Software version TC7.1
APRIL 2014

Codec C40/C60

Profile 42”

Profile 52”/55”

Profile 52” Dual / 55” Dual

Profile 65”

Administrator guide

For Cisco TelePresence System Codec C40/C60 and Profiles using C40/C60

www.cisco.com – Copyright © 2010-2014 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 Codec C60/C40 and Profiles using Codec C60/C40.

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
Profile 42" using Codec C40 at a glance 8
Profile 52"/55" at a glance 9
Profile 52" Dual / 55" Dual at a glance 10
Profile 65" at a glance 11
Codec C60 at a glance 12
Codec C40 at a glance 13

Web interface 14
Accessing the web interface 15
Changing the system password 16
The interactive menu 17
System information 18
Placing a call 19
Sharing content 20
Controlling and monitoring a call 21
Controlling your camera 22
Local layout control 23
Capturing snapshots 24
Controlling the far end camera 25
Accessing call information 26
System configuration 27
Changing system settings 28
Setting the Administrator Settings menu password 29
System status 30
Managing the favorites list 31
Favorite list folders 32
Choosing a wallpaper 33
Choosing a ringtone 34
Peripherals overview 35
User administration 36
Adding a sign in banner 40
Managing startup scripts 41
Application programming interface 42
Managing the video system's certificates 43
Managing the list of trusted certificate authorities 44
Adding audit certificates 45
Managing pre-installed certificates for Edge provisioning 46
Setting strong security mode 47
Changing the persistency mode 48
Deleting trust lists (CUCM only) 49
Troubleshooting 50
Downloading log files 51
Starting extended logging 52
Upgrading the system software 53
Backup and restore 54
Reverting to the previously used software version 55
Factory reset 56
Remote support user 57
Restarting the system 58

System settings 59
Overview of the system settings 60
Audio settings 64
Cameras settings 71
Conference settings 74
FacilityService settings 80
GPIO settings 81
H323 settings 82
Logging settings 85
Network settings 86
NetworkPort settings 93
NetworkServices settings 94
Phonebook settings 98
Provisioning settings 99
RTP settings 101
Security settings 102
SerialPort settings 104
SIP settings 105
Standby settings 109
SystemUnit settings 110
Time settings 112
UserInterface settings 113
Video settings 114
Experimental settings 133

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Setting passwords 134
Setting the system password 135
Setting the menu password 136

Appendices 137
Cisco VCS provisioning 138
About monitors when you have a Codec C60 139
About monitors when you have a Codec C40 140
Connecting the Cisco TelePresence Touch 8 controller 141
Advanced customization of video and audio 142
Optimal definition profiles 143
ClearPath – Packet loss resilience 144
Requirement for speaker systems connected to a Cisco TelePresence C Series codec 145
DNAM for Profile 42”/52”/55” 146
DNAM for Profile 65” 147
Factory resetting the codec 148
Factory resetting the Touch 8 control panel 149
Technical specifications 150
Supported RFCs 158
User documentation on the Cisco web site 159

Cisco contacts 160

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Chapter 1

Introduction

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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

Products covered in this guide:

- Profile 52” / 55” / 65” using C60
- Profile 52” Dual / 55” Dual using C60
- Profile 42” / 52” / 55” using C40
- Codec C60
- Codec C40

User documentation

The user documentation for the Cisco TelePresence Codec C Series has several guides suitable for various user groups.

- **Installation guides:**
  How to install the product
- **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 (remote control and Touch controller)
- **User guides:**
  How to use the product (remote control and Touch controller)
- **Camera user guide:**
  User guide for the PrecisionHD cameras
- **API reference guide:**
  How to use the Application Programmer Interface (API), and reference guide for the command line commands
- **User guide for the TC console application:**
  The free TC Console application provides a graphical interface to the advanced customizable features of the codec.
- **Physical interface guides**
- **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-integrator-c-series/tsd-products-support-series-home.html

www.cisco.com – Copyright © 2010-2014 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 TC7.1 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-integrator-c-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

Improved support for Collaboration Edge

Collaboration Edge now supports Cisco Unified Communications Manager (CUCM) User Data Service (UDS), which adds scalability towards the number of CUCMs in an Expressway deployment.

Collaboration Edge also supports and requires TLS verification for increased security. The endpoint will verify that the Edge server has a certificate signed by a Certificate Authority that Cisco trusts. If certificate validation fails, the endpoint will not receive the provisioning and not be registered.

Disabled root account

Cisco has decided to close down the root access permanently on TC software. This increases the security level of the endpoints, at the cost of reduced troubleshooting abilities.

Remote support user added for troubleshooting

A remote support user may be created on the codec with assistance from Cisco Technical Assistance Center (TAC). This will give read access to the system, and access to perform a limited set of commands that can aid troubleshooting. The remote support user should only be enabled for troubleshooting reasons when instructed by Cisco TAC.

Ethernet statistics for codec is now available via Touch

It is possible to get network statistics for the video system (codec) and Touch controller from the Administrator Settings menu the Touch controller. This may improve troubleshooting Touch pairing issues.

New default value for VLAN voice mode

The default value for *Network 1 VLAN Voice Mode* has changed from *Off* to *Auto*.

For endpoints that are shipped with TC7.1, and for endpoints that are factory reset, the default value is *Auto*. This enables an endpoint that used to be in the data VLAN to join the voice VLAN, if available.

For endpoints that are upgraded to TC7.1, the setting will keep the value that it had before the upgrade. If the setting had the old default value, it will remain *Off*. This will preserve the behavior for upgraded endpoints.

Minor changes on Touch interface

- Camera control improvements.
- *Present* has been changed to *Share* for portfolio alignment.
- *History* has been changed to *Recents*.

G.728 audio codec support

Support for the G.728 audio codec is added for point-to-point calls.

Improved presentation quality

The endpoint supports common laptop resolutions, and the quality for content with many details, e.g. Excel spreadsheets, is improved.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

System configuration changes

New configurations

Audio DefaultVolume

Cameras PowerLine Frequency

Conference ActiveControl Mode

Video Output Composite [3] Location HorizontalOffset *(only C60)*

Video Output Composite [3] Location VerticalOffset *(only C60)*

Video Output DVI [2] Location HorizontalOffset

Video Output DVI [2] Location VerticalOffset

Video Output HDMI [1] Location HorizontalOffset

Video Output HDMI [1] Location VerticalOffset

Configurations that are removed

Conference Presentation Policy

Video Layout Engine LocalMode

Configurations that are modified

Time Zone

The list of time zones is updated.

Video Wallpaper

OLD: <None/Custom/Growing/Summersky/Waves>

NEW: <None/Custom/Growing/Summersky/Waves/Blue>

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 42” using Codec C40 at a glance

See the installation sheet for the Profile 42” for instructions on how to install the system.

Codec C40

- Full HD video
- High resolution data sharing
- Full HD Multisite
- Rich I/O capabilities

PrecisionHD 1080p camera

Full HD Camera designed for visual communication with:

- 12 × optical zoom
- Fast and precise pan, tilt and zoom

Monitor

42” Full HD LCD, 16:9, 1080 × 1920 resolution

Audio module

Wide band audio module supporting:

- 20 kHz AAC-LD
- Full echo canceling
- Stereo

Audio amplifier

Optimized DNAM for the Profile system, providing crystal clear and natural audio

Microphones

2 × Microphones

Operating devices

- Touch 8 controller (for C Series)
- Remote control with AAA batteries

Base options

Floor standing footplate, wheel base, or wall mount on pedestal

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 52”/55” at a glance

See the installation sheets for the Profile 52”/55” for instructions on how to install the system.

Codec C60/C40

- Full HD video
- High resolution data sharing
- Full HD Multisite
- Rich I/O capabilities

PrecisionHD 1080p camera

Full HD Camera designed for visual communication with:

- 12 × optical zoom
- Fast and precise pan, tilt and zoom

Monitor

52”/55” Full HD LCD, 16:9, 1080 × 1920 resolution

Audio module

Wide band audio module supporting:

- 20 kHz AAC-LD
- Full echo canceling
- Stereo

Audio amplifier

Optimized DNAM for the Profile system, providing crystal clear and natural audio

Microphones

Three (with C60) / Two (with C40) microphones with cables

Operating devices

- Touch 8 controller
- Remote control with AAA batteries

Base options

Floor standing footplate, wheel base, or wall mount on pedestal

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 52” Dual / 55” Dual at a glance

See the installation sheets for the Profile 52” Dual / 55” Dual for instructions on how to install the system.

Codec C60

- Full HD video
- High resolution data sharing
- Full HD Multisite
- Rich I/O capabilities

PrecisionHD 1080p camera

Full HD Camera designed for visual communication with:

- 12 × optical zoom
- Fast and precise pan, tilt and zoom

Dual monitor

Dual 52” / Dual 55” Full HD LCD, 16:9, 1080 × 1920 resolution

Audio module

Wide band audio module supporting:

- 20 kHz AAC-LD
- Full echo canceling
- Stereo

Audio amplifier

Optimized DNAM for the Profile system, providing crystal clear and natural audio

Microphones

Four microphones with cables

Operating devices

- Touch 8 controller
- Remote control with AAA batteries

Base options

Floor standing footplate or wall mount on pedestal

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 65” at a glance

See the Profile 65” Installation Sheet for instructions of how to assemble the system.

Codec C60

- Full HD video
- High resolution data sharing
- Full HD Multisite
- Rich I/O capabilities

PrecisionHD 1080p camera

Full HD Camera designed for Visual communication with:

- 12 × optical zoom
- Fast and precise pan, tilt and zoom

Monitor 65”

65” Full HD LCD, 16:9, 1080 × 1920 resolution

Audio module

Wide band audio module supporting:

- 20 kHz AAC-LD
- Full echo canceling
- Stereo

Audio amplifier

Optimized DNAM for the Profile system, providing crystal clear and natural audio

Microphones

Three microphones with cables

Operating devices

- Touch 8 controller
- Remote control with AAA batteries

Base options

Floor standing footplate or wall mount on pedestal

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Codec C60 at a glance

The Codec C60 is the 1080p HD video collaboration engine. Based upon the same technology as the Codec C90, the C60 delivers Full HD video, HD collaboration and superior audio for natural communication at its finest, delivering unrivaled value.

The C60 is a standards-compliant codec for integration into team meeting rooms, boardrooms and industry projects.

- Full High Definition Video with up to 4 HD sources, and collaboration with optimal definition for the best video quality every time, regardless of environment.
- Highest Quality Audio with flexibility to add up to 4 microphones directly from the codec, and superior, full duplex audio with high quality stereo sound.
- Full APIs.
- Ensure successful, streamlined integration projects with standards-compliant professional connectors.

Integrator package

The integrator package of the Codec C60 comes with the PrecisionHD 1080p camera, microphone and cables.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Codec C40 at a glance

The Codec C40 provides all the power required to transform any conference room to a HD video collaboration room. Designed for any standard HD integration project, the Codec C40 is the ideal solution for everyday video conferencing and collaboration solution. 1080p HD video, and Multisite™ features combine to make the Codec C40 ideal for a variety of applications.

The Codec C40 is ideal for standard meeting rooms, executive offices and team collaboration rooms.

- Full High Definition Video with up to 2 HD sources, and collaboration with optimal definition for the best video quality every time, regardless of environment.
- Highest Quality Audio with flexibility to add up to 2 microphones directly from the codec, and superior, full duplex audio with high quality stereo sound.
- Full APIs.
- Ensure successful, streamlined integration projects with standards-compliant professional connectors.

Integrator package

The integrator package of the Codec C40 comes with the PrecisionHD 1080p camera, microphone and cables.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Chapter 2

Web interface

www.cisco.com – Copyright © 2010-2014 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.

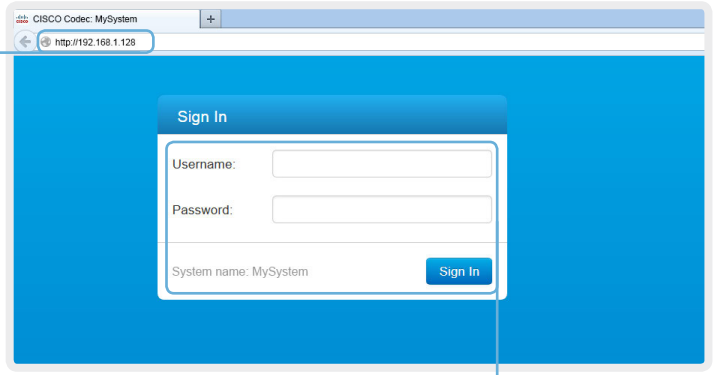
In this chapter you will find information how to use the web interface for system configuration and maintenance.

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.

To find the IP address (IPv4 or IPv6), open the *Settings** menu on the Touch controller and tap *System Information*; or navigate to *Home > Settings > System information* when using a remote control and the on-screen menu.

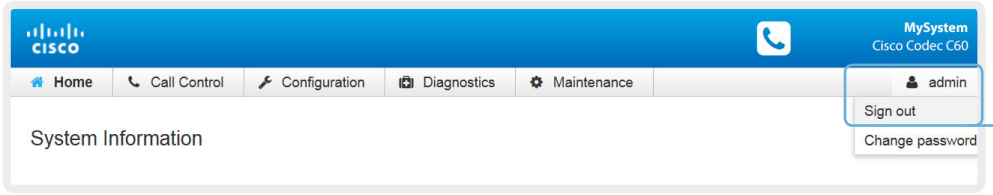


2. Sign in

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 (i.e. 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 your user name and choose *Sign out* from the drop-down list.

* 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 controller.

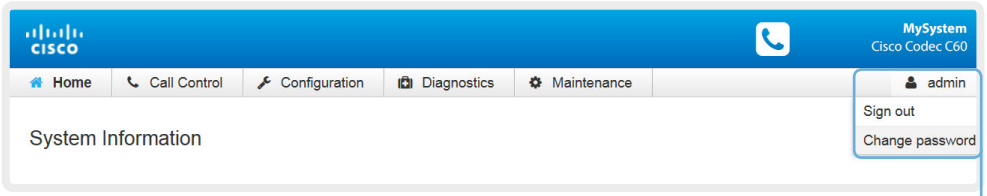
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Changing the system password

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

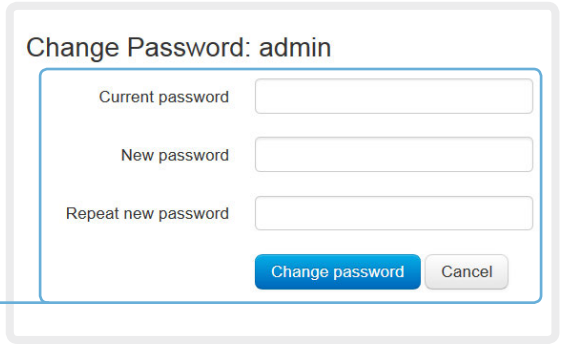
A warning, saying that the system password is not set, is shown on screen until you set a password.

You can read more about password protection in the ► Setting passwords chapter.



1. Open the Change Password dialog

Hover the mouse over your user 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 © 2010-2014 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.

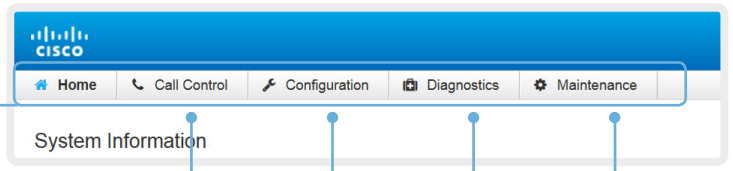
When you hover the mouse over an item in the main menu, you can navigate to its related sub-pages.

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 Contents Management
Personalization
Peripherals
User Administration
Sign In Banner
Startup Scripts
API
Security

Diagnostics
Troubleshooting
Call History
Log Files

Maintenance
Software Upgrade
Backup and Restore
System Recovery
Restart

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

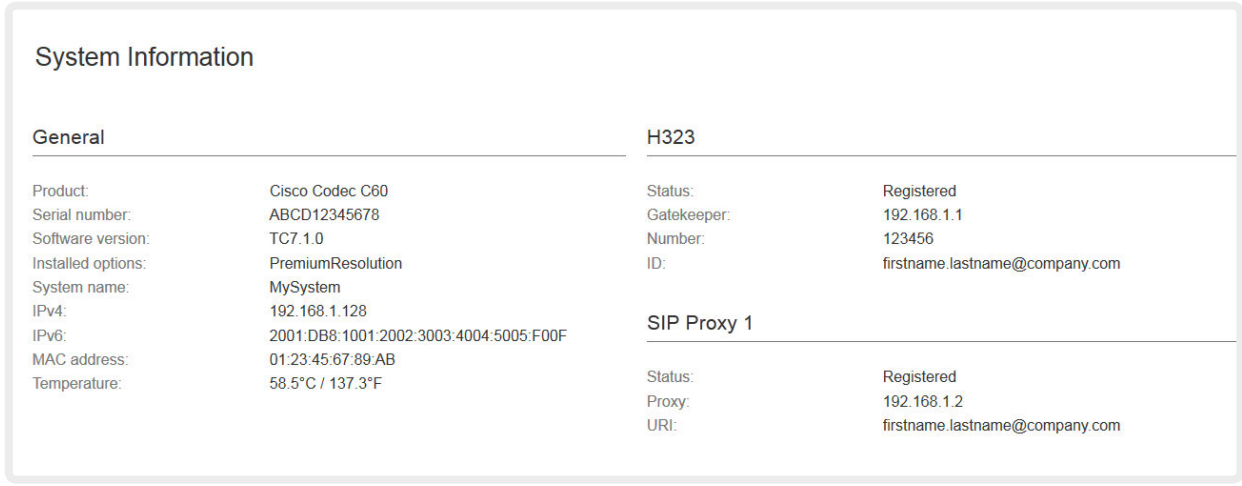
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Placing a call

You can use the Call Control page to place a call.

Even if the web interface is used to initiate the call, it is the video system (display, microphones and loudspeakers) that is used for the call; it is not the PC running the web interface.

Calling

You can call someone either by choosing a contact name in the *Favorites, 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 *Favorites, Directory* and *Recents* lists will be listed as you type.

Select the correct entry in the list before you click *Call*.

Calling more than one

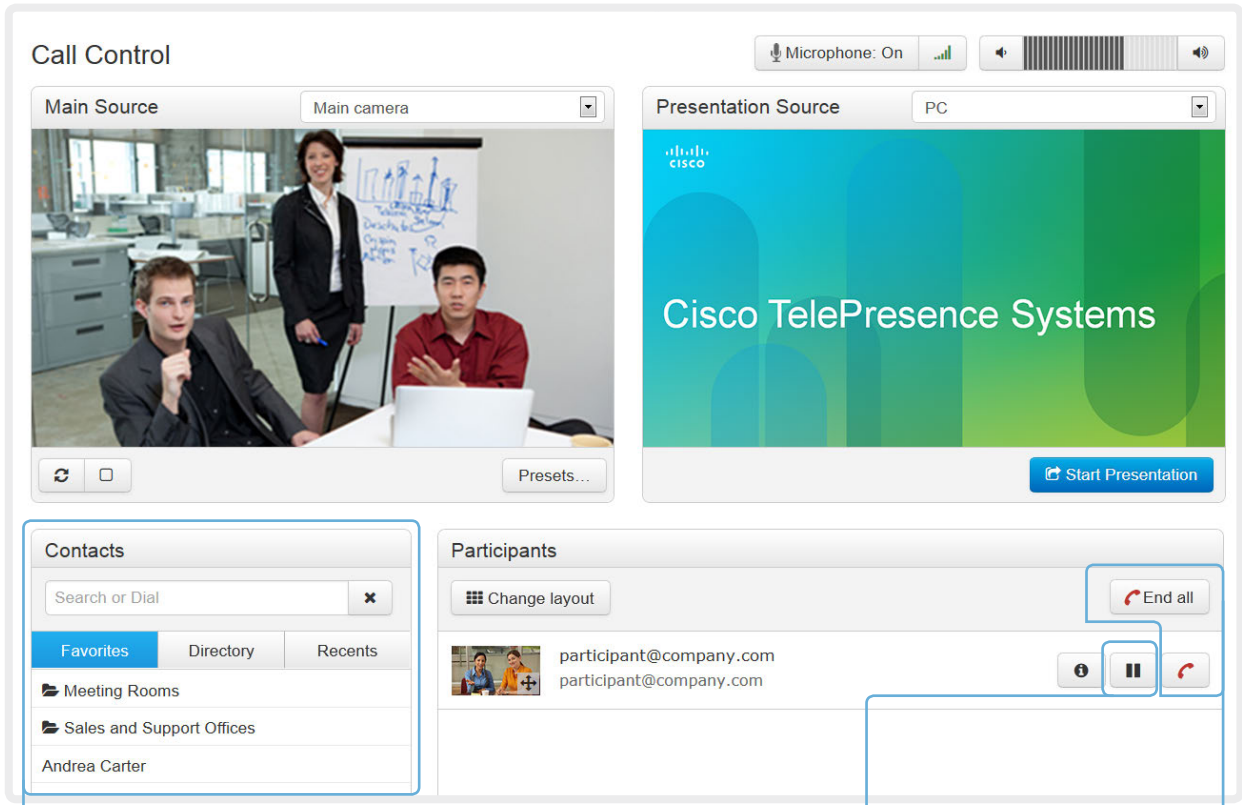
A point-to-point video call (a call involving two parties only) may be expanded to include more participants.

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

One additional participant can join on audio-only.

Follow the same procedure to call the next conference participant as you did when calling the first participant.

Navigate to: Call Control



Calling someone

Click a contact name, either in the *Favorites, 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

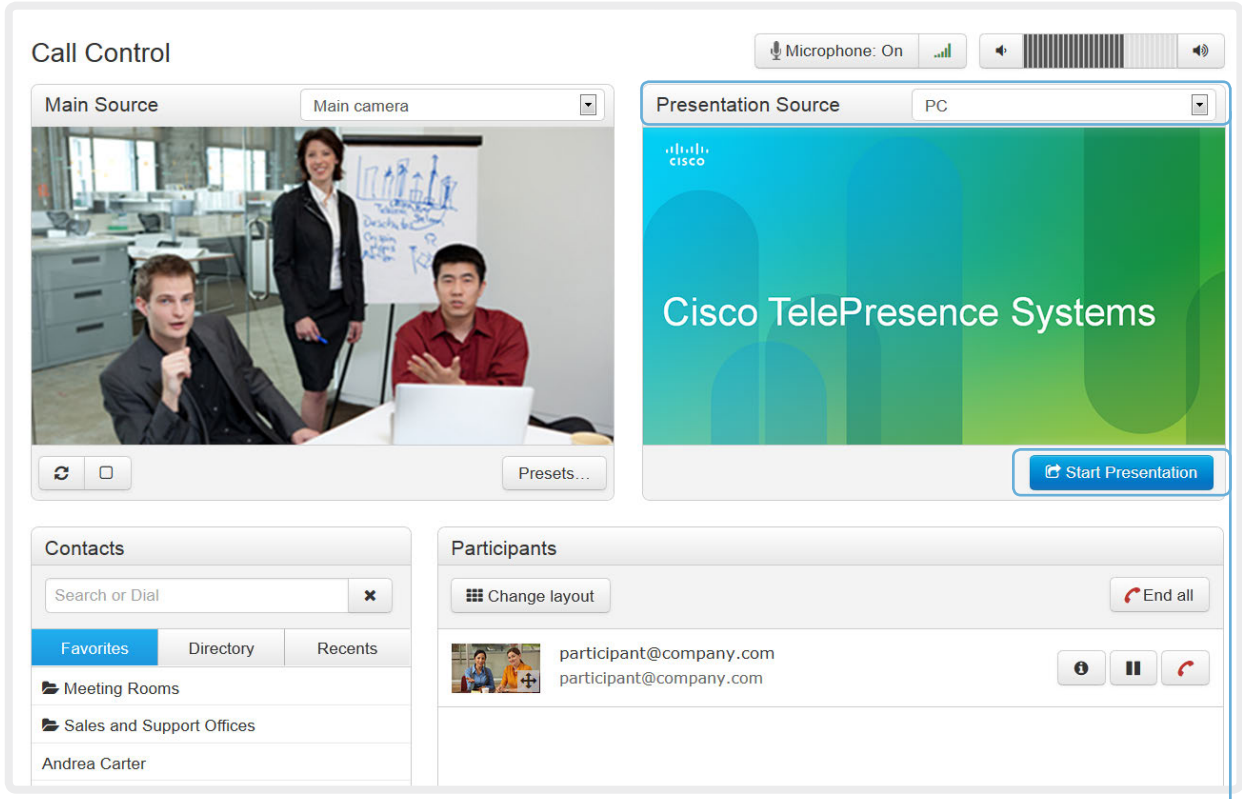
Sharing content

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 far end, that is the other participant(s) in the call.

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:

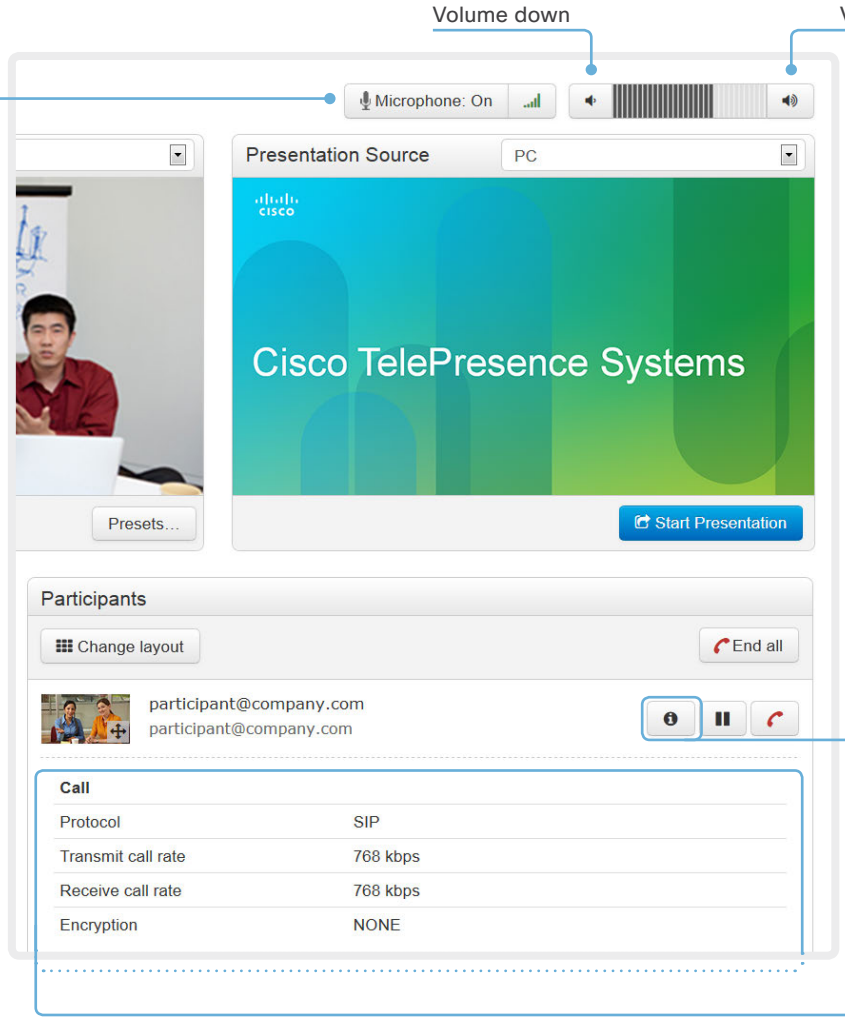
Click the *Stop Presentation* button that is present while sharing.

www.cisco.com – Copyright © 2010-2014 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 the call details.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

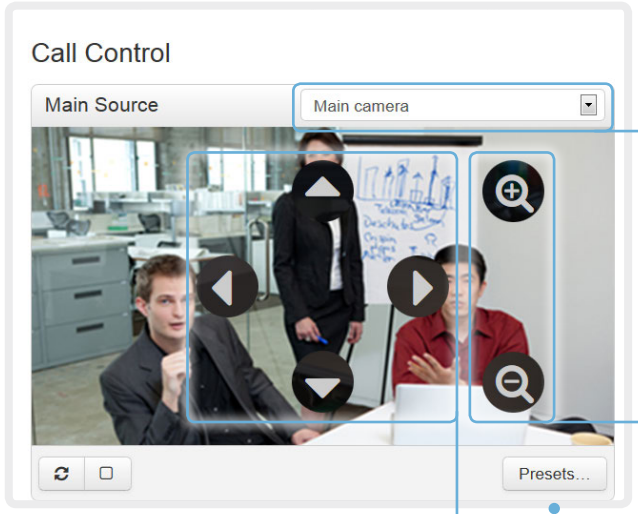
Controlling your camera

You can control the camera from the Call Control page.

The camera controls (pan, tilt, zoom) are available when the cursor is placed in the Main Source video area. Live snapshots are automatically taken during this period.

Note that the camera controls are not available if the system is in standby mode.

Navigate to: Call Control



Choose which camera to control

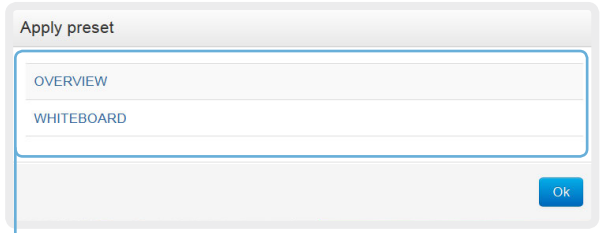
Click the arrow to open the drop-down list. Then choose the camera you want to control.

Zoom

Use + and - to zoom in and out.

Pan and tilt

Use the left and right arrows to pan the camera, and the up and down arrows to tilt it.



Camera presets

If a camera preset is defined it is listed here. Click the preset's name to move the camera(s) to the preset position.

Click *OK* to close the window.

