Collaboration Endpoint software version 9.1
JUNE 2017

Administrator guide

for Cisco TelePresence MX200 G2 and MX300 G2

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Thank you for choosing Cisco!

Your Cisco product has been designed to give you many years of safe, reliable operation.

This part of the product documentation is aimed at administrators working with the setup and configuration of the video system.

Our main objective with this Administrator guide is to address your goals and needs. Please let us know how well we succeeded!

May we recommend that you visit the Cisco web site regularly for updated versions of this guide.

The user documentation can be found on
► http://www.cisco.com/go/mx-docs

How to use this guide

The top menu bar and the entries in the Table of contents are all hyperlinks. You can click on them to go to the topic.

Table of contents

Introduction 4
User documentation and software 5
What's new in CE9 6
MX200 G2 and MX300 G2 at a glance 11
Power On and Off 14
LED indicators 15
How to administer the video system 16

Configuration 20
User administration 21
Change the system passphrase 22
System configuration 23
Add a sign in banner 24
Manage the service certificates of the video system 25
Manage the list of trusted certificate authorities (CAs) 26
Set up secure audit logging 27
Manage pre-installed certificates for CUCM via Expressway provisioning 28
Delete CUCM trust lists 29
Change the persistency mode 30
Set strong security mode 31
Set up Intelligent Proximity for content sharing 32
Adjust the video quality to call rate ratio 37
Packet loss resilience - ClearPath 38
Choose wallpaper 39
Choose a ringtone and set the ringtone volume 40
Manage the Favorites list 41

Peripherals 42
Extend the number of input sources 43
Connect the Touch 10 controller 44

Maintenance 47
Upgrade the system software 48
Add option keys 50
System status 51
Run diagnostics 52
Download log files 53
Create a remote support user 54
Backup or restore a configuration 55

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Revert to the previously used software image 56
Factory reset the video system 57
Factory reset the Touch 10 60
Capture user interface screenshots 61

System settings 62
Overview of the system settings 63
Audio settings 67
CallHistory settings 69
Cameras settings 70
Conference settings 73
FacilityService settings 78
H323 settings 79
Logging settings 82
Network settings 83
NetworkServices settings 90
Peripherals settings 95
Phonebook settings 97
Provisioning settings 98
Proximity settings 101
RoomAnalytics settings 102
RTP settings 103
Security settings 104
SerialPort settings 106
SIP settings 107
Standby settings 111
SystemUnit settings 112
Time settings 113
UserInterface settings 116
UserManagement settings 118
Video settings 120
Experimental settings 130

Appendices 131
How to use Touch 10 132
Set up remote monitoring 133
Access call information while using the web interface 134
Place a call using the web interface 135
Share content using the web interface 137
Local layout control 138
Control a local camera 139
Control a far end camera 140
Room analytics 141
Add in-room controls to Touch 10 142
Manage startup scripts 143
Access the video system's XML files 144
Execute API commands and configurations from the web interface 145
Serial interface 146
Open TCP Ports 147
Technical specification 148
Supported RFCs 152
User documentation on the Cisco web site 153
Cisco contacts 154

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Chapter 1

Introduction

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

User documentation and software

Products covered in this guide

- Cisco TelePresence MX200 G2
- Cisco TelePresence MX300 G2

User documentation

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

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

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:

▶ http://www.cisco.com/go/mx-docs

Documentation for cloud registered devices

For more information on Cisco Spark room devices, visit:

▶ https://help.webex.com/community/cisco-cloud-collab-mgmt

Cisco Project Workplace

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

▶ http://www.cisco.com/go/projectworkplace

Software

Download software for the endpoint from the Cisco web site:

▶ http://www.cisco.com/cisco/software/navigator.html

We recommend reading the Software release notes (CE9):

▶ http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

Converting to CE software

Before upgrading from *TC software* to *CE software*, it is important to consider the upgrade requirements; otherwise upgrading to CE software can leave you with a non-functional deployment that requires you to downgrade.

Refer to the software release notes, and the ▶ Upgrade the system software chapter.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

What's new in CE9

This chapter provides an overview of the new and changed system settings, and the new features and improvements in the Cisco Collaboration Endpoint software version 9 (CE9) compared to CE8.

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

► http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

New features and improvements in CE9.1

New wake-up experience

The new wake-up experience introduces a *Halfwake* state, which leads to a calmer wake-up of the system, and gives users better guidance on how to get started.

When wake-up on motion detection is enabled the system will automatically wake to the *Halfwake* state when people enter the room. It will also wake to this state when a user pairs a Cisco Proximity client to the system.

Additions for Room Analytics

Detect people presence in the room: The video system has the capability to find whether there are people present in the room. The feature is based on ultrasound, and it does not keep record of who was in the room, only whether or not the room is in use.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

New features and improvements in CE9.0

Updated user interface

The user interfaces on the Touch 10, on screen, and on integrated touch screens have been updated. The main menu items on the home screen have been replaced with more prominent activities.

Some of the settings have been removed from the Touch 10 advanced settings menu to align with the on-screen display menu.

Wakeup on motion detection

Wakeup on motion detection senses when a person walks into the conference room and the video system wakes up automatically. You need to enable the following setting for this feature to work:

```
xConfiguration Standby WakeupOnMotionDetection
```

You can't manually set the video system in standby when this feature is enabled.

Updated In-Room Control editor

The In-Room Control editor is updated with a new look, improved logic and usability for producing a control interface more efficiently. In addition, a new directional pad widget and an In-Room Control simulator is added.

Added language support

We have added support for Potuguese (Portugal) to the on-screen display and Touch controller menus.

Other changes

- Support for HTTPS client certificates has been added.
- Unplugging the presentation cable stops the presentation sharing instantly.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

System configuration changes in CE9.1

New configurations

RoomAnalytics PeoplePresenceDetector

Configurations that are removed

None.

Configurations that are modified

Conference DefaultCal Rate

OLD: Default value: 3072

NEW: Default value: 6000

Network [1] IEEE8021X Password

OLD: Valuespace: String(0, 32)

NEW: Valuespace: String(0, 50)

Standby WakeupOnMotionDetection

OLD: Default value: Off

NEW: Default value: On

Video Input Connector [n] PresentationSelection

OLD: Valuespace: AutoShare/Manual/OnConnect

NEW: Valuespace: AutoShare/Desktop/Manual/OnConnect

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

System configuration changes in CE9.0

New configurations

NetworkServices HTTPS Server MinimumTLSVersion

NetworkServices HTTPS StrictTransportSecurity

Peripherals Pairing CiscoTouchPanels EmcResilience

Standby WakeupOnMotionDetection

Configurations that are removed

UserInterface UserPreferences

Audio Microphones PhantomVoltage

Conference VideoBandwidth PresentationChannel Weight

Standby AudioMotionDetection

Video Layout DisableDisconnectedLocalOutputs

Configurations that are modified

Cameras Camera [n] *

OLD: User role: ADMIN, USER

NEW: User role: ADMIN, INTEGRATOR

Conference MultiStream Mode

OLD: Value space: Auto/Off

NEW: Value space: Off

UserInterface Language

NEW: Portuguese added to value space

Configurations with the new INTEGRATOR user role

A new user role – INTEGRATOR – is introduced in CE9.0. It has been added to the following configurations:

Audio DefaultVolume

Audio Input Microphone [n] *

Audio Microphones Mute Enabled

Audio SoundsAndAlerts *

CallHistory Mode

Cameras Camera [n] *

Cameras PowerLine Frequency

Conference DefaultCall Rate

Conference DoNotDisturb DefaultTimeout

FacilityService *

Peripherals Pairing Ultrasound Volume MaxLevel

Peripherals Pairing Ultrasound Volume Mode

Peripherals Profile *

SerialPort Mode

Standby *

SystemUnit Name

Time Zone

UserInterface OSD Output

UserInterface Wallpaper

Video ActiveSpeaker DefaultPIPPosition

Video Input Connector [n] CameraControl CameraId

Video Input Connector [n] CameraControl Mode

Video Input Connector [n] InputSourceType

Video Input Connector [n] Name

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Input Connector [n] OptimalDefinition Profile

Video Input Connector [n] PresentationSelection

Video Input Connector [n] Quality

Video Input Connector [n] RGBQuantizationRange

Video Input Connector [n] Visibility

Video Monitors

Video Output Connector [n] CEC Mode

Video Output Connector [n] Location HorizontalOffset

Video Output Connector [n] Location VerticalOffset

Video Output Connector [n] Resolution

Video Output Connector [n] RGBQuantizationRange

Video Presentation DefaultPIPPosition

Video Selfview Default *

Video Selfview OnCall *

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

MX200 G2 and MX300 G2 at a glance (page 1 of 3)

Cisco TelePresence® MX200 G2 and MX300 G2 are part of the second generation of MX Series multipurpose endpoints.

MX200 G2 and MX300 G2 blend aesthetics, functionality and ease of use. 1080p60 high-definition (HD) performance and new features such as dual display and an embedded four-way MultiSite conferenceing option deliver more power and flexibility. The Cisco TelePresence Touch 10 user interface offers a larger screen size and a user-friendly experience.

MX200 G2 and MX300 G2 systems are easy to install, so you can quickly transform any meeting space into a telepresence-enabled team room.

MX200 G2 and MX300 G2 can meet your needs whether you are just getting started with video communications or are planning to video-enable your entire organization.

MX200 G2

MX300 G2

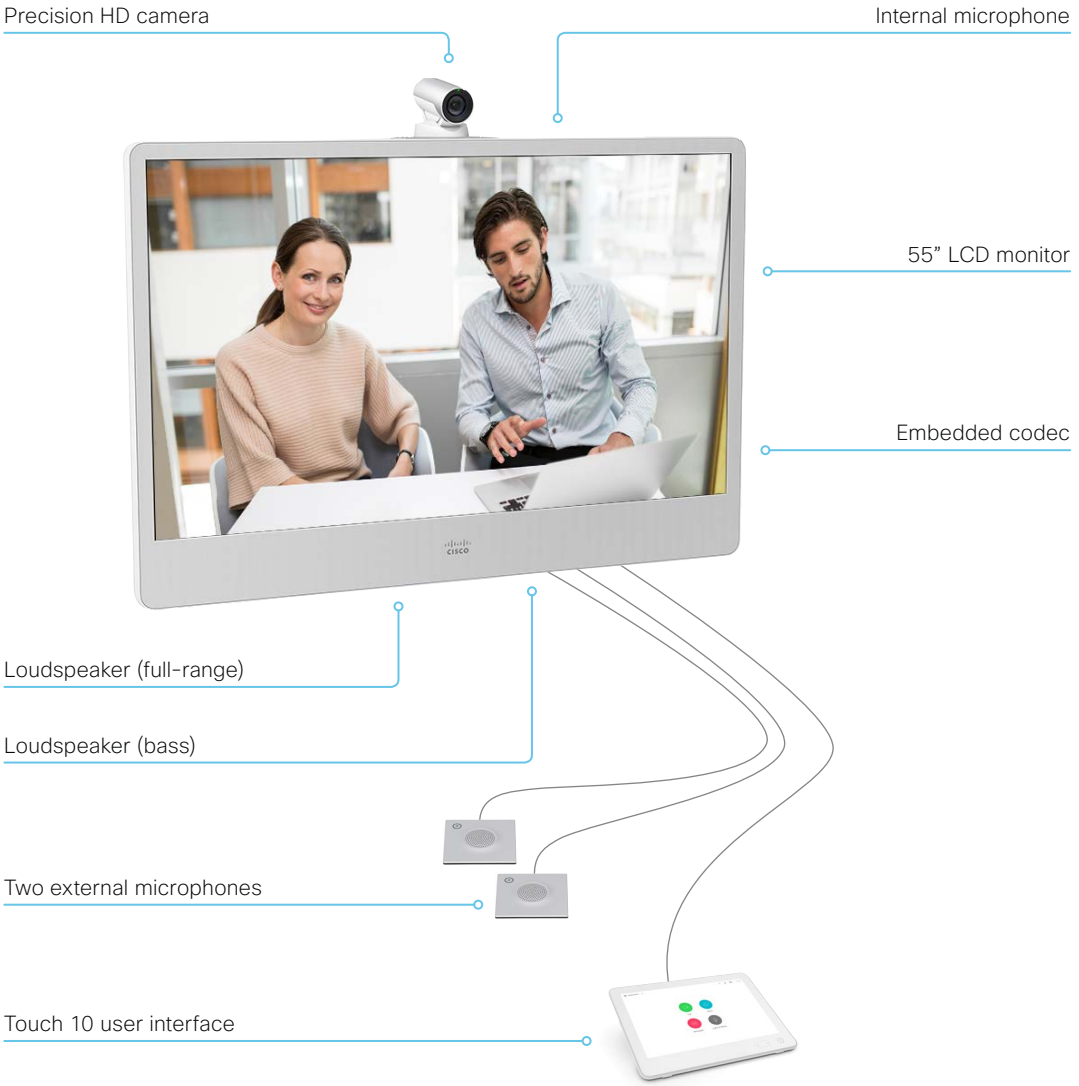
Features and benefits

- Easy to install – one piece plus floor stand, table stand (only MX200 G2), wheel base, or wall mount brackets (VESA mount).
- Registers with Cisco Unified Communications Manager (UCM) and Cisco TelePresence Video Communication Server (VCS).
- Cisco TelePresence Precision camera with pan, tilt, and zoom. MX200 G2 has 5x zoom, and MX300 G2 has 8x zoom.
- High-quality LCD display with 1920×1080 resolution (1080p60) and 16:9 aspect ratio. MX200 G2 has a 42 inch display, and MX300 G2 has a 55 inch display.
- Speaker system that provides superior audio quality.
- Integrated microphone, and support for two external Cisco TelePresence Table Microphone 20.
- 10 inch Cisco TelePresence Touch 10 user interface that offers simple control.
- Standards-based.
- Support for H.323 and Session Initiation Protocol (SIP) calls with bandwidth up to 6 Mbps point-to-point.
- Support for video resolutions up to 1080p60.
- Support for high-definition multimedia and presentation sharing at 1080p30 resolution.
- Support for the dual display feature that allows another screen to be added for content sharing.
- Support for the *one-button-to-push* feature for starting scheduled meetings.
- Embedded MultiSite conferencing option that allows up to three additional participants (individual transcoding, no external bridge).
- Natively supported by Cisco UCM version 8.6.2 and later.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

MX200 G2 and MX300 G2 at a glance (page 2 of 3)

MX300 G2



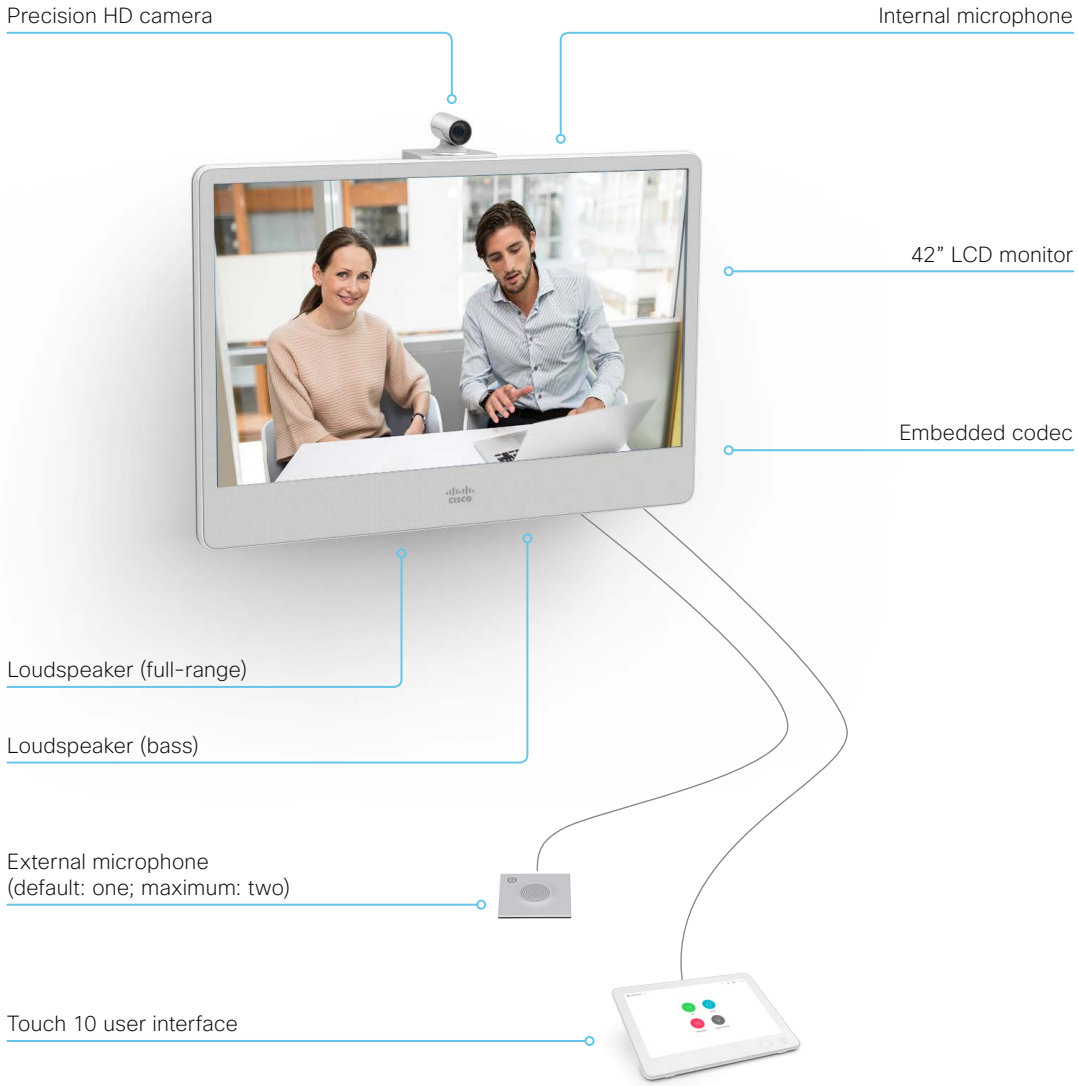
Mounting options

(floor stand, wheel base, wall mount)

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

MX200 G2 and MX300 G2 at a glance (page 3 of 3)

MX200 G2



Mounting options

(floor stand, wheel base, table stand, wall mount)

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

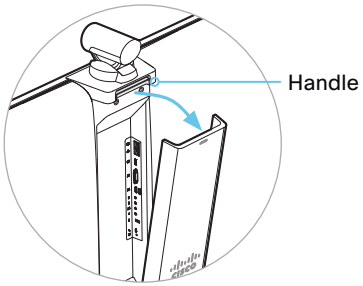
Power On and Off

Power On/Off with the Power switch

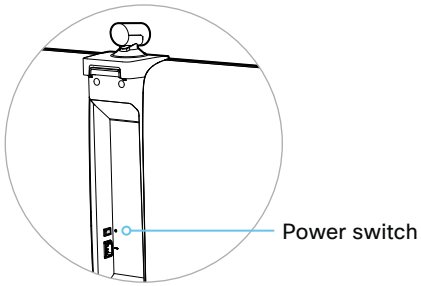
The power switch is behind the back cover, on the left side viewed from behind.

It is located in the same place for both MX200 G2 and MX300 G2, all mounting options.

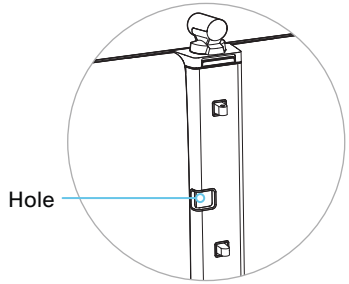
1. Only for floor stand, wheel base and table stand options: Lift the handle and remove the back cover.



2. The power switch is just above the power connector on the rear of the system.



For MX300 G2, wall mount option: Access the power button through the hole in the back cover.



Restart and standby using the user interface

Restart the system

1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *System Information > Restart*.
3. Select *Restart* again to confirm your choice.

Enter/exit standby mode

1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *Standby*.

Power Off or restart the system remotely

Sign in to the web interface and navigate to *Maintenance > Restart*.

Restart the system

Click *Restart device...* and confirm your choice.

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

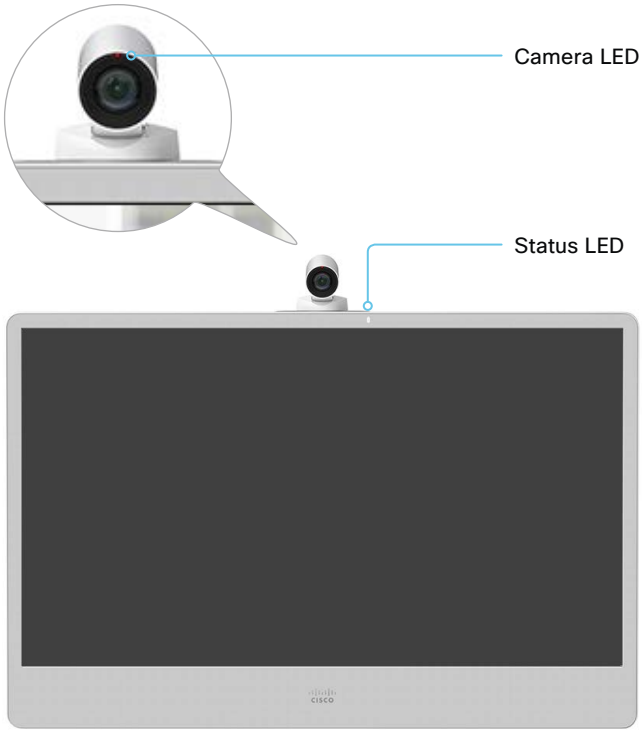
Power Off the system

Click *Shutdown device...* and confirm your choice.

You cannot power the system on again remotely.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

LED indicators



Status LED

The status LED is just below the camera. The normal LED color is white. A red light indicates hardware failure.

Normal operation (not standby):

No light.

In standby mode:

The LED pulsates slowly.

No network connection:

The LED repeatedly flashes twice.

During startup (boot):

The LED flashes. It fades out when the system is ready for use.

During factory reset:

No light until the system restarts.

Camera LED (only MX300 G2)

The camera LED is just above the camera lens.

Incoming call:

The LED flashes.

In call:

Steady light.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

How to administer the video system (page 1 of 4)

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

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

- HTTP or HTTPS (also used by the web interface)
- SSH
- Telnet
- Serial interface (RS-232)

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

Access method	Notes	How to enable/disable the methods
HTTP/HTTPS	• Used by the web interface of the video system • Non-secure (HTTP) or secure (HTTPS) communication • HTTP: *Enabled* by default HTTPS: *Enabled* by default	*NetworkServices > HTTP > Mode* Restart the video system for changes to take effect
Telnet	• Non-secure TCP/IP connection • *Disabled* by default	*NetworkServices > Telnet > Mode* You do not need to restart the video system. It may take some time for changes to take effect
SSH	• Secure TCP/IP connection • *Enabled* by default	*NetworkServices > SSH > Mode* You do not need to restart the video system. It may take some time for changes to take effect
Serial interface (RS-232)	• Connect to the video system with a cable. IP-address, DNS, or a network is not required • *Enabled* by default • We recommend using the default baud rate, because the video system may return much feedback (*SerialPort > BaudRate*) • For security reasons, you are asked to sign in by default (*SerialPort > LoginRequired*)	*SerialPort > Mode* Restart the video system for changes to take effect

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

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

How to administer the video system (page 2 of 4)

The web interface of the video system

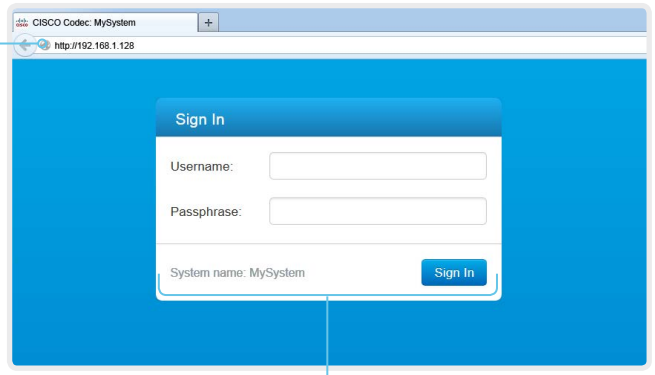
The web interface is the administration portal for the video system. You can connect from a computer and administer the system remotely. It provides full configuration access and offers tools and mechanisms for maintenance.

