Software version TC7.3
OCTOBER 2015

Administrator guide

for Cisco TelePresence MX200 G2 and MX300 G2

www.cisco.com – Copyright © 2013–2015 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 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/telepresence/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 5
- Software 5
- What's new in this version 6
- Cisco TelePresence MX200 G2 and MX300 G2 at a glance 7
- How to use Touch 10 10

Web interface **11**
- Accessing the web interface 12
- Changing the system password 13
- The interactive menu 14
- System information 15
- About snapshots and remote monitoring (TC7.3.3 and later) 16
- About snapshots and remote monitoring (TC7.3.0 to TC7.3.2) 17
- Placing a call 18
- Sharing content 19
- Controlling and monitoring a call 20
- Controlling your camera 21
- Local layout control 22
- Controlling the far end camera 23
- Accessing call information 24
- System configuration 25
- Changing system settings 26
- System status 27
- Managing the favorites list 28
- Favorite list folders 29
- Choosing a wallpaper 30
- Choosing a ringtone 31
- Peripherals overview 32
- User administration 33
- Adding a sign in banner 37
- Managing the video system's certificates 38
- Managing the list of trusted certificate authorities 39
- Managing pre-installed certificates for Edge provisioning 41
- Setting strong security mode 42
- Changing the persistency mode 43
- Deleting trust lists (CUCM only) 44
- Troubleshooting 45
- Downloading log files 46
- Starting extended logging 47
- Capturing user interface screenshots 48
- Upgrading the system software 49
- Adding option keys 50
- Backup and restore 51
- Reverting to the previously used software version 52
- Factory reset 53
- Remote support user 54
- Restarting the system 55

System settings **56**
- Overview of the system settings 57
- Audio settings 60
- Cameras settings 61
- Conference settings 63
- FacilityService settings 68
- H323 settings 69
- Logging settings 72
- Network settings 73
- NetworkServices settings 80
- Peripherals settings 85
- Phonebook settings 86
- Provisioning settings 87
- RTP settings 89
- Security settings 90
- SerialPort settings 92
- SIP settings 93
- Standby settings 97
- SystemUnit settings 98
- Time settings 99
- UserInterface settings 102
- Video settings 104
- Experimental settings 113

Setting passwords **114**
- Setting the system password 115

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Appendices....116
Connecting the Touch 10 user interface....117
Cisco VCS provisioning....120
Optimal definition profiles....121
Packet loss resilience - ClearPath....122
Factory resetting the video system....123
Factory resetting the Touch 10 user interface....124
Technical specification....125
Supported RFCs....128
User documentation on the Cisco web site....129

Cisco contacts....130

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Chapter 1

Introduction

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

This document provides you with the information required to administrate your product at an advanced level.

How to install the product and the initial configurations required are described in the Installation guide and Getting started guide, respectively.

Products covered in this guide

- Cisco TelePresence MX200 G2
- Cisco TelePresence MX300 G2

Note that the first generation of MX series products (MX300 and MX200) are covered in a separate guide.

User documentation

The user documentation for the Cisco TelePresence systems running the TC software includes several guides suitable for various user groups.

- **Installation guides:**
  How to install the products
- **Getting started guide:**
  Initial configurations required to get the system up and running
- **Administering TC Endpoints on CUCM:**
  Tasks to perform to start using the product with the Cisco Unified Communications Manager (CUCM)
- **Administrator guide (this guide):**
  Information required to administer your product
- **Quick reference guides:**
  How to use the product
- **User guides:**
  How to use the product
- **Knowledge base articles**
- **Video conferencing room primer:**
  General guidelines for room design and best practice
- **Video conference room acoustics guidelines:**
  Things to do to improve the perceived audio quality
- **Software release notes**
- **Regulatory compliance and safety information guide**
- **Legal & license information**

Downloading the user documentation

We recommend you visit the Cisco web site regularly for updated versions of the user documentation. Go to:

http://www.cisco.com/go/telepresence/docs

Guidelines how to find the documentation on the Cisco web site are included in the User documentation on the Cisco web site appendix.

Software

You can download the software for your product from the Cisco web site. Go to:

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

We recommend reading the Software Release Notes (TC7), go to:

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

What's new in this version

This section provides an overview of the new and changed system settings and new features in the TC7.3 software version.

Software release notes

For a complete overview of new features and changes, we recommend reading the Software Release Notes (TC7). Go to:

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

Software download

For software download go to:
http://www.cisco.com/cisco/software/navigator.html

New features and improvements

Local preview of presentation in a call

This allows the user to preview the presentation locally before sharing it with far end. The feature has previously been available for EX systems, and is now available across the portfolio.

TC7.3.0-TC7.3.2: Users are notified when snapshots are taken

Both the on screen display and web interface have warnings when the snapshots feature is enabled. A notification pops up on the on screen display, when a snapshot is taken. On the web interface the administrator is warned that this notice will show up when the feature is enabled.

The system also logs when snapshots are taken, and which IP address the request was initiated from.

It is possible to allow and disallow snapshots remotely, but not to observe the room without the users being notified.

TC7.3.3 and later: Remote Monitoring option key

Due to security reasons, taking snapshots of local and far end video streams from the call control page on the system's web interface now requires an option key to be installed on the endpoint.

The remote monitoring option key can only be added to systems that are upgraded to TC7.3.3 and above. Remote monitoring is enabled once the option key is added, and the system rebooted. Once this feature is enabled, the only way to disable it is to remove the option key.

This feature does not display warning messages or indicators on the local system that someone is monitoring the room. Please provide adequate notice to users of the system that the system administrator may monitor and control the camera and screen.

System configuration changes

New configurations

Cameras Preset TriggerAutofocus

H323 Profile [1..1] Encryption KeySize

NetworkServices CDP Mode

NetworkServices UPnP Mode *(TC7.3.4)*

NetworkServices UPnP Timeout *(TC7.3.4)*

Configurations that are removed

H323 Profile [1..1] Encryption MinKeySize

Video AllowWebSnapshots *(TC7.3.3)*

Configurations that are modified

FacilityService Service [1..5] Name
- OLD: <S: 0, 255>
- NEW: <S: 0, 1024>

FacilityService Service [1..5] Number
- OLD: <S: 0, 255>
- NEW: <S: 0, 1024>

Phonebook Server [1..1] Type
- OLD: <VCS/TMS/Callway/CUCM>
- NEW: <VCS/TMS/CUCM>

Provisioning Mode
- OLD: <Off/TMS/VCS/CallWay/CUCM/Auto/Edge>
- NEW: <Off/TMS/VCS/CUCM/Auto/Edge>

Video AllowWebSnapshots *(removed in TC7.3.3)*
- OLD: <Off/On>, default Off
- NEW: <Off/On/LocalDeviceOnly>, default LocalDeviceOnly

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Cisco TelePresence MX200 G2 and MX300 G2 at a glance

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

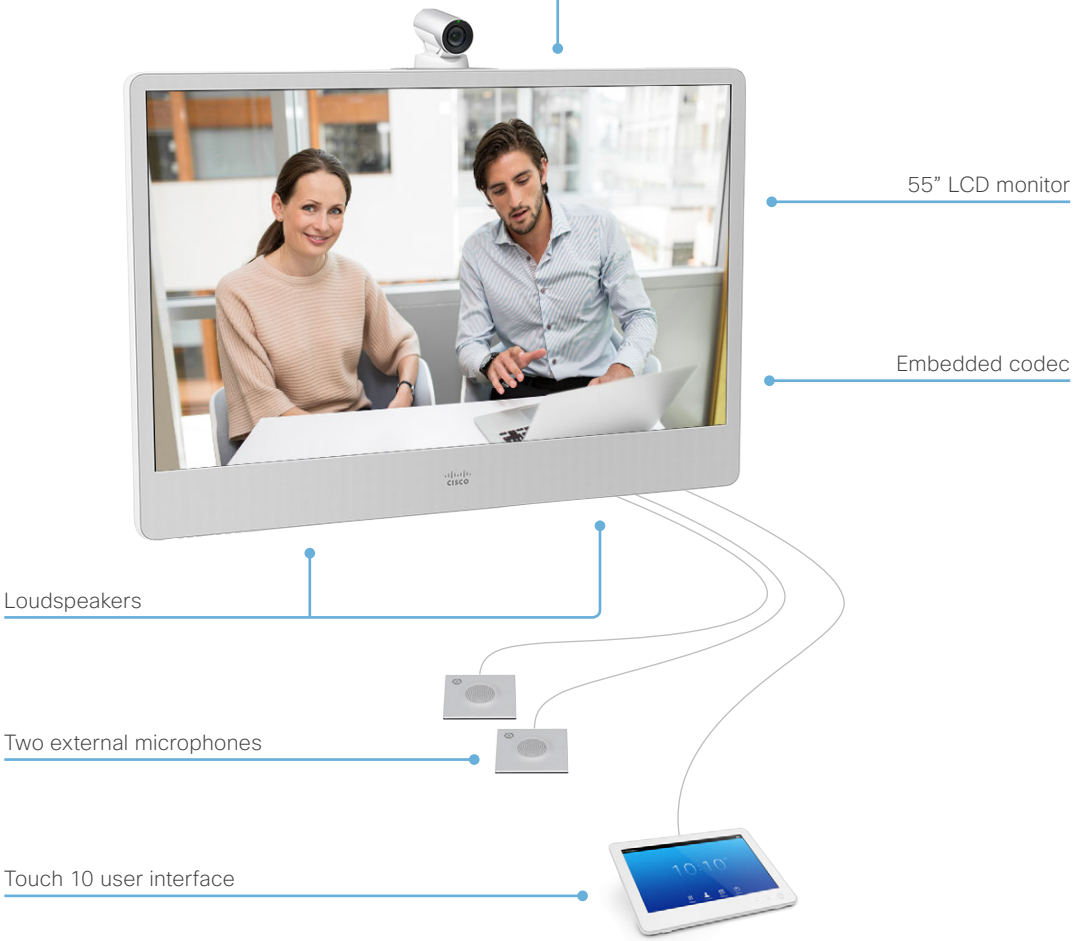
- Easy to install – one piece plus floor stand, wheel base, or wall mount brackets (VESA mount).
- Self-configuring with Cisco Unified Communications Manager (UCM), Cisco TelePresence Video Communication Server (VCS), or Cisco WebEx TelePresence provisioning. You need to authenticate your endpoint to the network.
- MX200 G2: Cisco TelePresence PrecisionHD camera with pan, tilt, and 5x zoom.

  MX300 G2: Cisco TelePresence PrecisionHD camera with pan, tilt, and 8x zoom.
- MX200 G2: High-quality 42 inch LCD display with 1920×1080 resolution (1080p60) and 16:9 aspect ratio.

  MX300 G2: High-quality 55 inch LCD display with 1920×1080 resolution (1080p60) and 16:9 aspect ratio.
- Two front speakers that provide 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.
- The systems take advantage of the Cisco TelePresence Total Solution approach, including Cisco TelePresence Multiway features, recording and streaming, and firewall traversal services.
- Natively supported by Cisco UCM version 8.6.2 and later.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

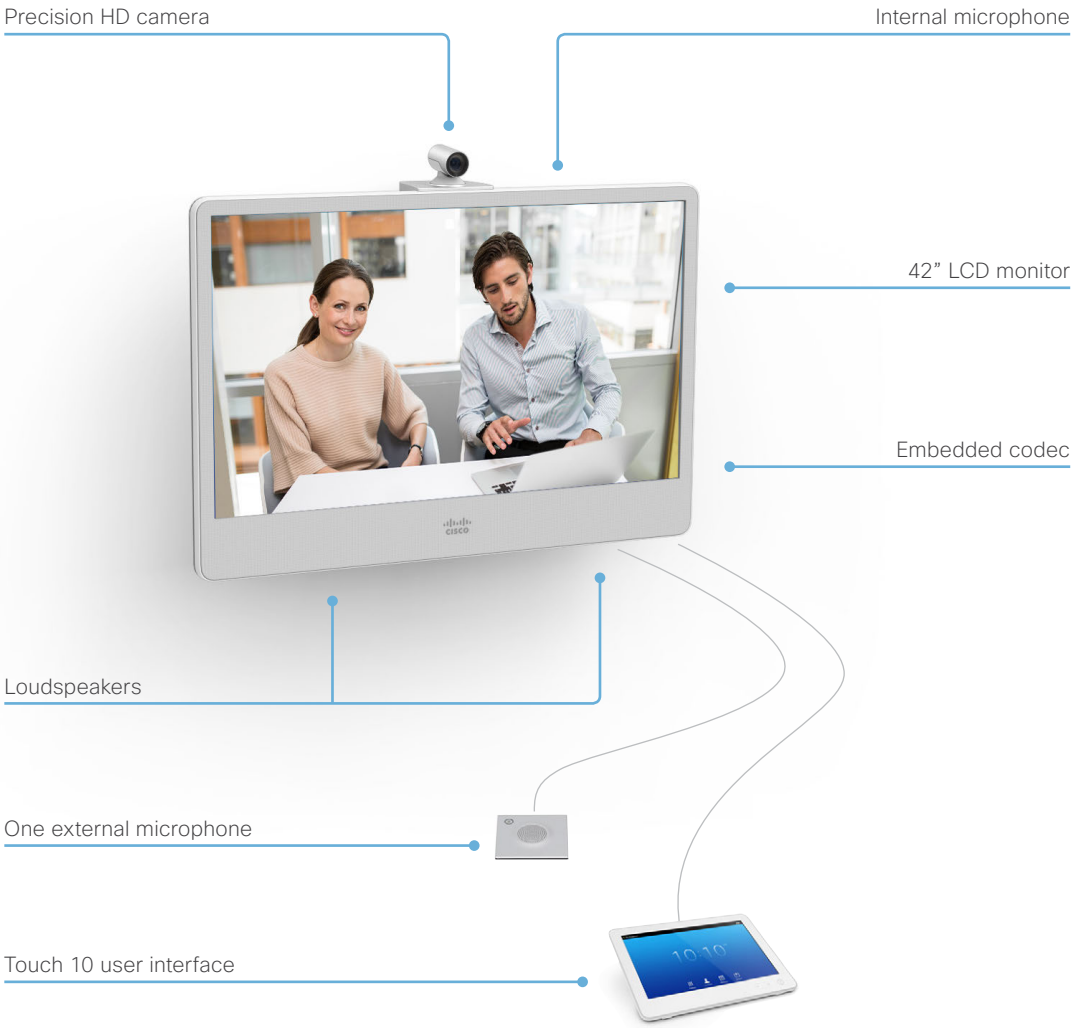
Cisco TelePresence MX300 G2



Mounting options
(floor stand, wheel base, wall mount)

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Cisco TelePresence MX200 G2



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

www.cisco.com – Copyright © 2013–2015 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 your video system.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Chapter 2

Web interface

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Accessing the web interface

The web interface provides full configuration access to your video conference system.

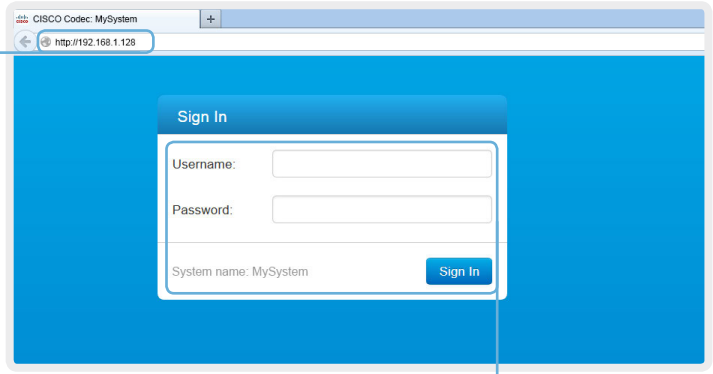
You can connect from a computer and administer the system remotely.

In this chapter you will find information how to use the web interface for system configuration and maintenance.

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

1. 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

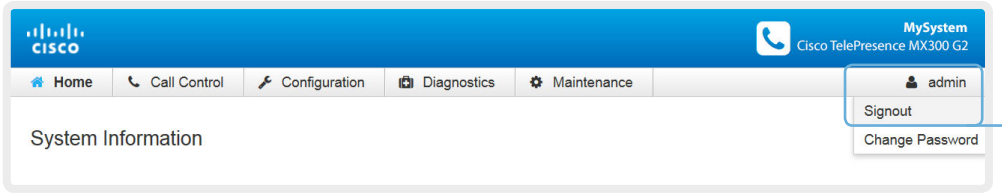
Touch controller: Tap the contact information in the upper left corner of the Touch controller and open the *Settings* menu. Then tap *System Information*.

2. Sign in

Enter the user name and password for your video system and click *Sign In*.

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

It is mandatory to set a password for the *admin* user, see the next page.



Signing out

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

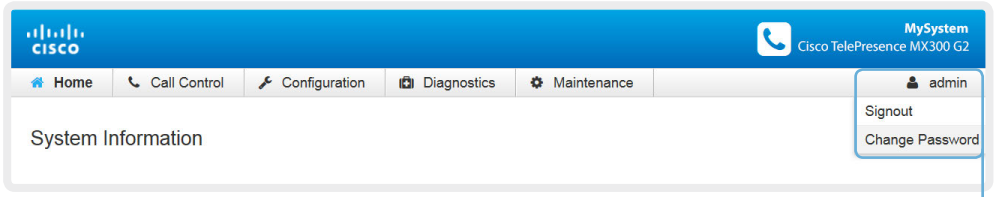
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Changing the system password

It is mandatory to set a password for a user with ADMIN rights in order to restrict access to system configuration. This includes the default *admin* user.

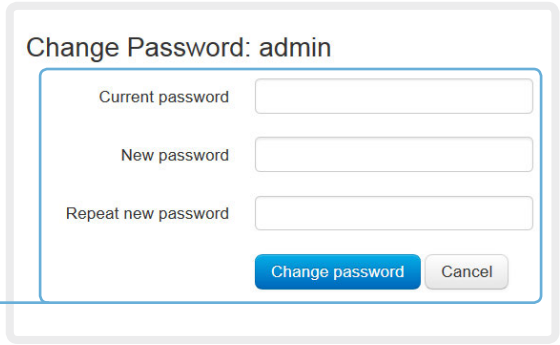
A warning, saying that the system password is not set, is shown on screen until you set a password.

You can read more about passwords in the Setting passwords chapter.



1. Open the Change Password dialog

Hover the mouse over your the name, and choose *Change password* in the drop-down list.



2. Set the new password

Enter your current and new passwords as requested, and click *Change password* for the change to take effect.

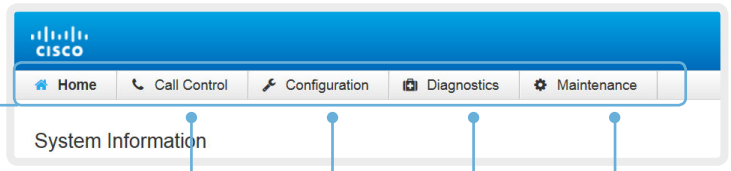
If the password currently is not set, leave the *Current password* field blank.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

The interactive menu

The web interface provides access to tasks and configurations. They are available from the main menu, which appears near the top of the page when you have signed in.

When you hover the mouse over an item in the main menu, you can navigate to its related sub-pages.



Main menu

Hover the mouse over a main menu item in order to see the titles of the related sub-pages.

Click a sub-page's title to open it. Click the main menu item itself if there are no sub-pages. Only pages that the user has access rights for are shown*.

Click *Home* to return to the System Information page.

Sub-pages

Call Control

Configuration
System Configuration
System Status
Local Contacts Management
Personalization
Peripherals
User Administration
Sign In Banner
Startup Scripts
API
Security

Diagnostics
Troubleshooting
Call History
Log Files
User Interface Screenshots

Maintenance
Software Upgrade
Option Keys
Backup and Restore
System Recovery
Restart

* You can read more about user administration, user roles and access rights in the User administration section.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

System information

The video system's Home page shows an overview of the basic set-up and status of the system*.

This includes information like system name and product type, which software version the system runs, its IP address, etc. Also the 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.

Navigate to: Home

* The system information shown in the illustration serve as an example. Your system may be different.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

About snapshots and remote monitoring (TC7.3.3 and later)

Snapshots of local input sources

If the *Remote Monitoring option key* is installed on the video system, snapshots of the video system's input sources are displayed on the Call Control page.

Snapshots are displayed both when the video system is idle, and when in a call.

This feature may be used when administering the video system from a remote location, for example to check the camera view and control the camera.

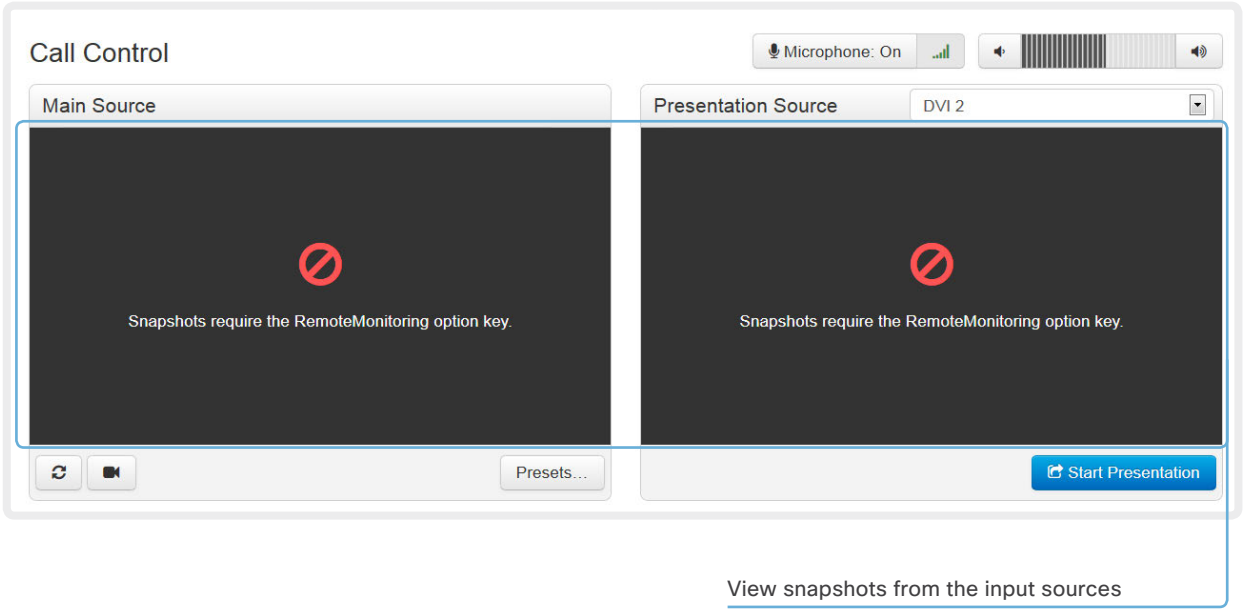
Far end snapshots

If the *Remote Monitoring option key* is installed on the video system, far end snapshots may also be captured. Whether or not the Remote Monitoring option key is installed on the far end video system, does not make any difference.

Far end snapshots are prohibited during encrypted calls.

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.

Navigate to: Call Control



View snapshots from the input sources

Install the Remote Monitoring option key in order to view snapshots from the selected main source or presentation source in this area.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

About snapshots and remote monitoring (TC7.3.0 to TC7.3.2)

Snapshots of local input sources

If the *snapshot feature* is enabled on the video system, snapshots of the video system's input sources are displayed on the Call Control page.

Snapshots are displayed both when the video system is idle, and when in a call.

This feature may be used when administering the video system from a remote location, for example to check the camera view and control the camera.

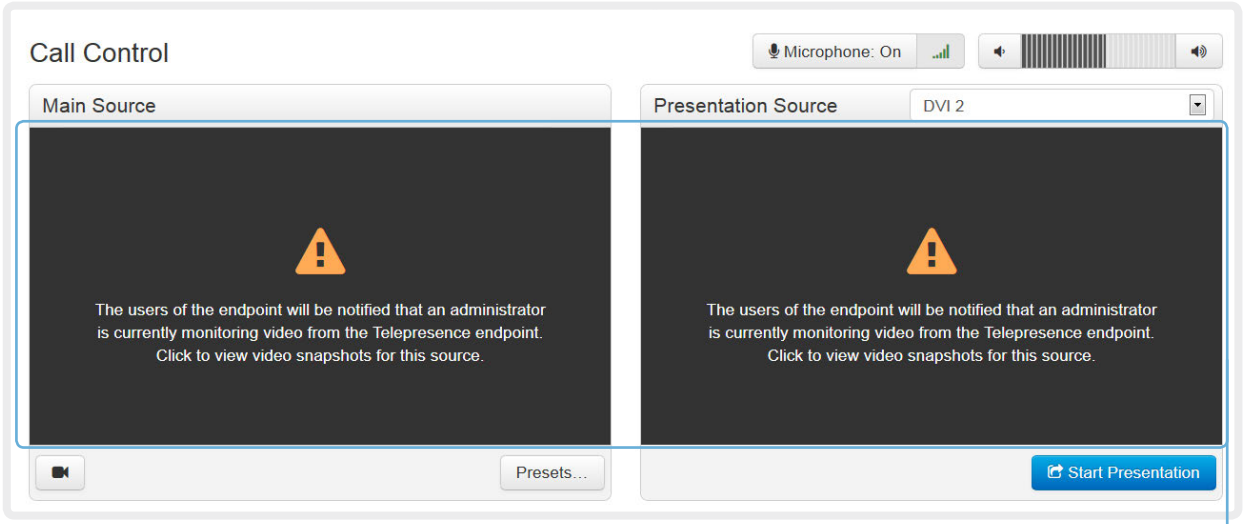
The users of the video system are notified when the snapshot feature is in use. A notification saying that the administrator is visually monitoring the room is displayed on the main display of the video system.

Far end snapshots

If the *snapshot feature* is enabled on the video system, far end snapshots may also be captured. Whether or not the snapshot feature is enabled on the far end video system, does not make any difference.

Far end snapshots are prohibited during encrypted calls.

Navigate to: Call Control



Enable the snapshot feature

By default, the snapshot feature is disabled.

Enable the feature using the web interface.

- Go to the *Configuration* tab and select *System Configuration*
- Navigate to *Video > AllowWebSnapshots* and choose **On**.
- Click *Save* for the change to take effect.

View snapshots from the input sources

Click in this area to view snapshots from the selected main source or presentation source.

Snapshots of the main or presentation source are displayed for approximately 10 seconds.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Placing a call

You can use the Call Control page to place a 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.

Calling

You can call someone either by choosing a contact name in the *Local, Directory* or *Recents* lists, or by typing a complete URI or number in the *Search or Dial* field. Then click *Call* in the associated contact card.

Searching the contact lists

Enter one or more characters in the *Search or Dial* field. Matching entries from the *Local, Directory* and *Recents* lists will be listed as you type.

Select the correct entry in the list and click *Call*.

Calling more than one

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

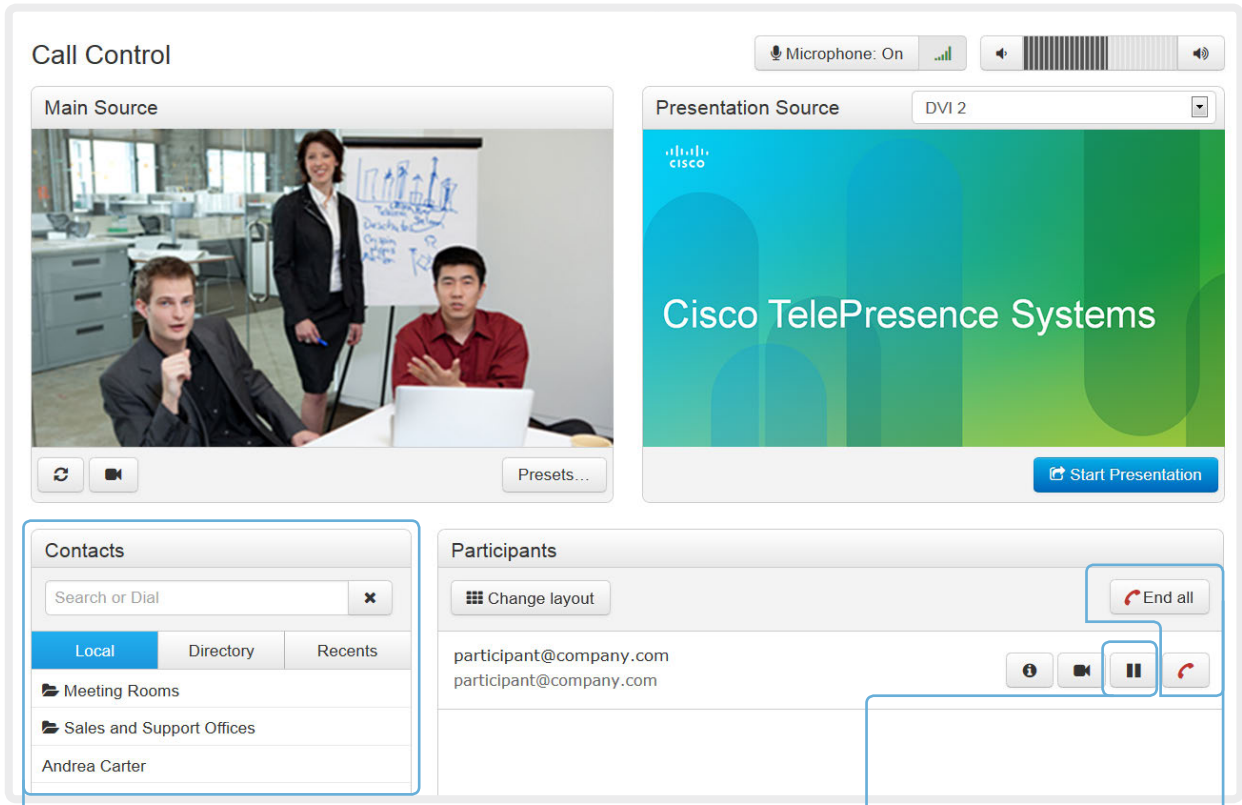
If your system is using the optional built-in MultiSite feature, up to four participants, yourself included, can join the video call (conference).