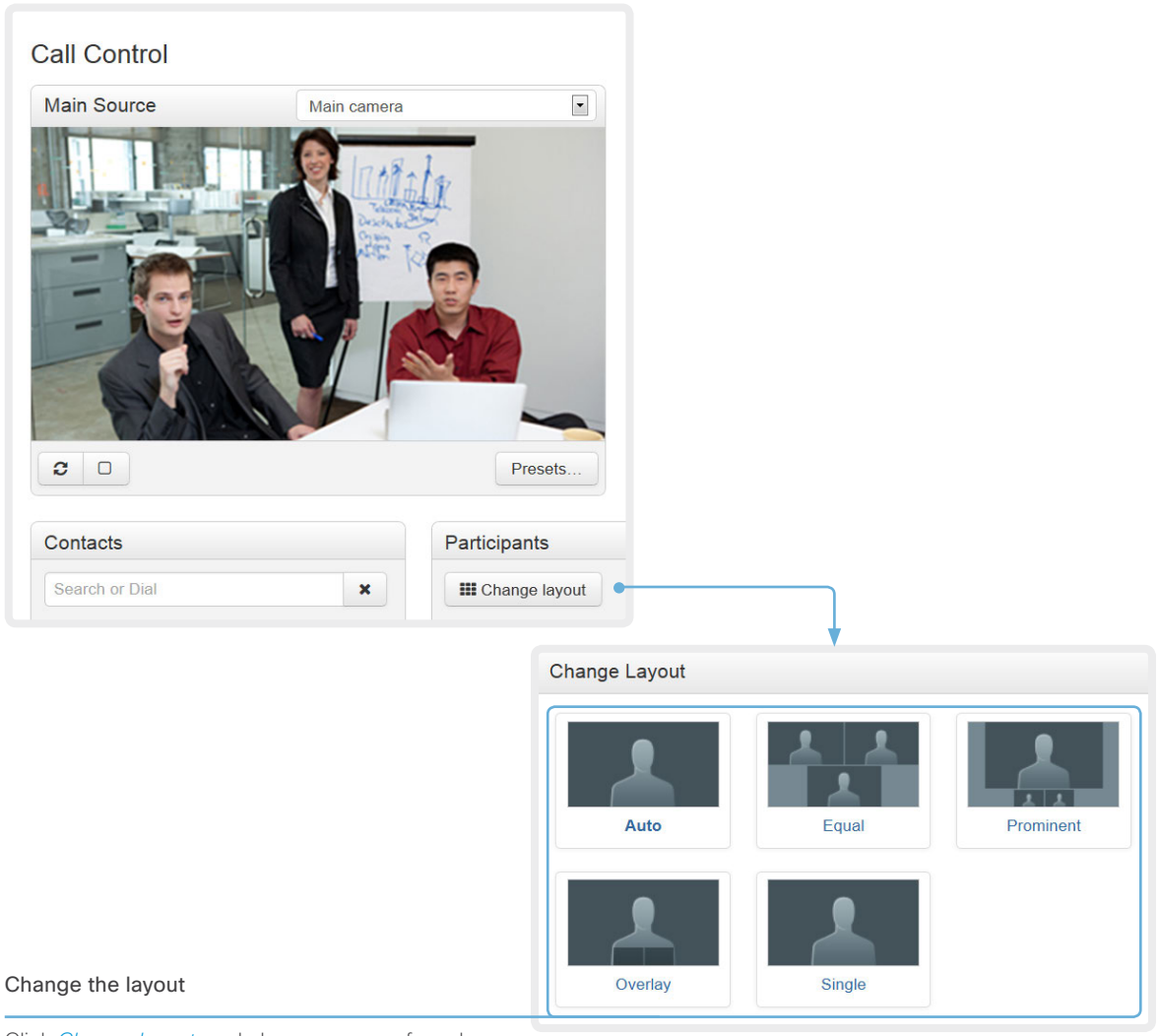
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 your 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.

You may change the layout while in a call.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Capturing snapshots

The snapshot feature, which is disabled by default, allows snapshots captured by your video system to be displayed on the Call Control page. Captures from your video system's camera as well as from its presentation channel will be displayed.

This feature might come in handy when administering the video system from a remote location, e.g. to check the camera view.

To use web snapshots you have to sign in with ADMIN credentials.

Enabling the snapshot feature

The snapshot feature is disabled by default. The feature must be enabled using the remote control and on screen menu, or the Touch controller. The Touch controller must be directly connected to the codec's second Ethernet port.

Touch controller:

- Open the *Settings** menu on the Touch controller and tap *Administrator*. You have to log in with an administrator user name and password to get access to the *Administrator* menu.
- Tap *Web Snapshots* and choose **ON**.

Remote control and on screen menu:

- Go to the Advanced configuration menu, navigate to *Video > AllowWebSnapshots* and choose **On**.

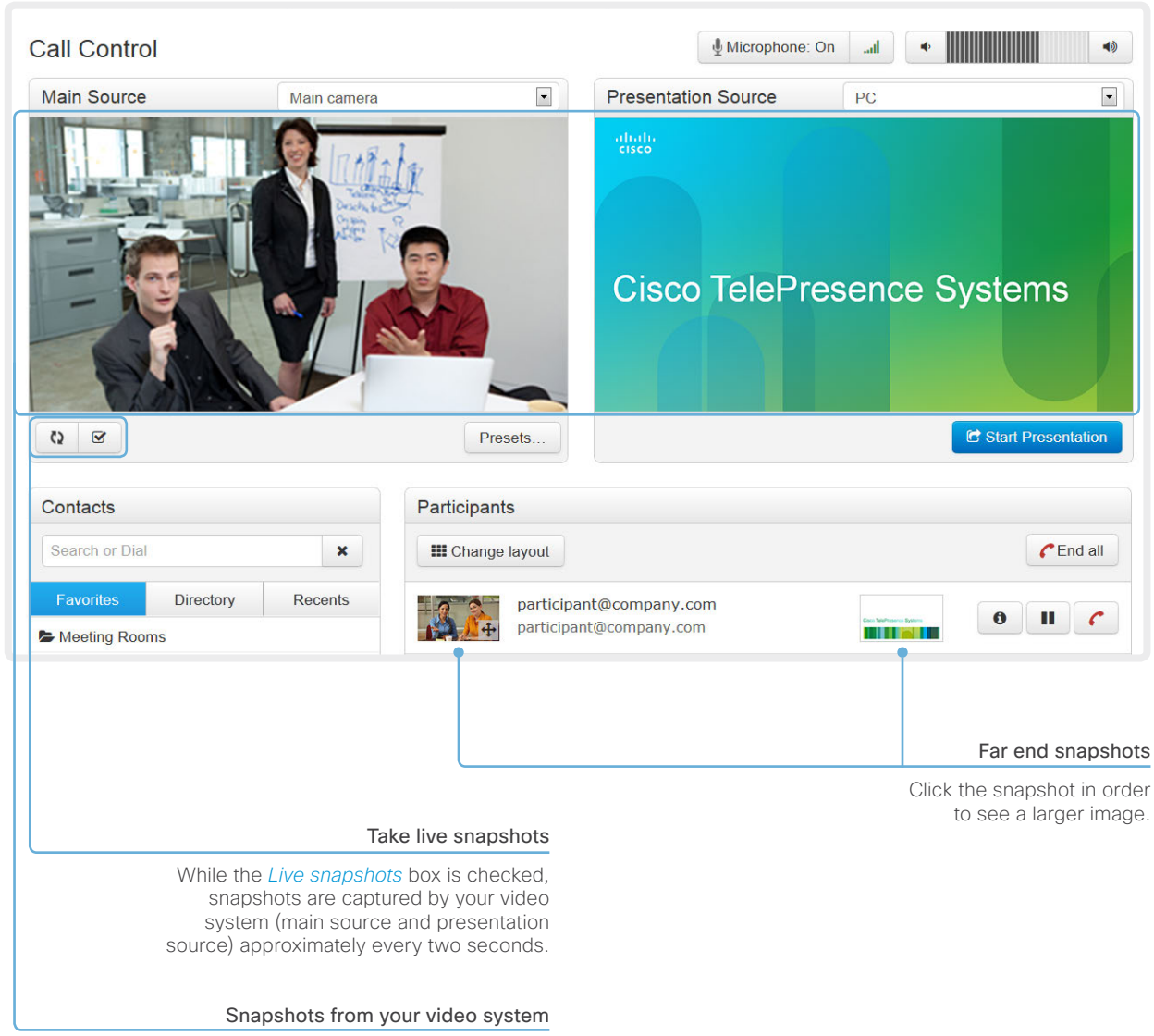
Far end snapshots while in a call

While in a call, snapshots of the remote participant's main camera and presentation channel (far end) will be captured and displayed as shown in the illustration. The snapshots are updated approximately every 30 seconds.

Far end snapshots are captured even if web snapshots are disallowed on the far end video system. Web snapshots are prohibited only for encrypted calls.

* 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 controller.

Navigate to: Call Control



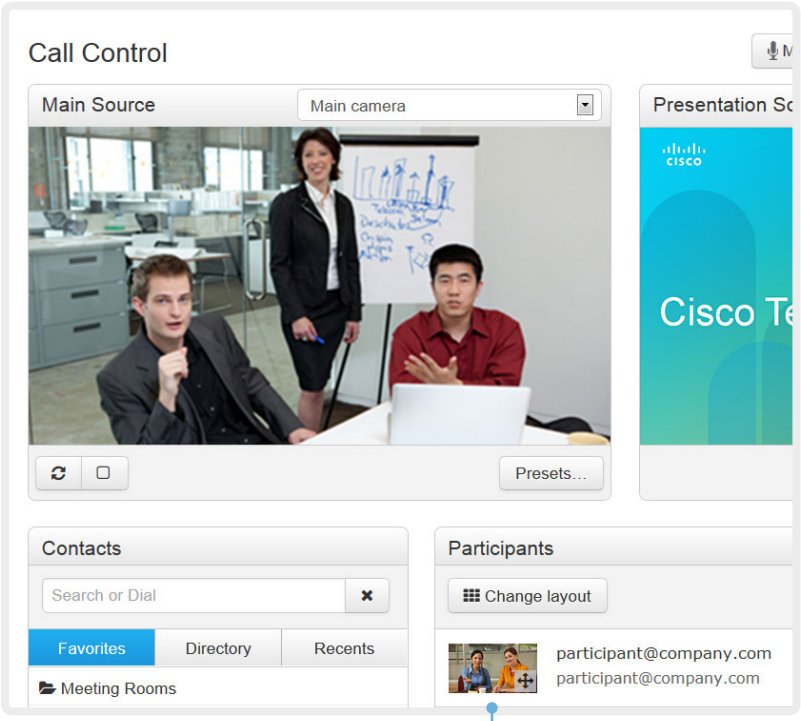
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

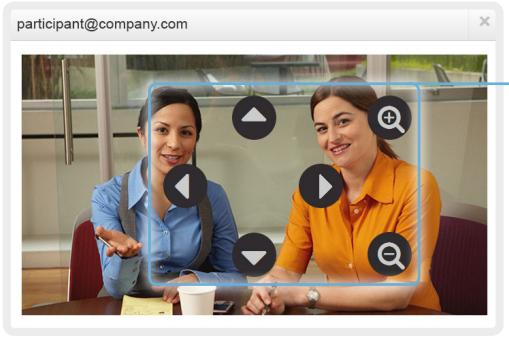
Controlling the far end camera

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

- The *Conference FarEndControl Mode* setting is switched **On** on the far end video system.
- The far end camera has pan, tilt or zoom functionality. Only the relevant controls will appear.

Navigate to: Call Control





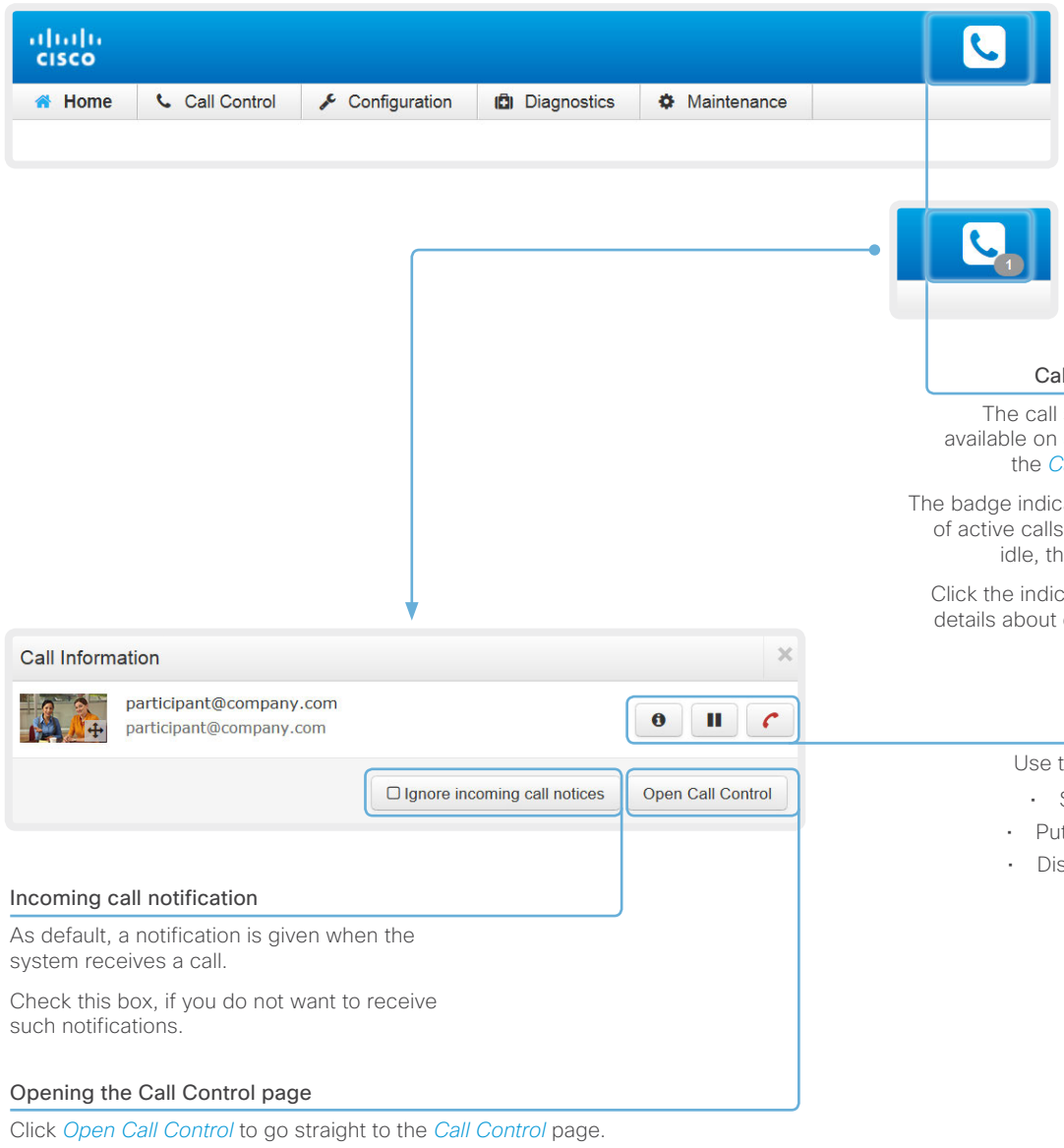
Control the remote participant's camera

1. Click the snapshot to show it in a larger window.
2. Place the cursor in the image to enable the controls.
3. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.

www.cisco.com – Copyright © 2010-2014 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.

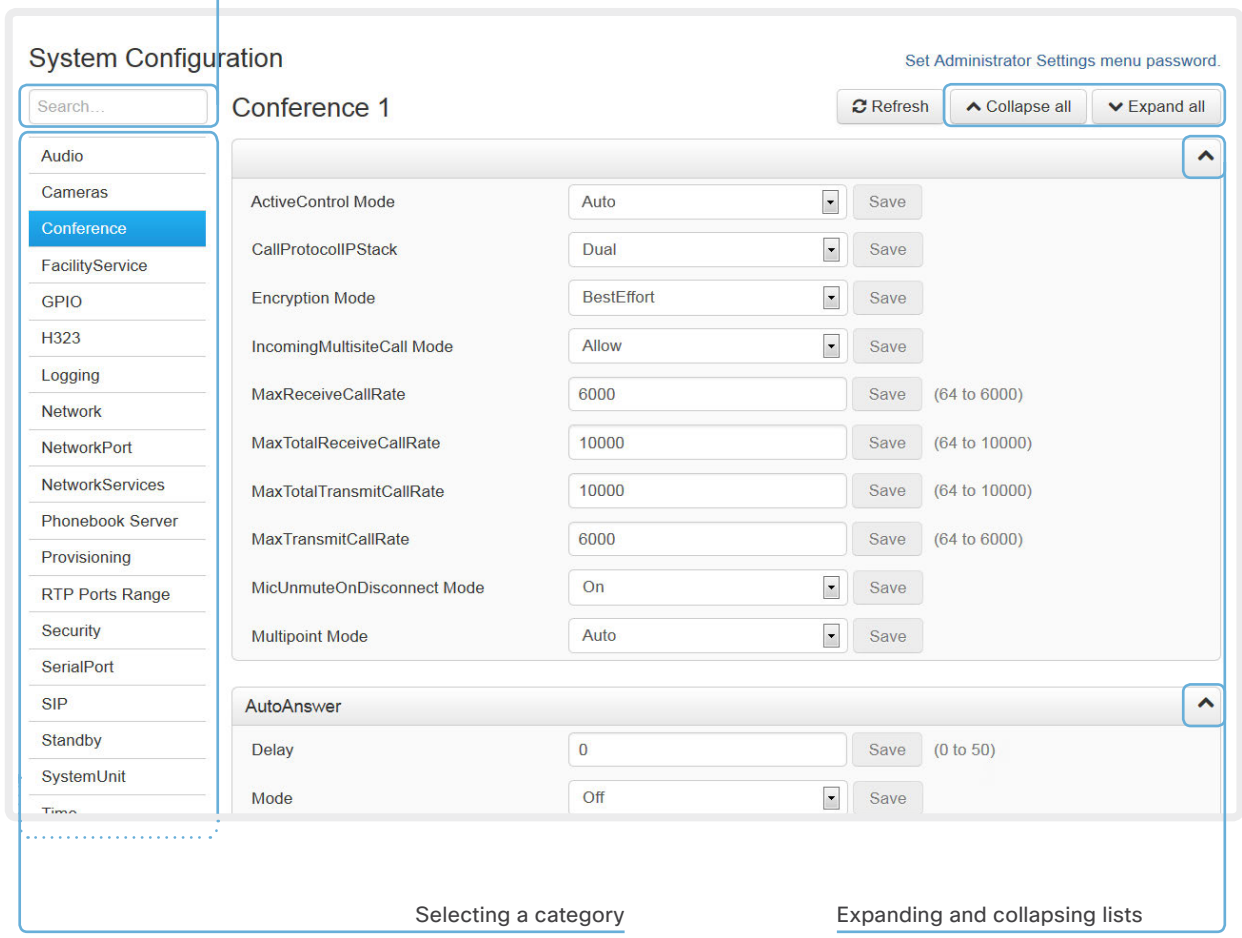
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 © 2010-2014 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.

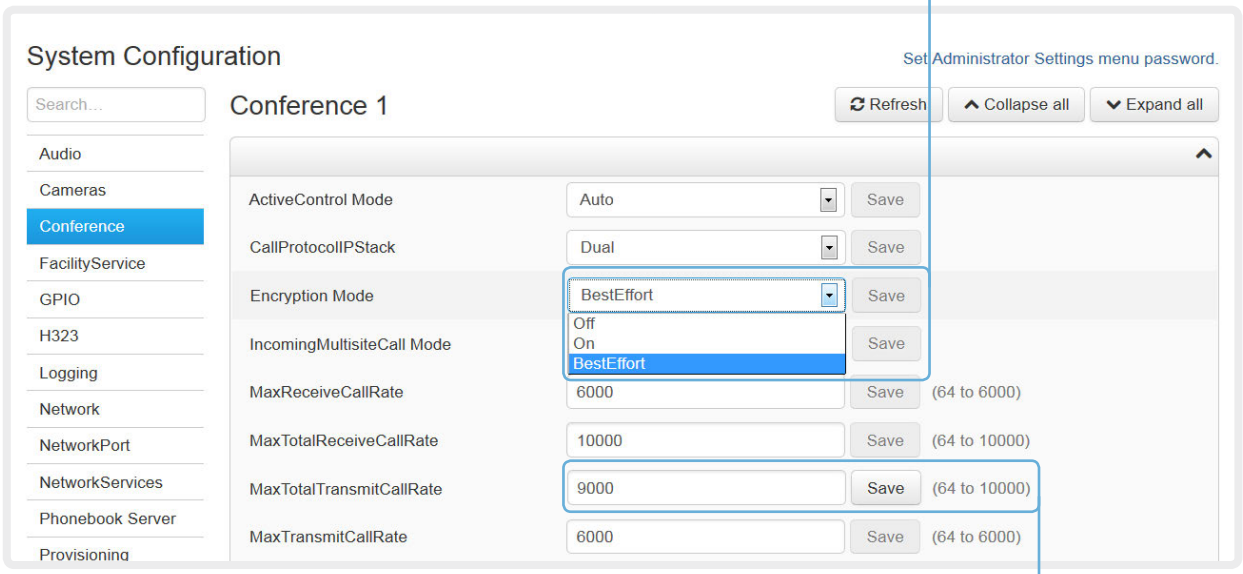
Different settings may require different user credentials. In order to be sure that an administrator is able to change all system settings, the user must possess all user roles.

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. Choose the preferred value and click *Save* for the change to take effect.



Text input field

Enter text in the input field and 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Setting the Administrator Settings menu password

This password restricts access to the Administrator Settings menu that is available on-screen when using the remote control.

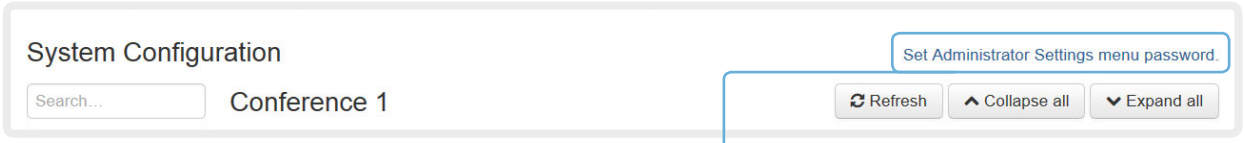
When starting up the video conference system for the first time anyone can access these settings, because the menu password is not set.

We strongly recommend that you set a menu password, because the administrator settings may severely affect the behavior of the system.

Note that the menu password, as from software version TC7.0, applies only to the on-screen Administrator Settings menu accessed with a TRC5 remote control; it does not apply to the Administrator menu on a Touch controller.

You can read more about password protection in the ► Setting passwords chapter.

Navigate to: Configuration > System Configuration

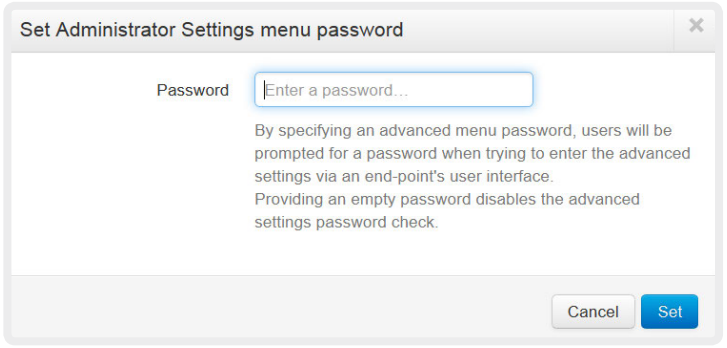


Changing the menu password

Click *Set/Change Administrator Settings menu password* to open this dialog.

Enter the new password in the text input field and click *Set* to set it.

Click *Set* without entering a password to leave the Administrator menu unprotected (not recommended).

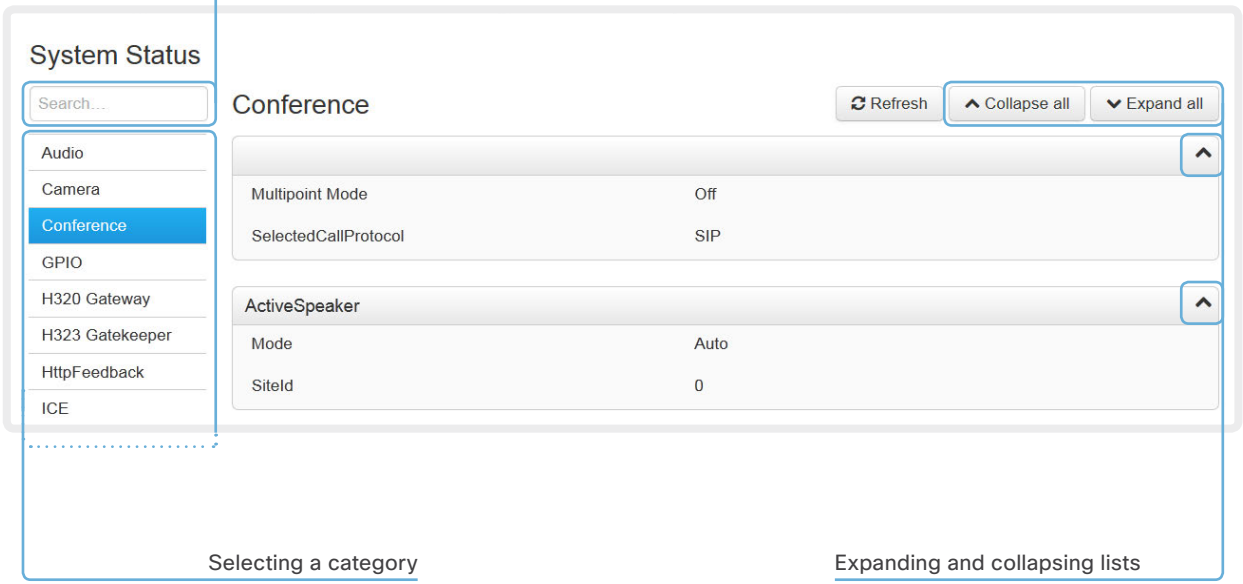


www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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



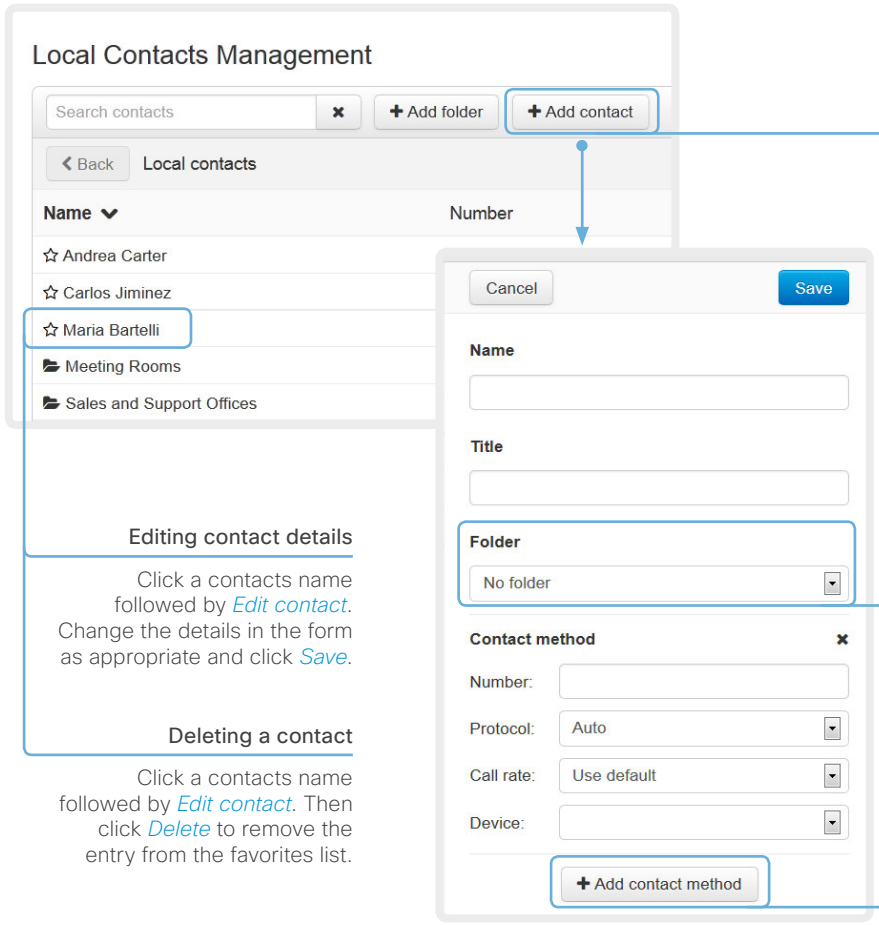
* The status shown in the illustration serve as an example. The status of your system may be different.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Managing the favorites list

The entries in the favorites list can be accessed from the Touch controller, the on-screen menu (the My contacts folder in the phone book) and the Web interface.

Navigate to: Configuration > Favorites 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.

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.