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

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

Connect to the video system

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



How to find the IP address

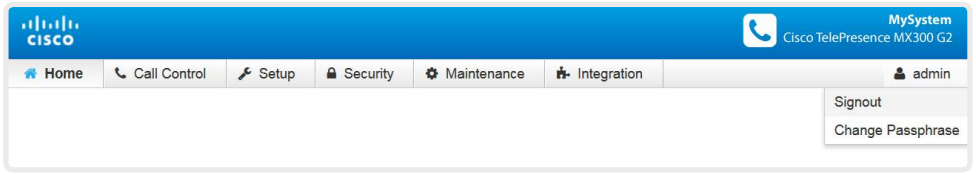
1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *System Information*.

Sign in

Enter user name and passphrase for the endpoint and click *Sign In*.

The system is delivered with a default user named *admin* with no passphrase. Leave the *Passphrase* field blank when signing in for the first time.

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



Sign out

Hover the mouse over the user name and choose *Signout* from the drop-down list.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

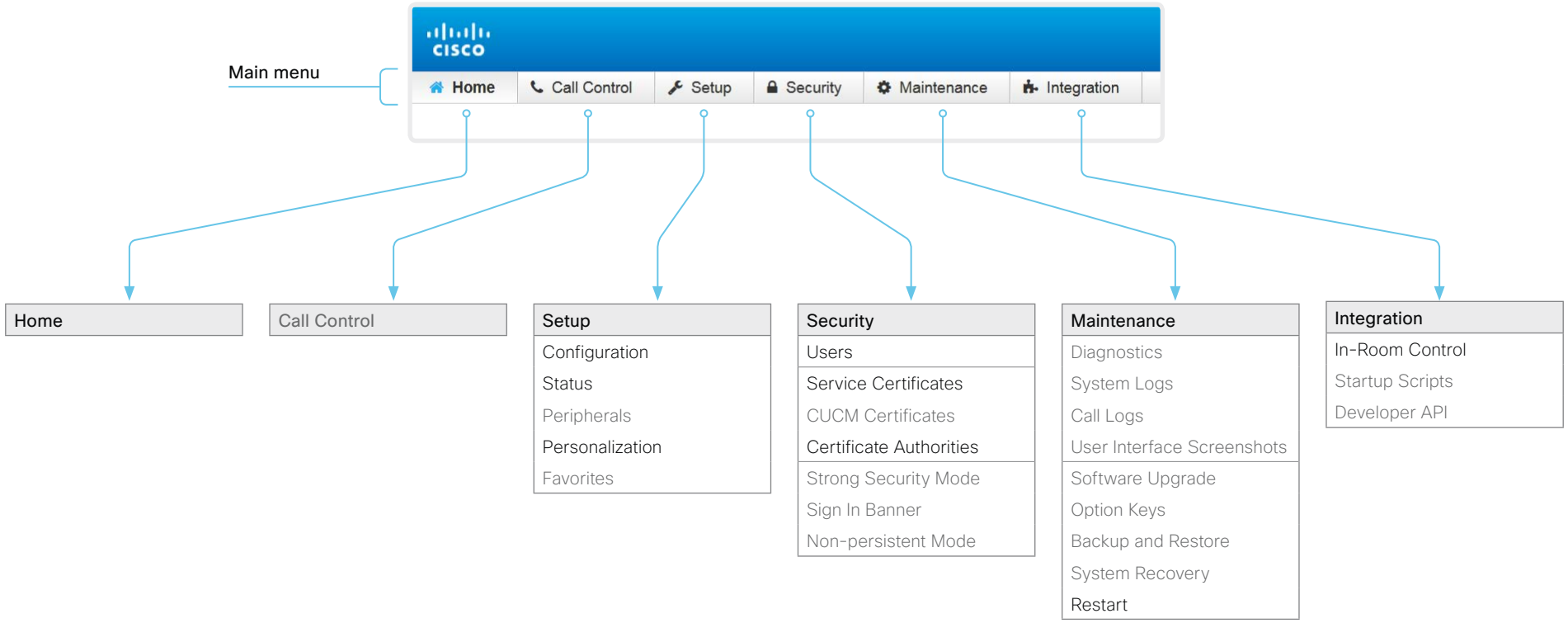
How to administer the video system (page 3 of 4)

How the web interface is organized

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

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.



www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

How to administer the video system (page 4 of 4)

Settings available on the user interface

You have access to some basic configurations and system tests on the video system's user interface. Some of the configurations and tests may be unavailable due to the actual system setup.

- Change the language
- Change the time zone
- Change the network settings for the video system
- Change the network settings for the Touch controller
- Select and activate a service (Cisco's cloud service, or Cisco UCM, VCS or Expressway on-premise services)
- Check the microphone level
- Run a system volume check, and set the default volume
- Set the default camera position
- View system diagnostics for troubleshooting
- Unpair the Touch controller from the video system, and select another system to pair with
- Factory reset the video system
- Enable extended logging

Most of these settings and tests are also part of the *Setup assistant* that is launched when the video system is powered up for the first time. The Setup assistant is described in the *Getting Started Guide* for systems running CE software.

Access Settings

1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *System information > Settings*.
3. Select the button next to the setting you want to change or the test you want to run.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Chapter 2

Configuration

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

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

Read how to set the passphrase in the ► Change the system passphrase chapter.

Create a new user account

1. Sign in to the web interface, and navigate to *Security > Users*.
2. Click *Add new user...*.
3. Fill in the *Username*, *Passphrase* and *Repeat passphrase* input fields.

   As a default, the user has to change the passphrase when he signs in for the first time.

   Fill in the *Client Certificate DN* (Distinguished Name) field only if you use client certificates for authentication.
4. Check the appropriate *Roles* check boxes.

   If you assign the ADMIN role to a user, enter your own passphrase in the *Your passphrase* input field for verification.
5. Set the *Status* to **Active** to activate the user.
6. Click *Create User*.

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

Edit an existing user account

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

Change the user privileges

1. Sign in to the web interface, and navigate to *Security > Users*.
2. Click the appropriate user in the list.
3. Choose user roles, set the status to **Acitve** or **Inactive**, and decide if the user has to change the passphrase on the next sign in.

   Fill in the Client Certificate DN (Distinguished Name) field only if you use certificate login on HTTPS.
4. Click *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 developement 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 video systems with 3rd party equipment. Such a user can also create in-room controls.

Cisco Spark registered systems

If a video system is registered to Cisco's could service (Cisco Spark), only local users with the INTEGRATOR and ROOMCONTROL user roles are available.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Change the system passphrase

You need to know the system passphrase in order to:

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

The default user account

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

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

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

Other user accounts

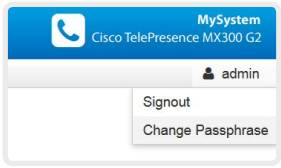
You can create many user accounts for the video system.

Read more about how to create and manage user accounts in the ► User administration chapter.

Change your passphrase

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

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



If the passphrase currently is not set, leave the *Current passphrase* field blank.

Change another user's passphrase

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

1. Sign in to the web interface, and navigate to *Security > Users*.
2. Click the appropriate user in the list.
3. Enter the new passphrase in the *Passphrase* and *Repeat passphrase* input fields.

   If the user holds the Admin role, you must enter your own passphrase in the *Your passphrase* input field for verification.
4. Click *Change passphrase* to save the change.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

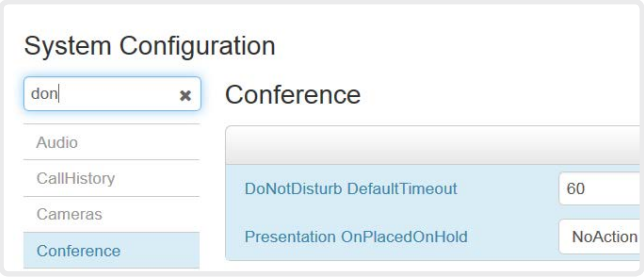
System configuration

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

Find a system setting

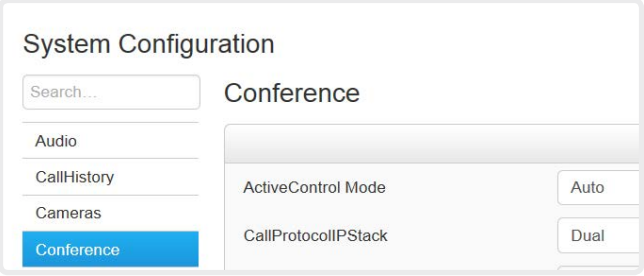
Search for settings

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



Select a category and navigate to settings

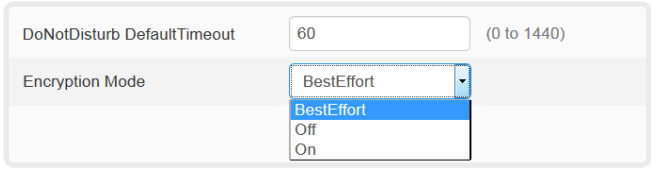
The system settings are grouped in categories. Choose a category in the left pane to show the associated settings.



Change a system setting

Check the value space

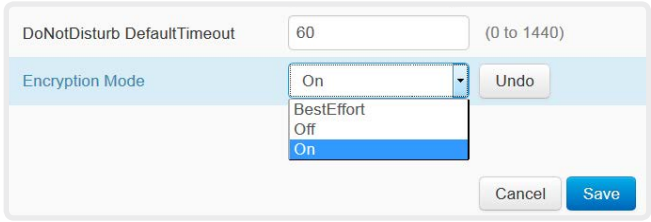
A settings's value space is specified either by text following the input field or in a drop-down list that opens when you click the arrow.



Change a value

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

   Use the *Undo* or *Cancel* buttons if you do not want to make any changes.



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

About system settings

All system settings can be changed from the web interface.

Each system setting is described in the ► System settings chapter.

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

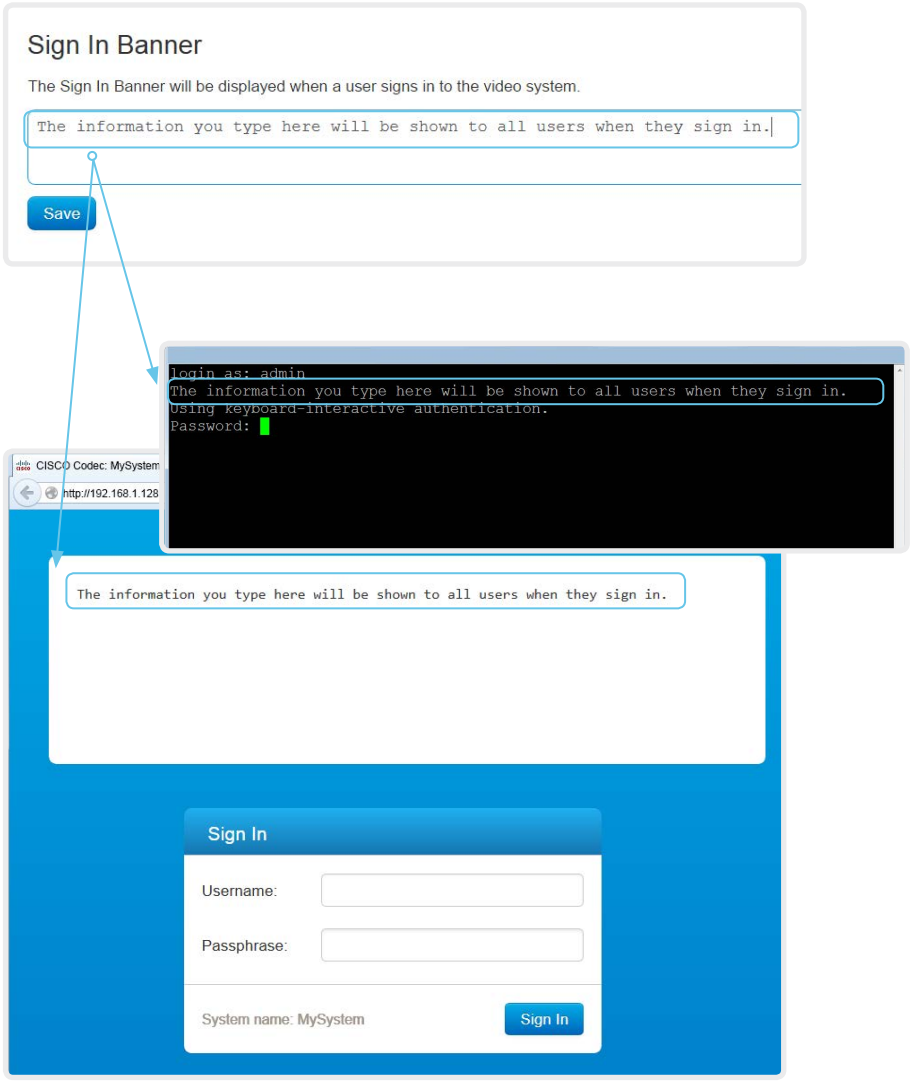
You can read more about user administration and user roles in the ► User administration chapter.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Add a sign in banner

Sign in to the web interface, and navigate to *Security > Sign In Banner*.

1. Enter the message that you want to present to the user when he signs in.
2. Click *Save* to activate the banner.



About sign in banner

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Manage the service certificates of the video system

Sign in to the web interface and navigate to *Security > Service Certificates*.

You need the following files:

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

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

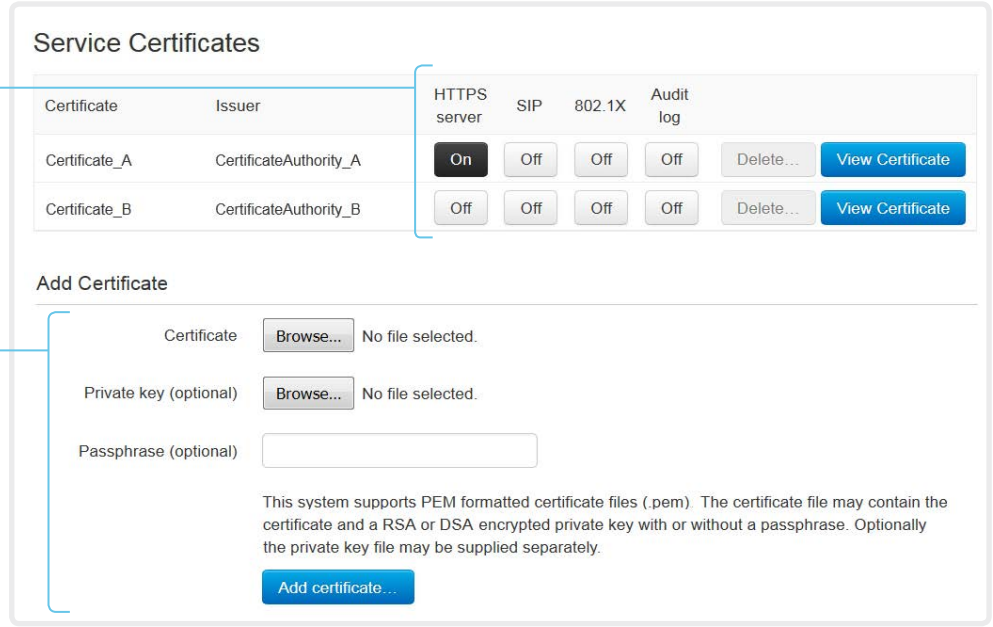
Enable or disable, view or delete a certificate

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

Use the corresponding button to view or delete a certificate.

Add a certificate

1. 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 video system.



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

About the service certificates of the video system

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

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

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

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

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

If authentication fails, the connection will not be established.

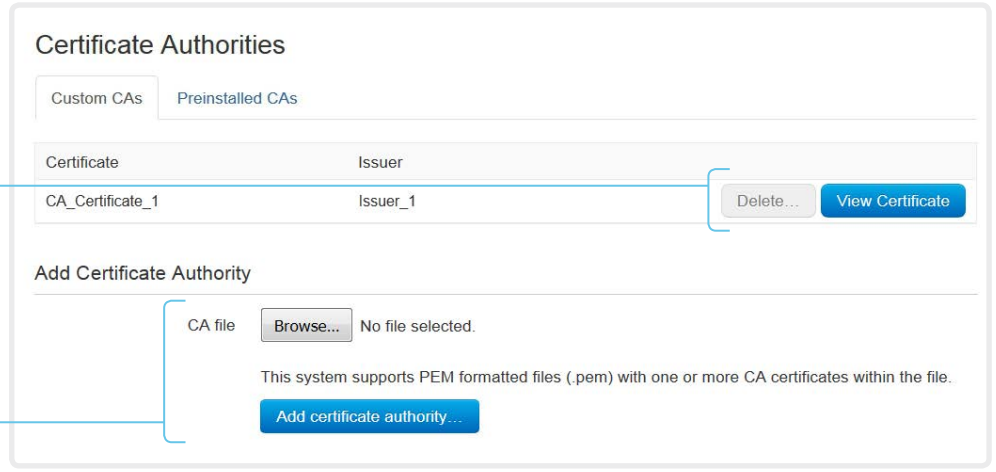
www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Manage the list of trusted certificate authorities (CAs)

Sign in to the web interface, navigate to *Security > Certificate Authorities*, and open the *Custom CAs* tab.

You need the following file:

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



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

View or delete a certificate

Use the corresponding button to view or delete a certificate.

Upload a list of certificate authorities

1. Browse to find the file containing a list of CA certificates on your computer (file format: .PEM).
2. Click *Add certificate authority...* to store the new CA certificates on the video system.

Previously stored certificates are not deleted automatically.

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

About trusted CAs

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

The video system may be set up to require that a server or client presents its certificate to the video system before communication can be set up.

The certificates are text files that verify the authenticity of a server or client. The certificates must be signed by a trusted CA.

In order to verify the signature of the certificates, a list of trusted CAs must reside on the video system.

The list must include all CAs needed in order to verify certificates for both audit logging and other connections.

If authentication fails, the connection will not be established.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Set up secure audit logging

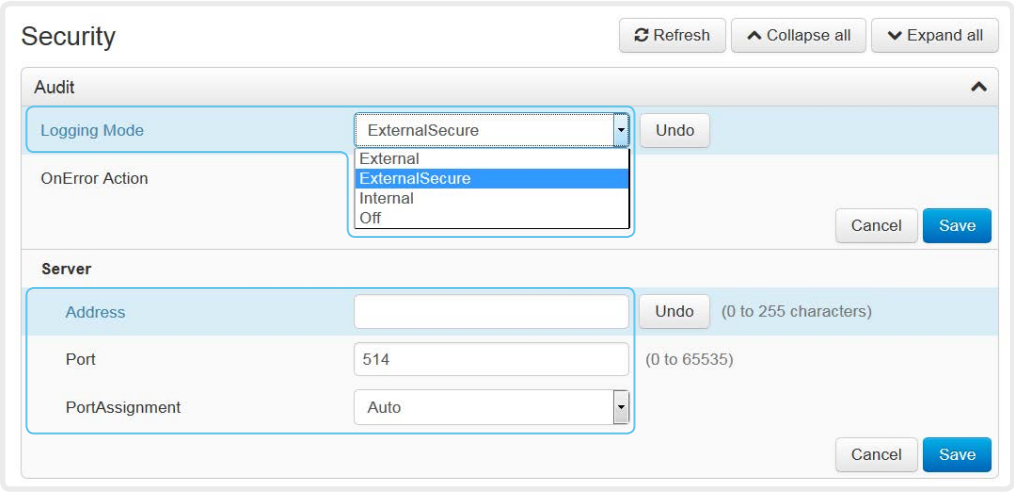
Sign in to the web interface, navigate to *Setup > Configuration*.

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

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

   Click *Save* for the changes to take effect.
3. Set *Audit > Logging > Mode* to **ExternalSecure**.

   Click *Save* for the change to take effect.



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

Refer to the ▶ Manage the list of trusted certificate authorities (CAs) chapter how to update the list.

About secure audit logging

When audit logging is enabled, all sign in activity and configuration changes on the video system are recorded.

Use the *Security > Audit > Logging > Mode* setting to enable audit logging. Audit logging is disabled by default.

In ExternalSecure audit logging mode the video system sends encrypted audit logs to an external audit server (syslog server), which identity must be verified by a signed certificate.

The signature of the audit server is verified using the same CA list as other servers/clients.

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

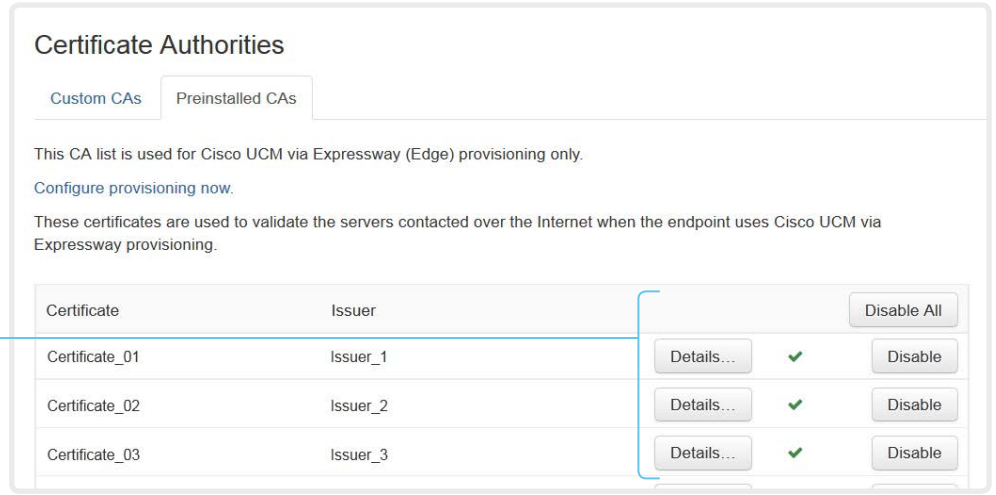
www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Manage pre-installed certificates for CUCM via Expressway provisioning

Sign in to the web interface, navigate to *Security > Certificate Authorities*, and open the *Preinstalled CAs* tab.

View or disable certificates

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



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

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

Refer to the ▶ Manage the list of trusted certificate authorities (CAs) chapter how to update the list of trusted certificates.

About pre-installed certificates

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

Only Cisco Expressway infrastructure certificates are checked against this list.

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Delete CUCM trust lists

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

Sign in to the web interface, navigate to *Security > CUCM Certificates*.

Delete the CUCM trust lists

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

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

In these cases, you must still delete them:

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

Overview of trust list fingerprints and certificates

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

This information may be useful for troubleshooting.

More information about trust lists

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Change the persistency mode

Sign in to the web interface and navigate to *Security > Non-persistent Mode*.

Check the persistency status

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

Alternatively, you can navigate to *Setup > Status*, 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 reboot...*.

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

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

Persistency mode

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

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

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

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

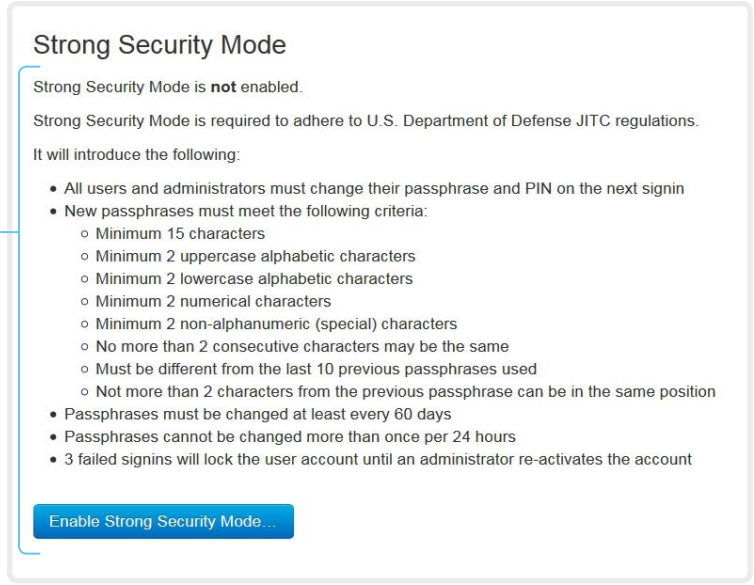
Information that was stored before changing to Non-persistent mode is not automatically cleared or deleted. You must factory reset the video system to delete such information.

There is more information about performing a factory reset in the ► Factory reset the video system chapter.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Set strong security mode

Sign in to the web interface, navigate to *Security > Strong Security Mode*.



