN, USER

Default value: True

Value space: False/True

False: Wi-Fi is disabled.

True: Wi-Fi is enabled.

## NetworkServices XMLAPI Mode

Enable or disable the device's XML API. For security reasons this may be disabled. Disabling the XML API will limit the remote manageability with for example TMS, which no longer will be able to connect to the device.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The XML API is disabled.

On: The XML API is enabled.



## Peripherals settings

### Peripherals Profile Cameras

Define the number of 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.

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: 0

0: The number of cameras that are expected to be connected to the device.

### Peripherals Profile ControlSystems

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

Such information is currently not available on this product.

Requires user role: ADMIN, INTEGRATOR

Default value: NotSet

Value space: NotSet

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

## Phonebook settings

### Phonebook Server [n] ID

n: 1..1

Define a name for the external phone book.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The name for the external phone book.

### Phonebook Server [n] Pagination

n: 1..1

Configure if the phonebook server supports pagination (paging) or not. Pagination means that the server supports consecutive searches, and these searches can be relative to an offset. This allows the user interface to perform as many consecutive searches as required to get the complete search result.

If Pagination is Disabled the device does a single search and returns a maximum of 100 entries in the search result. It is not possible to scroll to any further search results beyond that.

Requires user role: ADMIN

Default value: Enabled

Value space: Disabled/Enabled

Disabled: The phonebook server does not support pagination. The device does a single search, and the maximum number of entries in the search result is 100.

Enabled: The phonebook server supports pagination.

### Phonebook Server [n] Type

n: 1..1

Select the phonebook server type.

Requires user role: ADMIN

Default value: Off

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

Off: Do not use a phonebook.

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

Spark: The phonebook is located in the Cisco Webex cloud service.

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

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

### Phonebook Server [n] URL

n: 1..1

Define the address (URL) to the external phone book server.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid address (URL) to the phone book server.

## Provisioning settings

### Provisioning Connectivity

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Internal/External/Auto

Internal: Request internal configuration.

External: Request external configuration.

Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the "e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

### Provisioning ExternalManager Address

Define the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the device will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.

When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

### Provisioning ExternalManager AlternateAddress

Only applicable when the device is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Define the address of the alternate CUCM. If the main CUCM is not available, the device will be provisioned by the alternate CUCM. When the main CUCM is available again, the device will be provisioned by this CUCM.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

### Provisioning ExternalManager Protocol

Define whether to use the HTTP (unsecure communication) or HTTPS (secure communication) protocol when sending requests to the external manager / provisioning system.

The selected protocol must be enabled in the NetworkServices HTTP Mode setting.

Requires user role: ADMIN, USER

Default value: HTTP

Value space: HTTPS/HTTP

HTTPS: Send requests via HTTPS.

HTTP: Send requests via HTTP.

## Provisioning ExternalManager Path

Define the Path to the external manager / provisioning system. This setting is required when several management services reside on the same server, i.e. share the same External Manager address.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

A valid path to the external manager or provisioning system.

## Provisioning ExternalManager Domain

Define the SIP domain for the VCS provisioning server.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid domain name.

## Provisioning Mode

It is possible to configure a device using a provisioning system (external manager). This allows video conferencing network administrators to manage many devices simultaneously. With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/representative for more information.

Requires user role: ADMIN, USER

Default value: Auto

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

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

Auto: The provisioning server is automatically selected as set up in the DHCP server.

CUCM: Push configurations to the device from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the device from CUCM (Cisco Unified Communications Manager). The device connects to CUCM via the Expressway infrastructure. In order to register over Expressway the encryption option key must be installed on the device.

Webex: Push configurations to the device from the Cisco Webex cloud service.

TMS: Push configurations to the device from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the device from VCS (Cisco TelePresence Video Communication Server).

## Provisioning LoginName

This is the username part of the credentials used to authenticate the device with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 80)

A valid username.

## Provisioning Password

This is the password part of the credentials used to authenticate the device with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid password.

## Proximity settings

### Proximity Mode

Determine whether the device will emit ultrasound pairing messages or not.

When the device emits ultrasound, Proximity 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). In general, Cisco recommends enabling all the Proximity services.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The device does not emit ultrasound, and Proximity services cannot be used.

On: The device emits ultrasound, and Proximity clients can detect that they are close to the device. Enabled Proximity services can be used.

### Proximity Services CallControl

Enable or disable basic call control features on Proximity clients. When this setting is enabled, you are able to control a call using a Proximity client (for example dial, mute, adjust volume and hang up). This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Call control from a Proximity client is enabled.

Disabled: Call control from a Proximity client is disabled.

### Proximity Services ContentShare FromClients

Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the device, e.g. share your laptop screen. This service is supported by laptops (OS X and Windows). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Enabled

Value space: Enabled/Disabled

Enabled: Content sharing from a Proximity client is enabled.

Disabled: Content sharing from a Proximity client is disabled.

### Proximity Services ContentShare ToClients

Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the device. You can zoom in on details, view previous content and take snapshots. This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Content sharing to a Proximity client is enabled.

Disabled: Content sharing to a Proximity client is disabled.

## RoomAnalytics settings

### RoomAnalytics AmbientNoiseEstimation Mode

The device can estimate the stationary ambient noise level (background noise level) in the room. The result is reported in the RoomAnalytics AmbientNoise Level dBA status. The status is updated when a new ambient noise level is detected.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

On: The device regularly estimates the stationary ambient noise level.

Off: The device doesn't estimate the stationary ambient noise level.

### RoomAnalytics PeopleCountOutOfCall

By using face detection, the device has the capability to find how many persons are in the room. By default, the device only counts people when in a call, or when displaying the self-view picture.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

Off: The device counts people only when the device is in a call, or when self-view is on.

On: The device counts people as long as the device is not in standby mode. This includes outside of call, even if self-view is off.

### RoomAnalytics PeoplePresenceDetector

The device has the capability to find whether or not people are present in the room, and report the result in the RoomAnalytics PeoplePresence status. This feature is based on ultrasound. It takes a minimum of 2 minutes to detect whether people are present or not in the room, and it may take up to 2 minutes for the status to change after the room becomes vacant.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Off

Value space: Off/On

Off: The device's status does not show whether or not there are people present in the room.

On: The device's status shows whether or not there are people present in the room.

## RoomReset settings

### RoomReset Control

This setting is for use with control systems or macros. Macros allow you to write snippets of JavaScript code that can automate parts of your video conferencing device, thus creating custom behavior.

When a room has been idle for some time the video conferencing device can send an event to indicate that the room is ready to be reset.

The events that are sent when this setting is enabled are:

```
*e RoomReset SecondsToReset: 30
```

```
** end
```

```
*e RoomReset Reset
```

```
** end
```

Requires user role: ADMIN

Default value: On

Value space: CameraPositionsOnly/Off/On

CameraPositionsOnly: Not applicable.

Off: No RoomReset events will be sent.

On: The room reset control is enabled and RoomReset events will be sent.



## RTP settings

### RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the device is using the ports in the range 2326 to 2487 for RTP and RTCP media data. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2326

Value space: Integer (1024..65438)

Set the first port in the range of RTP ports. The value must be an even number.

### RTP Ports Range Stop

Define the last port in the range of RTP ports.

As default, the device is using the ports in the range 2326 to 2487 for RTP and RTCP media data. If the RTP Video Ports Range is enabled the device is using the ports in the range 1024 to 65436. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2486

Value space: Integer (1120..65535)

Set the last port in the range of RTP ports. The value must be an odd number. If you enter an even value, +1 will be automatically applied.

### RTP Video Ports Range Start

Define the first port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65454)

Set the first port in the range of RTP video ports.

### RTP Video Ports Range Stop

Define the last port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65535)

Set the last port in the range of RTP video ports.

## Security settings

### Security Audit Logging Mode

Define where to record or transmit the audit logs. The audit logs are sent to a syslog server. This setting has no effect if the Logging Mode setting is set to Off.

When using the External or ExternalSecure mode you must enter the address of the audit server in the Security Audit Server Address setting.

Requires user role: AUDIT

Default value: Internal

Value space: External/ExternalSecure/Internal/Off

**External:** The device sends the audit logs to an external syslog server. The syslog server must support UDP.

**ExternalSecure:** The device sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the device using the web interface. The `common_name` parameter of a certificate in the CA list must match the IP address or DNS name of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

**Internal:** The device records the audit logs to internal logs, and rotates logs when they are full.

**Off:** No audit logging is performed.

### Security Audit OnError Action

Define what happens when the connection to the syslog server is lost. This setting is only relevant when Security Audit Logging Mode is set to ExternalSecure.

Requires user role: AUDIT

Default value: Ignore

Value space: Halt/Ignore

**Halt:** If a halt condition is detected the device is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the syslog server. Halt conditions are: A network breach (no physical link), no syslog server running (or incorrect address or port to the syslog server), TLS authentication failed (if in use), local backup (re-spooling) log full.

**Ignore:** The device will continue its normal operation, and rotate internal logs when full. When the connection is restored it will again send its audit logs to the syslog server.

### Security Audit Server Address

Set the IP address or DNS name of the syslog server that the audit logs are sent to. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

Requires user role: AUDIT

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address, or DNS name.

### Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the device shall send its audit logs to. This setting is only relevant when Security Audit Server PortAssignment is set to Manual.

Requires user role: AUDIT

Default value: 514

Value space: Integer (0..65535)

Set the audit server port.

## Security Audit Server PortAssignment

The audit logs are sent to a syslog server. You can define how the port number of the external syslog server will be assigned. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure. To see which port number is used you can check the Security Audit Server Port status. Navigate to Setup > Status on the web interface or; if on a command line interface, run the command `xStatus Security Audit Server Port`.

Requires user role: AUDIT

Default value: Auto

Value space: Auto/Manual

Auto: Will use UDP port number 514 when the Security Audit Logging Mode is set to External. Will use TCP port number 6514 when the Security Audit Logging Mode is set to ExternalSecure.

Manual: Will use the port value defined in the Security Audit Server Port setting.

## Security Session FailedLoginsLockoutTime

Define how long the device will lock out a user after failed login to a web or SSH session. Restart the device for any change to this setting to take effect.

Requires user role: ADMIN

Default value: 60

Value space: Integer (0..10000)

Set the lockout time (minutes).

## Security Session InactivityTimeout

Define how long the device will accept inactivity from the user before he is automatically logged out from a web or SSH session.

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10000)

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

## Security Session MaxFailedLogins

Define the maximum number of failed login attempts per user for a web or SSH session. If the user exceeded the maximum number of attempts the user will be locked out. 0 means that there is no limit for failed logins.

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10)

Set the maximum number of failed login attempts per user.

## Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions per user.

## Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions in total.

## Security Session ShowLastLogon

When logging in to the device using SSH you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

On: Show information about the last session.

Off: Do not show information about the last session.

## SerialPort settings

### SerialPort Mode

Enable/disable the serial port.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the serial port.

On: Enable the serial port.

### SerialPort BaudRate

Set the baud rate (data transmission rate, bits per second) for the serial port.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

Requires user role: ADMIN, INTEGRATOR

Default value: 115200

Value space: 115200

Choose a baud rate from the baud rates listed (bps).

### SerialPort LoginRequired

Define if login shall be required when connecting to the serial port.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The user can access the device via the serial port without any login.

On: Login is required when connecting to the device via the serial port.

## SIP settings

### SIP ANAT

ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable ANAT.

On: Enable ANAT.

### SIP Authentication UserName

This is the username part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid username.

### SIP Authentication Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

### SIP DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/TCP/Tls/UDP

TCP: The device will always use TCP as the default transport method.

UDP: The device will always use UDP as the default transport method.

Tls: The device will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the device. If no such CA-list is available on the device then anonymous Diffie Hellman will be used.

Auto: The device will try to connect using transport protocols in the following order: TLS, TCP, UDP.

### SIP DisplayName

When configured the incoming call will report the display name instead of the SIP URI.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 550)

The name to be displayed instead of the SIP URI.

## SIP Ice DefaultCandidate

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

Requires user role: ADMIN

Default value: Host

Value space: Host/Rflx/Relay

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

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

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

## SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the devices can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the devices.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

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

Off: ICE is disabled.

On: ICE is enabled.

## SIP Line

When registered to a Cisco Unified Communications Manager (CUCM) the device may be part of a shared line. This means that several devices share the same directory number. The different devices sharing the same number receive status from the other appearances on the line as defined in RFC 4235.

Note that shared lines are set up by CUCM, not by the device. Therefore do not change this setting manually; CUCM pushes this information to the device when required.

Requires user role: ADMIN

Default value: Private

Value space: Private/Shared

Shared: The device is part of a shared line and is therefore sharing its directory number with other devices.