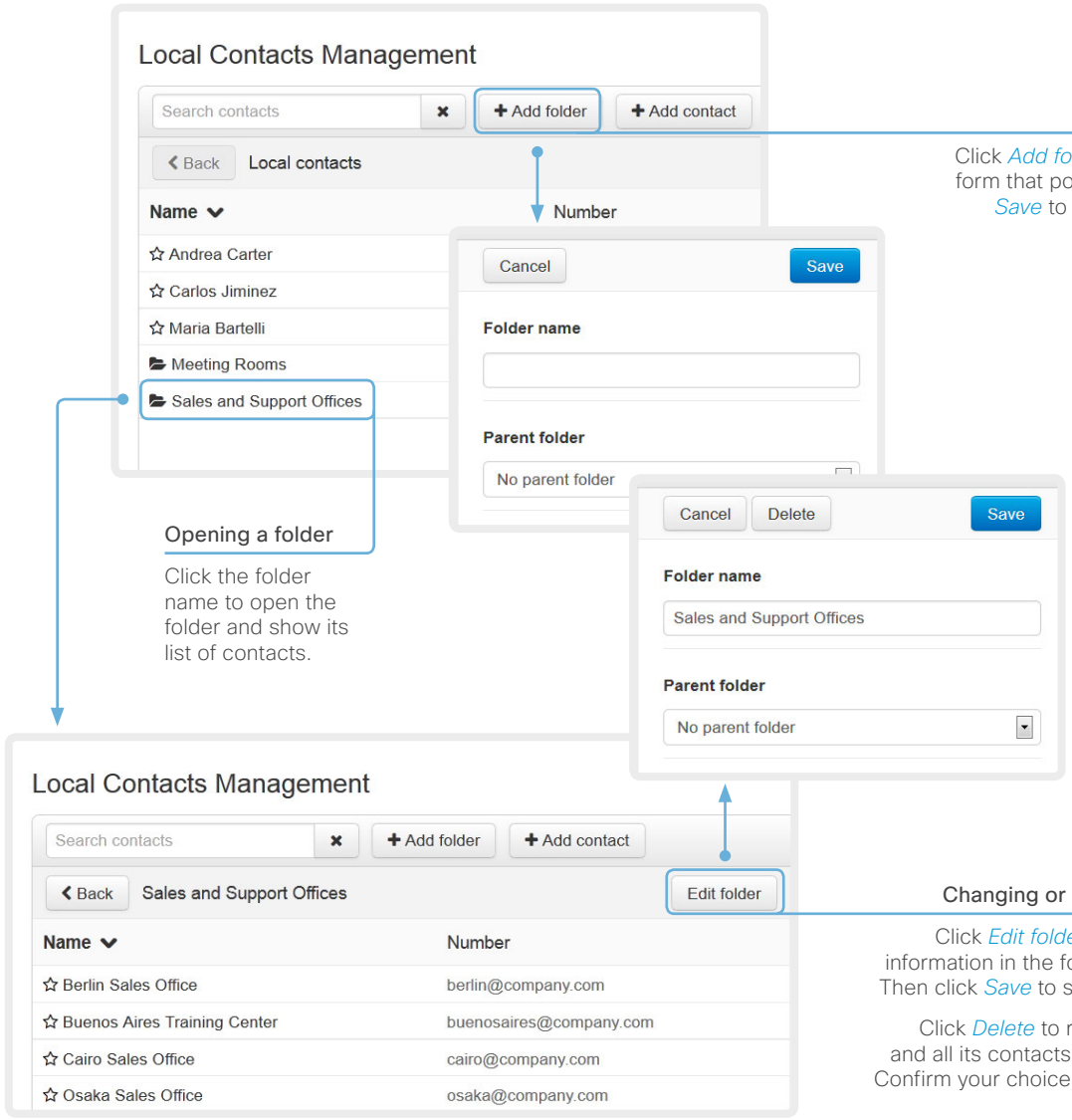
* Note that only the first contact method will appear in the Favorites list on the Cisco TelePresence Touch controller. All contact methods are available when using the remote control.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Favorite list folders

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

Navigate to: Configuration > Favorites Management



Adding a folder

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

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

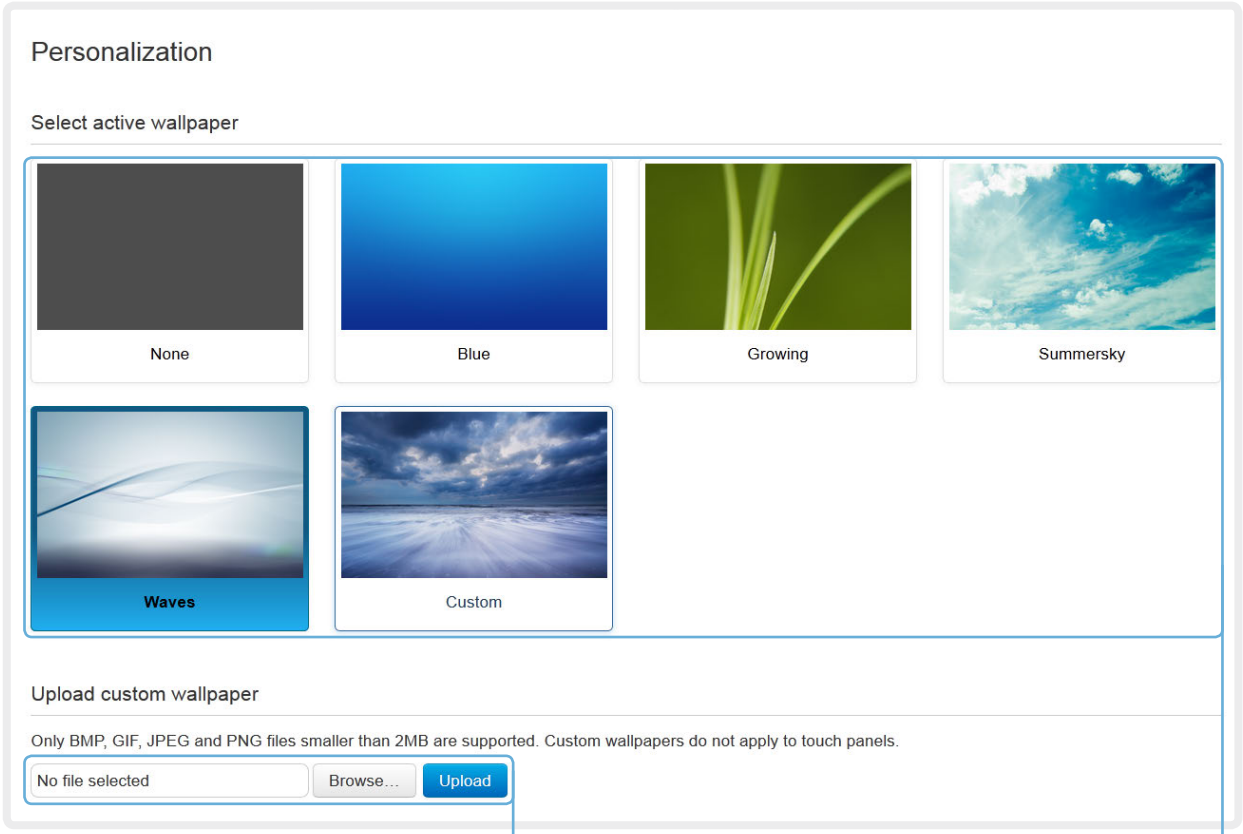
Choosing a wallpaper

You can choose from a set of predefined wallpapers to use as background on your display.

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

If you have a Touch controller: The custom wallpaper applies to only the main display and will not appear on the Touch controller.

Navigate to: Configuration > Personalization



Uploading a custom wallpaper file

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: 2 MByte

Choosing a wallpaper

Choose a wallpaper from the list.

If you have uploaded a custom wallpaper, it will appear in the list of miniatures together with the predefined wallpapers.

The chosen wallpaper is highlighted.

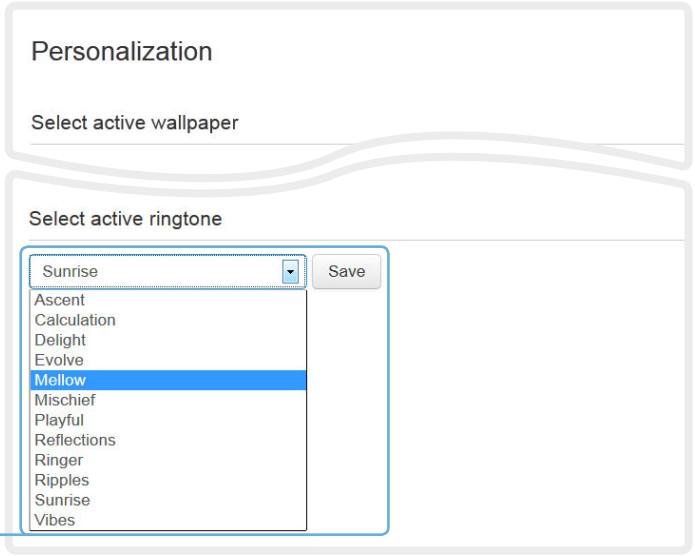
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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, not through the web interface.

Navigate to: Configuration > Personalization



Choosing a ringtone

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

Playing back a ringtone

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

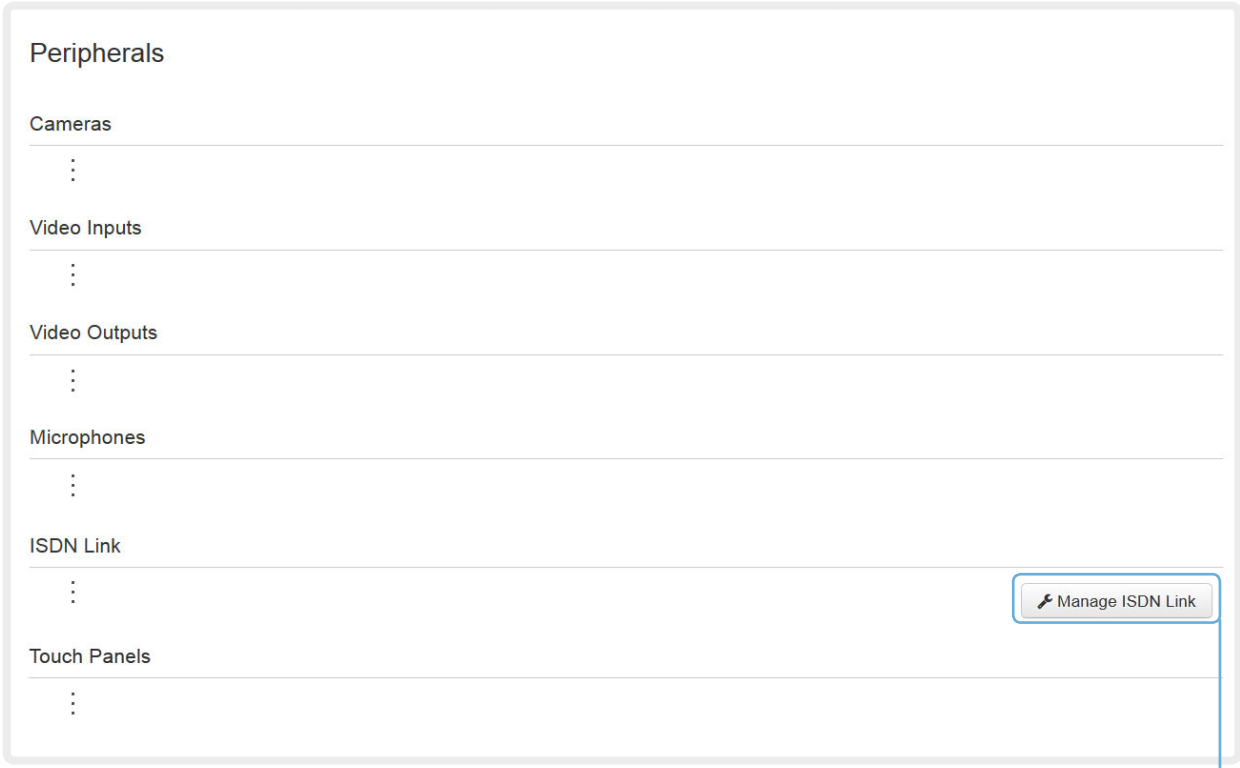
Use the stop button (■) to end the playback.

www.cisco.com – Copyright © 2010-2014 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, Touch controllers and ISDN Links*.

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

User administration

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:

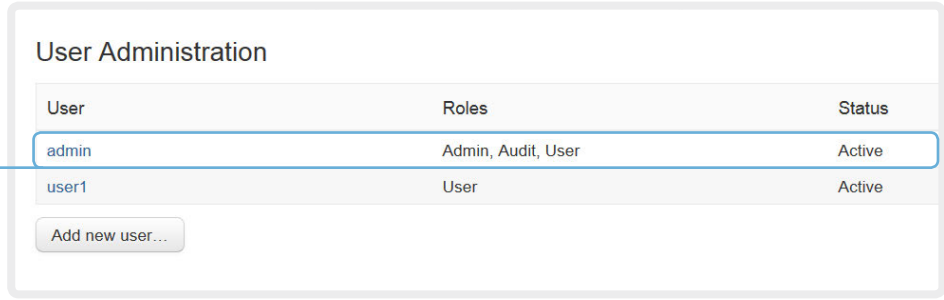
- ADMIN: A user holding this role can create new users and change most settings. The user neither can upload audit certificates nor change the security audit settings.
- USER: A user holding this role can make calls and search the phone book. The user can modify a few settings, e.g. adjusting the audio volume and changing the menu language.
- 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

User administration, continued

Creating a new user account

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

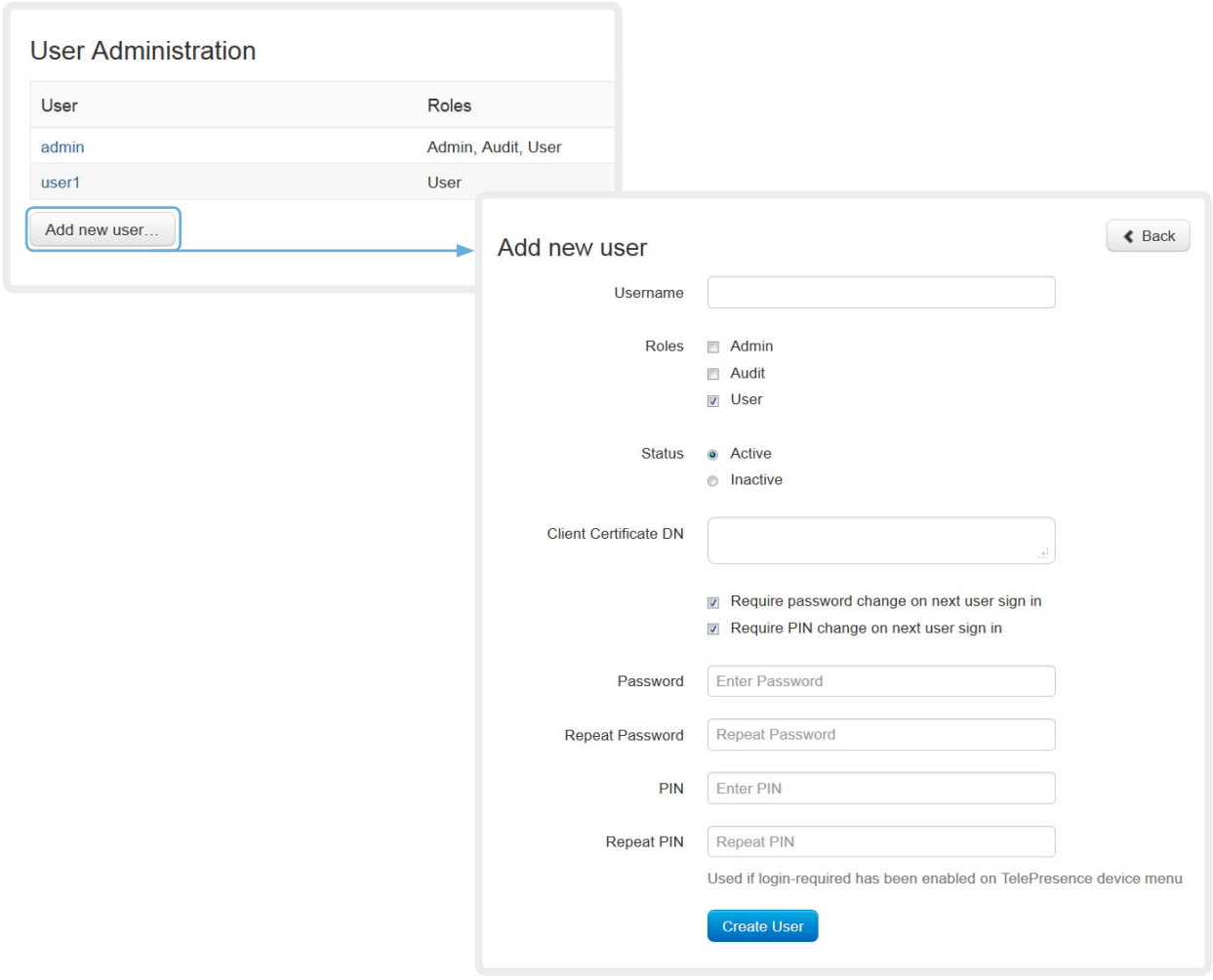
1. Click *Add new user...*.
2. Fill in the Username, Password and PIN code*, and check the appropriate user roles check boxes.

   As a default the user has to change the password and PIN code 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; the PIN code is used with the TRC5 remote control and on-screen menu when the *Video OSD LoginRequired* setting is switched **On**.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

User administration, continued

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 and PIN code 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 or PIN code

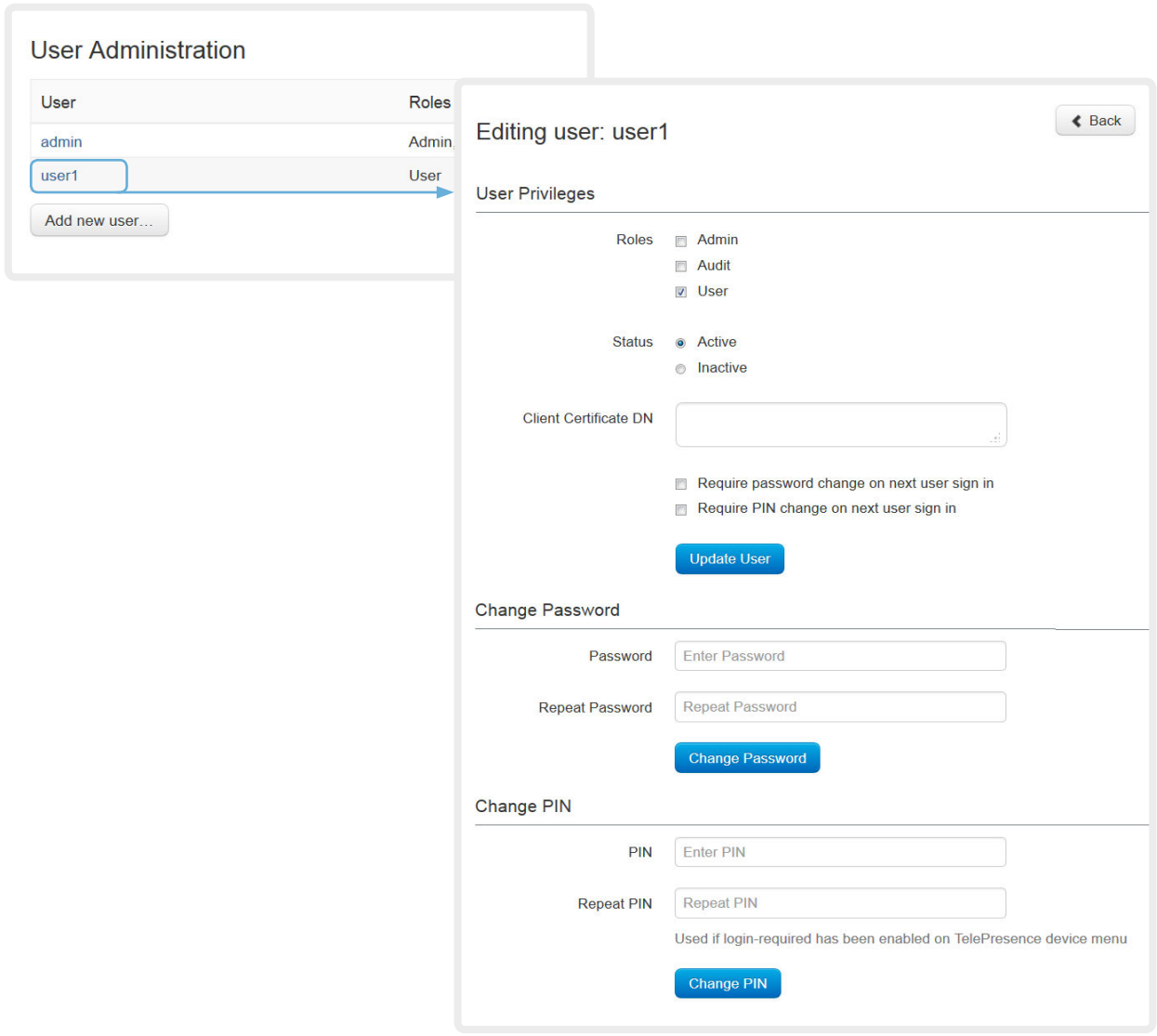
Follow these steps in order to change the password or PIN code*:

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

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

* The password is used with the web interface and command line interface; the PIN code is used with the remote control and on-screen menu when the *Video OSD LoginRequired* setting is switched **On**.

Navigate to: Configuration > User Administration



www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

User administration, continued

Deactivating a user account

Follow these steps in order to deactivate a user account:

Always keep at least one user with ADMIN rights **Active**.

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.

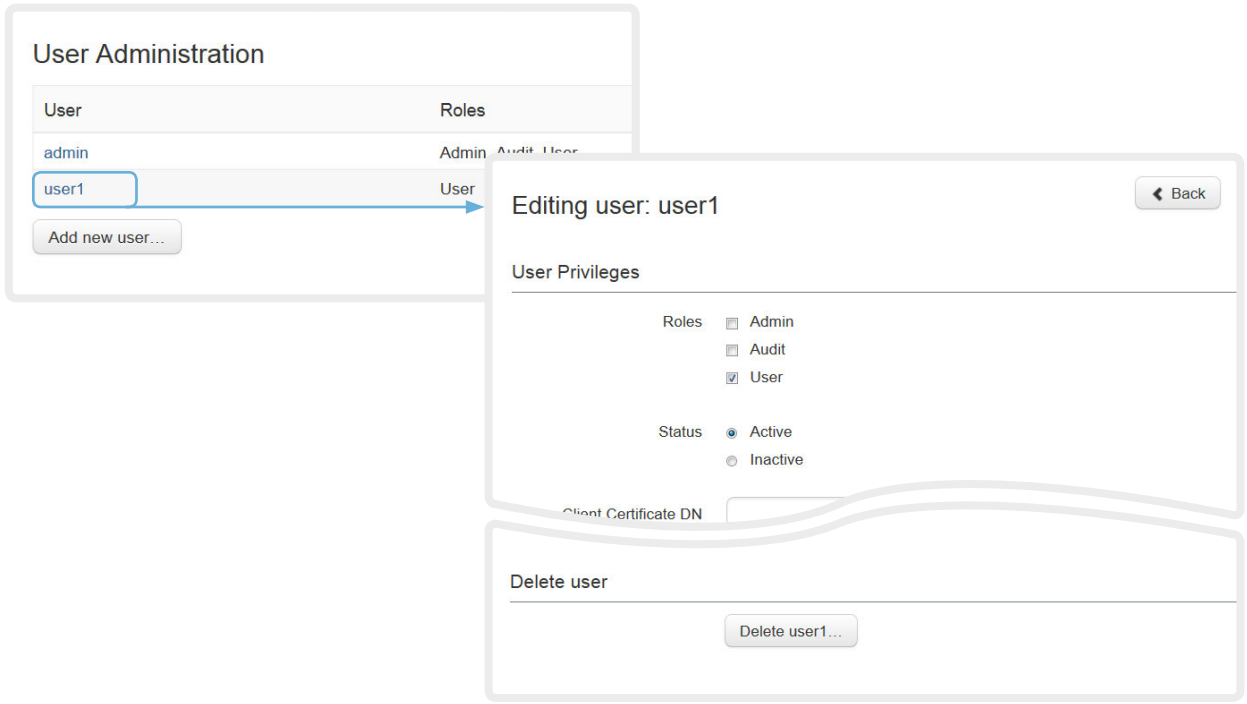
Deleting a user account

Follow these steps in order to delete a user account:

It is not possible to delete the default *admin* user. There must always be at least one user with ADMIN rights on the system.

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

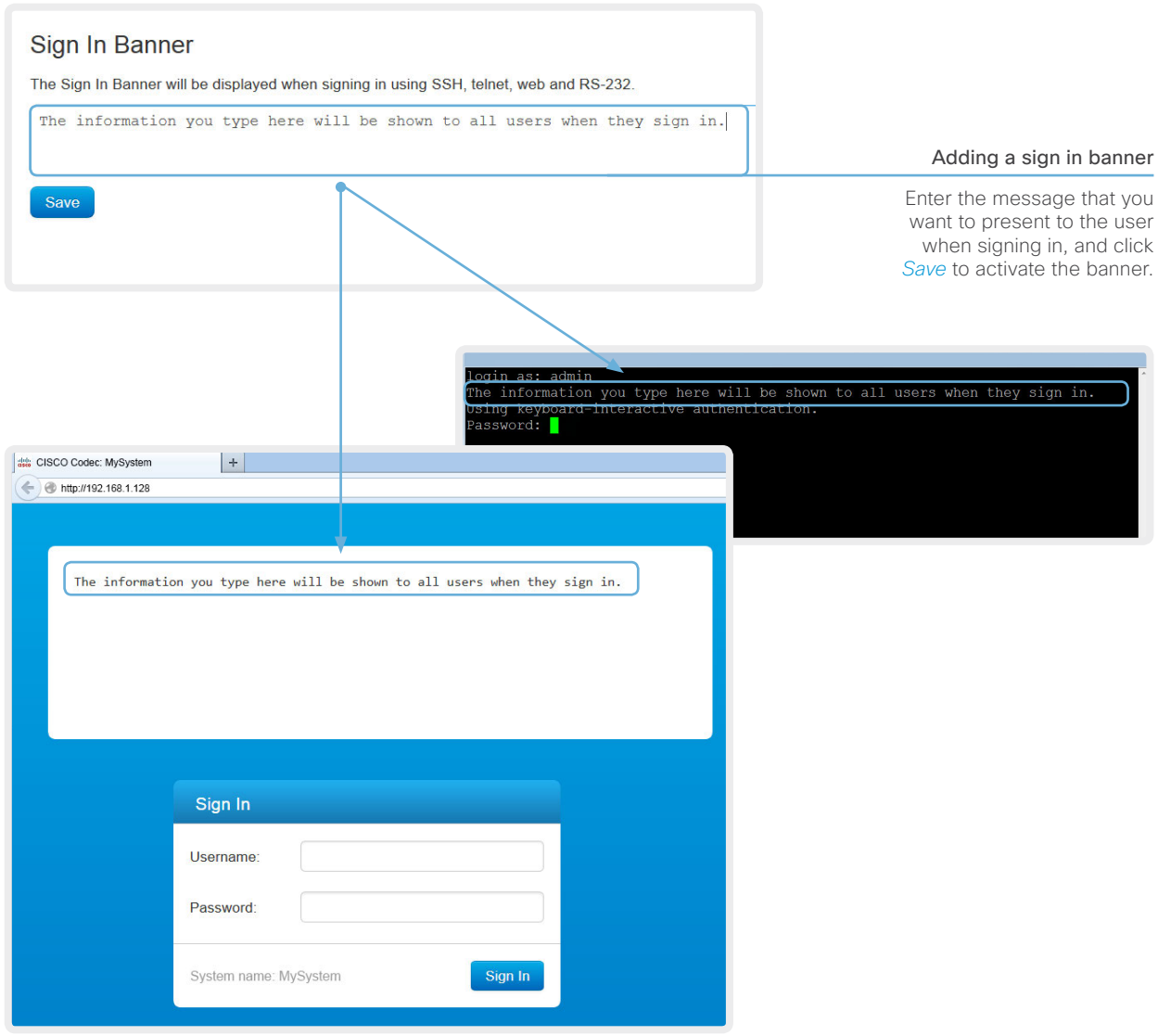


www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 or the command line interface.

Navigate to: Configuration > Sign In Banner



www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Managing startup scripts

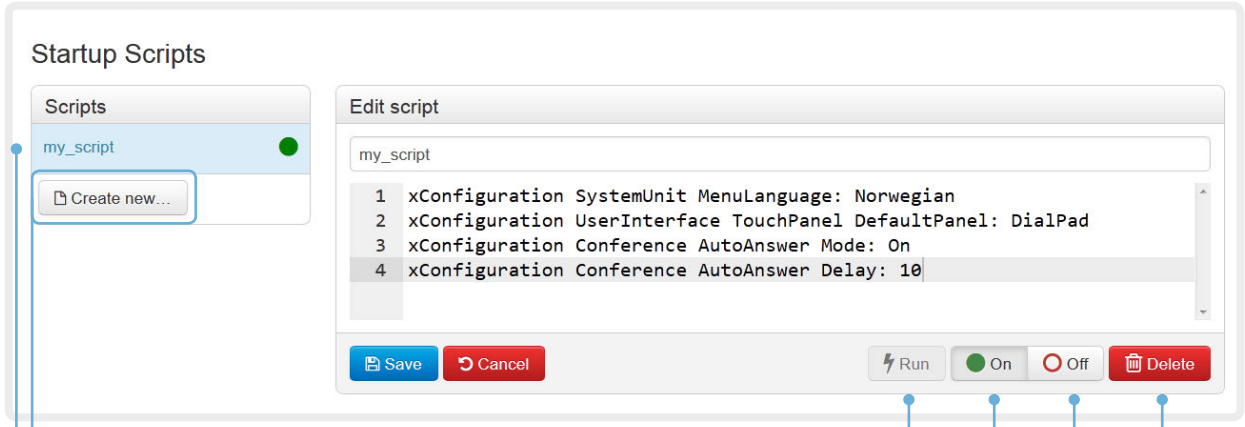
You can create one or more startup scripts* that will run every time the video system starts up.

A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure. A few commands and configurations cannot be placed in a startup script, e.g. `xCommand Boot`. It is not possible to save a script containing illegal commands and configurations.

Syntax and semantics for xCommand and xConfiguration are explained in the API guide for the product.

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

Navigate to: Configuration > Startup Scripts



Creating a startup script

1. Click *Create new...*.
2. Enter a name for your script in the title input filed.
3. Enter the commands (xConfiguration or xCommand) you want to issue in the command input field. Start each command on a new line.
4. Click *Save*.

Running the script immediately

Select the script you want to run and click *Run*.

Running the script at every start up

Select the script you want to activate and click *On*.

Not running the script at start up

Select the script you want to deactivate and click *Off*.

List of startup scripts

Startup scripts are listed here. A green dot appears next to an active script; a red ring appears next to an inactive script.

Deleting a script

Select the script you want to delete and click *Delete*.

* The script name and commands shown in the illustration serve as examples. You may make your own scripts.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Application programming interface

The application programming interface (API) is a tool for integration professionals and developers working with this video system. The API is described in detail in the API guide for the system.

XML files

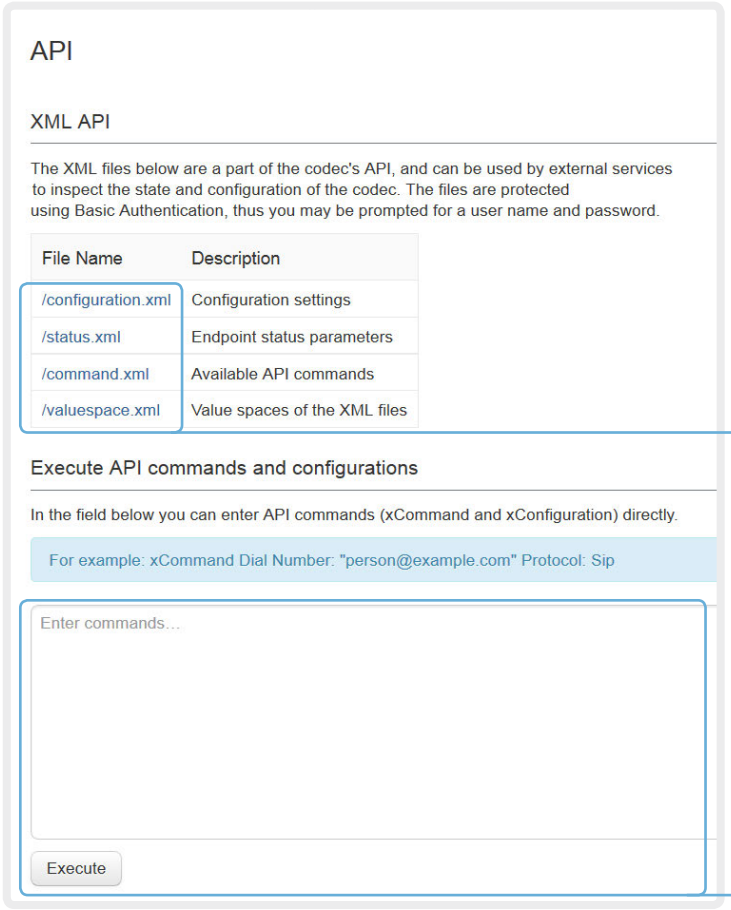
The XML files are part of the codec's API. They structure information about the codec in a hierarchy.