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 or MultiWay) is not supported from the web interface, even if it is supported by the video system itself.

Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

Navigate to: Call Control



Calling someone

Click a contact name, either in the *Local, Directory* or *Recents* lists. Then 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.

Holding and resuming

Use the ⏸ button next to the participant's name to put him on hold.

To resume the call, use the ▶ button that is present when a participant is on hold.

Ending a call

If you want to terminate a call or conference, click *End 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 © 2013–2015 Cisco Systems, Inc. All rights reserved.

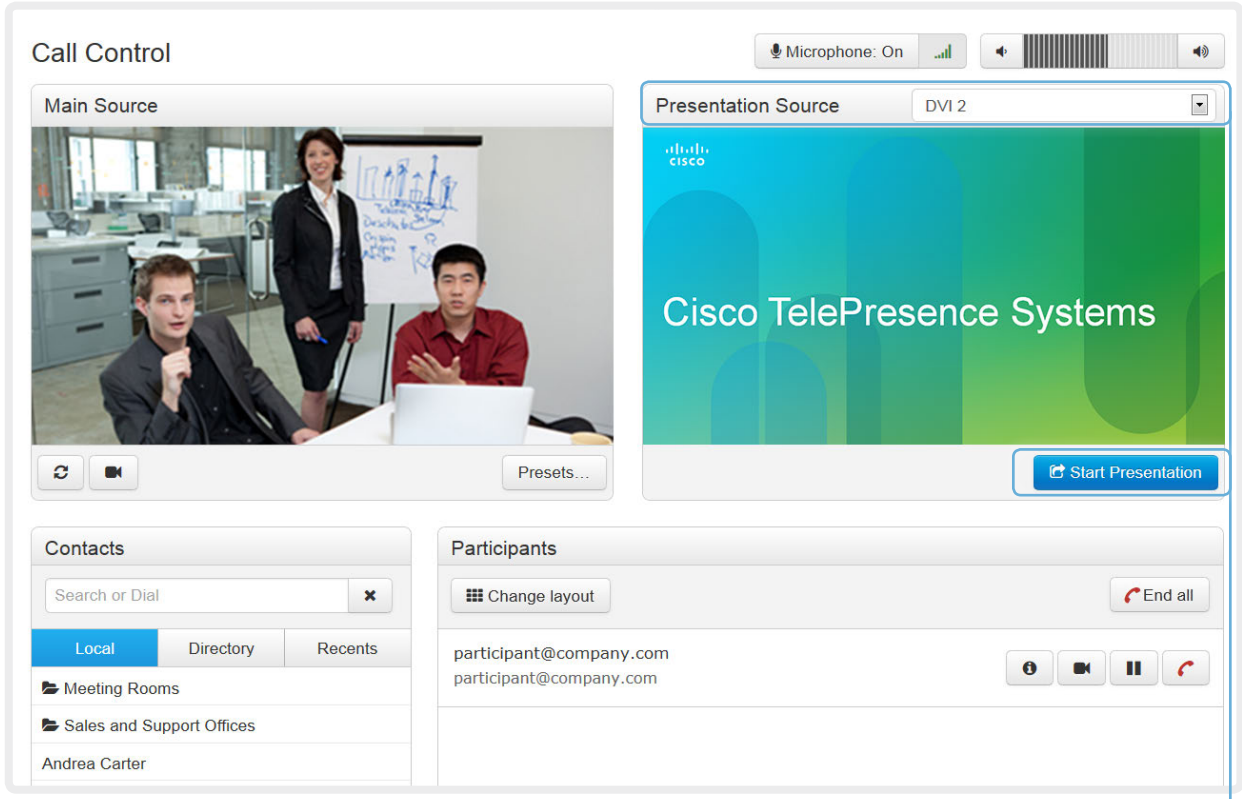
Sharing content

You can connect a presentation source to one of the external 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 on your display.

Navigate to: Call Control



Sharing content

1. Choose a Presentation source from the drop-down list.
2. Click *Start Presentation*.

Stop content sharing:

Click the *Stop Presentation* button that is present while sharing.

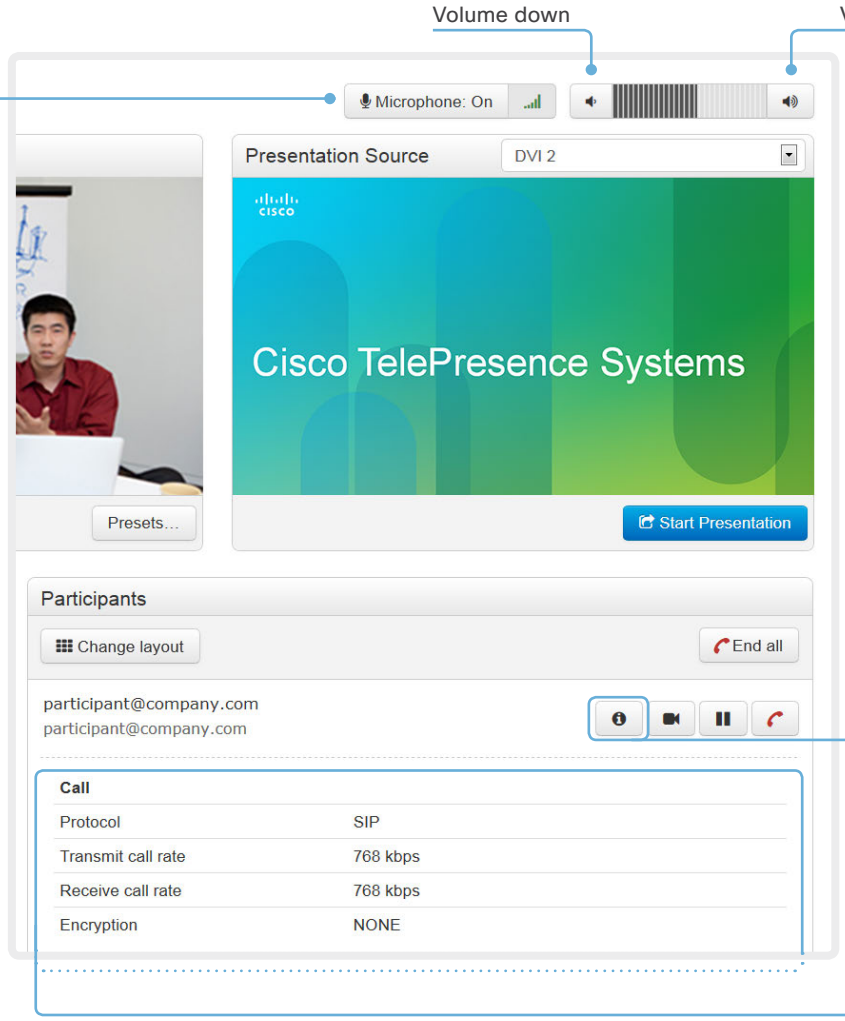
Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Controlling and monitoring a call

You can control and monitor several call features using the Call Control page.

Navigate to: Call Control



Microphone mute

Click the button to mute the microphone. Then the text changes to *Microphone: Off*.

Click again to unmute.

Show/hide call details

Click the information button to show details about the call.

Click the button again to hide the information.

Call details

If necessary, scroll your browser to see all call details.

Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Controlling your camera

For software version TC7.3.3 and later:

You can control the camera of the video system (pan, tilt, zoom) from the Call Control page. Only available camera controls will appear.

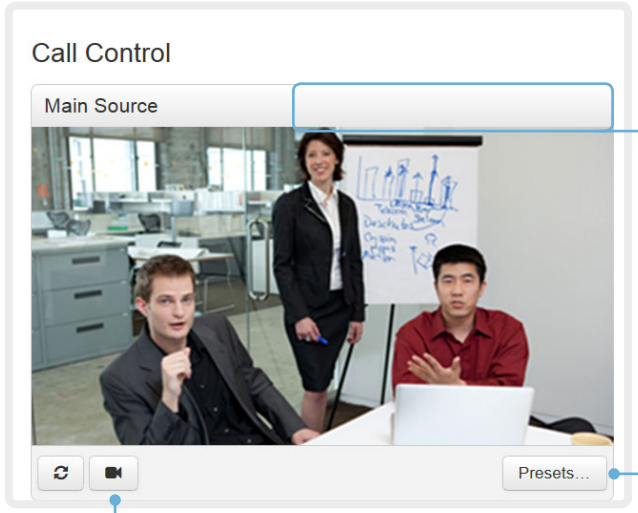
For software version TC7.3.0 to TC7.3.2:

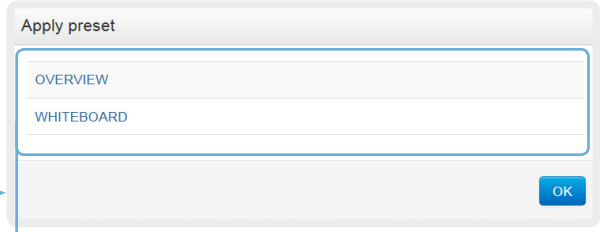
You can control the camera of the video system (pan, tilt, zoom) from the Call Control page provided that the *Video AllowWebSnapshots* setting is switched **On**. Only available camera controls will appear.

If snapshots from the camera are shown on the web interface, a notification will be sent to the users of the video system (shown on the main display) that an administrator is monitoring their video.

Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

Navigate to: Call Control





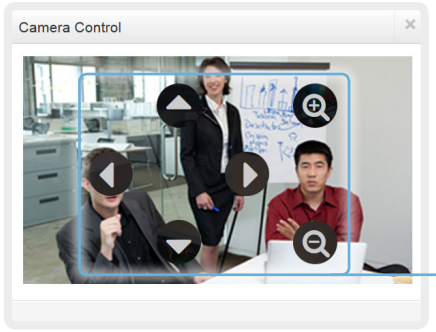
Camera presets

If one or more presets are defined, click *Presets...* to open a list of available presets.

Click a preset's name to move the camera(s) to the preset position.

Click *OK* to close the window.

You cannot use the web interface to define a preset; you should use the video system's Touch user interface.



Control the camera

1. Click the camera icon to open the 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.

For software versions TC7.3.0 to TC7.3.2, the cursor must be in the image to show the controls.

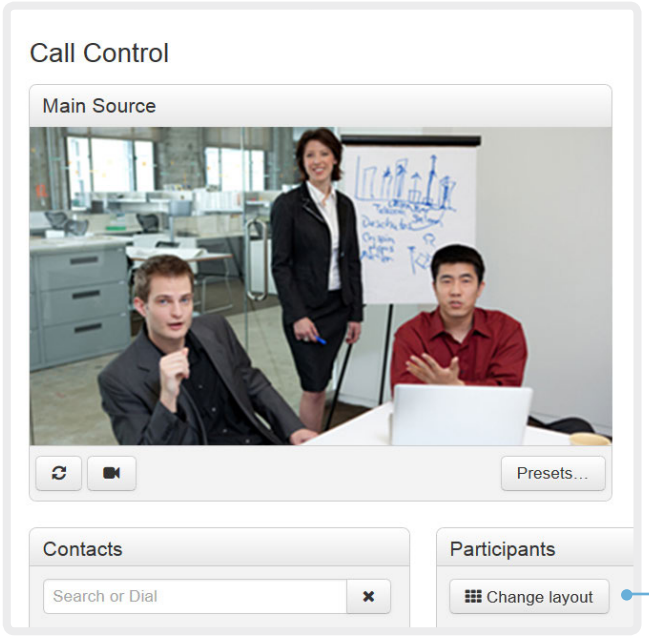
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Local layout control

You can choose a local layout using the Call Control page.

The term layout is used to describe the various ways the videos from the conference participants and a presentation can appear on the screen. Different types of meetings may require different layouts.

Navigate to: Call Control

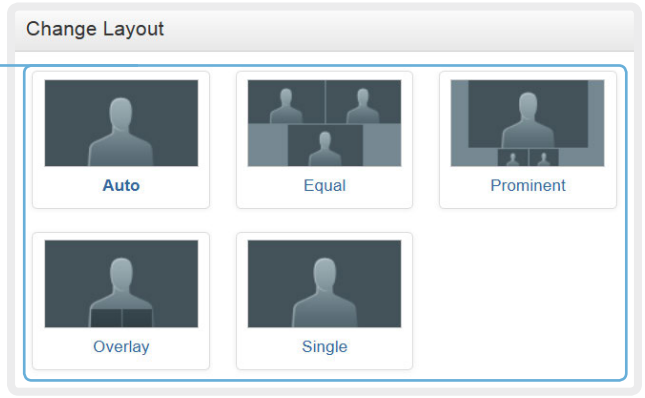


Change the layout

Click *Change layout*, and choose your preferred layout in the window that opens.

The set of layouts to choose from depends on the system configurations.

You may change the layout while in a call.



Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

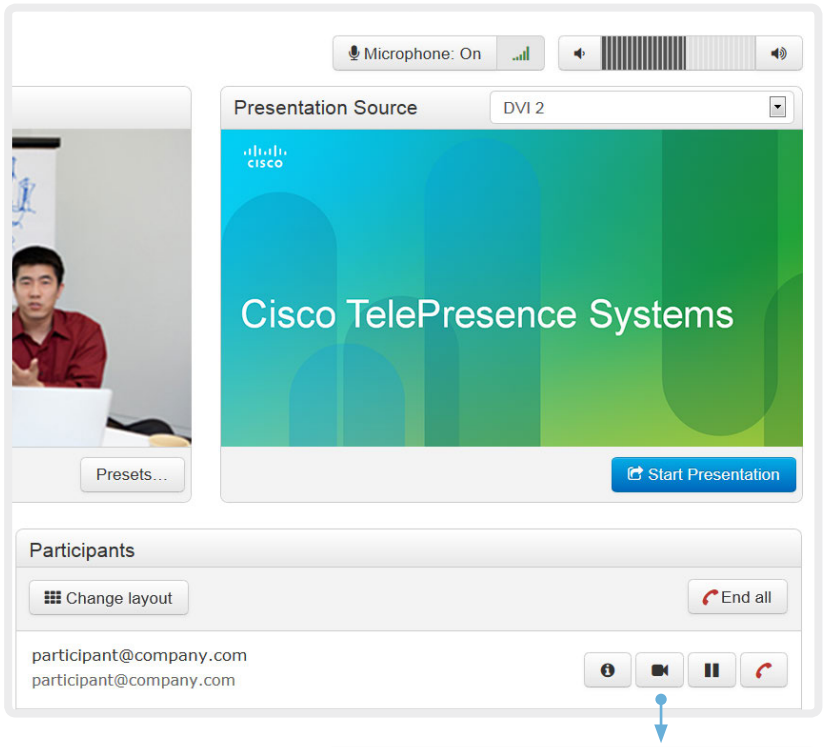
Controlling the far end camera

While in a call, you can control the remote participant's camera (far end) provided that:

- The Remote Monitoring option is installed on your video system (software version TC7.3.3 and later).
- The *Video AllowWebSnapshots* setting is switched **On** (software versions TC7.3.0 to TC7.3.2).
- Far end camera control (FECC) is enabled on the far end system. Only the available controls will appear.

Whether or not snapshots of input sources are shown as illustrated, depends on the software version, configuration, and options installed on the video system. Refer to the *About snapshots and remote monitoring* sections (TC7.3.3 or newer or TC7.3.0 to TC7.3.2).

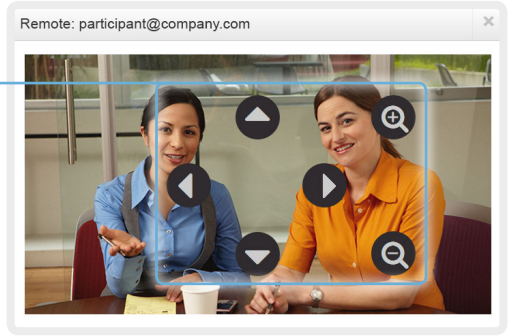
Navigate to: Call Control



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.

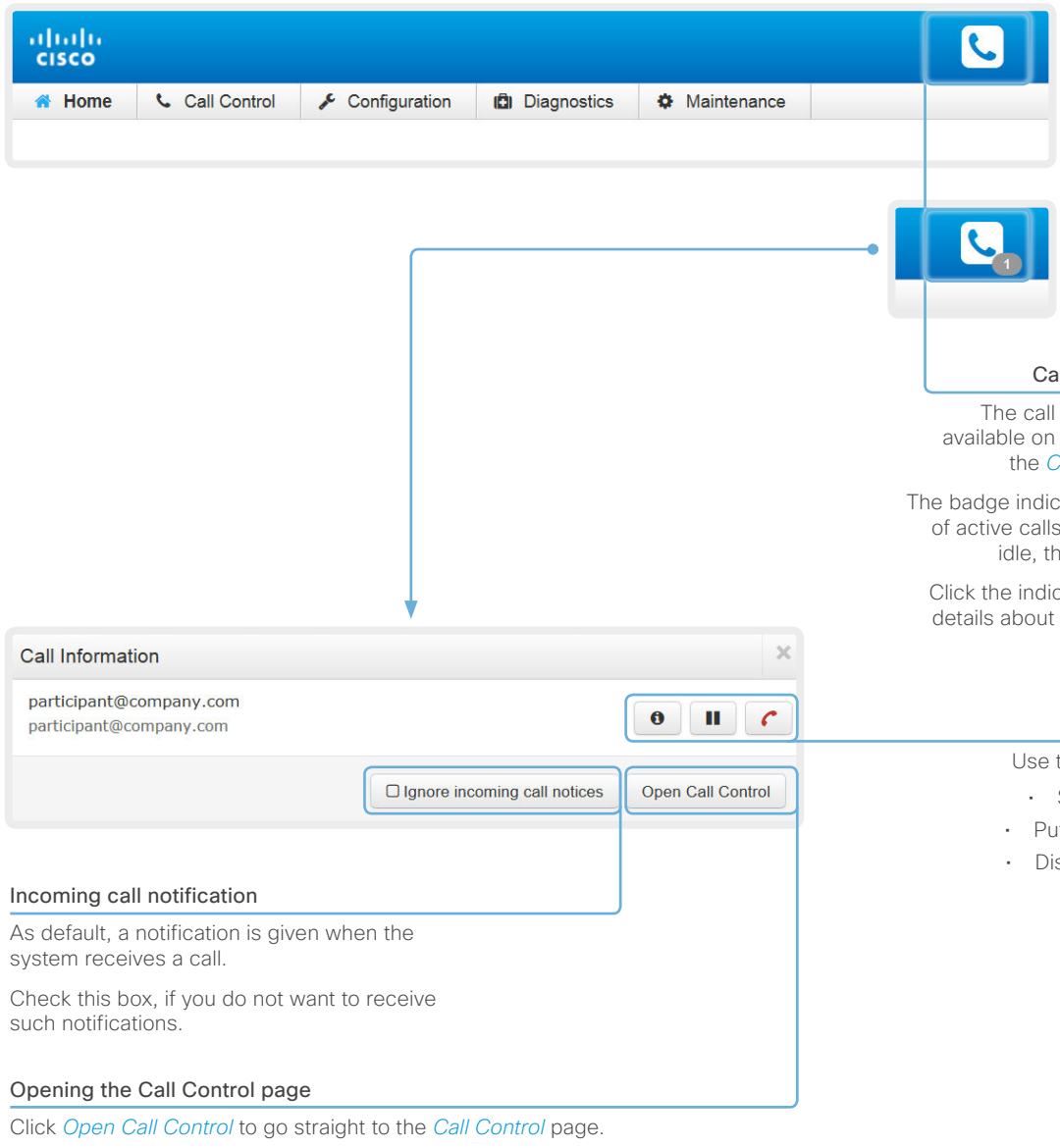
   For software versions TC7.3.0 to TC7.3.2, the cursor must be in the image to show the controls.



www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Accessing call information

A call state indicator is available in the top bar in the web interface. It 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.



Call state indicator

The call state indicator is available on all pages except the *Call Control* page.

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.

Call control

Use these buttons to:

- Show call details
- Put the call on hold
- Disconnect the call

Incoming call notification

As default, a notification is given when the system receives a call.

Check this box, if you do not want to receive such notifications.

Opening the Call Control page

Click *Open Call Control* to go straight to the *Call Control* page.

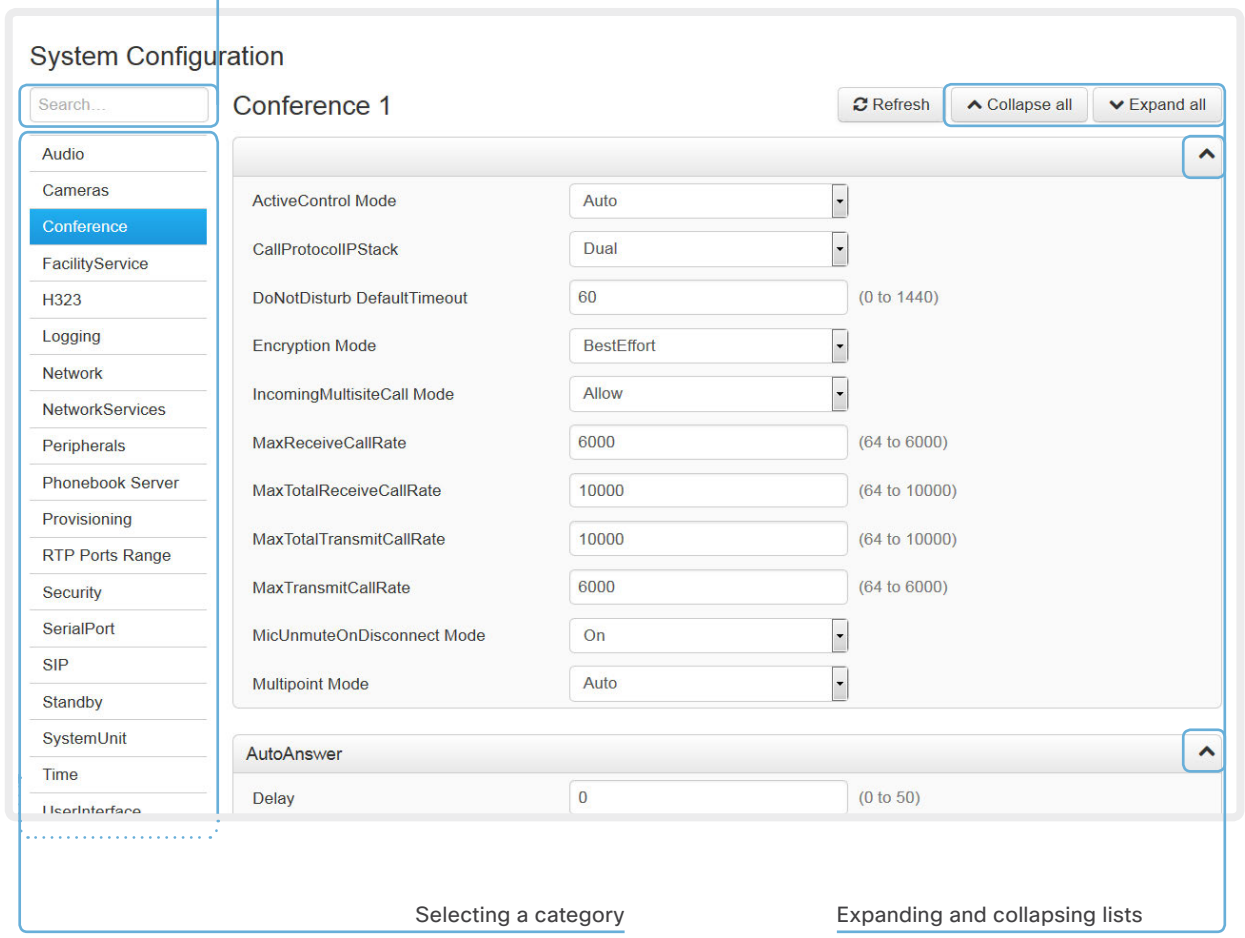
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

System configuration

The system settings are grouped in several categories. When you choose a category in the left pane all related settings appear to the right*.

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

Navigate to: Configuration > System Configuration



* The configuration shown in the illustration serve as an example. Your system may be configured differently.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Changing system settings

All system settings can be changed from the System Configuration page*. The value space for a setting is specified either in a drop-down list or by text following the input field.

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.

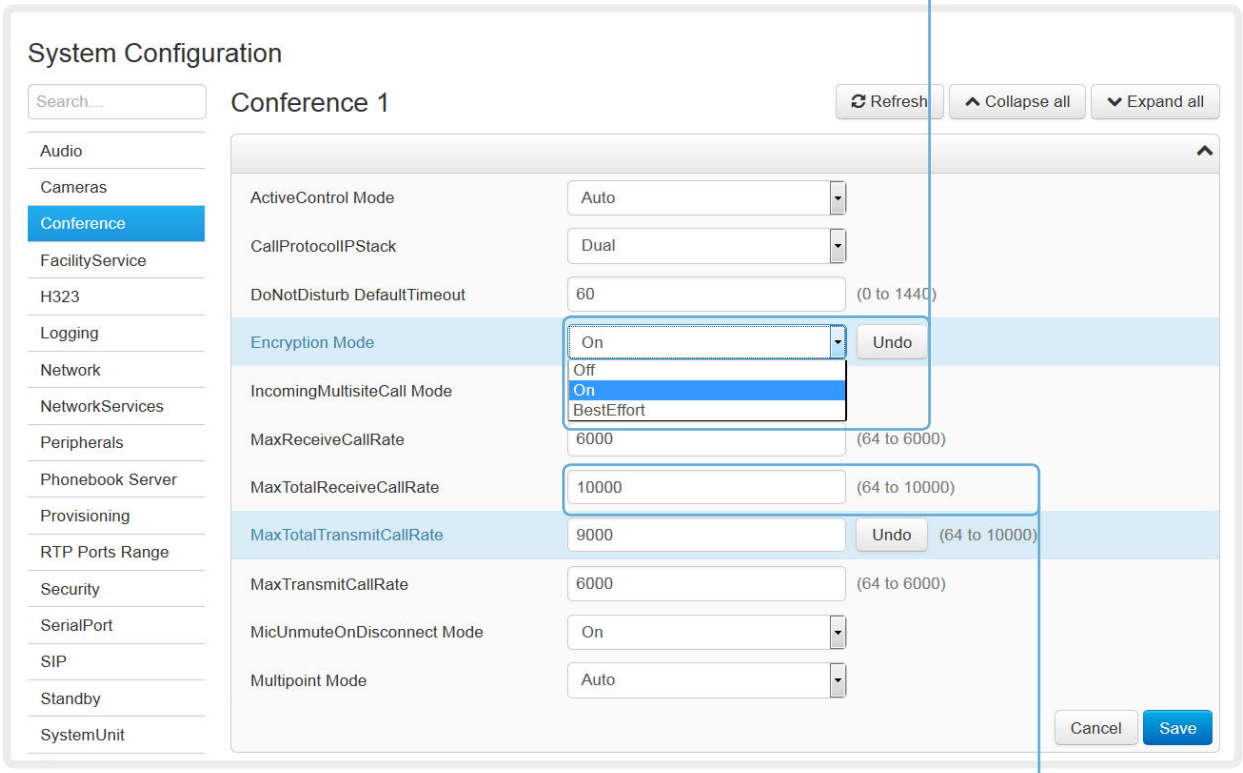
You can read more about user administration and user roles in the User administration chapter.

Navigate to: Configuration > System Configuration

Drop-down list

Click the arrow to open the drop-down list, and choose the preferred value.

Click *Save* for the change to take effect.



Text input field

Enter new text in the input field.

Click *Save* for the change to take effect.

* The configuration shown in the illustration serve as an example. Your system may be configured differently.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

System status

The system status is grouped in several categories. When you choose a category in the left column, the related status appears in the window to the right*.

Navigate to: Configuration > System Status

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Managing the favorites list

The entries in the favorites list can be accessed from the Touch controller and the Web interface.

Navigate to: Configuration > Local Contacts Management

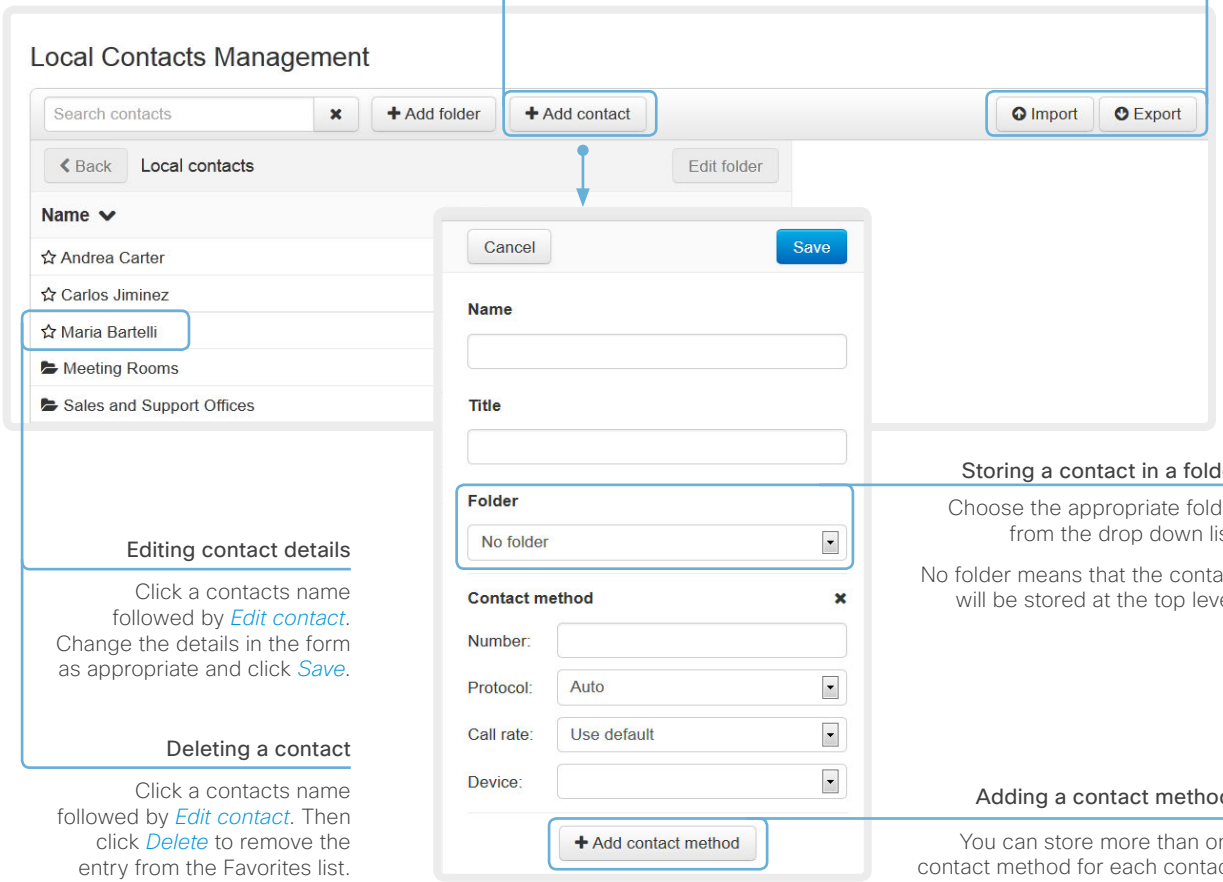
Adding a contact

Click *Add contact* and fill in the form that pops up. Then click *Save* to store the contact in the Favorites list.