Private: This device is not part of a shared line.

## SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the device will only be reachable through the SIP registrar (CUCM or VCS). As a security measure, SIP ListenPort should be Off when the device is registered to a SIP Proxy.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Listening for incoming connections on the SIP TCP/UDP ports is turned off.

On: Listening for incoming connections on the SIP TCP/UDP ports is turned on.

## SIP Mailbox

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid number or address. Leave the string empty if you do not have a voice mailbox.

## SIP MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.0

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

TLSv1.0: Support TLS version 1.0 or higher.

TLSv1.1: Support TLS version 1.1 or higher.

TLSv1.2: Support TLS version 1.2 or higher.

## SIP PreferredIPSignaling

Define the preferred IP version for signaling (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version. It also determines the priority of the A/AAAA lookups in DNS, so that the preferred IP version is used for registration.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

## SIP Proxy [n] Address

n: 1..4

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

## SIP TlsVerify

For TLS connections a SIP CA-list can be uploaded to the device. This can be done from the web interface.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.

On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

## SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the device will test if port allocation is possible.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Set to Off to disable discovery mode.

On: When set to On, the device will search for available Turn servers in DNS, and before making calls the device will test if port allocation is possible.

## SIP Turn DropRflx

DropRflx will make the device force media through the Turn relay, unless the remote device is on the same network.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable DropRflx.

On: The device will force media through the Turn relay when the remote device is on another network.



## SIP Turn Server

Define the address of the TURN (Traversal Using Relay NAT) server. It is used as a media relay fallback and it is also used to discover the device's own public IP address.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

The preferred format is DNS SRV record (e.g. `_turn._udp.<domain>`), or it can be a valid IPv4 or IPv6 address.

## SIP Turn UserName

Define the username needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid username.

## SIP Turn Password

Define the password needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

## SIP Type

Enables SIP extensions and special behavior for a vendor or provider.

Requires user role: ADMIN

Default value: Standard

Value space: Standard/Cisco

Standard: Use this when registering to standard SIP Proxy (tested with Cisco TelePresence VCS).

Cisco: Use this when registering to Cisco Unified Communication Manager.

## SIP URI

The SIP URI (Uniform Resource Identifier) is the address that is used to identify the device. The URI is registered and used by the SIP services to route inbound calls to the device. The SIP URI syntax is defined in RFC 3261.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

An address (URI) that is compliant with the SIP URI syntax.

## Standby settings

### Standby Control

Define whether the device should go into standby mode or not.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The device will not enter standby mode.

On: The device will enter standby mode when the Standby Delay has timed out. Requires the Standby Delay to be set to an appropriate value.

### Standby Delay

Define how long (in minutes) the device shall be in idle mode before it goes into standby mode. Requires the Standby Control to be enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: 4

Value space: Integer (1..480)

Set the standby delay (minutes).

### Standby WakeupOnMotionDetection

Automatic wake up on motion detection is a feature that will sense when a person walks into the room. The feature is based on ultrasound detection.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The wake up on motion detection is disabled.

On: When people walk into the room the device will automatically wake up from standby.

## SystemUnit settings

### SystemUnit Name

Define the device name. The device name will be sent as the hostname in a DHCP request and when the device is acting as an SNMP Agent.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

Define the device name.

### SystemUnit CrashReporting Advanced

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The ACR tool will perform standard log analyses.

On: The ACR tool will perform advanced log analyses.

### SystemUnit CrashReporting Mode

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: No logs will be sent to ACR tool.

On: The logs will automatically be sent to ACR tool.

### SystemUnit CrashReporting Url

If the device crashes, the device can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: "acr.cisco.com"

Value space: String (0..255)

The URL to the Cisco Automatic Crash Report tool (ACR).

## Time settings

### Time TimeFormat

Define the time format.

Requires user role: ADMIN, USER

Default value: 24H

Value space: 24H/12H

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours (AM/PM).

### Time DateFormat

Define the date format.

Requires user role: ADMIN, USER

Default value: DD\_MM\_YY

Value space: DD\_MM\_YY/MM\_DD\_YY/YY\_MM\_DD

DD\_MM\_YY: The date January 30th 2010 will be displayed: 30.01.10

MM\_DD\_YY: The date January 30th 2010 will be displayed: 01.30.10

YY\_MM\_DD: The date January 30th 2010 will be displayed: 10.01.30

## Time Zone

Define the time zone for the geographical location of the device. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Etc/UTC

Value space: Africa/Abidjan, Africa/Accra, Africa/Addis\_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar\_es\_Salaam, Africa/Djibouti, Africa/Douala, Africa/EL\_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Novo, Africa/Sao\_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos\_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La\_Rioja, America/Argentina/Mendoza, America/Argentina/Rio\_Gallegos, America/Argentina/Salta, America/Argentina/San\_Juan, America/Argentina/San\_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia\_Banderas, America/Barbados, America/Belem, America/Belize, America/Blanc-Sablon, America/Boa\_Vista, America/Bogota, America/Boise, America/Buenos\_Aires, America/Cambridge\_Bay, America/Campo\_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral\_Harbour, America/Cordoba, America/Costa\_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson\_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunepe, America/El\_Salvador, America/Ensenada, America/Fort\_Nelson, America/Fort\_Wayne, America/Fortaleza, America/Glace\_Bay, America/Godthab, America/Goose\_Bay, America/Grand\_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell\_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Juneau, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox\_IN, America/Kralendijk, America/La\_Paz, America/Lima, America/Los\_Angeles, America/Louisville, America/Lower\_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metlakatla, America/Mexico\_City, America/

Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New\_York, America/Nipigon, America/Nome, America/Noronha, America/North\_Dakota/Beulah, America/North\_Dakota/Center, America/North\_Dakota/New\_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port\_of\_Spain, America/Porto\_Acre, America/Porto\_Velho, America/Puerto\_Rico, America/Rainy\_River, America/Rankin\_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio\_Branco, America/Rosario, America/Santa\_Isabel, America/Santarem, America/Santiago, America/Santo\_Domingo, America/Sao\_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St\_Barthelemy, America/St\_Johns, America/St\_Kitts, America/St\_Lucia, America/St\_Thomas, America/St\_Vincent, America/Swift\_Current, America/Tegucigalpa, America/Thule, America/Thunder\_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDURville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South\_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Choibalsan, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho\_Chi\_Minh, Asia/Hong\_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabul, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala\_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Omsk, Asia/Oral, Asia/Phnom\_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Te\_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung\_Pandang, Asia/Ulaanbaatar, Asia/Ulan\_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape\_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan\_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South\_Georgia, Atlantic/St\_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken\_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord\_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/

GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle\_of\_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San\_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofu, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago\_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port\_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu

Select a time zone from the list.

## UserInterface settings

### UserInterface Accessibility IncomingCallNotification

You can enable an incoming call notification with amplified visuals. The screen and Touch 10 will flash red/white approximately once every second (1.75 Hz) to make it easier for hearing impaired users to notice an incoming call. If the device is already in a call the screen will not flash as this will disturb the on-going call, instead you will get a normal notification on screen and touch panel.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Default

Value space: AmplifiedVisuals/Default

AmplifiedVisuals: Enable the amplified visuals on screen and touch panel when the device receives a call.

Default: Enable the default behavior with a notification on screen and touch panel.

### UserInterface Branding AwakeBranding Colors

If the device is set up with branding customizations, this setting affects the colors of the logo that is shown when the device is awake. You can choose whether you want to show the logo in full color, or reduce the opacity of the logo so that it blends in more naturally with the background and other elements on the screen.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Native

Auto: The opacity of the logo is reduced.

Native: The logo has full colors.

### UserInterface ContactInfo Type

Choose which type of contact information to show in the user interface.

Requires user role: ADMIN

Default value: Auto

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

Auto: Show the address which another device should dial to reach this video conferencing device. The address depends on the default call protocol and device registration.

None: Do not show any contact information.

IPv4: Show the device's IPv4 address.

IPv6: Show the device's IPv6 address.

H323Id: Show the device's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the device's H.320 number as contact information (only supported if used with Cisco TelePresence ISDN Link).

E164Alias: Show the device's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

SipUri: Show the device's SIP URI (refer to the SIP URI setting).

SystemName: Show the device's name (refer to the SystemUnit Name setting).

DisplayName: Show the device's display name (refer to the SIP DisplayName setting).

### UserInterface KeyTones Mode

You can configure the device to make a keyboard click sound effect (key tone) when typing text or numbers.

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

## UserInterface Features Call End

Choose whether or not to remove the default End Call button from the user interface. The setting removes only the button, not its functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

## UserInterface Features Call MidCallControls

Choose whether or not to remove the default Hold, Transfer, and Resume in-call buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

## UserInterface Features Call Start

Choose whether or not to remove the default Call button (including the directory, favorites, and recent calls lists) and the default in-call Add participant button from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

## UserInterface Features Call VideoMute

Choose whether or not to show the default "Turn video off" button in the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the "Turn video off" button in the user interface if this feature is supported in the ongoing call.

Hidden: The "Turn video off" button is never shown in the user interface.

## UserInterface Features HideAll

Choose whether or not to remove all default buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: False

Value space: False/True

False: Shows all default buttons in the user interface.

True: Removes all default buttons from the user interface.

## UserInterface Features Share Start

Choose whether or not to remove the default buttons and other UI elements for sharing and previewing content, both in call and out of call, from the user interface. The setting removes only the buttons and UI elements, not their functionality as such. You can share content using Proximity or the Cisco Webex Teams app still.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons and UI elements in the user interface.

Hidden: Removes the default buttons and UI elements from the user interface.



## UserInterface Features Whiteboard Start

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.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

## UserInterface Language

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

Requires user role: ADMIN, USER

Default value: English

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

Select a language from the list.

## UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a locked padlock.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/AlwaysOn/AlwaysOff

Auto: If the call is encrypted, a "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. No encryption indicator icon is shown.

AlwaysOn: The "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

AlwaysOff: The encryption indicator is never displayed on screen.

## UserInterface OSD Output

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: 1

1: The device sends the on-screen information and indicators to the device's integrated screen.

## UserInterface Phonebook Mode

This setting determines if a user is allowed to add or change a contact in the Directory and Favorites list from the user interface of the device.

Requires user role: ADMIN, INTEGRATOR

Default value: ReadWrite

Value space: ReadOnly/ReadWrite

**ReadOnly:** You neither can add a contact to the Favorites list, edit a contact in the Favorites list, nor edit any contact from the Directory or Favorites list before calling.

**ReadWrite:** You are able to add a contact to the Favorites list, edit a contact in the Favorites list, and edit a contact from the Directory or Favorites list before calling.

## UserInterface Security Mode

This setting allows you to prevent important device information from being exposed in the user interface (drop down menu and Settings panel), for example the contact information and IP addresses of the video conferencing device, touch controller, and UCM/VCS registrars. It is important to note that such information is not hidden when navigating further into the Settings panel.

If you want to fully prevent that people without administrator rights can see the contact information, IP addresses, MAC address, serial number, and software version, you must also set the UserInterface SettingsMenu Mode to Locked, and of course have a passphrase for all user accounts with administrator rights.

Requires user role: ADMIN

Default value: Normal

Value space: Normal/Strong

**Normal:** IP addresses and other device information are shown on the user interface.

**Strong:** Contact information and IP addresses are not displayed on the user interface (drop down menu and Settings panel).

## UserInterface SettingsMenu Mode

The Settings panel in the user interface (Touch 10 or on-screen) can be protected by the device's admin password. If this password is blank, anyone can access the settings in the Settings panel, and for example factory reset the device. If authentication is enabled, all settings that require authentication have a padlock icon. You will be prompted to enter the administrator's username and passphrase when you select the setting. Some settings do not require authentication, they do not have a padlock icon.

Requires user role: ADMIN

Default value: Unlocked

Value space: Locked/Unlocked

**Locked:** Authentication with administrator's username and passphrase is required.

**Unlocked:** No authentication is required.

## UserInterface SettingsMenu Visibility

Choose whether or not to show the device name (or contact information) and the associated drop down menu and Settings panel on the user interface.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Hidden

**Auto:** Shows the device name with drop down menu and Settings panel on the user interface.

**Hidden:** Doesn't show the device name with drop down menu and Settings panel on the user interface.

## UserInterface SoundEffects Mode

You can configure the device to make a sound effect, e.g. when someone connects a laptop or mobile through Proximity.

The keyboard click sound effect when typing text is not affected by this setting (refer to the UserInterface Keytones Mode setting).

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: There are no sound effects.

On: The sound effects are switched on.