- *Configuration.xml* contains the current system settings (configuration). These settings are controlled from the web interface or from the API (Application Programmer Interface).
- The information in *status.xml* is constantly updated by the system to reflect system and process changes. The status information is normally monitored from the API.
- *Command.xml* contains an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- *Valuespace.xml* contains an overview of all the value spaces used in the system settings, status information, and commands.

API commands

Commands (xCommand) and configurations (xConfiguration) can be executed from this web page. Syntax and semantics are explained in the API guide for the product.

Navigate to: Configuration > API



Opening an XML file

Click the file name to open the XML file.

Executing API commands

Enter a command, or a sequence of commands, in the text area and click *Execute* to issue the command(s).

www.cisco.com – Copyright © 2010-2014 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, SIP and IEEE 802.1X.

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.

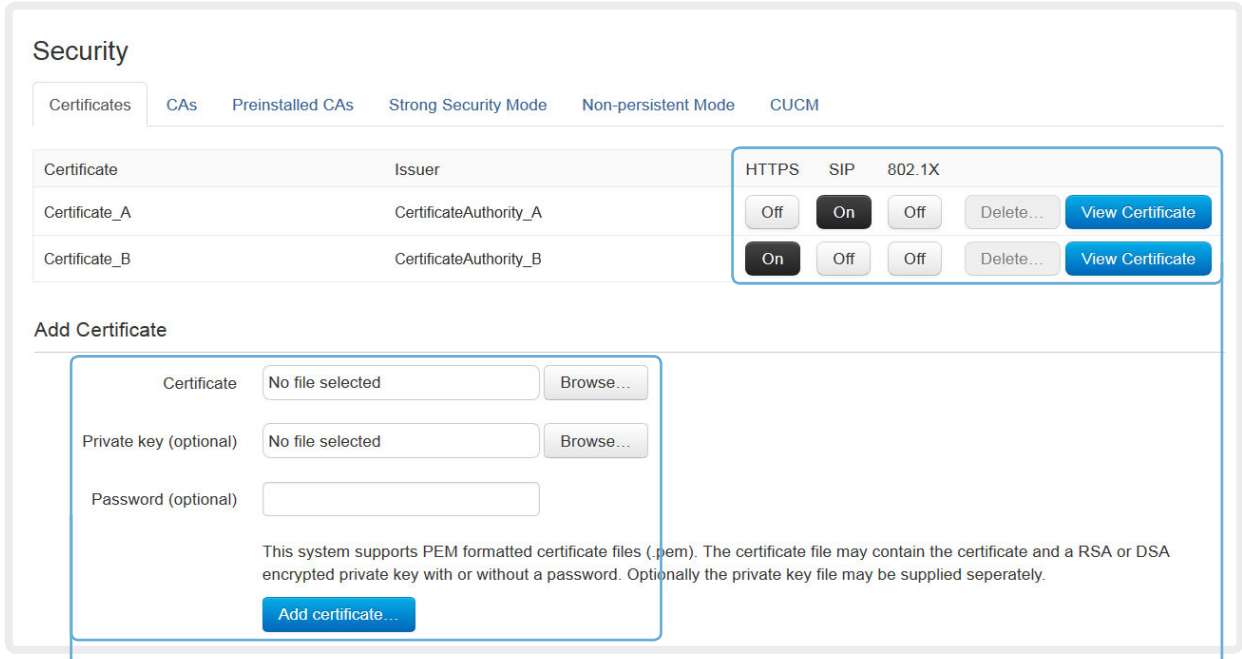
Contact your system administrator to obtain the following file(s):

- Certificate (file format: .PEM)
- Private key, may be 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.

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

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.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Managing the list of trusted certificate authorities

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 system before communication can be set up.

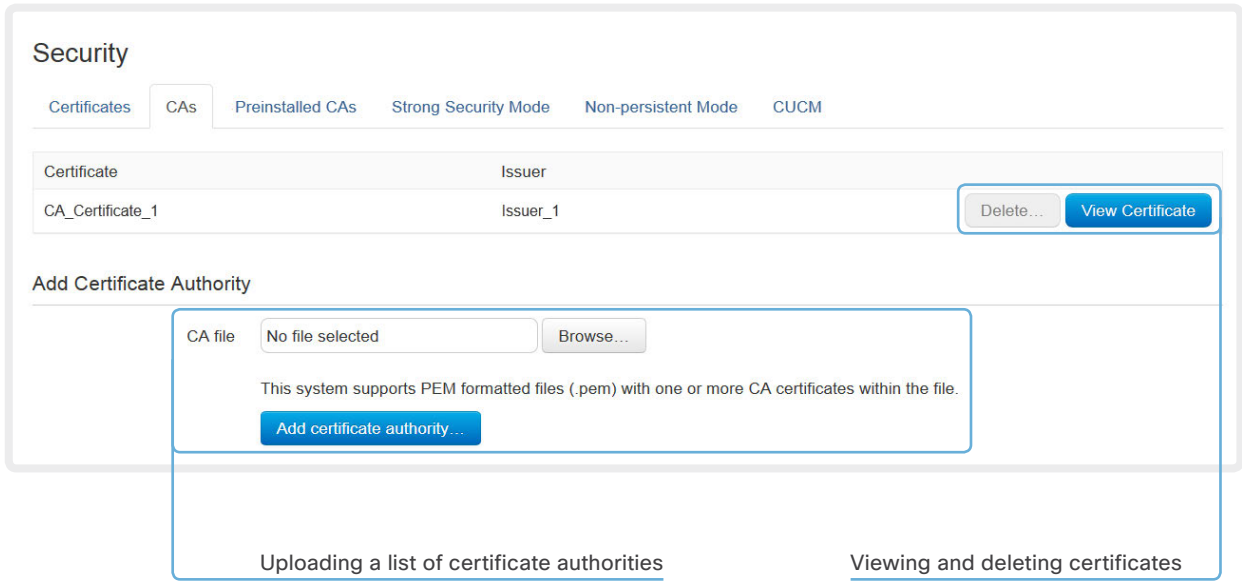
The certificates are text files that verify the authenticity of the server or client. The certificates must be signed by a trusted certificate authority (CA).

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 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, that is, 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Adding audit certificates

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 on the on-screen menu or the web interface.

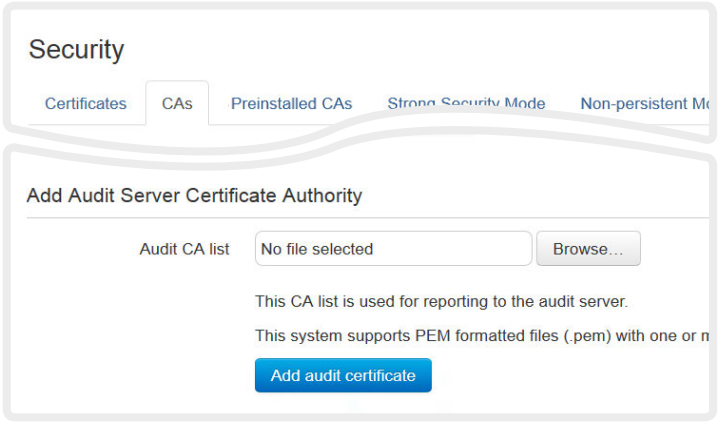
In ExternalSecure audit logging mode the video system sends encrypted audit logs to an external audit server (syslog server), which identity must be verified by a signed certificate.

To be able to verify the signature of the audit server certificates, a list of trusted audit certificate authorities (CAs) must reside on the video system.

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

Always upload the audit certificate list before enabling secure audit logging.

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



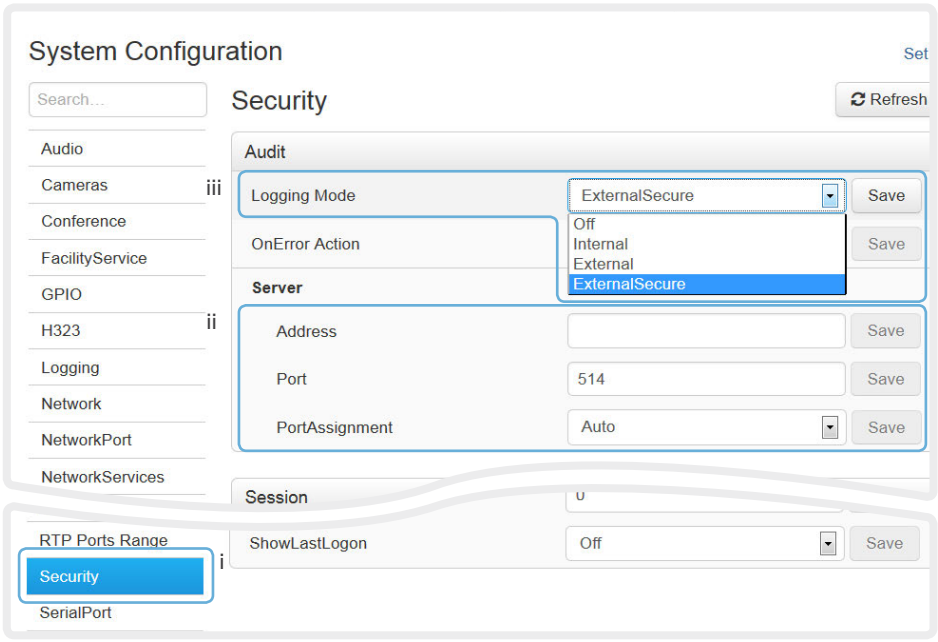
1. Upload a list of audit server certificates

The entries in a new file with CA certificates will overwrite the existing list, that is, any previously stored audit certificates will be lost when you add a new file.

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

ii. Click *Add audit certificate* to store the certificate(s) on your system.

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



2. 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

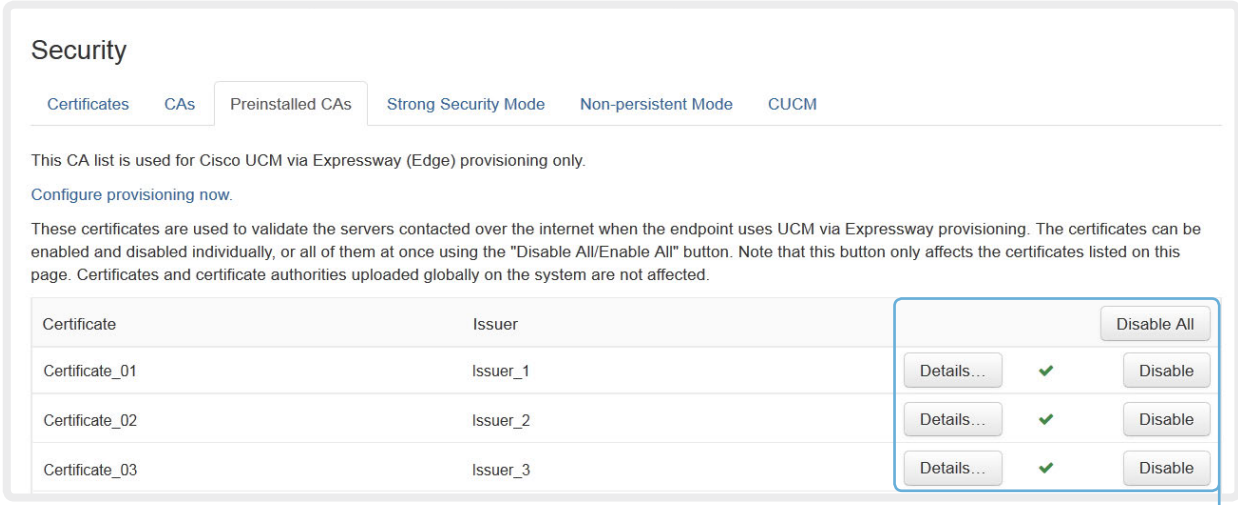
Managing pre-installed certificates for Edge provisioning

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Setting strong security mode

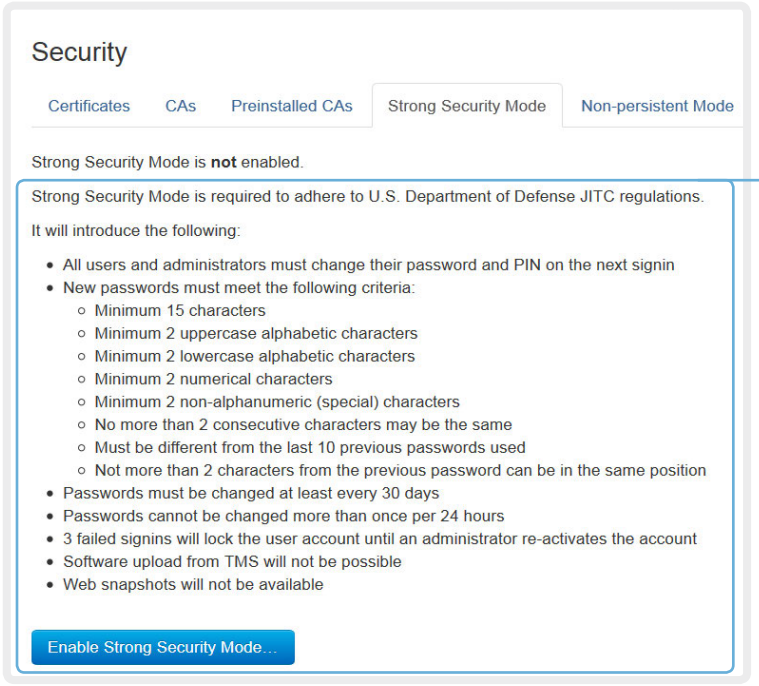
Strong security mode should be used only when compliance with DoD JITC regulations is required.

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.

Software upload from TMS, web snapshots and calling from the web interface are prohibited in strong security mode.

Navigate to: Configuration > Security: Strong Security Mode tab



Setting strong security mode

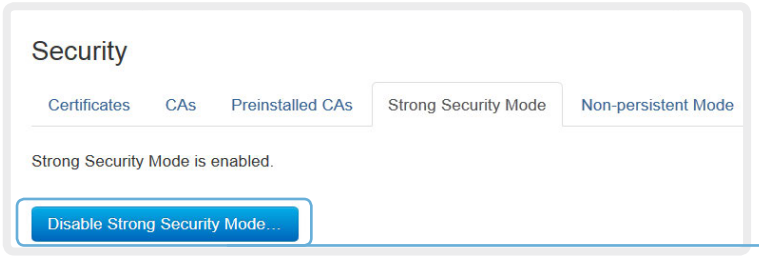
Read carefully about the consequences of strong security mode before you continue.

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 © 2010-2014 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:

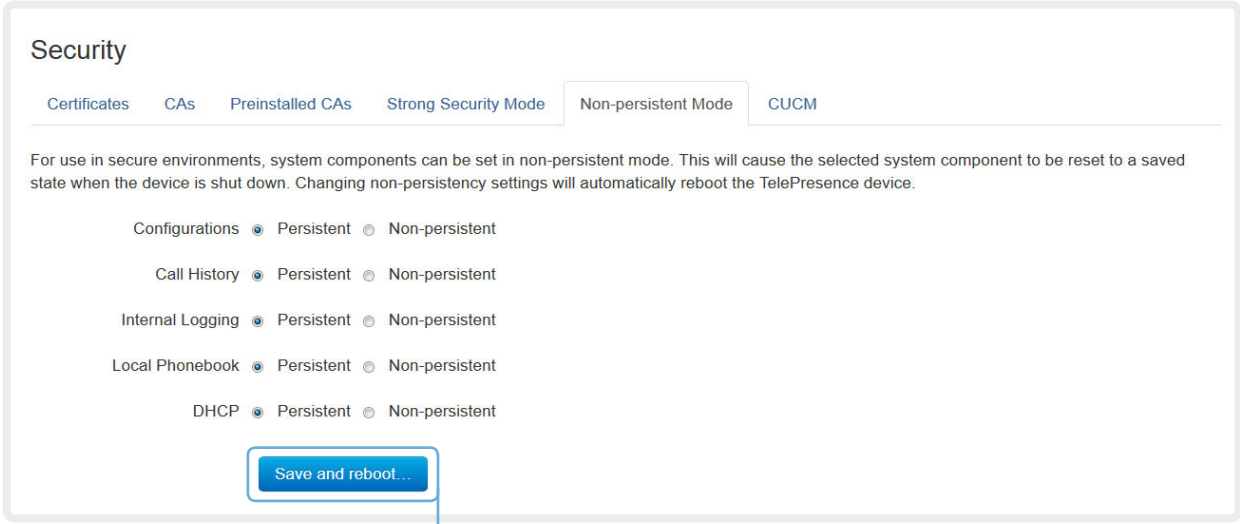
- System Configuration changes that have been made since the last system restart.
- Information about calls that are placed or received since the last system restart (call history).
- Internal log files that has been made since the last system restart.
- Changes that are made to the local phonebook / 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

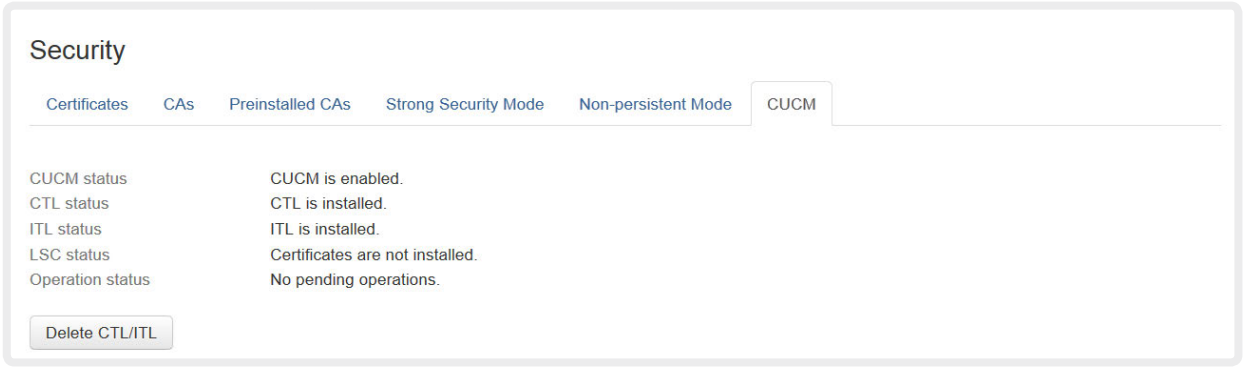
Deleting trust lists (CUCM only)

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.

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 © 2010-2014 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.

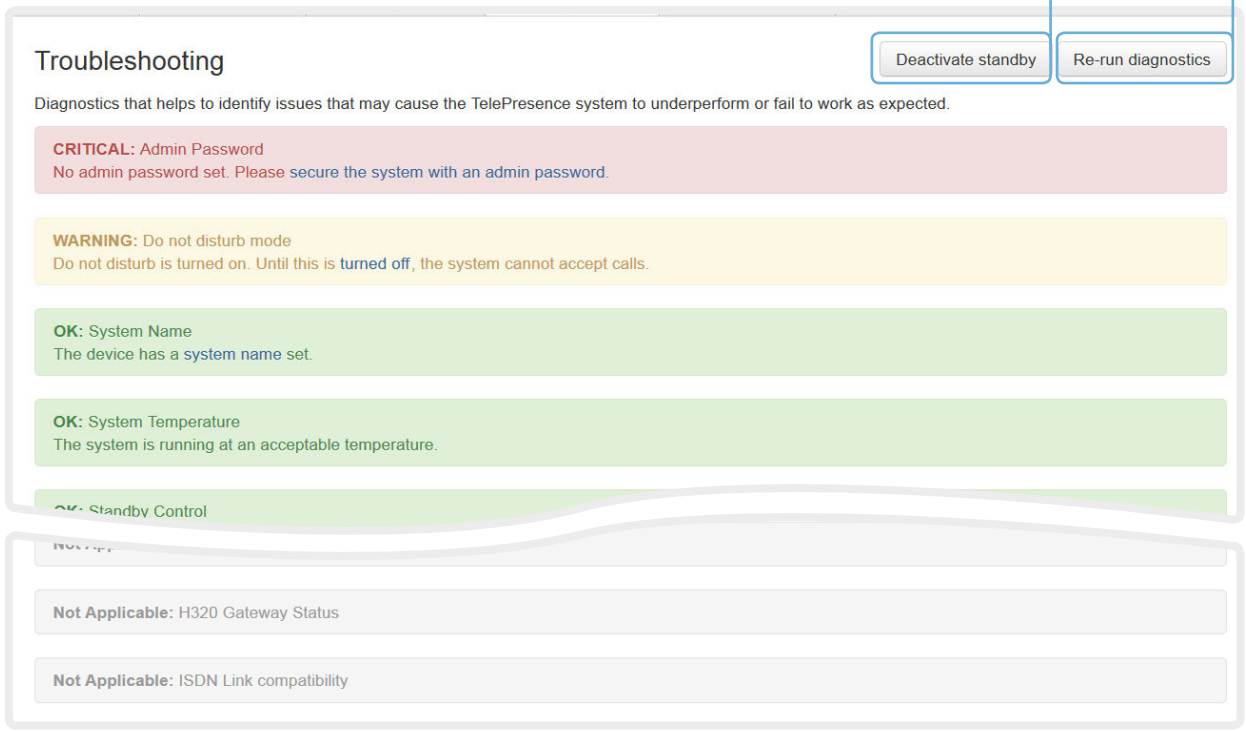
Navigate to: Diagnostics > Troubleshooting

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

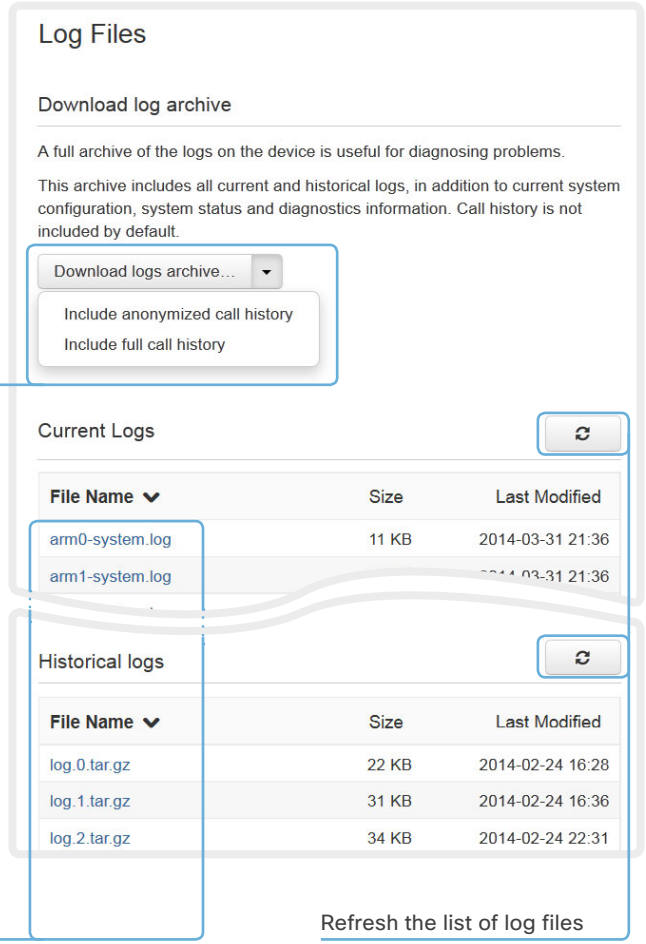
Downloading log files

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.

Use the drop down list if you want to include the call history in the archive. You can choose whether to include the full call history or to make the caller/callee anonymous.

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.

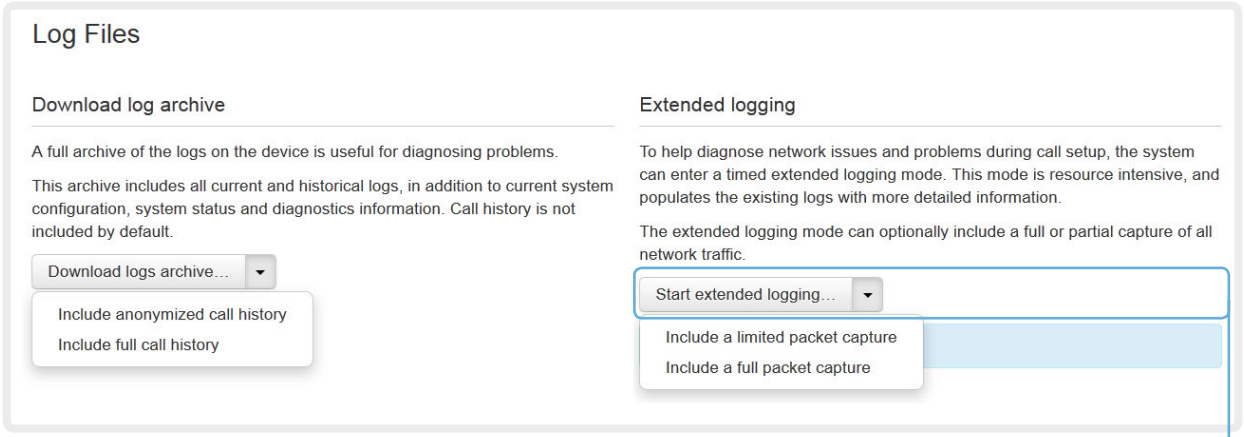
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 © 2010-2014 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 TC7.1.

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-integrator-c-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.

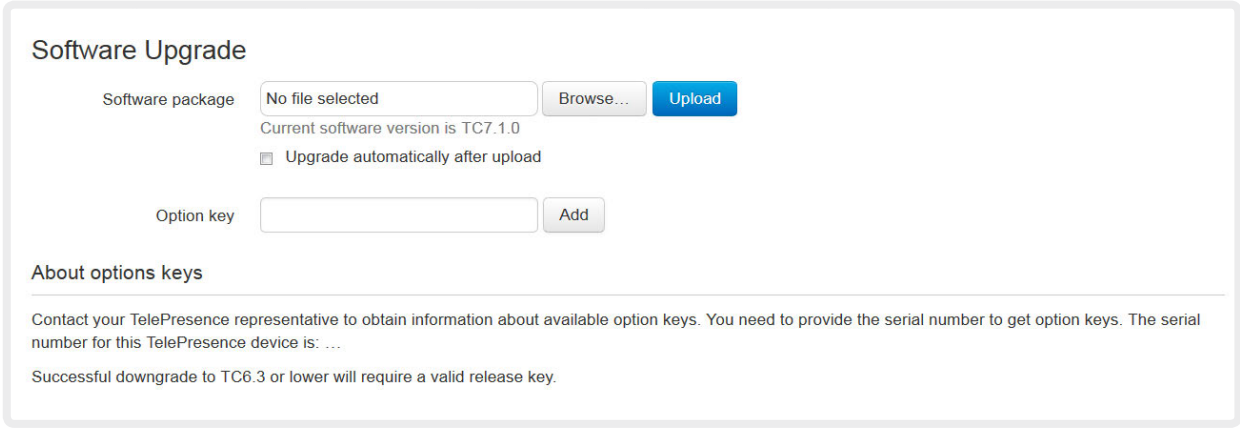
The format of the file name is "s52000tc7_1_0.pkg" (each software version has a unique file name).

Release key

You need a valid release key to be able to use the video system. As from version TC6.1, any TC release key will do. For older releases the release key is specific for each main release (e.g. TC4, TC5, TC6).

Normally, you do not need to install the release key yourself. The release key is preserved when you upgrade from an earlier software version, and the release key is pre-installed on new systems. As from TC7.0, it is no longer possible to enter a release key from the web interface.

Navigate to: Maintenance > Software Upgrade



Adding option keys

An *option key* is required to activate optional functionality. You may have several option keys in your system. If the keys are already installed, you can skip this point and continue with the software installation.

If you do not have the required key(s), contact your Cisco representative to obtain them.

i. Enter an *Option Key* in the appropriate text input field and click *Add*.

   If you have more than one option key, repeat this step for all keys.

Each system has unique keys, for example:

- 1R000-1-AA7A4A09

Installing 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. Check the *Upgrade automatically after upload* check box, then click *Upload* to start the installation process straight away.

   Keep the check box unchecked if you want to upload the software now and do the installation later.

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.

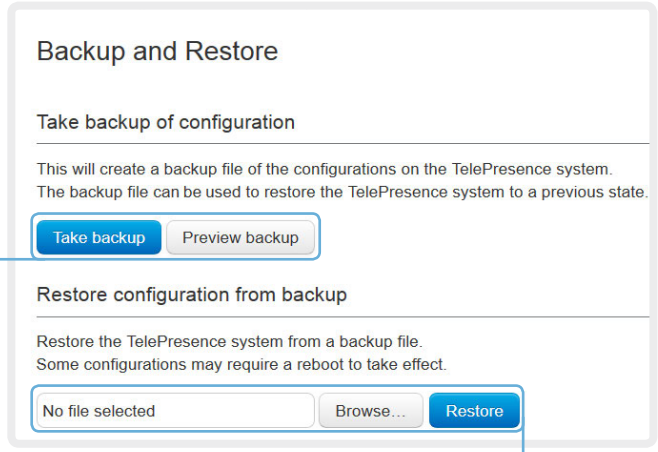
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 (.tsh).

The .tsh 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Reverting to the previously used software version

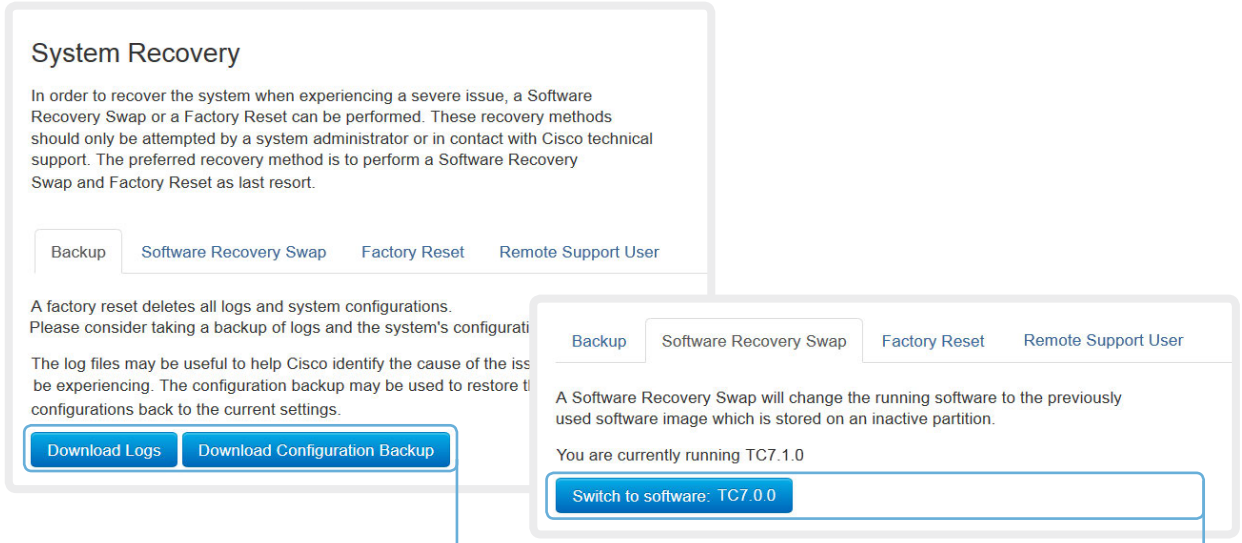
If there is a severe problem with the video system, switching to the previously used software version may help solving the problem.