Set strong security mode

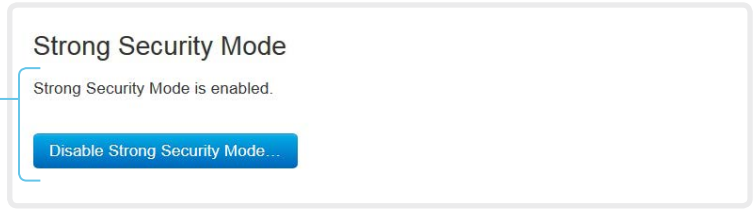
Read carefully about the consequences of strong security mode before you continue.

1. If you want to use strong security mode, click *Enable Strong Security Mode...*. and confirm your choice in the dialog box that appears.

   The video system restarts automatically.

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

   How to change the system passphrase is described in the ► Change the system passphrase chapter.



Return to normal mode

Click *Disable Strong Security Mode...* in order to restore the video system to normal mode. Confirm your choice in the dialog box that appears.

The video system restarts automatically.

About strong security mode

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

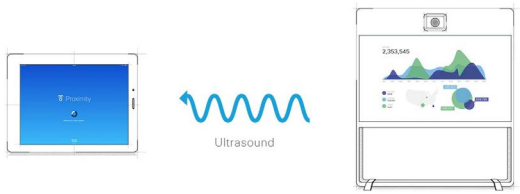
Strong security mode sets very strict passphrase requirements, and requires all users to change their passphrase on the next sign in.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

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

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



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

Video system	Maximum number of connections
Spark Room Kit	7
Codec Plus	7
SX80	10
SX20	7
SX10	7
MX700, MX800	10
MX200 G2, MX300 G2	7
DX70, DX80	3

Proximity services

Place calls and control the video system:

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

View shared content on a mobile device:

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

Wireless share from a desktop client:

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

Place calls and control the video system

View shared content on a mobile device

Wireless share from a mobile device

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

Install a Cisco Proximity client

Where to find the clients

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

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

End-user license agreement

Read the end-user license agreement carefully,
► http://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

Ultrasound emission

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

Use the *Proximity > Mode* setting to switch the Proximity feature – and thereby also ultrasound emission – **On** and **Off.**

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

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

Spark Room Kit, Spark 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.

Codec Plus, SX10, SX20, and SX80:

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

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

Headsets

Spark Room Kit, and Spark Room Kit Plus:

- The systems are not designed for headset use, and do not have a dedicated headset output. We don't recommend to connect a headset to these system.

DX70, DX80, and SX10N:

You can always use a headset with these systems because:

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

Codec Plus, SX10, SX20, SX80, and MX Series:

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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 system sends ultrasound pairing messages.
3. Enable the services you want to allow. Only *Wireless share from a mobile device* is enabled by default.

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

   Place calls and control the video system:

   - Go to *Proximity > Services > CallControl* and choose **Enabled**.

   View shared content on a mobile device:

   - Go to *Proximity > Services > ContentShare > FromClients* and choose **Enabled**.

   Wireless share from a desktop client:

   - Go to *Proximity > Services > ContentShare > ToClients* and choose **Enabled**.

Temporarily disable the Proximity services

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

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

1. Select the settings icon (cogwheel) in the status bar of the user interface to open the dropdown panel.
2. Switch Proximity on or off with the toggle button.

The Proximity indicator

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

The Proximity indicator has two states:

Proximity services are available for use.

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

About Proximity

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

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

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

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).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

Room considerations

Room acoustics

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

About privacy

In the Cisco Privacy statement and the Cisco Proximity Supplement you find information about data collection in the clients and privacy concerns that needs to be considered when deploying this feature in the organization. Refer to:
► http://www.cisco.com/web/siteassets/legal/privacy.html

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

Basic troubleshooting

Cannot detect devices with Proximity clients

- Some Windows laptops are not able to record sound in the ultrasound frequency range (20 kHz–22 kHz). This can be due to frequency limitations with the sound card, sound driver or the internal microphone of the particular device. Refer to the Support forum for more information.

Audio artifacts

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

Cannot share content from a laptop

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

Additional resources

Cisco Intelligent Proximity site:
► https://www.cisco.com/go/proximity

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Adjust the video quality to call rate ratio

Video input quality settings

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

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

Optimal definition profile

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

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

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

Threshold for sending video at 60 fps

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

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

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

1. Go to *Video > Input > Connector n > Quality* and set the video quality parameter to **Motion** (skip this step for Connector 1 (internal camera).
2. Go to *Video > Input > Connector n > OptimalDefinition > Profile* and choose the preferred optimal definition profile.
3. Go to *Video > Input > Connector n > OptimalDefinition > Threshold60fps* to set the threshold below which the maximum transmitted frame rate will be 30 fps.

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, 60 fps allowed at 512×288 and higher resolutions		
	Normal	*Medium*	*High*	*Normal*	*Medium*	*High*
128	320×180@30	512×288@20	512×288@30	320×180@30	512×288@20	512×288@30
256	512×288@30	640×360@30	768×448@30	512×288@30	640×360@30	512×288@60
384	640×360@30	768×448@30	768×448@30	640×360@30	512×288@60	640×360@60
576	768×448@30	1024×576@30	1280×720@30	512×288@60	768×448@60	768×448@60
768	1024×576@30	1280×720@30	1280×720@30	640×360@60	768×448@60	1024×576@60
1152	1280×720@30	1280×720@30	1280×720@30	768×448@60	1024×576@60	1280×720@60
1472	1280×720@30	1280×720@30	1920×1080@30	1024×576@60	1024×576@60	1280×720@60
1536	1280×720@30	1280×720@30	1920×1080@30	1024×576@60	1280×720@60	1280×720@60
2176	1280×720@30	1920×1080@30	1920×1080@30	1280×720@60	1280×720@60	1280×720@60
3232	1920×1080@30	1920×1080@30	1920×1080@30	1280×720@60	1920×1080@60	1920×1080@60
4736	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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Packet loss resilience - ClearPath

ClearPath introduces several mechanisms for advanced packet loss resilience. These mechanisms increase the experienced quality when you use your video system in an error prone environment.

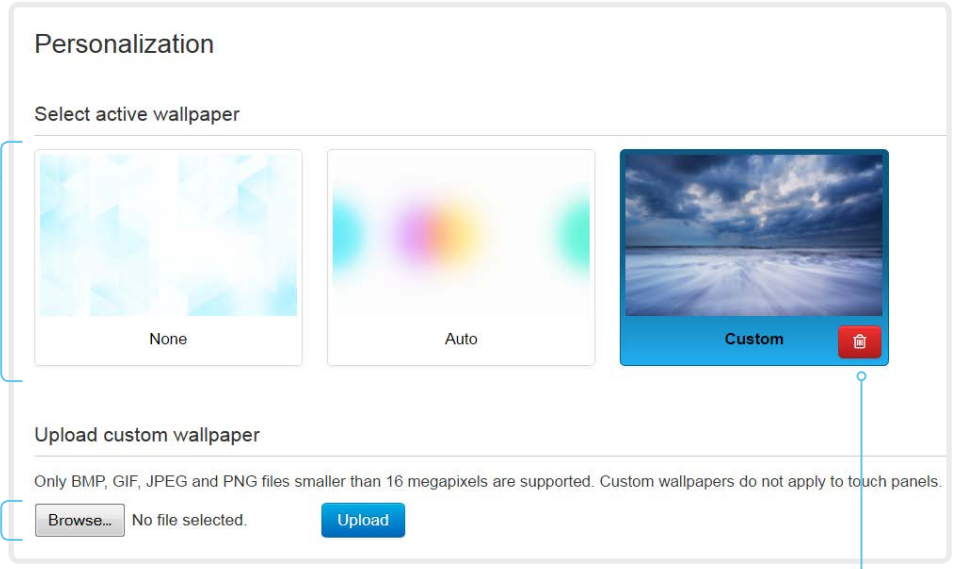
ClearPath is a Cisco proprietary protocol. All endpoints running CE software support ClearPath.

If the involved endpoints and infrastructure elements support ClearPath, all packet loss resilience mechanisms are used in point-to-point connections (including hosted conferences). Only some of the mechanisms are supported in MultiSite conferences.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Choose wallpaper

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



Choose wallpaper

Choose a wallpaper from the list.

The active wallpaper is highlighted.

Upload a custom wallpaper

Overwrites any old custom wallpaper.

1. Browse to find the custom wallpaper image file.
2. Click *Upload* to save the file on the video system.

   Supported file formats: BMP, GIF, JPEG, PNG

   Maximum file size: 16 megapixels

The custom wallpaper is automatically activated once uploaded.

Delete the custom wallpaper

Delete fully removes the custom wallpaper from the video system.

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

About a custom wallpaper

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

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

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

- The large clock
- The list of upcoming meetings

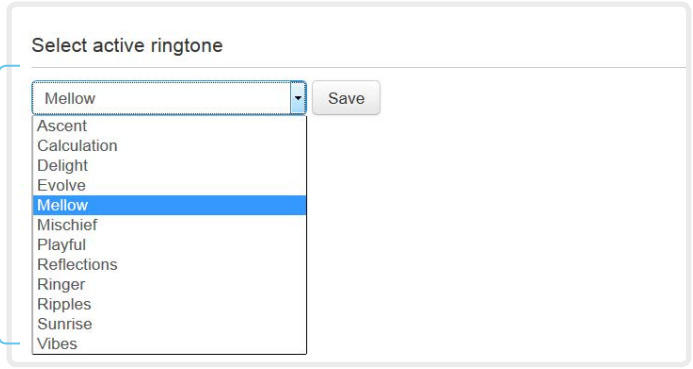
www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Choose a ringtone and set the ringtone volume

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

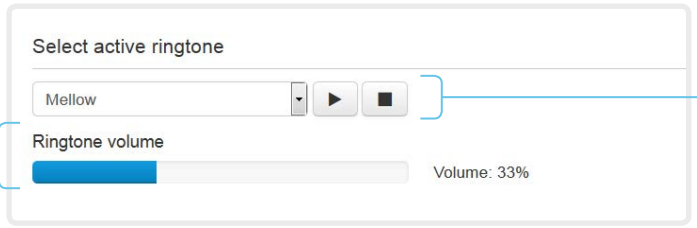
Change the ringtone

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



Set the ringtone volume

Use the slide bar to adjust the ringtone volume.



Play back the ringtone

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

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

About ringtones

A set of ringtones are installed on the video system. Use the web interface to choose a ringtone, and set the ringtone volume.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

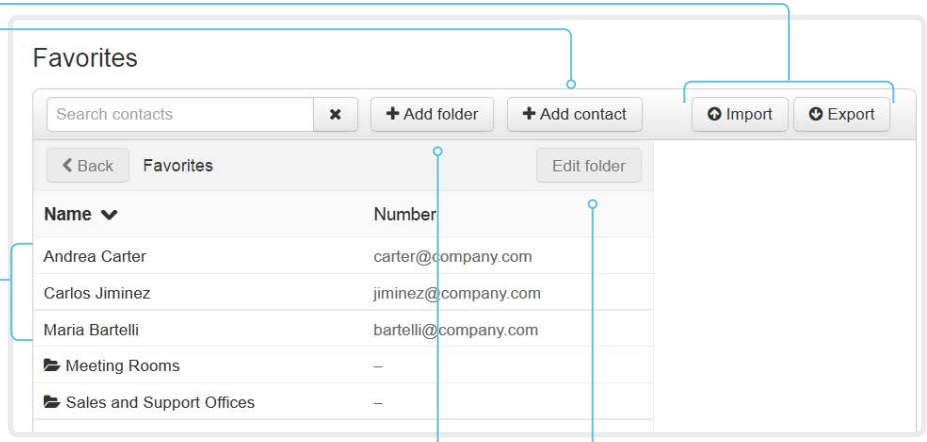
Manage the Favorites list

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 video system's user interface

Add a contact in the Favorites list

1. Select *Call* on the home screen.
2. Select the contact you want to add.
3. Select *Add to favorites*.

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

Remove a contact from the Favorites list

1. Select *Call* on the home screen.
2. Select the *Favorites* tab.
3. Select the contact you want to remove.
4. Select *Remove favorite*.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Chapter 3

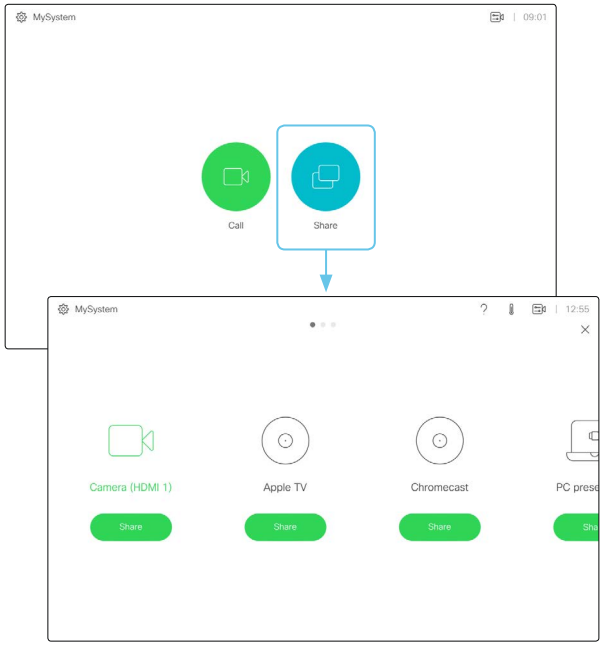
Peripherals

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Extend the number of input sources

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

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



User interface with multiple external input sources (example)

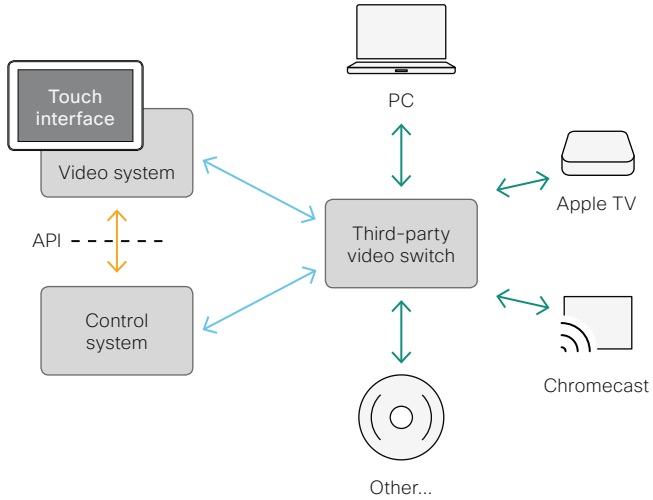
Consult the *In-Room Control guide* for full details about how to extend the user interface, and how to use the video system's API to set it up. Go to:

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

Architecture

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

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



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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Connect the Touch 10 controller (page 1 of 3)

Touch 10 must either be directly connected to the video system as described on this page, or paired to the video system via the network (LAN) as described on the next page. The latter is referred to as remote pairing.

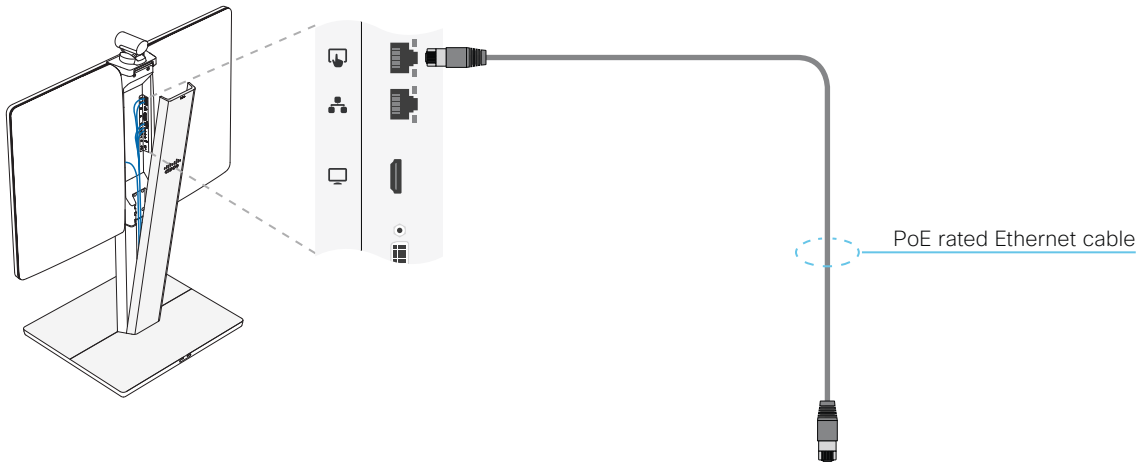
Connect Touch 10 directly to the video system

Connect Touch 10 to the video system's PoE injector as illustrated.

Touch 10 set-up

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

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

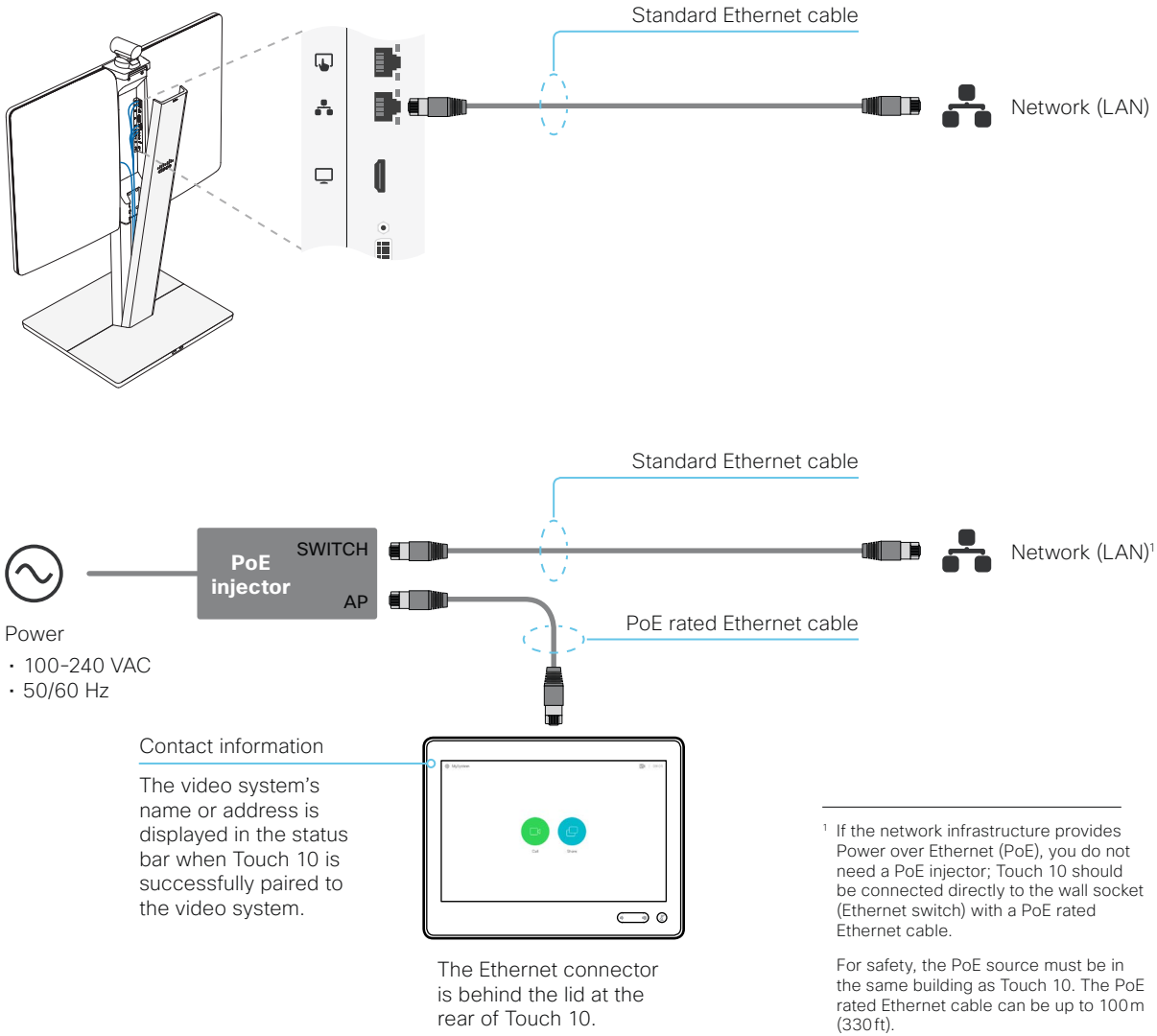


www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Connect the Touch 10 controller (page 2 of 3)

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

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



Touch 10 set-up

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

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

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

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

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

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

  Read more about how to create a user account and assign a role to it in the ► User administration chapter.

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

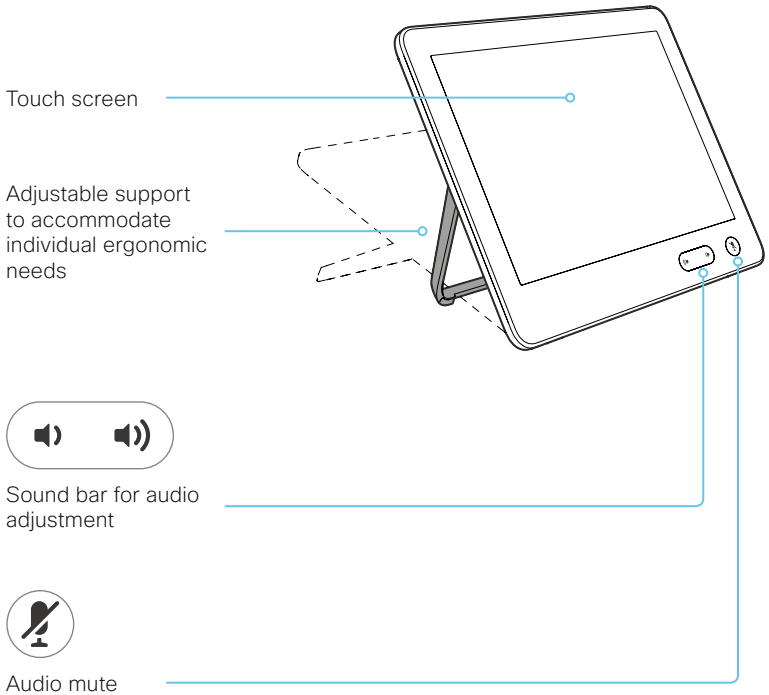
[1] If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

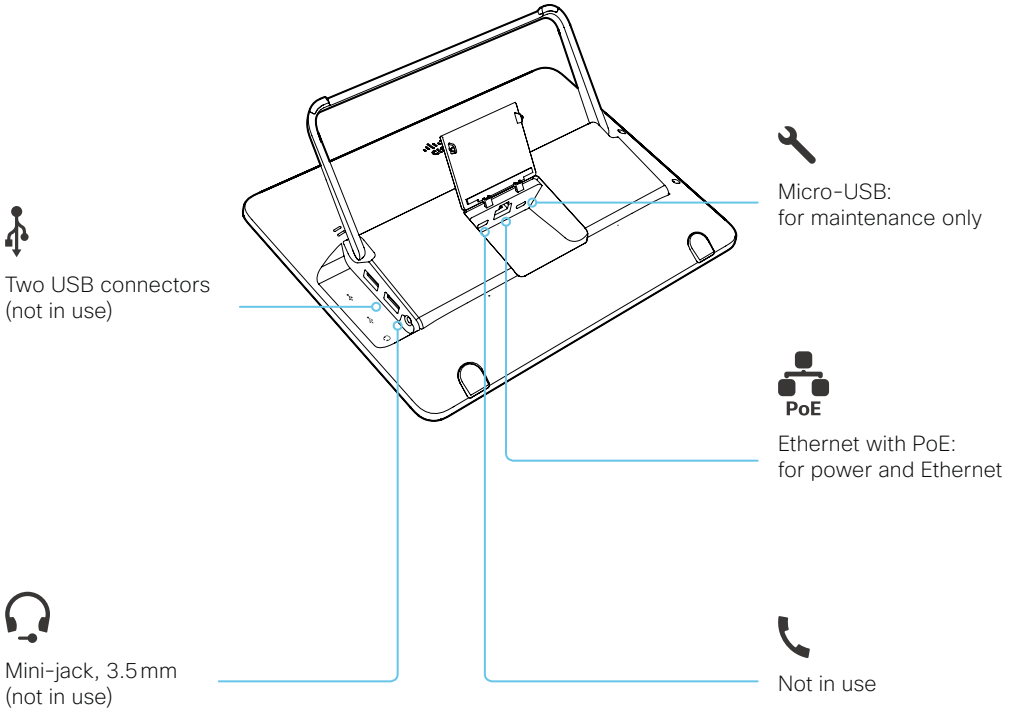
For safety, the PoE source must be in the same building as Touch 10. The PoE rated Ethernet cable can be up to 100 m (330 ft).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Connect the Touch 10 controller (page 3 of 3)

Touch 10 physical interface





www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Chapter 4

Maintenance

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Upgrade the system software (page 1 of 2)

Upgrading from TC to CE software

CE software is the evolution of TC software. We recommend that you upgrade to TC7.3.6 or later before you upgrade to CE software.

