Software version TC6.0
JANUARY 2013

MX200

MX300

Administrator guide

for Cisco TelePresence MX200 and MX300

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 MX200.

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

Chapter 1

Introduction

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

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

Products covered in this guide

- Cisco TelePresence MX300
- Cisco TelePresence MX200

User documentation

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

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

Downloading the user documentation

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

Go to: ► http://www.cisco.com/go/telepresence/docs

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

Software

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

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

We recommend reading the Software Release Notes (TC6), go to:

► http://www.cisco.com/en/US/products/ps11776/tsd_products_support_series_home.html

What’s new in this version

This section provides an overview of the new and changed system settings and new features in the TC6.0 software version.

Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (TC6).

Go to: ► http://www.cisco.com/en/US/products/ps11776/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

Administrator password not set warning on OSD

If the administrator password is not set, there is an on screen warning in the lower right corner indicating this. The warning disappears when the password is set.

Improved video layout

- Improved local layout control when using the Touch controller

  You can easily choose between the layout options using the Touch controller. Each option is illustrated by an icon reflecting the actual layout.

  You can choose between the predefined layout options as well as any custom layouts that have been created for this TelePresence system (for example created with the TC Console application).

- Picture-in-Picture support

  There is support for showing Picture-in-Picture (PIP), for example showing a full screen presentation with both remote video and self view as PIP.

  The PIPs can be moved to predefined drop zones, typically upper right, upper left, lower right etc. When using a Touch controller you can see the drop zones as you start moving the PIP.

Support for Cisco TelePresence ISDN Link

You can pair a TelePresence system with a Cisco TelePresence ISDN Link. As from software versions TC6.0 and IL1.1 automatic pairing mode is supported.

When making a call via ISDN Link, choose H320 (ISDN) as the call protocol.

Secure communication in a CUCM environment

As from version TC5 endpoints running TC software can register to a Cisco Unified Communications Manager (CUCM) version 8.6.2 or newer. In TC6.0 this feature is extended to also include secure (encrypted) connections. The encryption indicator is shown on the screen during a call.

This feature requires that security mode is installed and configured on CUCM. Read the *Administering TC Endpoints on CUCM 9.0* guide to find how to set up this feature.

Support for SIP URI dialing when registered to CUCM

As from Cisco Unified Communications Manager (CUCM) version 9.0, endpoints registered to CUCM support URI dialing. A URI is an alias for a directory number (DN). A call to the URI behaves as if the call was made directly to the directory number.

URI example: conference_room@company.com. The user name (left side) is case sensitive in CUCM 9.0, while the domain (right side) is not.

Support for encrypted Cisco TelePresence Multipoint Switch (CTMS) calls

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.

The TelePresence system must have a secure registration to VCS or CUCM to allow encrypted calls.

Troubleshooting and diagnostics

A new troubleshooting feature is introduced. The TelePresence system runs a set of tests to detect possible problems and provides links on the web interface to resolve the issues.

The Mediatrace diagnostics tool

Mediatrace is a diagnostics tool that discovers the routers and switches (layer 2 and 3 devices) along the path of an IP flow. It collects critical information hop by hop on specific media streams as they traverse the network. Mediatrace should be enabled on each network node you want to collect information from. Because the path of video data packets from the endpoints is traced, troubleshooting is facilitated and network performance can be optimized.

New and improved web interface features

- Local phone book management, for example creating a folder structure, and adding, modifying or deleting contacts.

  Note that the web interface's local phone book mirrors the Favorites list on the Touch controller.
- Improved interface for uploading certificates and certificate authority lists to the TelePresence system.
- Display of diagnostics information, including links how to resolve pending issues.
- Information about connected peripherals, e.g. Touch controller, cameras and displays.
- Configuration interface for the Cisco TelePresence ISDN Link gateway (only applicable if an ISDN Link gateway is connected to the TelePresence system).

New languages supported on Touch

- Czech
- Dutch
- Hungarian
- Italian
- Korean
- Polish
- Portuguese Brazilian
- Traditional Chinese
- Turkish

System configuration changes

New settings

Conference DoNotDisturb DefaultTimeout

Conference MaxTotalTransmitCallRate

Conference MaxTotalReceiveCallRate

Conference Presentation OnPlacedOnHold

Network QoS Diffserv ICMPv6

Network QoS Diffserv NTP

NetworkServices CTMS Mode

NetworkServices CTMS Encryption

SIP ListenPort

Video SelfviewDefault Mode

Video SelfviewDefault FullscreenMode

Video SelfviewDefault PIPPosition

Video SelfviewDefault OnMonitorRole

Video PIP ActiveSpeaker DefaultValue Position

Video PIP Presentation DefaultValue Position

Video Input Source[1..n] PresentationSelection

Video Input DVI[x, y] RGBQuantizationRange

Video OSD EncryptionIndicator

Settings that are removed

Audio VolumeHandset

Audio VolumeHeadset

Audio PreferredOutputConnector

Network DNS Server[4, 5] Address

SystemUnit Type

Settings that are modified

Cameras PowerLine Frequency

OLD: <Auto/50Hz/60Hz>

NEW: <50Hz/60Hz>

Conference DefaultCall Protocol

OLD: <H323/Sip>

NEW: <H323/Sip/H320>

Network IPv6 Assignment

OLD: <Static/Autoconf>

NEW: <Static/DHCPv6/Autoconf>

SystemUnit ContactInfo Type

OLD: <Auto/None/IPv4/IPv6/H323Id/E164Alias/SipUri/SystemName>

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

UserInterface TouchPanel DefaultPanel

OLD: <ContactList/MeetingList>

NEW: <ContactList/MeetingList/Dialpad>

Video Layout LocalLayoutFamily

OLD: <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>

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

Video Layout RemoteLayoutFamily

OLD: <Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>

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

Video Input Source[1..n] OptimalDefinition Threshold60fps

OLD: <512_288/768_448/1024_576/1280_720/Never>

NEW: <512_288/768_448/1024_576/1280_720/1920_1080/Never>

Video Output LCD[1] MonitorRole

OLD: <First/Second/PresentationOnly/InternalSetup>

NEW: <InternalSetup>

Video Wallpaper

OLD: <None/Growing/Summersky/Custom/Wallpaper01/Wallpaper02/Wallpaper03/Wallpaper04/Wallpaper05/Wallpaper06/Wallpaper07/Wallpaper08/Wallpaper09/Wallpaper10/Wallpaper11/Wallpaper12>

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

Cisco TelePresence MX Series at a glance

The Cisco TelePresence® MX Series makes telepresence more accessible to teams everywhere with ready-to-use simplicity and high quality. This highly integrated telepresence system is easy to install, so you can quickly transform any meeting space into a video-enabled team room. Whether you are just getting started with video communications or implementing a large-scale deployment, the Cisco TelePresence MX Series delivers high quality performance in a simple and intuitive way.