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.

Note that all current contacts will be discarded when importing new contacts from a file.



Editing contact details

Click a contacts name followed by *Edit contact*. Change the details in the form as appropriate and click *Save*.

Deleting a contact

Click a contacts name followed by *Edit contact*. Then click *Delete* to remove the entry from the Favorites list.

Storing a contact in a folder

Choose the appropriate folder from the drop down list.

No folder means that the contact will be stored at the top level.

Adding a contact method*

You can store more than one contact method for each contact, e.g. video, telephone and mobile.

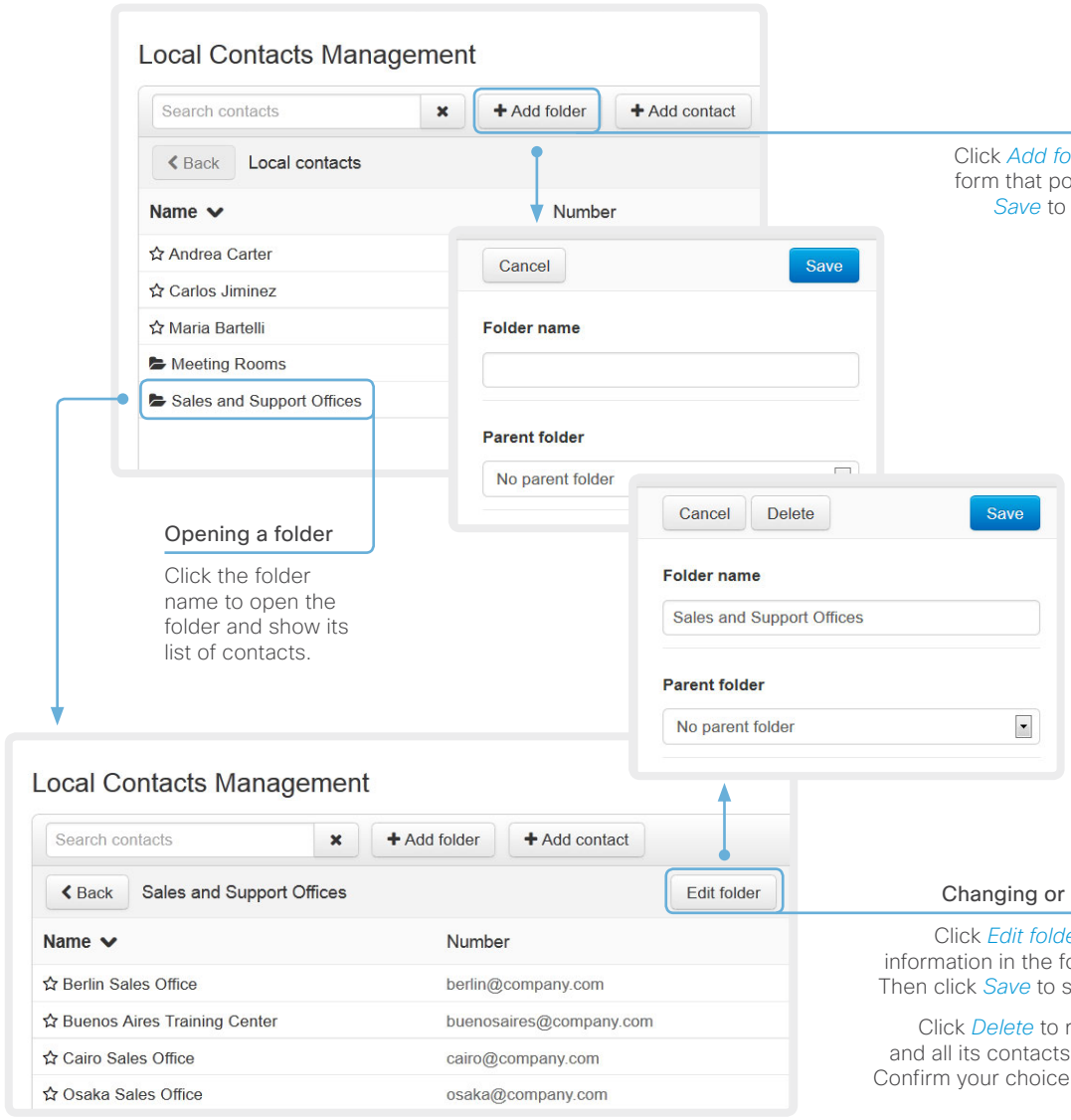
* Note that only the first contact method appears in the Favorites list on the Touch controller.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Favorite list folders

The entries in the Favorites list can be organized in folders.

Navigate to: Configuration > Local Contacts Management



Adding a folder

Click *Add folder* and fill in the form that pops up. Then click *Save* to create the folder.

Opening a folder

Click the folder name to open the folder and show its list of contacts.

Changing or Deleting a folder

Click *Edit folder* and update the information in the form that pops up. Then click *Save* to store the changes

Click *Delete* to remove the folder and all its contacts and sub-folders. Confirm your choice in the dialog that pops up.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Choosing a wallpaper

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

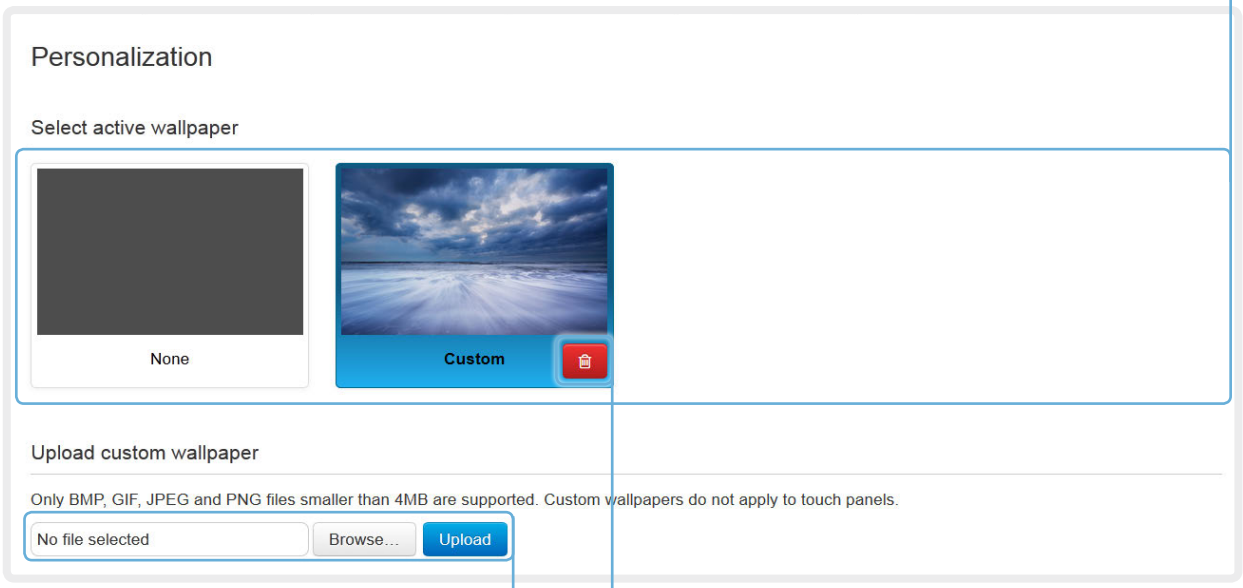
Navigate to: Configuration > Personalization

Activate/deactivate a wallpaper

Available wallpapers are represented by a miniature. If you have uploaded a custom wallpaper, it will appear in the list.

Click the miniature to switch to the corresponding wallpaper. Choose *None* if you do not want a wallpaper.

The chosen option is highlighted.



Upload a custom wallpaper

Click *Browse...* and locate your custom wallpaper image file.

Click *Upload* to save the file on the video system.

Supported file formats: BMP, GIF, JPEG, PNG
Maximum file size: 4 MByte

The custom wallpaper will be automatically activated once uploaded.

Delete the custom wallpaper

Click the delete symbol to remove the custom wallpaper from the video system. Note that this will remove the image file completely; you have to upload it anew if you want to use it again.

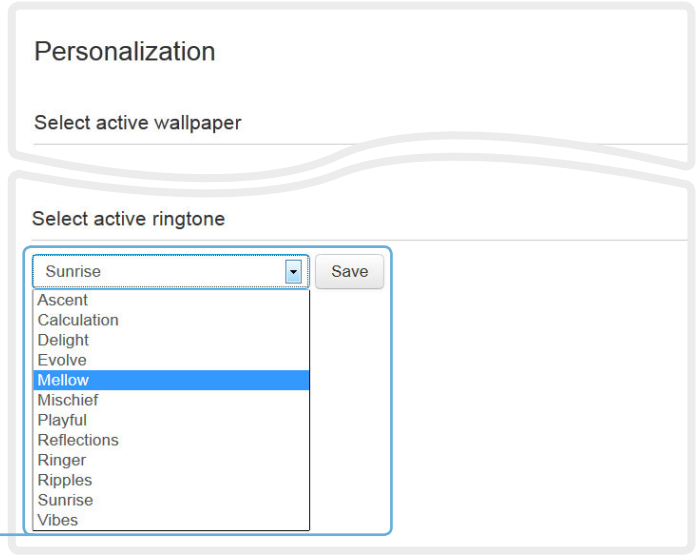
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Choosing a ringtone

You can choose from a set of predefined ringtones. The chosen ringtone can be played back from this page.

The ringtone will be played back on the video system itself, and not through the web interface.

Navigate to: Configuration > Personalization



Changing ringtone

Choose a ringtone from the drop-down list, and click *Save* to make it the active ringtone.

Playing back the ringtone

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

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

Set the ringtone volume

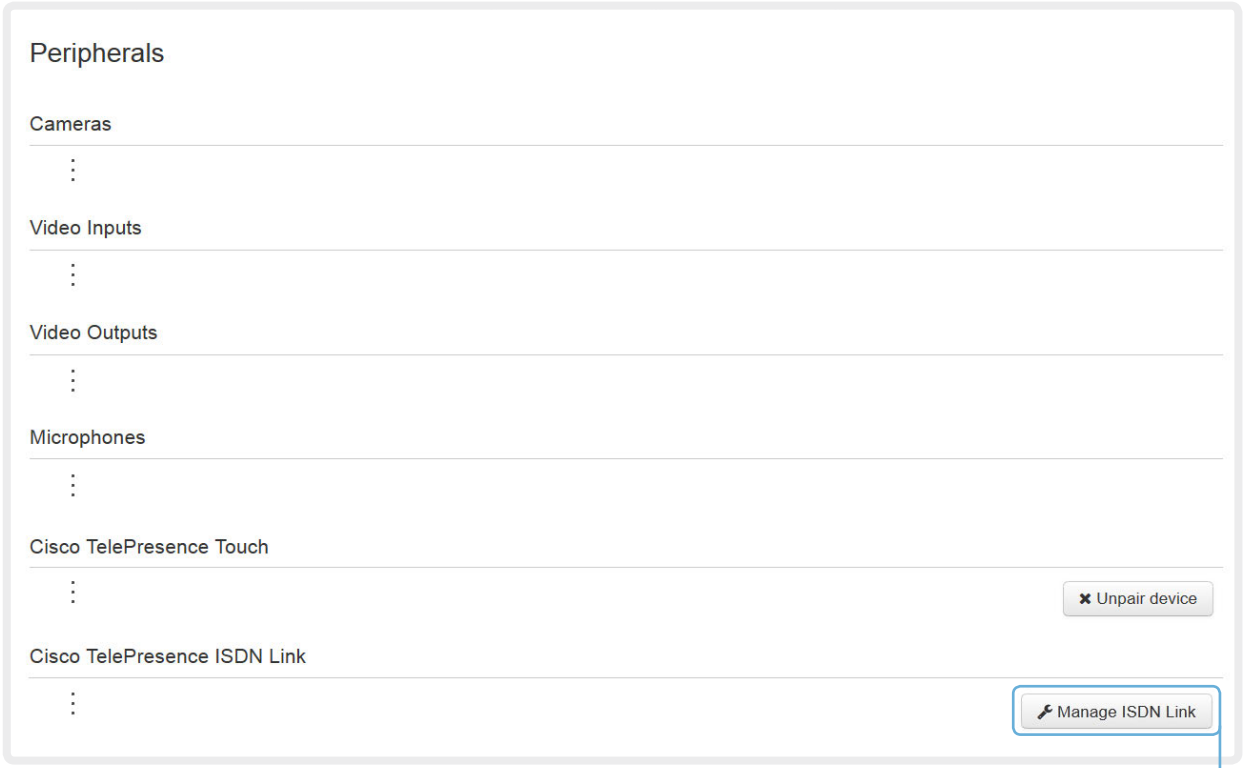
Use the slide bar to adjust the ringtone volume.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Peripherals overview

This page shows an overview of devices that are connected to the video system, like video inputs and outputs, cameras, microphones, ISDN Links and Touch controllers*.

Navigate to: Configuration > Peripherals



Managing ISDN Link

If an ISDN Link is paired to the video system it can be managed from this page.

How to configure and use the ISDN Link are described in the ISDN Link documentation on http://www.cisco.com/go/isdnlink-docs

* The peripherals shown in the illustration serve as examples. Your system may have different peripherals and video input/output configurations.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

User administration (page 1 of 4)

You can manage your video conference system's user accounts from this page.

The default user account

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

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

Read more about passwords in the Setting passwords chapter.

About user roles

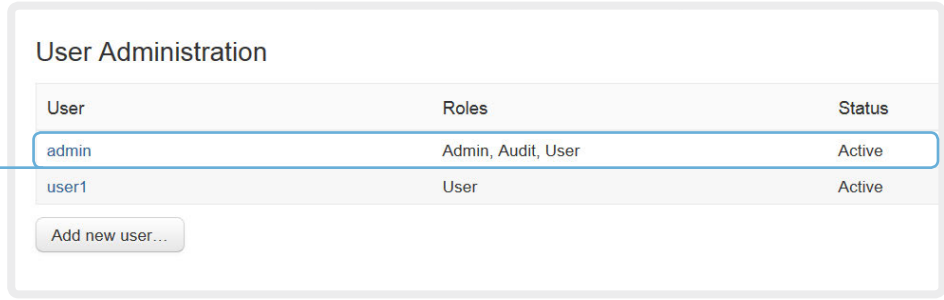
A user account must hold one or a combination of several *user roles*.

The following three user roles, with *non-overlapping rights,* exist:

- ADMIN: A user holding this role can create new users and change most settings. The user neither can upload audit certificates nor change the security audit settings.
- USER: A user holding this role can make calls and search the phone book. The user can modify a few settings, e.g. adjusting the ringtone volume and setting the time and date format.
- AUDIT: A user holding this role can change the security audit configurations and upload audit certificates.

An administrator user account with full access rights, like the default *admin* user, must possess all the three roles.

Navigate to: Configuration > User Administration



Default user account

The system comes with *admin* as the default user account. This user has full access rights.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

User administration (page 2 of 4)

Creating a new user account

Follow these steps in order to create a new user account:

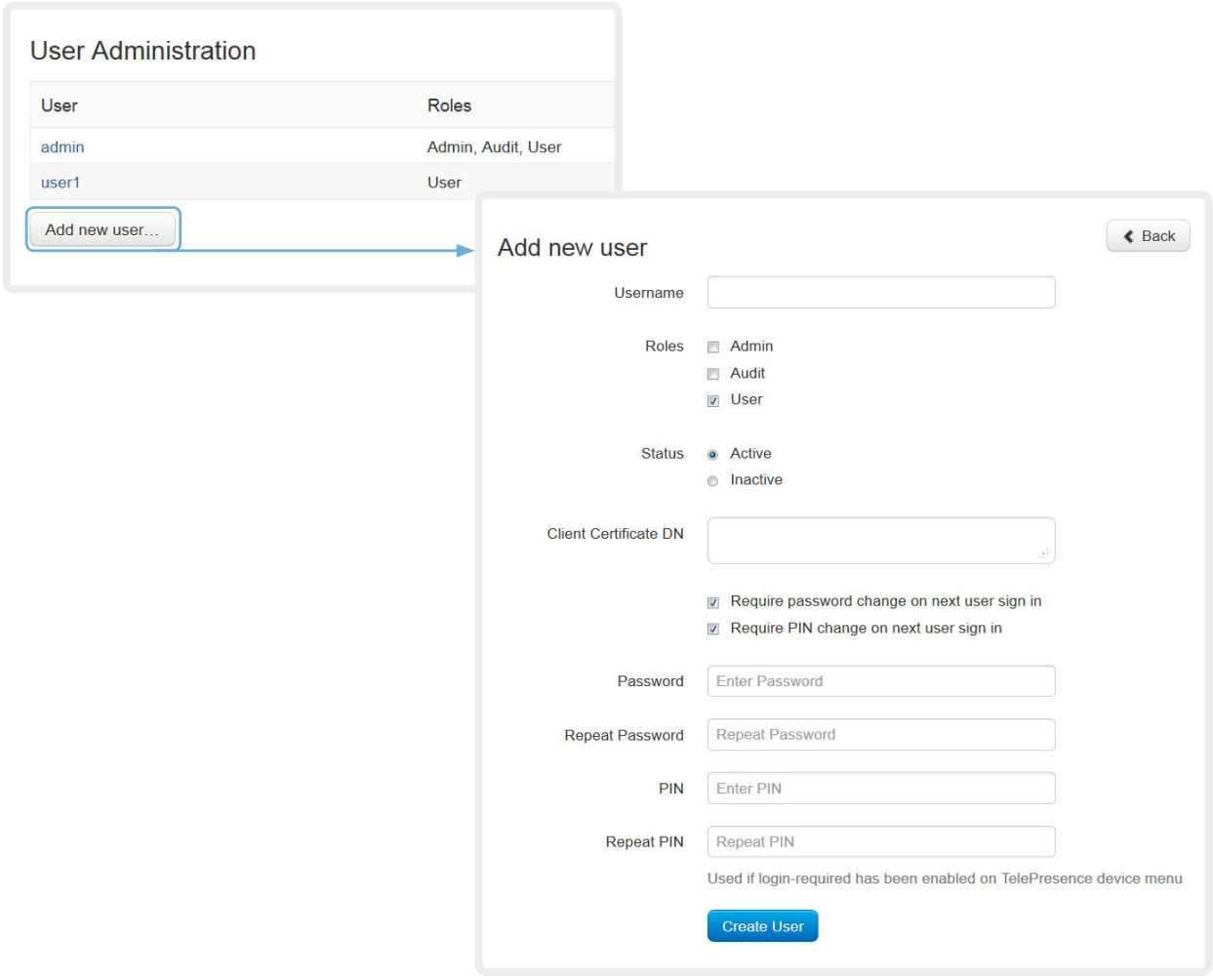
1. Click *Add new user...*.
2. Fill in the Username and Password*, and check the appropriate user roles check boxes.

   As a default the user has to change the password when signing in for the first time.

   Do not fill in the Client Certificate DN (Distinguished Name) field unless you want to use certificate login on HTTPS.
3. Set the Status to **Active** to activate the user.
4. Click *Create User* to save the changes.

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

Navigate to: Configuration > User Administration



* The password is used with the web interface and command line interface.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

User administration (page 3 of 4)

Changing user privileges

Follow these steps in order to change the user privileges:

1. Click the name of an existing user to open the Editing user window.
2. Check the appropriate user roles check boxes, decide if the user has to change the password on the next sign in, and fill in the Client Certificate DN field if using certificate login on HTTPS.
3. Click *Update User* to save the changes.

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

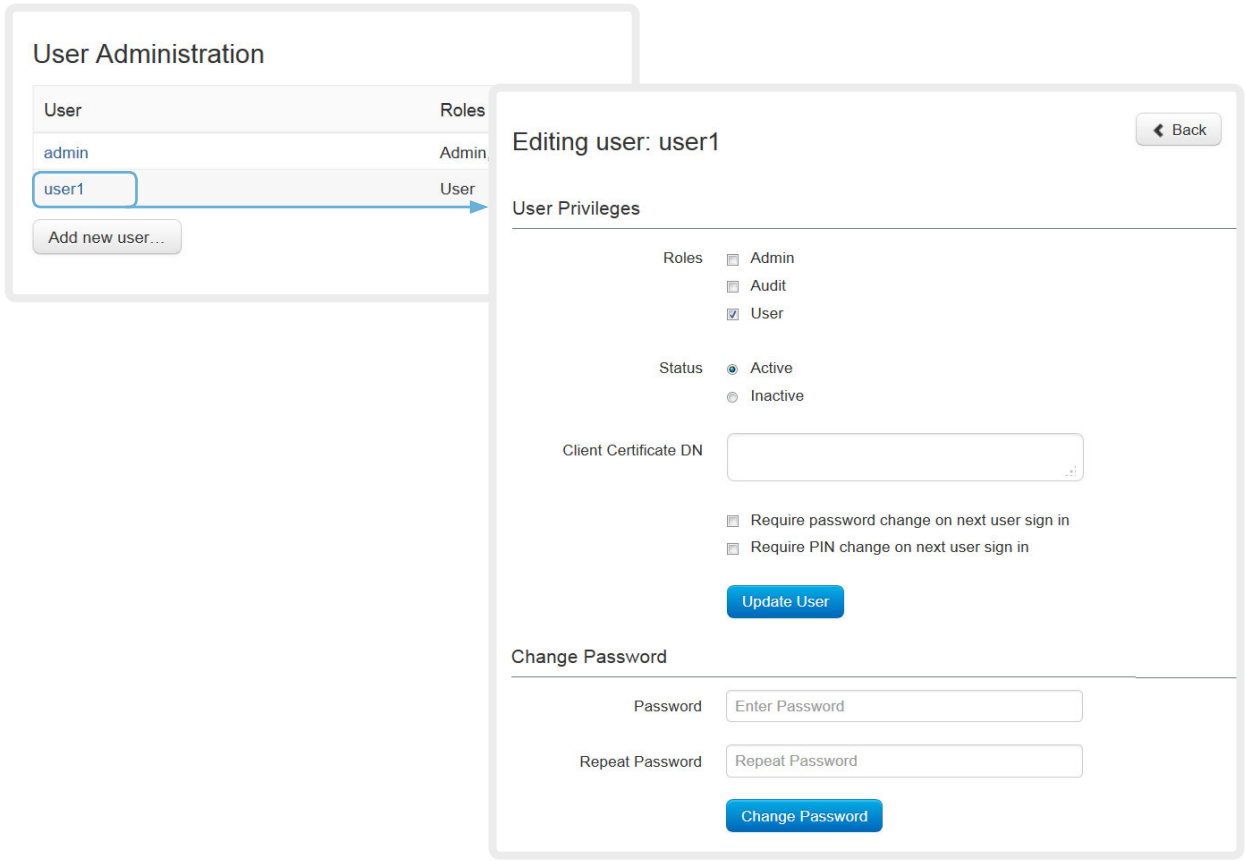
Changing the password

Follow these steps in order to change the password*:

1. Click the name of an existing user to open the Editing user window.
2. Enter the new password in the appropriate input fields.
3. Click *Change Password* to save the change.

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

Navigate to: Configuration > User Administration



* The password is used with the web interface and command line interface.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

User administration (page 4 of 4)

Deactivating a user account

Follow these steps in order to deactivate a user account:

1. Click the name of an existing user to open the Editing user window.
2. Set the Status to **Inactive**.
3. Click *Update User* to save the changes.

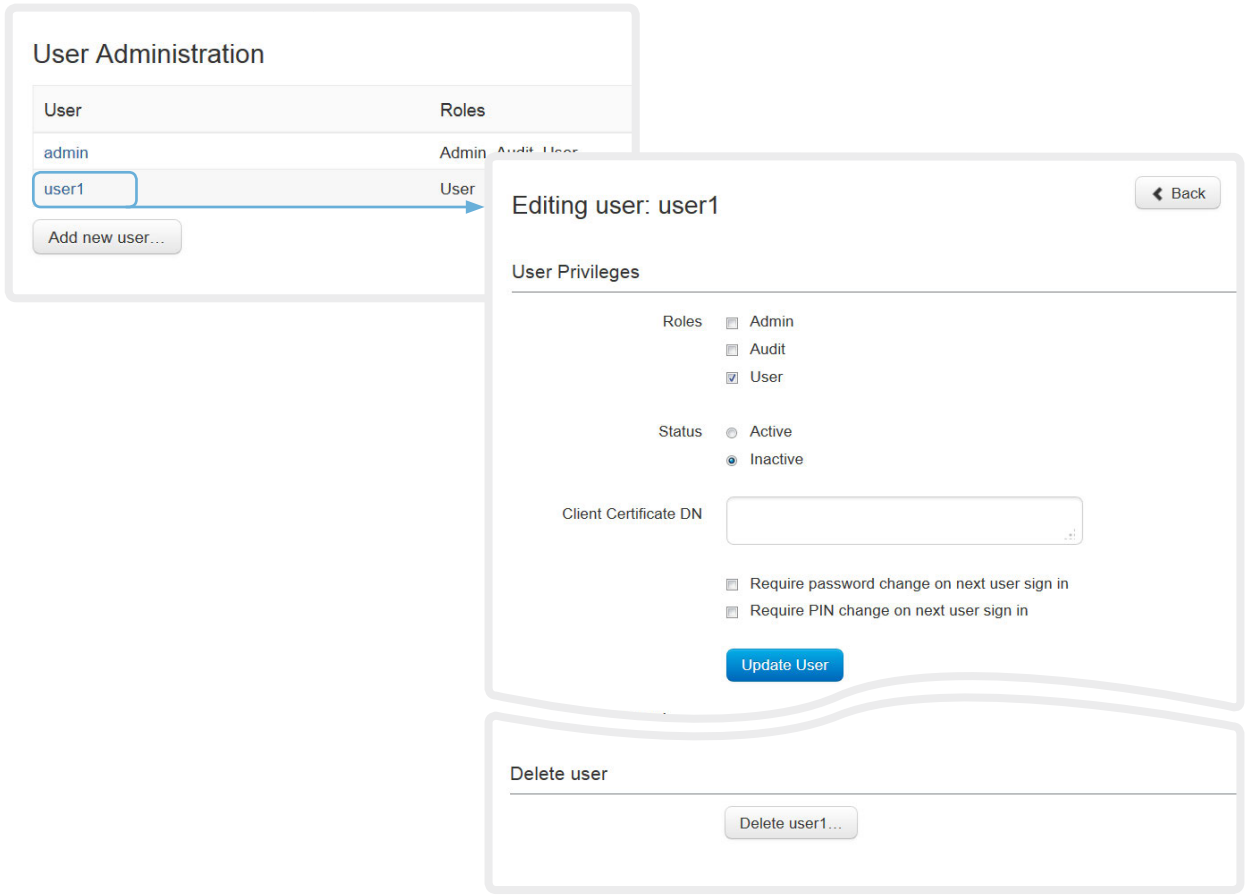
   Use the *Back* button to leave without making any changes.

Deleting a user account

Follow these steps in order to delete a user account:

1. Click the name of an existing user to open the Editing user window.
2. Click *Delete <user name>...* and confirm when prompted.