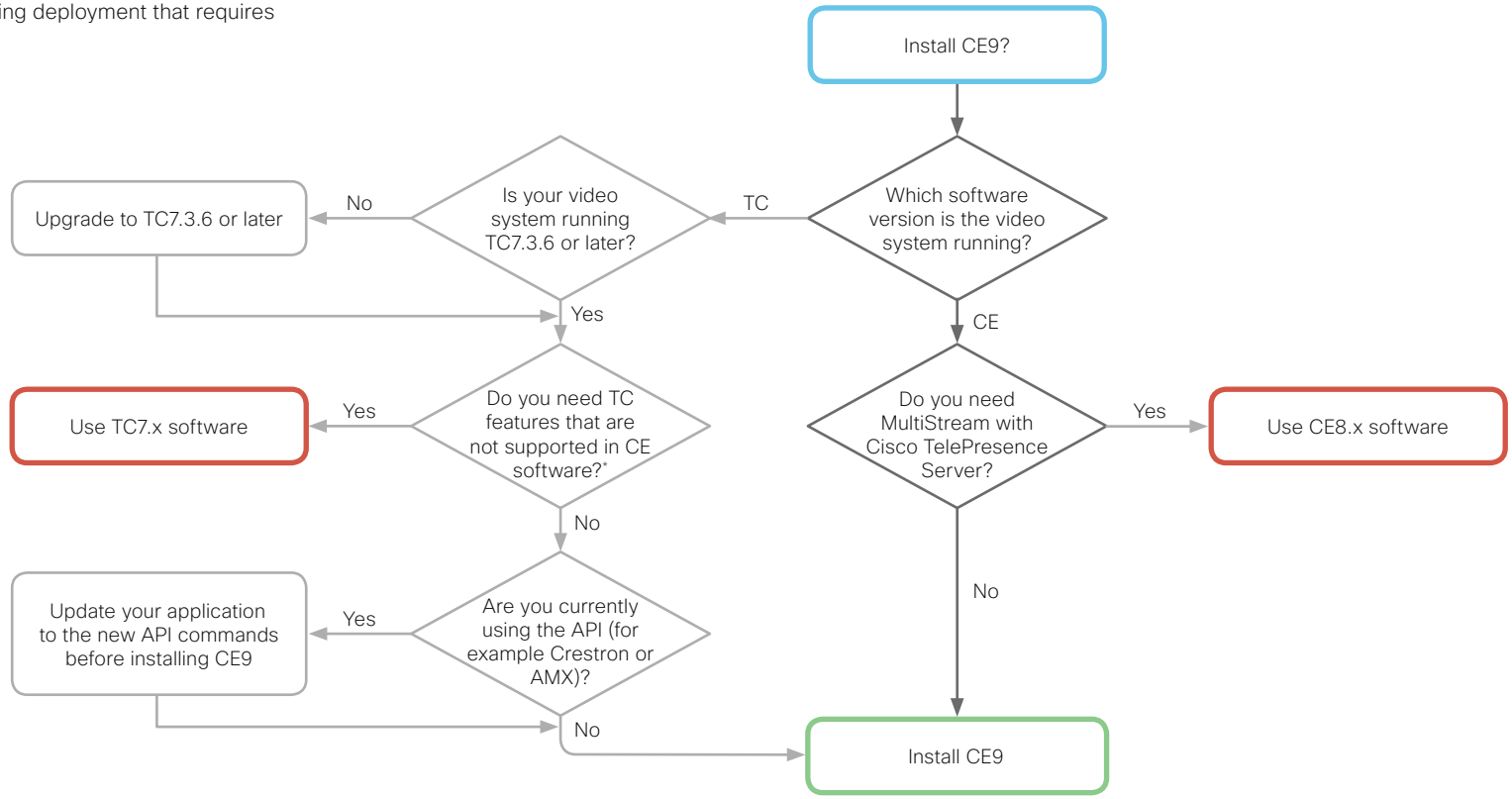
It is important that you read about upgrade requirements and functionality changes before you upgrade to CE software. Also check that your environment supports the changes. We recommend reading the Software Release Notes carefully.

If you don't take into account these considerations, upgrading to CE can leave you with a non-functioning deployment that requires you to downgrade.

Upgrading from CE8 to CE9

The MultiStream feature with Cisco TelePresence Server is deprecated in CE9.

Also, some features that were available from the Touch controller in CE8, are not available in the first CE9 releases. Read the Software Release Notes for details before you upgrade.



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

- MultiWay conferencing
- CTMS conferencing
- MediaNet
- Displays that do not support 16:9 resolution

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Upgrade the system software (page 2 of 2)

Sign in to the web interface and navigate to *Maintenance > Software Upgrade*.

Download new software

For software download, go to the Cisco Download Software web page, and navigate to your product:
► http://www.cisco.com/cisco/software/navigator.html.

Each software version has a unique file name. The format of the file name is “s52010ce9_1_x.pkg”.

Software release notes

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

Go to: ► http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

Install new software

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

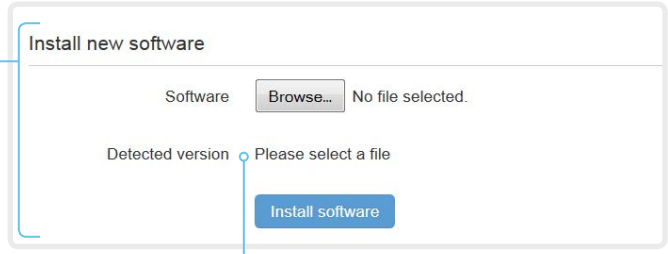
1. Click *Browse...* and find the .pkg file that contains the new software.

   The software version will be detected and shown.

2. Click *Install software* to start the installation process.

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

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



Check new software version

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

About software versions

This video conference system is using CE software. The version described in this document is CE9.1.x.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Add option keys

Sign in to the web interface and navigate to *Maintenance > Option Keys*.

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

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

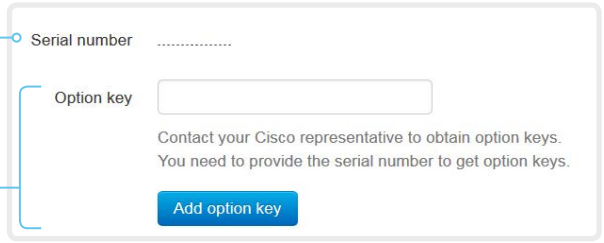
The video system's serial number

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

Add an option key

1. Enter an *Option Key* in the text input field.
2. Click *Add option key*.

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



About option keys

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

Each video system has unique option keys.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

System status

System information overview

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

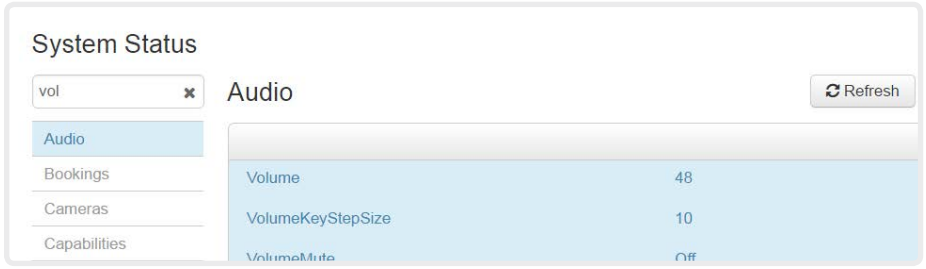
This page shows the product type, system name and basic information about the hardware, software, installed options and network address. Registration status for the video networks (SIP and H.323) is included, as well as the number/URI to use when making a call to the system.

Detailed system status

Sign in to the web interface, and navigate to *Setup > Status* in order to find more detailed status information*.

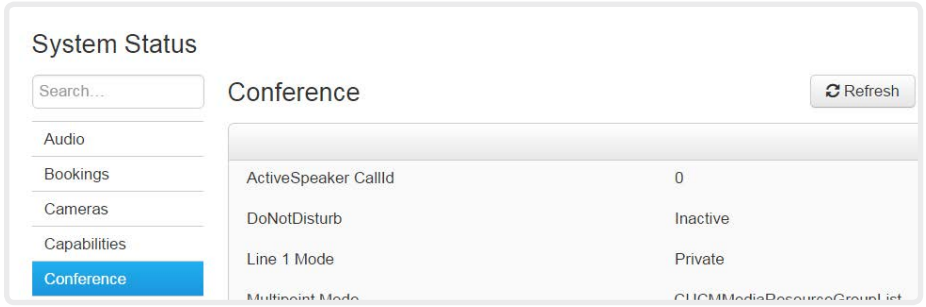
Search for a status entry

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



Select a category and navigate to the correct status

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



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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Run diagnostics

Sign in to the web interface and navigate to *Maintenance > Diagnostics*.

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

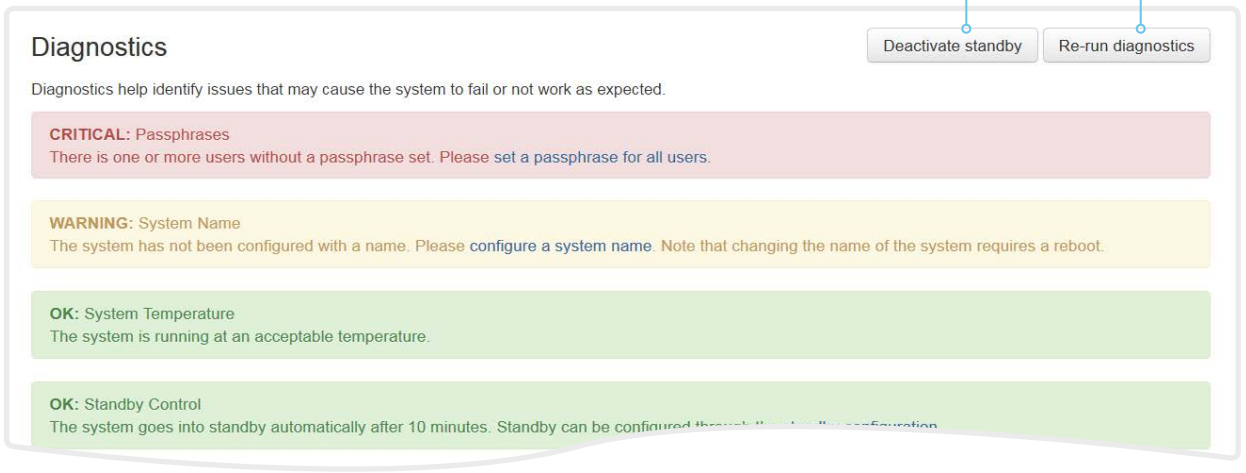
Errors and critical issues are clearly marked in red color; warnings are yellow.

Run diagnostics

Click *Re-run diagnostics* to ensure that the list is up to date.

Leave standby mode

Click *Deactivate standby* to wake up a video system that is in standby mode.



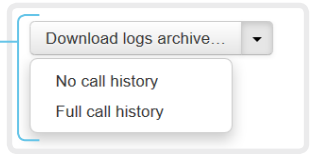
* The messages shown in the illustration serve as examples. Your system may show other information.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

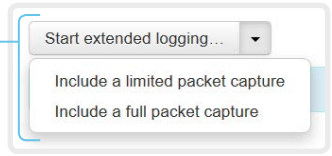
An anonymized call history is included in the log files by default.

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 video system restarts. If the maximum number of historical log files is reached, the oldest one will be overwritten.

Extended logging mode

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

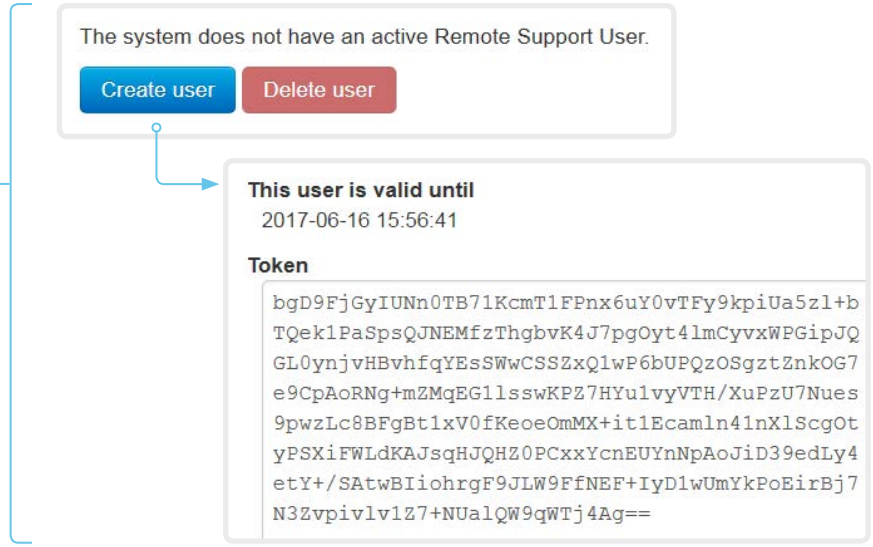
Extended logging uses more of the video system's resources, and may cause the video system to under-perform. Only use extended logging mode when you are troubleshooting an issue.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

Delete remote support user

Click *Delete user*.

About the remote support user

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

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Backup or restore a configuration

Sign in to the web interface and navigate to *Maintenance > Backup and Restore*.

Show the current configuration

Click *Preview backup* to display the current settings on-screen.

Back up the current configuration

Click *Take backup* to store the configuration as a text file.

Restore configuration from backup

1. Click *Browse...* and find the backup file with the configuration you want to restore.
2. Click *Restore* to reconfigure the system as defined in the file.

   Some settings require that you restart the video system before they take effect.

About configuration backup

All the system settings, which are available on the System configuration page, can be listed on-screen or stored as a backup text file.

The backup text file can be loaded back onto the system, thereby restoring the configuration.

We do not recommend that you load back a backup text file from TC software, onto a video system that is running CE software.

The configuration of the video system is likely to be incomplete, due to the differences between the two software generations.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Revert to the previously used software image

Sign in to the web interface and navigate to *Maintenance > System Recovery*.

We recommend you to back up the log files and configuration of the video system before you swap to the previously used software image.

Back up log files and system configuration

1. Select the *Backup* tab.
2. Click *Download Logs* and follow the instructions to save the log files on your computer.
3. Click *Download Configuration Backup* and follow the instructions to save the configuration file on your computer.

Revert to the previously used software image

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

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

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

About the previously used software image

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Factory reset the video system (page 1 of 3)

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

It is not possible to undo a factory reset.

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

We recommend that you use the web interface or user interface to factory reset the video system. If these interfaces are not available, use the reset button.

A factory reset implies:

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

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

We recommend that you back up the log files and configuration of the video system before you perform a factory reset; otherwise these data will be lost.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Factory reset the video system (page 2 of 3)

Factory reset using the web interface

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

Sign in to the web interface and navigate to *Maintenance > System Recovery*.

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

   When the system 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 video system before you continue with the factory reset.

1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *System information > Settings*.
3. Select *Reset system*.
4. Click *Reset* to confirm your choice, or *Back* if you have changed your mind.
5. Wait while the video system reverts to the default factory settings. When finished, the video system restarts automatically. This may take a few minutes.

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

Back up log files and system configuration

Sign in to the web interface and navigate to *Maintenance > System Recovery*.

Back up log files and system configuration

1. Select the *Backup* tab.
2. Click *Download Logs* and follow the instructions to save the log files on your computer.
3. Click *Download Configuration Backup* and follow the instructions to save the configuration file on your computer.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

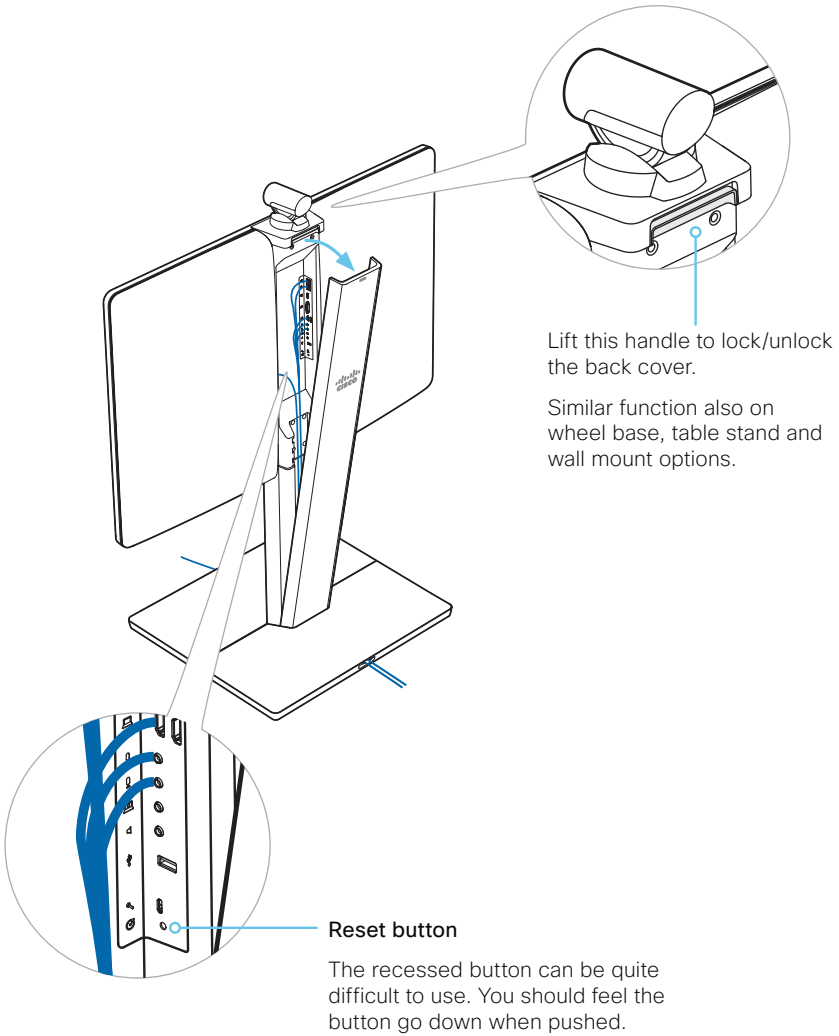
Factory reset the video system (page 3 of 3)

Factory reset using the reset button

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

1. Remove the video system's back cover.
2. Use the tip of a pen (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.
3. Wait while the video system reverts to the default factory settings. When finished, the video system restarts automatically. This may take a few minutes.

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



www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Factory reset the Touch 10

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

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

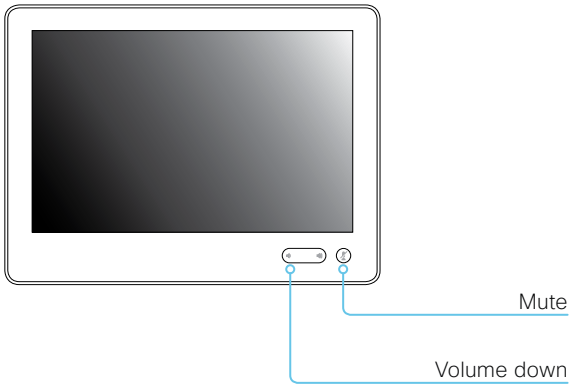
It is not possible to undo a factory reset.

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

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

   If Touch 10 is directly connected to the video system it receives a new configuration automatically from the video system.

   If Touch 10 is connected via LAN the device must be paired to the video system anew. When successfully paired it receives a new configuration automatically from the video system.



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

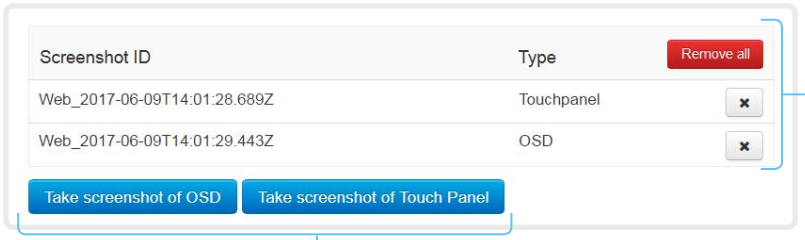
In order to use the Touch 10 controller, Touch 10 must either be directly connected to the codec, or paired to the codec via LAN. The latter is referred to as remote pairing.

Read about pairing and how to connect Touch 10 to the video system in the ▶ Connect the Touch 10 controller chapter.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Capture user interface screenshots

Sign in to the web interface and navigate to *Maintenance > User Interface Screenshots*.



Capture a screenshot

Click *Take screenshot of Touch Panel* to capture a screenshot of the Touch controller, or click *Take screenshot of OSD* to capture a screenshot of the on-screen display.

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

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

Delete screenshots

If you want to delete all screenshots, click *Remove all*.

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

About user interface screenshots

You can capture screenshots both of a Touch controller that is connected to the video system, and of the on-screen display (menus, indicators and messages on the main display).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Chapter 5

System settings

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Overview of the system settings

In the following pages you will find a complete list of the system settings which are configured from the *Setup > Configuration* page on the web interface.