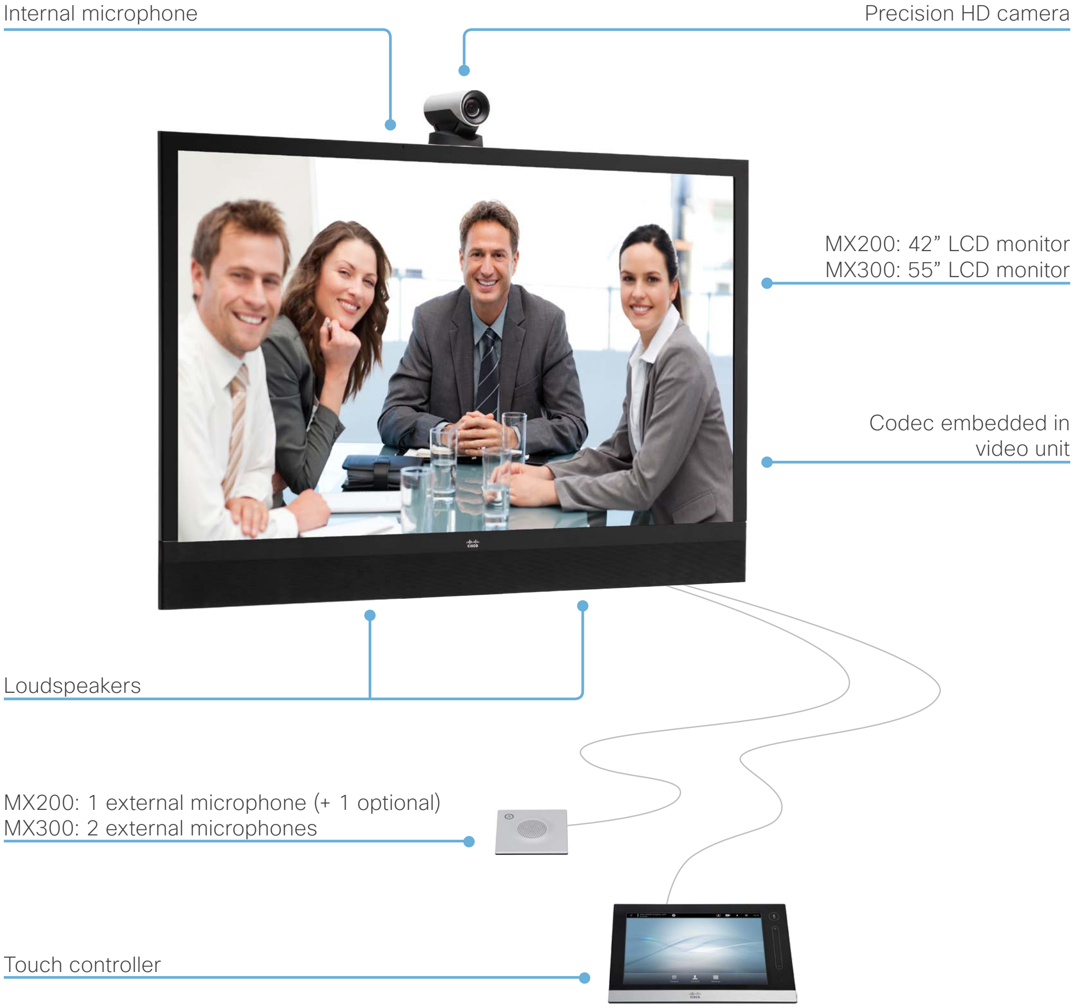
MX300

MX200

Features and benefits

- The systems are easy to install – one piece plus floor stand, table stand (MX200 only), or wall mount brackets (VESA mount).
- The systems are self-configuring with Cisco Unified Communications Manager (UCM), Cisco TelePresence Video Communication Server (VCS), or Cisco Callway provisioning. All you need is to authenticate your endpoint to the network.
- PrecisionHD camera with pan, tilt, and 4x optical zoom helps ensure optimal framing and video clarity.
- Dedicated camera presets provide flexibility and easy viewing for any meeting scenario.
- The 8-inch Touch interface offers simple control.
- Simple *one-button-to-push* calling integrates with common calendar programs.
- Video resolutions of 1080p30 and 720p60 bring telepresence experience to any meeting room or office.
- The high-quality 42-inch (MX200) and 55-inch (MX300) displays with 1920 x 1080 resolution enable clear images.
- You can easily connect and share your PC content at WXGA and 720p30 resolution and frame rate.
- The systems support H.323 and Session Initiation Protocol (SIP) with bandwidth up to 6 Mbps point-to-point.
- Two front speakers provide superior audio quality.
- The systems are standards-based.
- Capabilities for large conferences and transparent escalation from point-to-point to multipoint calls using the Cisco TelePresence Multiway™ technology.

Cisco TelePresence MX Series at a glance (continued)



Rear view

MX300 mounting options
(floor stand, wall mount)

MX200 mounting options
(floor stand, table stand, wall mount)

Chapter 2

Web interface

Starting 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.