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 © 2010-2014 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 backgrounds, certificates, and the favorites list (My contacts).
- The previous (inactive) software image will be deleted.
- Release keys and option keys will **not** be affected.

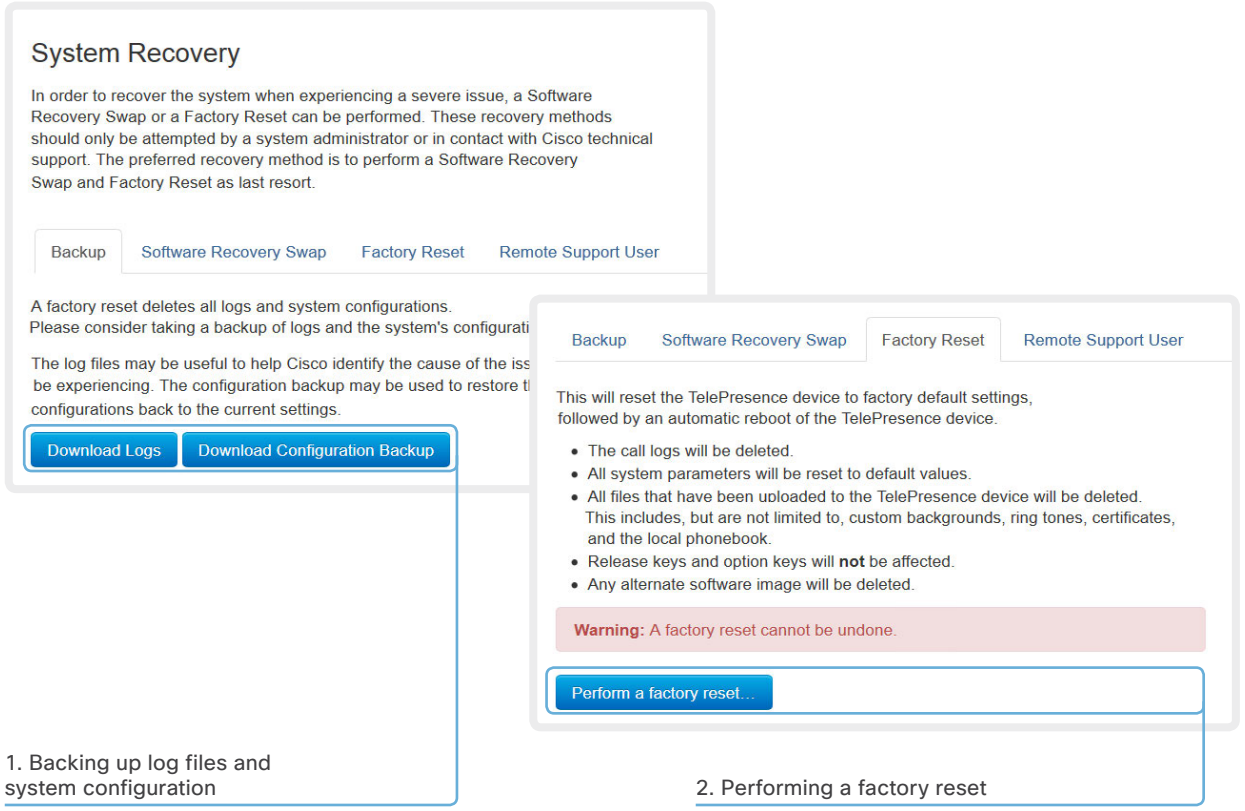
The system restarts automatically after the reset. It is using the same software image as before.

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 restore the factory settings by clicking *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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Remote support user

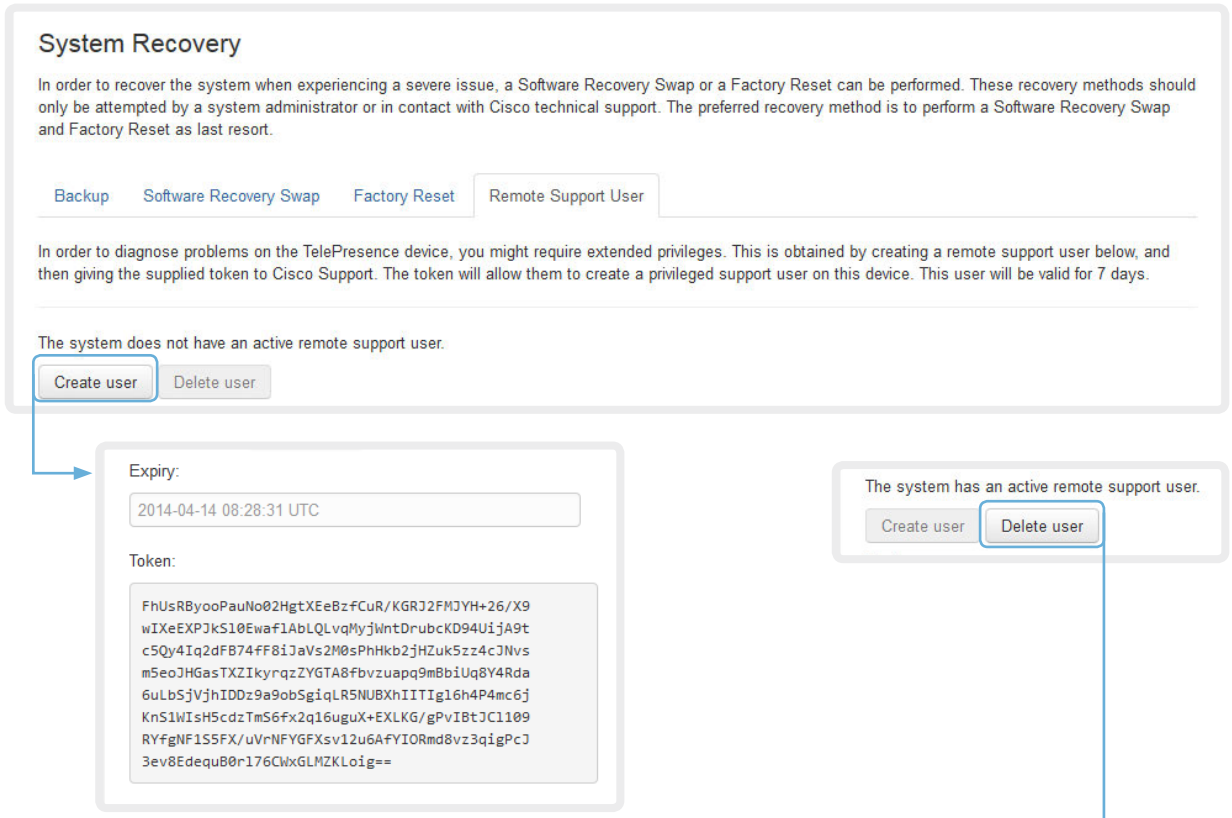
In cases where you need to diagnose problems on the TelePresence device you can create a remote support user.

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* that is valid for seven days, or until the remote support user is deleted.

Delete remote support user

Click Delete user.

www.cisco.com – Copyright © 2010-2014 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Chapter 3

System settings

www.cisco.com – Copyright © 2010-2014 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 controller and tap *System Information*; or navigate to *Home > Settings > System information* when using a remote control and the on-screen menu.

* 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 controller.

Audio settings 64
Audio DefaultVolume 69
Audio Input HDMI [2] Level 64
Audio Input HDMI [2] Mode 64
Audio Input HDMI [2] VideoAssociation MuteOnInactiveVideo 64
Audio Input HDMI [2] VideoAssociation VideoInputSource 64
Audio Input Line [1..2] Channel 65
Audio Input Line [1..2] Equalizer ID 64
Audio Input Line [1..2] Equalizer Mode 64
Audio Input Line [1..2] Level 65
Audio Input Line [1..2] LoopSuppression 65
Audio Input Line [1..2] Mode 65
Audio Input Line [1..2] VideoAssociation MuteOnInactiveVideo 65
Audio Input Line [1..2] VideoAssociation VideoInputSource 65
Audio Input Microphone [1..2]/[1..4] EchoControl Dereverberation 66
Audio Input Microphone [1..2]/[1..4] EchoControl Mode 66
Audio Input Microphone [1..2]/[1..4] EchoControl NoiseReduction 66
Audio Input Microphone [1..2]/[1..4] Equalizer ID 66
Audio Input Microphone [1..2]/[1..4] Equalizer Mode 66
Audio Input Microphone [1..2]/[1..4] Level 67
Audio Input Microphone [1..2]/[1..4] Mode 67
Audio Input Microphone [1..2]/[1..4] Type 67
Audio Input Microphone [1..2]/[1..4] VideoAssociation MuteOnInactiveVideo 67
Audio Input Microphone [1..2]/[1..4] VideoAssociation VideoInputSource 67
Audio Microphones Mute Enabled 69
Audio Output HDMI [1] Level 67
Audio Output HDMI [1] Mode 68
Audio Output Line [1..2] Channel 68
Audio Output Line [1..2] Equalizer ID 68
Audio Output Line [1..2] Equalizer Mode 68
Audio Output Line [1..2] Level 68
Audio Output Line [1..2] Mode 68
Audio Output Line [1] Type 68
Audio Output Line [2] Type 69
Audio SoundsAndAlerts KeyTones Mode 69
Audio SoundsAndAlerts RingTone 69
Audio SoundsAndAlerts RingVolume 69
Audio Volume 70

Cameras settings 71
Cameras Camera [1..7] Backlight 71
Cameras Camera [1..7] Brightness Level 71
Cameras Camera [1..7] Brightness Mode 71
Cameras Camera [1..7] DHCP 73
Cameras Camera [1..7] Flip 71
Cameras Camera [1..7] Focus Mode 72
Cameras Camera [1..7] Gamma Level 72
Cameras Camera [1..7] Gamma Mode 72
Cameras Camera [1..7] IrSensor 72
Cameras Camera [1..7] Mirror 72
Cameras Camera [1..7] MotorMoveDetection 73
Cameras Camera [1..7] Whitebalance Level 73
Cameras Camera [1..7] Whitebalance Mode 73
Cameras PowerLine Frequency 71

Conference settings 74
Conference [1..1] AutoAnswer Delay 74
Conference [1..1] AutoAnswer Mode 74
Conference [1..1] AutoAnswer Mute 74
Conference [1..1] CallProtocolIPStack 74
Conference [1..1] DefaultCall Protocol 76
Conference [1..1] DefaultCall Rate 76
Conference [1..1] DoNotDisturb DefaultTimeout 75
Conference [1..1] DoNotDisturb Mode 75
Conference [1..1] Encryption Mode 76
Conference [1..1] FarEndControl Mode 75
Conference [1..1] FarEndControl SignalCapability 75
Conference [1..1] IncomingMultisiteCall Mode 79
Conference [1..1] MaxReceiveCallRate 76
Conference [1..1] MaxTotalReceiveCallRate 77
Conference [1..1] MaxTotalTransmitCallRate 77
Conference [1..1] MaxTransmitCallRate 76

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Conference [1..1] MicUnmuteOnDisconnect Mode 75
Conference [1..1] Multipoint Mode 78
Conference [1..1] Presentation OnPlacedOnHold 78
Conference [1..1] Presentation RelayQuality 78
Conference [1..1] VideoBandwidth MainChannel Weight 77
Conference [1..1] VideoBandwidth Mode 77
Conference [1..1] VideoBandwidth PresentationChannel Weight 77
Conference ActiveControl Mode 74

FacilityService settings 80
FacilityService Service [1..5] CallType 80
FacilityService Service [1..5] Name 80
FacilityService Service [1..5] Number 80
FacilityService Service [1..5] Type 80

GPIO settings 81
GPIO Pin [1..4] Mode 81

H323 settings 82
H323 NAT Address 82
H323 NAT Mode 82
H323 Profile [1..1] Authentication LoginName 82
H323 Profile [1..1] Authentication Mode 82
H323 Profile [1..1] Authentication Password 83
H323 Profile [1..1] CallSetup Mode 83
H323 Profile [1..1] Gatekeeper Address 83
H323 Profile [1..1] Gatekeeper Discovery 83
H323 Profile [1..1] H323Alias E164 83
H323 Profile [1..1] H323Alias ID 83
H323 Profile [1..1] PortAllocation 84

Logging settings 85
Logging Mode 85

Network settings 86
Network [1..1] DHCP RequestTFTPServerAddress 87
Network [1..1] DNS Domain Name 87
Network [1..1] DNS Server [1..3] Address 87
Network [1..1] IEEE8021X AnonymousIdentity 90
Network [1..1] IEEE8021X Eap Md5 90
Network [1..1] IEEE8021X Eap Peap 91
Network [1..1] IEEE8021X Eap Tls 91
Network [1..1] IEEE8021X Eap Ttls 91
Network [1..1] IEEE8021X Identity 90
Network [1..1] IEEE8021X Mode 89
Network [1..1] IEEE8021X Password 90
Network [1..1] IEEE8021X TlsVerify 90
Network [1..1] IEEE8021X UseClientCertificate 90
Network [1..1] IPStack 86
Network [1..1] IPv4 Address 86
Network [1..1] IPv4 Assignment 86
Network [1..1] IPv4 Gateway 86
Network [1..1] IPv4 SubnetMask 86
Network [1..1] IPv6 Address 87
Network [1..1] IPv6 Assignment 86
Network [1..1] IPv6 DHCPOptions 87
Network [1..1] IPv6 Gateway 87
Network [1..1] MTU 91
Network [1..1] QoS Diffserv Audio 88
Network [1..1] QoS Diffserv Data 88
Network [1..1] QoS Diffserv ICMPv6 89
Network [1..1] QoS Diffserv NTP 89
Network [1..1] QoS Diffserv Signalling 89
Network [1..1] QoS Diffserv Video 88
Network [1..1] QoS Mode 88
Network [1..1] RemoteAccess Allow 92
Network [1..1] Speed 91
Network [1..1] TrafficControl Mode 91
Network [1..1] VLAN Voice Mode 92
Network [1..1] VLAN Voice VlanId 92

NetworkPort settings 93
NetworkPort [2] Mode 93

NetworkServices settings 94
NetworkServices CTMS Encryption 97
NetworkServices CTMS Mode 97
NetworkServices H323 Mode 94
NetworkServices HTTP Mode 94
NetworkServices HTTPS Mode 95
NetworkServices HTTPS OCSP Mode 95
NetworkServices HTTPS OCSP URL 96
NetworkServices HTTPS VerifyClientCertificate 95
NetworkServices HTTPS VerifyServerCertificate 95
NetworkServices MultiWay Address 95
NetworkServices MultiWay Protocol 95
NetworkServices NTP Address 96
NetworkServices NTP Mode 96
NetworkServices SIP Mode 94
NetworkServices SNMP CommunityName 96
NetworkServices SNMP Host [1..3] Address 96
NetworkServices SNMP Mode 96
NetworkServices SNMP SystemContact 97
NetworkServices SNMP SystemLocation 97
NetworkServices SSH AllowPublicKey 97
NetworkServices SSH Mode 97
NetworkServices Telnet Mode 94
NetworkServices WelcomeText 94
NetworkServices XMLAPI Mode 94

Phonebook settings 98
Phonebook Server [1..1] ID 98
Phonebook Server [1..1] Type 98
Phonebook Server [1..1] URL 98

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

RTP settings 101
RTP Ports Range Start 101
RTP Ports Range Stop 101

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Security settings 102
Security Audit Logging Mode 102
Security Audit OnError Action 102
Security Audit Server Address 102
Security Audit Server Port 102
Security Audit Server PortAssignment 102
Security Session InactivityTimeout 103
Security Session ShowLastLogon 103

SerialPort settings 104
SerialPort BaudRate 104
SerialPort LoginRequired 104
SerialPort Mode 104

SIP settings 105
SIP ANAT 105
SIP AuthenticateTransferror 105
SIP ListenPort 105
SIP OCSP DefaultResponder 105
SIP OCSP Mode 105
SIP PreferredIPMedia 105
SIP PreferredIPSignaling 105
SIP Profile [1..1] Authentication [1..1] LoginName 107
SIP Profile [1..1] Authentication [1..1] Password 107
SIP Profile [1..1] DefaultTransport 107
SIP Profile [1..1] DisplayName 107
SIP Profile [1..1] Ice DefaultCandidate 106
SIP Profile [1..1] Ice Mode 106
SIP Profile [1..1] Line 108
SIP Profile [1..1] Mailbox 108
SIP Profile [1..1] Outbound 108
SIP Profile [1..1] Proxy [1..4] Address 108
SIP Profile [1..1] Proxy [1..4] Discovery 108
SIP Profile [1..1] TlsVerify 107
SIP Profile [1..1] Turn BandwidthProbe 106
SIP Profile [1..1] Turn DiscoverMode 106
SIP Profile [1..1] Turn DropRflx 106
SIP Profile [1..1] Turn Password 107
SIP Profile [1..1] Turn Server 106
SIP Profile [1..1] Turn UserName 106
SIP Profile [1..1] Type 108
SIP Profile [1..1] URI 107

Standby settings 109
Standby BootAction 109
Standby Control 109
Standby Delay 109
Standby StandbyAction 109
Standby WakeupAction 109

SystemUnit settings 110
SystemUnit CallLogging Mode 110
SystemUnit ContactInfo Type 110
SystemUnit IrSensor 111
SystemUnit MenuLanguage 110
SystemUnit Name 110

Time settings 112
Time DateFormat 112
Time TimeFormat 112
Time Zone 112

UserInterface settings 113
UserInterface TouchPanel DefaultPanel 113
UserInterface UserPreferences 113

Video settings 114
Video AllowWebSnapshots 114
Video CamCtrlPip CallSetup Duration 114
Video CamCtrlPip CallSetup Mode 114
Video DefaultPresentationSource 114
Video Input DVI [3]/[2,3] RGBQuantizationRange 114
Video Input DVI [3]/[2,3] Type 115
Video Input HDMI [1..2] RGBQuantizationRange 115
Video Input Source [1..3] CameraControl CameraId 117
Video Input Source [1..3] CameraControl Mode 117
Video Input Source [1..3] Name 115
Video Input Source [1..3] OptimalDefinition Profile 117
Video Input Source [1..3] OptimalDefinition Threshold60fps 118
Video Input Source [1..3] PresentationSelection 116
Video Input Source [1..3] Quality 118
Video Input Source [1..3] Type 116
Video Input Source [1..3] Visibility 116
Video Input Source [1] Connector 115
Video Input Source [2] Connector 115
Video Input Source [3] Connector 116
Video Layout DisableDisconnectedLocalOutputs 118
Video Layout LocalLayoutFamily 119
Video Layout PresentationDefault View 119
Video Layout RemoteLayoutFamily 119
Video Layout ScaleToFrame 120
Video Layout ScaleToFrameThreshold 120
Video Layout Scaling 119
Video MainVideoSource 118
Video Monitors 122
Video OSD AutoSelectPresentationSource 124
Video OSD CallSettingsSelection 124
Video OSD EncryptionIndicator 123
Video OSD InputMethod Cyrillic 125
Video OSD InputMethod InputLanguage 125
Video OSD LanguageSelection 123
Video OSD LoginRequired 125
Video OSD MenuStartupMode 123
Video OSD MissedCallsNotification 123
Video OSD Mode 122
Video OSD MyContactsExpanded 124
Video OSD Output 124
Video OSD TodaysBookings 124
Video OSD VirtualKeyboard 123
Video OSD WallpaperSelection 122
Video Output Composite [3] Location HorizontalOffset 131
Video Output Composite [3] Location VerticalOffset 131
Video Output Composite [3] MonitorRole 132
Video Output Composite [3] OverscanLevel 132
Video Output Composite [3] Resolution 132
Video Output DVI [2] Location HorizontalOffset 128
Video Output DVI [2] Location VerticalOffset 129

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output DVI [2] MonitorRole 129
Video Output DVI [2] OverscanLevel.... 130
Video Output DVI [2] Resolution.... 130
Video Output DVI [2] RGBQuantizationRange 129
Video Output HDMI [1] CEC Mode 127
Video Output HDMI [1] Location HorizontalOffset....126
Video Output HDMI [1] Location VerticalOffset....126
Video Output HDMI [1] MonitorRole 127
Video Output HDMI [1] OverscanLevel....127
Video Output HDMI [1] Resolution....128
Video Output HDMI [1] RGBQuantizationRange 127
Video PIP ActiveSpeaker DefaultValue Position 120
Video PIP Presentation DefaultValue Position 120
Video Selfview 121
Video SelfviewDefault FullscreenMode 121
Video SelfviewDefault Mode....121
Video SelfviewDefault OnMonitorRole....122
Video SelfviewDefault PIPPosition....122
Video SelfviewPosition 121
Video WallPaper....132

Experimental settings 133

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio settings

Audio Input HDMI [2] Mode

Determine if the audio channels on the HDMI input shall be enabled. The HDMI input 2 has two audio channels.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable audio on the HDMI input.

On: Enable audio on the HDMI input.

Example: `Audio Input HDMI 2 Mode: On`

Audio Input HDMI [2] Level

Define the audio level of the HDMI input connector, in steps of 1 dB.

See the Audio Level tables in the Physical Interfaces Guide for the codec for a complete overview of the menu values represented in dB.

Requires user role: ADMIN

Value space: <-24..0>

Range: Select a value from -24 to 0 dB.

Example: `Audio Input HDMI 2 Level: 0`

Audio Input HDMI [2] VideoAssociation MuteOnInactiveVideo

Enable association of a video source to an HDMI audio input.

Requires user role: ADMIN

Value space: <Off/On>

Off: No video source is associated.

On: A video source is associated, and the audio will be muted if the associated video source is not displayed.

Example: `Audio Input HDMI 2 VideoAssociation MuteOnInactiveVideo: Off`

Audio Input HDMI [2] VideoAssociation VideoInputSource

Select the associated video input source.

Requires user role: ADMIN

Value space: <1/2/3>

Range: Select one of the video input sources.

Example: `Audio Input HDMI 2 VideoAssociation VideoInputSource: 1`

Audio Input Line [1..2] Equalizer ID

Select the audio input line equalizer ID.

Requires user role: ADMIN

Value space: <1..8>

Range: Select EqualizerID 1 to 8.

Example: `Audio Input Line 1 Equalizer ID: 1`

Audio Input Line [1..2] Equalizer Mode

Set the audio input line equalizer mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: No equalizer.

On: Enable the equalizer for the audio input line.

Example: `Audio Input Line 1 Equalizer Mode: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Input Line [1..2] VideoAssociation MuteOnInactiveVideo

Enable association of a video source to a Line audio input.

Requires user role: ADMIN

Value space: <Off/On>

Off: No video source is associated.

On: A video source is associated, and the audio will be muted if the associated video source is not displayed.

Example: `Audio Input Line 1 VideoAssociation MuteOnInactiveVideo: Off`

Audio Input Line [1..2] VideoAssociation VideoInputSource

Select the associated video input source.

Requires user role: ADMIN

Value space: <1/2/3>

Range: Select one of the video input sources.

Example: `Audio Input Line 1 VideoAssociation VideoInputSource: 1`

Audio Input Line [1..2] Channel

Define whether the Audio Line input is a mono signal or part of a multichannel signal.

Requires user role: ADMIN

Value space: <Right/Left/Mono>

Right: The Audio Line input signal is the right channel of a stereo signal.

Left: The Audio Line input signal is the left channel of a stereo signal.

Mono: The Audio Line input signal is a mono signal.

Example: `Audio Input 1 Channel: Left`

Audio Input Line [1..2] Level

Define the audio level of the Line input connector, in steps of 1 dB.

See the Audio Level tables in the Physical Interfaces Guide for the codec for a complete overview of the menu values represented in dB.

Requires user role: ADMIN

Value space: <0..24>

Range: Select a value from 0 to 24 dB.

Example: `Audio Input Line 1 Level: 10`

Audio Input Line [1..2] LoopSuppression

Codec C40 and C60 currently does not support loop suppression, hence it is always Off.

Requires user role: ADMIN

Value space: <Off>

Off: Deactivate Loop Suppression.

Example: `Audio Input Line 1 LoopSuppression: Off`

Audio Input Line [1..2] Mode

Set the audio input line mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the Audio Line input.

On: Enable the Audio Line input.

Example: `Audio Input Line 1 Mode: On`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Input Microphone [1..2]/[1..4] EchoControl Mode

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

The echo canceller continuously adjusts itself to the audio characteristics of the room and compensate for any changes it detects in the audio environment. If the changes in the audio conditions are very significant the echo canceller may take a second or two to re-adjust.

Requires user role: ADMIN

Value space: <Off/On>

Off: Echo Control should be switched Off if external echo cancellation or playback equipment is used.

On: Echo Control is normally set to On to prevent the far end from hearing their own audio. Once selected, echo cancellation is active at all times.

Example: `Audio Input Microphone 1 EchoControl Mode: On`

Audio Input Microphone [1..2]/[1..4] EchoControl NoiseReduction

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

The system has a built-in noise reduction which reduces constant background noise (for example noise from air-conditioning systems, cooling fans etc.). In addition, a high pass filter (Humfilter) reduces very low frequency noise. Requires the Echo Control Mode to be enabled for the microphone.

Requires user role: ADMIN

Value space: <Off/On>

Off: Turn off the Noise Reduction.

On: The Noise Reduction should be enabled in the presence of low frequency noise.

Example: `Audio Input Microphone 1 EchoControl NoiseReduction: On`

Audio Input Microphone [1..2]/[1..4] EchoControl Dereverberation

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

The system has built-in signal processing to reduce the effect of room reverberation. Requires the Echo Control Mode to be enabled for the microphone.

Requires user role: ADMIN

Value space: <Off/On>

Off: Turn off the dereverberation.

On: Turn on the dereverberation.

Example: `Audio Input Microphone 1 EchoControl Dereverberation: On`

Audio Input Microphone [1..2]/[1..4] Equalizer ID

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

Select the audio input microphone equalizer ID.

Requires user role: ADMIN

Value space: <1..8>

Range: Select Equalizer ID 1 to 8.

Example: `Audio Input Microphone 1 Equalizer ID: 1`

Audio Input Microphone [1..2]/[1..4] Equalizer Mode

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

Set the audio input microphone equalizer mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: No equalizer.

On: Enable the equalizer for the audio input microphone.

Example: `Audio Input Microphone 1 Equalizer Mode: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Input Microphone [1..2]/[1..4] VideoAssociation MuteOnInactiveVideo

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

Enable association of a video source to a microphone audio input.

Requires user role: ADMIN

Value space: <Off/On>

Off: No video source is associated.

On: A video source is associated, and the audio will be muted if the associated video source is not displayed.

Example: `Audio Input Microphone 1 VideoAssociation MuteOnInactiveVideo: On`

Audio Input Microphone [1..2]/[1..4] VideoAssociation VideoInputSource

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

Select the associated video input source.

Requires user role: ADMIN

Value space: <1/2/3>

Range: Select one of the video input sources.

Example: `Audio Input Microphone 1 VideoAssociation VideoInputSource: 1`

Audio Input Microphone [1..2]/[1..4] Level

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

Define the audio level of the Microphone input connector, in steps of 1 dB.

See the Audio Level tables in the Physical Interfaces Guide for the codec for a complete overview of the values represented in dB.

Requires user role: ADMIN

Value space: <0..24>

Range: Select a value from 0 to 24 dB.

Example: `Audio Input Microphone 1 Level: 14`

Audio Input Microphone [1..2]/[1..4] Mode

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

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 Input Microphone [1..2]/[1..4] Type

NOTE: Codec C40 has two microphone connectors. Codec C60 has four microphone connectors.

The microphone connectors are intended for electret type microphones. The microphone connector can be set to line or microphone mode.

Requires user role: ADMIN

Value space: <Microphone/Line>

Microphone: Select Microphone when you have 48 V Phantom voltage and the pre-amplification is On.

Line: Select Line when you have a standard balanced line input. The phantom voltage and pre-amplification is Off.

Example: `Audio Input Microphone 1 Type: Line`

Audio Output HDMI [1] Level

Define the output level of the HDMI output connector, in steps of 1 dB.

See the Audio Level tables in the Physical Interfaces Guide for the codec for a complete overview of the menu values represented in dB.

Requires user role: ADMIN

Value space: <-24..0>

Range: Select a value from -24 to 0dB.

Example: `Audio Output HDMI 1 Level: 0`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Output HDMI [1] Mode

Determine if the audio channel on the HDMI output connector shall be enabled.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the audio channel on the HDMI output.

On: Enable the audio channel on the HDMI output.

Example: `Audio Output HDMI 1 Mode: On`

Audio Output Line [1..2] Channel

Define whether the Audio Line output is a mono signal or part of a multichannel signal.

Requires user role: ADMIN

Value space: <Right/Left/Mono>

Right: The Audio Line output signal is the right channel of a stereo signal.

Left: The Audio Line output signal is the left channel of a stereo signal.

Mono: The Audio Line output signal is a mono signal.

Example: `Audio Output Line 1 Channel: left`

Audio Output Line [1..2] Equalizer ID

Select the audio output line equalizer ID.

Requires user role: ADMIN

Value space: <1..8>

Range: Select EqualizerID 1 to 8.

Example: `Audio Output Line 1 Equalizer ID: 1`

Audio Output Line [1..2] Equalizer Mode

Set the audio output line equalizer mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: No equalizer.

On: Enable the equalizer for the audio output line.

Example: `Audio Output Line 1 Equalizer Mode: Off`

Audio Output Line [1..2] Level

Define the output level of the Audio Output Line connector, in steps of 1 dB.

See the Audio Level tables in the Physical Interfaces Guide for the codec for a complete overview of the menu values represented in dB.

Requires user role: ADMIN

Value space: <-24..0>

Range: Select a value from -24 to 0 dB.

Example: `Audio Output Line 1 Level: -10`

Audio Output Line [1..2] Mode

Set the audio output line mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the Audio Line output.

On: Enable the Audio Line output.

Example: `Audio Output Line 1 Mode: On`

Audio Output Line [1] Type

Determine if the Audio Line output will be analog or digital type output. The digital output on the Cisco TelePresence Profile systems are identified as DNAM (Digital Natural Audio Module).

Requires user role: ADMIN

Value space: <Auto/SPDIF>

Auto: If a Digital NAM is detected then SPDIF mode will be selected, otherwise analog mode will be selected.

SPDIF: Set to SPDIF when you want the line output to be in digital mode.

Example: `Audio Output Line 1 Type: Auto`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Output Line [2] Type

Line output 2 is a dedicated analog output, hence type can be set to analog only.

Requires user role: ADMIN

Value space: <Analog>

Analog: Can be set to analog only.

Example: `Audio Output Line 2 Type: Analog`

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 pressing a key on the remote control, or 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 a key tone when you press a key or type text.

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.