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

How to find the IP address

1. Select the settings icon (cogwheel) in the status bar of the user interface.
2. Select *System Information*.

Audio settings 67
- Audio DefaultVolume 67
- Audio Input Microphone [1] Mode 68
- Audio Input Microphone [2..3] Level 67
- Audio Microphones Mute Enabled 67
- Audio Output InternalSpeaker Mode 68
- Audio SoundsAndAlerts RingTone 67
- Audio SoundsAndAlerts RingVolume 67

CallHistory settings 69
- CallHistory Mode 69

Cameras settings 70
- Cameras Camera [1] Backlight DefaultMode 70
- Cameras Camera [1] Brightness DefaultLevel 70
- Cameras Camera [1] Brightness Mode 70
- Cameras Camera [1] Focus Mode 70
- Cameras Camera [1] Gamma Level 71
- Cameras Camera [1] Gamma Mode 70
- Cameras Camera [1] Mirror 71
- Cameras Camera [1] Whitebalance Level 71
- Cameras Camera [1] Whitebalance Mode 71
- Cameras PowerLine Frequency 71
- Cameras Preset TriggerAutofocus 72

Conference settings 73
- Conference ActiveControl Mode 73
- Conference AutoAnswer Delay 73
- Conference AutoAnswer Mode 73
- Conference AutoAnswer Mute 73
- Conference CallProtocolIPStack 73
- Conference DefaultCall Protocol 74
- Conference DefaultCall Rate 74
- Conference DoNotDisturb DefaultTimeout 74
- Conference Encryption Mode 74
- Conference FarEndControl Mode 74
- Conference FarEndControl SignalCapability 75
- Conference IncomingMultisiteCall Mode 76

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference MaxReceiveCallRate ... 75
Conference MaxTotalReceiveCallRate ... 75
Conference MaxTotalTransmitCallRate ... 75
Conference MaxTransmitCallRate ... 75
Conference MicUnmuteOnDisconnect Mode ... 76
Conference Multipoint Mode ... 76
Conference MultiStream Mode ... 76
Conference Presentation OnPlacedOnHold ... 77
Conference Presentation RelayQuality ... 76
Conference VideoBandwidth Mode ... 77

FacilityService settings ... 78
FacilityService Service [1..5] CallType ... 78
FacilityService Service [1..5] Name ... 78
FacilityService Service [1..5] Number ... 78
FacilityService Service [1..5] Type ... 78

H323 settings ... 79
H323 Authentication LoginName ... 79
H323 Authentication Mode ... 79
H323 Authentication Password ... 79
H323 CallSetup Mode ... 79
H323 Encryption KeySize ... 80
H323 Gatekeeper Address ... 80
H323 H323Alias E164 ... 80
H323 H323Alias ID ... 80
H323 NAT Address ... 81
H323 NAT Mode ... 80
H323 PortAllocation ... 81

Logging settings ... 82
Logging External Mode ... 82
Logging External Protocol ... 82
Logging External Server Address ... 82
Logging External Server Port ... 82
Logging Mode ... 82

Network settings ... 83
Network [1] DNS Domain Name ... 83
Network [1] DNS Server [1..3] Address ... 83
Network [1] IEEE8021X AnonymousIdentity ... 84
Network [1] IEEE8021X Eap Md5 ... 84
Network [1] IEEE8021X Eap Peap ... 85
Network [1] IEEE8021X Eap Tls ... 84
Network [1] IEEE8021X Eap Ttls ... 84
Network [1] IEEE8021X Identity ... 84
Network [1] IEEE8021X Mode ... 83
Network [1] IEEE8021X Password ... 84
Network [1] IEEE8021X TlsVerify ... 83
Network [1] IEEE8021X UseClientCertificate ... 83
Network [1] IPStack ... 85
Network [1] IPv4 Address ... 85
Network [1] IPv4 Assignment ... 85
Network [1] IPv4 Gateway ... 85
Network [1] IPv4 SubnetMask ... 85
Network [1] IPv6 Address ... 86
Network [1] IPv6 Assignment ... 86
Network [1] IPv6 DHCPOptions ... 86
Network [1] IPv6 Gateway ... 86
Network [1] MTU ... 86
Network [1] QoS Diffserv Audio ... 87
Network [1] QoS Diffserv Data ... 87
Network [1] QoS Diffserv ICMPv6 ... 88
Network [1] QoS Diffserv NTP ... 88
Network [1] QoS Diffserv Signalling ... 87
Network [1] QoS Diffserv Video ... 87
Network [1] QoS Mode ... 86
Network [1] RemoteAccess Allow ... 88
Network [1] Speed ... 88
Network [1] TrafficControl Mode ... 89
Network [1] VLAN Voice Mode ... 89
Network [1] VLAN Voice VlanId ... 89

NetworkServices settings ... 90
NetworkServices CDP Mode ... 90
NetworkServices H323 Mode ... 90
NetworkServices HTTP Mode ... 90
NetworkServices HTTPS OCSP Mode ... 91
NetworkServices HTTPS OCSP URL ... 91
NetworkServices HTTPS Server MinimumTLSVersion ... 90
NetworkServices HTTPS StrictTransportSecurity ... 91

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

NetworkServices HTTPS VerifyClientCertificate ... 91
NetworkServices HTTPS VerifyServerCertificate ... 91
NetworkServices NTP Mode ... 92
NetworkServices NTP Server [1..3] Address ... 92
NetworkServices SIP Mode ... 92
NetworkServices SNMP CommunityName ... 93
NetworkServices SNMP Host [1..3] Address ... 92
NetworkServices SNMP Mode ... 92
NetworkServices SNMP SystemContact ... 93
NetworkServices SNMP SystemLocation ... 93
NetworkServices SSH AllowPublicKey ... 93
NetworkServices SSH Mode ... 93
NetworkServices Telnet Mode ... 93
NetworkServices UPnP Mode ... 94
NetworkServices UPnP Timeout ... 94
NetworkServices WelcomeText ... 94
NetworkServices XMLAPI Mode ... 94

Peripherals settings ... 95
Peripherals Pairing CiscoTouchPanels EmcResilience ... 95
Peripherals Pairing CiscoTouchPanels RemotePairing ... 95
Peripherals Pairing Ultrasound Volume MaxLevel ... 95
Peripherals Pairing Ultrasound Volume Mode ... 95
Peripherals Profile Cameras ... 96
Peripherals Profile ControlSystems ... 96
Peripherals Profile TouchPanels ... 96

Phonebook settings ... 97
Phonebook Server [1] ID ... 97
Phonebook Server [1] Type ... 97
Phonebook Server [1] URL ... 97

Provisioning settings ... 98
Provisioning Connectivity ... 98
Provisioning ExternalManager Address ... 99
Provisioning ExternalManager AlternateAddress ... 99
Provisioning ExternalManager Domain ... 100
Provisioning ExternalManager Path ... 99
Provisioning ExternalManager Protocol ... 99
Provisioning HttpMethod ... 99
Provisioning LoginName ... 98
Provisioning Mode ... 98
Provisioning Password ... 99

Proximity settings ... 101
Proximity Mode ... 101
Proximity Services CallControl ... 101
Proximity Services ContentShare FromClients ... 101
Proximity Services ContentShare ToClients ... 101

RoomAnalytics settings ... 102
RoomAnalytics PeoplePresenceDetector ... 102

RTP settings ... 103
RTP Ports Range Start ... 103
RTP Ports Range Stop ... 103

Security settings ... 104
Security Audit Logging Mode ... 104
Security Audit OnError Action ... 104
Security Audit Server Address ... 104
Security Audit Server Port ... 105
Security Audit Server PortAssignment ... 105
Security Session InactivityTimeout ... 105
Security Session MaxSessionsPerUser ... 105
Security Session MaxTotalSessions ... 105
Security Session ShowLastLogon ... 105

SerialPort settings ... 106
SerialPort LoginRequired ... 106
SerialPort Mode ... 106

SIP settings ... 107
SIP ANAT ... 107
SIP Authentication Password ... 107
SIP Authentication UserName ... 107
SIP DefaultTransport ... 107
SIP DisplayName ... 107
SIP Ice DefaultCandidate ... 108
SIP Ice Mode ... 108
SIP Line ... 108
SIP ListenPort ... 108
SIP Mailbox ... 108

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SIP PreferredIPMedia ... 109
SIP PreferredIPSignaling ... 109
SIP Proxy [1..4] Address ... 109
SIP TlsVerify ... 109
SIP Turn DiscoverMode ... 109
SIP Turn DropRflx ... 109
SIP Turn Password ... 110
SIP Turn Server ... 110
SIP Turn UserName ... 110
SIP Type ... 110
SIP URI ... 110

Standby settings ... 111
Standby BootAction ... 111
Standby Control ... 111
Standby Delay ... 111
Standby StandbyAction ... 111
Standby WakeupAction ... 111
Standby WakeupOnMotionDetection ... 111

SystemUnit settings ... 112
SystemUnit Name ... 112

Time settings ... 113
Time DateFormat ... 113
Time TimeFormat ... 113
Time Zone ... 114

UserInterface settings ... 116
UserInterface ContactInfo Type ... 116
UserInterface KeyTones Mode ... 116
UserInterface Language ... 116
UserInterface OSD EncryptionIndicator ... 116
UserInterface OSD Output ... 117
UserInterface Wallpaper ... 117

UserManagement settings ... 118
UserManagement LDAP Admin Filter ... 119
UserManagement LDAP Admin Group ... 119
UserManagement LDAP Attribute ... 119
UserManagement LDAP Encryption ... 118
UserManagement LDAP MinimumTLSVersion ... 118
UserManagement LDAP Mode ... 118
UserManagement LDAP Server Address ... 118
UserManagement LDAP Server Port ... 118
UserManagement LDAP VerifyServerCertificate ... 119

Video settings ... 120
Video ActiveSpeaker DefaultPIPPosition ... 120
Video DefaultLayoutFamily Local ... 120
Video DefaultLayoutFamily Remote ... 121
Video DefaultMainSource ... 121
Video Input Connector [1..4] CameraControl CameraId ... 121
Video Input Connector [1..4] CameraControl Mode ... 121
Video Input Connector [1..4] InputSourceType ... 122
Video Input Connector [1..4] Name ... 122
Video Input Connector [1..4] OptimalDefinition Profile ... 123
Video Input Connector [1..4] OptimalDefinition Threshold60fps ... 123
Video Input Connector [1..4] Visibility ... 124
Video Input Connector [2..4] PresentationSelection ... 124
Video Input Connector [2..4] Quality ... 122
Video Input Connector [2..4] RGBQuantizationRange ... 124
Video Input Connector [2] DviType ... 122
Video Monitors ... 125
Video Output Connector [1..2] Resolution ... 126
Video Output Connector [1] Brightness ... 125
Video Output Connector [1] Whitebalance Level ... 127
Video Output Connector [2] CEC Mode ... 125
Video Output Connector [2] Location HorizontalOffset ... 125
Video Output Connector [2] Location VerticalOffset ... 126
Video Output Connector [2] OverscanLevel ... 126
Video Output Connector [2] RGBQuantizationRange ... 127
Video Presentation DefaultPIPPosition ... 127
Video Presentation DefaultSource ... 127
Video Selfview Default FullscreenMode ... 128
Video Selfview Default Mode ... 128
Video Selfview Default OnMonitorRole ... 128
Video Selfview Default PIPPosition ... 128
Video Selfview OnCall Duration ... 129
Video Selfview OnCall Mode ... 129

Experimental settings ... 130

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Audio settings

Audio DefaultVolume

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

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

Select a value between 1 and 100. This corresponds to the dB range from -34.5 dB to 15 dB, in steps of 0.5 dB. If set to 0 the audio is switched off.

Audio Microphones Mute Enabled

Define the microphone mute behaviour on the video system.

Requires user role: ADMIN, INTEGRATOR

Default value: True

Value space: True/InCallOnly

True: Muting of audio is always available.

InCallOnly: Muting of audio is only available when the device is in a call. When Idle it is not possible to mute the microphone. This is useful when an external telephone service/ audio system is connected via the codec and is to be available when the codec is not in a call. When set to InCallOnly this will prevent the audio-system from being muted by mistake.

Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Sunrise

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

Select a ringtone from the list.

Audio SoundsAndAlerts RingVolume

Define the ring volume for incoming calls.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: 40

Value space: Integer (0..100)

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

Audio Input Microphone [2..3] Level

Define the audio level of the Microphone input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: 14

Value space: Integer (0..24)

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Audio Input Microphone [1] Mode

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

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the audio input microphone connector.

On: Enable the audio input microphone connector.

Audio Output InternalSpeaker Mode

Define whether or not to use the video system's integrated speakers.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the video system's integrated speakers.

On: Enable the video system's integrated speakers.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Cameras settings

Cameras Camera [1] Backlight DefaultMode

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

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Cameras Camera [1] Brightness Mode

Define the camera brightness mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

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

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

Cameras Camera [1] Brightness DefaultLevel

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

Requires user role: ADMIN, INTEGRATOR

Default value: 20

Value space: Integer (1..31)

The brightness level.

Cameras Camera [1] Focus Mode

Define the camera focus mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: The camera will auto focus once a call is connected, as well as after moving the camera (pan, tilt, zoom). The system will use auto focus only for a few seconds to set the right focus; then auto focus is turned off to prevent continuous focus adjustments of the camera.

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

Cameras Camera [1] Gamma Mode

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Cameras Camera [1] Gamma Level

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 Camera [1] Mirror

With Mirror mode (horizontal flip) you can mirror the image on screen. Mirroring applies both to the self-view and the video that is transmitted to the far end.

Requires user role: ADMIN, INTEGRATOR

Default value: MX300G2: Off MX200G2: On

Value space: Off/On

Off: For MX300G2, display the image as other people see you; for MX200G2, display the image as you see yourself in a mirror.

On: For MX300G2, display the image as you see yourself in a mirror; for MX200G2, display the image as other people see you.

Cameras Camera [1] Whitebalance Mode

Define the camera white balance mode.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Manual

Auto: The camera will continuously adjust the white balance depending on the camera view.

Manual: Enables manual control of the camera white balance. The white balance level is set using the Cameras Camera [n] Whitebalance Level setting.

Cameras Camera [1] Whitebalance Level

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

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: Integer (1..16)

The white balance level.

Cameras PowerLine Frequency

The video system's camera is able to compensate for any flicker noise from the electrical power supply (power line frequency anti-flickering). The camera also supports auto detection of line frequency. Select the Auto option (default), or set this camera configuration based on your power line frequency.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: 50Hz/60Hz/Auto

50Hz: Use this value when the power line frequency is 50 Hz.

60Hz: Use this value when the power line frequency is 60 Hz.

Auto: Allow the camera to detect the power frequency automatically.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Cameras Preset TriggerAutofocus

The current position (pan and tilt), zoom and focus are stored with a preset. Use this setting to determine if the camera should refocus or use the focus value that is stored with the preset.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

Auto: Whether the camera refocuses or not when selecting a preset, depends on the camera type.

Off: The focus value that is stored with the preset will be used. The camera will not refocus when selecting a preset.

On: The camera will refocus when selecting a preset. The focus value that is stored with the preset may be overridden.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference settings

Conference ActiveControl Mode

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

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off

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

Off: Active control is disabled.

Conference AutoAnswer Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: You must answer incomming calls manually by tapping Answer on the Touch controller.

On: The system automatically answers incoming calls, except if you are already in a call. You must always answer or decline incoming calls manually when you are already engaged in a call.

Conference AutoAnswer Mute

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The incoming call will not be muted.

On: The incoming call will be muted when automatically answered.

Conference AutoAnswer Delay

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..50)

The auto answer delay (seconds).

Conference CallProtocolIPStack

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference DefaultCall Protocol

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

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 system cannot register, the auto-selection chooses H323.

H320: All calls are set up as H.320 calls (only applicable if connected to 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 Spark registered systems. Do not use.

Conference DefaultCall Rate

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

Requires user role: ADMIN, INTEGRATOR

Default value: 6000

Value space: Integer (64..6000)

The default call rate (kbps).

Conference DoNotDisturb DefaultTimeout

This setting determines the default duration of a Do Not Disturb session, i.e. the period when incoming calls are rejected and registered as missed calls. The session can be terminated earlier by using the user interface. The default value is 60 minutes.

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 video system, the encryption mode is always Off.

Requires user role: ADMIN

Default value: BestEffort

Value space: Off/On/BestEffort

Off: The system will not use encryption.

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

BestEffort: The system will use encryption whenever possible.

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

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

Conference FarEndControl Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference FarEndControl SignalCapability

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

Conference MaxReceiveCallRate

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum receive call rate (kbps).

Conference MaxTransmitCallRate

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum transmitt call rate (kbps).

Conference MaxTotalReceiveCallRate

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

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

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

Requires user role: ADMIN

Default value: 6000

Value space: Integer (64..6000)

The maximum receive call rate (kbps).

Conference MaxTotalTransmitCallRate

This configuration applies when using a video system'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).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference MicUnmuteOnDisconnect Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

On: Unmute the microphones after the call is disconnected.

Conference Multipoint Mode

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

If registered to a Cisco TelePresence Video Communication Server (VCS), the video system can use its own built-in MultiSite feature. If registered to a Cisco Unified Communications Manager (CUCM) version 8.6.2 or newer, the video system can use either the CUCM conference bridge, or the video system'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 built-in MultiSite allows up to four participants (yourself included).

The built-in MultiSite is optional and may not be available on all video systems.

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 MultiStream Mode

The video system supports multistream video for conferences.

Requires user role: ADMIN

Default value: Off

Value space: Off

Off: Multistream is disabled.

Conference IncomingMultisiteCall Mode

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

Requires user role: ADMIN

Default value: Allow

Value space: Allow/Deny

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

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

Conference Presentation RelayQuality

This configuration applies to video systems that are using the built-in MultiSite feature (optional) to host a multipoint video conference. When a remote user shares a presentation, the video system 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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Conference Presentation OnPlacedOnHold

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

Requires user role: ADMIN

Default value: NoAction

Value space: Stop/NoAction

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

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

Conference VideoBandwidth Mode

Define the conference video bandwidth mode.

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

FacilityService settings

FacilityService Service [1..5] Type

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

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 [1..5] Name

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

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 [1..5] Number

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

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 1024)

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

FacilityService Service [1..5] CallType

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

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

H323 settings

H323 Authentication Mode

Define the authenticatin mode for the H.323 profile.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

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

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

H323 Authentication LoginName

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication login name.

H323 Authentication Password

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The authentication password.

H323 CallSetup Mode

Defines whether to use a Gatekeeper or Direct calling when establishing H.323 calls.

Direct H.323 calls can be made also when H323 CallSetup Mode is set to Gatekeeper.

Requires user role: ADMIN

Default value: Gatekeeper

Value space: Direct/Gatekeeper

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

H323 Encryption KeySize

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

Requires user role: ADMIN

Default value: Min1024bit

Value space: Min1024bit/Max1024bit/Min2048bit

Min1024bit: The minimum size is 1024 bit.

Max1024bit: The maximum size is 1024 bit.

Min2048bit: The minimum size is 2048 bit.

H323 Gatekeeper Address

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

H323 H323Alias E164

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 30)

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

H323 H323Alias ID

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 49)

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

H323 NAT Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Auto/Off/On

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

Off: The system will signal the real IP address.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

H323 NAT Address

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

In the router, the following ports must be routed to the system's IP address:

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

H323 PortAllocation

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

Requires user role: ADMIN

Default value: Dynamic

Value space: Dynamic/Static

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Logging settings

Logging External Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable logging to a remote syslog server.

On: Enable logging to a remote syslog server.

Logging External Protocol

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

Requires user role: ADMIN

Default value: SyslogTLS

Value space: Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

Logging External Server Address

The address of the remote syslog server.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

Logging External Server Port

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

Requires user role: ADMIN

Default value: 514

Value space: Integer (0..65535)

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

Logging Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the system logging service.

On: Enable the system logging service.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network settings

Network [1] DNS Domain Name

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

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The DNS domain name.

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

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address or IPv6 address.

Network [1] IEEE8021X Mode

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

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

Off: The 802.1X authentication is disabled (default).

On: The 802.1X authentication is enabled.

Network [1] IEEE8021X TlsVerify

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

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

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

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

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

Network [1] IEEE8021X UseClientCertificate

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

Requires user role: ADMIN, USER

Default value: Off

Value space: Off/On

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] IEEE8021X Identity

Define the user name for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The user name for 802.1X authentication.

Network [1] IEEE8021X Password

Define the password for 802.1X authentication.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 50)

The password for 802.1X authentication.

Network [1] IEEE8021X AnonymousIdentity

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

The 802.1X Anonymous ID string.

Network [1] IEEE8021X Eap Md5

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled (default).

Network [1] IEEE8021X Eap Ttls

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled (default).

Network [1] IEEE8021X Eap Tls

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled (default).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] IEEE8021X Eap Peap

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled (default).

Network [1] IPStack

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

Requires user role: ADMIN, USER

Default value: Dual

Value space: Dual/IPv4/IPv6

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

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

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

Network [1] IPv4 Assignment

Define how the system will obtain its IPv4 address, subnet mask and gateway address. This setting applies only to systems on IPv4 networks.

Requires user role: ADMIN, USER

Default value: DHCP

Value space: Static/DHCP

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

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

Network [1] IPv4 Address

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

Network [1] IPv4 Gateway

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

Network [1] IPv4 SubnetMask

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] IPv6 Assignment

Define how the system will obtain its IPv6 address and the default gateway address. This setting applies only to systems on IPv6 networks.

Requires user role: ADMIN, USER

Default value: Autoconf

Value space: Static/DHCPv6/Autoconf

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

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

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

Network [1] IPv6 Address

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

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

Network [1] IPv6 Gateway

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv6 address.

Network [1] IPv6 DHCPOptions

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

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

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

Network [1] MTU

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

Requires user role: ADMIN, USER

Default value: 1500

Value space: Integer (576..1500)

Set a value for the MTU (bytes).

Network [1] QoS Mode

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

Requires user role: ADMIN, USER

Default value: Diffserv

Value space: Off/Diffserv

Off: No QoS method is used.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] QoS Diffserv Audio

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

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the audio packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Video

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the video packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Data

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

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the data packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Signalling

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

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the signalling packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] QoS Diffserv ICMPv6

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

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the ICMPv6 packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv NTP

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

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

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

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

Requires user role: ADMIN, USER

Default value: 0

Value space: Integer (0..63)

Set the priority of the NTP packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] RemoteAccess Allow

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

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

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 255)

A valid IPv4 address or IPv6 address.

Network [1] Speed

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

Requires user role: ADMIN, USER

Default value: Auto

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

Auto: Autonegotiate link speed.

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

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

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

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Network [1] TrafficControl Mode

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

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: Transmit video packets at link speed.

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

Network [1] VLAN Voice Mode

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

Requires user role: ADMIN, USER

Default value: Auto

Value space: Auto/Manual/Off

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

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

Off: VLAN is not enabled.

Network [1] VLAN Voice VlanId

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

Requires user role: ADMIN, USER

Default value: 1

Value space: Integer (1..4094)

Set the VLAN voice ID.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

NetworkServices settings

NetworkServices CDP Mode

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

NetworkServices H323 Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

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

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

NetworkServices HTTP Mode

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

If you need extra security (encryption and decryption of requests, and pages that are returned by the web server), allow only HTTPS.

Requires user role: ADMIN

Default value: HTTP+HTTPS

Value space: Off/HTTP+HTTPS/HTTPS

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

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

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

NetworkServices HTTPS 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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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 system connects to an external HTTPS server (like a phone book server or an external manager), this server will present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify server certificates.

On: Requires the system to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS VerifyClientCertificate

When the video system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the video system to identify itself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Do not verify client certificates.

On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS OCSP Mode

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

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable OCSP support.

On: Enable OCSP support.

NetworkServices HTTPS OCSP URL

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid URL.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the system's time and date to a reference time server. The time server will be queried regularly for time updates.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Manual/Off

Auto: The system will use an NTP server for time reference. As default, the server address will be obtained from the network's DHCP server. If a DHCP server is not used, or if the DHCP server does not provide an NTP server address, the NTP server address that is specified in the NetworkServices NTP Server [n] Address setting will be used.

Manual: The system will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The system will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

NetworkServices NTP Server [1..3] Address

The address of the NTP server that will be used when NetworkServices NTP Mode is set to Manual, and when NetworkServices NTP Mode is set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN

Default value: 0.tandberg.pool.ntp.org

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SIP Mode

Define whether the system should be able to place and receive SIP calls or not.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Disable the possibility to place and receive SIP calls.

On: Enable the possibility to place and receive SIP calls (default).

NetworkServices SNMP Mode

SNMP (Simple Network Management Protocol) is used in network management systems to monitor network-attached devices (routers, servers, switches, projectors, etc) for conditions that warrant administrative attention. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

Requires user role: ADMIN

Default value: ReadOnly

Value space: Off/ReadOnly/ReadWrite

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

ReadWrite: Enable the SNMP network service for both queries and commands.

NetworkServices SNMP Host [1..3] Address

Define the address of up to three SNMP Managers.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), for example about system location and system contact. SNMP traps are not supported.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

NetworkServices SNMP CommunityName

Define the name of the Network Services SNMP Community. SNMP Community names are used to authenticate SNMP requests. SNMP requests must have a password (case sensitive) in order to receive a response from the SNMP Agent in the codec. The default password is "public". If you have the Cisco TelePresence Management Suite (TMS) you must make sure the same SNMP Community is configured there too. NOTE: The SNMP Community password is case sensitive.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The SNMP community name.

NetworkServices SNMP SystemContact

Define the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The name of the SNMP system contact.

NetworkServices SNMP SystemLocation

Define the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

The name of the SNMP system location.

NetworkServices SSH Mode

SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

NetworkServices SSH AllowPublicKey

Secure Shell (SSH) public key authentication can be used to access the codec.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The SSH public key is not allowed.

On: The SSH public key is allowed.

NetworkServices Telnet Mode

Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The Telnet protocol is disabled. This is the factory setting.

On: The Telnet protocol is enabled.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

NetworkServices UPnP Mode

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video system has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video system. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting. Use the video system's web interface to set the timeout.

When UPnP is enabled, the video system advertises its presence on the network. The advertisement permits a Touch controller to discover video systems automatically, and you do not need to manually enter the video system's IP address in order to pair the Touch controller.

Requires user role: ADMIN

Default value: On

Value space: <Off/On>

Off: UPnP is disabled. The video system does not advertise its presence, and you have to enter the video system's IP address manually in order to pair a Touch controller to the video system.

On: UPnP is enabled. The video system advertises its presence until the timeout period expires.

NetworkServices UPnP Timeout

Define for how many seconds UPnP shall stay enabled after the video system is switched on or restarted. The NetworkServices UPnP Mode setting must be On for this setting to take any effect.

Requires user role: ADMIN

Default value: 600

Value space: <0..3600>

Range: Select a value between 0 and 3600 seconds.

NetworkServices WelcomeText

Choose which information the user should see when logging on to the codec through Telnet/SSH.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The welcome text is: Login successful

On: The welcome text is: Welcome to <system name>; Software version; Software release date; Login successful.