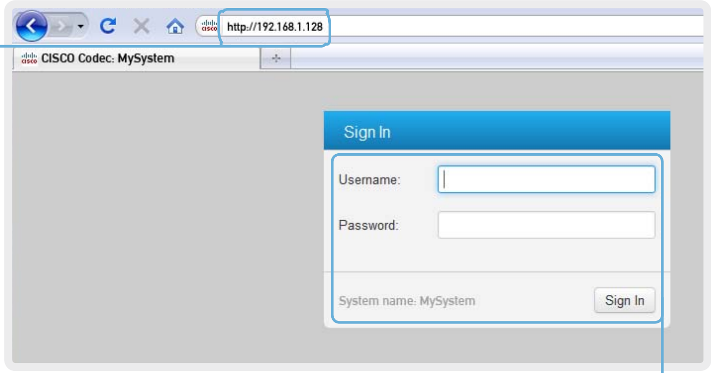
Browsers:

- The latest releases of Internet Explorer, Mozilla Firefox, Opera, Chrome or Safari are recommended
- Major TC6.0 functionality works with Internet Explorer 7

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), tap *Settings* (🔧) on the Touch controller.



http://192.168.1.128

CISCO Codec: MySystem

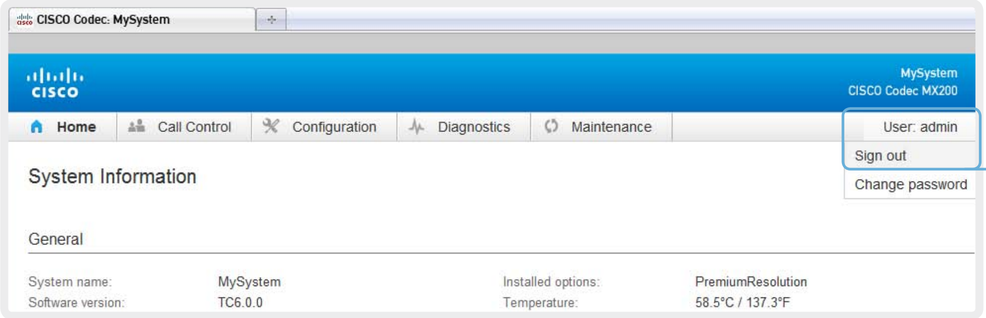
System name: MySystem

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).

We strongly recommend that you set a password for the *admin* user, see the next page.



CISCO Codec: MySystem

MySystem
CISCO Codec MX200

System Information

General

System name: MySystem

Software version: TC6.0.0

Installed options: PremiumResolution

Temperature: 58.5°C / 137.3°F

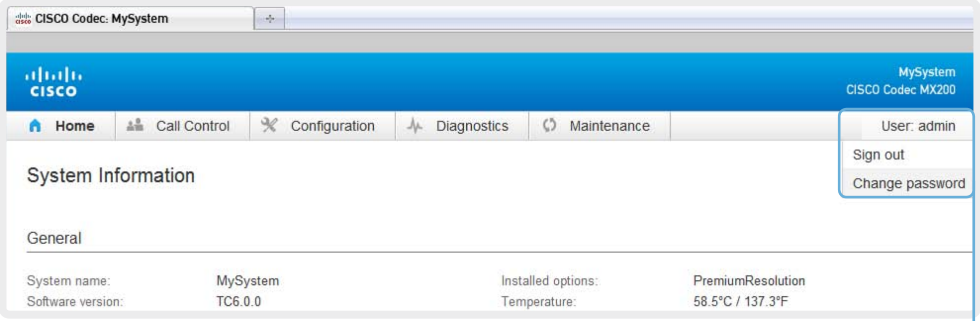
Signing out

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

Changing the system password

We strongly recommend that you set a password for any user with ADMIN rights, including the default *admin* user, to restrict access to system configuration.

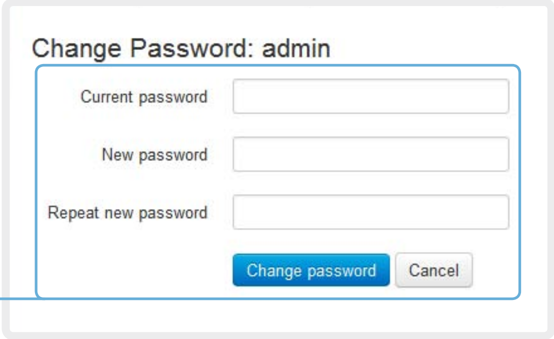
You can read more about password protection in the ► Setting passwords chapter.



System name: MySystem
Software version: TC6.0.0
Installed options: PremiumResolution
Temperature: 58.5°C / 137.3°F

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.

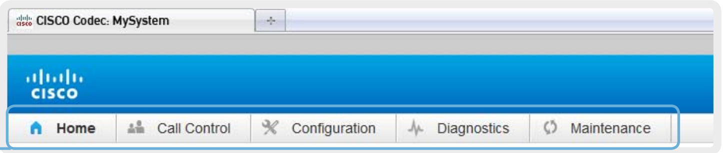
If the password currently is not set, leave the *Current password* field blank.

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 a main menu item, you can navigate to its related sub-pages.

Main menu



Hover the mouse over a main menu item, the titles of related sub-pages drops down.

Click a sub-page's title to open it. Only pages that the user has access rights for can be opened; the others are dimmed. *

Click Home on the main menu to return to the System Information page.

Sub-pages

Call Control
Call Control
Local Phone Book

Configuration
System Configuration
System Status
Personalization
Peripherals
User Administration
Sign In Banner
API
Security