Navigate to: Configuration > User Administration

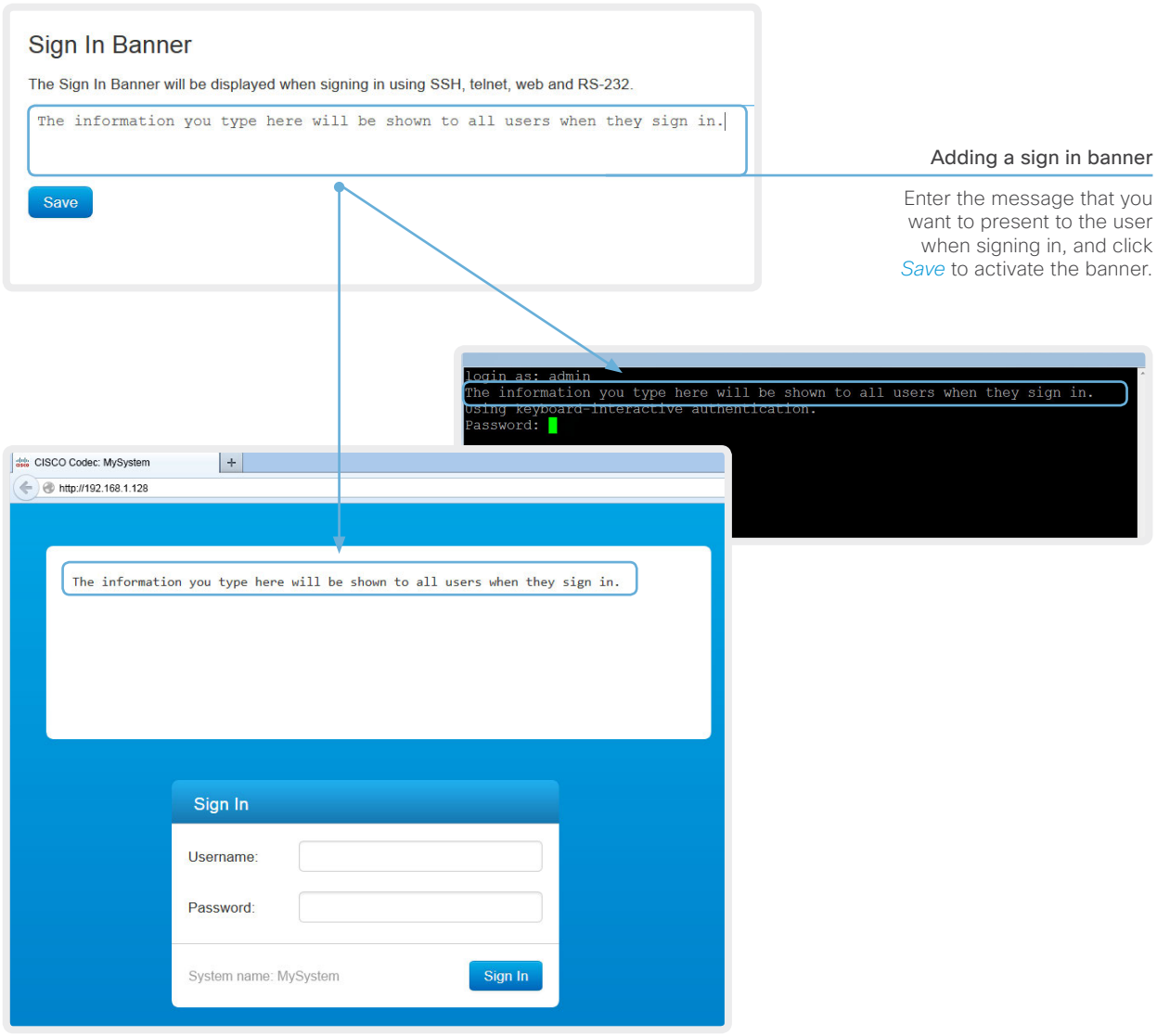


www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Adding a sign in banner

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

Navigate to: Configuration > Sign In Banner



www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Managing the video system's certificates

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

A server or client may require that your 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).

The certificates are listed as shown in the illustration to the right*. They can be used for the following services: HTTPS server, SIP, IEEE 802.1X and audit logging.

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

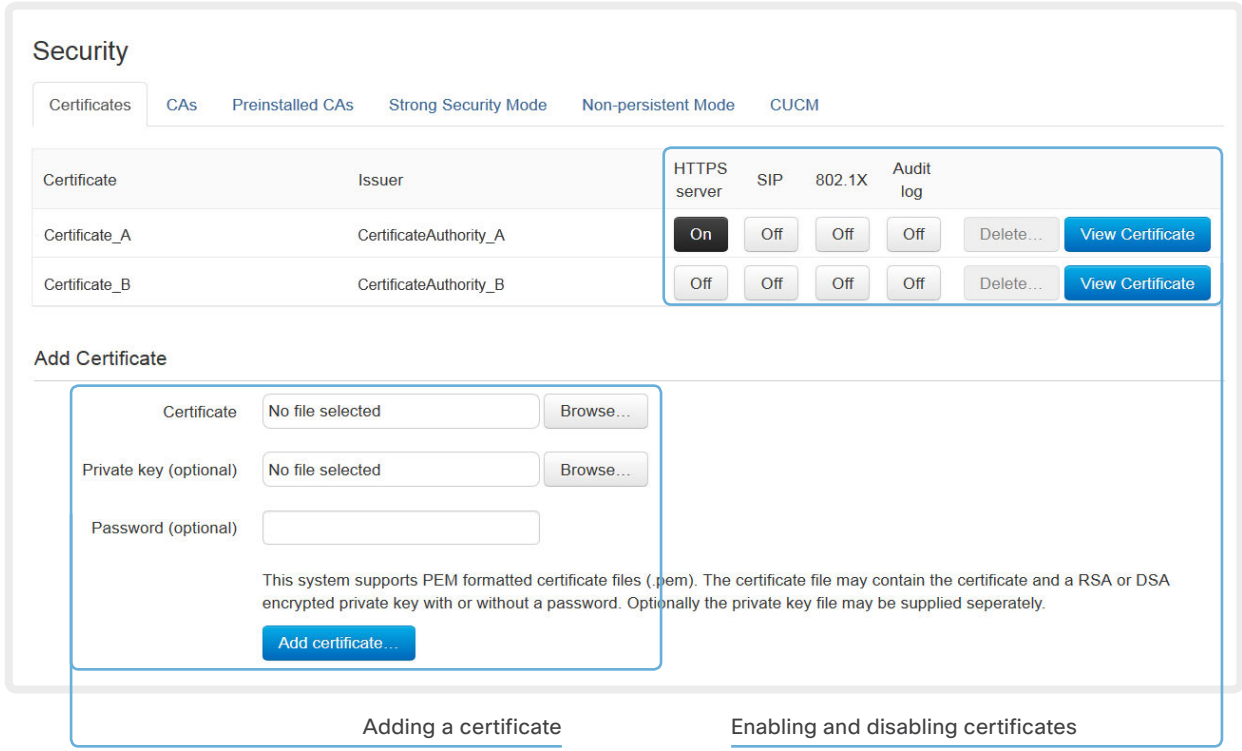
If authentication fails, the connection will not be established.

Contact your system administrator to obtain the following file(s):

- Certificate (file format: .PEM)
- Private key, either as a separate file or included in the same file as the certificate (file format: .PEM format)
- Password (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.

Navigate to: Configuration > Security: Certificates tab



Adding a certificate

1. Click *Browse...* and find the Certificate and Private key file(s) on your computer.
2. Fill in the *Password* if required.
3. Click *Add certificate...* to store the certificate on your system.

Enabling and disabling certificates

Use the buttons to switch a certificate on or off for the different services.

You can also view a certificate, and delete a certificate using the corresponding buttons.

* The certificates and certificate issuers shown in the illustration serve as examples. Your system may have other certificate(s).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Managing the list of trusted certificate authorities (page 1 of 2)

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

Your 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.

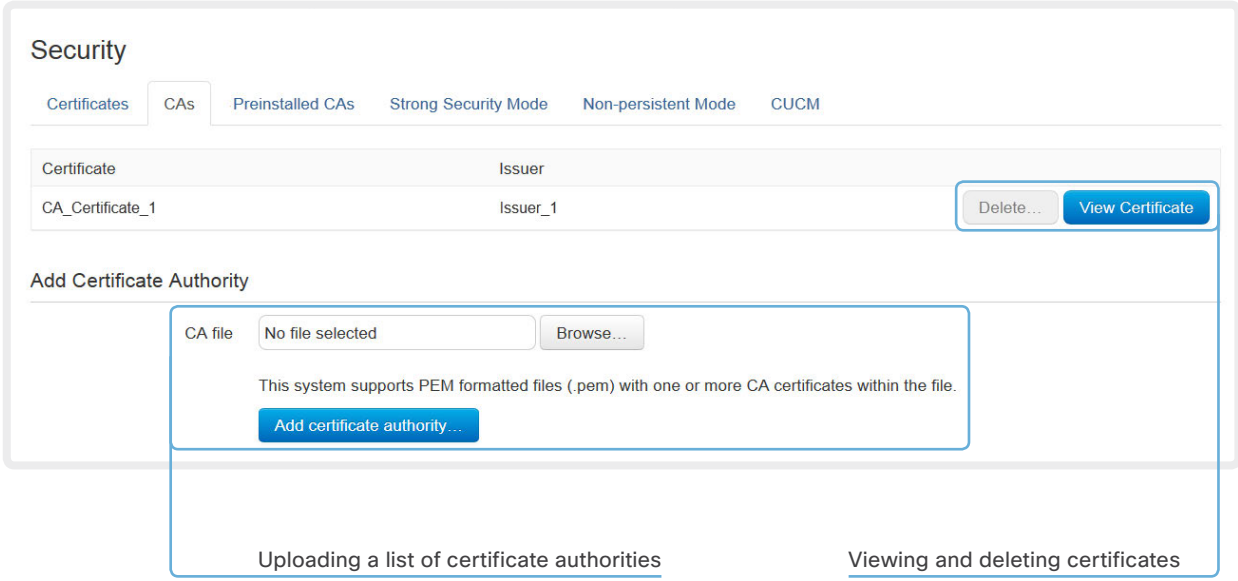
The certificates are text files that verify the authenticity of the server or client. The certificates must be signed by a trusted certificate authority (CA).

To be able to verify the signature of the certificates, a list of trusted CAs must reside on the video system. The certificates of the CAs are listed as shown in the illustration to the right*.

The list must include all CAs needed in order to verify certificates for audit logging, HTTPS, SIP and IEEE 802.1X connections.

If the server cannot be authenticated, the connection will not be established.

Navigate to: Configuration > Security: CAs tab



Uploading a list of certificate authorities

The entries in a new file with CA certificates will be appended to the existing list, so that the previously stored certificates will not be deleted.

i. Click *Browse...* and find the file containing a list of CA certificates (file format: .PEM) on your computer.

ii. Click the *Add certificate authority...* to store the new CA certificate(s) on your system.

Contact your system administrator to obtain the CA certificate list (file format: .PEM).

Viewing and deleting certificates

You can view a certificate, and delete a certificate using the corresponding buttons.

* The certificate and certificate issuers shown in the illustration serve as examples. Your system will have other certificate(s).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Managing the list of trusted certificate authorities (page 2 of 2)

As from software version TC7.2, the signature of an audit server is verified using the same CA list as other servers/clients.

Setting up secure audit logging

Audit logging records all sign in activity and configuration changes on your video system.

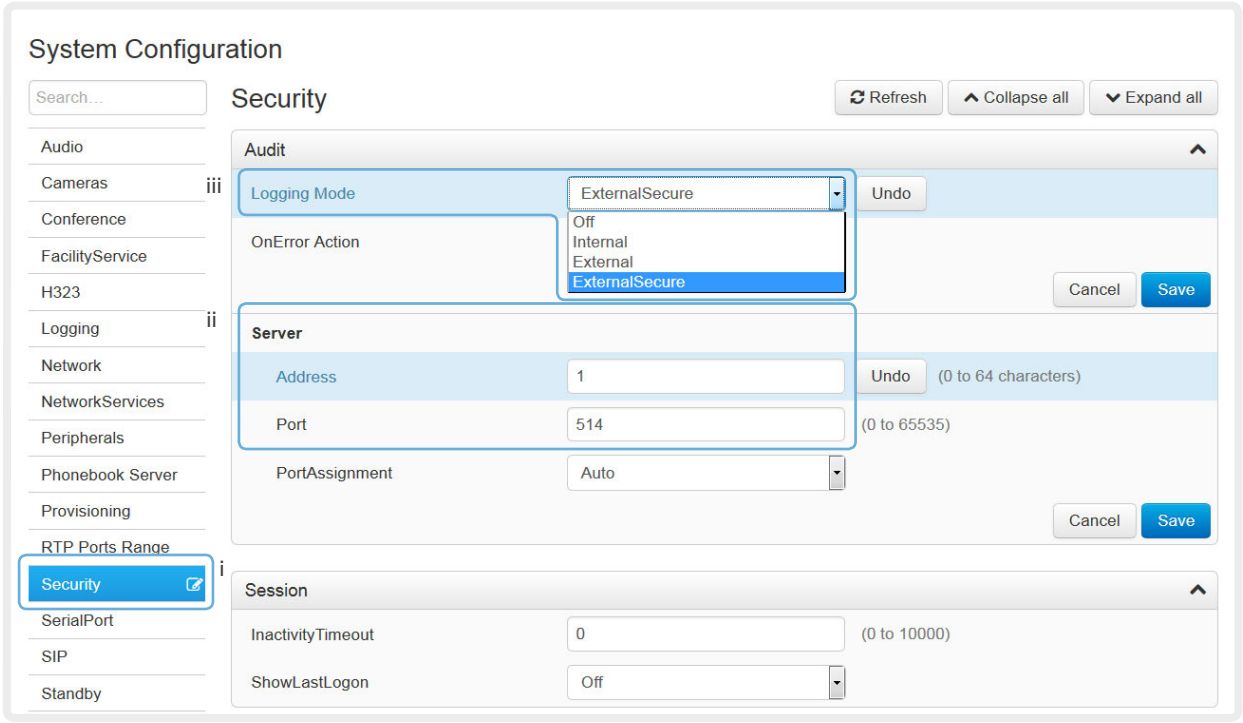
Audit logging is disabled by default, but you can enable it using the *Security > Audit > Logging > Mode* setting.

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.

If the audit server cannot be authenticated, the logs will not be sent.

Always upload the list of trusted certificate authorities before enabling secure audit logging.

Navigate to: Configuration > Security: CAs tab / Configuration > System Configuration



Enable secure audit logging

i. Go to the *System Configuration* page and choose the *Security* category.

ii. Enter the *Address* of the audit server. If you choose **Manual** *PortAssignment,* you must also enter a *Port* number for the audit server. Click *Save* for the changes to take effect.

iii. Choose **ExternalSecure** from the *Logging Mode* drop-down list. Click *Save* for the change to take effect.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

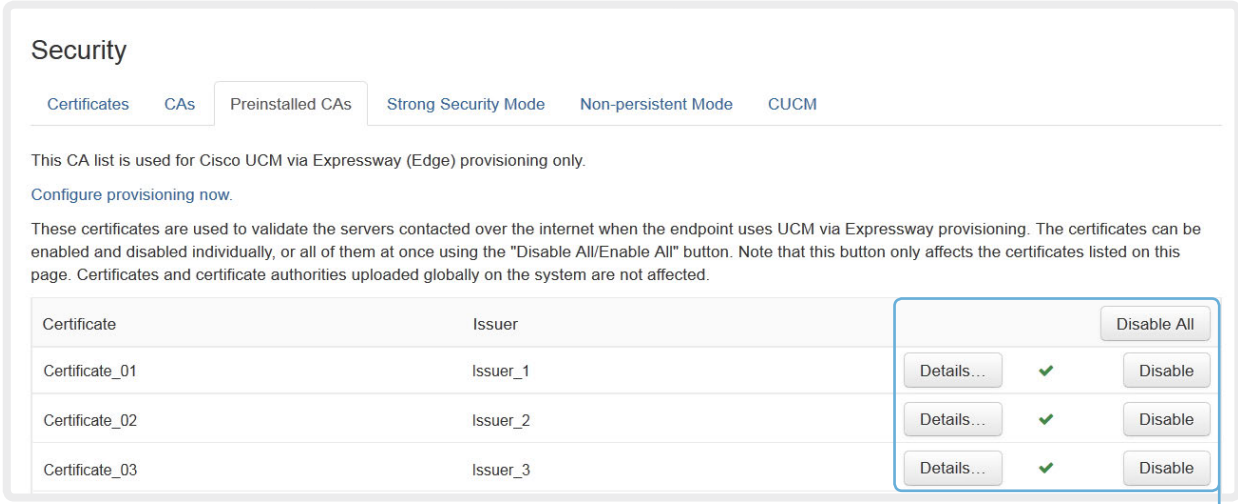
Managing pre-installed certificates for Edge provisioning

The list of pre-installed certificates that is shown on this page in the web interface*, contains certificates that will be used when the video system is provisioned by Cisco Unified Communications Manager (CUCM) via Expressway (Edge). Only Edge infrastructure certificates will be checked against this list.

If the Edge infrastructure certificate validation fails, the video system will not receive the provisioning and not be registered.

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

Navigate to: Configuration > Security: Preinstalled CAs tab



Viewing or disabling certificates

You can view a certificate, and disable a certificate using the corresponding buttons.

You can disable all the pre-installed certificates, and use a manually uploaded list of certificates for verification instead. See the *Configuration > Security: CAs* page how to upload trusted certificates to the video system manually.

* The certificate and certificate issuers shown in the illustration serve as examples. Your system will have other certificate(s).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

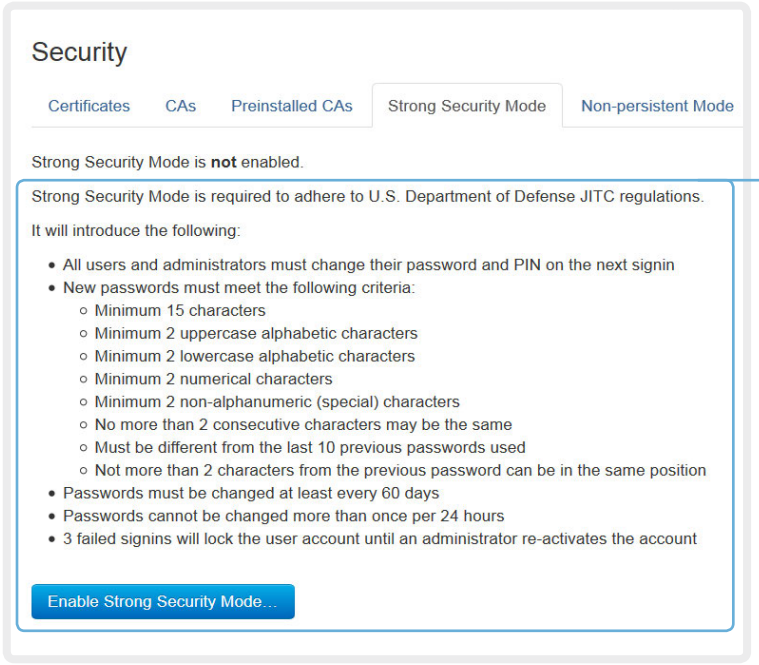
Setting strong security mode

Strong security mode should be used only when compliance with DoD JITC regulations is required.

Read the provided information carefully before setting strong security mode.

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

Navigate to: Configuration > Security: Strong Security Mode tab



Setting strong security mode

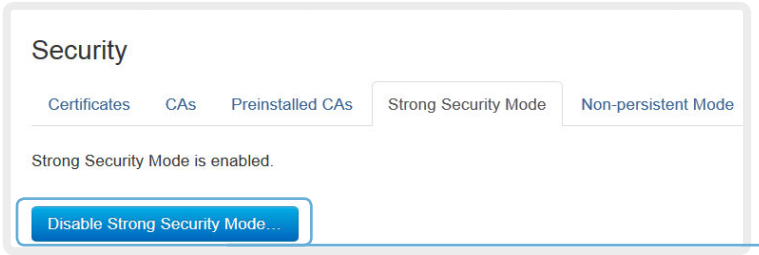
Read carefully about the consequences of strong security mode before you continue.

1. If you want to use strong security mode, click *Enable strong security mode...*. Confirm your choice in the dialog box that appears.

   The system will restart automatically.

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

   How to change the system password is described in the Setting passwords section.



Return to normal mode

When in strong security mode, the system can be restored to normal mode by clicking *Disable strong security mode...*. Confirm your choice in the dialog box that appears

The system will restart automatically.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Changing the persistency mode

By default, all persistency settings are set to **Persistent**. This means that configurations, call history, internal logs, local phonebook / favorites list and IP connectivity information are stored as normal. A system restart does not delete information.

As a general rule, we recommend NOT to change the default settings for persistency. But in the case were a new user is not supposed to see or trace back to any kind of logged information from the previous session, **Non-persistent** mode must be used.

In order to clear/delete information that was stored before changing to Non-persistent mode, you should consider to factory reset the video system.

There is more information about performing a factory reset in the Factory resetting appendix.

When in Non-persistent mode, the following information will be lost/cleared each time the system restarts:

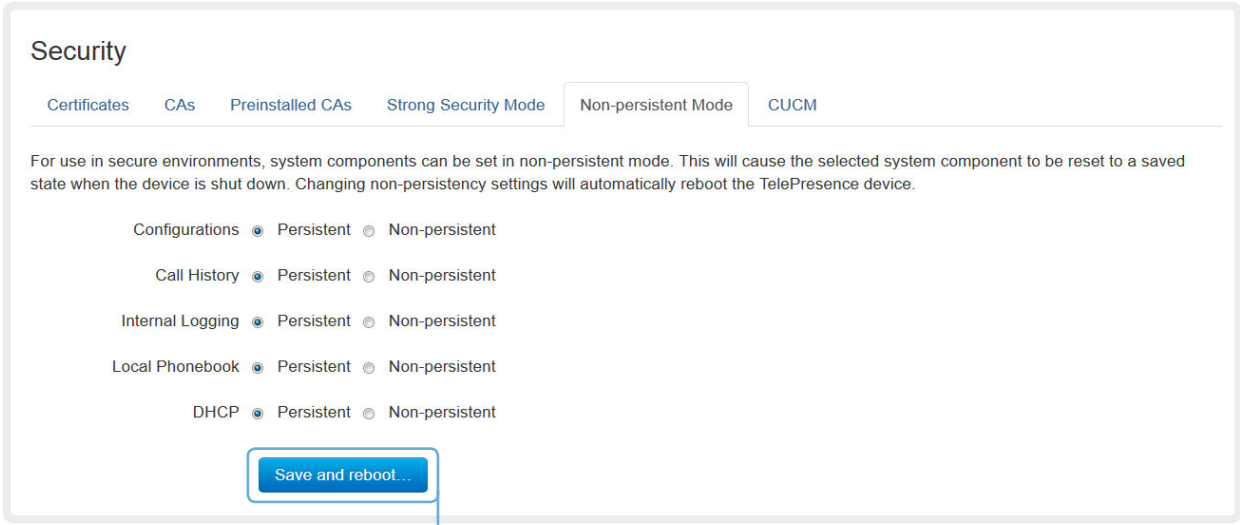
- System Configuration changes that have been made since the last system restart.
- Information about calls that are placed or received since the last system restart (call history).
- Internal log files that has been made since the last system restart.
- Changes that are made to the local contacts / favorites list since the last system restart.
- All IP related information (DHCP) from the last session.

Checking the persistency status

The radio buttons that are active when you open the *Security* page and go to the *Non-persistent Mode* tab, shows the current persistency status of the video system.

You can also see the status by checking *Security > Persistency* on the *Configuration > System Status* page.

Navigate to: Configuration > Security: Non-persistent Mode tab



Changing the persistency settings

1. Set the persistency settings for the five categories as desired.
2. Click *Save and reboot...*.

   The system will restart. After the restart, behavior according to the new persistency settings will start.

   Note that logs, configurations etc. that was stored before you switch to Non-persistent mode, will not be cleared or deleted.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Deleting trust lists (CUCM only)

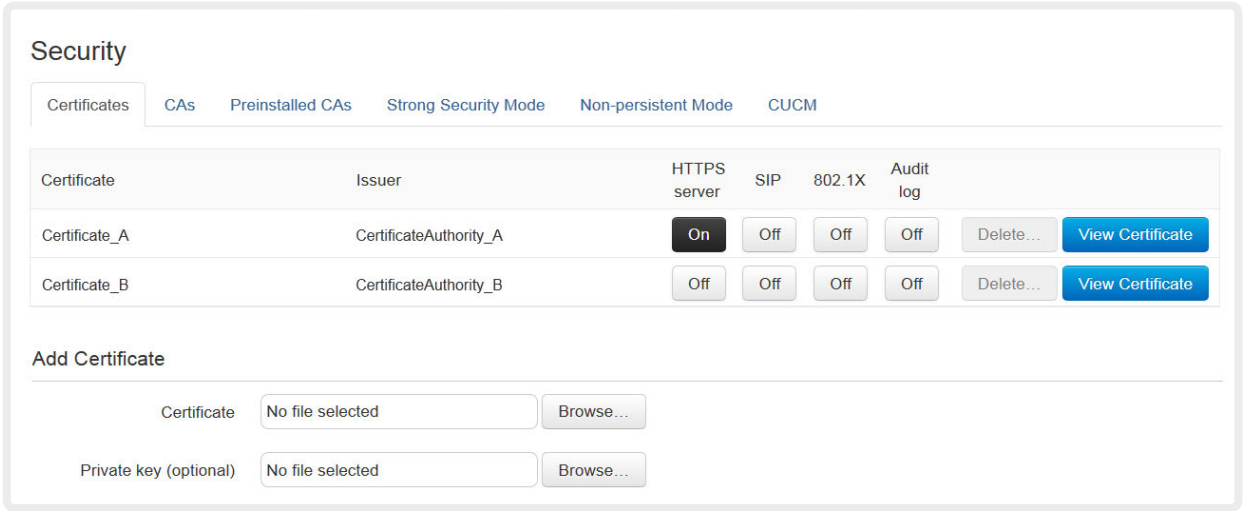
The information on this page is only relevant for video systems that are registered to a Cisco Unified Communications Manager (CUCM).

The web interface can be used to delete existing trust lists (CTL and ITL) that are stored on the video system. Normally, you will not delete the old CTL and ITL files, but there are a few cases when you will need to delete them.

The trust lists' fingerprints and an overview of the certificates in the lists are displayed on the web page. This information can be useful for troubleshooting.

For more information about CUCM and trust lists, read the *Administering TC Endpoints on CUCM* guide available on the Cisco web site.

Navigate to: Configuration > Security: CUCM tab



www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Troubleshooting

The troubleshooting page lists the status for some common sources of errors. The list may be different for different products and installations*.

Note that critical issues and errors are clearly marked in red color; warnings are yellow.

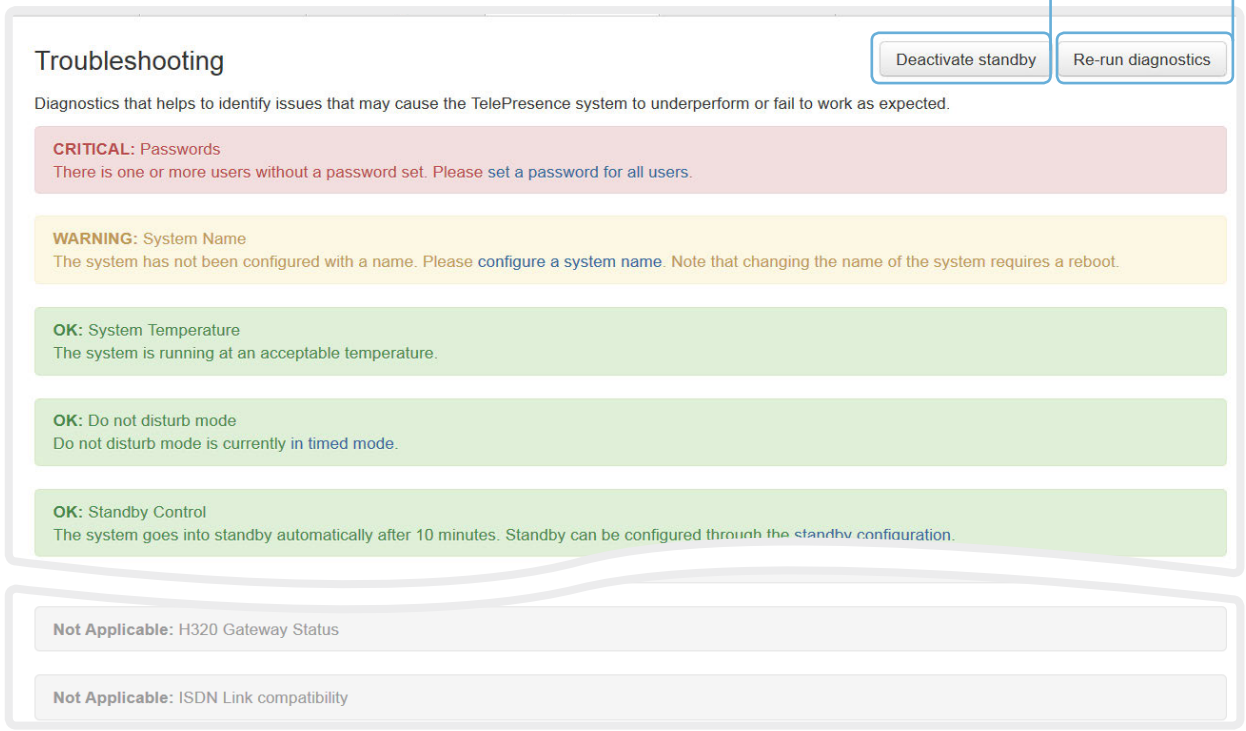
Navigate to: Diagnostics > Troubleshooting

Run diagnostics

Click *Re-run diagnostics* to make sure the information in the list is up-to-date.

Leave standby mode

This button is only visible when the system is in standby mode. If in standby mode, click *Deactivate standby* to wake up the system.