NetworkServices XMLAPI Mode

Enable or disable the video system's XML API. For security reasons this may be disabled. Disabling the XML API will limit the remote manageability with for example TMS, which no longer will be able to connect to the video system.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The XML API is disabled.

On: The XML API is enabled (default).

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Peripherals settings

Peripherals Pairing CiscoTouchPanels EmcResilience

If the Touch controller is used in environments with considerable amounts of electromagnetic noise present, you may experience an appearance of false signals—for example as if someone tapped the Touch controller when obviously nobody did so. To cope with this you may enable the EMC Resilience Mode.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The EMC resilience is disabled.

On: The EMC resilience is enabled.

Peripherals Pairing CiscoTouchPanels RemotePairing

In order to use Cisco Touch 10 (touch panel) as user interface for the video system, Touch 10 must be either directly connected to the video system or paired to the video system via LAN. The latter is referred to as remote pairing.

Remote pairing is allowed by default; you must switch this setting Off if you want to prevent remote pairing.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Remote pairing of Touch 10 is not allowed.

On: Remote pairing of Touch 10 is allowed.

Peripherals Pairing Ultrasound Volume Mode

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

Requires user role: ADMIN, INTEGRATOR

Default value: Dynamic

Value space: Dynamic/Static

Dynamic: The video system adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Peripherals Pairing Ultrasound Volume MaxLevel setting.

Static: Use only if advised by Cisco.

Peripherals Pairing Ultrasound Volume MaxLevel

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message. Refer to the Peripherals Pairing Ultrasound Volume Mode setting.

Requires user role: ADMIN, INTEGRATOR

Default value: 60

Value space: Integer (0..80)

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Peripherals Profile Cameras

Define the number of cameras that are expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected cameras does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN, INTEGRATOR

Default value: Minimum1

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

NotSet: No camera check is performed.

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

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

Peripherals Profile ControlSystems

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: NotSet

Value space: 1/NotSet

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

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

Peripherals Profile TouchPanels

Define the number of Cisco Touch controllers that are expected to be connected to the video system. This information is used by the video system's diagnostics service. If the number of connected Touch controllers does not match this setting, the diagnostics service will report it as an inconsistency.

Requires user role: ADMIN, INTEGRATOR

Default value: Minimum1

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

NotSet: No touch panel check is performed.

Minimum1: At least one Cisco Touch controller should be connected to the video system.

0-5: Select the number of Touch controllers that are expected to be connected to the video system. Note that only one Cisco Touch controller is officially supported.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Phonebook settings

Phonebook Server [1] ID

Define a name for the external phone book.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 64)

The name for the external phone book.

Phonebook Server [1] Type

Select the phonebook server type.

Requires user role: ADMIN

Default value: Off

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

Off: Do not use a phonebook.

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

Spark: The phonebook is located on Spark.

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

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

Phonebook Server [1] URL

Define the address (URL) to the external phone book server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid address (URL) to the phone book server.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Provisioning settings

Provisioning Connectivity

This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN, USER

Default value: Auto

Value space: Internal/External/Auto

Internal: Request internal configuration.

External: Request external configuration.

Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the "e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

Provisioning Mode

It is possible to configure a video system using a provisioning system (external manager). This allows video conferencing network administrators to manage many video systems simultaneously. With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/ representative for more information.

Requires user role: ADMIN, USER

Default value: Auto

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

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

Auto: Automatically select the provisioning server.

CUCM: Push configurations to the video system from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the video system from CUCM (Cisco Unified Communications Manager). The system connects to CUCM via the Collaboration Edge infrastructure.

Spark: Push configurations to the video system from Spark.

TMS: Push configurations to the video system from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the video system from VCS (Cisco TelePresence Video Communication Server).

Provisioning LoginName

This is the username part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 80)

A valid username.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Provisioning Password

This is the password part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid password.

Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

Requires user role: ADMIN, USER

Default value: POST

Value space: GET/POST

GET: Select GET when the provisioning server supports GET.

POST: Select POST when the provisioning server supports POST.

Provisioning ExternalManager Address

Define the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the system will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.

When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager AlternateAddress

Only applicable when the endpoint is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Define the address of the alternate CUCM. If the main CUCM is not available, the endpoint will be provisioned by the alternate CUCM. When the main CUCM is available again, the endpoint will be provisioned by this CUCM.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager Protocol

Define whether to use the HTTP (unsecure communication) or HTTPS (secure communication) protocol when sending requests to the external manager / provisioning system.

The 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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Proximity settings

Proximity Mode

Determine whether the video system will emit ultrasound pairing messages or not.

When the video system emits ultrasound, Proximity clients can detect that they are close to the video system. In order to use a client, at least one of the Proximity services must be enabled (refer to the Proximity Services settings). In general, Cisco recommends enabling all the Proximity services.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: The video system does not emit ultrasound, and Proximity services cannot be used.

On: The video system emits ultrasound, and Proximity clients can detect that they are close to the video system. Enabled Proximity services can be used.

Proximity Services CallControl

Enable or disable basic call control features on Proximity clients. When this setting is enabled, you are able to control a call using a Proximity client (for example dial, mute, adjust volume and hang up). This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Call control from a Proximity client is enabled.

Disabled: Call control from a Proximity client is disabled.

Proximity Services ContentShare FromClients

Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the video system, e.g. share your laptop screen. This service is supported by laptops (OS X and Windows). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Enabled

Value space: Enabled/Disabled

Enabled: Content sharing from a Proximity client is enabled.

Disabled: Content sharing from a Proximity client is disabled.

Proximity Services ContentShare ToClients

Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the video system. You can zoom in on details, view previous content and take snapshots. This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER

Default value: Disabled

Value space: Enabled/Disabled

Enabled: Content sharing to a Proximity client is enabled.

Disabled: Content sharing to a Proximity client is disabled.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

RoomAnalytics settings

RoomAnalytics PeoplePresenceDetector

The video system 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 video system's status does not show whether or not there are people present in the room.

On: The video system's status shows whether or not there are people present in the room.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

RTP settings

RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

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

Requires user role: ADMIN

Default value: 2326

Value space: Integer (1024..65438)

Set the first port in the range of RTP ports.

RTP Ports Range Stop

Define the last port in the range of RTP ports.

As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

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

Requires user role: ADMIN

Default value: 2486

Value space: Integer (1120..65535)

Set the last port in the range of RTP ports.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Security settings

Security Audit Logging Mode

Define where to record or transmit the audit logs. The audit logs are sent to a syslog server.

When using the External/ExternalSecure modes and setting the port assignment to manual in the Security Audit Server PortAssignment setting, you must also enter the address and port number for the audit server in the Security Audit Server Address and Security Audit Server Port settings.

Requires user role: AUDIT

Default value: Off

Value space: Off/Internal/External/ExternalSecure

Off: No audit logging is performed.

Internal: The system records the audit logs to internal logs, and rotates logs when they are full.

External: The system sends the audit logs to an external syslog server. The syslog server must support UDP.

ExternalSecure: The system sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the codec using the web interface. The common_name parameter of a certificate in the CA list must match the IP address of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

Security Audit OnError Action

Define what happens when the connection to the syslog server is lost. This setting is only relevant when Security Audit Logging Mode is set to ExternalSecure.

Requires user role: AUDIT

Default value: Ignore

Value space: Halt/Ignore

Halt: If a halt condition is detected the system codec is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the syslog server. Halt conditions are: A network breach (no physical link), no syslog server running (or incorrect address or port to the syslog server), TLS authentication failed (if in use), local backup (re-spooling) log full.

Ignore: The system will continue its normal operation, and rotate internal logs when full. When the connection is restored it will again send its audit logs to the syslog server.

Security Audit Server Address

The audit logs are sent to a syslog server. Define the IP address of the syslog server. Only valid IPv4 or IPv6 address formats are accepted. Host names are not supported. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

Requires user role: AUDIT

Default value: ""

Value space: String (0, 255)

A valid IPv4 address or IPv6 address

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the system shall send its audit logs to. This setting is only relevant when Security Audit Server PortAssignment is set to Manual.

Requires user role: AUDIT

Default value: 514

Value space: Integer (0..65535)

Set the audit server port.

Security Audit Server PortAssignment

The audit logs are sent to a syslog server. You can define how the port number of the external syslog server will be assigned. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure. To see which port number is used you can check the Security Audit Server Port status. Navigate to Configuration > System status on the web interface or; if on a command line interface, run the command xStatus Security Audit Server Port.

Requires user role: AUDIT

Default value: Auto

Value space: Auto/Manual

Auto: Will use UDP port number 514 when the Security Audit Logging Mode is set to External. Will use TCP port number 6514 when the Security Audit Logging Mode is set to ExternalSecure.

Manual: Will use the port value defined in the Security Audit Server Port setting.

Security Session InactivityTimeout

Define how long the system will accept inactivity from the user before he is automatically logged out from a web, Telnet, or SSH session.

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10000)

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

Security Session MaxSessionsPerUser

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..100)

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

Security Session MaxTotalSessions

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..100)

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

Security Session ShowLastLogon

When logging in to the system using SSH or Telnet you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

On: Show information about the last session.

Off: Do not show information about the last session.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SerialPort settings

SerialPort Mode

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

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Disable the serial port.

On: Enable the serial port.

SerialPort LoginRequired

Define if login shall be required when connecting to the serial port.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The user can access the codec via the serial port without any login.

On: Login is required when connecting to the codec via the serial port.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SIP settings

SIP ANAT

ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable ANAT.

On: Enable ANAT.

SIP Authentication UserName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid username.

SIP Authentication Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

SIP DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Default value: Auto

Value space: TCP/UDP/Tls/Auto

TCP: The system will always use TCP as the default transport method.

UDP: The system will always use UDP as the default transport method.

Tls: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the video system. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.

Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

SIP DisplayName

When configured the incoming call will report the display name instead of the SIP URI.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 550)

The name to be displayed instead of the SIP URI.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the video systems can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the video systems.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Off/On

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

Off: ICE is disabled.

On: ICE is enabled.

SIP Ice DefaultCandidate

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

Requires user role: ADMIN

Default value: Host

Value space: Host/Rflx/Relay

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

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

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

SIP Line

When registered to a Cisco Unified Communications Manager (CUCM) the endpoint may be part of a shared line. This means that several devices share the same directory number. The different devices sharing the same number receive status from the other appearances on the line as defined in RFC 4235.

Note that shared lines are set up by CUCM, not by the endpoint. Therefore do not change this setting manually; CUCM pushes this information to the endpoint when required.

Requires user role: ADMIN

Default value: Private

Value space: Private/Shared

Shared: The system is part of a shared line and is therefore sharing its directory number with other devices.

Private: This system is not part of a shared line (default).

SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the endpoint will only be reachable through the SIP registrar (CUCM or VCS).

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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SIP PreferredIPMedia

Define the preferred IP version for sending and receiving media (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for media is IPv4.

IPv6: The preferred IP version for media is IPv6.

SIP PreferredIPSignaling

Define the preferred IP version for signaling (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version. It also determines the priority of the A/AAAA lookups in DNS, so that the preferred IP version is used for registration.

Requires user role: ADMIN

Default value: IPv4

Value space: IPv4/IPv6

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

SIP Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

SIP TlsVerify

For TLS connections a SIP CA-list can be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.

On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the system will test if port allocation is possible.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Set to Off to disable discovery mode.

On: When set to On, the system will search for available Turn servers in DNS, and before making calls the system will test if port allocation is possible.

SIP Turn DropRflx

DropRflx will make the endpoint force media through the Turn relay, unless the remote endpoint is on the same network.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: Disable DropRflx.

On: The system will force media through the Turn relay when the remote endpoint is on another network.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SIP Turn Server

Define the address of the TURN (Traversal Using Relay NAT) server. It is used as a media relay fallback and it is also used to discover the endpoint's own public IP address.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The preferred format is DNS SRV record (e.g. _turn._udp.<domain>), or it can be a valid IPv4 or IPv6 address.

SIP Turn UserName

Define the user name needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid user name.

SIP Turn Password

Define the password needed for accessing the TURN server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

A valid password.

SIP Type

Enables SIP extensions and special behavior for a vendor or provider.

Requires user role: ADMIN

Default value: Standard

Value space: Standard/Cisco

Standard: Use this when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)

Cisco: Use this when registering to Cisco Unified Communication Manager.

SIP URI

The SIP URI (Uniform Resource Identifier) is the address that is used to identify the video system. The URI is registered and used by the SIP services to route inbound calls to the system. The SIP URI syntax is defined in RFC 3261.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

An address (URI) that is compliant with the SIP URI syntax.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Standby settings

Standby Control

Define whether the system should go into standby mode or not.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: The system will not enter standby mode.

On: The system will enter standby mode when the Standby Delay has timed out. Requires the Standby Delay to be set to an appropriate value.

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. Requires the Standby Control to be enabled.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..480)

Set the standby delay (minutes).

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: DefaultCameraPosition

Value space: None/DefaultCameraPosition/RestoreCameraPosition

None: No action.

RestoreCameraPosition: When the video system restarts, the camera returns to the position that it had before the restart.

DefaultCameraPosition: When the video system restarts, the camera moves to the factory default position.

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN, INTEGRATOR

Default value: PrivacyPosition

Value space: None/PrivacyPosition

None: No action.

PrivacyPosition: When the video system enters standby, the camera turns to a sideways position for privacy.

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: RestoreCameraPosition

Value space: None/RestoreCameraPosition/DefaultCameraPosition

None: No action.

RestoreCameraPosition: When the video system leaves standby, the camera returns to the position that it had before entering standby.

DefaultCameraPosition: When the video system leaves standby, the camera moves to the factory default position.

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, and the Proximity Mode setting must be On to make the feature work.

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 system will automatically wake up from standby.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

SystemUnit settings

SystemUnit Name

Define the system name. The system name will be sent as the hostname in a DHCP request and when the codec is acting as an SNMP Agent.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 50)

Define the system name.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Time Zone

Define the time zone for the geographical location of the video system. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: ADMIN, 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/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu

Select a time zone from the list.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

UserInterface settings

UserInterface ContactInfo Type

Choose which type of contact information to show in the status field in the upper left corner of the display and Touch controller.

Requires user role: ADMIN

Default value: Auto

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

Auto: Show the address which another system should dial to reach this video system. The address depends on the default call protocol and system registration.

None: Do not show any contact information.

IPv4: Show the system's IPv4 address.

IPv6: Show the system's IPv6 address.

H323Id: Show the system's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the system's H.320 number as contact information (only applicable if connected to Cisco TelePresence ISDN Link).

E164Alias: Show the system's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

SipUri: Show the system's SIP URI (refer to the SIP URI setting).

SystemName: Show the system's name (refer to the SystemUnit Name setting).

DisplayName: Show the system's display name (refer to the SIP DisplayName setting).

UserInterface KeyTones Mode

You can configure the system to make a keyboard click sound effect (key tone) when typing text or numbers.

Requires user role: ADMIN, USER

Default value: On

Value space: Off/On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

UserInterface Language

Select the language to be used in menus and messages on the screen and Touch controller.

Requires user role: ADMIN, USER

Default value: English

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

Select a language from the list. Arabic and Hebrew are not supported in this software version.

UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator (a padlock) is shown on screen. The icon for encrypted calls is a locked padlock, and the icon for non-encrypted calls is a crossed out locked padlock.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/AlwaysOn/AlwaysOff

Auto: If the call is encrypted, a “Call is encrypted” notification is shown for 5 seconds, while the encryption indicator icon is shown for the duration of the call.

If the call is not encrypted, a “Call is not encrypted” notification is shown for 5 seconds. Also the encryption indicator icon disappears from screen after 5 seconds.

AlwaysOn: The encryption indicator is displayed on screen during the entire call.

AlwaysOff: The encryption indicator is never displayed on screen.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

UserInterface OSD Output

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/1/2

Auto: The system sends the on-screen information and indicators to the system's integrated LCD display.

Range 1-2: The system sends the information and indicators to the specified output. Choose 1 to send the on-screen information and indicators to the integrated LCD display; choose 2 to send the OSD to a display that is connected to the system's HDMI output.

UserInterface Wallpaper

Select a background image (wallpaper) for the video screen when idle.

You may upload a custom wallpaper to the video system using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 4 MByte. When you use a custom wallpaper, the clock and the list of upcoming meetings are removed from the main display

Requires user role: ADMIN, 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 system, the setting will revert to the default value.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

UserManagement settings

UserManagement LDAP Mode

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

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: LDAP authentication is not allowed.

On: For client certificate verification to work when LDAP authentication is enabled, the codec requires a CA (Certificate Authority) certificate, and the user must have a Client Certificate that matches their user distinguishing name (DN) in the active directory (AD).

UserManagement LDAP Server Address

Set the IP address or hostname of the LDAP server.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

A valid IPv4 address, IPv6 address or hostname.

UserManagement LDAP Server Port

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..65535)

The LDAP server port number.

UserManagement LDAP Encryption

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

Requires user role: ADMIN

Default value: LDAPS

Value space: LDAPS/None/STARTTLS

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

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

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

UserManagement LDAP MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.2

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

TLSv1.0: Support TLS version 1.0 or higher.

TLSv1.1: Support TLS version 1.1 or higher.

TLSv1.2: Support TLS version 1.2 or higher.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

UserManagement LDAP VerifyServerCertificate

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

Requires user role: ADMIN

Default value: On

Value space: Off/On

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

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

UserManagement LDAP Admin Filter

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

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

UserManagement LDAP Admin Group

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

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

UserManagement LDAP Attribute

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

Requires user role: ADMIN

Default value: ""

Value space: String (0, 255)

The attribute name.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video settings

Video ActiveSpeaker DefaultPIPPosition

Define the position on screen of the active speaker picture-in-picture (PiP). The setting only takes effect when using a video layout where the active speaker is a PiP, i.e. the Overlay layout, or possibly a Custom layout (refer to the Video DefaultLayoutFamily Local setting). The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the active speaker PiP will be kept unchanged when leaving a call.

UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.

UpperCenter: The active speaker PiP will appear in the upper center position.

UpperRight: The active speaker PiP will appear in the upper right corner of the screen.

CenterLeft: The active speaker PiP will appear in the center left position.

CentreRight: The active speaker PiP will appear in the center right position.

LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.

LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

Video DefaultLayoutFamily Local

Select which video layout family to use locally.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single>

Auto: The default layout family, as given in the layout database provided by the system, will be used as the local layout.

Equal: The Equal layout family will be used as the local layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the local layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the local layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video DefaultLayoutFamily Remote

Select which video layout family to be used for the remote participants.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single

Auto: The default layout family, as given by the local layout database, will be used as the remote layout.

Equal: The Equal layout family will be used as the remote layout. All videos have equal size, as long as there is space enough on the screen.

Prominent: The Prominent layout family will be used as the remote layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.

Overlay: The Overlay layout family will be used as the remote layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.

Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video DefaultMainSource

Define which video input source shall be used as the main video source.

Requires user role: ADMIN, USER

Default value: 1

Value space: 1/2/3

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

Video Input Connector [1..4] CameraControl Mode

Define whether the camera that is connected to this video input connector can be controlled or not.

Note that camera control is not available for Connector 2 (HDMI), Connector 3 (HDMI) and Connector 4 (DVI-I).

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: On Connector 2,3,4: Off

Value space: Connector 1: Off/On Connector 2,3,4: Off

Off: Disable camera control.

On: Enable camera control.

Video Input Connector [1..4] CameraControl CameraId

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

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: 1

The camera ID is fixed and cannot be changed.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Input Connector [2] DviType

The official DVI standard supports both digital and analog signals. In most cases the default AutoDetect setting can detect whether the signal is analog RGB or digital. However, in some rare cases when DVI-I cables are used (these cables can carry both the analog and digital signals) the auto detection fails. This setting makes it possible to override the AutoDetect and select the correct DVI video input.

Requires user role: ADMIN

Default value: AutoDetect

Value space: AutoDetect/Digital/AnalogRGB/AnalogYPbPr

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.

Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Video Input Connector [1..4] InputSourceType

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: camera Other connectors: PC

Value space: Connector 1: camera Other connectors: PC/camera/document_camera/mediaplayer/whiteboard/other

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.

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

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

Other: Use this when the other options do not match.

Video Input Connector [1..4] Name

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 50)

Name for the video input connector.

Video Input Connector [2..4] Quality

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

Requires user role: ADMIN, INTEGRATOR

Default value: Sharpness

Value space: Motion/Sharpness

Motion: Gives the highest possible frame rate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Input Connector [1..4] OptimalDefinition Profile

This setting will only take effect if the corresponding Video Input Connector [n] Quality setting is set to Motion.

The optimal definition profile reflects the lighting conditions in the video conferencing room and the quality of the camera. The better lighting conditions and the better quality of the camera, the higher the profile. Generally, the Normal or Medium profiles are recommended. However, when the lighting conditions are very good, the High profile can be set in order to increase the resolution for a given call rate. The resolution must be supported by both the calling and called systems.

Use the Video Input Connector [n] OptimalDefinition Threshold60fps setting to set the lowest resolution where 60 fps is allowed. Below this threshold 30 fps is the manxiumum frame rate.

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 [1..4] OptimalDefinition Threshold60fps

For each video input, this setting tells the system the lowest resolution where it can transmit 60 fps. So for all resolutions lower than this, the maximum transmitted frame rate would be 30 fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Requires user role: ADMIN

Default value: 1280_720

Value space: 512_288/768_448/1024_576/1280_720/1920_1080/Never

512_288: Set the threshold to 512x288.

768_448: Set the threshold to 768x448.

1024_576: Set the threshold to 1024x576.

1280_720: Set the threshold to 1280x720.

1920_1080: Set the threshold to 1920x1080.

Never: Do not set a threshold for transmitting 60fps.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Input Connector [2..4] PresentationSelection

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: OnConnect

Value space: AutoShare/Desktop/Manual/OnConnect

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

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

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

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

Video Input Connector [2..4] RGBQuantizationRange

The devices connected to the video input should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any source.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 2: Full Connector 3, 4: Auto

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on video format according to CEA-861-E. CE video formats will use limited quantization range levels. IT video formats will use full quantization range levels.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Input Connector [1..4] Visibility

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

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

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Never Connector 2: Always Connector 3, 4: IfSignal

Value space: Connector 1: Never Connector 2, 3, 4: Always/IfSignal/Never

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: Yhe menu selection for the video input connector will only be visible when something is connected to the video input.

Never: The input source is not expected to be used as a presentation source, and will not show up on the user interface.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Monitors

Define the monitor layout mode to reflect the number of different layouts you want in your room setup. Note that the second monitor can be reserved for presentations.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/DualPresentationOnly

Auto: If a second monitor is connected, the layout is distributed on two monitors. Otherwise, everything is displayed on the main monitor.

DualPresentationOnly: All participants in the call are shown on the main monitor. If a presentation is part of the layout, the presentation is shown on the second monitor.

Video Output Connector [1] Brightness

Define the brightness level for the video system's integrated display.

Requires user role: ADMIN, USER

Default value: 80

Value space: Integer (0..100)

Range: The value must be between 0 and 100.

Video Output Connector [2] CEC Mode

This video output (HDMI) supports Consumer Electronics Control (CEC). When this setting is On, the system will use CEC to set the monitor in standby when the system itself enters standby. Likewise the system will wake up the monitor when the system itself wakes up from standby. For this to happen, the monitor that is connected to the output must be CEC compatible and CEC must be configured on the monitor.

Note that the different manufacturers uses different marketing names for CEC, for example Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: CEC is disabled.

On: CEC is enabled.

Video Output Connector [2] Location HorizontalOffset

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs. The integrated display has HorizontalOffset = 0 and VerticalOffset = 0 (implicit, not configurable).

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have two displays side by side, one in center and one to the left. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display.

Example: You have two displays, one in center and one below. Then the following settings will apply: VerticalOffset = 0 for the center display, Vertical Offset = -1 for the lower display.

The default values for the different outputs are:

Video Output Connector [2] Location: HorizontalOffset = 1, VerticalOffset = 0

Requires user role: ADMIN, INTEGRATOR

Default value: 1

Value space: Integer (-100..100)

Range: The value must be between -100 and 100.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Output Connector [2] Location VerticalOffset

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs. The integrated display has HorizontalOffset = 0 and VerticalOffset = 0 (implicit, not configurable).

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have two displays side by side, one in center and one to the left. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display.

Example: You have two displays, one in center and one below. Then the following settings will apply: VerticalOffset = 0 for the center display, Vertical Offset = -1 for the lower display.