## UserInterface Wallpaper

Select a background image (wallpaper) for the video screen when idle.

You may upload a custom wallpaper to the device using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 4 MByte. When you use a custom wallpaper, the clock and the list of upcoming meetings are removed from the main display

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Auto

Value space: Auto/Custom/None

Auto: Use the default wallpaper.

None: There is no background image on the screen.

Custom: Use the custom wallpaper as background image on the screen. If no custom wallpaper is uploaded to the device, the setting will revert to the default value.

## UserManagement settings

### UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges.

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

Refer to the LDAP specification for the syntax of this string. Example:

```
"(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)
(sAMAccountName=username))"
```

### UserManagement LDAP Admin Group

Members of this AD (Active Directory) group will be given administrator access. This setting is a shorthand for saying (memberof:1.2.840.113556.1.4.1941:=<group name>).

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

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

### UserManagement LDAP Attribute

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

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

The attribute name.

### UserManagement LDAP BaseDN

The distinguishing name of the entry at which to start a search (base).

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

The distinguishing name of the base. Example: "DC=company, DC=com"

### UserManagement LDAP Encryption

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

Requires user role: ADMIN

Default value: LDAPS

Value space: LDAPS/None/STARTTLS

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

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

STARTTLS: Connect to the LDAP server on port 389, then send a STARTTLS command to upgrade to an encrypted connection (TLS).

## UserManagement LDAP MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.2

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

TLSv1.0: Support TLS version 1.0 or higher.

TLSv1.1: Support TLS version 1.1 or higher.

TLSv1.2: Support TLS version 1.2 or higher.

## UserManagement LDAP Mode

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

If you switch on LDAP Mode, make sure to configure the other UserManagement LDAP settings to suit your setup. Here is a few examples.

Example 1:

- UserManagement LDAP Mode: On
- UserManagement LDAP Address: "192.0.2.20"
- UserManagement LDAP BaseDN: "DC=company, DC=com"
- UserManagement LDAP Admin Group: "CN=admin group, OU=company groups, DC=company, DC=com"

Example 2:

- UserManagement LDAP Mode: On
- UserManagement LDAP Address: "192.0.2.20"
- UserManagement LDAP BaseDN: "DC=company, DC=com"
- UserManagement LDAP Admin Filter: "(!(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: LDAP authentication is not allowed.

On: LDAP authentication is allowed.

## UserManagement LDAP Server Address

Set the IP address or hostname of the LDAP server.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address or hostname.

## UserManagement LDAP Server Port

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..65535)

The LDAP server port number.

## UserManagement LDAP VerifyServerCertificate

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

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

## Video settings

### Video ActiveSpeaker DefaultPIPPosition

Define the position on screen of the active speaker picture-in-picture (PiP). The setting only takes effect when using a video layout where the active speaker is a PiP, i.e. the Overlay layout, or possibly a Custom layout (refer to the Video DefaultLayoutFamily Local setting). The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the active speaker PiP will be kept unchanged when leaving a call.

UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.

UpperCenter: The active speaker PiP will appear in the upper center position.

UpperRight: The active speaker PiP will appear in the upper right corner of the screen.

CenterLeft: The active speaker PiP will appear in the center left position.

CentreRight: The active speaker PiP will appear in the center right position.

LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.

LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

### Video DefaultLayoutFamily Remote

Select which video layout family to be used in the stream that is sent to the remote participants (far end). This setting applies only when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single

Auto: The default layout family, as given by the local layout database, will be used as the remote layout.

Equal: The Equal layout family will be used as the remote layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the remote layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the remote layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

### Video DefaultMainSource

Define which video input source to be used as the default main video source when you start a call.

Requires user role: ADMIN, USER

Default value: 1

Value space: 1

The source that is used as the default main video source.

## Video Input Connector [n] CameraControl Camerald

n: 1..2

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: 1

Value space: Connector n: 1

The camera ID is fixed and cannot be changed.

## Video Input Connector [n] CameraControl Mode

n: 1..2

Define whether the camera that is connected to this video input connector can be controlled or not.

Note that camera control is not available for Connector 2 (HDMI).

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: On Connector 2: Off

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

Off: Disable camera control.

On: Enable camera control.

## Video Input Connector [n] CEC Mode

n: 2..2

The video input (HDMI) supports Consumer Electronics Control (CEC). When this setting is enabled, information about the connected device (for example device type and device name) is available in the video conferencing device status (Video Input Connector[n] ConnectedDevice CEC [n]), provided that the connected device also supports CEC.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Connector n: Off/On

Off: CEC is disabled.

On: CEC is enabled.

## Video Input Connector [n] InputSourceType

n: 1..2

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: camera Connector 2: PC

Value space: Connector 1: camera Connector 2: PC/camera/document\_camera/mediaplayer/whiteboard/other

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

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

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

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

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

other: Use this when the other options do not match.

## Video Input Connector [n] Name

n: 1..2

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

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

Value space: String (0, 50)

Name for the video input connector.

## Video Input Connector [n] OptimalDefinition Profile

n: 1..2

This setting will not take effect if the corresponding Video Input Connector [n] Quality setting is set to Sharpness.

The optimal definition profile reflects the lighting conditions in the video conferencing room and the quality of the camera. The better lighting conditions and the better quality of the camera, the higher the profile. Generally, the Normal or Medium profiles are recommended. However, when the lighting conditions are very good, the High profile can be set in order to increase the resolution for a given call rate. The resolution must be supported by both the calling and called devices.

Requires user role: ADMIN, INTEGRATOR

Default value: Medium

Value space: Normal/Medium/High

Normal: Use this profile for a normally to poorly lit environment. Resolutions will be set rather conservative.

Medium: Requires good and stable lighting conditions and a good quality video input. For some call rates this leads to higher resolution.

High: Requires nearly optimal video conferencing lighting conditions and a good quality video input in order to achieve a good overall experience. Rather high resolutions will be used.

## Video Input Connector [n] PreferredResolution

n: 2..2

Define the preferred screen resolution and refresh rate that the video conferencing device advertises to the input sources that are connected via HDMI (for example a laptop). The logic for selection of the resolution on the source side will choose this resolution and refresh rate automatically, unless it is overridden manually by the source device (for example the laptop's display configuration software).

Note that the formats 2560\_1440\_60 and 3840\_2160\_30 use about twice the amount of data compared to the 1920\_1080\_60 format, and requires a presentation cable (or adapter) that is qualified for at least HDMI 1.4b data rates.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: 1920\_1080\_60

Value space: Connector n: 1920\_1080\_60/2560\_1440\_60/3840\_2160\_30

1920\_1080\_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

2560\_1440\_60: The resolution is 2560 x 1440, and the refresh rate is 60 Hz.

3840\_2160\_30: The resolution is 3840 x 2160, and the refresh rate is 30 Hz.



## Video Input Connector [n] PresentationSelection

n: 2..2

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: AutoShare

Value space: Connector n: AutoShare/Desktop/Manual/OnConnect

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

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

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

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

## Video Input Connector [n] Quality

n: 2..2

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: Sharpness

Value space: Connector n: Motion/Sharpness

**Motion:** Gives the highest possible frame rate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

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

## Video Input Connector [n] RGBQuantizationRange

n: 2..2

The devices connected to the video input should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any source.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Full/Limited

**Auto:** RGB quantization range is automatically selected based on video format according to CEA-861-E. CE video formats will use limited quantization range levels. IT video formats will use full quantization range levels.

**Full:** Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

**Limited:** Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

## Video Input Connector [n] Visibility

n: 1..2

Define the visibility of the video input connector in the menus on the user interface. Note that Connector 1 is the device's integrated camera, which is not available as a presentation source.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Never Connector 2: IfSignal

Value space: Connector 1: Never Connector 2: Always/IfSignal/Never

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: The menu selection for the video input connector will only be visible when something is connected to the video input.

Never: The input source is not expected to be used as a presentation source, and will not show up on the user interface.

## Video Output Connector [n] Resolution

n: 1..1

The resolution and refresh rate for the integrated screen. This value is fixed and cannot be changed.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 3840\_2160\_60

Value space: 3840\_2160\_60

3840\_2160\_60: The resolution is 3840 x 2160, and the refresh rate is 60 Hz.

## Video Presentation DefaultPiPPosition

Define the position on screen of the presentation picture-in-picture (PiP). The setting only takes effect when the presentation is explicitly minimized to a PiP, for example using the user interface. The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the presentation PiP will be kept unchanged when leaving a call.

UpperLeft: The presentation PiP will appear in the upper left corner of the screen.

UpperCenter: The presentation PiP will appear in the upper center position.

UpperRight: The presentation PiP will appear in the upper right corner of the screen.

CenterLeft: The presentation PiP will appear in the center left position.

CenterRight: The presentation PiP will appear in the center right position.

LowerLeft: The presentation PiP will appear in the lower left corner of the screen.

LowerRight: The presentation PiP will appear in the lower right corner of the screen.

## Video Presentation DefaultSource

Define which video input source to use as a default presentation source. This setting may be used by the API and third-party user interfaces. It is not relevant when using the user interfaces provided by Cisco.

Requires user role: ADMIN, USER

Default value: 2

Value space: 1/2

The video input source to use as default presentation source.

## Video Presentation Priority

Determine how to distribute the bandwidth between the presentation channel and the main video channel.

Requires user role: ADMIN

Default value: Equal

Value space: Equal/High/Low

Equal: The available bandwidth is shared equally between the presentation channel and the main video channel.

High: The presentation channel is assigned a larger portion of the available bandwidth at the expense of the main video channel.

Low: The main video channel is assigned a larger portion of the available bandwidth at the expense of the presentation channel.

## Video Selfview Default FullscreenMode

Define if the main video source (self-view) shall be shown in full screen or as a small picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Off/Current/On

Off: Self-view will be shown as a PiP.

Current: The size of the self-view picture will be kept unchanged when leaving a call, i.e. if it was a PiP during the call, it remains a PiP after the call; if it was fullscreen during the call, it remains fullscreen after the call.

On: The self-view picture will be shown in fullscreen.

## Video Selfview Default Mode

Define if the main video source (self-view) shall be displayed on screen after a call. The position and size of the self-view window is determined by the Video Selfview Default PIPPosition and the Video Selfview Default FullscreenMode settings respectively.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Off/Current/On

Off: Self-view is switched off when leaving a call.

Current: Self-view is left as is, i.e. if it was on during the call, it remains on after the call; if it was off during the call, it remains off after the call.

On: Self-view is switched on when leaving a call.

## Video Selfview Default OnMonitorRole

Define which screen/output to display the main video source (self-view) after a call. The value reflects the monitor roles set for the different outputs in the Video Output Connector [n] MonitorRole setting.

The setting applies both when self-view is displayed in full screen, and when it is displayed as picture-in-picture (PiP).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/First/Second

Current: When leaving a call, the self-view picture will be retained on the same output as it was during the call.

First: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to First.

Second: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to Second.

## Video Selfview Default PIPPosition

Define the position on screen of the small self-view picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting) and fullscreen view is switched off (see the Video Selfview Default FullscreenMode setting).

Requires user role: ADMIN, INTEGRATOR

Default value: LowerRight

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the self-view PiP will be kept unchanged when leaving a call.

UpperLeft: The self-view PiP will appear in the upper left corner of the screen.

UpperCenter: The self-view PiP will appear in the upper center position.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear in the center left position.

CenterRight: The self-view PiP will appear in the center right position.

LowerLeft: The self-view PiP will appear in the lower left corner of the screen.

LowerRight: The self-view PiP will appear in the lower right corner of the screen.

## Video Selfview OnCall Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video Selfview OnCall Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Self-view is not shown automatically during call setup.

On: Self-view is shown automatically during call setup.