Diagnostics
Troubleshooting
Log Files

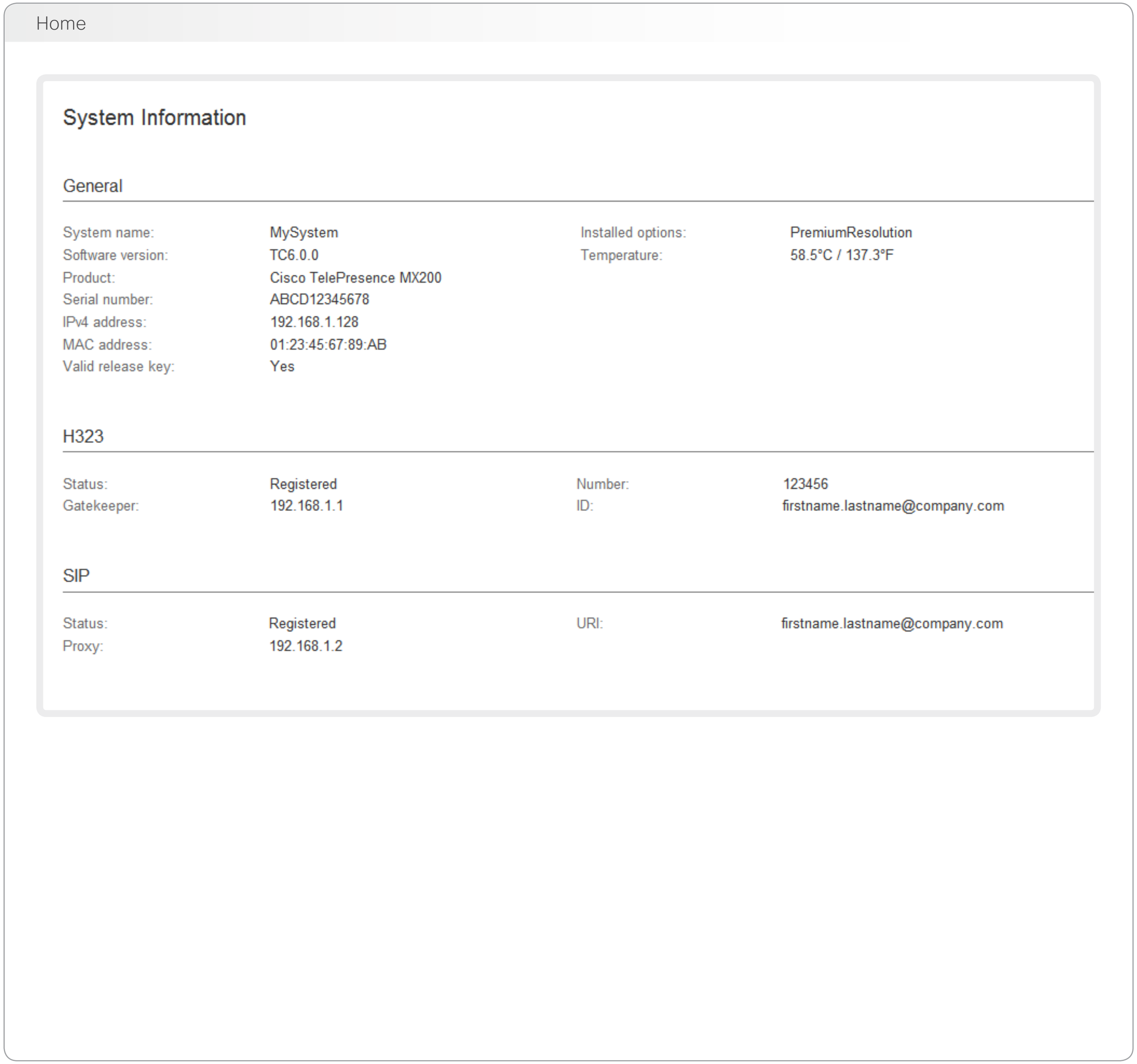
Maintenance
Software Upgrade
Backup and Restore
Factory Reset
Restart

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

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.



Home

System Information

General

System name:	MySystem	Installed options:	PremiumResolution
Software version:	TC6.0.0	Temperature:	58.5°C / 137.3°F
Product:	Cisco TelePresence MX200		
Serial number:	ABCD12345678		
IPv4 address:	192.168.1.128		
MAC address:	01:23:45:67:89:AB		
Valid release key:	Yes		

H323

Status:	Registered	Number:	123456
Gatekeeper:	192.168.1.1	ID:	firstname.lastname@company.com

SIP

Status:	Registered	URI:	firstname.lastname@company.com
Proxy:	192.168.1.2		

Placing a call

You can use the Call Control page of the web interface to initiate 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 *Local phone book* or *Directory*, or by typing a complete URI or number in the *Search and 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 both the Local phone book and the Directory will be listed as you type.

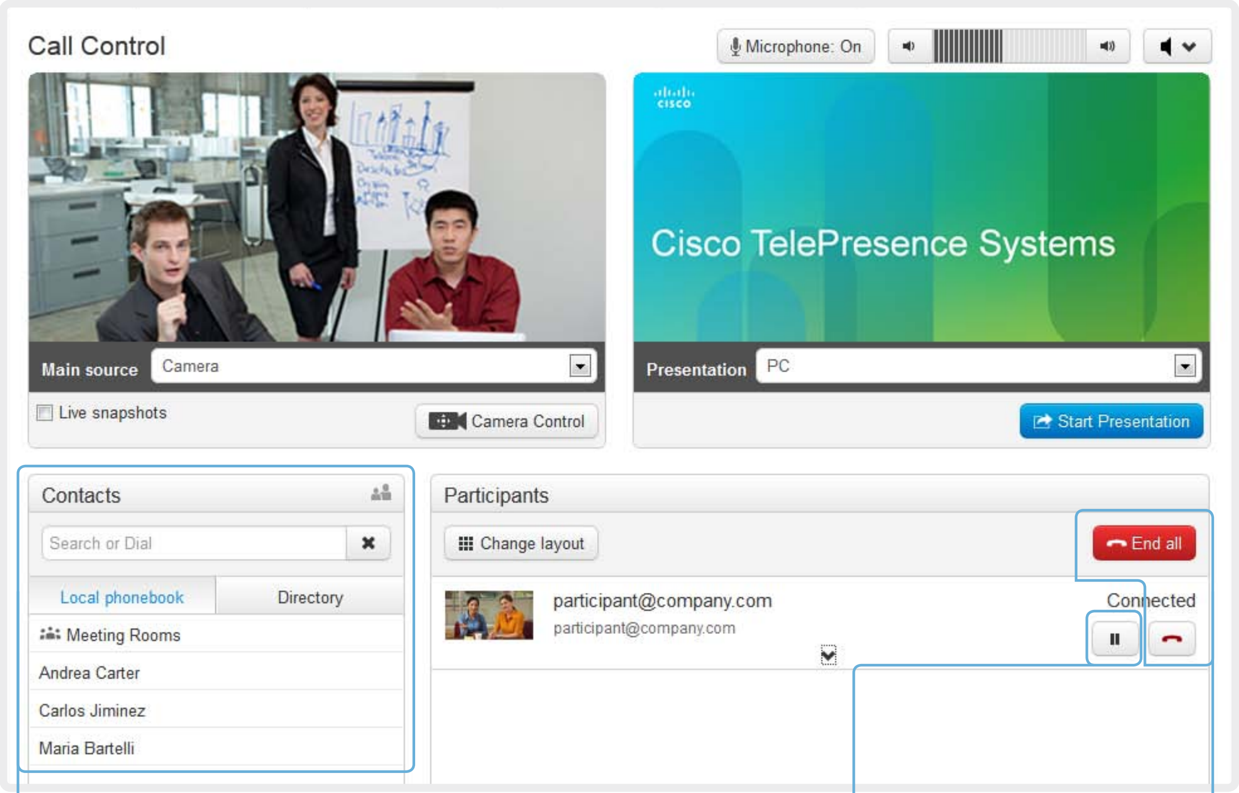
Select the entry in the phone book or directory before you click *Call*.