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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

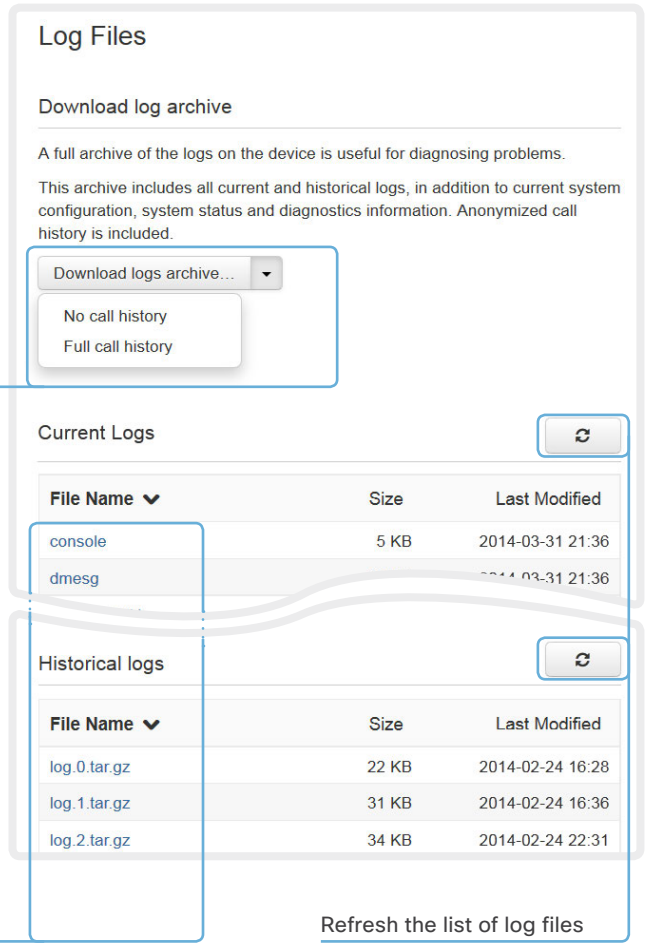
Downloading log files

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

Navigate to: Diagnostics > Log Files



Downloading 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 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.

Refresh the list of log files

* The log files shown in the illustration serve as examples. Your system may have other files.

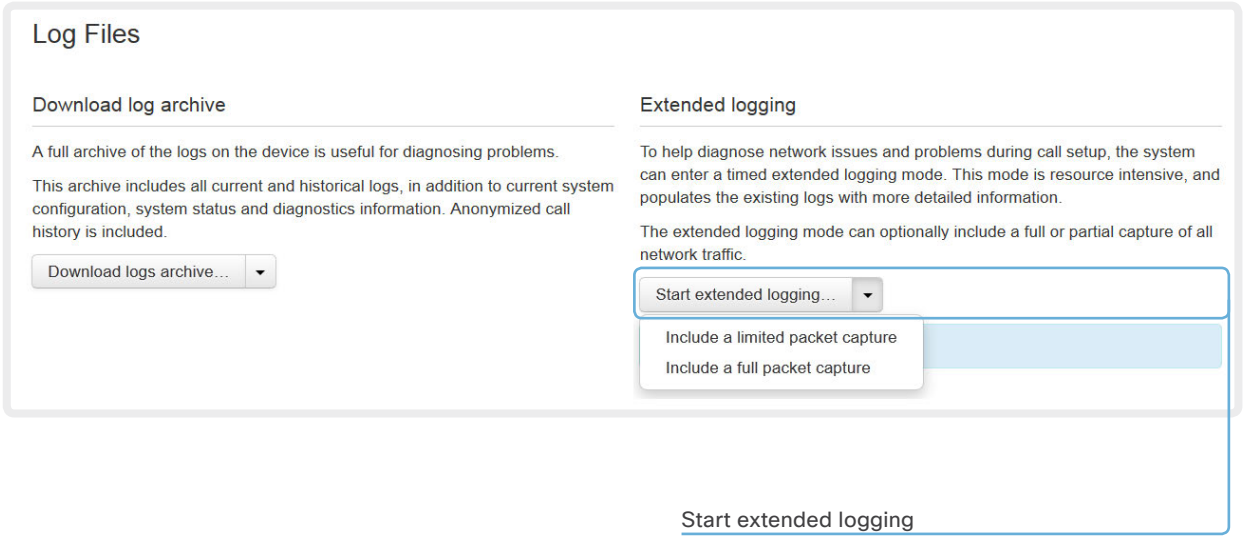
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Starting extended logging

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.

Note that extended logging uses more of your video system's resources, and may cause your video system to under-perform. You should only use extended logging mode when troubleshooting an issue.

Navigate to: Diagnostics > Log Files



Start extended logging

Click *Start extended logging*.

Extended logging lasts for 10 minutes. You can stop the extended logging before it times out by clicking the *Stop extended logging* button that appears when extended logging is on.

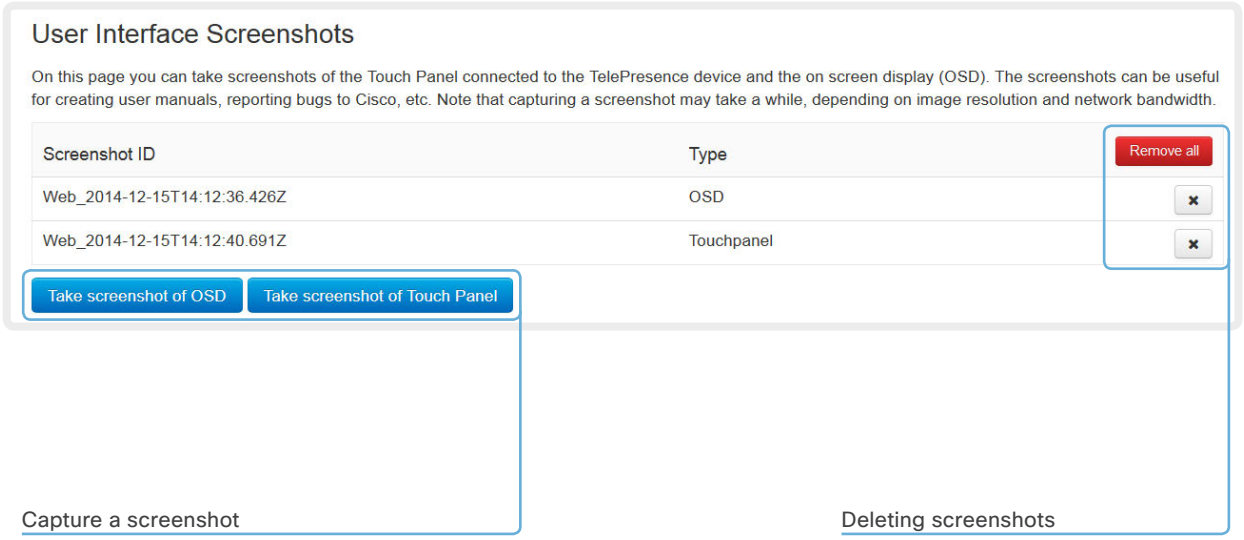
As default, the network traffic is not captured. Use the drop down menu if you want to include a full or partial capture of the network traffic.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Capturing 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).

Navigate to: Diagnostics > 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 will display in the area below the buttons. Note that it can 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.

Deleting screenshots

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

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Upgrading the system software

This video conference system is using TC software. The version described in this document is TC7.3.

Contact your system administrator if you have questions about the software version.

Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (TC7).

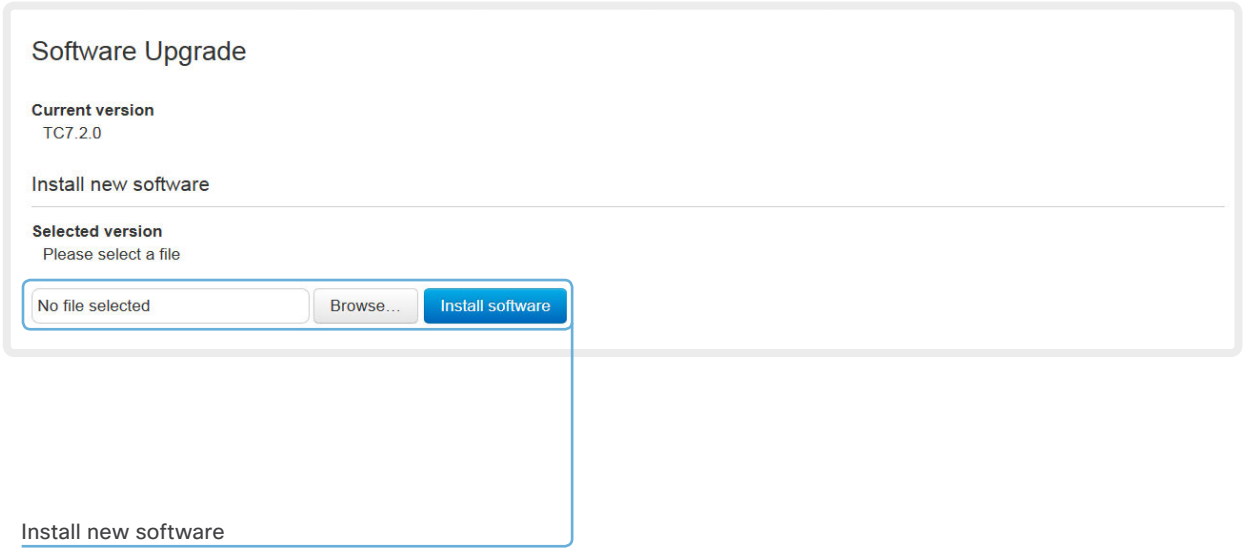
Go to: http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/tsd-products-support-series-home.html

New software

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

The format of the file name is “s52010tc7_3_0.pkg” (each software version has a unique file name).

Navigate to: Maintenance > Software Upgrade



Install new software

Download the appropriate software package from the Cisco Software Download web page (see link to the left) and store it on your local computer. This is a .pkg file.

i. Click *Browse...* and find the downloaded .pkg file that contains the new software.
ii. Click *Install software* to start the installation process.

The complete installation may take up to 30 minutes. You can follow the progress on the web page. The system restarts automatically after the installation.

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Adding option keys

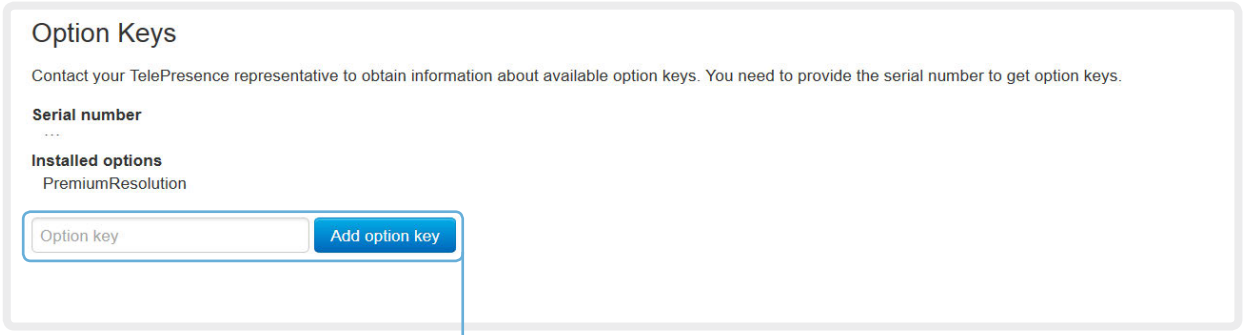
Your video system may or may not have one or more software options installed. In order to activate the optional functionality the corresponding *option key* must be present on the video system.

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

Each video system has unique option keys, for example: 1R000-1-AA7A4A09

Contact your Cisco representative to obtain information about available option keys, and how to get the required key(s).

Navigate to: Maintenance > Option Keys



Add an option key

i. Enter an *Option Key* in the appropriate text input field.
ii. Click *Add option key*.

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

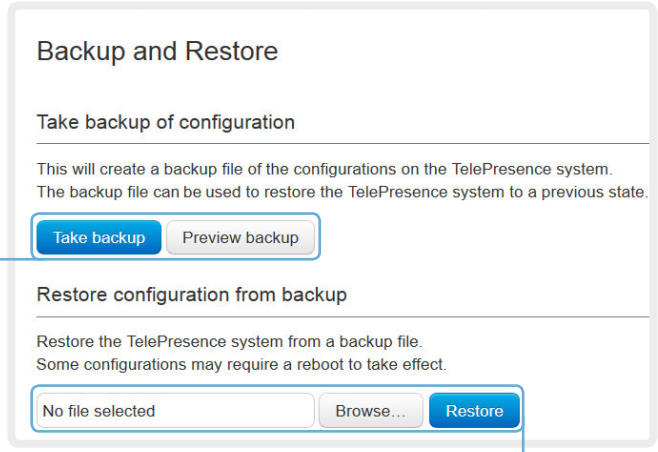
www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Backup and restore

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

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

Navigate to: Maintenance > Backup and Restore



Backing up or showing the current configuration

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

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

Restoring an earlier configuration

Click *Browse...* and find the file with the configuration you want to restore.

Click *Restore* to reconfigure the system as defined in the file.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Reverting to the previously used software version

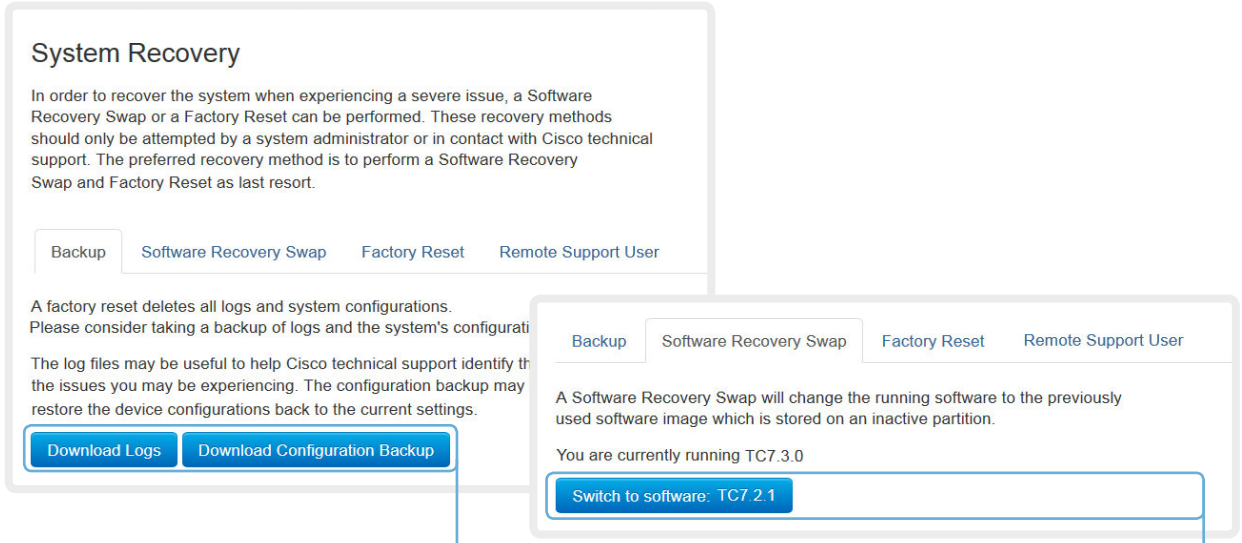
If there is a severe problem with the video system, switching to the previously used software version may help solving the problem.

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.

Reverting to the previously used software version should only be done by a system administrator or in contact with Cisco technical support.

We strongly recommend that you backup your system's log files and configuration before you swap to the other software image.

Navigate to: Maintenance > System Recovery: Backup tab and Software Recovery Swap tab



1. Backing up log files and system configuration

We recommend that you backup your system's log files and configuration before you swap to the other software image.

Click *Download Logs* and *Download Configuration Backup* and follow the instructions to save the files on your computer.

2. Reverting to the previously used software version

1. Revert to the previously used software version by clicking *Switch to software TCx.y.z...*, where x.y.z indicates the software version.
2. Click *Yes* to confirm your choice, or *Cancel* if you have changed your mind.

   Wait while the system resets. The system will restart automatically when finished.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Factory reset

If there is a severe problem with the video system, the last resort may be to reset it to its default factory settings. Always consider reverting to the previously used software image before performing a factory reset. In many situations this will recover the system*.

A factory reset should only be performed by a system administrator or in contact with Cisco technical support.

When factory resetting the video system the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.
- All system parameters will be reset to default values.
- All files that have been uploaded to the system will be deleted. This includes, but is not limited to, custom wallpapers, certificates and favorites list.
- The previous (inactive) software image will be deleted.
- Option keys will **not** be affected.

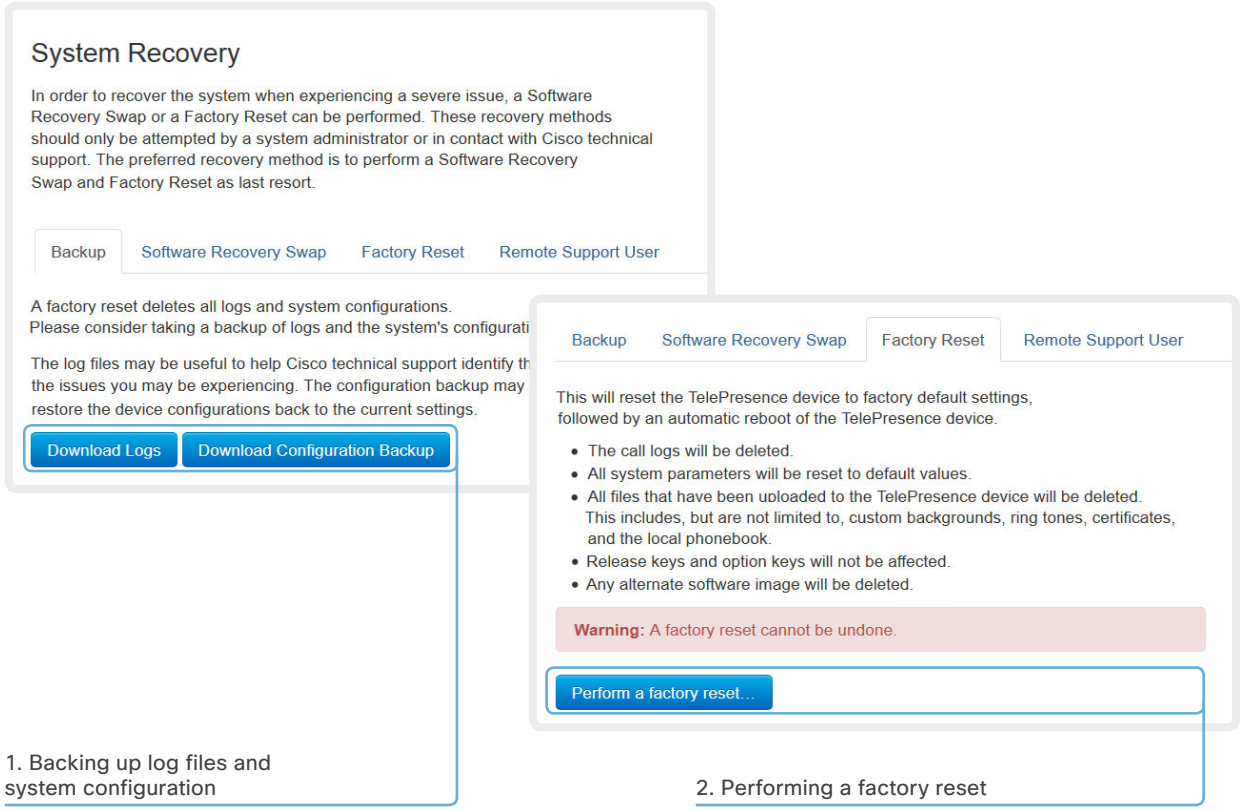
The system restarts automatically after the reset. It is using the same software image as before.

We strongly recommend that you backup your system's log files and configuration before you perform a factory reset.

It is *not* possible to undo a factory reset.

There is more information about performing a factory reset in the Factory resetting appendix.

Navigate to: Maintenance > System Recovery: Backup tab and Factory Reset tab



1. Backing up log files and system configuration

We strongly recommend that you backup your system's log files and configuration before you perform a factory reset; otherwise these data will be lost.

Click *Download Logs* and *Download Configuration Backup* and follow the instructions to save the files on your computer.

2. Performing a factory reset

Read the provided information carefully before you click *Perform a factory reset...*.

Click *Yes* to confirm your choice, or *Cancel* if you have changed your mind.

Wait while the system resets. The system will restart automatically when finished.

* Read about software swapping in the Reverting to the previously used software version section.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Remote support user

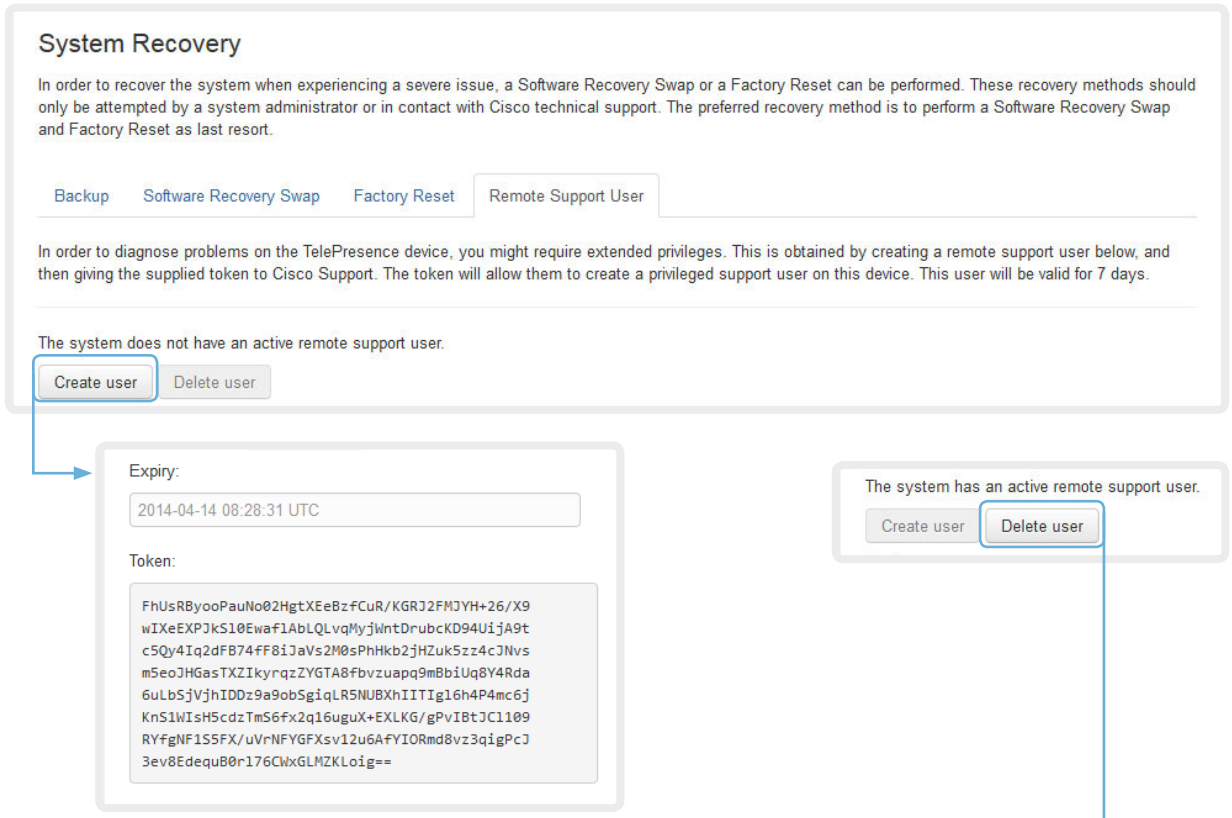
In cases where you need to diagnose problems on the video system you can create a remote support user.

The remote support user will be granted read access to the system and will have 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.

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

Navigate to: Maintenance > System Recovery: Remote Support User tab



Create remote support user

1. Open a case with Cisco TAC.
2. Click *Create user*.
3. Copy the text in the *Token* field and send 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*.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Restarting the system

The system can be shut down or restarted remotely using the web interface.

Navigate to: Maintenance > Restart

Restarting the system

Click *Restart TelePresence device...* to restart the system.

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

Shutting down the system

Click *Shutdown TelePresence device...* to shut down the system.

The system cannot be turned on again remotely; you must press its power button physically to turn it on.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Chapter 3

System settings

www.cisco.com – Copyright © 2013–2015 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 *System Configuration* page on the web interface. The examples show either the default value or an example of a value.

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

To find the IP address (IPv4 or IPv6), open the *Settings** menu on the Touch user interface and tap *System Information*.

* The *Settings* menu can be accessed from the drop down window that appears when you tap the contact information in the upper, left corner of the Touch user interface.

Audio settings 60
- Audio DefaultVolume 60
- Audio Input Microphone [1] Mode 60
- Audio Microphones Mute Enabled 60
- Audio SoundsAndAlerts KeyTones Mode 60
- Audio SoundsAndAlerts RingTone 60
- Audio SoundsAndAlerts RingVolume 60

Cameras settings 61
- Cameras Camera [1] Backlight 61
- Cameras Camera [1] Brightness Level 61
- Cameras Camera [1] Brightness Mode 61
- Cameras Camera [1] Focus Mode 62
- Cameras Camera [1] Gamma Level 62
- Cameras Camera [1] Gamma Mode 62
- Cameras Camera [1] Mirror 62
- Cameras Camera [1] Whitebalance Level 62
- Cameras Camera [1] Whitebalance Mode 62
- Cameras PowerLine Frequency 61
- Cameras Preset TriggerAutofocus 61

Conference settings 63
- Conference [1..1] ActiveControl Mode 63
- Conference [1..1] AutoAnswer Delay 63
- Conference [1..1] AutoAnswer Mode 63
- Conference [1..1] AutoAnswer Mute 63
- Conference [1..1] CallProtocolIPStack 63
- Conference [1..1] DefaultCall Protocol 65
- Conference [1..1] DefaultCall Rate 65
- Conference [1..1] DoNotDisturb DefaultTimeout 64
- Conference [1..1] Encryption Mode 64
- Conference [1..1] FarEndControl Mode 64
- Conference [1..1] FarEndControl SignalCapability 64
- Conference [1..1] IncomingMultisiteCall Mode 67
- Conference [1..1] MaxReceiveCallRate 65
- Conference [1..1] MaxTotalReceiveCallRate 66
- Conference [1..1] MaxTotalTransmitCallRate 65
- Conference [1..1] MaxTransmitCallRate 65
- Conference [1..1] MicUnmuteOnDisconnect Mode 64
- Conference [1..1] Multipoint Mode 67
- Conference [1..1] Presentation OnPlacedOnHold 66
- Conference [1..1] Presentation RelayQuality 66
- Conference [1..1] VideoBandwidth MainChannel Weight 66
- Conference [1..1] VideoBandwidth Mode 66
- Conference [1..1] VideoBandwidth PresentationChannel Weight 66

FacilityService settings 68
- FacilityService Service [1..5] CallType 68
- FacilityService Service [1..5] Name 68
- FacilityService Service [1..5] Number 68
- FacilityService Service [1..5] Type 68

H323 settings 69
- H323 NAT Address 69
- H323 NAT Mode 69
- H323 Profile [1..1] Authentication LoginName 69
- H323 Profile [1..1] Authentication Mode 69
- H323 Profile [1..1] Authentication Password 70
- H323 Profile [1..1] CallSetup Mode 70
- H323 Profile [1..1] Encryption KeySize 70
- H323 Profile [1..1] Gatekeeper Address 70
- H323 Profile [1..1] Gatekeeper Discovery 70
- H323 Profile [1..1] H323Alias E164 70
- H323 Profile [1..1] H323Alias ID 71
- H323 Profile [1..1] PortAllocation 71

Logging settings 72
- Logging Mode 72

Network settings 73
- Network [1..1] DHCP RequestTFTPServerAddress 74
- Network [1..1] DNS Domain Name 74
- Network [1..1] DNS Server [1..3] Address 74
- Network [1..1] IEEE8021X AnonymousIdentity 77
- Network [1..1] IEEE8021X Eap Md5 77
- Network [1..1] IEEE8021X Eap Peap 78
- Network [1..1] IEEE8021X Eap Tls 78
- Network [1..1] IEEE8021X Eap Ttls 78
- Network [1..1] IEEE8021X Identity 77

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..1] IEEE8021X Mode ... 76
Network [1..1] IEEE8021X Password ... 77
Network [1..1] IEEE8021X TlsVerify ... 77
Network [1..1] IEEE8021X UseClientCertificate ... 77
Network [1..1] IPStack ... 73
Network [1..1] IPv4 Address ... 73
Network [1..1] IPv4 Assignment ... 73
Network [1..1] IPv4 Gateway ... 73
Network [1..1] IPv4 SubnetMask ... 73
Network [1..1] IPv6 Address ... 74
Network [1..1] IPv6 Assignment ... 73
Network [1..1] IPv6 DHCPOptions ... 74
Network [1..1] IPv6 Gateway ... 74
Network [1..1] MTU ... 78
Network [1..1] QoS Diffserv Audio ... 75
Network [1..1] QoS Diffserv Data ... 75
Network [1..1] QoS Diffserv ICMPv6 ... 76
Network [1..1] QoS Diffserv NTP ... 76
Network [1..1] QoS Diffserv Signalling ... 76
Network [1..1] QoS Diffserv Video ... 75
Network [1..1] QoS Mode ... 75
Network [1..1] RemoteAccess Allow ... 79
Network [1..1] Speed ... 78
Network [1..1] TrafficControl Mode ... 78
Network [1..1] VLAN Voice Mode ... 79
Network [1..1] VLAN Voice VlanId ... 79

NetworkServices settings ... 80
NetworkServices CDP Mode ... 80
NetworkServices CTMS Encryption ... 84
NetworkServices CTMS Mode ... 83
NetworkServices H323 Mode ... 80
NetworkServices HTTP Mode ... 80
NetworkServices HTTPS Mode ... 81
NetworkServices HTTPS OCSP Mode ... 81
NetworkServices HTTPS OCSP URL ... 82
NetworkServices HTTPS VerifyClientCertificate ... 81
NetworkServices HTTPS VerifyServerCertificate ... 81
NetworkServices Medianet Metadata ... 82
NetworkServices MultiWay Address ... 81
NetworkServices MultiWay Protocol ... 81
NetworkServices NTP Address ... 82
NetworkServices NTP Mode ... 82
NetworkServices SIP Mode ... 80
NetworkServices SNMP CommunityName ... 83
NetworkServices SNMP Host [1..3] Address ... 82
NetworkServices SNMP Mode ... 82
NetworkServices SNMP SystemContact ... 83
NetworkServices SNMP SystemLocation ... 83
NetworkServices SSH AllowPublicKey ... 83
NetworkServices SSH Mode ... 83
NetworkServices Telnet Mode ... 80
NetworkServices UPnP Mode ... 84
NetworkServices UPnP Timeout ... 84
NetworkServices WelcomeText ... 80
NetworkServices XMLAPI Mode ... 80