The default values for the different outputs are:

Video Output Connector [2] Location: HorizontalOffset = 1, VerticalOffset = 0

Requires user role: ADMIN, INTEGRATOR

Default value: 0

Value space: Integer (-100..100)

Range: The value must be between -100 and 100.

Video Output Connector [2] OverscanLevel

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

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

Requires user role: ADMIN

Default value: None

Value space: None/Medium/High

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

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

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

Video Output Connector [1..2] Resolution

Connector 1: The resolution and refresh rate for the integrated display. This value is fixed and cannot be changed.

Connector 2: Define the resolution and refresh rate for the monitor that is connected to the video system's HDMI output.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Connector 1: 1920_1080_60; Connector 2: Auto

Value space: Connector 1: 1920_1080_60 Connector 2: Auto/1024_768_60/1280_1024_60/1280_720_50/1280_720_60/1920_1080_50/1920_1080_60/1280_768_60/1360_768_60/1366_768_60

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

1280_720_50: The resolution is 1280 x 720, and the refresh rate is 50 Hz.

1280_720_60: The resolution is 1280 x 720, and the refresh rate is 60 Hz.

1920_1080_50: The resolution is 1920 x 1080, and the refresh rate is 50 Hz.

1920_1080_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Output Connector [2] RGBQuantizationRange

Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any display. Most HDMI displays expects full quantization range.

Requires user role: ADMIN, INTEGRATOR

Default value: Full

Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe. If no AVI infoframe is available, RGB quantization range is selected based on video format according to CEA-861-E.

Full: Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

Limited: Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

Video Output Connector [1] Whitebalance Level

The integrated display's color temperature (white balance) is adjustable from 4000 K (warm) to 9000 K (cool).

Requires user role: ADMIN, USER

Default value: 6500

Value space: Integer (4000..9000)

The color temperature in Kelvin.

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 3rd party user interfaces. It is not relevant when using the user interfaces provided by Cisco.

Requires user role: ADMIN, USER

Default value: 2

Value space: 2

The video input source to use as default presentation source.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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 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 OnMonitorRole

Define which monitor/output to display the main video source (self-view) on after a call.

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: First/Second/Current

First: The self-view picture will be shown on the main screen.

Second: The self-view picture will be shown on the secondary screen.

Current: When leaving a call, the self-view picture will be kept on the same screen as it was during the call.

Video Selfview Default PIPPosition

Define the position on screen of the small self-view picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting) and fullscreen view is switched off (see the Video Selfview Default FullscreenMode setting).

Requires user role: ADMIN, INTEGRATOR

Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Current: The position of the self-view PiP will be kept unchanged when leaving a call.

UpperLeft: The self-view PiP will appear in the upper left corner of the screen.

UpperCenter: The self-view PiP will appear in the upper center position.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear in the center left position.

CentreRight: The self-view PiP will appear in the center right position.

LowerLeft: The self-view PiP will appear in the lower left corner of the screen.

LowerRight: The self-view PiP will appear in the lower right corner of the screen.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Video Selfview OnCall Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video Selfview OnCall Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Self-view is not shown automatically during call setup.

On: Self-view is shown automatically during call setup.

Video Selfview OnCall Duration

This setting only has an effect when the Video Selfview OnCall Mode setting is switched On. In this case, the number of seconds set here determines for how long self-view is shown before it is automatically switched off.

Requires user role: ADMIN, INTEGRATOR

Default value: 10

Value space: Integer (1..60)

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

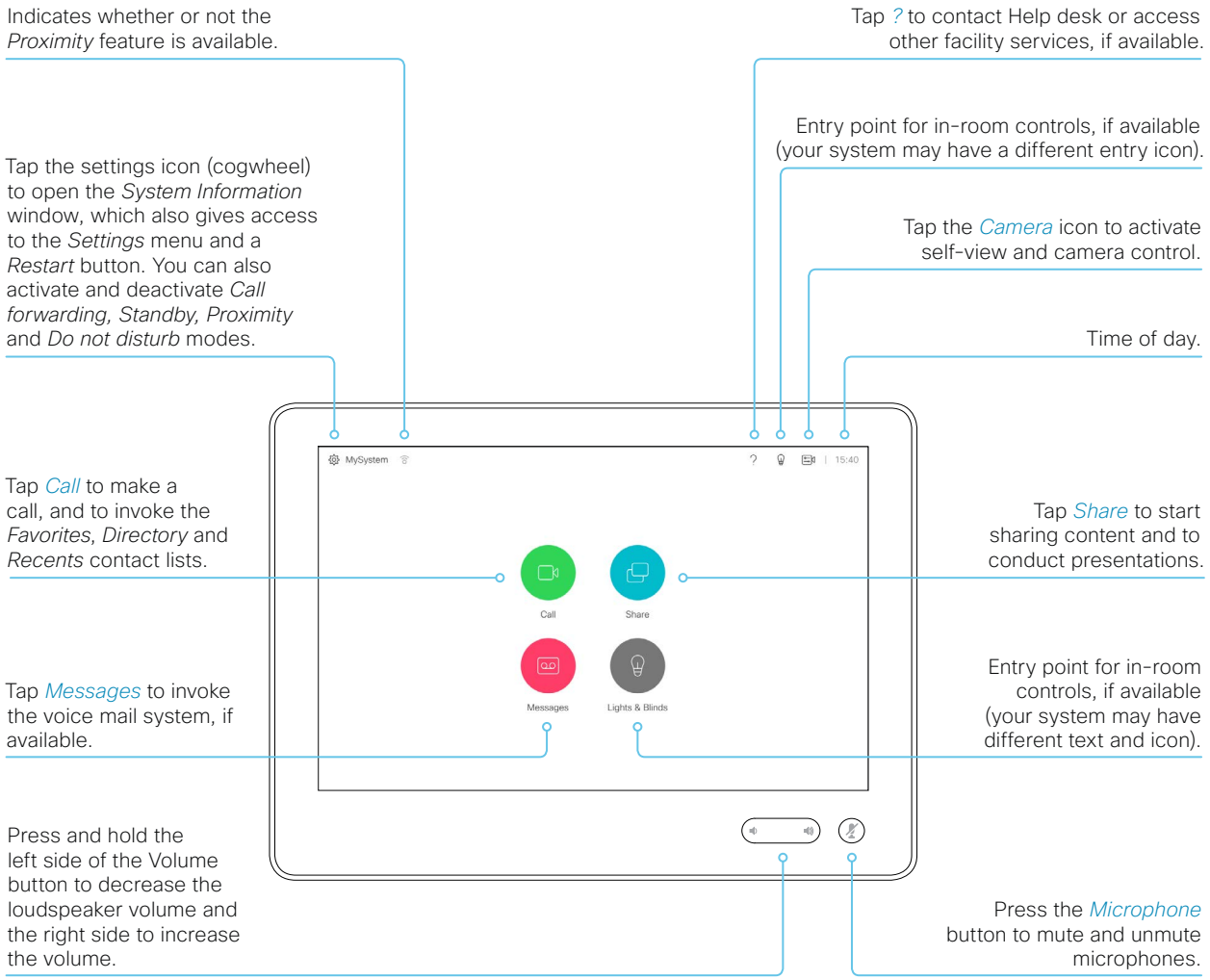
www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Appendices

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

How to use Touch 10

The Touch 10 user interface and its use are described in full detail in the User guide for the video system.



www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Set up remote monitoring

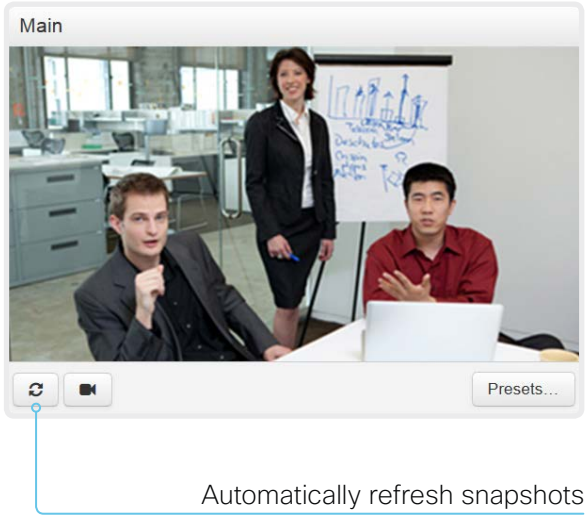
Requirement:

- *RemoteMonitoring* option

Remote monitoring is useful when you want to control the video system from another location.

Snapshots from input sources appear in the web interface, so you can check the camera view and control the camera without being in the room.

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



Check whether or not the video system has the *RemoteMonitoring* option

1. Sign in to the web interface.
2. Check the Home page to see if *RemoteMonitoring* is on the list of Installed options.

   If not on the list, remote monitoring is not available.

Enable remote monitoring

Install the *RemoteMonitoring* option key. How to install option keys are described in the ► Add option keys chapter.

PLEASE BE AWARE THAT IF YOU ENABLE THE REMOTE MONITORING OPTION YOU MUST MAKE SURE THAT YOU COMPLY WITH LOCAL LAWS AND REGULATIONS WITH REGARD TO PRIVACY AND PROVIDE ADEQUATE NOTICE TO USERS OF THE SYSTEM THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS YOUR RESPONSIBILITY TO COMPLY WITH PRIVACY REGULATIONS WHEN USING THE SYSTEM AND CISCO DISCLAIMS ALL LIABILITY FOR ANY UNLAWFUL USE OF THIS FEATURE.

About snapshots

Local input sources

Snapshots of the local input sources of the video system appear on the Call Control page.

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

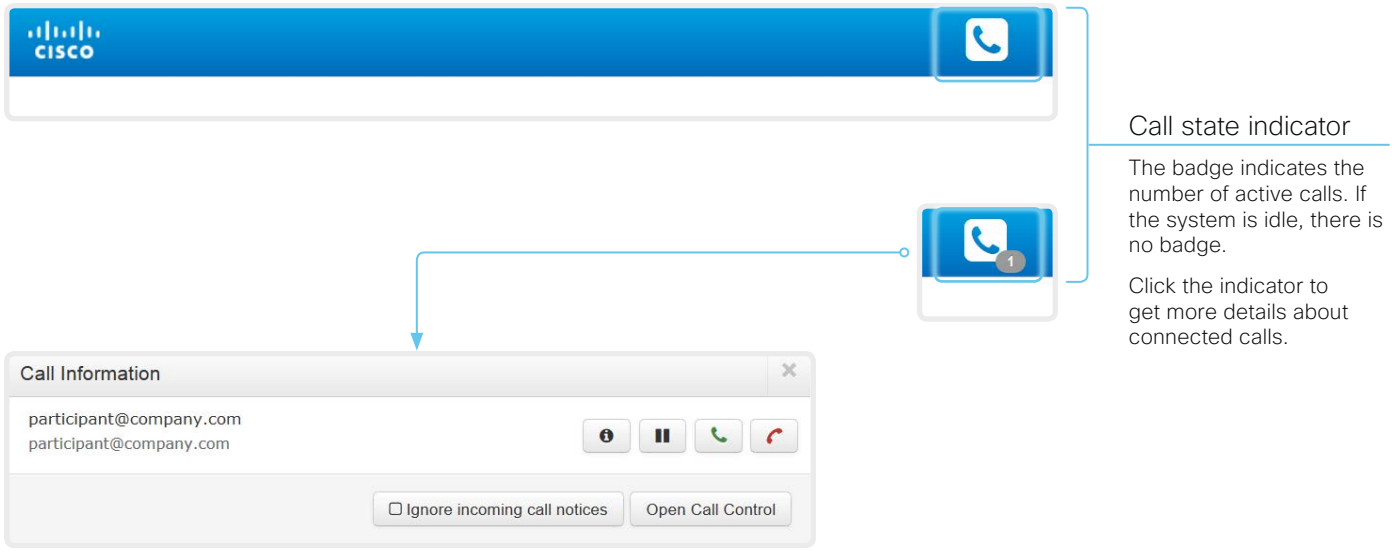
Far end snapshots

When in call, you may also see snapshots from the far end camera. It does not matter whether or not the far end video system has the *RemoteMonitoring* option.

Far end snapshots are not displayed if the call is encrypted.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Access call information while using the web interface



Call state indicator

The badge indicates the number of active calls. If the system is idle, there is no badge.

Click the indicator to get more details about connected calls.

Open the Call Information window

Click the *Call state indicator* to open the *Call Information* window manually.

As default, the *Call Information* window pops up automatically when the video system receives a call.

Switch incoming call notifications on or off

Click *Ignore incoming call notices*, to decide whether or not the *Call Information* window should pop up automatically when the video system receives a call.

When the check box is checked, the *Call Information* window will not open automatically.

Open the Call Control page

Click *Open Call Control* to go straight to the *Call Control* page.

Control the call(s)

Relevant control buttons appear in the *Call Information* window. Use the buttons to:

- Show call details
- Put the call on hold
- Answer the call
- Disconnect the call

About the call state indicator

The call state indicator shows whether the system is in a call or not, and how many calls it is engaged in. You may also be notified about incoming calls.

The call state indicator is available on all pages except the *Call Control* page.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Place a call using the web interface (page 1 of 2)

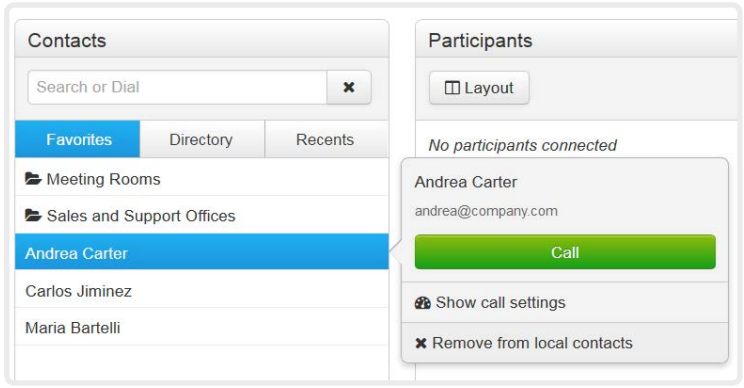
Sign in to the web interface and navigate to *Call Control*.

Place a call

Even if the web interface is used to initiate the call, it is the video system (display, microphones and loudspeakers) that is used for the call; it is not the PC running the web interface.

1. Navigate the *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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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 system 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.

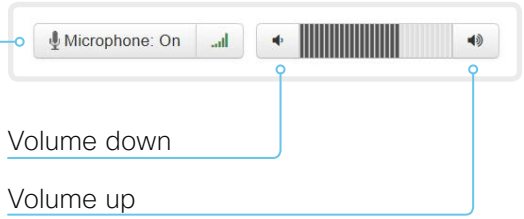
Calling more than one using a conference bridge (CUCM ad hoc conferencing) is not supported from the web interface, even if it is supported by the video system itself.

Adjust the volume

Mute the microphone

Click *Microphone: On* to mute the microphone. Then the text changes to *Microphone: Off*.

Click *Microphone: Off* to unmute.



www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Share content using the web interface

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

Share content

1. Choose which content source to share in the *Presentation* source drop down list.
2. Click *Start Presentation*. Then the text changes to *Stop Presentation*.

Stop content sharing:

Click the *Stop Presentation* button that is present while sharing.

Presentation source drop down list

Choose which input source to share, from the drop down list.

Snapshot area

Shows snapshots of the selected presentation source.

Only available on video systems that have the *Remote Monitoring* option.

About content sharing

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

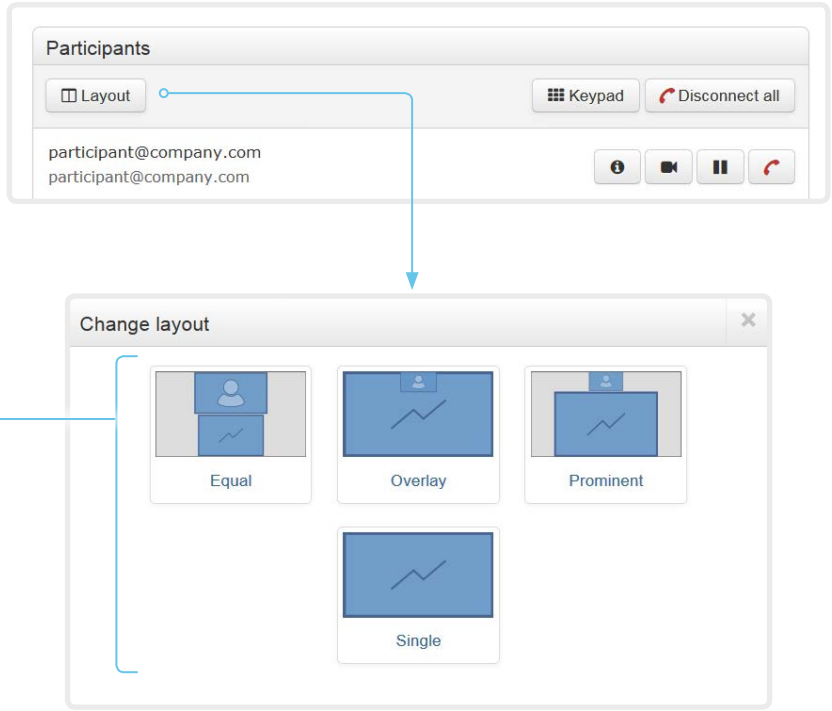
While in a call you can share content with the other participant(s) in the call (far end).

If you are not in a call, the content is shared locally.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Local layout control

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



Change the layout

Click *Layout*, and choose your preferred layout in the window that opens.

The set of layouts to choose from depends on the system configuration.

You may change the layout both when idle and in a call.

About layouts

The term layout is used to describe the various ways presentations and videos can appear on the screens. Different types of meetings may require different layouts.

The number of call or conference participants are reflected in the available choices.

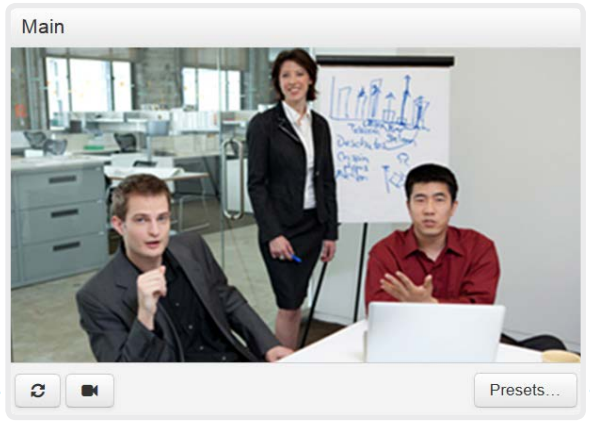
www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Control a local camera

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

Prerequisites

- The *Video > Input > Connector n > CameraControl > Mode* setting is switched **On** .
- The camera has pan, tilt or zoom functionality.
- Speaker tracking is switched Off.

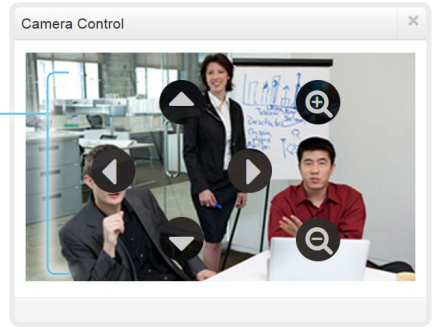


Snapshot area

Shows snapshots of the main input source.

Only available on video systems that have the *Remote Monitoring* option.

Automatically refresh snapshots



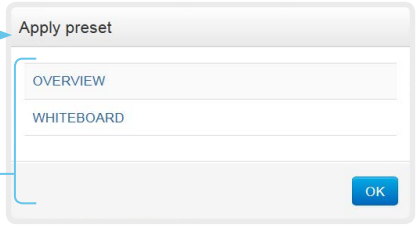
Move the camera using the pan/tilt/zoom controls

1. Click the camera icon to open the camera control window.

   Video snapshots from the room are only displayed for video systems that have the *Remote Monitoring* option.

2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.

   Only relevant controls appear in the window.



Move the camera to a preset position

1. Click *Presets...* to open a list of available presets.

   If no presets are defined, the button is disabled and named *No presets*.

2. Click a preset's name to move the camera to the preset position.

3. Click *OK* to close the window.

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

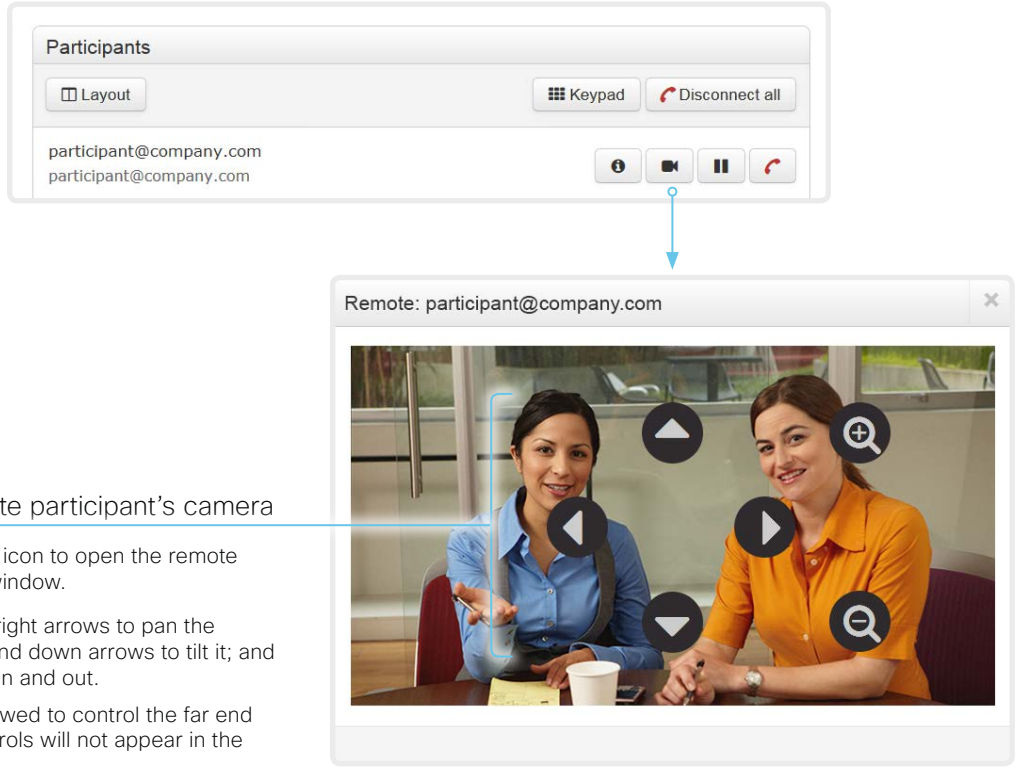
Control a far end camera

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

Prerequisites

While in a call, you can control the remote participant's camera (far end) provided that:

- The *Conference > FarEndControl > Mode* setting is switched **On** on the far end video system.
- The far end camera has pan, tilt or zoom functionality. Only the relevant controls will appear.
- Speaker tracking is not switched On on the far end camera.
- The local video system has the *Remote Monitoring* option.



Control the remote participant's camera

1. Click the camera icon to open the remote camera control window.
2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and – to zoom in and out.

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Room analytics

The room analytics feature use several variables from the conference room and re-uses them to analyze the room utilization over time or per call.

People presence detection

The video system 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 on/off the people presence detection from the web interface. Sign in to the web interface, and navigate to *Setup > Configuration > RoomAnalytics > PeoplePresenceDetector*.