Calling more than one

A point-to-point video call (a call involving two parties only) may be expanded to include one more participant. This 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 > Call Control



Calling someone

Click a contact name, either in the *Local phone book* or in the *Directory*. 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 appears for the participant on hold.

Ending a call

To disconnect just one participant in a call, click the ☎ button for that participant.

Click the *End all* button to terminate the entire call.

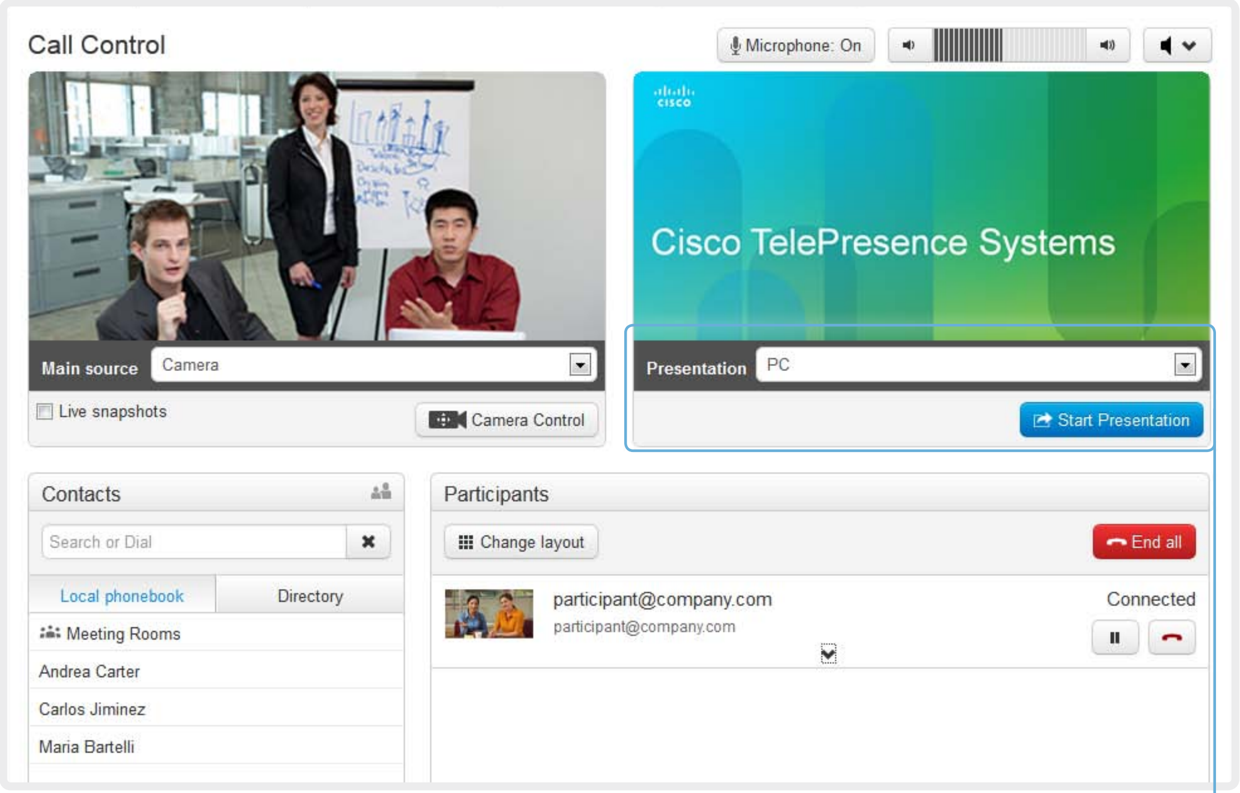
Sharing content

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 in the call.

If you are not in a call, the content is shared locally on your display.

Navigate to: Call Control > Call Control



Sharing content

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

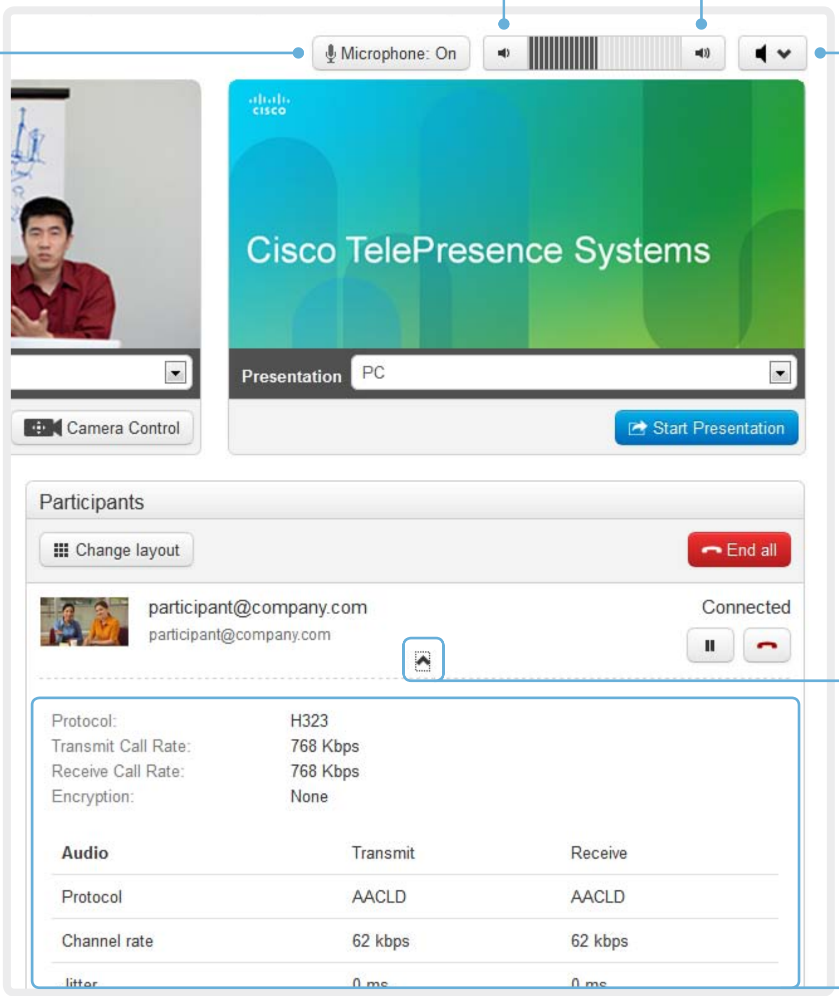
Stop content sharing:

Click the *Stop Presentation* button that becomes visible while sharing.