## Video Selfview OnCall Duration

This setting only has an effect when the Video Selfview OnCall Mode setting is switched On. In this case, the number of seconds set here determines for how long self-view is shown before it is automatically switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..60)

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

## Experimental settings

The Experimental settings are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

# Appendices

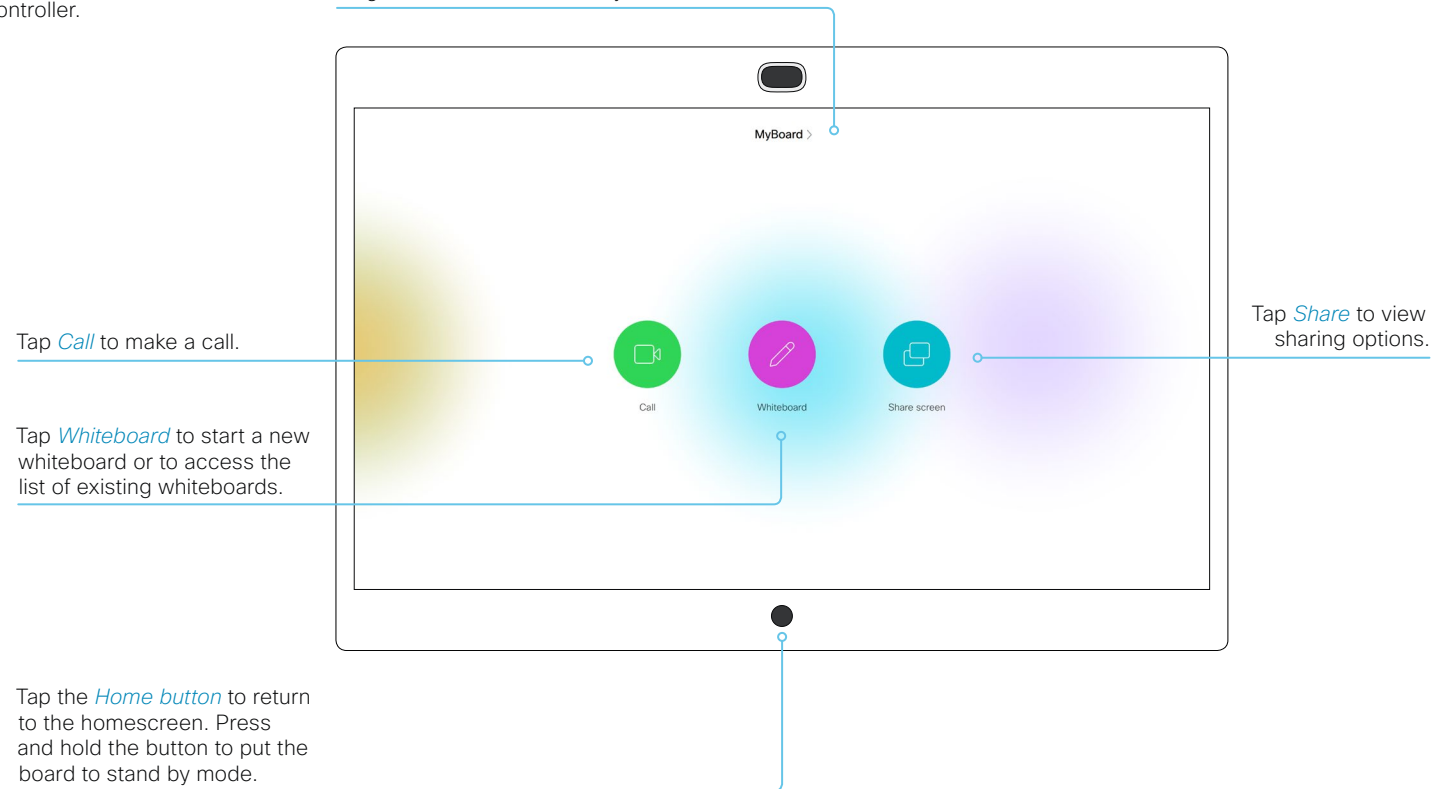
## How to use the Webex Board

The Webex Board's user interface and how to use the board is 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.

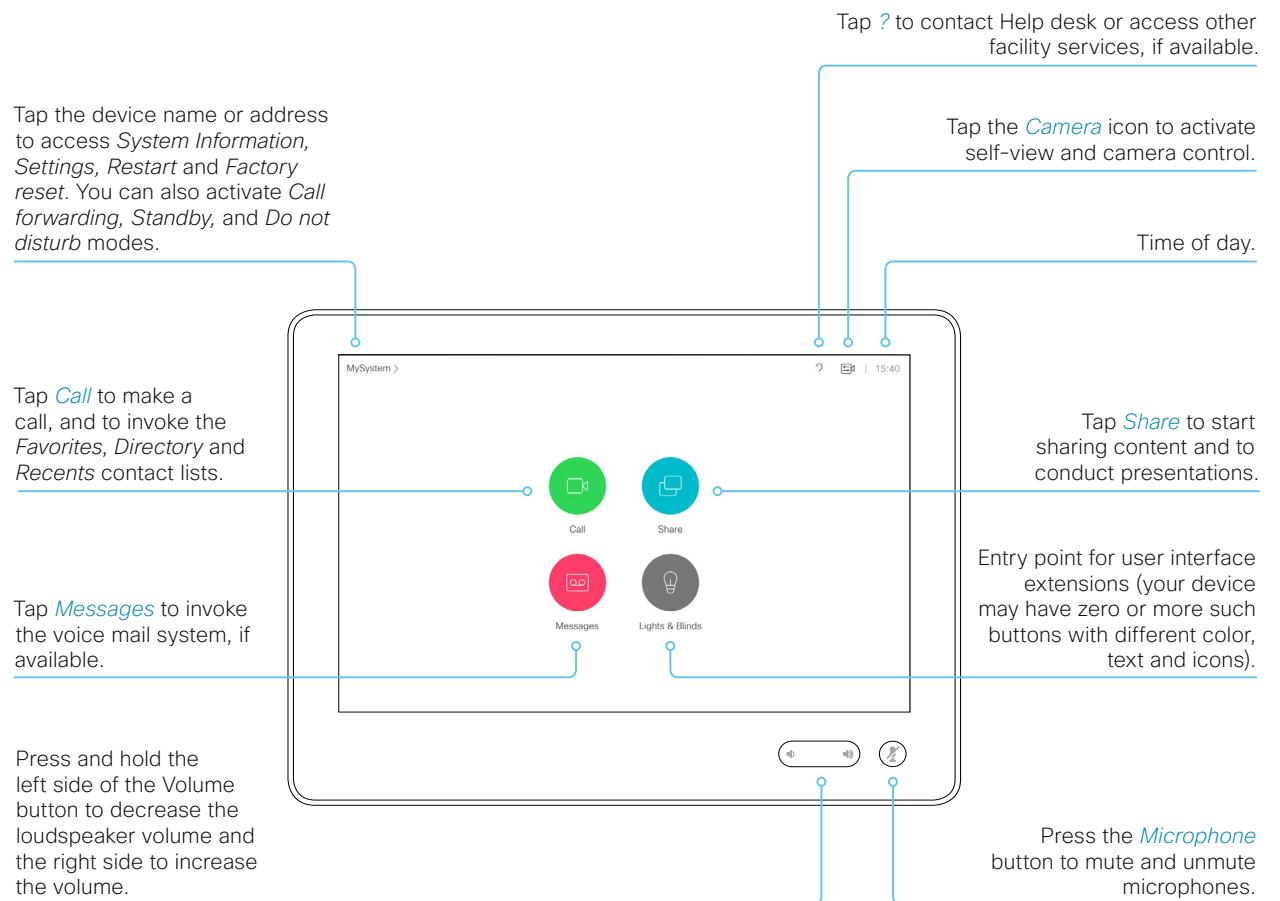
If you have a Touch controller connected to the board, additional settings are available on the Touch controller.

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.*



## How to use Touch 10

The Touch 10 user interface and its use are described in full detail in the User guide for the video conferencing device.





## Set up remote monitoring

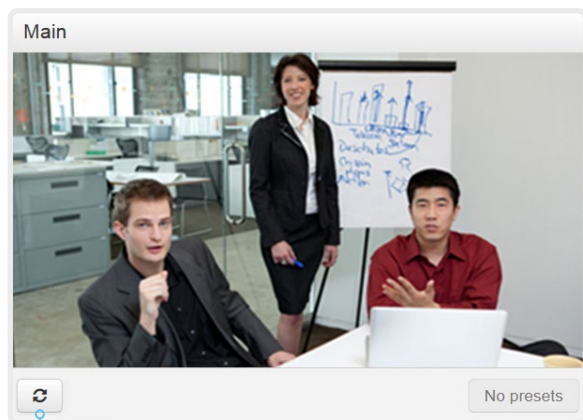
Requirement:

- *RemoteMonitoring* option

Remote monitoring is useful when you want to control the device from another location.

Snapshots from input sources appear in the web interface, so you can check the camera view and control the camera without being in the room.

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



Automatically refresh snapshots

Check whether or not the device has the *RemoteMonitoring* option

1. Sign in to the web interface.
2. Check the Home page to see if *RemoteMonitoring* is on the list of Installed options.

If not on the list, remote monitoring is not available.

### Enable remote monitoring

Install the *RemoteMonitoring* option key. How to install option keys are described in the [Add option keys](#) chapter.

PLEASE BE AWARE THAT IF YOU ENABLE THE REMOTE MONITORING OPTION YOU MUST MAKE SURE THAT YOU COMPLY WITH LOCAL LAWS AND REGULATIONS WITH REGARD TO PRIVACY AND PROVIDE ADEQUATE NOTICE TO USERS OF THE DEVICE THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS YOUR RESPONSIBILITY TO COMPLY WITH PRIVACY REGULATIONS WHEN USING THE DEVICE AND CISCO DISCLAIMS ALL LIABILITY FOR ANY UNLAWFUL USE OF THIS FEATURE.

## About snapshots

### Local input sources

Snapshots of the local input sources of the device appear on the Call Control page.

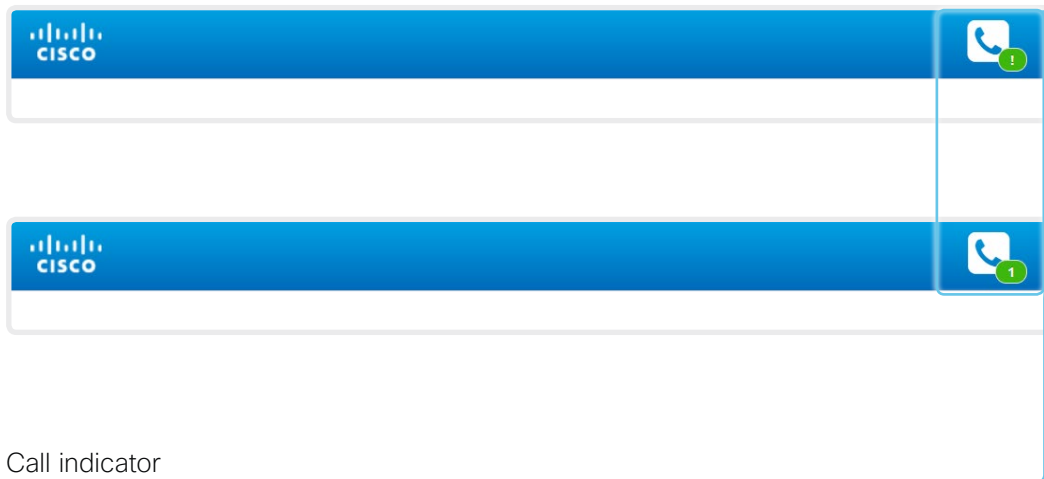
Snapshots appear both when the device is idle, and when in a call.

### Far end snapshots

When in call, you may also see snapshots from the far end camera. It does not matter whether or not the far end device has the *RemoteMonitoring* option.

Far end snapshots are not displayed if the call is encrypted.

## Access call information and answer a call while using the web interface



### Notification of an incoming call

Click the *Call indicator* to open the *Call Control* page, where you can accept or decline the call.

### The device is in a call

The badge indicates the number of active calls.





### Call indicator

The call indicator is present to notify you about an incoming call, and to show when the device is in a call.

If the device is idle, there is no call indicator.

### Control the call

Relevant control buttons are present on the *Call Control* page. Use the buttons to:

-  Show call details
-  Put the call on hold
-  Answer the call
-  Disconnect the call

## Place a call using the web interface (page 1 of 2)

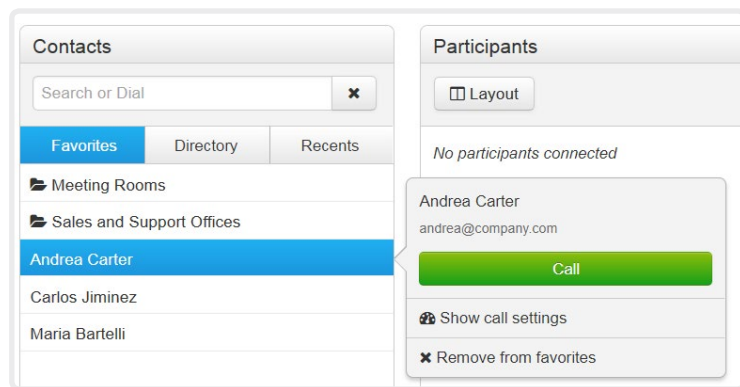
Sign in to the web interface and navigate to [Call Control](#).