Remote control: Under Sounds and Alerts in the Settings menu on screen.

API: Run xCommand Audio SoundsAndAlerts Ringtone.

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: 50`

Audio DefaultVolume

Set the default speaker volume. The volume returns to this value when you switch on or restart the video system. You can also run the following API command to return to the default value: xCommand Audio Volume SetToDefault. Run the xCommand Audio Volume commands, or use the remote control or 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: 70`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Audio Volume

Set the speaker volume. This setting is obsoleted by the Audio DefaultVolume setting.

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 Volume: 70`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Cameras settings

Cameras PowerLine Frequency

If your camera supports power line frequency anti-flickering, the camera is able to compensate for any flicker noise from the electrical power supply. You should set this camera configuration based on your power line frequency. If your camera supports auto detection of line frequency, you can select the Auto option in the configuration.

All Cisco Precision cameras support both anti-flickering and auto detection of line frequency. Auto is the default value, so you should change this setting if you have a camera that does not support auto detection.

Requires user role: ADMIN

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 Camera [1..7] 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..7] 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..7] 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 from 1 to 31.

Example: `Cameras Camera 1 Brightness Level: 1`

Cameras Camera [1..7] Flip

With Flip mode (vertical flip) you can flip the image upside down.

Requires user role: ADMIN

Value space: <Auto/Off/On>

Auto: When the camera is placed upside down the image is automatically flipped upside down. This setting will only take effect for a camera that automatically detects which way it is mounted.

Off: Display the video on screen the normal way.

On: When enabled the video on screen is flipped. This setting is used when a camera is mounted upside down, but cannot automatically detect which way it is mounted.

Example: `Cameras Camera 1 Flip: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Cameras Camera [1..7] 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..7] Gamma Mode

Applies to cameras which support gamma mode. Gamma describes the nonlinear relationship between image pixels and monitor brightness. The Cisco TelePresence PrecisionHD 720p camera supports gamma mode. The PrecisionHD 1080p camera does not support gamma mode.

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..7] 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 from 0 to 7.

Example: `Cameras Camera 1 Gamma Level: 0`

Cameras Camera [1..7] IrSensor

The IR sensor LED is located in the front of the camera and flickers when the IR sensor is activated from the remote control. Both the Codec C Series and PrecisionHD camera have IR sensors, and only one of them needs to be enabled at the time.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the IR sensor on the camera.

On: Enable the IR sensor on the camera.

Example: `Cameras Camera 1 IrSensor: On`

Cameras Camera [1..7] Mirror

With Mirror mode (horizontal flip) you can mirror the image on screen.

Requires user role: ADMIN

Value space: <Auto/Off/On>

Auto: When the camera is placed upside down the image is automatically mirrored. Use this setting with cameras that can be mounted upside down, and that can auto detect that the camera is mounted upside down.

Off: See the self-view in normal mode, that is the experience of self-view is as seeing yourself as other people see you.

On: See the self-view in mirror mode, that is the self-view is reversed and the experience of self-view is as seeing yourself in a mirror.

Example: `Cameras Camera 1 Mirror: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Cameras Camera [1..7] MotorMoveDetection

This setting applies only when using a Cisco TelePresence PrecisionHD 1080p12x camera.

If adjusting the camera position by hand you can configure whether the camera should keep its new position or return to the preset or position it had before.

Requires user role: ADMIN

Value space: <Off/On>

Off: When the camera position is adjusted manually the camera will keep this position until adjusted again. WARNING: If moving the camera by hand, the camera will not register the new pan and tilt values since there is no position feedback. This will result in wrong pan and tilt values when recalling the camera presets subsequently.

On: When the camera position is adjusted manually, or the camera detects that the motors have moved, it will first re-initialize (i.e. go to default position) then return to the preset/position it had before the camera was adjusted.

Example: `Cameras Camera 1 MotorMoveDetection: Off`

Cameras Camera [1..7] Whitebalance Mode

Set the camera whitebalance mode.

Requires user role: ADMIN

Value space: <Auto/Manual>

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

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

Example: `Cameras Camera 1 Whitebalance Mode: Auto`

Cameras Camera [1..7] Whitebalance Level

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

Requires user role: ADMIN

Value space: <1..16>

Range: Select a value from 1 to 16.

Example: `Cameras Camera 1 Whitebalance Level: 1`

Cameras Camera [1..7] DHCP

Applies to cameras which support DHCP over LAN. When set, the command enables support for software upgrade of daisy chained cameras.

Requires user role: ADMIN

Value space: <Off/On>

Off: When the camera is not connected to a LAN, set to Off to disable DHCP.

On: Set to On to enable DHCP for the camera. The camera is automatically re-booted, and after re-boot the camera's DHCP function will force start of MAC and IP address retrieval. To see the result, you can run the following API command: "xStatus Camera". When the camera no longer is connected to a LAN, set to Off.

Example: `Cameras Camera 1 DHCP: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Conference settings

Conference ActiveControl Mode

Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server 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 H323 and SIP calls.

IPv4: When set to IPv4, the call protocol (SIP, H323) will use IPv4.

IPv6: When set to IPv6, the call protocol (SIP, H323) will use IPv6.

Example: `Conference 1 CallProtocolIPStack: Dual`

Conference [1..1] AutoAnswer Mode

Set the auto answer mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: An incoming call must be answered manually by pressing the OK key or the green Call key on the remote control, or by tapping the Accept key on the Touch controller.

On: Enable auto answer to let the system automatically answer all incoming calls.

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 from 0 to 50 seconds.

Example: `Conference 1 AutoAnswer Delay: 0`

www.cisco.com – Copyright © 2010-2014 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 Mode

Determine whether to allow incoming calls.

Requires user role: USER

Value space: <Off/On/Timed>

Off: The incoming calls will come through as normal.

On: All incoming calls will be rejected and they will be registered as missed calls. The calling side will receive a busy signal. A message telling that Do Not Disturb is switched on will display on the Touch controller or main display. NOTE: This setting is not recommended as all calls will be rejected until the setting is manually turned off. The recommended option is Timed.

Timed: When set to timed (default), the system will revert back and allow incoming calls after the specified timeout, defined by the setting: Conference DoNotDisturb DefaultTimeout.

Example: `Conference 1 DoNotDisturb Mode: Timed`

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 (remote control or Touch controller) or the Conference DoNotDisturb Mode setting. 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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Conference [1..1] Encryption Mode

Set 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: Requires the Encryption Option Key to be installed. When the Encryption Option Key is not installed the encryption mode is set to 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`

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: H323 ensures that calls are set up as H.323 calls.

Sip: Sip ensures that calls are set up as SIP calls.

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

Example: `Conference 1 DefaultCall Protocol: H323`

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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`

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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`

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) plus one additional audio call.

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 © 2010-2014 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. Note that the facility services are not available when using the remote control and on-screen menu.

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, and the name will show on the facility service call button. The facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 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 facility services are not available when using the remote control and on-screen menu.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 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. Facility services are not available when using the remote control and on-screen menu.

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

GPIO settings

GPIO Pin [1..4] Mode

NOTE: Applies only to Codec C60

The four GPIO pins are configured individually. The state can be retrieved by "xStatus GPIO Pin [1..4] State". The default pin state is High (+12 V). When activated as output, they are set to 0 V. To activate them as input, they must be pulled down to 0 V.

Requires user role: ADMIN

Value space: <InputNoAction/OutputManualState/OutputInCall/OutputMicrophonesMuted/OutputPresentationOn/OutputAllCallsEncrypted/OutputStandbyActive/InputMuteMicrophones>

InputNoAction: The pin state can be set, but no operation is performed.

OutputManualState: The pin state can be set by "xCommand GPIO ManualState Set PinX: <High/Low>" (to +12 V or 0 V, respectively).

OutputInCall: The pin is activated when in call, deactivated when not in call.

OutputMicrophonesMuted: The pin is activated when microphones are muted, deactivated when not muted.

OutputPresentationOn: The pin is activated when presentation is active, deactivated when presentation is not active.

OutputAllCallsEncrypted: The pin is activated when all calls are encrypted, deactivated when one or more calls are not encrypted.

OutputStandbyActive: The pin is activated when the system is in standby mode, deactivated when no longer in standby.

InputMuteMicrophones: When the pin is activated (0 V), the microphones will be muted. When deactivated (+ 12 V), the microphones are unmuted.

Example: `GPIO Pin 1 Mode: InputNoAction`

www.cisco.com – Copyright © 2010-2014 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 authenticatin 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 © 2010-2014 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] 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"`

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"`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

H323 Profile [1..1] PortAllocation

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

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. For RTP and RTCP media data, the system is using UDP ports in the range 2326 to 2487. Each media channel is using two adjacent ports, ie 2330 and 2331 for RTP and RTCP respectively. 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Logging settings

Logging Mode

Not applicable in this version.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Network settings

Network [1..1] IPStack

Select if the sFystem 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 © 2010-2014 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 © 2010-2014 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 © 2010-2014 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 © 2010-2014 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 © 2010-2014 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 from 576 to 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Network [1..1] RemoteAccess Allow

Filter IP addresses for access to ssh/telnet/HTTP/HTTPS.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters, comma separated IP adresses or IP range.

Example: `Network 1 RemoteAccess Allow: "192.168.1.231, 192.168.1.182"`

Network [1..1] VLAN Voice Mode

Set the VLAN voice mode. The VLAN Voice Mode will be set to Auto automatically if you choose Cisco UCM (Cisco Unified Communications Manager) as provisioning infrastructure via the Provisioning Wizard on the Touch controller.

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 from 1 to 4094.

Example: `Network 1 VLAN Voice VlanId: 1`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

NetworkPort settings

NetworkPort [2] Mode

Define if the network port 2 shall be enabled for direct pairing with a Cisco TelePresence Touch controller.

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

Requires user role: ADMIN

Value space: <Inactive/DirectPairing>

Inactive: Set the NetworkPort 2 to Inactive when no device is connected.

DirectPairing: Set the NetworkPort 2 to DirectPairing when you have a Cisco TelePresence Touch controller connected to the port. This will enable for direct pairing between the Touch controller and the codec.

Example: `NetworkPort 2 Mode: Inactive`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

NetworkServices settings

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

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

Requires user role: ADMIN

Value space: <Off/On>

Off: The XML API is disabled.

On: The XML API is enabled (default).

Example: `NetworkServices XMLAPI Mode: On`

www.cisco.com – Copyright © 2010-2014 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: The Codec C60/C40 must run software version TC4.0 (or later), 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 © 2010-2014 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 NTP Mode

The Network Time Protocol (NTP) is used to synchronize the time of the system to a reference time server. The time server will subsequently be queried every 24th hour for time updates. The time will be displayed on the top of the screen. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers requiring H.235 authentication. The system will use the time to timestamp messages transmitted to Gatekeepers or Border Controllers that requires H.235 authentication. It is also used for timestamping Placed Calls, Missed Calls and Received Calls.

Requires user role: ADMIN

Value space: <Auto/Off/Manual>

Auto: The system will use the NTP server, by which address is supplied from the DHCP server in the network. If no DHCP server is used, or the DHCP server does not provide the system with a NTP server address, the system will use the static defined NTP server address specified by the user.

Off: The system will not use an NTP server.

Manual: The system will always use the static defined NTP server address specified by the user.

Example: `NetworkServices NTP Mode: Manual`

NetworkServices NTP Address

Enter the NTP Address to define the network time protocol server address. This address will be used if NTP Mode is set to Manual, or if 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: "1.ntp.tandberg.com"`

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: ReadWrite`

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: ""`

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"`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 running software TC5.0 or later 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 TC6.0 and 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`

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`

www.cisco.com – Copyright © 2010-2014 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: Select Callway if the phonebook is to be provided by the WebEx TelePresence subscription service (formerly called CallWay). Contact your WebEx TelePresence provider for more information.

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 © 2010-2014 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.

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: The video system will be configured using the WebEx TelePresence subscription service (formerly named Callway).

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

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

Edge: The system will be configured using CUCM via Expressway.

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. If Provisioning Mode is Callway (WebEx TelePresence), enter the video number.

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. If Provisioning Mode is Callway (WebEx TelePresence), enter the activation code.

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 © 2010-2014 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

RTP settings

RTP Ports Range Start

Specify the first port in the range of RTP ports. Also see the H323 Profile [1..1] PortAllocation setting.

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

Requires user role: ADMIN

Value space: <1024..65502>

Range: Select a value from 1024 to 65502.

Example: `RTP Ports Range Start: 2326`

RTP Ports Range Stop

Specify the last RTP port in the range. Also see the H323 Profile [1..1] PortAllocation setting.

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

Requires user role: ADMIN

Value space: <1056..65535>

Range: Select a value from 1056 to 65535.

Example: `RTP Ports Range Stop: 2486`

www.cisco.com – Copyright © 2010-2014 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 from 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 © 2010-2014 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

SerialPort settings

SerialPort Mode

Enable/disable the serial port (COM port).

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the serial port.

On: Enable the serial port.

Example: `SerialPort Mode: On`

SerialPort BaudRate

Specify the baud rate (data transmission rate, bits per second) for the serial port. The default value is 38400.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

Requires user role: ADMIN

Value space: <9600/19200/38400/57600/115200>

Range: Select a baud rate from the baud rates listed (bps).

Example: `SerialPort BaudRate: 38400`

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 © 2010-2014 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: <On/Off>

On: Listening for incoming connections on the SIP TCP/UDP ports is turned on.

Off: Listening for incoming connections on the SIP TCP/UDP ports is turned off.

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 © 2010-2014 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: <Off/On>

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 © 2010-2014 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 © 2010-2014 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.

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. It is possible to use a fully qualified domain name, or an IP address. The default port is 5060 for TCP and UDP but another one can be provided. If SIP Profile Outbound is enabled, multiple proxies can be addressed.

Requires user role: ADMIN

Value space: <S: 0, 255>

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

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 behaviour for a vendor or provider.

NOTE: The SIP types Alcatel, Avaya, Microsoft, and Nortel are no longer supported from software version TC6.3.

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 © 2010-2014 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 from 1 to 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

SystemUnit settings

SystemUnit Name

Enter a System Name to define a name of the system unit. If the H.323 Alias ID is configured on the system then this ID will be used instead of the system name. The system name will be displayed:

1) When the codec is acting as an SNMP Agent.
2) Towards a DHCP server.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: `SystemUnit Name: "Meeting Room"`

SystemUnit MenuLanguage

Select the language to be used in the menus on screen, or on the Touch controller. All languages are not supported on both user interfaces. 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/SpanishLatin/Swedish/Turkish/Arabic/Hebrew>

Example: `SystemUnit MenuLanguage: English`

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 or using the xHistory command.

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 main display and Touch controller. The information can also be read with the command xStatus SystemUnit ContactInfo.

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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

SystemUnit IrSensor

Both the Codec C Series and PrecisionHD camera have IR sensors, and only one of them needs to be enabled at the time. The IR sensor LED is located on the front of the codec and the camera and flickers when an IR signal is received from the remote control.

Requires user role: ADMIN

Value space: <Auto/Off/On>

Auto: The system will automatically disable the IR sensor on the codec if the IR sensor at camera is enabled. Otherwise, the IR sensor on the codec will be enabled.

Off: Disable the IR sensor on the codec.

On: Enable the IR sensor on the codec.

Example: `SystemUnit IrSensor: Auto`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Time settings

Time Zone

Set the time zone where the system is located, using Windows time zone description format.

Requires user role: USER

Value space: <GMT-12:00 (International Date Line West)/GMT-11:00 (Midway Island, Samoa)/GMT-10:00 (Hawaii)/GMT-09:00 (Alaska)/GMT-08:00 (Pacific Time (US & Canada); Tijuana)/GMT-07:00 (Arizona)/GMT-07:00 (Mountain Time (US & Canada))/GMT-07:00 (Chihuahua, La Paz, Mazatlan)/GMT-06:00 (Central America)/GMT-06:00 (Saskatchewan)/GMT-06:00 (Guadalajara, Mexico City, Monterrey)/GMT-06:00 (Central Time (US & Canada))/GMT-05:00 (Indiana (East))/GMT-05:00 (Bogota, Lima, Quito)/GMT-05:00 (Eastern Time (US & Canada))/GMT-04:30 (Caracas)/GMT-04:00 (La Paz)/GMT-04:00 (Santiago)/GMT-04:00 (Atlantic Time (Canada))/GMT-03:30 (Newfoundland)/GMT-03:00 (Buenos Aires, Georgetown, Montevideo)/GMT-03:00 (Greenland)/GMT-03:00 (Brasilia)/GMT-02:00 (Mid-Atlantic)/GMT-01:00 (Cape Verde Is.)/GMT-01:00 (Azores)/GMT (Casablanca, Monrovia)/GMT (Coordinated Universal Time)/GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)/GMT+01:00 (West Central Africa)/GMT+01:00 (Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna)/GMT+01:00 (Brussels, Copenhagen, Madrid, Paris)/GMT+01:00 (Sarajevo, Skopje, Warsaw, Zagreb)/GMT+01:00 (Belgrade, Bratislava, Budapest, Ljubljana, Prague)/GMT+02:00 (Harare, Pretoria)/GMT+02:00 (Jerusalem)/GMT+02:00 (Athens, Istanbul, Minsk)/GMT+02:00 (Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius)/GMT+02:00 (Cairo)/GMT+02:00 (Bucharest)/GMT+03:00 (Nairobi)/GMT+03:00 (Kuwait, Riyadh)/GMT+04:00 (Moscow, St. Petersburg, Volgograd)/GMT+03:00 (Baghdad)/GMT+03:30 (Tehran)/GMT+04:00 (Abu Dhabi, Muscat)/GMT+04:00 (Baku, Tbilisi, Yerevan)/GMT+04:30 (Kabul)/GMT+05:00 (Islamabad, Karachi, Tashkent)/GMT+05:00 (Ekaterinburg)/GMT+05:30 (Chennai, Kolkata, Mumbai, New Delhi)/GMT+05:45 (Kathmandu)/GMT+06:00 (Sri Jayawardenepura)/GMT+06:00 (Astana, Dhaka)/GMT+06:00 (Almaty, Novosibirsk)/GMT+06:30 (Rangoon)/GMT+07:00 (Bangkok, Hanoi, Jakarta)/GMT+07:00 (Krasnoyarsk)/GMT+08:00 (Perth)/GMT+08:00 (Taipei)/GMT+08:00 (Kuala Lumpur, Singapore)/GMT+08:00 (Beijing, Chongqing, Hong Kong, Urumqi)/GMT+08:00 (Ulaan Baatar)/GMT+09:00 (Osaka, Sapporo, Tokyo)/GMT+09:00 (Seoul)/GMT+09:00 (Irkutsk)/GMT+09:30 (Darwin)/GMT+09:30 (Adelaide)/GMT+10:00 (Guam, Port Moresby)/GMT+10:00 (Brisbane)/GMT+10:00 (Yakutsk)/GMT+10:00 (Hobart)/GMT+10:00 (Canberra, Melbourne, Sydney)/GMT+11:00 (Magadan, Solomon Is., New Caledonia)/GMT+11:00 (Vladivostok)/GMT+12:00 (Fiji, Kamchatka, Marshall Is.)/GMT+12:00 (Auckland, Wellington)/GMT+13:00 (Nuku alofa)>

Range: Select a time zone from the list time zones. If using a command line interface; watch up for typos.

Example: `Time Zone: "GMT (Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London)"`

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

UserInterface settings

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: On`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video settings

Video AllowWebSnapshots

Allow or disallow snapshots being taken of the local input sources, remote sites and presentation channel. If allowed, the web interface Call Control page will show snapshots both when idle and in a call.

NOTE: This feature is disabled by default, and must be enabled from the on-screen menu, from a directly connected Touch controller, or via the codec's serial port (COM port).

Requires user role: ADMIN

Value space: <Off/On>

Off: Capturing web snapshots is not allowed.

On: Web snapshots can be captured and displayed on the web interface.

Example: `Video AllowWebSnapshots: Off`

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: Off`

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 DefaultPresentationSource

Define which video input source shall be used as the default presentation source when you press the Presentation key on the remote control. If using the Touch controller this setting has no effect. The Video Input Source n Connector setting defines which input connector to use for input source n.

Requires user role: USER

Value space: <1/2/3>

Range: Select the video source to be used as the presentation source.

Example: `Video DefaultPresentationSource: 3`

Video Input DVI [3]/[2,3] RGBQuantizationRange

NOTE: Codec C40 has one DVI input (DVI-I 3). Codec C60 has two DVI inputs (DVI-I 2 and 3).

All devices with DVI inputs 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 DVI 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 1 DVI 3 RGBQuantizationRange: Full`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Input DVI [3]/[2,3] Type

NOTE: Codec C40 has one DVI input (DVI-I 3). Codec C60 has two DVI inputs (DVI-I 2 and 3).

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.

This setting should also be used if the video input is an analog component (YPbPr) type signal. This is used by some cameras (Sony EVI-HD1) and DVD/Blu-ray players. Since it is not possible to auto detect the difference between AnalogRGB and AnalogYPbPr, the AnalogYPbPr setting must be selected.

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 DVI 3 Type: AutoDetect`

Video Input HDMI [1..2] RGBQuantizationRange

All devices with HDMI inputs should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any source.

Requires user role: ADMIN

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 Input 1 HDMI 1 RGBQuantizationRange: Auto`

Video Input Source [1..3] Name

Enter a name for the video input source.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

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

Video Input Source [1] Connector

Select which video input connector to be active on video input source 1.

Requires user role: ADMIN

Value space: <HDMI>

HDMI: Select HDMI when you want to use the HDMI 1 as input source 1.

Example: `Video Input Source 1 Connector: HDMI`

Video Input Source [2] Connector

NOTE: Codec C40 has one DVI input (DVI-I 3). Codec C60 has two DVI inputs (DVI-I 2 and 3).

Select which video input connector to be active on video input source 2.

Requires user role: ADMIN

Value space: <HDMI/DVI>

HDMI: Select HDMI when you want to use the HDMI 2 as input source 2.

DVI: Select DVI-I when you want to use the DVI-I 2 as input source 2.

Example: `Video Input Source 2 Connector: HDMI`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Input Source [3] Connector

NOTE: Codec C40 has one DVI input (DVI-I 3). Codec C60 has two DVI inputs (in this context, use DVI-I 3).

Select which video input connector to be active on video input source 3.

Requires user role: ADMIN

Value space: <DVI/Composite/YC>

DVI: Select DVI when you want to use the DVI-I 3 as input source 3.

Composite: Select Composite when you want to use the Composite as input source 3.

YC: Select YC when you want to use the S-Video (YC) as input source 3. Connect to the two connectors marked Y/Comp and C.

Example: `Video Input Source 3 Connector: DVI`

Video Input Source [1..3] Type

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

Requires user role: ADMIN

Value space: <other/camera/PC/DVD/document_camera>

Other: Select Other when some other type of equipment is connected to the selected video input.

Camera: Select Camera when you have a camera connected to the selected video input.

PC: Select PC when you have a PC connected to the selected video input.

DVD: Select DVD when you have a DVD player connected to the selected video input.

Document_Camera: Select Document_Camera when you have a document camera connected to the selected video input.

Example: `Video Input Source 1 Type: PC`

Video Input Source [1..3] PresentationSelection

Define how the video system will behave when a presentation source is connected to the video input. In general, any input source can be used as a presentation source; normally, the main camera (self-view) will not be used as a presentation source. Note that sharing the presentation with the far end always requires additional action (tap Start Presenting on the Touch controller, or press the Presentation key on the remote control).

Requires user role: ADMIN

Value space: <Manual/Automatic/OnConnect/Hidden>

Manual: In manual mode (default value), the contents of the input source will not be presented on the screen until you select it. Use either the remote control or the Touch controller to choose which input source to present.

Automatic: In automatic mode, the content on the input source 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 was active (presented) when the call was disconnected, the content will still be displayed locally.

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

Hidden: In hidden mode, the contents of the input source do not appear in the graphical user interface.

Example: `Video Input Source 1 PresentationSelection: Manual`

Video Input Source [1..3] Visibility

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

Requires user role: ADMIN

Value space: <Never/Always/IfSignal>

Never: Set to Never when the input source is not expected to be used as a presentation source.

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

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

Example: `Video Input Source 1 Visibility: IfSignal`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Input Source [1..3] CameraControl Mode

Select whether or not to enable camera control for the selected video input source when the video input is active.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable camera control.

On: Enable camera control.

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

Video Input Source [1..3] CameraControl CameraId

Select the ID of the camera in the Visca chain that is connected to this camera source. The CameraId setting represents the camera's position in the Visca chain.

Requires user role: ADMIN

Value space: <1/2/3/4/5/6/7>

Range: Select the ID of the camera in the Visca chain.

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

Video Input Source [1..3] OptimalDefinition Profile

The Video Input Source Quality setting must be set to Motion for the optimal definition settings to take any effect.

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.

Generally, we recommend using the Normal or Medium profiles. However, when the lighting conditions are 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. It is assumed that dual video is not used. 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	1280×720 *
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1280×720 *	1280×720 *
	High	512×288	1024×576	1280×720	1280×720	1280×720 *	1280×720 *	1280×720 *

* The resolution will be 1920×1080 for 1080p60 capable C60 codecs (main board rev F and later).

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 Source 1 OptimalDefinition Profile: Normal`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Input Source [1..3] 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 Source 1 OptimalDefinition Threshold60fps: 1280 _ 720`

Video Input Source [1..3] 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. The Quality setting specifies whether to give priority to high frame rate or to high resolution for a given 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 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 Source 1 Quality: Motion`

Video MainVideoSource

Define which video input source shall be used as the main video source.

Requires user role: USER

Value space: <1/2/3>

Range: Select the source to be used as the main video source.

Example: `Video MainVideoSource: 1`

Video Layout DisableDisconnectedLocalOutputs

Determine whether or not the built-in layout engine shall set layouts on local outputs that have no monitor connected.

Requires user role: ADMIN

Value space: <Off/On>

Off: The built-in layout engine sets layout on all local outputs, also the ones not having any monitor connected.

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

Example: `Video Layout DisableDisconnectedLocalOutputs: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 by the layout database, will be used as the local layout. For more information about the layout database, see the xCommand Video Layout LoadDb command.

FullScreen: The FullScreen layout family will be used as the local layout. It means that the active speaker or presentation will be shown in full screen. Using this value is not recommended as from TC6.0.

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(s).

PresentationSmallSpeaker: The PresentationSmallSpeaker layout family will be used as the local layout. Using this value is not recommended as from TC6.0.

PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the local layout. Using this value is not recommended as from TC6.0.

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`

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. For more information about the layout database, see the command: xCommand Video Layout LoadDb.

FullScreen: The FullScreen layout family will be used as the remote layout. It means that the active speaker or presentation will be shown in full screen. Using this value is not recommended as from TC6.0.

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: The PresentationSmallSpeaker layout family will be used as the remote layout. Using this value is not recommended as from TC6.0.

PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the remote layout. Using this value is not recommended as from TC6.0.

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 from 0 to 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

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 remote control or 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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Selfview

Determine if the main video source (self-view) shall be displayed on screen.
This setting is obsoleted by the Video SelfviewDefault Mode setting.

Requires user role: USER

Value space: <Off/On>

Off: Do not display self-view on screen.

On: Display self-view on screen.

Example: `Video Selfview: On`

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: LowerRight`

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`

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`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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. The value reflects the monitor roles set for the different outputs in the Video Output HDMI/DVI/Composite MonitorRole settings.

The setting applies both when self-view is displayed in full screen, and when it is displayed as picture-in-picture (PiP), but only if the Video Monitors setting is set to Dual.

Requires user role: ADMIN

Value space: <First/Second/Current>

First: The self-view picture will be shown on outputs with the Video Output HDMI/DVI/Composite MonitorRole set to First.

Second: The self-view picture will be shown on outputs with the Video Output HDMI/DVI/Composite MonitorRole set to Second.

Current: When leaving the call, the self-view picture will be kept on the same output as during the call.

Example: `Video SelfviewDefault OnMonitorRole: Current`

Video Monitors

Set the monitor layout mode.

Requires user role: ADMIN

Value space: <Single/Dual/DualPresentationOnly>

Single: The same layout is shown on all monitors.

Dual: The layout is distributed on two monitors.

DualPresentationOnly: All participants in the call will be shown on the first monitor, while the presentation (if any) will be shown on the second monitor.

Example: `Video Monitors: Single`

Video OSD Mode

The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control. Define which icons and information to be displayed on screen.

Requires user role: ADMIN

Value space: <Off/On>

Off: Hide the on-screen menus, icons and indicators.

On: Display the on-screen menus, icons and indicators.

Example: `Video OSD Mode: On`

Video OSD WallpaperSelection

In cases where you want to prevent users from easily changing the wallpaper setting from the Settings menu, the wallpaper setting can be made available from within the Administrator Settings menu. The administrator settings can be password protected. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <Off/On>

Off: The wallpaper setting will be available from within the Video settings in the Administrator Settings.

On: The Wallpaper menu will be available from the Settings menu.

Example: `Video OSD WallpaperSelection: On`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video 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. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <Off/On>

Off: The language settings will be available from within the SystemUnit settings in the Administrator Settings.

On: The Language menu will be available from the Settings menu.

Example: `Video OSD LanguageSelection: On`

Video OSD MenuStartupMode

Configure the state of the on-screen menus after a video system / codec boot.

Requires user role: ADMIN

Value space: <Closed/Home>

Closed: The on-screen menu will NOT expand automatically. This setting is recommended for 3rd party integrations that need full control of what is shown on the OSD.

Home: The on-screen menu will show the home menu expanded.

Example: `Video OSD MenuStartUpMode: Home`

Video OSD VirtualKeyboard

Determine whether or not the virtual keyboard will automatically show on screen when text is to be entered in an input field. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <UserSelectable/AlwaysOn>

UserSelectable: The user has to press a softbutton to open or close the virtual keyboard.

AlwaysOn: The virtual keyboard is automatically shown on screen as long as text can be entered in an input field.

Example: `Video OSD VirtualKeyboard: UserSelectable`

Video 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: `Video OSD EncryptionIndicator: Auto`

Video OSD MissedCallsNotification

Define if there should be a missed calls notification on screen. The setting only applies when the video system is operated by a remote control and the on-screen menu. When using the Touch controller the notification dialog box will appear on the Touch controller, and not on the OSD.

Requires user role: ADMIN

Value space: <Off/On>

Off: The OSD will NOT show any indication that there have been any missed calls. This setting is recommended for 3rd party integrations that need full control of what is shown on the OSD.

On: The OSD will show a notification of missed calls.

Example: `Video OSD MissedCallsNotifications: On`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video OSD AutoSelectPresentationSource

Determine if the presentation source should be automatically selected.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable automatic selection of the presentation source.

On: Enable automatic selection of the presentation source.

Example: `Video OSD AutoSelectPresentationSource: Off`

Video OSD CallSettingsSelection

In cases where you want to prevent users from easily changing the call settings from the Settings menu, the call settings can be made available from within the Administrator Settings menu. The administrator settings can be password protected. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <Off/On>

Off: The call settings will be available from within the Conference settings in the Administrator Settings.