Peripherals settings ... 85
Peripherals Pairing CiscoTouchPanels RemotePairing ... 85
Peripherals Profile TouchPanels ... 85

Phonebook settings ... 86
Phonebook Server [1..1] ID ... 86
Phonebook Server [1..1] Type ... 86
Phonebook Server [1..1] URL ... 86

Provisioning settings ... 87
Provisioning Connectivity ... 87
Provisioning ExternalManager Address ... 88
Provisioning ExternalManager AlternateAddress ... 88
Provisioning ExternalManager Domain ... 88
Provisioning ExternalManager Path ... 88
Provisioning ExternalManager Protocol ... 88
Provisioning HttpMethod ... 87
Provisioning LoginName ... 87
Provisioning Mode ... 87
Provisioning Password ... 87

RTP settings ... 89
RTP Ports Range Start ... 89
RTP Ports Range Stop ... 89

Security settings ... 90
Security Audit Logging Mode ... 90
Security Audit OnError Action ... 90
Security Audit Server Address ... 90
Security Audit Server Port ... 90
Security Audit Server PortAssignment ... 90
Security Session InactivityTimeout ... 91
Security Session ShowLastLogon ... 91

SerialPort settings ... 92
SerialPort LoginRequired ... 92
SerialPort Mode ... 92

SIP settings ... 93
SIP ANAT ... 93
SIP AuthenticateTransferror ... 93
SIP ListenPort ... 93
SIP OCSP DefaultResponder ... 93
SIP OCSP Mode ... 93
SIP PreferredIPMedia ... 93
SIP PreferredIPSignaling ... 93
SIP Profile [1..1] Authentication [1..1] LoginName ... 95
SIP Profile [1..1] Authentication [1..1] Password ... 95
SIP Profile [1..1] DefaultTransport ... 95
SIP Profile [1..1] DisplayName ... 95
SIP Profile [1..1] Ice DefaultCandidate ... 94
SIP Profile [1..1] Ice Mode ... 94
SIP Profile [1..1] Line ... 96
SIP Profile [1..1] Mailbox ... 96
SIP Profile [1..1] Outbound ... 96
SIP Profile [1..1] Proxy [1..4] Address ... 96
SIP Profile [1..1] Proxy [1..4] Discovery ... 96
SIP Profile [1..1] TlsVerify ... 95
SIP Profile [1..1] Turn BandwidthProbe ... 94
SIP Profile [1..1] Turn DiscoverMode ... 94
SIP Profile [1..1] Turn DropRflx ... 94
SIP Profile [1..1] Turn Password ... 95
SIP Profile [1..1] Turn Server ... 94
SIP Profile [1..1] Turn UserName ... 94
SIP Profile [1..1] Type ... 96
SIP Profile [1..1] URI ... 95

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Standby settings 97
Standby BootAction 97
Standby Control 97
Standby Delay 97
Standby StandbyAction 97
Standby WakeupAction 97

SystemUnit settings 98
SystemUnit CallLogging Mode 98
SystemUnit ContactInfo Type 98
SystemUnit MenuLanguage 98
SystemUnit Name 98

Time settings 99
Time DateFormat 99
Time OlsonZone 100
Time TimeFormat 99
Time Zone 99

UserInterface settings 102
UserInterface Language 102
UserInterface OSD EncryptionIndicator 102
UserInterface OSD LanguageSelection 102
UserInterface OSD LoginRequired 102
UserInterface OSD Output 102
UserInterface TouchPanel DefaultPanel 103
UserInterface UserPreferences 103
UserInterface Wallpaper 103

Video settings 104
Video AllowWebSnapshots 104
Video CamCtrlPip CallSetup Duration 104
Video CamCtrlPip CallSetup Mode 104
Video Input Connector [1..4] CameraControl CameraId 105
Video Input Connector [1..4] CameraControl Mode 105
Video Input Connector [1..4] InputSourceType 104
Video Input Connector [1..4] Name 104
Video Input Connector [1..4] OptimalDefinition Profile 106
Video Input Connector [1..4] OptimalDefinition Threshold60fps 106
Video Input Connector [1..4] Visibility 105
Video Input Connector [2..4] PresentationSelection 106
Video Input Connector [2..4] Quality 105
Video Input Connector [2..4] RGBQuantizationRange 107
Video Input Connector [2] DviType 107
Video Layout DisableDisconnectedLocalOutputs 107
Video Layout LocalLayoutFamily 107
Video Layout PresentationDefault View 108
Video Layout RemoteLayoutFamily 108
Video Layout ScaleToFrame 108
Video Layout ScaleToFrameThreshold 108
Video Layout Scaling 108
Video Monitors 110
Video OSD EncryptionIndicator 110
Video OSD LanguageSelection 110
Video OSD LoginRequired 110
Video OSD Output 110
Video Output Connector [1..2] Resolution 112
Video Output Connector [1] Brightness 111
Video Output Connector [1] Whitebalance Level 111
Video Output Connector [2] CEC Mode 111
Video Output Connector [2] Location HorizontalOffset 111
Video Output Connector [2] Location VerticalOffset 112
Video Output Connector [2] OverscanLevel 111
Video Output Connector [2] RGBQuantizatonRange 112
Video PIP ActiveSpeaker DefaultValue Position 109
Video PIP Presentation DefaultValue Position 109
Video SelfviewDefault FullscreenMode 110
Video SelfviewDefault Mode 109
Video SelfviewDefault OnMonitorRole 110
Video SelfviewDefault PIPPosition 110
Video SelfviewPosition 109
Video WallPaper 112

Experimental settings 113

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Audio settings

Audio Input Microphone [1] Mode

Set the audio input microphone mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the microphone connector.

On: Enable the microphone connector.

Example: `Audio Input Microphone 1 Mode: On`

Audio Microphones Mute Enabled

Determine whether audio-mute is allowed or not. The default value is True.

Requires user role: ADMIN

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.

Example: `Audio Microphones Mute Enabled: True`

Audio SoundsAndAlerts KeyTones Mode

The system can be configured to make a keyboard click sound effect (key tone) when typing text or numbers on the Touch controller.

Requires user role: USER

Value space: <Off/On>

Off: No key tones will be played when you type.

On: You will hear key tones when you type.

Example: `Audio SoundsAndAlerts KeyTones Mode: Off`

Audio SoundsAndAlerts RingTone

This setting defines which ringtone to use for incoming calls. You need to enter the exact name of the ringtone. You can find the available ringtones the following ways.

Web interface: On the Configuration > Personalization page.

Touch controller: On the Ringtone & Sound panel of the Settings menu. This panel is either in the open part of the Settings menu, or included in the password protected Administrator menu. The UserInterface UserPreference setting defines which panels will be in the password protected area.

Requires user role: USER

Value space: <S: 1, 100>

Format: String with a maximum of 100 characters.

Example: `Audio SoundsAndAlerts RingTone: "Sunrise"`

Audio SoundsAndAlerts RingVolume

Sets the ring volume for an incoming call.

Requires user role: USER

Value space: <0..100>

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

Example: `Audio SoundsAndAlerts RingVolume: 40`

Audio DefaultVolume

Set the default speaker volume. The volume returns 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.

Requires user role: USER

Value space: <0..100>

Range: The value must be between 0 and 100. The values from 1 to 100 correspond to the range from -34.5 dB to 15 dB (0.5 dB steps). The value 0 means that the audio is switched off.

Example: `Audio DefaultVolume: 50`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Cameras settings

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

Value space: <Auto/50Hz/60Hz>

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

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

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

Example: `Cameras PowerLine Frequency: Auto`

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

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.

Example: `Cameras Preset TriggerAutofocus: Auto`

Cameras Camera [1] Backlight

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

Value space: <Off/On>

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Example: `Cameras Camera 1 Backlight: Off`

Cameras Camera [1] Brightness Mode

Set the camera brightness mode.

Requires user role: ADMIN

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 Brightness Level setting.

Example: `Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1] Brightness Level

Set the brightness level. Requires the Camera Brightness Mode to be set to Manual.

Requires user role: ADMIN

Value space: <1..31>

Range: Select a value between 1 and 31.

Example: `Cameras Camera 1 Brightness Level: 20`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Cameras Camera [1] Focus Mode

Set the camera focus mode.

Requires user role: ADMIN

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.

Example: `Cameras Camera 1 Focus Mode: Auto`

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

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 [1..n] Gamma Level.

Example: `Cameras Camera 1 Gamma Mode: Auto`

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 Gamma Mode to be set to Manual.

Requires user role: ADMIN

Value space: <0..7>

Range: Select a value between 0 and 7.

Example: `Cameras Camera 1 Gamma Level: 0`

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

Value space: <Off/On>

Off: Display the image as other people see you.

On: Display the image as you see yourself in a mirror.

Example: `Cameras Camera 1 Mirror: Off`

Cameras Camera [1] Whitebalance Mode

Set the camera white balance mode.

Requires user role: ADMIN

Value space: <Auto/Manual>

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

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

Example: `Cameras Camera 1 Whitebalance Mode: Auto`

Cameras Camera [1] Whitebalance Level

Set the white balance level. Requires the Camera Whitebalance Mode to be set to manual.

Requires user role: ADMIN

Value space: <1..16>

Range: Select a value between 1 and 16.

Example: `Cameras Camera 1 Whitebalance Level: 1`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Conference settings

Conference [1..1] ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server using the video system's interfaces (not available from the TRC5 remote control and on-screen display). 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). Change this setting if you want to disable the active control features.

Requires user role: ADMIN

Value space: <Auto/Off>

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

Off: Active control is disabled.

Example: `Conference ActiveControl Mode: Auto`

Conference [1..1] CallProtocolIPStack

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

Requires user role: ADMIN

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.

Example: `Conference 1 CallProtocolIPStack: Dual`

Conference [1..1] AutoAnswer Mode

Set 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

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.

Example: `Conference 1 AutoAnswer Mode: Off`

Conference [1..1] AutoAnswer Mute

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

Requires user role: ADMIN

Value space: <Off/On>

Off: The incoming call will not be muted.

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

Example: `Conference 1 AutoAnswer Mute: Off`

Conference [1..1] 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

Value space: <0..50>

Range: Select a value between 0 and 50 seconds.

Example: `Conference 1 AutoAnswer Delay: 0`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Conference [1..1] MicUnmuteOnDisconnect Mode

Determine 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

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.

Example: `Conference 1 MicUnmuteOnDisconnect Mode: On`

Conference [1..1] 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 (Touch controller). The default value is 60 minutes.

Requires user role: ADMIN

Value space: <0..1440>

Range: Select the number of minutes (between 0 and 1440, i.e. 24 hours) before the Do Not Disturb session times out automatically.

Example: `Conference 1 DoNotDisturb DefaultTimeOut: 60`

Conference [1..1] 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

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.

Example: `Conference 1 FarEndControl Mode: On`

Conference [1..1] FarEndControl SignalCapability

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

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

Example: `Conference 1 FarEndControl SignalCapability: On`

Conference [1..1] 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

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.

Example: `Conference 1 Encryption Mode: BestEffort`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Conference [1..1] DefaultCall Protocol

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

Requires user role: ADMIN

Value space: <Auto/H323/Sip/H320>

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, or the call protocol is not enabled, the auto-selection chooses H323.

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

Sip: All calls are set up as SIP calls.

H320: All calls are set up as H.320 calls (only applicable if connected to a Cisco TelePresence ISDN Link gateway).

Example: `Conference 1 DefaultCall Protocol: Auto`

Conference [1..1] DefaultCall Rate

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

Requires user role: ADMIN

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 DefaultCall Rate: 1920`

Conference [1..1] MaxTransmitCallRate

Specify 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

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxTransmitCallRate: 6000`

Conference [1..1] MaxReceiveCallRate

Specify 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

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxReceiveCallRate: 6000`

Conference [1..1] MaxTotalTransmitCallRate

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

Specify 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

Value space: <64..10000>

Range: Select a value between 64 and 10000.

Example: `Conference 1 MaxTotalTransmitCallRate: 10000`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Conference [1..1] MaxTotalReceiveCallRate

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

Specify 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

Value space: <64..10000>

Range: Select a value between 64 and 10000.

Example: `Conference 1 MaxTotalReceiveCallRate: 10000`

Conference [1..1] VideoBandwidth Mode

Set the conference video bandwidth mode.

Requires user role: ADMIN

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.

Example: `Conference 1 VideoBandwidth Mode: Dynamic`

Conference [1..1] VideoBandwidth MainChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Value space: <1..10>

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth MainChannel Weight: 5`

Conference [1..1] VideoBandwidth PresentationChannel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "MainChannel Weight" and "PresentationChannel Weight". If the main channel weight is 2 and the presentation channel weight is 1, then the main channel will use twice as much bandwidth as the presentation channel.

Requires user role: ADMIN

Value space: <1..10>

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth PresentationChannel Weight: 5`

Conference [1..1] 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 (codec) 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

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.

Example: `Conference 1 Presentation RelayQuality: Sharpness`

Conference [1..1] Presentation OnPlacedOnHold

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

Requires user role: ADMIN

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.

Example: `Conference 1 Presentation OnPlacedOnHold: NoAction`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Conference [1..1] Multipoint Mode

Define how the video system handles multiparty video conferences.

If registered to a Cisco TelePresence Video Communication Server (VCS), the video system can either use its own built-in MultiSite feature, or it can rely on the MultiWay network solution. MultiWay requires that the video network includes a multipoint control unit (MCU).

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 one to use is set-up by CUCM.

Both MultiWay and the CUCM conference bridge allows you to set up conferences with many participants. The built-in MultiSite allows up to four participants (yourself included).

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

Requires user role: ADMIN

Value space: <Auto/Off/MultiSite/MultiWay/CUCMMediaResourceGroupList>

Auto: The multipoint method available will be choosen automatically; if none are available the Multipoint Mode will automatically be set to Off. If both MultiWay and MultiSite are available, the MultiWay service takes priority over the built-in MultiSite.

Off: Multiparty conferences are not allowed.

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

MultiWay: Multiparty conferences are set up using the MultiWay service. If MultiWay is chosen when the MultiWay service is not available, the Multipoint Mode will automatically be set to Off. This may occur when the NetworkServices MultiWay Address setting is empty or not properly set.

CUCMMediaResourceGroupList: Multiparty conferences (ad hoc 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.

Example: `Conference 1 Multipoint Mode: Auto`

Conference [1..1] IncomingMultisiteCall Mode

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

Requires user role: ADMIN

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 MultiSite or MultiWay support).

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.

Example: `Conference 1 IncomingMultisiteCall Mode: Allow`

www.cisco.com – Copyright © 2013–2015 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 Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 with Type Helpdesk is available on the Touch controller; the other options are available for system integrators using the API (Application Programming Interface) command set.

Requires user role: ADMIN

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

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

Concierge: Select this option for concierge services.

Helpdesk: Select this option for helpdesk services.

Emergency: Select this option for emergency services.

Security: Select this option for security services.

Catering: Select this option for catering services.

Transportation: Select this option for transportation services.

Example: `FacilityService Service 1 Type: Helpdesk`

FacilityService Service [1..5] Name

Enter 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 Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 is available on the Touch controller. The name will show on the facility service call button, which appears when you tap the question mark icon in the top bar. The other services are available for system integrators using the API (Application Programming Interface) command set.

Requires user role: ADMIN

Value space: <S: 0, 1024>

Format: String with a maximum of 1024 characters.

Example: `FacilityService Service 1 Name: ""`

FacilityService Service [1..5] Number

Enter 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 Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 is available on the Touch controller; the other options are available for system integrators using the API (Application Programming Interface) command set.

Requires user role: ADMIN

Value space: <S: 0, 1024>

Format: String with a maximum of 1024 characters.

Example: `FacilityService Service 1 Number: ""`

FacilityService Service [1..5] CallType

Set 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 Name and the FacilityService Service Number settings are properly set. Only FacilityService Service 1 is available on the Touch controller; the other options are available for system integrators using the API (Application Programming Interface) command set.

Requires user role: ADMIN

Value space: <Video/Audio>

Video: Select this option for video calls.

Audio: Select this option for audio calls.

Example: `FacilityService Service 1 CallType: Video`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

H323 settings

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

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.

Example: `H323 NAT Mode: Off`

H323 NAT Address

Enter 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

Value space: <S: 0, 64>

Format: A valid IPv4 address or IPv6 address.

Example: `H323 NAT Address: ""`

H323 Profile [1..1] Authentication Mode

Set the authentication mode for the H.323 profile.

Requires user role: ADMIN

Value space: <Off/On>

Off: If the H.323 Gatekeeper Authentication Mode is set to Off the system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

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

Example: `H323 Profile 1 Authentication Mode: Off`

H323 Profile [1..1] Authentication LoginName

The system sends the Authentication Login Name and the Authentication Password to a 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 Gatekeeper Authentication Mode to be enabled.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication LoginName: ""`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

H323 Profile [1..1] Authentication Password

The system sends the Authentication Login Name and the Authentication Password to a 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 Gatekeeper Authentication Mode to be enabled.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication Password: ""`

H323 Profile [1..1] CallSetup Mode

The H.323 Call Setup Mode defines whether to use a Gatekeeper or Direct calling when establishing H323 calls.

NOTE: Direct H.323 calls can be made even though the H.323 Call Setup Mode is set to Gatekeeper.

Requires user role: ADMIN

Value space: <Direct/Gatekeeper>

Direct: An IP address must be used when dialing in order to make the H323 call.

Gatekeeper: The system will use a Gatekeeper to make a H.323 call. When selecting this option the H323 Profile Gatekeeper Address and H323 Profile Gatekeeper Discovery settings must also be configured.

Example: `H323 Profile 1 CallSetup Mode: Gatekeeper`

H323 Profile [1..1] 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

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.

Example: `H323 Profile 1 Encryption MinKeySize: Max1024bit`

H323 Profile [1..1] Gatekeeper Discovery

Determine how the system shall register to a H.323 Gatekeeper.

Requires user role: ADMIN

Value space: <Manual/Auto>

Manual: The system will use a specific Gatekeeper identified by the Gatekeeper's IP address.

Auto: The system will automatically try to register to any available Gatekeeper. If a Gatekeeper responds to the request sent from the codec within 30 seconds this specific Gatekeeper will be used. This requires that the Gatekeeper is in auto discovery mode as well. If no Gatekeeper responds, the system will not use a Gatekeeper for making H.323 calls and hence an IP address must be specified manually.

Example: `H323 Profile 1 Gatekeeper Discovery: Manual`

H323 Profile [1..1] Gatekeeper Address

Enter the IP address of the Gatekeeper. Requires the H.323 Call Setup Mode to be set to Gatekeeper and the Gatekeeper Discovery to be set to Manual.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: A valid IPv4 address, IPv6 address or DNS name.

Example: `H323 Profile 1 Gatekeeper Address: "192.0.2.0"`

H323 Profile [1..1] 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

Value space: <S: 0, 30>

Format: Compact string with a maximum of 30 characters. Valid characters are 0-9, * and #.

Example: `H323 Profile 1 H323Alias E164: "90550092"`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

H323 Profile [1..1] H323Alias ID

Lets you specify 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. Example: "firstname.lastname@company.com", "My H.323 Alias ID"

Requires user role: ADMIN

Value space: <S: 0, 49>

Format: String with a maximum of 49 characters.

Example: `H323 Profile 1 H323Alias ID: "firstname.lastname@company.com"`

H323 Profile [1..1] PortAllocation

The H.323 Port Allocation setting affects the H.245 port numbers used for H.323 call signaling.

Requires user role: ADMIN

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].

Example: `H323 Profile 1 PortAllocation: Dynamic`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Logging settings

Logging Mode

Not applicable in this version.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network settings

Network [1..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

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.

Example: `Network 1 IPStack: Dual`

Network [1..1] IPv4 Assignment

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

Requires user role: ADMIN

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.

Example: `Network 1 IPv4 Assignment: DHCP`

Network [1..1] IPv4 Address

Enter the static IPv4 network address for the system. This setting is only applicable when Network Assignment is set to Static.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: A valid IPv4 address.

Example: `Network 1 IPv4 Address: "192.0.2.2"`

Network [1..1] IPv4 Gateway

Define the IPv4 network gateway. This setting is only applicable when the Network Assignment is set to Static.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: A valid IPv4 address.

Example: `Network 1 IPv4 Gateway: "192.0.2.1"`

Network [1..1] IPv4 SubnetMask

Define the IPv4 network subnet mask. This setting is only applicable when the Network Assignment is set to Static.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: The valid IPv4 address format.

Example: `Network 1 IPv4 SubnetMask: "255.255.255.0"`

Network [1..1] IPv6 Assignment

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

Requires user role: ADMIN

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.

Example: `Network 1 IPv6 Assignment: Autoconf`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..1] IPv6 Address

Enter the static IPv6 network address for the system. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: A valid IPv6 address.

Example: `Network 1 IPv6 Address: "2001:0DB8:0000:0000:0000:0000:0000:0002"`

Network [1..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

Value space: <S: 0, 64>

Format: A valid IPv6 address.

Example: `Network 1 IPv6 Gateway: "2001:0DB8:0000:0000:0000:0000:0000:0001"`

Network [1..1] IPv6 DHCPOptions

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

Requires user role: ADMIN

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.

Example: `Network 1 IPv6 DHCPOptions: On`

Network [1..1] DHCP RequestTFTPServerAddress

This setting is used only for video systems that are registered to a Cisco Unified Communications Manager (CUCM).

The setting determines whether the endpoint should ask the DHCP server for DHCP option 150, so that it can discover the address of the TFTP server (provisioning server) automatically.

If this setting is Off or the DHCP server does not support option 150, the TFTP server address must be set manually using the Provisioning ExternalManager Address setting.

If the Network VLAN Voice Mode setting is Auto and the Cisco Discovery Protocol (CDP) assigns an ID to the voice VLAN, then a request for option 150 will always be sent. That is, the Network DHCP RequestTFTPServerAddress setting will be ignored.

Requires user role: ADMIN

Value space: <Off/On>

Off: The video system will not send a request for DHCP option 150 and the address of the TFTP server must be set manually. See the note above for any exception to this rule.

On: The video system will send a request for option 150 to the DHCP server so that it can automatically discover the address of the TFTP server.

Example: `Network 1 DHCP RequestTFTPServerAddress: On`

Network [1..1] DNS Domain Name

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

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 DNS Domain Name: ""`

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

Define the network addresses for DNS servers. Up to 3 addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: A valid IPv4 address or IPv6 address.

Example: `Network 1 DNS Server 1 Address: ""`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..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

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.

Example: `Network 1 QoS Mode: Diffserv`

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv Audio: 0`

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv Video: 0`

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv Data: 0`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv Signalling: 0`

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv ICMPv6: 0`

Network [1..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

Value space: <0..63>

Range: Select a value between 0 to 63 - the higher the number, the higher the priority. The default value is 0 (best effort).

Example: `Network 1 QoS Diffserv NTP: 0`

Network [1..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

Value space: <Off/On>

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

On: The 802.1X authentication is enabled.

Example: `Network 1 IEEE8021X Mode: Off`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..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..1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN

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.

Example: `Network 1 IEEE8021X TlsVerify: Off`

Network [1..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

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.

Example: `Network 1 IEEE8021X UseClientCertificate: Off`

Network [1..1] IEEE8021X Identity

The 802.1X Identity is the user name needed for 802.1X authentication.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X Identity: ""`

Network [1..1] IEEE8021X Password

The 802.1X Password is the password needed for 802.1X authentication.

Requires user role: ADMIN

Value space: <S: 0, 32>

Format: String with a maximum of 32 characters.

Example: `Network 1 IEEE8021X Password: ""`

Network [1..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

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X AnonymousIdentity: ""`

Network [1..1] IEEE8021X Eap Md5

Set 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

Value space: <Off/On>

Off: The EAP-MD5 protocol is disabled.

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

Example: `Network 1 IEEE8021X Eap Md5: On`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..1] IEEE8021X Eap Ttls

Set 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

Value space: <Off/On>

Off: The EAP-TTLS protocol is disabled.

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

Example: `Network 1 IEEE8021X Eap Ttls: On`

Network [1..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

Value space: <Off/On>

Off: The EAP-TLS protocol is disabled.

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

Example: `Network 1 IEEE8021X Eap Tls: On`

Network [1..1] IEEE8021X Eap Peap

Set 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

Value space: <Off/On>

Off: The EAP-PEAP protocol is disabled.

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

Example: `Network 1 IEEE8021X Eap Peap: On`

Network [1..1] MTU

Set the Ethernet MTU (Maximum Transmission Unit).

Requires user role: ADMIN

Value space: <576..1500>

Range: Select a value between 576 and 1500 bytes.

Example: `Network 1 MTU: 1500`

Network [1..1] Speed

Set the Ethernet link speed.

Requires user role: ADMIN

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.

Example: `Network 1 Speed: Auto`

Network [1..1] TrafficControl Mode

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

Requires user role: ADMIN

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.

Example: `Network 1 TrafficControl: On`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Network [1..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

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `Network 1 RemoteAccess Allow: "10.11.2.3 192.168.0.0/24 2001:0db8:0000:0000:0000:ff00:0042:8329 2001:db8:abcd:0012::0/64"`

Network [1..1] VLAN Voice Mode

Set 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

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.

Example: `Network 1 VLAN Voice Mode: Auto`

Network [1..1] VLAN Voice VlanId

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

Requires user role: ADMIN

Value space: <1..4094>

Range: Select a value between 1 and 4094.

Example: `Network 1 VLAN Voice VlanId: 1`

www.cisco.com – Copyright © 2013–2015 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

Value space: <Off/On>

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

Example: `NetworkServices CDP Mode: On`

NetworkServices H323 Mode

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

Requires user role: ADMIN

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).

Example: `NetworkServices H323 Mode: On`

NetworkServices HTTP Mode

Set the HTTP mode to enable/disable access to the system through a web browser. The web interface is used for system management, call management such as call transfer, diagnostics and software uploads.

Requires user role: ADMIN

Value space: <Off/On>

Off: The HTTP protocol is disabled.

On: The HTTP protocol is enabled.

Example: `NetworkServices HTTP Mode: On`

NetworkServices SIP Mode

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

Requires user role: ADMIN

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).

Example: `NetworkServices SIP Mode: On`

NetworkServices Telnet Mode

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

Requires user role: ADMIN

Value space: <Off/On>

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

On: The Telnet protocol is enabled.

Example: `NetworkServices Telnet Mode: Off`

NetworkServices WelcomeText

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

Requires user role: ADMIN

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.

Example: `NetworkServices WelcomeText: On`

NetworkServices XMLAPI Mode

Not applicable in this version.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

NetworkServices MultiWay Address

The MultiWay address must be equal to the Conference Factory Alias, as configured on the Video Communication Server. The MultiWay™ conferencing enables video endpoint users to introduce a 3rd party into an existing call.

MultiWay™ can be used in the following situations:

1) When you want to add someone else in to your existing call.

2) When you are called by a 3rd party while already in a call and you want to include that person in the call.

Requirements: Video Communication Server (VCS) version X5 (or later) and Codian MCU version 3.1 (or later). Video systems invited to join the MultiWay™ conference must support the H.323 routeToMC facility message if in an H.323 call, or SIP REFER message if in a SIP call.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters (a valid dial URI).

Example: `NetworkServices MultiWay Address: "h323:multiway@company.com"`

NetworkServices MultiWay Protocol

Determine the protocol to be used for MultiWay calls.

Requires user role: ADMIN

Value space: <Auto/H323/Sip>

Auto: The system will select the protocol for MultiWay calls.

H323: The H323 protocol will be used for MultiWay calls.

Sip: The SIP protocol will be used for MultiWay calls.

Example: `NetworkServices MultiWay Protocol: Auto`

NetworkServices HTTPS Mode

HTTPS is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the web server.

Requires user role: ADMIN

Value space: <Off/On>

Off: The HTTPS protocol is disabled.

On: The HTTPS protocol is enabled.

Example: `NetworkServices HTTPS Mode: On`

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

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.

Example: `NetworkServices HTTPS VerifyServerCertificate: Off`

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

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.

Example: `NetworkServices HTTPS VerifyClientCertificate: Off`

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

Value space: <Off/On>

Off: Disable OCSP support.

On: Enable OCSP support.

Example: `NetworkServices HTTPS OCSP Mode: Off`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

NetworkServices HTTPS OCSP URL

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

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `NetworkServices HTTPS OCSP URL: "http://ocspserver.company.com:81"`

NetworkServices Medianet Metadata

Switch On or Off the capability to tag media flows with metadata related to the Cisco Medianet deployment.

Requires user role: ADMIN

Value space: <Off/On>

Off: Media flows will not be tagged with such metadata.

On: Media flows will be tagged with such metadata.

Example: `NetworkServices Medianet Metadata: Off`

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

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 Address setting will be used.

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

Off: The system will not use an NTP server. The Network Services NTP Address setting will be ignored.

Example: `NetworkServices NTP Mode: Auto`

NetworkServices NTP 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

Value space: <S: 0, 64>

Format: A valid IPv4 address, IPv6 address or DNS name.

Example: `NetworkServices NTP Address: "0.tandberg.pool.ntp.org"`

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

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.

Example: `NetworkServices SNMP Mode: ReadOnly`

NetworkServices SNMP Host [1..3] Address

Enter 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

Value space: <S: 0, 64>

Format: A valid IPv4 address, IPv6 address or DNS name.

Example: `NetworkServices SNMP Host 1 Address: ""`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

NetworkServices SNMP CommunityName

Enter 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

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP CommunityName: "public"`

NetworkServices SNMP SystemContact

Enter the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemContact: ""`

NetworkServices SNMP SystemLocation

Enter the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemLocation: ""`

NetworkServices SSH Mode

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

Requires user role: ADMIN

Value space: <Off/On>

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

Example: `NetworkServices SSH Mode: On`

NetworkServices SSH AllowPublicKey

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

Requires user role: ADMIN

Value space: <Off/On>

Off: The SSH public key is not allowed.