### Place a call

**i** Even if the web interface is used to initiate the call, it is the video conferencing device (display, microphones and loudspeakers) that is used for the call; it is not the PC running the web interface.

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

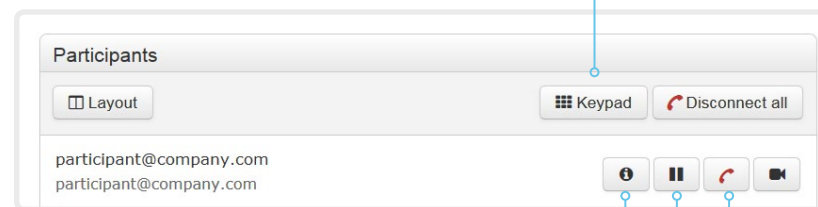
Alternatively, enter the complete URI or number in the *Search and Dial* field. Then click the [Call](#) button that appears next to the URI or number.



\* When searching, matching entries from the *Favorites*, *Directory* and *Recents* lists will be listed as you type.

### Send DTMF tones

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



### Show/hide call details

Click the information button to show details about the call.

Click the button again to hide the information.

### Hold and resume a call

Use the button next to a participant's name to put that participant on hold.

To resume the call, use the button that is present when a participant is on hold.

### End a call

If you want to terminate a call or conference, click [Disconnect all](#). Confirm your choice in the dialog that appears.

To disconnect just one participant in a conference, click the button for that participant.

## Place a call using the web interface (page 2 of 2)

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

### Calling more than one

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

If your device is using the optional built-in MultiSite feature, up to four participants, yourself included, can join the video call (conference).

Follow the same procedure to call the next conference participant as you did when calling the first participant.

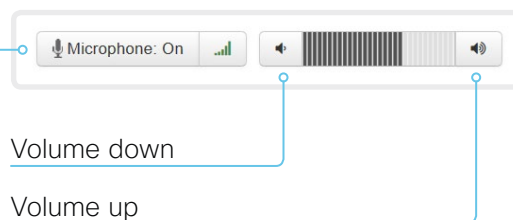
Calling more than one using a conference bridge (CUCM ad hoc conferencing) is not supported from the web interface, even if it is supported by the video conferencing device itself.

### Adjust the volume

#### Mute the microphone

Click [Microphone: On](#) to mute the microphone. Then the text changes to [Microphone: Off](#).

Click [Microphone: Off](#) to unmute.



## Share content using the web interface

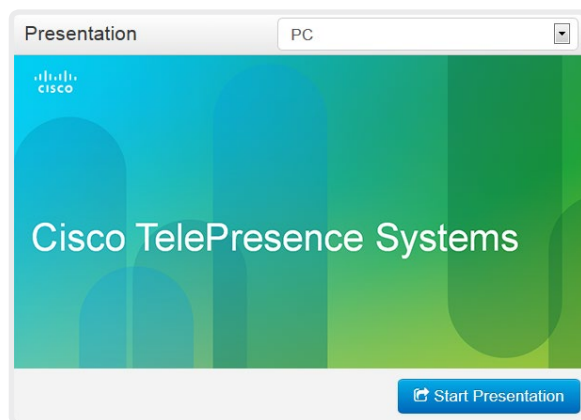
Sign in to the web interface and navigate to [Call Control](#).

### Share content

1. Click [Start Presentation](#). Then the text changes to [Stop Presentation](#).

#### Stop content sharing:

Click the [Stop Presentation](#) button that is present while sharing.



#### 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 the video input of your device. Most often a PC is used as presentation source, but other options may be available depending on your device setup.

While in a call you can share content with the other participant(s) in the call (far end).

If you are not in a call, the content is shown locally.

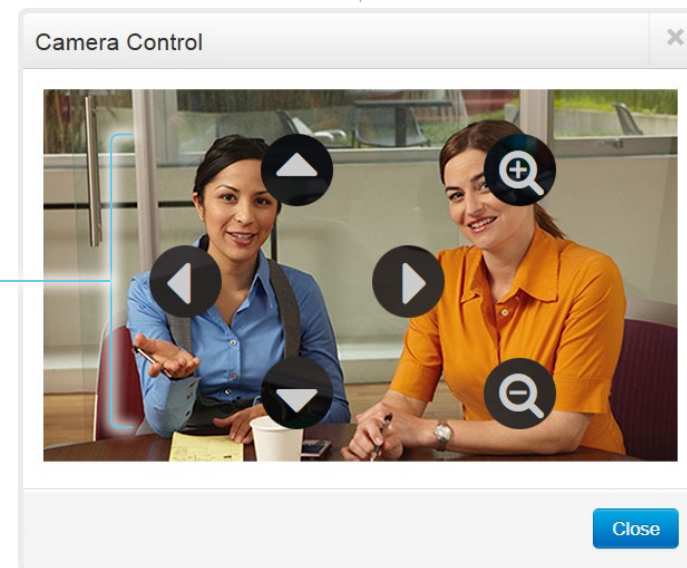
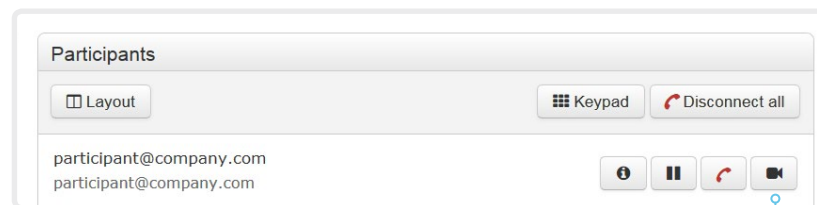
## Control a far end camera

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

### Prerequisites

While in a call, you can control the remote participant's camera (far end) provided that:

- The [Conference > FarEndControl > Mode](#) setting is switched **On** on the far end device.
- The far end camera has pan, tilt or zoom functionality. Only the relevant controls will appear.
- Speaker tracking is not switched On on the far end camera.
- The local device has the *Remote Monitoring* option.



### Control the remote participant's camera

1. Click the camera icon to open the remote camera control window.
2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.

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

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

## Packet loss resilience - ClearPath

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

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

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

## Room analytics (page 1 of 2)

The room analytics feature use several variables from the conference room and re-uses them to analyze the room utilization over time or per call.

### People presence detection

The device has the capability to find whether or not people are present in the room. It takes a minimum of two minutes to detect whether people are present or not in the room. After the room becomes vacant, it may take up to two minutes for the status to change.

This feature is based on ultrasound. It will not keep record of who was in the room, only whether or not there are people present in the room.

You can turn the people presence detection on or off from the web interface. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > PeoplePresenceDetector](#).

### People count

By using face detection, the device can find how many persons are in the room. It will not keep record of who was in the room, only the average number of faces that were detected. Persons that have not faced the camera will not be counted. If there are objects or pictures in the room that can be detected as faces these might be counted.

The call must have a duration of minimum two minutes in order to get a reliable average. Calls that last less than two minutes, and calls which are made with people count disabled, will display "N/A" when you retrieve call history.

By default, the device only counts people when in a call, or when it displays the self-view picture.

You can choose to count people outside of call. When enabled, the device counts people as long as the device is not in standby mode. This includes outside of call, even if self-view is off. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > PeopleCountOutOfCall](#).

### Status

You may see the status at a given moment of people's presence and people count. Sign in to the web interface and navigate to [Setup > Status > RoomAnalytics](#).

### Diagnostics

You can see the live people counter on-screen by enabling the SpeakerTrack Diagnostics mode from the Touch 10 controller. Turn on selfview, and tap the device name or address at the top of the user interface and open the [Settings](#) menu. Tap [Issues & diagnostics](#) and switch on [SpeakerTrack diagnostics](#).

Alternatively, you can open the [Technical support screen](#) on the board (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 for your product to for details.

Go to: ► <https://www.cisco.com/go/board-docs>



## Room analytics (page 2 of 2)

### Ambient noise reporting

The devices can report the stationary ambient noise level in the room. The reported value is an A-weighted decibel value (dBA), which reflects the response of the human ear. All signal processing related to this feature is local, the only data transmitted is the calculated noise level.

This value can be used to detect abnormal changes to the noise level. Such changes may be caused by noise that can be an annoyance for people working in the room. Facility management can then quickly intervene to troubleshoot the issue.

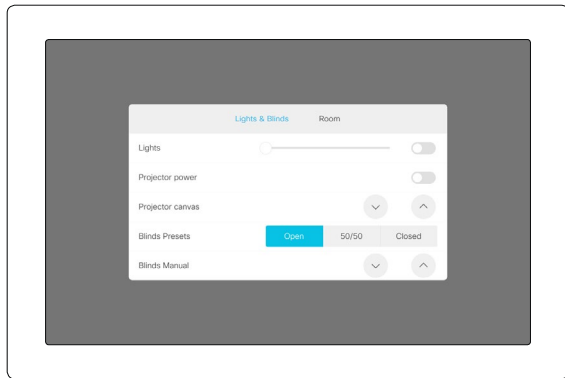
You can turn the ambient noise detection on or off from the web interface. Sign in to the web interface and navigate to [Setup > Configuration > RoomAnalytics > AmbientNoiseEstimation > Mode](#).

Customization

# Customize the video conferencing device's user interface (page 1 of 2)

You can customize the user interface to allow control of peripherals in a meeting room, for example lights and blinds, or to modify the video conferencing device's behavior by triggering macros.

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



Example in-room control panel \*

Consult the *Customization guide* for full details about how to design custom user interface panels (in-room control panels) using the In-Room Control editor, and how to use the video conferencing device's API to program the in-room controls. Go to:

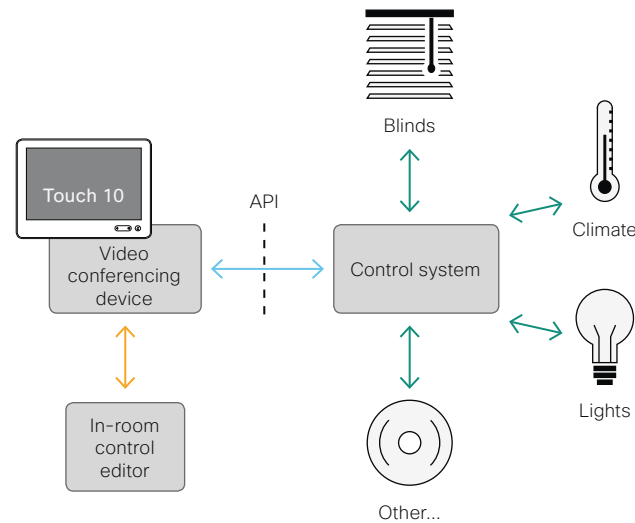
► <https://www.cisco.com/go/in-room-control-docs>

\* If you have connected a Touch controller to the board, the in-room control panels are on the Touch controller; not on the board itself.

## In-room control architecture

You need a Cisco video conferencing device with a touch interface\*, and a control system. The control system may be a third-party system, such as Crestron or AMX, with hardware drivers for peripherals. It is the control system, not the video conferencing device, that controls the peripherals.

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



In-room control schematics

The video conferencing device's macro framework may also serve as a control system. In this case the control system can use the device's API to trigger all sorts of local functionality: Speed dial, language selection, customized system reset, and much more.

Customization

## Customize the video conferencing device's user interface (page 2 of 2)

### The In-Room Control editor

#### Free of charge editor

An easy to use drag-and-drop editor, which you should use to compose the custom user interface panels (in-room control panels), comes free of charge with the video conferencing device's software.

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

- Click [Launch Editor](#) to launch the editor directly from the device's web interface.  
You can push a new in-room control panel to the device, and see the result immediately on the Touch controller.
- Click [Download Editor](#) to download a stand-alone version that you can run locally on your browser from your hard drive.

Then you can compose your custom interfaces without being connected to a device. You can export and import to file to move your work between your local version and the device later.

#### Preview function

The editor also provides a preview function, which allows you to see how the custom interfaces will appear on the user interface.

The preview function is also a complete software version of your custom (in-room control) 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 in-room controls from a remote location

### The room simulator

You can use the room simulator to visualise how the in-room controls on the user interface changes the state of the room.



Back up any existing in-room configuration you may have before you export the simulator configuration to the device. The simulator configuration will replace the existing configuration on the device.

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

- Click [Launch Simulator](#) to open a room simulator in your browser.  
The room simulator contains a predefined in-room control configuration that you can export to the device. Then you can control the simulator's virtual meeting room from your real user interface.
- Click [Load simulator config](#) to export the simulator configuration to the device.

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

Customization

## Customize the video conferencing device's behavior using macros

With macros, you can create your own snippets of code that run on the device. The language is JavaScript / ECMAScript 6 with support for features such as arrow functions, promises and classes.