Controlling and monitoring a call

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

Navigate to: Call Control > Call Control



Protocol: H323
Transmit Call Rate: 768 Kbps
Receive Call Rate: 768 Kbps
Encryption: None

Audio	Transmit	Receive
Protocol	AACLD	AACLD
Channel rate	62 kbps	62 kbps
Jitter	0 ms	0 ms

Microphone mute

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

Click again to unmute.

Volume down

Volume up

Audio output selector

Choose between speakers, headset and handset.

Show/hide call details

Click the arrow to show details about the call.

Click the arrow again to hide the information.

Call details

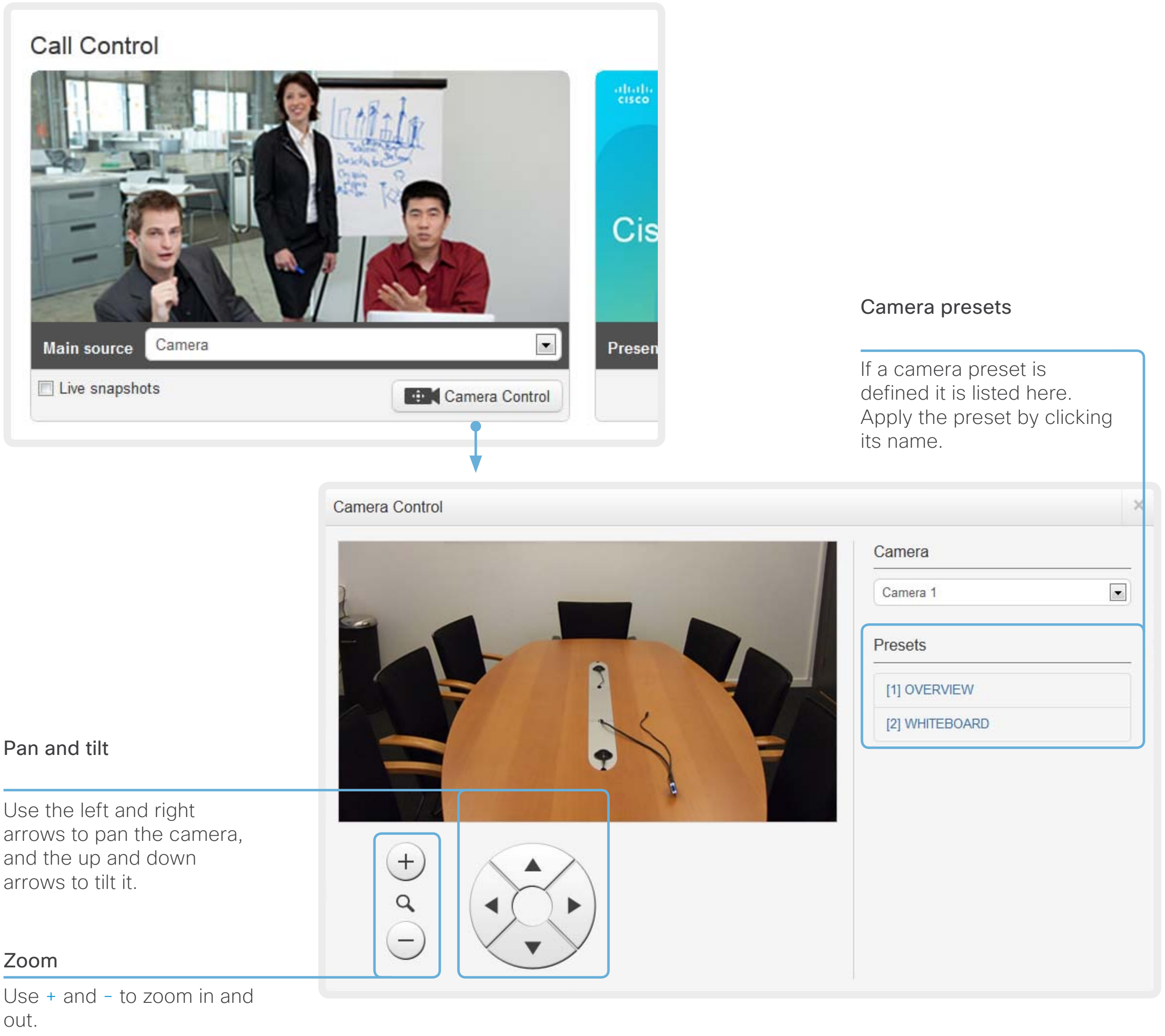
If necessary, scroll your browser to see the call details.

Controlling the camera

You can control the camera using the Call Control page.

Click the *Camera Control* button to open the window where you can pan, tilt and zoom the camera, and apply camera presets.

Navigate to: Call Control > Call Control



Camera presets

If a camera preset is defined it is listed here. Apply the preset by clicking its name.

Pan and tilt

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

Zoom

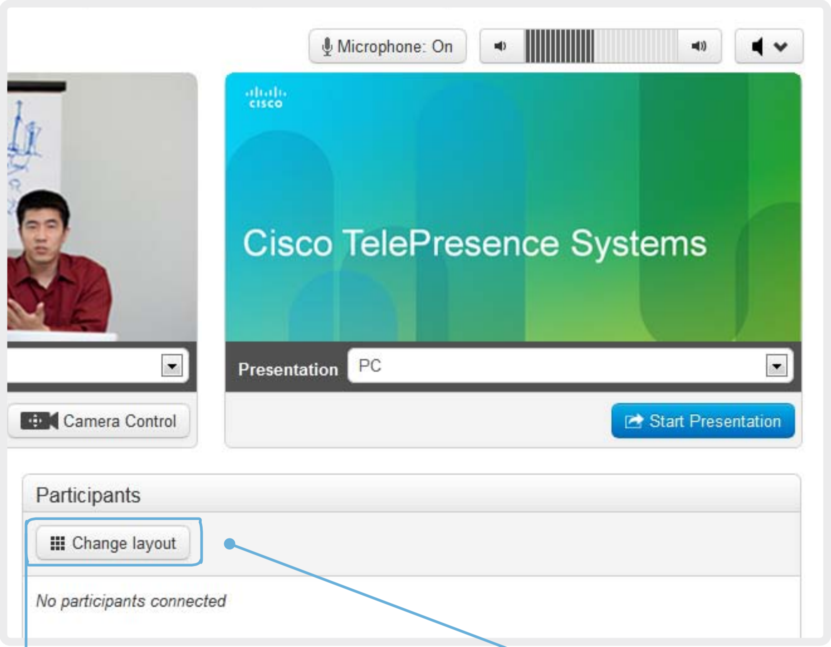
Use + and – to zoom in and out.