On: The SSH public key is allowed.

Example: `NetworkServices SSH AllowPublicKey: On`

NetworkServices CTMS Mode

This setting determines whether or not to allow multiparty conferences controlled by a Cisco TelePresence Multipoint Switch (CTMS).

Video systems are able to initiate or join non-encrypted multiparty conferences controlled by CTMS version 1.8 or later. Encrypted conferences are supported as from software versions CTMS 1.9.1. Encryption is addressed in the NetworkServices CTMS Encryption setting.

Requires user role: ADMIN

Value space: <Off/On>

Off: Multiparty conferencing via CTMS is prohibited.

On: Multiparty conferencing via CTMS is allowed.

Example: `NetworkServices CTMS Mode: On`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

NetworkServices CTMS Encryption

This setting indicates whether or not the video system supports encryption when participating in a multiparty meeting controlled by a Cisco TelePresence Multipoint Switch (CTMS).

CTMS allows three security settings for meetings: non-secure (not encrypted), best effort (encrypted if all participants support encryption, otherwise not encrypted) and secure (always encrypted).

Requires user role: ADMIN

Value space: <Off/BestEffort>

Off: The video system does not allow encryption and therefore cannot participate in a secure CTMS meeting (encrypted). When participating in a best effort CTMS meeting, the meeting will be downgraded to non-secure (not encrypted).

BestEffort: The video system can negotiate encryption parameters with CTMS and participate in a secure CTMS meeting (encrypted). Do not use this value if the CTMS version is older than 1.9.1.

Example: `NetworkServices CTMS Encryption: Off`

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.

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

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.

Example: `NetworkServices UPnP Mode: On`

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

Value space: <0..3600>

Range: Select a value between 0 and 3600 seconds.

Example: `NetworkServices UPnP Timeout: 600`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Peripherals settings

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

Value space: <Off/On>

Off: Remote pairing of Touch 10 is not allowed.

On: Remote pairing of Touch 10 is allowed.

Example: `Peripherals Pairing CiscoTouchPanels RemotePairing: On`

Peripherals Profile TouchPanels

Set the number of touch panels 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 panels does not match this setting, the diagnostics service will report it as an inconsistency. Note that only one Cisco Touch controller is supported in this version.

Requires user role: ADMIN

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

NotSet: No touch panel check is performed.

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

0-5: This number of Touch controllers should be connected to the video system.

Example: `Peripherals Profile TouchPanels: Minimum1`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Phonebook settings

Phonebook Server [1..1] ID

Enter a name for the external phone book.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Phonebook Server 1 ID: ""`

Phonebook Server [1..1] Type

Select the phonebook server type.

Requires user role: ADMIN

Value space: <VCS/TMS/Callway/CUCM>

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

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

Callway: Not applicable. Removed as from TC7.3.3.

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

Example: `Phonebook Server 1 Type: TMS`

Phonebook Server [1..1] URL

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

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `Phonebook Server 1 URL: "http://tms.company.com/tms/public/external/phonebook/phonebookservice.asmx"`

www.cisco.com – Copyright © 2013–2015 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

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.

Example: `Provisioning Connectivity: Auto`

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

Value space: <Off/TMS/VCS/CallWay/CUCM/Auto/Edge>

Off: The video system will not be configured by a provisioning system.

Auto: The provisioning server will automatically be selected by the video system.

TMS: The video system will be configured using TMS (Cisco TelePresence Management System).

VCS: The video system will be configured using VCS (Cisco TelePresence Video Communication Server).

Callway: Not applicable. Removed as from TC7.3.3.

CUCM: The video system will be configured using CUCM (Cisco Unified Communications Manager).

Edge: The system will connect to CUCM via the Collaboration Edge infrastructure.

Example: `Provisioning Mode: Auto`

Provisioning LoginName

This is the user name 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

Value space: <S: 0, 80>

Format: String with a maximum of 80 characters.

Example: `Provisioning LoginName: ""`

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

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Provisioning Password: ""`

Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

Requires user role: ADMIN

Value space: <GET/POST>

GET: Select GET when the provisioning server supports GET.

POST: Select POST when the provisioning server supports POST.

Example: `Provisioning HttpMethod: POST`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Provisioning ExternalManager Address

Enter 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

Value space: <S: 0, 64>

Format: A valid IPv4 address, IPv6 address or DNS name.

Example: `Provisioning ExternalManager Address: ""`

Provisioning ExternalManager AlternateAddress

Only applicable when the endpoint is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Enter 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

Value space: <S: 0, 64>

Format: A valid IPv4 address, IPv6 address or DNS name.

Example: `Provisioning ExternalManager AlternateAddress: ""`

Provisioning ExternalManager Protocol

Determine whether to use secure management or not.

Requires user role: ADMIN

Value space: <HTTP/HTTPS>

HTTP: Set to HTTP to disable secure management. Requires HTTP to be enabled in the NetworkServices HTTP Mode setting.

HTTPS: Set to HTTPS to enable secure management. Requires HTTPS to be enabled in the NetworkServices HTTPS Mode setting.

Example: `Provisioning ExternalManager Protocol: HTTP`

Provisioning ExternalManager Path

Set 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

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `Provisioning ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

Provisioning ExternalManager Domain

Enter the SIP domain for the VCS provisioning server.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: `Provisioning ExternalManager Domain: "any.domain.com"`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

RTP settings

RTP Ports Range Start

Specify 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

Value space: <1024..65438>

Range: Select a value between 1024 and 65438.

Example: `RTP Ports Range Start: 2326`

RTP Ports Range Stop

Specify the last RTP port in the range.

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

Value space: <1120..65535>

Range: Select a value between 1120 and 65535.

Example: `RTP Ports Range Stop: 2486`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Security settings

Security Audit Logging Mode

Determine 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

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.

Example: `Security Audit Logging Mode: Off`

Security Audit OnError Action

Determine 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

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.

Example: `Security Audit OnError Action: Ignore`

Security Audit Server Address

The audit logs are sent to a syslog server. Enter 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

Value space: <S: 0, 64>

Format: A valid IPv4 address or IPv6 address

Example: `Security Audit Server Address: ""`

Security Audit Server Port

The audit logs are sent to a syslog server. Enter the port of the syslog server that the system shall send its audit logs to. This setting is only relevant when Security Audit PortAssignment is set to Manual.

Requires user role: AUDIT

Value space: <0..65535>

Range: Select a value between 0 to 65535.

Example: `Security Audit Server Port: 514`

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

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.

Example: `Security Audit Server PortAssignment: Auto`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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

Value space: <Off/On>

On: Show information about the last session.

Off: Do not show information about the last session.

Example: `Security Session ShowLastLogon: Off`

Security Session InactivityTimeout

Determine how long the system will accept inactivity from the user before he is automatically logged out.

Requires user role: ADMIN

Value space: <0..10000>

Range: Select a value between 1 and 10000 seconds; or select 0 when inactivity should not enforce automatic logout.

Example: `Security Session InactivityTimeout: 0`

www.cisco.com – Copyright © 2013–2015 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

Value space: <Off/On>

Off: Disable the serial port.

On: Enable the serial port.

Example: `SerialPort Mode: On`

SerialPort LoginRequired

Determine if login shall be required when connecting to the serial port.

Requires user role: ADMIN

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.

Example: `SerialPort LoginRequired: On`

www.cisco.com – Copyright © 2013–2015 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

Value space: <Off/On>

Off: Disable ANAT.

On: Enable ANAT.

Example: `SIP ANAT: Off`

SIP AuthenticateTransferror

Not applicable in this version.

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). It is recommended to leave this setting at its default value.

Requires user role: ADMIN

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.

Example: `SIP ListenPort: On`

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

Value space: <IPv4/IPv6>

IPv4: The preferred IP version for media is IPv4.

IPv6: The preferred IP version for media is IPv6.

Example: `SIP PreferredIPMedia: IPv4`

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

Value space: <IPv4/IPv6>

IPv4: The preferred IP version for signaling is IPv4.

IPv6: The preferred IP version for signaling is IPv6.

Example: `SIP PreferredIPSignaling: IPv4`

SIP OCSP Mode

Not applicable in this version.

SIP OCSP DefaultResponder

Not applicable in this version.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

SIP Profile [1..1] Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the endpoints can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the endpoints. NOTE: ICE is not supported when registered to CUCM (Cisco Unified Communication Manager).

Requires user role: ADMIN

Value space: <Auto/Off/On>

Auto: When set to Auto, ICE will be enabled if a turn server is provided, otherwise ICE will be disabled.

Off: Set to Off to disable ICE.

On: Set to On to enable ICE.

Example: `SIP Profile 1 Ice Mode: Auto`

SIP Profile [1..1] Ice DefaultCandidate

This is the default IP address that the endpoint will receive media on until ICE has reached a conclusion about which media route to use (up to the first 5 seconds of a call.

Requires user role: ADMIN

Value space: <Host/Rflx/Relay>

Host: The endpoint will receive media on its own IP address.

Rflx: The endpoint will receive media on its public IP address as seen by the TURN server.

Relay: The endpoint will receive media on the IP address and port allocated on the TURN server, and is used as a fallback until ICE has concluded.

Example: `SIP Profile 1 Ice DefaultCandidate: Host`

SIP Profile [1..1] Turn DiscoverMode

Set 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

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.

Example: `SIP Profile Turn DiscoverMode: On`

SIP Profile [1..1] Turn BandwidthProbe

Not applicable in this version.

SIP Profile [1..1] 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

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.

Example: `SIP Profile Turn DropRflx: Off`

SIP Profile [1..1] Turn Server

This is the address of the TURN (Traversal Using Relay NAT) server that the endpoints will use. 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

Value space: <S: 0, 255>

Format: The preferred format is DNS SRV record (e.g. _turn._udp.<domain>), or it can be a valid IPv4 or IPv6 address.

Example: `SIP Profile 1 Turn Server: "_turn._udp.example.com"`

SIP Profile [1..1] Turn UserName

The user name needed for accessing the TURN server.

Requires user role: ADMIN

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Turn UserName: ""`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

SIP Profile [1..1] Turn Password

The password needed for accessing the TURN server.

Requires user role: ADMIN

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Turn Password: ""`

SIP Profile [1..1] 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

Value space: <S: 0, 255>

Format: String with maximum 255 characters and compliant with the SIP URI syntax.

Example: `SIP Profile 1 URI: "sip:firstname.lastname@company.com"`

SIP Profile [1..1] DisplayName

When configured the incoming call will report the DisplayName instead of the SIP URI.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

Example: `SIP Profile 1 DisplayName: ""`

SIP Profile [1..1] Authentication [1..1] LoginName

This is the user name part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Authentication 1 LoginName: ""`

SIP Profile [1..1] Authentication [1..1] Password

This is the password part of the credentials used to authenticate towards the SIP proxy.

Requires user role: ADMIN

Value space: <S: 0, 128>

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Authentication 1 Password: ""`

SIP Profile [1..1] DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

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.

Example: `SIP Profile 1 DefaultTransport: Auto`

SIP Profile [1..1] 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

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.

Example: `SIP Profile 1 TlsVerify: Off`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

SIP Profile [1..1] Outbound

Turn on or off the client initiated connections mechanism for firewall traversal, connection reuse and redundancy. The current version supports RFC 5626.

Requires user role: ADMIN

Value space: <Off/On>

Off: Connect to the single proxy configured first in Proxy Address list.

On: Set up multiple outbound connections to servers in the Proxy Address list. A random proxy is selected from the list for each SIP outbound request.

Example: `SIP Profile 1 Outbound: Off`

SIP Profile [1..1] Proxy [1..4] Address

The Proxy Address is the manually configured address for the outbound proxy. The default port is 5060 for TCP and UDP but another one can be provided.

If SIP Profile Outbound is enabled, multiple proxies can be addressed.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: If SIP Profile Outbound is enabled, use a fully qualified domain name. If SIP Profile Outbound is disabled, you can also use a valid IPv4 address or IPv6 address.

Example: `SIP Profile 1 Proxy 1 Address: ""`

SIP Profile [1..1] Proxy [1..4] Discovery

Select if the SIP Proxy address is to be obtained manually or by using Dynamic Host Configuration Protocol (DHCP).

Requires user role: ADMIN

Value space: <Auto/Manual>

Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).

Manual: When Manual is selected, the manually configured SIP Proxy address will be used.

Example: `SIP Profile 1 Proxy 1 Discovery: Manual`

SIP Profile [1..1] Type

Enables SIP extensions and special behavior for a vendor or provider.

Requires user role: ADMIN

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.

Example: `SIP Profile 1 Type: Standard`

SIP Profile [1..1] Mailbox

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox. Enter the number (address) of the mailbox in this setting, or leave the string empty if you do not have a voice mailbox.

Requires user role: ADMIN

Value space: <S: 0, 255>>

Format: String with a maximum of 255 characters.

Example: `SIP Profile 1 Mailbox: "12345678"`

SIP Profile [1..1] 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

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).

Example: `SIP Profile 1 Line: Private`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Standby settings

Standby Control

Determine whether the system should go into standby mode or not.

Requires user role: ADMIN

Value space: <Off/On>

Off: The system will not enter standby mode.

On: Enter standby mode when the Standby Delay has timed out. Requires the Standby Delay to be set to an appropriate value.

Example: `Standby Control: On`

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

Value space: <1..480>

Range: Select a value between 1 and 480 minutes.

Example: `Standby Delay: 10`

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN

Value space: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None: No action.

Preset1 to Preset15: After a reboot the camera position will be set to the position defined by the selected preset.

RestoreCameraPosition: After a reboot the camera position will be set to the position it had before the last boot.

DefaultCameraPosition: After a reboot the camera position will be set to the factory default position.

Example: `Standby BootAction: DefaultCameraPosition`

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN

Value space: <None/PrivacyPosition>

None: No action.

PrivacyPosition: Turns the camera to a sideways position for privacy.

Example: `Standby StandbyAction: PrivacyPosition`

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN

Value space: <None/Preset1/Preset2/Preset3/Preset4/Preset5/Preset6/Preset7/Preset8/Preset9/Preset10/Preset11/Preset12/Preset13/Preset14/Preset15/RestoreCameraPosition/DefaultCameraPosition>

None: No action.

Preset1 to Preset15: When leaving standby the camera position will be set to the position defined by the selected preset.

RestoreCameraPosition: When leaving standby the camera position will be set to the position it had before entering standby.

DefaultCameraPosition: When leaving standby the camera position will be set to the factory default position.

Example: `Standby WakeupAction: RestoreCameraPosition`

www.cisco.com – Copyright © 2013–2015 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.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

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `SystemUnit Name: "Meeting Room"`

SystemUnit MenuLanguage

This has been replaced with the UserInterface Language setting.

SystemUnit CallLogging Mode

Set the call logging mode for calls that are received or placed by the system. The call logs may then be viewed via the web interface.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable logging.

On: Enable logging.

Example: `SystemUnit CallLogging Mode: On`

SystemUnit ContactInfo Type

Choose which type of contact information to show in the status field in the upper left corner of the Touch controller.

Requires user role: ADMIN

Value space: <Auto/None/IPv4/IPv6/H323Id/E164Alias/H320Number/SipUri/SystemName/DisplayName>

Auto: Show the address which another system can dial to reach this system. The address depends on the default call protocol and system registration.

None: Do not show any contact information in the status field.

IPv4: Show the IPv4 address as contact information.

IPv6: Show the IPv6 address as contact information.

H323Id: Show the H.323 ID as contact information (see the H323 Profile [1..1] H323Alias ID setting).

E164Alias: Show the H.323 E164 Alias as contact information (see the H323 Profile [1..1] H323Alias E164 setting).

H320Number: Show the H.320 number as contact information (only applicable if connected to a Cisco TelePresence ISDN Link gateway).

SipUri: Show the SIP URI as contact information (see the SIP Profile [1..1] URI setting).

SystemName: Show the system name as contact information (see the SystemUnit Name setting).

DisplayName: Show the display name as contact information (see the SIP Profile [1..1] DisplayName setting).

Example: `SystemUnit ContactInfo Type: Auto`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Time settings

Time TimeFormat

Set the time format.

Requires user role: USER

Value space: <24H/12H>

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours (AM/PM).

Example: `Time TimeFormat: 24H`

Time DateFormat

Set the date format.

Requires user role: USER

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

Example: `Time DateFormat: DD_MM_YY`

Time Zone

This has been replaced with the Time OlsonZone setting as of software version TC7.2.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Time OlsonZone

Set 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: USER

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_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/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/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, 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/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Ujung_Pandang, Asia/Ulaanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/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/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn,

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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/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/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>

Range: Select a time zone from the list.

Example: `Time OlsonZone: Etc/UTC`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

UserInterface settings

UserInterface Language

Select the language to be used in menus and messages on the screen and Touch controller. The default language is English.

Requires user role: USER

Value space: <English/ChineseSimplified/ChineseTraditional/Catalan/Czech/Danish/Dutch/Finnish/French/German/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/Swedish/Turkish/Arabic/Hebrew>

Range: Select a language from the list.

Example: `UserInterface Language: English`

UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator (a padlock) will be shown on screen. The setting applies to both encrypted and non-encrypted calls, i.e. both to secure and non-secure conferences. 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

Value space: <Auto/AlwaysOn/AlwaysOff>

Auto: If the Conference Encryption Mode setting is set to BestEffort and the call is encrypted, the encryption indicator is shown during the first seconds of a call. If the Conference Encryption Mode setting is set to BestEffort and the call is non-encrypted, the crossed out encryption indicator is shown during the entire call. If the Conference Encryption Mode setting is NOT set to BestEffort, the encryption indicator is not shown at all.

AlwaysOn: The encryption indicator is displayed on screen during the entire call. This applies to both encrypted and non-encrypted calls for all Conference Encryption Mode settings.

AlwaysOff: The encryption indicator is never displayed on screen. This applies to both encrypted and non-encrypted calls for all Conference Encryption Mode settings.

Example: `UserInterface OSD EncryptionIndicator: Auto`

UserInterface OSD LanguageSelection

In cases where you want to prevent users from easily changing the language settings from the Settings menu, the language settings can be made available from within the Administrator Settings menu. The administrator settings can be password protected.

Requires user role: ADMIN

Value space: <Off/On>

Off: The language is set from the Administrator Settings menu.

On: The language is set from the Settings menu.

Example: `UserInterface OSD LanguageSelection: On`

UserInterface OSD LoginRequired

Not applicable in this version.

UserInterface OSD Output

Define on which monitor the on-screen information and indicators should be displayed.

Requires user role: ADMIN

Value space: <Auto/1/2>

Auto: The system will send the information and indicators to the system's integrated LCD display.

Range 1-2: The system will send the information and indicators to the specified output. Choose 1 to send the 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.

Example: `UserInterface OSD Output: Auto`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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 2 MByte.

Requires user role: USER

Value space: <None/Custom>

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.

Example: `UserInterface Wallpaper: None`

UserInterface TouchPanel DefaultPanel

Define what (contact list, meeting list, or dial pad) the Touch controller will display on wake up.

Requires user role: USER

Value space: <None/LastUsed/ContactList/MeetingList/Dialpad>

None: None of the below options will appear as default on the Touch controller.

LastUsed: The last used (contact list, meeting list, or dial pad) will appear as default on the Touch controller.

ContactList: The contact list (favorites, directory and history) will appear as default on the Touch controller.

MeetingList: The list of scheduled meetings will appear as default on the Touch controller.

DialPad: The dial pad will appear as default on the Touch controller.

Example: `UserInterface TouchPanel DefaultPanel: None`

UserInterface UserPreferences

Some user preferences (ringtone, volume, language, date and time, etc) can be made available from the Settings menu, or from the Settings > Administrator menu on the Touch controller. Accessing the Administrator menus requires that the user has admin privileges.

Requires user role: ADMIN

Value space: <Off/On>

Off: The user preferences are available from the Settings > Administrator menu on the Touch controller, for users with admin privileges.

On: The user preferences are available from the Settings menu on the Touch controller.

Example: `UserInterface UserPreferences: Off`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Video settings

Video AllowWebSnapshots

Note: This setting is only available in TC7.3.0 to TC7.3.2.

Allow or disallow snapshots being taken of the local input sources, remote sites and presentation channel. If snapshots are allowed, the snapshots may be captured both when idle and in a call.

When snapshots are taken from a remote device, e.g. the web interface, a notification appears on the video system's screens to alert the users that remote monitoring is in operation.

Requires user role: ADMIN

Value space: <Off/On/LocalDeviceOnly>

Off: It is not possible to capture snapshots.

On: Snapshots can be captured and displayed anywhere, e.g. on the web interface.

LocalDeviceOnly: Snapshots can only be captured and displayed on devices running the experimental Cisco Proximity feature. The devices must be in the same room as the video system. It will not be possible to take and see snapshots on the web interface or by using 3rd party integrations.

Example: `Video AllowWebSnapshots: LocalDeviceOnly`

Video CamCtrlPip CallSetup Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video CamCtrlPip CallSetup Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN

Value space: <Off/On>

Off: self-view is not shown automatically during call setup.

On: self-view is shown automatically during call setup.

Example: `Video CamCtrlPip CallSetup Mode: On`

Video CamCtrlPip CallSetup Duration

This setting only has an effect when the Video CamCtrlPip CallSetup 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

Value space: <1..60>

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

Example: `Video CamCtrlPip CallSetup Duration: 10`

Video Input Connector [1..4] Name

Enter a name for the video input connector.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `Video Input Connector 1 Name: ""`

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

Value space: Connector 1: <camera> Other connectors: <other/camera/PC/DVD/document_camera/whiteboard>

other: Use this when none of the below options match.

camera: Use this when a camera is connected to the video input.

PC: Use this when a computer is connected to the video input.

DVD: Use this when a DVD player is connected to the video input.

document_camera: Use this when a document camera is connected to the video input.

whiteboard: Use this when a whiteboard camera is connected to the video input.

Example: `Video Input Connector 2 InputSourceType: PC`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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.

> The default value is Always for Video Input Connector 2 Visibility (the DVI connector).

> The default value is IfSignal for Video Input Connector 3,4 Visibility.

Requires user role: ADMIN

Value space: Connector 1: <Never> Other connectors: <Never/Always/IfSignal>

Never: When the input source is not expected to be used as a presentation source, set to Never.

Always: When set to Always, the menu selection for the video input connector will always be visible on the graphical user interface.

IfSignal: When set to IfSignal, the menu selection for the video input connector will only be visible when something is connected to the video input.

Example: `Video Input Connector 2 Visibility: Always`

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

Value space: Connector 1: <Off/On> Connector 2,3,4: <Off>

Off: Disable camera control.

On: Enable camera control.

Example: `Video Input Connector 1 CameraControl Mode: On`

Video Input Connector [1..4] CameraControl CameraId

Define the camera ID. This value is fixed and cannot be changed.

Requires user role: ADMIN

Value space: <1>

Range: This value is fixed and cannot be changed.

Example: `Video Input Connector 1 CameraControl CameraId: 1`

Video Input Connector [2..4] Quality

When encoding and transmitting video there will be 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.

Requires user role: ADMIN

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.

Example: `Video Input Connector 3 Quality: Sharpness`

www.cisco.com – Copyright © 2013–2015 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 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. In good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate. 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.

Some typical resolutions used for different optimal definition profiles, call rates and transmit frame rates are shown in the table below. The resolution must be supported by both the calling and called systems. Use the Video Input Source OptimalDefinition Threshold60fps setting to decide when to use the 60 fps frame rate.

Typical resolutions used for different optimal definition profiles, call rates and frame rates

Frame rate	Optimal Definition Profile	Call rate						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*Normal*	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	*Normal*	256×144	512×288	768×448	1024×576	1280×720	1280×720	1920×1080
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
	High	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

Requires user role: ADMIN

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.

Example: `Video Input Connector 1 OptimalDefinition Profile: Medium`

Video Input Connector [1..4] OptimalDefinition Threshold60fps

For each video input, this setting tells the system the lowest resolution where it should transmit 60fps. So for all resolutions lower than this, the maximum transmitted frame rate would be 30fps, while above this resolution 60fps would also be possible, if the available bandwidth is adequate.

Requires user role: ADMIN

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.

Example: `Video Input Connector 1 OptimalDefinition Threshold60fps: 1280_720`

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. Note that sharing the presentation with the far end always requires additional action (press Share on the user interface).

Requires user role: ADMIN

Value space: <Manual/Automatic/OnConnect>

Manual: In manual mode, the contents of the video input will not be presented on the screen until you choose it from the user interface.

Automatic: In automatic mode, the contents on the video input will be presented on screen automatically. If more than one source is set to Automatic, the last connected source will be used. If any content is active (presented) when a call is disconnected, the content will still be displayed locally.

OnConnect: When in on-connect mode, the content on the video input will be presented on screen when a cable is connected. Otherwise, the behavior is the same as in manual mode.

Example: `Video Input Connector 2 PresentationSelection: OnConnect`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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. The default value is set to Full because most sources expects full quantization range.

Requires user role: ADMIN

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.

Example: `Video Input Connector 2 RGBQuantizationRange: Full`

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

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.

Example: `Video Input Connector 2 DviType: AutoDetect`

Video Layout DisableDisconnectedLocalOutputs

This setting is fixed to On.

Requires user role: ADMIN

Value space: <On>

On: The built-in layout engine does only set layout on local outputs having a monitor connected.

Example: `Video Layout DisableDisconnectedLocalOutputs: On`

Video Layout LocalLayoutFamily

Select which video layout family to use locally.

Requires user role: ADMIN

Value space: <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/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.

FullScreen: Do not use this value.

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.

PresentationSmallSpeaker: Do not use this value.

PresentationLargeSpeaker: Do not use this value.

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.

Example: `Video Layout LocalLayoutFamily: Auto`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Video Layout PresentationDefault View

Determine how the presentation will show on screen when you start sharing a presentation.

Requires user role: ADMIN

Value space: <Default/Minimized/Maximized>

Default: The presentation is a part of the layout.

Minimized: The presentation starts up in PIP mode.

Maximized: The presentation starts up in full screen mode.

Example: `Video Layout PresentationDefault View: Default`

Video Layout RemoteLayoutFamily

Select which video layout family to be used for the remote participants.

Requires user role: ADMIN

Value space: <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker/Prominent/Overlay/Single>

Auto: The default layout family, as given by the local layout database, will be used as the remote layout.

FullScreen: Do not use this value.

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.

PresentationSmallSpeaker: Do not use this value.

PresentationLargeSpeaker: Do not use this value.

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.

Example: `Video Layout RemoteLayoutFamily: Auto`

Video Layout Scaling

Define how the system shall adjust the aspect ratio for images or frames when there is a difference between the image and the frame it is to be placed in.

Requires user role: ADMIN

Value space: <Off/On>

Off: No adjustment of the aspect ratio.

On: Let the system automatically adjust aspect ratio.

Example: `Video Layout Scaling: On`

Video Layout ScaleToFrame

Define what to do if the aspect ratio of a video input source doesn't match the aspect ratio of the corresponding image frame in a composition. For example if you have a 4:3 input source (like XGA) to be displayed on a 16:9 output (like HD720).

Requires user role: ADMIN

Value space: <Manual/MaintainAspectRatio/StretchToFit>

Manual: If the difference in aspect ratio between the video input source and the target image frame is less than the Video Layout ScaleToFrameThreshold setting (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.

MaintainAspectRatio: Maintain the aspect ratio of the input source, and fill in black in the rest of the frame (letter boxing or pillar boxing).

StretchToFit: Stretch (horizontally or vertically) the input source to fit into the image frame. NOTE: The general limitation is that you cannot upscale in one direction and at the same time downscale in the other direction. In such situations the codec will apply letterboxing.

Example: `Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

Only applicable if the Video Layout ScaleToFrame setting is set to manual. If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold setting (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value between 0 and 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Video PIP ActiveSpeaker DefaultValue Position

Determine 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 (see the Video Layout LocalLayoutFamily 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

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.

Example: `Video PIP ActiveSpeaker DefaultValue Position: Current`

Video PIP Presentation DefaultValue Position

Determine 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 Touch controller. 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

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.

CentreRight: 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.

Example: `Video PIP Presentation DefaultValue Position: Current`

Video SelfviewPosition

Select where the small self-view PiP (Picture-in-Picture) will appear on screen.

This setting is obsoleted by the Video SelfviewDefault PIPPosition setting.

Requires user role: ADMIN

Value space: <UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight>

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 of the screen.

UpperRight: The self-view PiP will appear in the upper right corner of the screen.

CenterLeft: The self-view PiP will appear on the left side of the screen, in center.

CenterRight: The self-view PiP will appear on the right side of the screen, in center.

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.

Example: `Video SelfviewPosition: CenterRight`

Video SelfviewDefault Mode

Determine 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 SelfviewDefault PIPPosition and the Video SelfviewDefault FullscreenMode settings respectively.

Requires user role: ADMIN

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.

Example: `Video SelfviewDefault Mode: Current`

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Video SelfviewDefault FullscreenMode

Determine 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 SelfviewDefault Mode setting).

Requires user role: ADMIN

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.

Example: `Video SelfviewDefault FullscreenMode: Current`

Video SelfviewDefault PIPPosition

Determine 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 SelfviewDefault Mode setting) and fullscreen view is switched off (see the Video SelfviewDefault FullscreenMode setting).

Requires user role: ADMIN

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.

Example: `Video SelfviewDefault PIPPosition: Current`

Video SelfviewDefault OnMonitorRole

Determine which monitor/output to display the main video source (self-view) on after a call.

Requires user role: ADMIN

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.

Example: `Video SelfviewDefault OnMonitorRole: Current`

Video Monitors

Set 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

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.

Example: `Video Monitors: Auto`

Video OSD LanguageSelection

This has been replaced with the UserInterface OSD LanguageSelection setting.

Video OSD EncryptionIndicator

This has been replaced with the UserInterface OSD EncryptionIndicator setting.