The macro framework allows an integrator to write scripts that tailor a device's behavior to suite an individual customer's requirements. The integrators can, for example, implement their own features or variations of features, automate specific configurations or re-configurations, and create custom tests and monitoring functions.

By combining the use of macros and creation of a custom user interface panel (also referred to as in-room control panel), you can amend the user interface to trigger customized local functionality. For examples:

- Add speed dialling buttons
- Add a button for room reset, which set all configurations back to your preferred default setup

Consult the *Customization guide* for details about macros and how to use the device's built in Macro editor. Go to:

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

### Allow using macros on the device

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

- Set [Macros > Mode](#) to **On**.

If you try to launch the Macro editor while this setting is **Off**, a pop-up message appears. If you respond by tapping [Enable Macros](#), the [Macros > Mode](#) setting will automatically change to **On**, and the editor will launch.

### Launch the macro editor

Sign in\* to the web interface and navigate to [Integration > Macro Editor](#).

We don't offer a stand-alone version of the editor that you can use to work offline.

### The Macro editor

The Macro editor is a powerful tool where you can:

- Load our code examples, which you can modify, use as is, or use as inspiration when writing your own macros.
- Read our detailed macro scripting tutorial, which also explains the code examples in more detailed.
- Write your own macros, and upload them to the device.
- Enable/Disable individual macros.
- Check in an embedded Log Console what happens when you run a macro.

---

\* You need a user that holds the ADMIN user role in order to access the Macro editor.

Customization

## Remove default buttons from the user interface


In some use cases, you may never use a default button, like *Call* or *Share*. Such unused buttons may cause confusion. In these cases, you can remove the unused buttons from the user interface. Custom In-Room Control panels 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 (In-Room Controls) for the tasks that are going to be performed.

### Configurations

Use the following configurations to remove default buttons from the user interface (applies both to the board itself and the Touch controller). The configurations are available both from the web interface of the device, and in the API.

- *UserInterface > Features > Call > Start*: Removes the default *Call* button. Also removes the *Add* participant button from the Touch controller while in a call.
- *UserInterface > Features > Share > Start*: Removes the default user interface for sharing and previewing content, both in call and out of call.
- *UserInterface > Features > Whiteboard > Start*: Removes the default button for starting a whiteboard.
- *UserInterface > Features > Call > VideoMute*: Removes the default *Turn video off* button.
- *UserInterface > Features > HideAll*: Removes all the default buttons. In-Room Control buttons are not removed.
- *UserInterface > Features > Call > End*: Removes the *End Call* button.
- *UserInterface > Features > Call > MidCallControls*: Removes the *Hold*, *Resume*, and *Transfer* in-call buttons from the Touch controller.

 The configurations remove only the buttons, not the functionality as such. You can share content using Proximity, even if you have removed the *Share* button from the user interface.

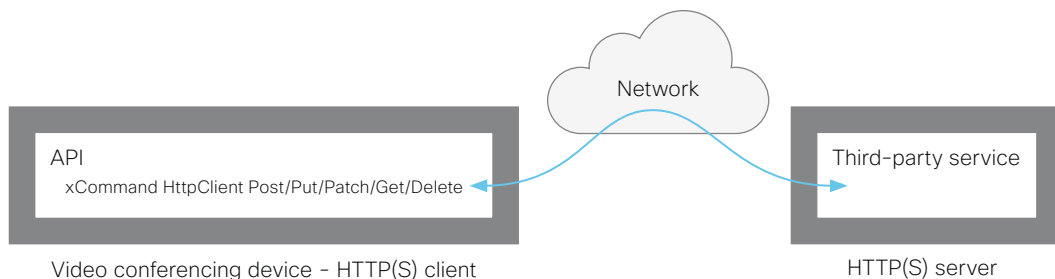
### Further Information

Find more details about how to remove buttons and customize the user interface in the *Customization guide*. Go to:

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

Customization

## Sending HTTP(S) requests



The HTTP(S) request feature makes it possible to send arbitrary HTTP(S) requests from a video conferencing device to an HTTP(S) server. Furthermore, the device receives the response that the server sends back. The device supports the **Post**, **Put**, **Patch**, **Get**, and **Delete** methods.

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

Security measures:

- The HTTP(S) request feature is disabled by default. A system administrator must explicitly enable the feature by setting `HttpClient > Mode` to **On**.
- The system administrator can prevent the use of HTTP by setting `HttpClient > AllowHTTP` to **False**.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent HTTP(S) requests is limited.

### List of Allowed HTTP(S) servers

The system administrator can use these commands to set up and maintain a list of up to ten allowed HTTP(S) servers (hosts):

- `xCommand HttpClient Allow Hostname Add Expression: <Regular expression that matches the host name or IP address of the HTTP(S) server>`
- `xCommand HttpClient Allow Hostname Clear`
- `xCommand HttpClient Allow Hostname List`
- `xCommand HttpClient Allow Hostname Remove Id: <id of an entry in the list>`

If the list is not empty, you can send HTTP(S) requests only to the servers in the list. If the list is empty, you can send the requests to any HTTP(S) server.

The check against the list of allowed servers is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

### HTTPS without certificate validation

When sending requests over HTTPS, the video conferencing device checks the certificate of the HTTPS server by default. If the HTTPS server certificate is not found to be valid, you get an error message. The device doesn't send any data to that server.

We recommend using HTTPS with certificate validation. If certificate validation is not possible, the system administrator can set `HttpClient > AllowInsecureHTTPS` to **On**. This allows the use of HTTPS without validating the certificate of the server.

### Sending HTTP(S) requests

Once the HTTP(S) request feature is enabled, you can use the following commands to send requests to an HTTP(S) server:

```
xCommand HttpClient <Method>
  [AllowInsecureHTTPS: <True/False>]
  [Header: <Header text>]
  [ResponseSizeLimit: <Maximum response size>]
  [ResponseBody: <None/PlainText/Base64>]
  [Timeout: <Timeout period>]
  Url: <URL to send the request to>
```

where <Method> is either Post, Put, Patch, Get, or Delete.

The Post, Put, and Patch commands are multiline commands. Read the API guide to find out how to use multiline commands, and also to find a detailed description of the command parameters

### Further information

Find more information about HTTP(S) Post requests in the *Customization guide*. Go to:

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

## Presentation source composition (page 1 of 2)

You can use the device's API to combine up to four presentation sources in a single video stream.

The maximum number of *different* presentation sources depends on the device:

Video conferencing device	Maximum number of different presentation sources
Room Kit, Room Kit Mini, SX20, MX200 G2, MX300 G2, Board	2
Codec Plus, Room 55, Room 55 Dual, Room 70	3
SX80, MX700, MX800, Codec Pro, Room 70 G2	4
SX10, DX70, DX80	Not applicable

You can only share sources that has been shared through a cable (DVI, VGA, HDMI - depending on the device).

### Source composition

#### Composition layout

You can choose between two layouts:

- Equal
- Prominent

You can change the number of sources at any time, both in call and outside of call. The image sizes cannot be modified.

The order in which the sources appear on the screen depends on the order they have in the command; starting from upper left, ending at bottom right.

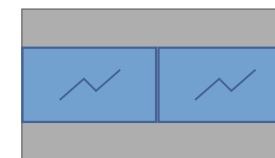
#### Change compositions and layouts on demand

Presentation source composition is only available using API commands; we don't provide a dedicated user interface for it.

To be able to easily change compositions and layouts on demand, we recommend that you use macros and create a custom user interface panel (in-room control panel) for it.

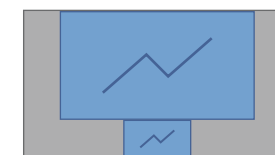
### Layouts

#### Equal



Number of sources: 2

#### Prominent



Number of sources: 2

## Presentation source composition (page 2 of 2)

### API command

```
xCommand Presentation Start
  ConnectorId: <1..n>
  PresentationSource: <1..n>
  Instance: <New, 1..n>
  Layout: <Equal, Prominent>
  SendingMode: <LocalRemote, LocalOnly>
```

where

The input source can be identified by either the physical connector that it is connected to (ConnectorId), or by the logical source identifier (PresentationSource). There cannot be a mix of different types of identifiers in the same command; use either ConnectorId or PresentationSource. You can find these identifiers in the *Video Input Connector* and *Video Input Source* statuses.

Refer to the API-guide for more details.

### Examples

```
xCommand Presentation Start PresentationSource: 1 PresentationSource: 2 Layout: Equal
```



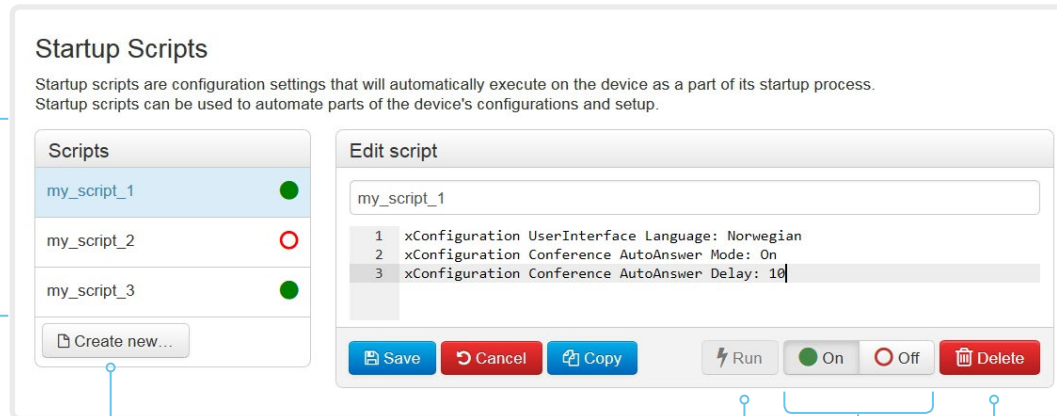
```
xCommand Presentation Start ConnectorId: 1 ConnectorId: 2 Layout: Prominent
```





## Manage startup scripts

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



The script names and configurations shown in the illustration serve as examples. You may make your own scripts.

### List of startup scripts

You can create one or more startup scripts\*.

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

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

### Create a startup script

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

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

### Run a startup script immediately

1. Select the startup script from the list.
2. Click [Run](#).  
Both active and inactive startup scripts can be run immediately.

### Activate or deactivate a startup script

1. Select the startup script from the list.
2. Click [On](#) to activate, or [Off](#) to deactivate a script.  
Active startup scripts will run every time the device starts up.

### Delete a startup script

1. Select the startup script from the list.
2. Click [Delete](#).

## About startup scripts

A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure.

A few commands and configurations cannot be placed in a startup script, for example xCommand SystemUnit Boot. It is not possible to save a script that contains illegal commands and configurations.

Syntax and semantics for xCommand and xConfiguration are explained in the API guide for the product.

## Access the device's XML files

Sign in to the web interface and navigate to [Integration > Developer API](#).

The XML files are part of the device's API. They structure information about the device in a hierarchy.

- *Configuration.xml* contains the current device settings (configuration). These settings are controlled from the web interface or from the API (Application Programmer Interface).
- The information in *status.xml* is constantly updated by the device to reflect system and process changes. The status information is monitored from the web interface or from the API.
- *Command.xml* contains an overview of the commands available to instruct the device to perform an action. The commands are issued from the API.
- *Valuespace.xml* contains an overview of all the value spaces of device settings, status information, and commands.

### Open an XML file

Click the file name to open the XML file.

### About the API

The application programming interface (API) is a tool for integration professionals and developers working with the device. The API is described in detail in the API guide for the device.

## Execute API commands and configurations from the web interface

Sign in to the web interface and navigate to [Integration > Developer API](#).

Commands (xCommand) and configurations (xConfiguration) can be executed from the web interface. Syntax and semantics are explained in the API guide for the device.

### Execute API commands and configurations

1. Enter a command (xCommand or xConfiguration), or a sequence of commands, in the text area.
2. Click [Execute](#) to issue the command(s).

**Execute API commands and configurations**

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

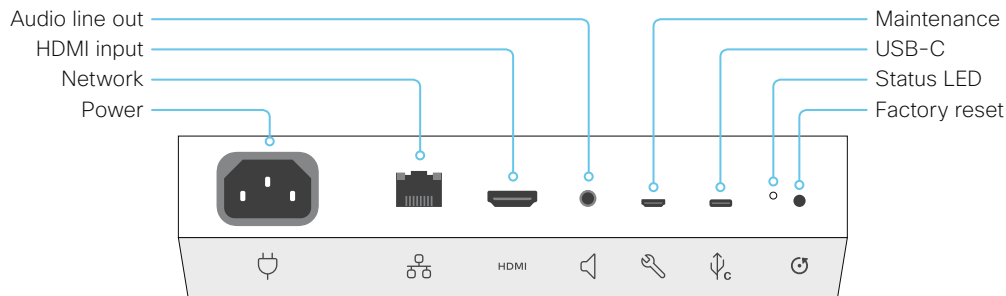
Enter commands...