On: The Call Settings menu will be available from the Settings menu.

Example: `Video OSD CallSettingsSelection: Off`

Video OSD TodaysBookings

This setting can be used to display the system's bookings for today on the main on-screen menu. This requires that the system is bookable by an external booking system, like for example the Cisco TelePresence Management Suite (TMS).

Requires user role: ADMIN

Value space: <Off/On>

Off: Do not display todays bookings.

On: Displays information about this systems bookings on screen.

Example: `Video OSD TodaysBookings: Off`

Video OSD MyContactsExpanded

Set how the local contacts will be displayed in the phone book dialog on screen. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <Off/On>

Off: The local contacts will be placed in a separate folder called MyContacts in the phonebook dialog.

On: The local contacts in the phone book will be shown in the top level of the phonebook dialog.

Example: `Video OSD MyContactsExpanded: Off`

Video OSD Output

Define on which monitor the on-screen menus, information and icons should be displayed. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

Requires user role: ADMIN

Value space: <Auto/1/2>

Auto: The system will detect when a monitor is connected to the video output, and send the OSD to the first monitor you connect. If you have a multi-monitor setup, and all monitors are connected before switching on the system, the OSD will be sent to the video output with the lowest numbering, starting on Video OSD Output 1. If the OSD does not show on the desired monitor, disconnect all monitors and reconnect the monitors.

Range 1-2: If you want the OSD to be sent to one specific output, select 1 for HDMI 1 output, or select 2 for DVI-I 2 output. Make sure you connect a monitor to the corresponding video output connector.

Example: `Video OSD Output: Auto`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video OSD InputMethod InputLanguage

The codec can be enabled for Cyrillic input characters in the menus on screen. Requires that Video OSD InputMethod Cyrillic is set to On.

Requires user role: ADMIN

Value space: <Latin/Cyrillic>

Latin: Latin characters can be entered when using the remote control (default).

Cyrillic: Cyrillic characters can be entered using the remote control. Requires a Cisco TelePresence Remote Control with Cyrillic fonts.

Example: `Video OSD InputMethod InputLanguage: Latin`

Video OSD InputMethod Cyrillic

Set the Cyrillic mode for the menu input language in the menus on screen.

Requires user role: ADMIN

Value space: <Off/On>

Off: Cyrillic mode is NOT available as a menu input language in the menus on screen.

On: Cyrillic mode is available as a menu input language in the menus on screen. This will enable the setting Video OSD InputMethod InputLanguage.

Example: `Video OSD InputMethod Cyrillic: Off`

Video OSD LoginRequired

Determine if the system should require the user to login before accessing the menus on screen. If enabled, the user must enter his username and his PIN code. After the user has logged in he can only execute to the configurations changes and commands allowed by his role. The OSD (On Screen Display) is where you find the menus, dialogs, icons and indicators, and the navigation is done with a remote control.

NOTE: The PIN code must be set before enabling this setting, this is done from a web interface. Login to the system from a web browser, navigate to Configuration > User Administration, select the user and add the PIN code.

Requires user role: ADMIN

Value space: <Off/On>

Off: No login to the menus on screen (OSD) is required.

On: The user must log in to access the menus on screen (OSD).

Example: `Video OSD LoginRequired: Off`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output HDMI [1] 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.

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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] Location: HorizontalOffset = 1, VerticalOffset = 0 (Only for Codec C60)

Requires user role: ADMIN

Value space: <-100..100>

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

Example: `Video Output HDMI 1 Location HorizontalOffset: -1`

Video Output HDMI [1] 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.

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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] Location: HorizontalOffset = 1, VerticalOffset = 0 (Only for Codec C60)

Requires user role: ADMIN

Value space: <-100..100>

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

Example: `Video Output HDMI 1 Location Vertical Offset: 0`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output HDMI [1] RGBQuantizationRange

Devices connected to an HDMI output should follow the rules for RGB video quantization range defined in CEA-861. Unfortunately some devices do not follow the standard and this configuration may be used to override the settings to get a perfect image with any display. 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 HDMI 1 RGBQuantizationRange: Full`

Video Output HDMI [1] CEC Mode

The HDMI outputs support 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. The monitor connected to the HDMI output must be CEC compatible and CEC must be configured on the monitor for this to happen.

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 HDMI 1 CEC Mode: Off`

Video Output HDMI [1] MonitorRole

The HDMI monitor role describes which video stream will be shown on the monitor connected to the video output HDMI connector.

Requires user role: ADMIN

Value space: <Auto/First/Second/PresentationOnly/Recorder>

Auto: The system will detect when a monitor is connected and assign a monitor role to it. The first monitor connected will be assigned monitor role First. In a multi-monitor setup the next monitor will be assigned monitor role Second.

First/Second: Define the role of the monitor in a multi-monitor setup. In a single-monitor setup, there is no difference between First and Second.

PresentationOnly: Show presentation video stream if active, and nothing else.

Recorder: Show all participants, including the local main video. If active, also show the presentation.

Example: `Video Output HDMI 1 MonitorRole: Auto`

Video Output HDMI [1] OverscanLevel

Some monitors may not present the entire image that it receives. This means that the outer parts of the image that is sent out on the systems video output may be cut off when displayed on the monitor.

Use this setting to instruct the video system to not use the outer part of the available frame, i.e. to not use the part that might not be presented on 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 system will use all of the output resolution.

Medium: The system will not use the outer 3% of the output resolution.

High: The system will not use the outer 6% of the output resolution.

Example: `Video Output HDMI 1 OverscanLevel: None`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output HDMI [1] Resolution

Set the resolution and refresh rate for the monitor that is connected to the HDMI output.

Requires user role: ADMIN

Value space: <Auto/640_480_60/800_600_60/1024_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_60/1600_1200_60/1680_1050_60/1920_1200_60>

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

640_480_60: The resolution is 640 x 480, and the refresh rate is 60 Hz.

800_600_60: The resolution is 800 x 600, and the refresh rate is 60 Hz.

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.

1600_1200_60: The resolution is 1600 x 1200, and the refresh rate is 60 Hz.

1680_1050_60: The resolution is 1680 x 1050, and the refresh rate is 60 Hz.

1920_1200_60: The resolution is 1920 x 1200, and the refresh rate is 60 Hz.

Example: `Video Output HDMI 1 Resolution: Auto`

Video Output DVI [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.

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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] Location: HorizontalOffset = 1, VerticalOffset = 0 (Only for Codec C60)

Requires user role: ADMIN

Value space: <-100..100>

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

Example: `Video Output DVI 2 Location HorizontalOffset: 0`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output DVI [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.

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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] Location: HorizontalOffset = 1, VerticalOffset = 0 (Only for Codec C60)

Requires user role: ADMIN

Value space: <-100..100>

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

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

Video Output DVI [2] RGBQuantizationRange

Devices connected to a DVI 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 DVI displays 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 Output DVI 2 RGBQuantizationRange: Full`

Video Output DVI [2] MonitorRole

The DVI monitor role describes which video stream will be shown on the monitor connected to the video output DVI-I connector.

Requires user role: ADMIN

Value space: <Auto/First/Second/PresentationOnly/Recorder>

Auto: The system will detect when a monitor is connected and assign a monitor role to it. The first monitor connected will be assigned monitor role First. In a multi-monitor setup the next monitors will be assigned monitor role Second.

First/Second: Define the role of the monitor in a multi-monitor setup. In a single-monitor setup, there is no difference between First and Second.

PresentationOnly: Show presentation video stream if active, and nothing else.

Recorder: Show all participants, including the local main video. If active, also show the presentation.

Example: `Video Output DVI 2 MonitorRole: Auto`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output DVI [2] OverscanLevel

Some monitors may not present the entire image that it receives. This means that the outer parts of the image that is sent out on the systems video output may be cut off when displayed on the monitor.

Use this setting to instruct the video system to not use the outer part of the available frame, i.e. to not use the part that might not be presented on 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 system will use all of the output resolution.

Medium: The system will not use the outer 3% of the output resolution.

High: The system will not use the outer 6% of the output resolution.

Example: `Video Output DVI 2 OverscanLevel: None`

Video Output DVI [2] Resolution

Set the resolution and refresh rate for the monitor that is connected to the DVI-I output.

Requires user role: ADMIN

Value space: <Auto/640_480_60/800_600_60/1024_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_60/1600_1200_60/1680_1050_60/1920_1200_60>

Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.

640_480_60: The resolution is 640 x 480, and the refresh rate is 60 Hz.

800_600_60: The resolution is 800 x 600, and the refresh rate is 60 Hz.

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.

1600_1200_60: The resolution is 1600 x 1200, and the refresh rate is 60 Hz.

1680_1050_60: The resolution is 1680 x 1050, and the refresh rate is 60 Hz.

1920_1200_60: The resolution is 1920 x 1200, and the refresh rate is 60 Hz.

Example: `Video Output DVI 2 Resolution: Auto`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output Composite [3] Location HorizontalOffset

NOTE: Applies only to Codec C60.

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have three displays side by side, with the left and right displays at equal distance from center. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display, and HorizontalOffset = 1 for the right 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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] 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 Composite 3 Location HorizontalOffset: 1`

Video Output Composite [3] Location VerticalOffset

NOTE: Applies only to Codec C60.

HorizontalOffset and VerticalOffset settings are associated with each video output. These settings are used to signal the relative position of the displays that are connected to these outputs.

HorizontalOffset = 0 and VerticalOffset = 0 indicates that the display is positioned in center, both horizontally and vertically. A negative horizontal offset indicates that the monitor is left of center, and a positive horizontal offset indicates that the monitor is right of center. A negative vertical offset indicates that the monitor is below center, and a positive vertical offset indicates that the monitor is above center. The magnitude of the offset indicates how far the display is from center (relative to other displays).

Example: You have three displays side by side, with the left and right displays at equal distance from center. Then the following settings will apply: HorizontalOffset = 0 for the center display, HorizontalOffset = -1 for the left display, and HorizontalOffset = 1 for the right 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 HDMI [1] Location: HorizontalOffset = -1, VerticalOffset = 0

Video Output DVI [2] Location: HorizontalOffset = 0, VerticalOffset = 0

Video Output Composite [3] 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 Composite 3 Location Vertical Offset: 0`

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Video Output Composite [3] MonitorRole

NOTE: Applies only to Codec C60.

The Composite monitor role describes which video stream will be shown on the monitor connected to the video output Composite connector.

Requires user role: ADMIN

Value space: <Auto/First/Second/PresentationOnly/Recorder>

Auto: The system will detect when a monitor is connected and assign a monitor role to it. The first monitor connected will be assigned monitor role First. In a multi-monitor setup the next monitors will be assigned monitor role Second.

First/Second: Define the role of the monitor in a multi-monitor setup. In a single-monitor setup, there is no difference between First and Second.

PresentationOnly: Show presentation video stream if active, and nothing else.

Recorder: Show all participants, including the local main video. If active, also show the presentation.

Example: `Video Output Composite 3 MonitorRole: Auto`

Video Output Composite [3] OverscanLevel

NOTE: Applies only to Codec C60

Some monitors may not present the entire image that it receives. This means that the outer parts of the image that is sent out on the systems video output may be cut off when displayed on the monitor.

Use this setting to instruct the video system to not use the outer part of the available frame, i.e. to not use the part that might not be presented on 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 system will use all of the output resolution.

Medium: The system will not use the outer 3% of the output resolution.

High: The system will not use the outer 6% of the output resolution.

Example: `Video Output Composite 3 OverscanLevel: None`

Video Output Composite [3] Resolution

NOTE: Applies only to Codec C60

Select the preferred resolution for the monitor connected to the video output Composite connector. This will force the resolution on the monitor.

Requires user role: ADMIN

Value space: <PAL/NTSC>

Range: PAL, NTSC

Example: `Video Output Composite 3 Resolution: NTSC`

Video WallPaper

Select a background image (wallpaper) for the video screen when idle.

Requires user role: USER

Value space: <None/Custom/Growing/Summersky/Waves/Blue>

None: There is no background image on the screen, i.e. the background is black.

Custom: Use the custom wallpaper that is stored on the system as background image on the screen. As default, there is no custom wallpaper stored and the background will be black. You can upload a custom wallpaper to the system using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 2 MByte.

Growing, Summersky, Waves, Blue: The chosen background image is shown on the screen.

Example: `Video Wallpaper: Summersky`

www.cisco.com – Copyright © 2010-2014 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Chapter 4

Setting passwords

www.cisco.com – Copyright © 2010-2014 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 and command line interfaces, and to get access to the Administrator settings from a Touch 8 control panel.

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.

About access to administrator settings when using a remote control and the on-screen menu

Note that the on-screen Administrator Settings menu that is available when using a remote control, is NOT protected by the system password; you have to set a menu password (see next page).

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 *Maintenance* 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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

Setting the menu password

The menu password protects the Administrator Settings menu that is available on-screen when using the remote control.

When starting up the video conference system for the first time anyone can access these settings, because the menu password is not set.

We strongly recommend that you set a menu password, because the administrator settings may severely affect the behavior of the system.

Note that the menu password, as from software version TC7.0, applies only to the on-screen Administrator Settings menu; it does not apply to the Administrator menu on the Touch 8 controller.

Setting the menu password from the web interface

1. Sign in to the web interface with your user name and current password.
2. Go to *Configuration > System Configuration*.
3. Click *Set/Change Administrator Settings menu password* to open the menu password dialog.
4. Enter the password in the input field.
5. Click *Save* to set/change the password.

Use the remote control and on-screen menu, or the Touch controller to find the IP address (IPv4 or IPv6).

Remote control and on-screen menu: Navigate to *Home > Settings > System information*.

Touch controller: Tap the upper, left corner of the Touch controller to open the drop down window. Then tap *Settings > System Information*.

Setting the menu password using the remote control

1. In the on screen menu, go to *Home > Settings > Administrator settings > Set menu password*.

   The password should be a string with 0–255 characters.

   To deactivate the password leave the password input field empty.
2. Enter the menu password in the input field. The password you enter is hidden; each character is replaced with a star (*).

   On the remote control, press the # key to toggle between lower or upper case characters and numbers: abc/ABC/123.
3. Select *Save* to save the changes, or *Cancel* to leave without saving.
4. Press *Home* ( ) to exit.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Appendices

www.cisco.com – Copyright © 2010-2014 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 for the Profile series here:

► http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-profile-series/products-release-notes-list.html

You can download the templates for the C series here:

► http://www.cisco.com/c/en/us/support/collaboration-endpoints/telepresence-integrator-c-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 © 2010-2014 Cisco Systems, Inc. All rights reserved.

About monitors when you have a Codec C60

Connecting the main monitor

The main monitor can be connected to video output HDMI 1 (the default connector for the main monitor) or DVI-I 2.

The codec will read the native resolution of the monitor and output this if possible. Typically this will give the best possible picture for the connected monitor. If auto fails, you will have to select the resolution manually using the *Video > Output > HDMI 1 > Resolution* and *Video > Output > DVI 2 > Resolution* settings.

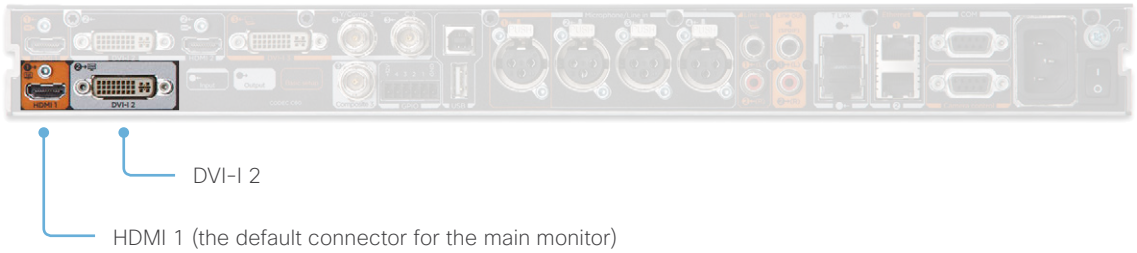
Connecting to HDMI 1

When connecting the main monitor to HDMI 1 the menu, icons and other information on screen (OSD - on screen display) will be displayed on the monitor automatically. This is because HDMI 1 is the default video output of the codec.

Connecting to DVI-I 2

When connecting the main monitor to the DVI-I 2 output, the menus, icons and other information are not automatically displayed on screen. You must move the OSD to the chosen output.

The video outputs of Codec C60



Moving the OSD

You can move the OSD using the remote control or the web interface.

Remote control

Check which connector the main monitor is connected to, and run the following key sequence on the remote control.

- *Disconnect * # * # 0* x *#* x=1 (HDMI 1) x=2 (DVI-I 2)

Example: Setting DVI-I 2 as the OSD output.

- *- * - # - * - # - 0 - 2 - #*

Web interface

Open the System Configuration page. Go to *Video > OSD > Output* and choose the video output connector for the main monitor.

Dual monitors

When you want to run a dual monitor setup, connect the main monitor to video output HDMI 1 and the second monitor to video output DVI-I 2 on the codec.

Dual monitor configuration

To distribute the layout on the two monitors, go to Advanced configuration (menu on screen) or open the System Configuration page (web interface). Then go to *Video > Monitors* and choose **Dual**.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

About monitors when you have a Codec C40

Connecting the main monitor

The main monitor can be connected to video output HDMI 1 (the default connector for the main monitor) or DVI-I 2.

The codec will read the native resolution of the monitor and output this if possible. Typically this will give the best possible picture for the connected monitor. If auto fails, you will have to select the resolution manually using the *Video > Output > HDMI 1 > Resolution* and *Video > Output > DVI 2 > Resolution* settings.

Connecting to HDMI 1

When connecting the main monitor to HDMI 1 the menu, icons and other information on screen (OSD - on screen display) will be displayed on the monitor automatically. This is because HDMI 1 is the default video output of the codec.

Connecting to DVI-I 2

When connecting the main monitor to the DVI-I 2 output, the menus, icons and other information are not automatically displayed on screen. You must move the OSD to the chosen output.

The video outputs of Codec C40

Moving the OSD

You can move the OSD using the remote control or the web interface.

Remote control

Check which connector the main monitor is connected to, and run the following key sequence on the remote control.

- *Disconnect * # * # 0* x *#* x=1 (HDMI 1) x=2 (DVI-I 2)

Example: Setting DVI-I 2 as the OSD output.

- *- * - # - * - # - 0 - 2 - #*

Web interface

Open the System Configuration page. Go to *Video > OSD > Output* and choose the video output connector for the main monitor.

Dual monitors

When you want to run a dual monitor setup, connect the main monitor to video output HDMI 1 and the second monitor to video output DVI-I 2 on the codec.

Dual monitor configuration

To distribute the layout on the two monitors, go to Advanced configuration (menu on screen) or open the System Configuration page (web interface). Then go to *Video > Monitors* and choose **Dual**.

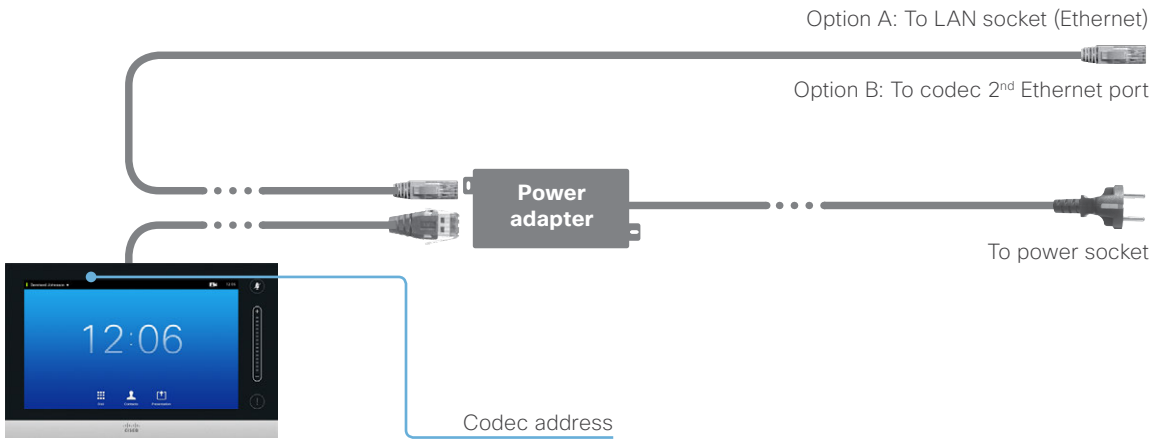
www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Connecting the Cisco TelePresence Touch 8 controller

The Cisco TelePresence Touch 8 controller is an alternative to the remote control and on screen menus.

When a Touch controller is connected to the codec, the remote control cannot be used. You have to disconnect (unpair) the Touch controller in order to to use the remote control.

Touch 8 can can be used with a C Series codec running software version TC4.1 or later.



Connecting the Touch controller

There are two options how to connect the Touch controller to the codec. In both cases the connection is via the provided power adapter, as illustrated above.

A. Connecting the Touch controller to the codec via LAN.

   To enable this mode of operation make sure that the *NetworkServices > SSH > Mode** setting is turned **On**.

   The process of associating the Touch controller to the codec is called paring. The codec is signalling that it is available for pairing for 30 minutes after it is switched on.

   We recommend that the Touch controller and video system is kept on the same subnet.

B. Connecting the Touch controller directly to the codec's second Ethernet port.

   To enable this mode of operation use the remote control and navigate to *Home > Settings > Administrator settings > Pairing > Direct pairing* and choose **On**.

   Alternatively, set the *NetworkPort 2 > Mode** setting to **DirectPairing**.

   Restart the codec for the change to take effect.

Touch controller set-up

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

If you have connected the unit to the codec via LAN, you have to choose which codec to pair with. If the codec is not in the list of available codecs displayed on the Touch controller, you can choose a codec manually by entering its IP address.

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

You can verify that the Touch controller is successfully paired to the codec by checking that the codec address is displayed in the top banner.

If you want more details on Touch installation, please read the *Cisco TelePresence Touch 8 inch Installation Guide*, which is available on the Cisco web site.

* You will find this setting in the Advanced Configuration on-screen menu (remote control) or in the System Configuration page on the web interface.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Advanced customization of video and audio

The codec supports full customization of the audio routing and video layouts/templates allowing support for advanced meeting room setups and integrations.

The TC Console application, which is a free software tool that runs on PC/Mac, provides a graphical interface to the advanced customizable features of the codec. TC Console includes the following modules:

Video compositor

- Modify the default video compositing behavior of the codec
- Add new layouts
- Change the automatically chosen layout
- Control what video sources are shown where and when

Audio console

- Configure the audio system of the codec.
- Change the default mixing, routing and equalizers
- Set various input and output connector properties

GPIO

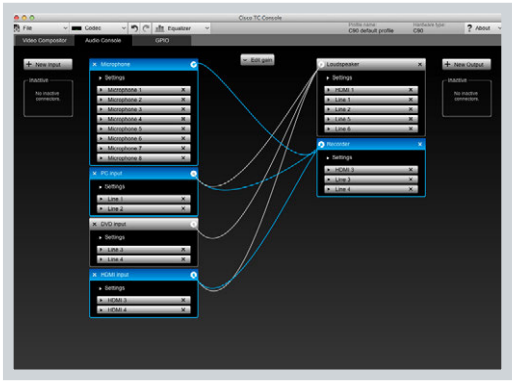
- Change the behavior of the GPIO, i.e. what the codec should do when pins go high/low

For more details about the functionality, see the user guide included in the TC Console application itself or download the TC Console user guide from
► http://www.cisco.com/go/cseries-docs

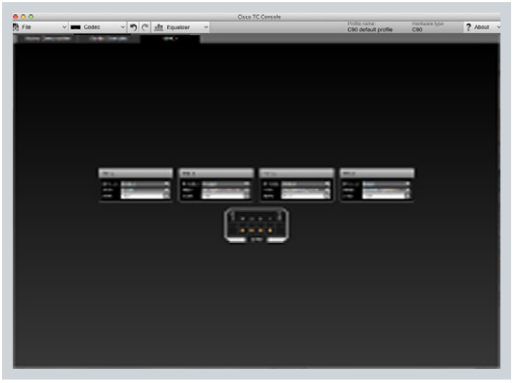
How to obtain the TC Console application

Download the TC Console application for free from the Cisco Developer Network (CDN) web site. Go to:
► http://developer.cisco.com/web/telepresence-developer

Video compositor



Audio console



GPIO

www.cisco.com – Copyright © 2010-2014 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	1280×720 *
	Medium	256×144	768×448	1024×576	1024×576	1280×720	1280×720 *	1280×720 *
	High	512×288	1024×576	1280×720	1280×720	1280×720 *	1280×720 *	1280×720 *

* The resolution will be 1920×1080 for 1080p60 capable C60 codecs (main board rev F and later).

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

ClearPath – Packet loss resilience

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

We recommend that you keep ClearPath enabled on your video system.

Go to Advanced configuration (menu on screen) or open the System Configuration page (web interface):

- Navigate to *Conference 1 > PacketLossResilience > Mode*

  Choose **Off** to disable ClearPath and **On** to enable ClearPath.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Requirement for speaker systems connected to a Cisco TelePresence C Series codec

Cisco has put in a lot of effort to minimize the camera to screen delay on our TelePresence endpoints.

New consumer TVs are usually equipped with “Motion Flow” or similar technology to insert new video frames between standard frames to create smoother images. This processing takes time and to maintain lip synchronization, the TV will delay the audio so that the audio and video arrives at the same time.

The echo canceller in the Cisco endpoints can handle such delay up to 30 ms. Many consumer TVs are not made for real time video communication and may introduce more than 30 ms of delay.

If you use such a TV together with a C Series codec it is recommended that you turn off “Motion Flow”, “Natural Motion” or any other video processing that introduces additional delay.

Some consumer TVs also support advanced audio processing like “Virtual Surround” effects and “Dynamic Compression” to improve the TV experience. Such processing will make any acoustic echo canceller malfunction and should hence be switched off.

Some monitors are equipped with a setting called ‘Game Mode’. This mode is specifically designed to help reduce the response time and will usually help to reduce the delay.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

DNAM for Profile 42”/52”/55”

The DNAM (Digital Natural Audio Module) is built on two specially designed and separate modules: the amplifier and the loudspeaker cabinet.

The DNAM loudspeaker

3-way center loudspeaker system

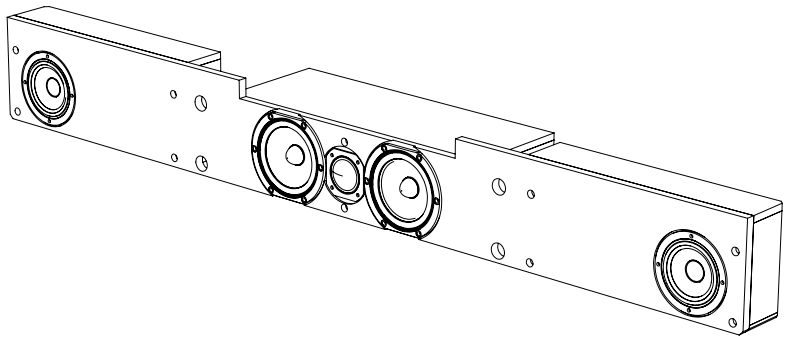
- Frequency range 50 Hz - 20 kHz
- 2 × 100 mm low- and midrange loudspeaker 8 ohm nominal, excellent quality (SEAS Prestige series)
- 1 × 25 mm dome tweeter, 6 ohm nominal, excellent quality
- Digitally filtered audio signals received from DNAM amplifier
- Long time max power 70 watt on all loudspeakers
- Enclosed MDF loudspeaker cabinet

Integrated stereo loudspeaker

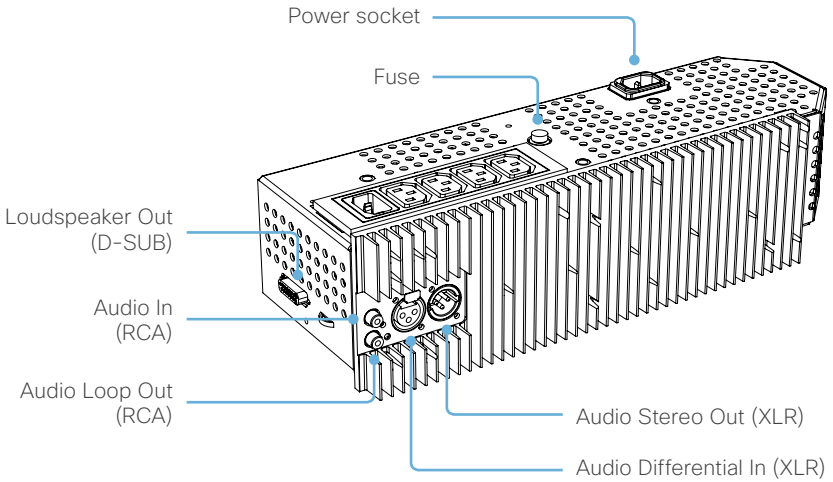
Each side has:

- 1 × 90 mm fullrange loudspeaker, 8 ohm nominal, excellent quality
- Frequency range 70 Hz - 20 kHz
- Enclosed MDF loudspeaker cabinet

DNAM loudspeaker



DNAM amplifier



Some DNAM amplifier models are delivered without XLR connectors, and with a different RCA connector placement.

The DNAM amplifier

- 5 × 50 watt continuous average output power
- Full frequency range for audio (20 Hz – 20 kHz)
- Digital signal processing and filtering on all channels for best audio detail clarity
- Digital crossover filtering on center channels
- In/out:

  Audio In: SPDIF (stereo) or Analog (mono) using the same connector

  Audio Loop Out: line out directly from the input; always analog even with SPDIF in

  Audio Differential In: female XLR, pinout: 1 - GND, 2 – Signal (+), 3 – Signal (-)

  Audio Stereo Out: male XLR, common GND configuration

  Loudspeaker Out: female D-SUB 15-pin
- Fuse 2 A 250 V slow, 5 × 20 mm, Littelfuse type 215002.

Always use this type of fuse. Using a different type may lead to serious hardware malfunction.

Spare fuses

The Profile system is delivered with two spare DNAM fuses in the column.

Take care not to damage the fuse and fuse holder when replacing a fuse.

- Push the fuse holder slightly inwards and turn counter-clockwise to release the fuse.
- When reinserting the fuse and fuse holder, push slightly inwards and turn the holder carefully clockwise until it locks in place.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

DNAM for Profile 65”

The DNAM (Digital Natural Audio Module) is built on two specially designed and separate modules: the amplifier and the loudspeaker cabinet.