Video OSD Output

This has been replaced with the UserInterface OSD Output setting.

Video OSD LoginRequired

This has been replaced with the UserInterface OSD LoginRequired setting.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Video Output Connector [1] Brightness

Set the brightness level for the video system's LCD screen. The default value is 50.

Requires user role: USER

Value space: <0..100>

Range: The value must be between 0 and 100.

Example: `Video Output Connector 1 Brightness: 80`

Video Output Connector [1] Whitebalance Level

The LCD display's color temperature (white balance) is adjustable from 4000 K (warm) to 9000 K (cool). The default value is 6500 K.

Requires user role: USER

Value space: <4000..9000>

Range: The value must be between 4000 and 9000.

Example: `Video Output Connector 1 Whitebalance Level: 6500`

Video Output Connector [2] CEC Mode

This video output (HDMI) supports Consumer Electronics Control (CEC). When this setting is On (default is Off), 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

Value space: <Off/On>

Off: Disable CEC control

On: Enable CEC control

Example: `Video Output Connector 2 CEC Mode: Off`

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

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.

Example: `Video Output Connector 2 OverscanLevel: None`

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 LCD 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

Value space: <-100..100>

Range: The value must be between -100 and 100.

Example: `Video Output Connector 2 Location HorizontalOffset: 1`

www.cisco.com – Copyright © 2013–2015 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 LCD 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

Value space: <-100..100>

Range: The value must be between -100 and 100.

Example: `Video Output Connector 2 Location Vertical Offset: 0`

Video Output Connector [2] RGBQuantizatonRange

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. The default value is set to Full because most HDMI displays expects full quantization range.

Requires user role: ADMIN

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.

Example: `Video Output Connector 2 RGBQuantizatonRange: Full`

Video Output Connector [1..2] Resolution

Connector 1 (integrated LCD display): This value is fixed and cannot be changed.

Connector 2: Set the resolution and refresh rate for the monitor that is connected to the video system's HDMI output.

Requires user role: ADMIN

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.

1024_768_60: The resolution is 1024 x 768, and the refresh rate is 60 Hz.

1280_1024_60: The resolution is 1280 x 1024, and the refresh rate is 60 Hz.

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.

1280_768_60: The resolution is 1280 x 768, and the refresh rate is 60 Hz.

1360_768_60: The resolution is 1360 x 768, and the refresh rate is 60 Hz.

1366_768_60: The resolution is 1366 x 768, and the refresh rate is 60 Hz.

Example: `Video Output Connector 2 Resolution: Auto`

Video WallPaper

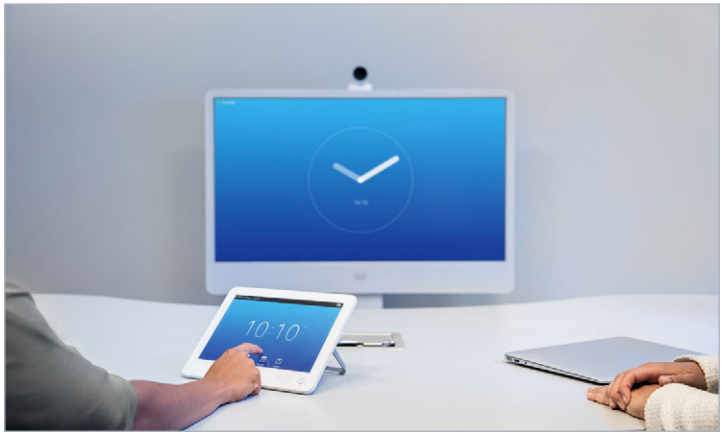
This has been replaced with the UserInterface Wallpaper setting.

www.cisco.com – Copyright © 2013–2015 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 © 2013–2015 Cisco Systems, Inc. All rights reserved.



Chapter 4

Setting passwords

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Setting the system password

The system password protects the video system. You have to sign in to be able to use the web interface, and to get access to the Administrator settings from a Touch 10 user interface.

The *admin* user

The video system is delivered with a default user account with full credentials. The user name is *admin*, and initially, no password is set for the default user.

It is mandatory to set a password for the *admin* user in order to restrict access to system configuration. Also set a password for any other user with similar credentials.

Make sure to keep a copy of the password in a safe place. You have to factory reset the unit if you have forgotten the password.

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

Other user accounts

You can create as many user accounts as you like for your video system.

You can read more about how to create and manage user accounts in the User administration section.

Changing your own system password

Perform the following steps to change the system password.

If a password is currently not set, use a blank *Current password*; to remove a password, leave the *New password* fields blank.

1. Sign in to the web interface with your user name and current password.
2. Click your user name in the upper right corner and choose *Change password* in the drop down menu.
3. Enter the *Current password*, the *New password*, and repeat the new password in the appropriate input fields.

   The password format is a string with 0–64 characters.
4. Click *Change password*.

Changing another user's system password

If you have administrator access rights, you can change all users' passwords by performing the following steps:

1. Sign in to the web interface with your user name and password.
2. Go to the *Configuration* tab and select *User Administration*.
3. Choose the appropriate user from the list.
4. Enter a new password and PIN code.
5. Click *Save*.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Appendices

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Connecting the Touch 10 user interface (page 1 of 3)

The Touch 10 user interface must either be directly connected to the MX200 G2 or MX300 G2 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.

The procedures in this chapter apply to all MX200 G2 and MX300 G2 video systems.

Connecting Touch 10 directly to the video system

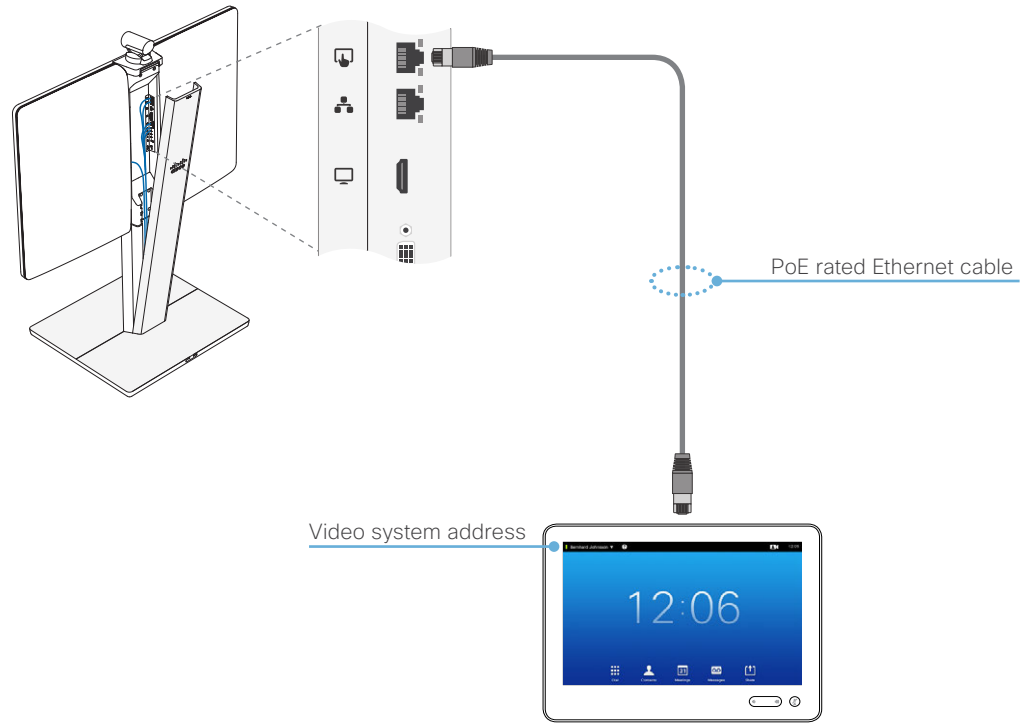
Connect Touch 10 to the video system's PoE injector as illustrated.

Touch 10 set-up

Once Touch 10 is connected, 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.

You can verify that Touch 10 is successfully connected to the video system by checking that the video system's address is displayed in the top banner.



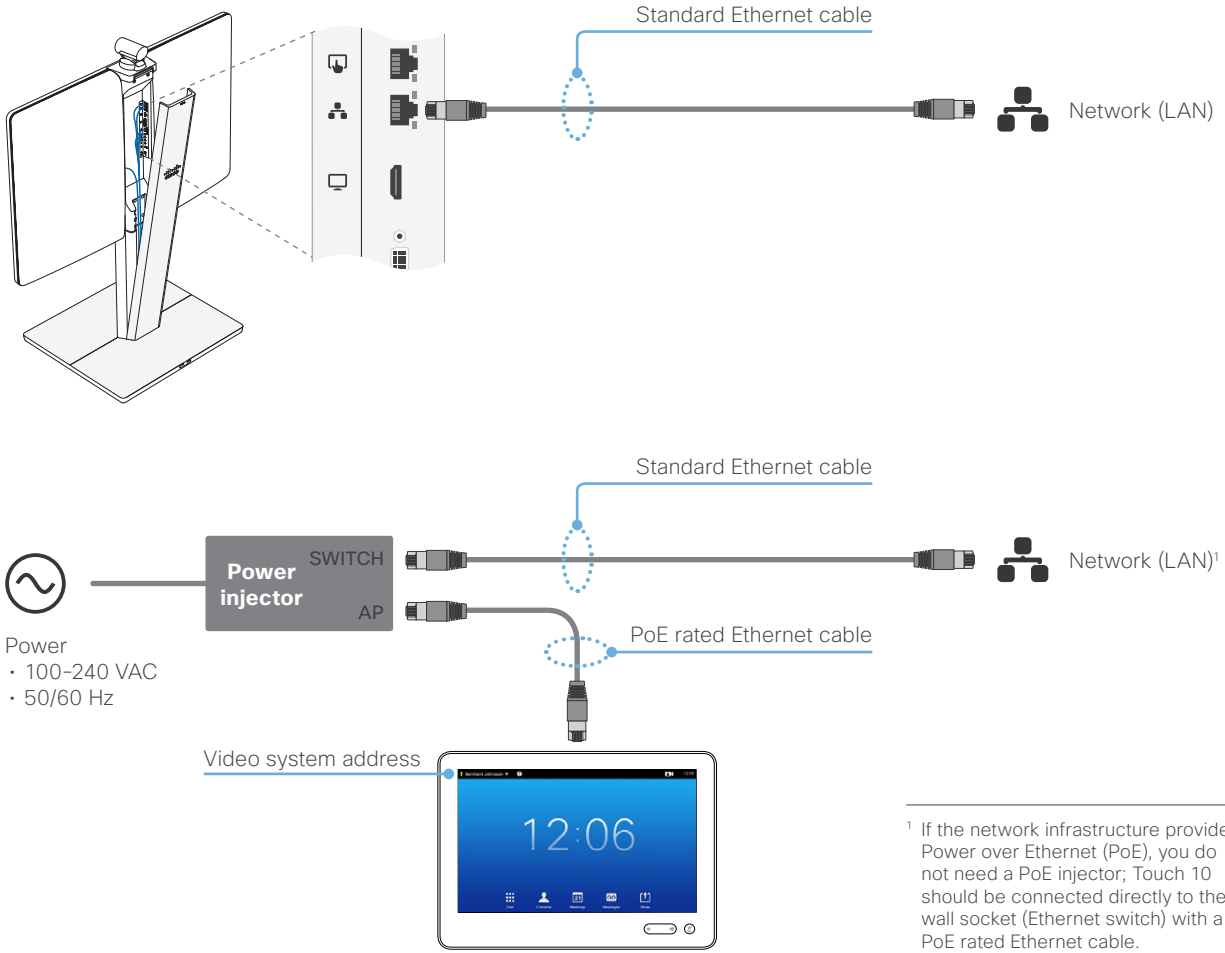
The Ethernet connector is behind the lid at the rear of Touch 10.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Connecting the Touch 10 user interface (page 2 of 3)

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

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



The Ethernet connector is behind the lid at the rear of Touch 10.

Touch 10 set-up

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

When the *Select codec to pair with* dialog appears, note the following:

- A list of video systems signalling that they are available for paring will show up in the dialog. Tap the name of the system you want to pair to followed by *Start Pairing*.

  The following is required for the video system to appear in the list:

  - Video system and Touch 10 on the same subnet.
  - Video system restarted recently (because the video system advertises that it is available for pairing only for a short period of time after it is switched on, refer to the *NetworkServices.> UPnP* settings).
- If your video system does not appear in the list of available codecs, you can pair the devices manually. Click *Select codec manually...*, enter the IP address or host name of the video system, and tap *Start Pairing*.
- You have to enter the video system's administrator username and password for the paring to commence.

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.

You can verify that Touch 10 is successfully connected to the video system by checking that the video system's address is displayed in the top banner.

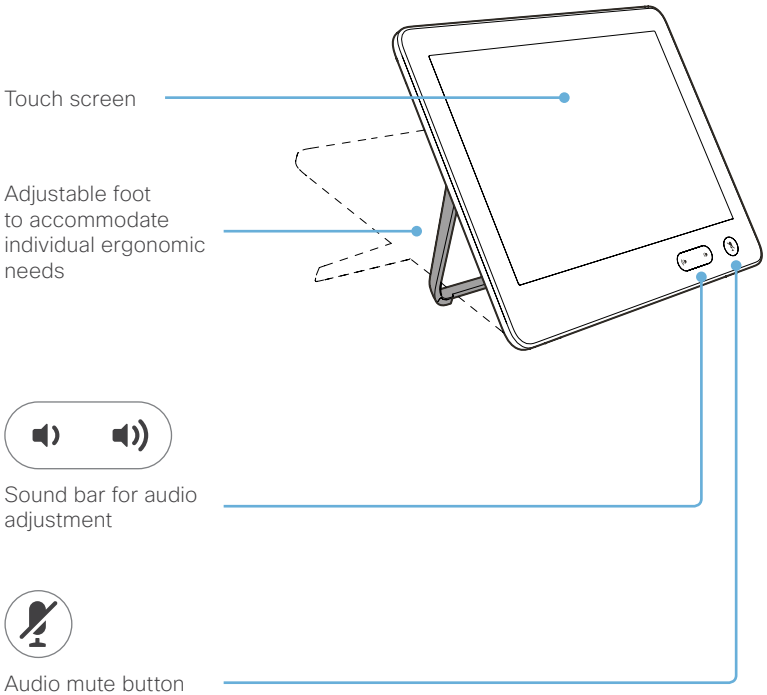
[1] If the network infrastructure provides Power over Ethernet (PoE), you do not need a PoE injector; Touch 10 should be connected directly to the wall socket (Ethernet switch) with a PoE rated Ethernet cable.

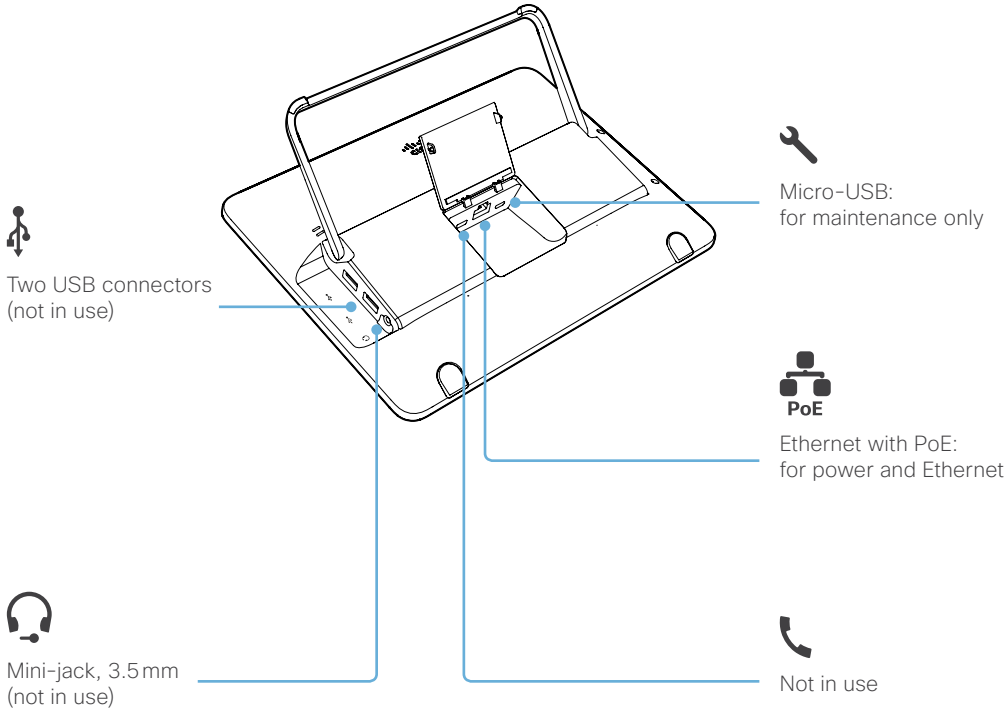
For safety, the PoE source must be in the same building as Touch 10. The PoE rated Ethernet cable can be up to 100 m (330 ft).

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Connecting the Touch 10 user interface (page 3 of 3)

Touch 10 physical interface





www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Cisco VCS provisioning

When using Cisco VCS (Video Communication Server) provisioning, a template containing all the settings that can be provisioned must be uploaded to Cisco TMS (TelePresence Management System). This is called the *Cisco TMS provisioning configuration template*.

All the system settings for your video system are included in this template. All settings except *SystemUnit Name* and *SIP Profile [1..1] URI* can be automatically provisioned to the video system.

The settings are described in the System settings chapter in this guide. Examples showing either the default value or an example value are included.

Downloading the provisioning configuration template

You can download the templates here:

http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-mx-series/products-release-notes-list.html

For each software release there is one provisioning configuration template (XML file) for each video system model. Take care to use the correct file.

Read the *Cisco TMS Provisioning Deployment Guide* to find how to upload the file to Cisco TMS, and how to set the desired values for the parameters to be provisioned. If not set by Cisco TMS, the default values will be used.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Optimal definition profiles

Under ideal lighting conditions the bandwidth (call rate) requirements can be substantially reduced.

The optimal definition profile should reflect the lighting conditions in your room and the quality of the video input (camera); the better the lighting conditions and video input, the higher the profile. Then, in good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate.

In general, we recommend the optimal definition profile set to Normal. However, if lighting conditions are good we recommend that you test the endpoint on the various Optimal Definition Profile settings before deciding on a profile.

Go to System Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Profile* to choose the preferred optimal definition profile.

You can set a resolution threshold to determine 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 will be possible if the available bandwidth is adequate.

Go to System Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Threshold60fps* to set the threshold.

The video input quality settings 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.

Go to System Configuration on the web interface and navigate to *Video > Input > Source [1..n] > Quality* to set the video quality parameter to Motion.

You can read more about the video settings in the System settings chapter.

High

Typically used in dedicated video conferencing rooms. Requires very good lighting conditions and a good quality video input to achieve a good overall experience.

Under ideal conditions the bandwidth requirements can be reduced by up to 50% compared to Normal.

Medium

Typically used in rooms with good and stable lighting conditions and a good quality video input.

The bandwidth requirements can be reduced by up to 25% compared to Normal.

Normal

This setting is typically used in office environments where the room is normally to poorly lit.

Typical resolutions used for different optimal definition profiles, call rates and frame rates

Frame rate	Optimal Definition Profile	Call rate						
		256 kbps	*768 kbps*	*1152 kbps*	*1472 kbps*	*2560 kbps*	*4 Mbps*	*6 Mbps*
30 fps	*Normal*	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	Medium	640×360	1280×720	1280×720	1280×720	1920×1080	1920×1080	1920×1080
	High	768×448	1280×720	1280×720	1920×1080	1920×1080	1920×1080	1920×1080
60 fps	*Normal*	256×144	512×288	768×448	1024×576	1280×720	1280×720	1920×1080
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1920×1080	1920×1080
	High	512×288	1024×576	1280×720	1280×720	1920×1080	1920×1080	1920×1080

www.cisco.com – Copyright © 2013–2015 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 TC software support ClearPath.

If the involved endpoints and infrastructure elements support ClearPath, all packet loss resilience mechanisms are used in point-to-point connections. Only some of the mechanisms are supported when using the optional built-in MultiSite feature.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Factory resetting the video system

It is not possible to undo a factory reset.

You should always backup the log files and the current configuration before you factory reset a system. Open the web interface, sign in, and follow these steps:

- Navigate to *Maintenance > System Recovery* and choose the *Backup* tab.
- Click *Download Logs* and *Download Configuration Backup* and follow the instructions to save the files on your computer.

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

Always consider reverting to the previously used software version before performing a factory reset. In many situations this will recover the system. Note that both the current and the previous software images reside on the system. Read about software swapping in the Reverting to the previously used software version section.

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

When factory resetting the video system the following happens:

- The call logs will be deleted.
- Passwords will be reset to default.
- All system parameters will be reset to default values.
- All files that have been uploaded to the system will be deleted. This includes, but is not limited to, custom backgrounds, certificates, and the favorites list (My contacts).
- The previous (inactive) software image will be deleted.
- Option keys will **not** be affected.

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

User interface: Touch

1. Tap gently on the Touch screen if the unit is in sleep mode.
2. Open the *Settings** menu and navigate to *Administrator > Reset*. You have to log in with an administrator user name and password to access the *Administrator* menu.
3. Tap the *Factory Reset* button.

   The system reverts to the default factory settings and restarts automatically. This will take a few minutes.

   The system confirms the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.

User interface: Web

Open the *Settings** menu and tap *System Information* on the Touch user interface to find the system's IP address (IPv4 or IPv6).

1. Open a web browser and enter the IP address of the video system in the address bar.
2. Navigate to *Maintenance > System Recovery* and choose the *Factory Reset* tab.
3. Read the provided information carefully before you click *Perform a factory reset...*.
4. Click the red *Yes* button to confirm that you want to perform a factory reset.

   The system reverts to the default factory settings and restarts automatically. This will take a few minutes.

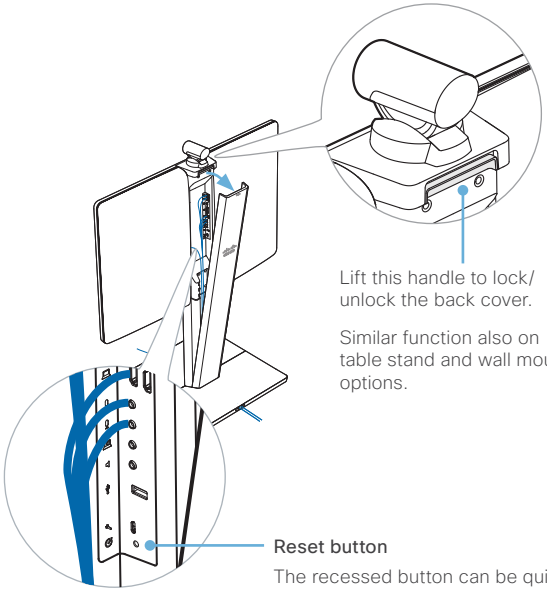
   The system confirms the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.

Using the reset button

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.

   The system reverts to the default factory settings and restarts automatically. This will take a few minutes.

   The system confirms the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.



* The *Settings* menu can be accessed from the drop down window that appears when you tap the contact information in the upper, left corner of the Touch user interface.

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Factory resetting the Touch 10 user interface

In an error situation it may be required to factory reset the Touch 10 user interface to recover connectivity. This should be done only when in contact with the Cisco support organization.

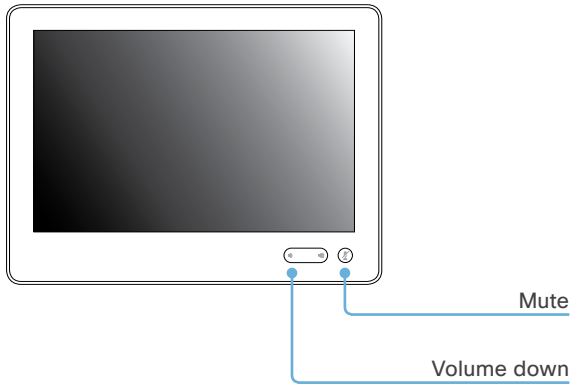
When factory resetting Touch 10 the pairing information is lost, and the Touch itself (not the video system) is reverted to factory defaults.

Touch 10 restarts after the reset and receives a new configuration automatically from the video system.

It is not possible to undo a factory reset.

Factory resetting Touch 10

1. Locate the *Mute* and *Volume down* buttons.



2. Press and hold the *Mute* button until it starts blinking (red and green). It takes approximately 10-15 seconds.
3. Press the *Volume down* button twice.

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Technical specification

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

MX300 G2:

- Cisco TelePresence Software Version TC7.0 or later

Components

Fully integrated unit including:

- Codec
- Display
- Camera
- Integrated microphone and loudspeakers

Cisco TelePresence Table Microphone 20 (two microphones are shipped with the system)

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 (version 1.3)

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 and base speakers
- Integrated full-range microphone
- Support for two Cisco TelePresence Table Microphone 20
- Mini jack audio input (e.g. for PC)
- Mini jack audio output

User interface

Cisco TelePresence Touch 10

- Ten inch projected capacitive touch screen
- Resolution: 1280 x 800

Language support

- English, Arabic, Catalan, Czech, Danish, Dutch, Finnish, French, German, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese-Brazilian, Russian, Simplified Chinese, Spanish, Swedish, Traditional Chinese, Turkish (depends on software version)

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)

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

Approvals and compliance

EU/EEC

- Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN 60950-1
- Directive 2004/108/EC (EMC Directive)
  - Standard EN 55022, Class A
  - Standard EN 55024
  - Standard EN 61000-3-2/-3-3
- Directive 2011/65/EU (RoHS)

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

USA

- Approved according to UL 60950-1
- Complies with FCC15B Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

- Approved according to CAN/CSA C22.2 No. 60950-1-07
- This Class A digital apparatus complies with Canadian ICES-003
- Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

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 (version 1.3) 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)

Video output (one output)

One HDMI output (version 1.3)

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 @ 30 fps (QCIF) (decode only)
- 352 × 288 @ 30 fps (CIF)
- 512 × 288 @ 30 fps (w288p)
- 576 × 448 @ 30 fps (448p)
- 640 × 480 @ 30 fps (VGA)
- 704 × 576 @ 30 fps (4CIF)
- 768 × 448 @ 30 fps (w448p)
- 800 × 600 @ 30 fps (SVGA)
- 1024 × 576 @ 30 fps (w576p)
- 1024 × 768 @ 30 fps (XGA)
- 1280 × 720 @ 30 fps (720p30)
- 1280 × 768 @ 30 fps (WXGA)
- 1280 × 1024 @ 30 fps (SXGA)
- 1440 × 900 @ 30 fps (WXGA+)*
- 1600 × 1200 @ 30 fps (UXGA)*
- 1680 × 1050 @ 30 fps (WSXGA+)*
- 1920 × 1080 @ 30 fps (1080p30)*
- 512 × 288 @ 60 fps (w288p60)*
- 768 × 448 @ 60 fps (w448p60)*
- 1024 × 576 @ 60 fps (w576p60)*
- 1280 × 720 @ 60 fps (720p60)*
- 1920 × 1080 @ 60 fps (HD1080p60)*

* Requires premium resolution option

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 TelePresence Multiway support (requires Cisco TelePresence Video Communication Server [Cisco VCS] and Cisco TelePresence Multipoint Control Unit [MCU])
- Ability to natively join multipoint conferences hosted on Cisco TelePresence Multipoint Switch (CTMS)

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

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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
- Medianet: Mediatrace and Metadata

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)
- Cisco WebEx TelePresence

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.

July 2015

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).

Current RFCs and drafts supported

- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2460 Internet protocol, version 6 (IPv6) specification
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3388 Grouping of Media Lines in the Session Description Protocol (SDP)
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3891 The SIP "Replaces" Header
- RFC 3892 Referred-By Mechanism
- RFC 3960 Early Media
- RFC 3986 Uniform Resource Identifier (URI): Generic Syntax
- RFC 4028 Session Timers in SIP
- 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 4145 TCP-Based Media Transport in the SDP
- RFC 4235 An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- 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 4583 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams

  draft-ietf-bfcpbis-rfc4583bis-00 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5104 Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)
- RFC 5168 XML Schema for Media Control
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5389 Session Traversal Utilities for NAT (STUN)
- RFC 5577 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 5589: SIP Call Control Transfer
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5768 Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6156 Traversal Using Relays around NAT (TURN) Extension for IPv6
- RFC 6184 RTP Payload Format for H.264 Video
- RFC 6185 RTP Payload Format for H.264 Reduced-Complexity Decoding Operation (RCDO)

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

User documentation on the Cisco web site

In general, user documentation for the Cisco TelePresence products is available here:

http://www.cisco.com/go/telepresence/docs

You have to choose your product category in the right pane until you find your product. This is the path you have to follow:

Collaboration Room Endpoints >
Cisco TelePresence MX Series

Alternatively, you can use the following short-link to find the documentation:

http://www.cisco.com/go/mx-docs

The documents are organized in the following categories:

Installation guides:
Install and Upgrade > Install and Upgrade Guides

Getting started guide:
Install and Upgrade > Install and Upgrade Guides
Maintain and Operate > Maintain and Operate Guides

Administrator guides:
Maintain and Operate > Maintain and Operate Guides

User guides and Quick reference guides:
Maintain and Operate > End-User Guides

Knowledge base articles and frequently asked questions:
Troubleshoot and Alerts > Troubleshooting Guides

CAD drawings:
Reference Guides > Technical References

Video conferencing room guidelines:
Design > Design Guides

Software licensing information:
Software Downloads, Release and General Information > Licensing Information

Regulatory compliance and safety information:
Install and Upgrade > Install and Upgrade Guides

Software release notes:
Software Downloads, Release and General Information > Release Notes

www.cisco.com – Copyright © 2013–2015 Cisco Systems, Inc. All rights reserved.

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.

TANDBERG is now a part of Cisco. TANDBERG® is a registered trademark belonging to Tandberg ASA.

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 contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: http://www.cisco.com/web/siteassets/contacts

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134 USA