Execute

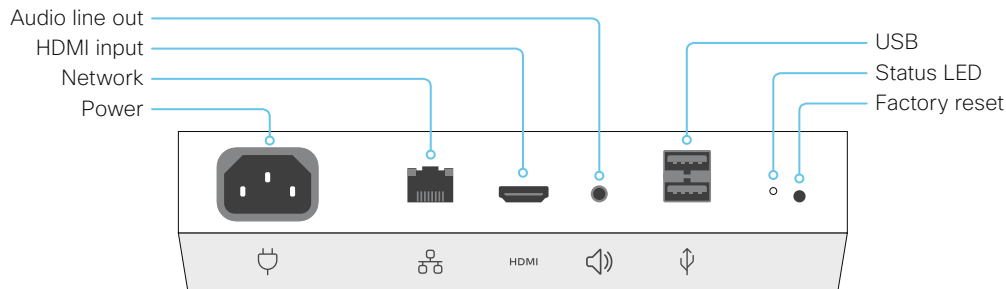
### About the API

The application programming interface (API) is a tool for integration professionals and developers working with the device. The API is described in detail in the API guide for the device.

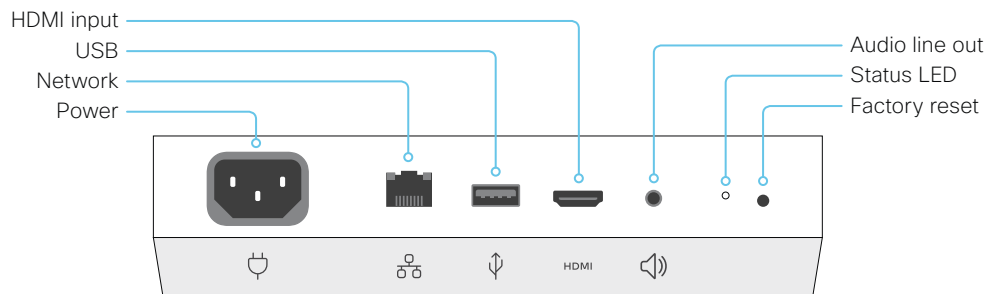
## Connector panel



Webex Board 55S, 70S, and 85S <sup>1</sup>



Webex Board 55



Webex Board 70

### Power

- Board 55S: 100-240 VAC, 3.0-1.5A, 50/60Hz
- Board 70S: 100-240 VAC, 3.5-2.0A, 50/60Hz
- Board 85S: 100-240 VAC, 4.6-2.0A, 50/60Hz
- Board 55, 70: 100-240VAC, 3.5A max, 50/60Hz

### Network

- Ethernet interface, 10Mb/ 100Mb/ 1 Gb Ethernet LAN interface (RJ45). <sup>2</sup>

### 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

- 3.5mm 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.

<sup>1</sup> The second generation Webex Board family (*S Series*) has some minor hardware platform optimizations.

<sup>2</sup> All models also support Wi-Fi.

## About Ethernet ports

### The main network port

The main network port – Network port 1 – is always reserved for the connection to LAN. This applies to all video conferencing devices.

Depending on the device, Network port 1 is marked with the number 1, the network symbol (🌐), or both.

### Auxiliary network ports

Some video conferencing devices have more than one network port. The additional ports can be used for peripheral devices like cameras, Touch 10, third-party control systems, and more.

A device that is connected to such a network port gets a local IP address from the codec, and therefore is not part of the corporate network. It is not possible for packets to traverse the codec between the main network port (LAN) and the auxiliary network ports (link-local).

- A Cisco peripheral device is assigned a dynamic IP address in the range (DHCP): 169.254.1.41 to 169.254.1.240
- A non-Cisco device is assigned the dynamic IP address (DHCP): 169.254.1.30

**NOTE:** Only one non-Cisco device can get a dynamic IP address at a time.

- A non-Cisco device can be assigned a static IP address in the range: 169.254.1.241 to 169.254.1.254

This method can also be used to connect to the codec with SSH. In this case you can use the IP address 169.254.1.1.

### Power over Ethernet (PoE)

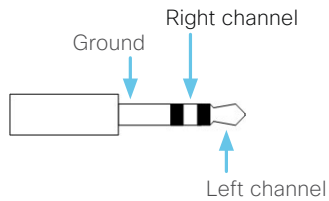
Some of the auxiliary network ports provide Power over Ethernet (PoE). These ports can power peripherals like the Touch 10 controller.

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

\* These products have a separate PoE injector that is connected to one of the auxiliary network ports. The PoE injector is used for the Touch 10 controller.

## Mini-jack connector pin-out schemes

3.5 mm mini-jack, 3-pin (line-out)



Audio connectors (mini-jack)	
	Line-out
Connector pin out	Tip = Left channel Ring = Right channel Shield = GND
Signal type	Unbalanced
Connector (codec)	Mini-jack 3.5 mm, 3-conductor
Input impedance	N/A
Output impedance	470 Ohm
Maximum input level	N/A
Maximum output level	8.2 dBu ±2 dB
Phantom power	N/A
Phantom power resistor pin "tip"	N/A
Phantom power resistor pin "ring 1"	N/A
Frequency response	20 Hz-20 kHz ±1 dB
Signal to Noise Ratio	-100 dB

## Serial interface for maintenance for Webex Board 55S, 70S, and 85S

Use the micro USB connector for direct communication with the device. You need a micro USB to USB cable. If the computer doesn't auto-install a serial port driver, you need to install a serial port driver on the computer manually<sup>1</sup>.

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

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

Parameters:

- Baud rate: 115200 bps
- Data bits: 8
- Parity: None
- Stop bit: 1
- Hardware flow control: Off

### Device settings

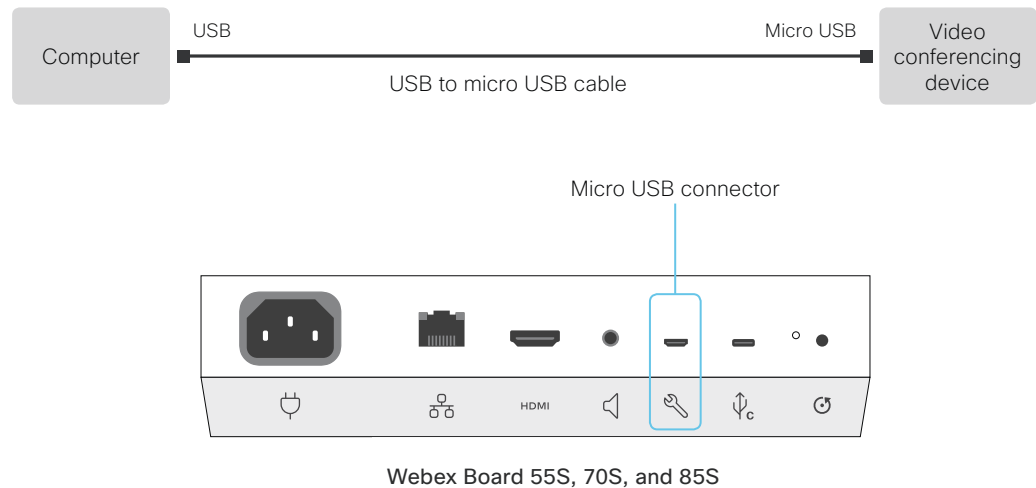
Serial communication is enabled by default. Use the following configuration to change the behavior:

`SerialPort > Mode`

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

`SerialPort > LoginRequired`

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



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.

<sup>1</sup> You need a CP210x USB to UART Bridge Virtual COM Port (VCP) driver, see <http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>

## Serial interface for maintenance for Webex Board 55 and 70

Board 55 and 70 have a USB-A port that offers some maintenance capabilities. There is no serial connection to the main CPU on these devices. You only get a virtual serial interface on top of USB. This means that your computer can't see the device, unless the device is almost fully operational.

If the computer doesn't auto-install a serial port driver, you need to install a serial port driver on the computer manually<sup>1</sup>.

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

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

Parameters:

- Baud rate: 115200 bps
- Data bits: 8
- Parity: None
- Stop bit: 1
- Hardware flow control: Off

### Device settings

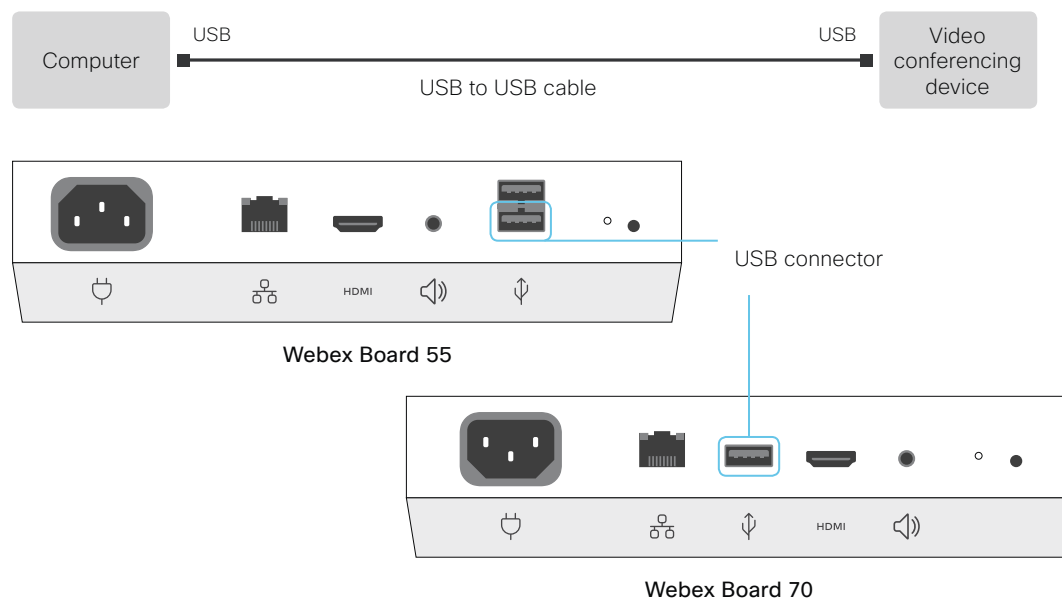
Serial communication is enabled by default. Use the following configuration to change the behavior:

[SerialPort > Mode](#)

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

[SerialPort > LoginRequired](#)

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



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`.
  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.
- NOTE:** If you power up the board before you connect the computer, the computer can't see the board

<sup>1</sup> You need a CP210x USB to UART Bridge Virtual COM Port (VCP) driver, see <http://www.silabs.com/products/development-tools/software/usb-to-uart-bridge-vcp-drivers>



## Open TCP Ports

The web server within the codec prohibit or restrict the use of nonsecure or unnecessary ports, protocols, modules, and/or services. Some ports are open or closed by default.

### TCP 22: SSH

You can close the port by setting SSH mode to **Off**.

```
NetworkServices SSH Mode: Off/On
```

### TCP 80: HTTP

You can close the port by setting HTTP mode to **Off** or **HTTPS**.

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

### TCP 443: HTTPS

You can close the port by setting HTTP mode to **Off**.

```
NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off
```

### TCP 4043: Remote pairing software download

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4045: Remote pairing version information

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4047: Remote pairing session connection

The port is only available (and open) when a Touch panel is remote paired with the video conferencing device. You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 4053: Remote pairing port

You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

### TCP 5060/5061: SIP listen ports

The SIP listen ports are open by default. The SIP listen ports are disabled by the Cisco UCM (Unified Communication Manager). You can close the ports by setting the SIP listen ports to **Off**.

```
SIP ListenPort: Off/On
```

The device settings are configured from the [Setup > Configuration](#) page on the web interface. Open a web browser and enter the IP address of the device then sign in.

## HTTPFeedback address from TMS

When a device is added to Cisco TelePresence Management Suite (TMS), it is automatically configured to send information (events) back to TMS. The device receives the address, that these events should be sent to, from TMS (HTTPFeedback address). If this address is absent or misconfigured, the device cannot send events to TMS.

### Missing response to events

If the device does not receive a response to an event, it will retry sending it to the HTTPFeedback address up to 6 times at increasing intervals.