Status

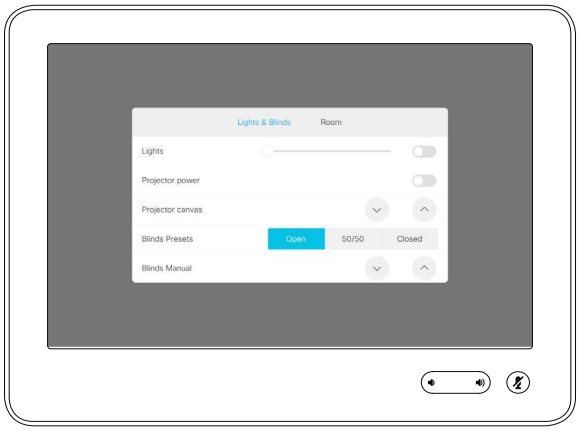
You may see the status at a given moment of people's presence. Sign in to the web interface, and navigate to *Setup > Status > RoomAnalytics*.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Add in-room controls to Touch 10

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

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



Example in-room control panel on Touch 10

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

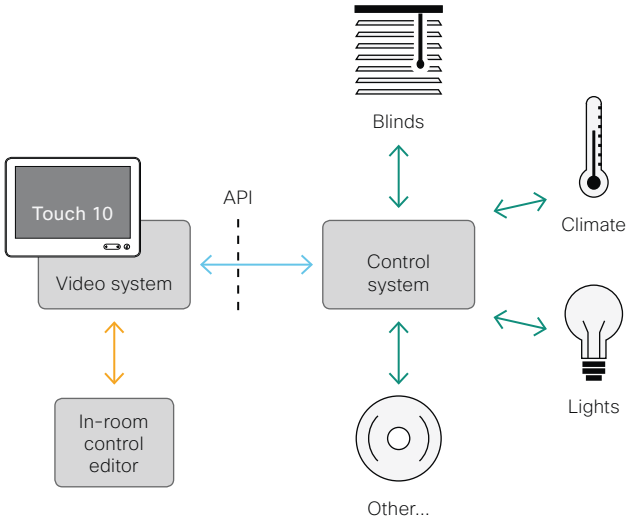
► http://www.cisco.com/go/in-room-control-docs

Architecture

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

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

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



In-room control schematics

The In-Room Control editor

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

Sign in* to the web interface, and navigate to *Integration > In-Room Control*.

- Click *Launch Editor* to launch the editor directly from the video system's web interface.

  You can push a new in-room control panel to the video system, and see the result immediately on the Touch controller.
- Click *Download Editor* to download a stand-alone version that you can use to work offline.

The room simulator

You can use the room simulator to visualise how the in-room controls on Touch 10 changes the state of the room.

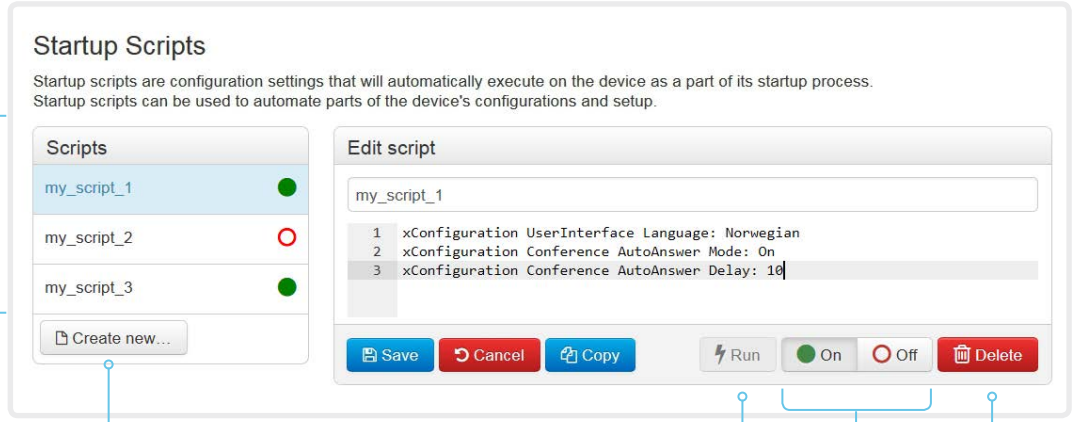
- Click *Launch Simulator* to open a room simulator in your browser.
- The room simulator contains a predefined in-room control configuration that you can push to the video system. Then you can control the virtual meeting room from your real Touch 10 user interface.

* 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.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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.

Creat 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 video system starts up.

Delete a startup script

1. Select the startup script from the list.
2. Click *Delete*.

About startup scripts

A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure.

A few commands and configurations cannot be placed in a startup script, for example `xCommand SystemUnit Boot`. It is not possible to save a script that contains illegal commands and configurations.

Syntax and semantics for xCommand and xConfiguration are explained in the API guide for the product.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Access the video system's XML files

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

The XML files are part of the video system's API. They structure information about the system in a hierarchy.

- *Configuration.xml* contains the current system settings (configuration). These settings are controlled from the web interface or from the API (Application Programmer Interface).
- The information in *status.xml* is constantly updated by the video system to reflect system and process changes. The status information is monitored from the web interface or from the API.
- *Command.xml* contains an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- *Valuespace.xml* contains an overview of all the value spaces of system settings, status information, and commands.

Open an XML file

Click the file name to open the XML file.

About the API

The application programming interface (API) is a tool for integration professionals and developers working with the video system. The API is described in detail in the API guide for the video system.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

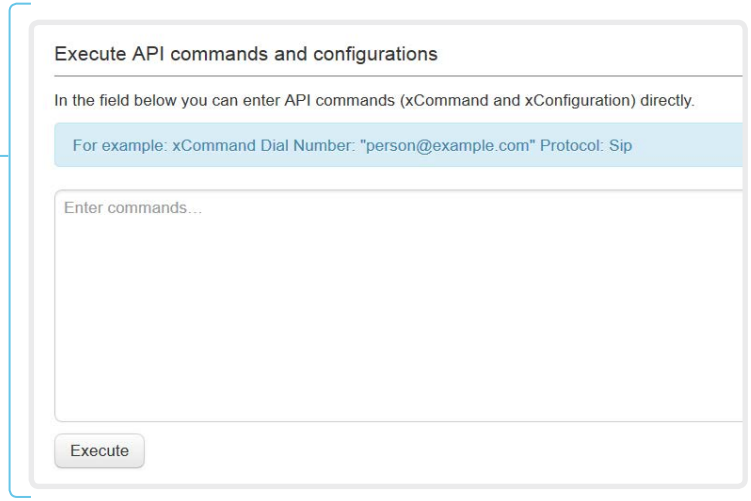
Execute API commands and configurations from the web interface

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

Commands (xCommand) and configurations (xConfiguration) can be executed from the web interface. Syntax and semantics are explained in the API guide for the video system.

Execute API commands and configurations

1. Enter a command (xCommand or xConfiguration), or a sequence of commands, in the text area.
2. Click *Execute* to issue the command(s).



About the API

The application programming interface (API) is a tool for integration professionals and developers working with the video system. The API is described in detail in the API guide for the video system.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Serial interface

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

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

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

Parameters:

- Baud rate: 115200 bps
- Data bits: 8
- Parity: None
- Stop bit: 1
- Hardware flow control: Off

Video system settings

Serial communication is enabled by default. Use the following configuration to change the behavior:

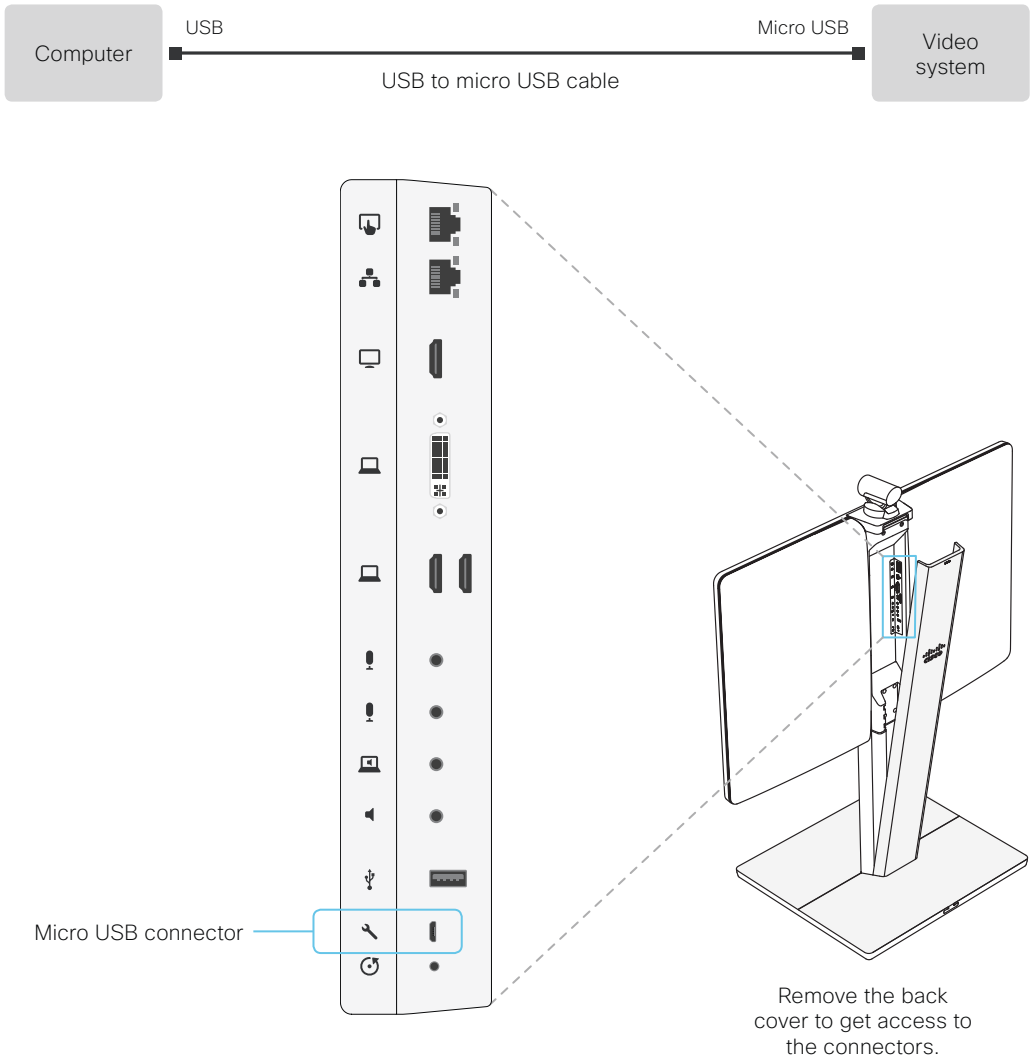
SerialPort > Mode

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

SerialPort > LoginRequired

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

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



www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

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 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 4051: Remote pairing session connection

The port is only available (and open) when a Touch panel is remote paired with the video system. You can close the port by setting remote pairing for the Touch panel to **Off**.

```
Peripherals Pairing CiscoTouchPanels RemotePairing: Off/On
```

TCP 4052: Remote pairing and forwarding

The port is only available (and open) when a Touch panel is remote paired with the video system. 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 pors 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 system settings are configured from the *Setup > Configuration* page on the web interface. Open a web browser and enter the IP address of the video system then sign in.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Technical specification (page 1 of 4)

PRODUCT SPECIFICATION

PRODUCT COMPATIBILITY

Fully compatible with standards-compliant telepresence and video systems

SOFTWARE COMPATIBILITY

MX200 G2:

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

MX300 G2:

- Cisco TelePresence Software Version TC7.0 or later
- Collaboration Endpoint Software Version 8.0 or later

COMPONENTS

Fully integrated unit including:

- Codec
- Display
- Camera
- Integrated microphone and loudspeakers

Cisco TelePresence Table Microphone 20
(as default, two microphones are shipped with the MX300 G2, and one with the MX200 G2)

Cables: DVI-I-to-VGA cable, mini jack (3.5 mm) audio cable, LAN cable, and power cable

DISPLAY

MX200 G2:

- 42 inch TFT-LCD monitor, edge LED backlight
- Resolution: 1920 × 1080 (16:9)
- Contrast ratio: Typically 1300:1
- Viewing angle: ±178°
- Response time: Typical 8 ms
- Brightness: Typical 450 cd/m^2

MX300 G2:

- 55 inch TFT-LCD monitor, edge LED backlight
- Resolution: 1920 × 1080 (16:9)
- Contrast ratio: Typically 4000:1
- Viewing angle: ±178°
- Response time: Typical 8 ms
- Brightness: Typical 450 cd/m^2

PC AND SECOND-SOURCE VIDEO INPUT

DVI-I

2 × HDMI

SUPPORTED PC INPUT RESOLUTIONS

SVGA (800 x 600) to 1080p (1920 x 1080)

CAMERA OVERVIEW

MX200 G2:

- 2.5x optical zoom (5x including digital zoom)
- Motorized +5°/-25° tilt, ±30° pan
- 83° horizontal field of view
- 51.5° vertical field of view
- Resolutions: 1080p60 and 720p60
- F 2.0
- Automatic or manual focus, brightness and white balance
- Far-end camera control
- Focus distance: 0.98 ft (0.3 m) to infinity

MX300 G2:

- 4x optical zoom (8x including digital zoom)
- Motorized +15°/-25° tilt, ±90° pan
- 72° horizontal field of view
- 43.5° vertical field of view
- Resolutions: 1080p60 and 720p60
- F 1.7
- Automatic or manual focus, brightness and white balance
- Far-end camera control
- Focus distance: 0.98 ft (0.3 m) to infinity

AUDIO SYSTEM

- Integrated full-range microphone
- Support for two Cisco TelePresence Table Microphone 20
- Mini jack audio input (e.g. for PC)
- Mini jack audio output

MX200 G2:

- Mono 2-way loudspeaker
- 1 closed box full range loudspeaker
- 1 closed box bass loudspeaker
- 40 W amplifier system
- Individual digital processing for each speaker
- Frequency response 100-20000 Hz, ±3 dB
- Frequency response 73-22000 Hz, -10 dB
- Max continuous sound pressure 90 dB @ 1 m

MX300 G2:

- Mono 2-way loudspeaker
- 1 closed box full range loudspeaker
- 1 balanced dual driver bass loudspeaker
- 40 W amplifier system
- Individual digital processing for each speaker
- Frequency response 90-20000 Hz, ±3 dB
- Frequency response 65-22000 Hz, -10 dB
- Max continuous sound pressure 90 dB @ 1 m

USER INTERFACE

Cisco TelePresence Touch 10

- Ten inch projected capacitive touch screen
- Resolution: 1280 x 800

LANGUAGE SUPPORT

(depends on software version)

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

POWER

- Autosensing power supply
- 100–240 VAC, 50–60 Hz
- Power consumption under normal operating conditions as defined in IEC 60950-1:
  - MX200 G2: 130 W
  - MX300 G2: 235 W

TEMPERATURE RANGE

Operating temperature and humidity:

- Ambient temperature: 32 to 95°F (0 to 35°C)
- Relative humidity (RH): 10 to 90%
- Storage and transport temperature at RH 10–90% (noncondensing): -4 to 140°F (-20 to 60°C)

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Technical specification (page 2 of 4)

PHYSICAL DIMENSIONS

MX200 with floor stand:
Height: 1397 mm / 55 in.
Width: 995 mm / 39.2 in.
Depth: 602 mm / 23.7 in.
Weight: 37 kg / 109 lb

MX200 with table stand:
Height: 781 mm / 30.7 in.
Width: 995 mm / 39.2 in.
Depth: 259 mm / 10.2 in.
Weight: 26 kg / 57 lb

MX200 with wall mount:
Height: 671 mm / 26.4 in.
Width: 995 mm / 39.2 in.
Depth: 146 mm / 5.7 in.
Weight: 26 kg / 57 lb

MX200 with wheel base:
Height: 1480 mm / 58.3 in.
Width: 995 mm / 39.2 in.
Depth: 711 mm / 28.0 in.
Weight: 34 kg / 73 lb

MX300 with floor stand:
Height: 1521 mm / 59.9 in.
Width: 1278 mm / 50.4 in.
Depth: 671 mm / 26.5 in.
Weight: 53 kg / 117 lb

MX300 with wall mount:
Height: 948 mm / 37.4 in.
Width: 1278 mm / 50.4 in.
Depth: 200 mm / 7.9 in.
Weight: 40 kg / 88 lb

MX300 with wheel base:
Height: 1606 mm / 63.3 in.
Width: 1278 mm / 50.4 in.
Depth: 755 mm / 29.8 in.
Weight: 47 kg / 104 lb

APPROVALS AND COMPLIANCE

- Directive 2014/35/EU (Low-Voltage Directive)
- Directive 2014/30/EU (EMC Directive) – Class A
- Directive 2011/65/EU (RoHS)
- Directive 2002/96/EC (WEEE)

- NRTL approved (Product Safety)
- FCC CFR 47 Part 15B (EMC) – Class A

Please check Product Approval Status Database www.ciscofax.com for approval documents per country.

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Technical specification (page 3 of 4)

VIDEO AND AUDIO SPECIFICATIONS

BANDWIDTH

- H.323 and SIP up to 6 Mbps point-to-point

MINIMUM BANDWIDTH FOR RESOLUTION AND FRAME RATE

- 720p30 from 768 kbps
- 720p60 from 1152 kbps
- 1080p30 from 1472 kbps
- 1080p60 from 2560 kbps

VIDEO STANDARDS

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

VIDEO FEATURES

- Widescreen: 16:9
- Advanced screen layouts
- Intelligent video management
- Local auto-layout

VIDEO INPUTS (THREE INPUTS)

Two HDMI** and one DVI-I (analog and digital) input

Support formats up to maximum 1920 × 1080@60fps (HD1080p60), including:

- 640 × 480
- 720 × 480
- 720 × 576
- 800 × 600
- 848 × 480
- 1024 × 768
- 1152 × 864
- 1280 × 720
- 1280 × 768
- 1280 × 800
- 1280 × 960
- 1280 × 1024
- 1360 × 768
- 1366 × 768
- 1400 × 1050
- 1440 × 900
- 1680 × 1050
- 1920 × 1080

Extended Display Identification Data (EDID)

HDCP is not supported

VIDEO OUTPUT (ONE OUTPUT)

One HDMI output**

Supports formats up to maximum 1920 × 1080@60fps (1080p60), including:

- 1280 × 720 (720p)
- 1280 × 768 (WXGA)
- 1360 × 768 (WXGA)
- 1366 × 768 (WXGA)
- 1920 × 1080 (1080p)

VESA Monitor Power Management

Extended Display Identification Data (EDID)

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

Supports encode/decode video formats up to maximum 1920 × 1080@60fps (HD1080p60), including:

- 176 × 144 @ 30fps (QCIF) (decode only)
- 352 × 288 @ 30fps (CIF)
- 512 × 288 @ 30fps (w288p)
- 576 × 448 @ 30fps (448p)
- 640 × 480 @ 30fps (VGA)
- 704 × 576 @ 30fps (4CIF)
- 768 × 448 @ 30fps (w448p)
- 800 × 600 @ 30fps (SVGA)
- 1024 × 576 @ 30fps (w576p)
- 1024 × 768 @ 30fps (XGA)
- 1280 × 720 @ 30fps (720p30)
- 1280 × 768 @ 30fps (WXGA)
- 1280 × 1024 @ 30fps (SXGA)
- 1440 × 900 @ 30fps (WXGA+)*
- 1600 × 1200 @ 30fps (UXGA)*
- 1680 × 1050 @ 30fps (WSXGA+)*
- 1920 × 1080 @ 30fps (1080p30)*
- 512 × 288 @ 60fps (w288p60)*
- 768 × 448 @ 60fps (w448p60)*
- 1024 × 576 @ 60fps (w576p60)*
- 1280 × 720 @ 60fps (720p60)*
- 1920 × 1080 @ 60fps (HD1080p60)*

AUDIO FEATURES

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

AUDIO STANDARDS

- 64 and 128 kbps AAC-LD
- G.722
- G.722.1
- G.711
- G.728
- G.729AB

DUAL STREAM

- H.239 (H.323) dual stream
- Binary Floor Control Protocol (BFCP) dual stream (SIP)
- Support for resolutions up to 1080p (1920 × 1080)

MULTIPOINT SUPPORT

- Four-way embedded SIP/H.323 multipoint support, ref. MultiSite
- Cisco Ad-Hoc Conferencing (requires Cisco Unified Communications Manager (CUCM), Cisco TelePresence Server and Conductor)

MULTISITE FEATURES (EMBEDDED MULTIPOINT)

- Adaptive SIP/H-323 MultiSite
- Three-way resolution up to 720p30
- Four-way resolution up to 576p30
- Full individual audio and video transcoding
- Individual layouts in multisite continuous presence
- H.323, SIP and Voice over IP (VoIP) in the same conference
- Support for presentation (H.239 and BFCP) from any participant at resolutions up to 1080p30/SXGA
- Best Impression (automatic continuous presence layouts)
- H.264, encryption and dual stream from any site
- IP downspeeding
- Dial in and dial out
- Conference rates up to 6 Mbps

* Requires premium resolution option

** HDMI version 1.3

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Technical specification (page 4 of 4)

NETWORK, SECURITY AND MANAGEMENT SPECIFICATIONS

PROTOCOLS
- H.323 and SIP (dual call stack support)
- ISDN (requires Cisco TelePresence ISDN Link)

NETWORK INTERFACES
- One LAN or Ethernet (RJ-45) 10/100/1000 Mbps for LAN

OTHER INTERFACES
- Micro USB for maintenance

IP NETWORK FEATURES
- Domain Name System (DNS) lookup for service configuration
- Differentiated Services (quality of service (QoS))
- IP adaptive bandwidth management (including flow control)
- Auto-gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 dual-tone multifrequency (DTMF) tones in H.323
- Date and time support with Network Time Protocol (NTP)
- Packet loss based downspeeding
- DNS based URI dialing
- TCP/IP
- Dynamic Host Configuration Protocol (DHCP)
- IEEE 802.1x network authentication
- IEEE 802.1q VLAN
- IEEE 802.1p QoS and class of service
- Cisco ClearPath

IPV6 NETWORK SUPPORT
- Dual stack (IPv4 and IPv6) for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ
- Support for static IP address assignment, stateless autoconfiguration and DHCPv6

FIREWALL TRAVERSAL
- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal
- SIP ICE (Interactive Connectivity Establishment)

EMBEDDED ENCRYPTION
- H.323 and SIP point-to-point
- Standards-based: H.235v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Support in dual stream

SECURITY FEATURES
- Management through Secure HTTP (HTTPS) and Secure Shell (SSH) Protocol
- Password protected IP administration
- Password protected Administration menu
- Disable IP services
- Network settings protection

SUPPORTED INFRASTRUCTURE
- Cisco Unified Communications Manager 8.6.2 and newer
- Cisco TelePresence Video Communication Server (Cisco VCS)

SYSTEM MANAGEMENT
- Support for the Cisco TelePresence Management Suite (Cisco TMS)
- Total management through embedded Simple Network Management Protocol (SNMP), Telnet, SSH, XML, and Simple Object Access Protocol (SOAP)
- Remote software upload: Through web server, HTTP, and HTTPS

DIRECTORY SERVICES
- Support for local directories (Favorites)
- Corporate directory
- Unlimited entries using server directory supporting Lightweight Directory Access Protocol (LDAP) and H.350
- Unlimited number for corporate directory (available with Cisco TelePresence Management Suite)
- Local directory: 200 numbers
- Received calls with date and time
- Placed calls with date and time
- Missed calls with date and time

All specifications are subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

April 2017

Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

CE software supports a range of RFCs, including the following:

- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3263 Locating SIP Servers
- RFC 3361 DHCP Option for SIP Servers
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
- RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
- RFC 4582 The Binary Floor Control Protocol

  draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

User documentation on the Cisco web site

User documentation for the Cisco Collaboration products is available at ► http://www.cisco.com/go/telepresence/docs

Choose a product category in the right pane until you find the correct product. These are the paths you have to follow for the different product series:

Collaboration Room Endpoints >
Spark Room Series >
Spark Room Series

Collaboration Room Endpoints >
TelePresence MX Series >
TelePresence MX Series

Collaboration Room Endpoints >
TelePresence SX Series >
TelePresence SX Series

Collaboration Desk Endpoints >
DX Series >
DX Series

Alternatively, use the following short-links to find the documentation:

- ► http://www.cisco.com/go/roomkit-docs
- ► http://www.cisco.com/go/mx-docs
- ► http://www.cisco.com/go/sx-docs
- ► http://www.cisco.com/go/dx-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 system up and running
- *RCSI guide:* Regulatory compliance and safety information

Maintain and Operate > Maintain and Operate Guides

- *Getting started guide:* Initial configurations required to get the system up and running
- *Administrator guide:* Information required to administer your product
- *Deployment guide for TelePresence endpoints on CUCM:* Tasks to perform to start using the video system with the Cisco Unified Communications Manager (CUCM)
- *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 measurements

Configure > Configuration Guides

- *In-room control guide:* How to design an in-room control panel, and how to use the video system's API to program the in-room controls
- *CE Console user guide:* How to use the CE Console application, which provides a graphical interface to advanced customizable features of the video system

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*

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.

Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ► http://www.cisco.com/go/offices

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA

Intellectual property rights

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

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

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

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

Cisco product security overview

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

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

www.cisco.com – Copyright © 2017 Cisco Systems, Inc. All rights reserved.