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 will require different layouts.

Navigate to: Call Control > Call Control



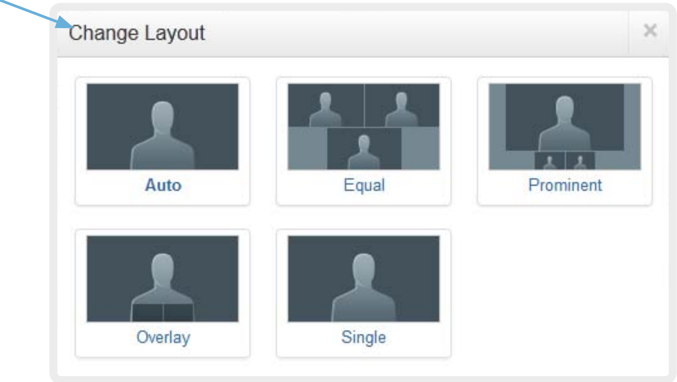
No participants connected

Change the layout

1. Click *Change layout*.

2. Choose your preferred layout in the window that opens.

You may change the layout while in a call.



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 Touch controller.

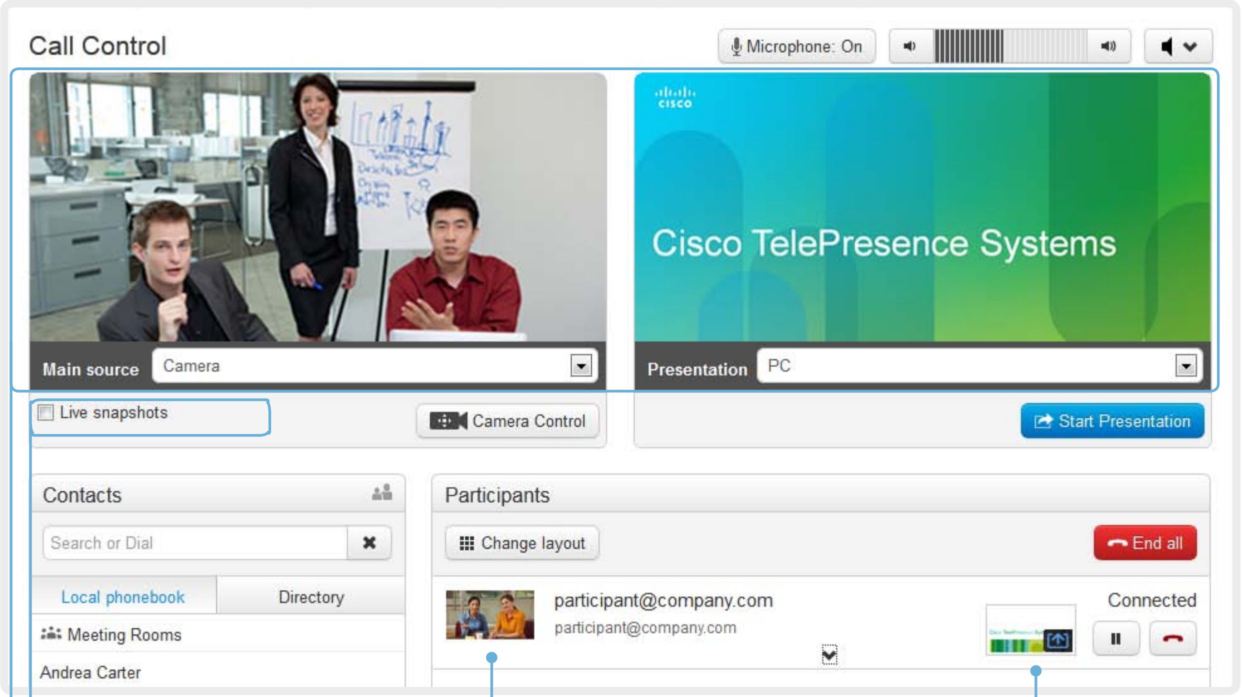
- Tap *Settings (✕) > Administrator Settings > Web Snapshots* and choose **On**.

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 20 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.

Navigate to: Call Control > Call Control



Far end snapshots

Take live snapshots

While the *Live snapshots* box is checked, snapshots are captured by your video system (main camera and presentation) approximately every two seconds.