If the device does not receive a response to any of the retries, the endpoint tries to send a message to the HTTPFeedback address every ten minutes. The HTTPFeedback status will indicate that it has failed, and there is a diagnostic message indicating the type of failure.

While retrying to send messages, there will be a loss of Call Detail Records (CDR) on TMS.

### Get a new HTTPFeedback address from TMS

In order to get a new address to send events to, you must restart the device and wait for the next management address push from TMS (scheduled or triggered by the TMS administrator).

## Register a device to the Cisco Webex cloud service

You can register a device to Cisco Webex remotely from the web interface instead of using the on-screen setup assistant.

To register a device, you need to create an activation code on Control Hub first. To learn how to create an activation code, see [Create a Place and Add Services for a Cisco Webex Room Device or a Cisco Webex Board](#)

From the web interface, you can only register a device that is not currently registered to a service.

**NOTE:** All local users and any customizations that have been created for this device will be deactivated.

1. Sign in to the web interface, and click [Click here to register to Webex](#) on the Home screen.

This link is only available if the device is not registered to a service already.

2. A pop-up appears and you can enter the activation code you have created on Control Hub.

Format:

- xxxx-xxxx-xxxx-xxxx, or
- xxxxxxxxxxxxxxxx

3. After registration, you must setup the time zone and language settings from the on-screen setup assistant. If the wizard times out, default settings will be applied.

### Limitations

Some of the available configurations only apply to on-premises registered devices. They don't apply to Webex registered devices. In the API guide's *Supported Commands Matrix*, these items are marked with "On-prem only".

Among the non-applicable configurations, are those related to H.323, H.320, SIP, NTP, CUCM, LDAP, Proximity, and Far End Camera Control.

### System Information

General		H323	
Product:	Cisco ...	Status	Inactive
System time:	12:30	Gatekeeper	-
Browser time:	12:30	Number	-
Last boot:	yesterday at 15:00	ID	-
Serial number:			
Software version:	ce...		
Installed options:	Encryption		
	RemoteMonitoring		
System name:	MySystem		
IPv4:			
IPv6:			
MAC address:			
Temperature:	65.7°C / 150.3°F		

SIP	
Status	Inactive
Proxy	-

**This video system is not registered**

In order to place calls with this video system, it needs to be registered to a call service.

[Click here to register to Webex](#)

## Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

CE software supports a range of RFCs, including the following:

- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3263 Locating SIP Servers
- RFC 3361 DHCP Option for SIP Servers
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
- RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
- RFC 4582 The Binary Floor Control Protocol  
draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5321 Simple Mail Transfer Protocol
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

## Technical specification (page 1 of 2)

### SOFTWARE COMPATIBILITY

- Cisco Collaboration Endpoint Software Version 9.8 or later
- RoomOS

### COMPONENTS

Fully integrated unit including:

- Multi-touch LED display
  - Webex Board 55/55S: 55 inch
  - Webex Board 70/70S: 70 inch
  - Webex Board 85S: 85 inch
- 4K camera
- 12-microphone array
- Speakers
- Whiteboarding pen

Mounting options:

- Floor stand (freestanding or wall-secured)
- Wall mount

Optional hardware components:

- HDMI presentation cable 8 m / 26.2 ft.
- Pen kit (2 pens and 6 extra tips)

### DISPLAY

Webex Board 55/55S:

- Edge LED LCD, 55 inch, 4K, 350 nits, 16:9
- Viewing angle: +/- 89 degrees (all directions)
- Number of colors: 1.07 billion (10 bit)
- Contrast: 1:4000
- Response time: 8 ms

Webex Board 70/70S:

- Edge LED LCD, 70 inch, 4K, 300 nits, 16:9
- Viewing angle: +/- 88 degrees (all directions)
- Number of colors: 1.07 billion (10 bit)
- Contrast: 1:4000
- Response time: 6 ms

Webex Board 85S:

- Direct LED LCD, 85 inch, 4K, 300 nits, 16:9
- Viewing angle: +/- 89 degrees (all directions)
- Number of colors: 1.07 billion (10 bit)
- Contrast: 1:4000
- Response time: 6.5 ms

### USER INTERFACE

- Capacitive touch
- Protective glass with optical bonding
- Multi-touch

### CAMERA OVERVIEW

- Fixed-focus lens
- 4Kp60
- F-value: 2.8
- 83° horizontal field of view
- 55° vertical field of view
- Camera mounted tilted: -25°

### AUDIO SYSTEM

- 12-element microphone array with intelligent voice tracking
- Integrated voice-optimized speakers

### AUDIO FEATURES

- High-quality 20-kHz audio
- Acoustic echo cancellation
- Automatic Gain Control (AGC)
- Automatic noise reduction
- Active lip synchronization
- Microphone array with intelligent voice tracking capabilities

### BANDWIDTH REQUIREMENTS

- Minimum bandwidth:
  - 720p30 from 768 Kbps
  - 1080p30 from 1.72 Mbps
- Maximum bandwidth:
  - Transmit: 4.3 Mbps
  - Receive: 10 Mbps

### PRESENTATION CAPABILITIES

- Local presentation up to 4K
- Audio over HDMI

### LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

- Main video:
  - Up to 1920 × 1080@30 (HD1080p)
- Presentation sharing:
  - Up to 1920 × 1080@30 (HD1080p)

### INPUTS AND OUTPUTS

- One HDMI input:
  - Supports formats up to 4K (3840 × 2160)
  - Frame rate of 60 fps for up to 1080p and 30 fps for 2160p
  - Extended Display Identification Data (EDID)
- 3.5-mm mini jack audio out (line out)
- Factory reset pinhole
- Ethernet

Webex Board 55:

- Two USB 3.0 (service)

Webex Board 70:

- One USB 3.0 (service)

Webex Board 55S/70S/85S:

- USB-C (future use)
- USB micro (service)

### NETWORK INTERFACES

- One Ethernet (RJ-45) 100/1000Mbps
- Wi-Fi: 802.11a/b/g/n; 802.11ac (2.4 and 5 GHz)
- Bluetooth ready
- IPv4 DHCP/Static
- IPv6 (static IP address assignment, stateless autoconfiguration, and DHCPv6)
- Network Time Protocol (NTP)
- HTTP Proxy support (for signaling, not media)
- Inspecting TLS Proxy supported
- Cisco Discovery Protocol (CDP)
- 802.1X network authentication (Passphrase or X.509 client certificate)
- 802.1Q virtual LAN
- 802.1p (Qos and Class of Service [CoS])

### USER CONTROLS

- Control Cisco Webex Board directly from the touchscreen, use the Cisco Webex Teams app, or use a Cisco Touch 10 controller

### LANGUAGE SUPPORT

- English, Spanish, German, French, French Canadian, Portuguese, Japanese, Czech, Danish, Dutch, Norwegian, Swedish, Latin American Spanish, Italian, Finnish, Polish, Turkish in CE9.8
- Additional languages may be supported in future software releases

### SUPPORTED INFRASTRUCTURE

- Cisco Unified Communications Manager 10.5.2 and newer
- Cisco TelePresence Video Communication Server (Cisco VCS)
- Cisco Webex cloud service (managed through Control Hub)

### ENCRYPTION

- Real-time media (voice, video, and screen sharing) is encrypted using the Secure Real-Time Transport Protocol (SRTP)
- End-to-end encryption uses Advanced Encryption Standard (AES) 128, AES 256, SHA1, SHA256, and RSA

### OPERATING TEMPERATURE AND HUMIDITY

- Ambient temperature: 0°C to 35°C (32°F to 95°F)
- Relative humidity (RH): 10% to 90%

## Technical specification (page 2 of 2)

### POWER

- Autosensing power supply
- 100-240VAC, 50/60Hz

#### Webex Board 55:

- Power consumption:
  - Standby: 45 W
  - Idle or in-use: 185W

#### Webex Board 55S:

- Power consumption (Max 4.6A):
  - Standby: 33 W
  - Idle or in-use: 170W

#### Webex Board 70:

- Power consumption:
  - Standby: 55 W
  - Idle or in-use: 240 W

#### Webex Board 70S:

- Power consumption (Max 4.6A):
  - Standby: 33 W
  - Idle or in-use: 222W

#### Webex Board 85S:

- Power consumption (Max 4.6A):
  - Standby: 41 W
  - Idle or in-use: 352 W

### PHYSICAL DIMENSIONS

#### Webex Board 55/55S:

- Width: 1283 mm / 50.5 in.
- Height: 814 mm / 32.1 in.
- Depth: 48.3 / 1.9 in.
- Weight: 39.8 kg / 87.7 lbs

#### Webex Board 70/70S:

- Width: 1627 mm / 64.1 in.
- Height: 1034 mm / 40.7 in.
- Depth: 61 mm / 2.4 in.
- Weight: 64.3 kg / 141.8 lbs

#### Webex Board 85S:

- Width: 1966 mm / 77.4 in.
- Height: 1221 mm / 48.1 in.
- Depth: 76 mm / 3 in.
- Weight: 100 kg / 220 lbs

### APPROVALS AND COMPLIANCE

#### Webex Board 55, 70:

- Directive 2014/35/EU (Low-Voltage Directive)
- Directive 2014/30/EU (EMC Directive) – Class A
- Directive 2014/53/EU (Radio Equipment Directive)
- Directive 2011/65/EU (RoHS)
- Directive 2002/96/EC (WEEE)
- NRTL approved (Product Safety)
- FCC CFR 47 Part 15B (EMC) – Class A
- FCC Listed (Radio Equipment)

#### Webex Board 55S, 70S, 85S:

- Regulatory compliance:
  - Directive 2014/30/EU (EMC Directive)
  - Directive 2014/53/EU (Radio Equipment Directive)
  - Directive 2011/65/EU (RoHS)
  - Directive 2002/96/EU (WEEE)
  - NRTL approved (product safety)
  - FCC Listed (radio equipment)
- Standards:
  - Radio: EN 300 328, EN 301 893, EN 300 440
  - EMC: EN 301 489-1 and -17, EN 55032 – Class A, EN 55024
  - Safety: EN 60950-1, EN 62479, EN 62311 (for the radio versions)
  - FCC CFR 47 Part 15B (EMC) – Class A
  - FCC CFR 47 Part 15C (RF)
  - FCC CFR 47 Part 15E (R)

Please check the Product Approval Status Database at <http://www.ciscofax.com> for approval documents per country.

All specifications are subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

June 2019

## User documentation on the Cisco web site

Use the following short-links to find the documentation for the product series running CE software.

### Room Series:

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

### MX Series:

▶ <https://www.cisco.com/go/mx-docs>

### SX Series:

▶ <https://www.cisco.com/go/sx-docs>

### DX Series:

▶ <https://www.cisco.com/go/dx-docs>

### Boards:

▶ <https://www.cisco.com/go/board-docs>

In general, you can find user documentation for all Cisco Collaboration endpoints at ▶ <https://www.cisco.com/go/telepresence/docs>

The documents are organized in the following categories – some documents are not available for all products:

### Install and Upgrade > Install and Upgrade Guides

- *Installation guides*: How to install the product
- *Getting started guide*: Initial configurations required to get the device up and running
- *RCSI guide*: Regulatory compliance and safety information

### Maintain and Operate > Maintain and Operate Guides

- *Getting started guide*: Initial configurations required to get the device up and running
- *Administrator guide*: Information required to administer your product
- *Deployment guide for TelePresence endpoints on CUCM*: Tasks to perform to start using the device with the Cisco Unified Communications Manager (CUCM)
- *Spare parts overview, Spare parts replacement guides, Cable schemas*: Useful information when replacing spare parts

### Maintain and Operate > End-User Guides

- *User guides*: How to use the product
- *Quick reference guides*: How to use the product
- *Physical interface guide*: Details about the codec's physical interface, including the connector panel and LEDs

### Reference Guides > Command references

- *API reference guides*: Reference guide for the Application Programmer Interface (API)

### Reference Guides > Technical References

- *CAD drawings*: 2D CAD drawings with dimensions.

### Configure > Configuration Guides

- *Customization guide*: How to customize the user interface, how to use the device's API to program in-room controls, making macros, configure advanced audio set-ups using the Audio Console, and other customizations.

### Design > Design Guides

- *Video conferencing room guidelines*: General guidelines for room design and best practice
- *Video conferencing room guidelines*: Things to do to improve the perceived audio quality

### Software Downloads, Release and General Information > Licensing Information

- *Open source documentation*: Licenses and notices for open source software used in this product

### Software Downloads, Release and General Information > Release Notes

- *Software release notes*

## Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ► <https://www.cisco.com/go/offices>

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134 USA

### Intellectual property rights

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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

### Cisco product security overview

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

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