The DNAM loudspeaker

3-way center loudspeaker system

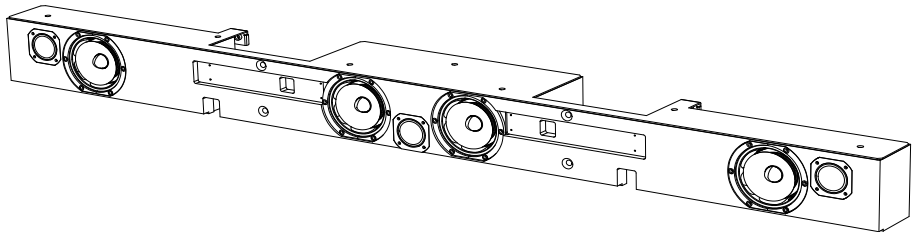
- Frequency range 50 Hz - 20 kHz
- 2 × 100 mm low- and midrange loudspeakers, 8 ohm nominal, reference quality (SEAS Excel series)
- 1 × 25 mm dome tweeter, 6 ohm nominal, excellent quality
- Digitally filtered audio signals received from DNAM amplifier
- Long time max power 70 watt on all loudspeakers
- Enclosed MDF loudspeaker cabinet

2-way integrated stereo loudspeaker

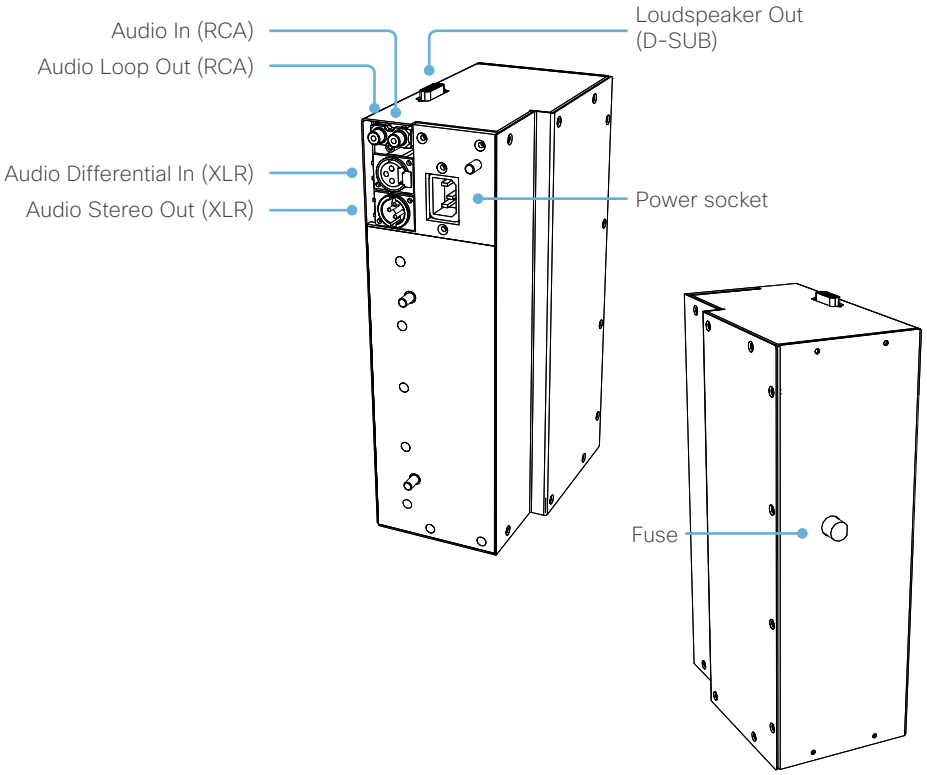
Each side has:

- 1 × 100 mm low- and midrange loudspeaker, 8 ohm nominal, reference quality (SEAS Excel series)
- 1 × 25 mm dome tweeter, 6 ohm nominal, excellent quality
- Passive crossover filter
- Frequency range 70 Hz - 20 kHz
- Long time max power 70 watt
- Enclosed MDF loudspeaker cabinet

DNAM loudspeaker



DNAM amplifier



The DNAM amplifier

- 5 × 50 watt continuous average output power
- Full frequency range for audio (20 Hz – 20 kHz)
- Digital signal processing and filtering on all channels for best audio detail clarity
- Digital crossover filtering on center channels
- In/out:

  Audio In: SPDIF (stereo) or Analog (mono) using the same connector

  Audio Loop Out: line out directly from the input; always analog even with SPDIF in

  Audio Differential In: female XLR, pinout: 1 - GND, 2 - Signal (+), 3 - Signal (-)

  Audio Stereo Out: male XLR, common GND configuration

  Loudspeaker Out: female D-SUB 15-pin
- Fuse 2 A 250 V slow, 5 × 20 mm, Littelfuse type 215002

Always use this type of fuse. Using a different type may lead to serious hardware malfunction.

Spare fuses

The Profile system is delivered with two spare DNAM fuses in the column.

Take care not to damage the fuse and fuse holder when replacing a fuse.

- Push the fuse holder slightly inwards and turn counter-clockwise to release the fuse.
- When reinserting the fuse and fuse holder, push slightly inwards and turn the holder carefully clockwise until it locks in place.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Factory resetting the codec

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, resetting it to its default factory settings should be the last resort.

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 a Touch controller or the web interface to factory reset the system. If these interfaces are not available, you can connect to the system's standard serial interface and issue a factory reset command.

The remote control and on-screen menu do not give access to factory reset.

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.
- Release keys and 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 controller, or navigate to *Home > Settings > System information* using the remote control, 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 serial interface

You have to connect to the video system's COM port with a serial cable. The serial port is enabled as a default, but it may have been disabled.

The connection parameters for the COM port are as follows:

- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None
- Baud rate: The default value is 38400 bps, but it may have been changed

You can read more about the system's serial port settings in the ▶ System settings chapter.

1. Login as admin (administrator rights).
2. Issue the following command:

   ```
   xCommand SystemUnit FactoryReset Confirm: Yes
   ```

   You will see the following text:

   ```
   *r FactoryResetResult:
   **end
   OK
   ```

   The system will revert to the default factory settings and automatically restart. 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 controller.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Factory resetting the Touch 8 control panel

You can reset the Touch 8 control panel to its default factory settings using the New message indicator and the Mute button.

When factory resetting Touch 8 the logs are cleared, and the configuration and pairing information are lost.

Touch 8 restarts after the reset and must receive a new configuration from the video system.

- If Touch 8 is directly connected to the video system it receives the configuration automatically.
- If it is connected via LAN it receives the new configuration as soon as it is successfully paired to the video system.

It is not possible to undo a factory reset.

1. Locate the *New message indicator* and *Mute* buttons.

   The *New message indicator* is a bit hard to see, but it is the button with the exclamation mark on it.

2. Press and hold the *New message indicator* until it lights up (approximately 10 seconds).
3. Press the *Mute* button twice.

   The Touch controller automatically reverts to the default factory settings and restarts.

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Technical specifications

Codec C60/C40

UNIT DELIVERED COMPLETE WITH:
- Video conferencing codec, wireless remote control, rack mounting rails (C60), rack mounting ears (C40), LAN cable, power cable

BANDWIDTH
- H.323/SIP up to 6 Mbps point-to-point

FIREWALL TRAVERSAL
- Cisco TelePresence Expressway technology
- H.460.18, H.460.19 firewall traversal
- SIP ICE (Interactive Connectivity Establishment)

VIDEO STANDARDS
- H.261
- H.263
- H.263+
- H.264

VIDEO FEATURES
- Native 16:9 widescreen
- Advanced screen layouts
- Intelligent video management
- Local auto layout
- 7 embedded individual video compositors – 1 for every output and 1 for every encoder (C60 only) **

VIDEO INPUTS (5 INPUTS (C60) / 4 INPUTS (C40))

Two HDMI inputs; supported formats:
- 1920 × 1080@60, 59.94 Hz (1080p60)
- 1920 × 1080@50 Hz (1080p50)
- 1920 × 1080@30, 29.97 Hz (1080p30)
- 1920 × 1080@25 Hz (1080p25)
- 1920 × 1080@24, 23.97 Hz (1080p24)
- 1280 × 720@60, 59.94 Hz (720p60)
- 1280 × 720@50 Hz (720p50)
- 720 × 480@60, 59.94 Hz (480p60)
- 640 × 480@60 Hz (480p60)
- 1600 × 1200@50, 60 Hz (UXGA)
- 1280 × 1024@60, 75 Hz (SXGA)
- 1024 × 768@60, 70, 75, 85 Hz (XGA)
- 800 × 600@56, 60, 72, 75, 85 Hz (SVGA)
- 1920 × 1200@50, 60 Hz (WUXGA)
- 1680 × 1050@60 Hz (WSXGA+)
- 1440 × 900@60 Hz (WXGA+)
- 1280 × 768@60 Hz (WXGA)

Two (C60), one (C40) × DVI-I inputs; supported formats:

Analog (VGA):
- 1920 × 1080@60 Hz (1080p60)
- 1280 × 720@60 Hz (720p60)
- 1600 × 1200@60 Hz (UXGA)
- 1280 × 1024@60, 75 Hz (SXGA)
- 1280 × 960@60 Hz
- 1024 × 768@60, 70, 75, 85 Hz (XGA)
- 1920 × 1200@50 Hz (WUXGA)
- 1680 × 1050@60 Hz (WSXGA+)
- 1440 × 900@60 Hz (WXGA+)
- 1280 × 800@60 Hz (WXGA)
- 1280 × 768@60 Hz (WXGA)

Analog (YPbPr):
- 1920 × 1080@60 Hz (1080p60)
- 1920 × 1080@50 Hz (1080p50)
- 1920 × 1080@30 Hz (1080p30)
- 1920 × 1080@25 Hz (1080p25)
- 1280 × 720@60 Hz (720p60)
- 1280 × 720@50 Hz (720p50)
- 1280 × 720@30 Hz (720p30)
- 720 × 576@50 Hz (576p50)
- 720 × 480@60 Hz (480p60)

Digital (DVI-D):
- Same as HDMI, ref. above.

One S-video/Composite input (BNC connector):
- PAL/NTSC

- Extended Display Identification Data (EDID)

VIDEO OUTPUTS (3 OUTPUTS (C60) / 2 OUTPUTS (C40))

One HDMI output, one DVI-I output; supported formats:
- 1920 × 1080@60 Hz (1080p60)
- 1280 × 720@60 Hz (720p60)
- 1600 × 1200@60 Hz (UXGA)
- 1280 × 1024@60 Hz (SXGA)
- 1024 × 768@60 Hz (XGA)
- 800 × 600@60 Hz (SVGA)
- 640 × 480@60 Hz (VGA)
- 1920 × 1200@60Hz (WUXGA)
- 1360 × 768@60 Hz
- 1366 × 768@60 Hz
- 1280 × 768@60 Hz (WXGA)

One composite output (BNC connector) (C60 only):
- PAL/NTSC

- VESA Monitor Power Management
- Extended Display Identification Data (EDID)

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)
- 176 × 144@30 fps (QCIF)
- 352 × 288@30 fps (CIF)
- 512 × 288@30 fps (w288p)
- 576 × 448@30 fps (448p)
- 768 × 448@30 fps (w448p)
- 704 × 576@30 fps (4CIF)
- 1024 × 576@30 fps (w576p)
- 1280 × 720@30 fps (720p30)
- 1920 × 1080@30 fps (1080p30)*
- 640 × 480@30 fps (VGA)
- 800 × 600@30 fps (SVGA)
- 1024 × 768@30 fps (XGA)
- 1280 × 1024@30 fps (SXGA) (C60 only)
- 1280 × 768@30 fps (WXGA)
- 1440 × 900@30 fps (WXGA+)* (C60 only)
- 1680 × 1050@30 fps (WSXGA+)* (C60 only)
- 1600 × 1200@30 fps (UXGA)* (C60 only)
- 1920 × 1200@25fps (WUXGA)* (C60 only)
- 512 × 288@60 fps (w288p60)*
- 768 × 448@60 fps (w448p60)*
- 1024 × 576@60 fps (w576p60)*
- 1280 × 720@60 fps (720p60)*

- 720p30 from 768kbps
- 720p60 from 1152kbps*
- 1080p30 from 1472 kbps*

AUDIO STANDARDS
- G.711
- G.722
- G.722.1
- G.729AB
- 64 kbps and 128 kbps AAC-LD, mono and stereo

AUDIO FEATURES
- CD quality 20 kHz mono and stereo
- Four (C60) / Two (C40) separate acoustic echo cancellers
- 4-port (C60) / 2-port (C40) audio mixer
- Automatic gain control (AGC)
- Automatic noise reduction
- Active lip synchronization

AUDIO INPUTS (7 INPUTS (C60), 5 INPUTS (C40))
- Four microphones (C60) / two microphones (C40), 48 V phantom powered, XLR connector, each with separate echo cancellers and noise reduction; all microphones can be set for balanced line level
- Two RCA/Phono inputs, line level: Stereo PC input, configurable to two RCA/Phono inputs, line level: Mono auxiliary/DVD input
- One HDMI input, digital: stereo PC/DVD input

AUDIO OUTPUTS (3 OUTPUTS)
- Two RCA/Phono outputs, line level, stereo main audio, configurable to S/PDIF or two RCA/Phono outputs, line level, mono to recording device
- One HDMI output, digital, stereo main audio

DUAL STREAM
- H.239 (H.323) dual stream
- BFCP (SIP) dual stream
- Support for resolutions up to 1080p30/WUXGA (C60) / WXGAp30 (C40), independent of main stream resolution

---

* Requires option
** Multiwindow compositing not supported on the dual stream
*** Not supported on 4 x zoom camera

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

MULTIPOINT SUPPORT
- Four-way embedded SIP/H.323 MultiPoint, reference MultiSite
- Cisco TelePresence Multiway support (requires Cisco TelePresence Video Communication Server [Cisco VCS] and Cisco TelePresence MCU)
- Ability to natively join multipoint conferences hosted on Cisco Telepresence Multipoint Switch (CTMS)

MULTISITE FEATURES*
(embedeed multipoint)
- Four-way SIP/H.323 MultiSite. Resolution up to 720p30 (C60) / w576p30 (C40)
- Full individual audio and video transcoding
- Individual layouts in multisite continuous presence (takes out selfview)
- H.323/SIP/VoIP in the same conference
- Support for Presentation (H.239/BFCP) from any participant at resolutions up to WXGAp30 (C60) / WXGAp30 (C40)
- Best Impression (automatic continuous presence layouts)
- H.264, encryption, and dual stream from any site
- Dial in and dial out
- Additional telephone call (no license required)
- Conference rates up to 10 Mbps

PROTOCOLS
- H.323
- SIP
- ISDN (requires Cisco TelePresence ISDN Link)

EMBEDDED ENCRYPTION
- H.323/SIP point-to-point
- Standards-based: H.235 v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Supported in Dual Stream

IP NETWORK FEATURES
- DNS lookup for service configuration
- Differentiated Services (QoS)
- IP adaptive bandwidth management (including flow control)
- Auto gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 DTMF tones in H.323
- Date and time support via NTP
- Packet loss based downspeeding
- URI Dialing
- TCP/IP
- DHCP
- 802.1x Network authentication
- 802.1Q Virtual LAN
- 802.1p QoS and class of service
- ClearPath
- Medianet: Mediatrace and Metadata

IPV6 NETWORK SUPPORT
- Single call stack support for both H323 and SIP
- Dual-stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ
- Support for both static and autoconfiguration (stateless address autoconfiguration)

CISCO UNIFIED COMMUNICATIONS MANAGER
(requires Cisco UCM version 8.6 or later)
- Native registration with Cisco Unified Communications Manager
- Basic Cisco Unified Communications Manager provisioning
- Firmware upgrade from Cisco Unified Communications Manager
- Cisco Discovery Protocol and DHCP option 150 support
- Basic telephony features such as hold, resume, transfer, and corporate directory lookup

SECURITY FEATURES
- Management through HTTPS and SSH
- IP administration password
- Menu administration password
- Disable IP services
- Network settings protection

NETWORK INTERFACES
- One LAN/Ethernet (RJ-45) 10/100/1000 Mbit
- One LAN/Ethernet (RJ-45) interface to be used for the Cisco TelePresence Touch for C-series user interface device only

OTHER INTERFACES
- USB host for future usage (C60 only)
- USB device for future usage
- GPIO – General purpose input/output (C60 only)

PRECISIONHD 1080P CAMERA
- 1/3" CMOS
- 12 × zoom (C60)
- 12 × zoom / 4 × zoom (C40)
- +15°/-25° tilt, +/- 90° pan
- 43.5° vertical field of view
- 72° horizontal field of view
- Focus distance 0.3 m-infinity
- 1920 × 1080 pixels progressive @ 60fps (12 × zoom version)
- 1920 × 1080 pixels progressive @ 30fps (4 × zoom version)
- Other formats supported (configurable through dip-switch):
  - 1920 × 1080@60 Hz (HDMI only)***
  - 1920 × 1080@50 Hz (HDMI only)***
  - 1920 × 1080@30 Hz
  - 1920 × 1080@25 Hz
  - 1280 × 720@60 Hz***
  - 1280 × 720@50 Hz ***
  - 1280 × 720@30 Hz
  - 1280 × 720@25 Hz
- Automatic or manual focus/brightness/white balance
- Far-end camera control
- Daisy-chain support (Visca protocol camera)***
- Dual HDMI and HD-SDI outputs
- Upside-down mounting with automatic flipping of picture

SYSTEM MANAGEMENT
- Support for the Cisco TelePresence Management Suite (Cisco TMS)
- Total management through embedded SNMP, Telnet, SSH, XML, SOAP
- Remote software upload through web server, SCP, HTTP, HTTPS
- One RS-232 for local control and diagnostics
- Remote control and on-screen menu system

DIRECTORY SERVICES
- Support for local directories (My Contacts)
- Corporate directory
- Unlimited entries using server directory supporting LDAP and H.350 (requires Cisco TMS)
- Unlimited number for corporate directory (through Cisco TMS)
- Received calls with date and time
- Placed calls with date and time
- Missed calls with date and time

POWER
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz
- 175 watts max for codec and main camera

OPERATING TEMPERATURE AND HUMIDITY
- 0° C to 35° C (32° F to 95° F) ambient temperature
- 10% to 90% relative humidity (RH)

STORAGE AND TRANSPORT TEMPERATURE
- -20° C to 60° C (-4° F to 140° F) at RH 10-90% (non-condensing)

DIMENSIONS
- Length: 17.4 in. / 44.2 cm
- Height: 1.7 in. / 4.4 cm
- Depth: 10.9 in. / 27.8 cm
- Weight: 8.8 lbs / 4 kg

* Requires option
** Multiwindow compositing not supported on the dual stream
*** Not supported on 4 x zoom camera

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

APPROVALS

EU/EEC

- Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN60950-1
- Directive 2004/108/EC (EMC Directive)
  - Standard EN55022, Class A
  - Standard EN55024
  - Standard EN61000-3-2/-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 UL60950-1
- 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
- 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

MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:

Power On Hours (POH) > 69 000 hours

Useful Life Cycle > 6 years

ISO 9001 certificate is available upon request

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.

June 2013

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 52”/55” using C60

UNIT DELIVERED COMPLETE WITH:
- Full HD LCD display, Codec C60, Touch 8 user interface device, remote control, PrecisionHD Camera (1080p), microphone (3x with single screen, 4x with dual screen), Digital Audio Module, integrated speakers and integrated cabling.
- Choice of installation configuration: floor stand, wheel base or wall mount on pedestal.
- Choice of screen size and configuration.

MONITOR available with:
- 52”/55’’ Full HD LCD, 16:9, 1080 × 1920 resolution

BASE available with:
- Floor standing foot plate
- Wheel base (not available on 52” Dual / 55” Dual)
- Wall mount on pedestal

BANDWIDTH
The same as Codec C60

FIREWALL TRAVERSAL
The same as Codec C60

VIDEO STANDARDS
The same as Codec C60

VIDEO FEATURES
The same as Codec C60

VIDEO INPUTS (5 INPUTS)
The same as Codec C60

VIDEO OUTPUTS (3 OUTPUTS)
The same as Codec C60

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)
The same as Codec C60

AUDIO STANDARDS
The same as Codec C60

AUDIO FEATURES
The same as Codec C60

AUDIO INPUTS (7 INPUTS)
The same as Codec C60

AUDIO OUTPUTS (3 OUTPUTS)
The same as Codec C60

DUAL STREAM
The same as Codec C60

MULTIPOINT SUPPORT
The same as Codec C60

MULTISITE FEATURES*
The same as Codec C60

PROTOCOLS
The same as Codec C60

EMBEDDED ENCRYPTION
The same as Codec C60

IP NETWORK FEATURES
The same as Codec C60

IPV6 NETWORK SUPPORT
The same as Codec C60

CISCO UNIFIED COMMUNICATIONS MANAGER
The same as Codec C60

SECURITY FEATURES
The same as Codec C60

NETWORK INTERFACES
The same as Codec C60

OTHER INTERFACES
The same as Codec C60

PRECISIONHD 1080P CAMERA
The same as Codec C60

SYSTEM MANAGEMENT
The same as Codec C60, as well as
- Cisco TelePresence Touch 8 user interface device

DIRECTORY SERVICES
The same as Codec C60

POWER

Profile 52’’ / 52” Dual
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz, 6 A max
- 175 W max for codec and main camera
- Maximum power rating complete system, 526 W (52”) / 870 W (52” Dual)

Profile 55’’ / 55” Dual
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz, 4.5 A max (55”) / 8 A (55” Dual)
- 175 W max for codec and main camera
- Maximum power rating complete system, 350 W (55”) / 550 W (55” Dual)
- The display complies with ENERGY STAR requirements

OPERATING TEMPERATURE AND HUMIDITY
- 0° C to 35° C (32° F to 95° F) ambient temperature
- 10% to 90% relative humidity (RH)

STORAGE AND TRANSPORT TEMPERATURE
- -20° C to 60° C (-4° F to 140° F) at RH 10-90% (non-condensing)

DIMENSIONS

Profile 52’’
- Height: 63.78 in. / 162 cm
- Width: 47.25 in. / 120 cm
- Depth: 6.7 in. / 17 cm (without footplate)
- Weight: 253.5 lbs / 115 kg (with floor standing footplate)
- 229.3 lbs / 104 kg (with wheel base)

Profile 52’’ Dual
- Height: 63.8 in. / 162 cm
- Width: 94.5 in. / 240 cm
- Depth: 6.7 in. / 17 cm (without footplate)
- Weight: 515.9 lbs / 234 kg (with floor standing footplate)

Profile 55’’
- Height: 64.6 in. / 164 cm
- Width: 49.6 in. / 126 cm
- Depth: 6.7 in. / 17 cm (without footplate)
- Weight: 245 lbs / 111 kg (with floor standing footplate)
- 225lbs / 102 kg (with wheel base)

Profile 55’’ Dual
- Height: 64.6 in. / 164 cm
- Width: 99.2 in. / 252 cm
- Depth: 6.7 in. / 17 cm (without footplate)
- Weight: 443 lbs / 201 kg (with floor standing footplate)

* Requires option

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

APPROVALS

EU/EEC

- Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN60950-1
- Directive 2004/108/EC (EMC Directive)
  - Standard EN55022, Class A
  - Standard EN55024
  - Standard EN61000-3-2/-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 UL60950-1
- 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
- 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

MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:

Power On Hours (POH) > 69 000 hours

Useful Life Cycle > 6 years

ISO 9001 certificate is available upon request

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.

June 2013

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 65” using C60

UNIT DELIVERED COMPLETE WITH:

- Full HD LCD display, Codec C60, Touch 8 user interface device, remote control, PrecisionHD 1080p Camera, microphones, Digital Audio Module, integrated speakers and integrated cabling.

MONITOR available with:

- 65’’ Full HD LCD, 16:9, 1080 × 1920 resolution

BASE available with:

- Floor standing footplate
- Wall mount on pedestal

BANDWIDTH

The same as Codec C60

FIREWALL TRAVERSAL

The same as Codec C60

VIDEO STANDARDS

The same as Codec C60

VIDEO FEATURES

The same as Codec C60

VIDEO INPUTS (5 INPUTS)

The same as Codec C60

VIDEO OUTPUTS (3 OUTPUTS)

The same as Codec C60

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

The same as Codec C60

AUDIO STANDARDS

The same as Codec C60

AUDIO FEATURES

The same as Codec C60

AUDIO INPUTS (7 INPUTS)

The same as Codec C60

AUDIO OUTPUTS (3 OUTPUTS)

The same as Codec C60

DUAL STREAM

The same as Codec C60

MULTIPOINT SUPPORT

The same as Codec C60

MULTISITE FEATURES*

The same as Codec C60

PROTOCOLS

The same as Codec C60

EMBEDDED ENCRYPTION

The same as Codec C60

IP NETWORK FEATURES

The same as Codec C60

IPV6 NETWORK SUPPORT

The same as Codec C60

CISCO UNIFIED COMMUNICATIONS MANAGER

The same as Codec C60

SECURITY FEATURES

The same as Codec C60

NETWORK INTERFACES

The same as Codec C60

OTHER INTERFACES

The same as Codec C60

PRECISIONHD 1080P CAMERA

The same as Codec C60

SYSTEM MANAGEMENT

The same as Codec C60, as well as

- Cisco TelePresence Touch 8 user interface device

DIRECTORY SERVICES

The same as Codec C60

POWER

- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz
- 175 W max for codec and main camera
- Maximum power rating complete system, 650 W

OPERATING TEMPERATURE AND HUMIDITY

- 0° C to 35° C (32° F to 95° F) ambient temperature
- 10% to 90% relative humidity (RH)

STORAGE AND TRANSPORT TEMPERATURE

- -20° C to 60° C (-4° F to 140° F) at RH 10–90% (non-condensing)

DIMENSIONS

- Height: 65 in. / 165 cm
- Width: 59.1 in. / 150 cm
- Depth: 5.9 in. / 15 cm
- Weight: 330 lbs / 150 kg (with floor standing footplate)

APPROVALS

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
- 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

MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:

Power On Hours (POH) > 69 000 hours

Useful Life Cycle > 6 years

ISO 9001 certificate is available upon request

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.

June 2013

* Requires option

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

Profile 42”/52”/55” using C40

UNIT DELIVERED COMPLETE WITH:
- Full HD LCD display, Codec C40, Touch 8 user interface device, remote control, PrecisionHD Camera (1080p), microphones (2x), Digital Audio Module, integrated speakers and integrated cabling.
- Choice of installation configuration: floor stand, wheel base or wall mount on pedestal.

MONITOR available with:
- 42’’ Full HD LCD, 16:9, 1080 × 1920 resolution
- 52’’ Full HD LCD, 16:9, 1080 × 1920 resolution
- 55’’ Full HD LCD, 16:9, 1080 × 1920 resolution

BASE available with:
- Floor standing footplate
- Wheel base
- Wall mount on pedestal

BANDWIDTH

The same as Codec C40

FIREWALL TRAVERSAL

The same as Codec C40

VIDEO STANDARDS

The same as Codec C40

VIDEO FEATURES

The same as Codec C40

VIDEO INPUTS (4 INPUTS)

The same as Codec C40

VIDEO OUTPUTS (2 OUTPUTS)

The same as Codec C40

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)

The same as Codec C40

AUDIO STANDARDS

The same as Codec C40

AUDIO FEATURES

The same as Codec C40

AUDIO INPUTS (5 INPUTS)

The same as Codec C40

AUDIO OUTPUTS (3 OUTPUTS)

The same as Codec C40

DUAL STREAM

The same as Codec C40

MULTIPOINT SUPPORT

The same as Codec C40

MULTISITE FEATURES*

The same as Codec C40

PROTOCOLS

The same as Codec C40

EMBEDDED ENCRYPTION

The same as Codec C40

IP NETWORK FEATURES

The same as Codec C40

IPV6 NETWORK SUPPORT

The same as Codec C40

CISCO UNIFIED COMMUNICATIONS MANAGER

The same as Codec C40

SECURITY FEATURES

The same as Codec C40

NETWORK INTERFACES

The same as Codec C40

OTHER INTERFACES

The same as Codec C40

PRECISIONHD 1080P CAMERA

The same as Codec C40 with 12 × zoom camera

SYSTEM MANAGEMENT

The same as Codec C40, as well as
- Cisco TelePresence Touch 8 user interface device

DIRECTORY SERVICES

The same as Codec C40

POWER

Profile 42’’
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz, 6 A max
- 175 W max for codec and main camera
- Maximum power rating complete system 365 W

Profile 52’’
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz, 6 A max
- 175 W max for codec and main camera
- Maximum power rating complete system 526 W

Profile 55’’
- Auto-sensing power supply
- 100-120/200-240 VAC, 60/50 Hz, 4.5 A max
- 175 W max for codec and main camera
- Maximum power rating complete system, 350 W
- The display complies with ENERGY STAR requirements

OPERATING TEMPERATURE AND HUMIDITY
- 0° C to 35° C (32° F to 95° F) ambient temperature
- 10% to 90% relative humidity (RH)

STORAGE AND TRANSPORT TEMPERATURE
- -20° C to 60° C (-4° F to 140° F) at RH 10–90% (non-condensing)

DIMENSIONS

Profile 42’’
- Height: 63.78 in. / 162 cm
- Width: 38.58 in. / 98 cm
- Depth: 6.7 in. / 17 cm
- Weight: 220.5 lbs / 100 kg (with floor standing footplate)
- 200.6 lbs / 91 kg (with wheel base)

Profile 52’’
- Height: 63.78 in. / 162 cm
- Width: 47.25 in. / 120 cm
- Depth: 6.7 in. / 17 cm
- Weight: 253.5 lbs / 115 kg (with floor standing footplate)
- 229.3 lbs / 104 kg (with wheel base)

Profile 55’’
- Height: 64.6 in. / 164 cm
- Width: 49.6 in. / 126 cm
- Depth: 6.7 in. / 17 cm (without footplate)
- Weight: 245 lbs / 111 kg (with floor standing footplate)
- 225lbs / 102 kg (with wheel base)

* Requires option

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

APPROVALS

EU/EEC

- Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN60950-1
- Directive 2004/108/EC (EMC Directive)
  - Standard EN55022, Class A
  - Standard EN55024
  - Standard EN61000-3-2/-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 UL60950-1
- 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
- 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

MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:

Power On Hours (POH) > 69 000 hours

Useful Life Cycle > 6 years

ISO 9001 certificate is available upon request

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.

June 2013

www.cisco.com – Copyright © 2010-2014 Cisco Systems, Inc. All rights reserved.

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 4587 RTP Payload Format for H.261 Video Streams
- 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

www.cisco.com – Copyright © 2010-2014 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. Follow one of these paths:

TelePresence Integration Solutions >
Cisco TelePresence Integrator C Series

Collaboration Room Endpoints >
Cisco TelePresence Profile Series

Alternatively, you can use the following short-links to find the documentation:

- http://www.cisco.com/go/cseries-docs
- http://www.cisco.com/go/profile-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

API reference guides:
Reference Guides | Command references

Knowledge base articles and frequently asked questions:
Troubleshoot and Alerts > Troubleshooting Guides

Physical interface guides:
Maintain and Operate | End-User Guides

CAD drawings:
Reference Guides > Technical References

TC Console user guide:
Configure > Configuration Guides

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 © 2010-2014 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.

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. (1005R)

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.

TANDBERG is now a part of Cisco. TANDBERG® is a registered trademark belonging to Tandberg ASA.

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