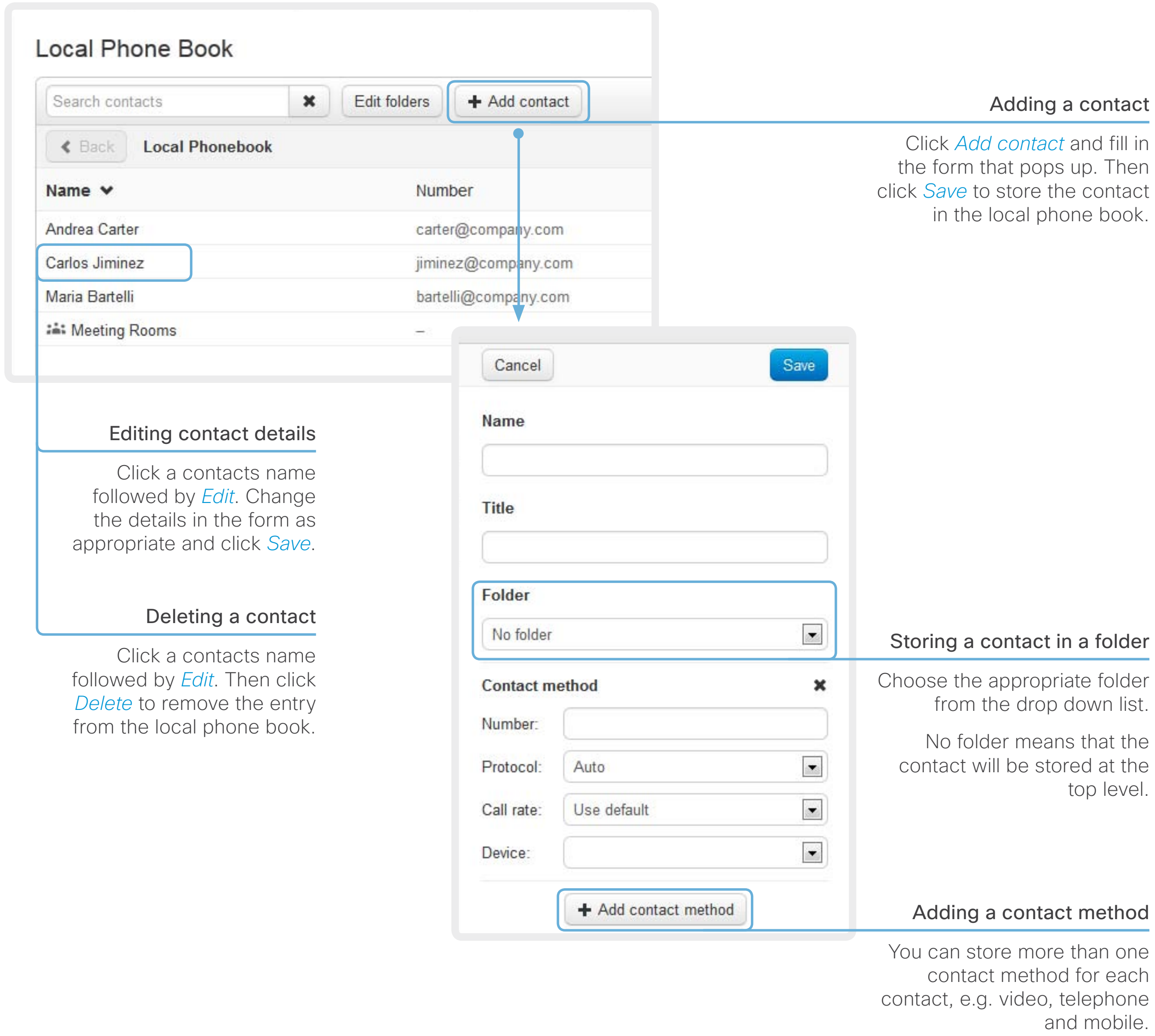
Snapshots from your video system

Managing the local phone book

The entries in the local phone book can be accessed from the following interfaces:

- Touch controller: The Favorites list
- Web interface: The local phone book on the call control page

Navigate to: Call Control > Local Phone Book



Local Phone Book

Name	Number
Andrea Carter	carter@company.com
Carlos Jiminez	jiminez@company.com
Maria Bartelli	bartelli@company.com
Meeting Rooms	–

Name:

Title:

Folder: No folder

Contact method

Number:

Protocol: Auto

Call rate: Use default

Device:

Adding a contact

Click *Add contact* and fill in the form that pops up. Then click *Save* to store the contact in the local phone book.

Editing contact details

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

Deleting a contact

Click a contacts name followed by *Edit*. Then click *Delete* to remove the entry from the local phone book.

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.

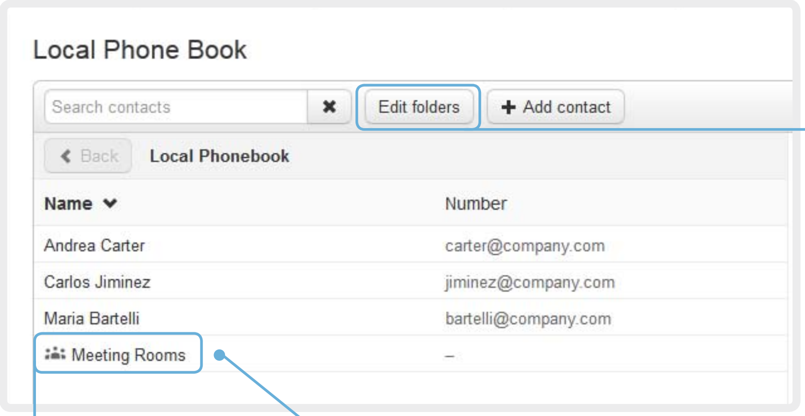
Adding a contact method

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

Local phone book folders

The entries in the local phone book can be hierarchically organized in folders.

Navigate to: Call Control > Local Phone Book



Name	Number
Andrea Carter	carter@company.com
Carlos Jiminez	jiminez@company.com
Maria Bartelli	bartelli@company.com
Meeting Rooms	–

Managing folders

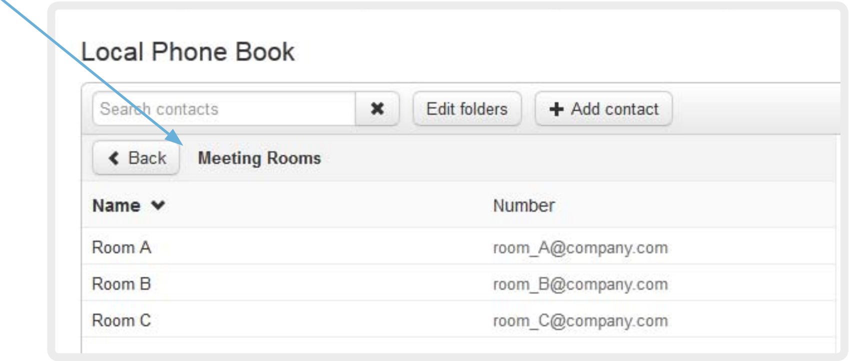
i. Click *Edit folders*.

ii. Click *Add folder* and fill in its details to create at new folder; or click the name of an existing folder to view and edit its details.

iii. Click *Save folder* to store the details; or click *Delete folder* to remove a folder and all its contacts and sub-folders.

Opening a folder

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



Name	Number
Room A	room_A@company.com
Room B	room_B@company.com
Room C	room_C@company.com

System configuration

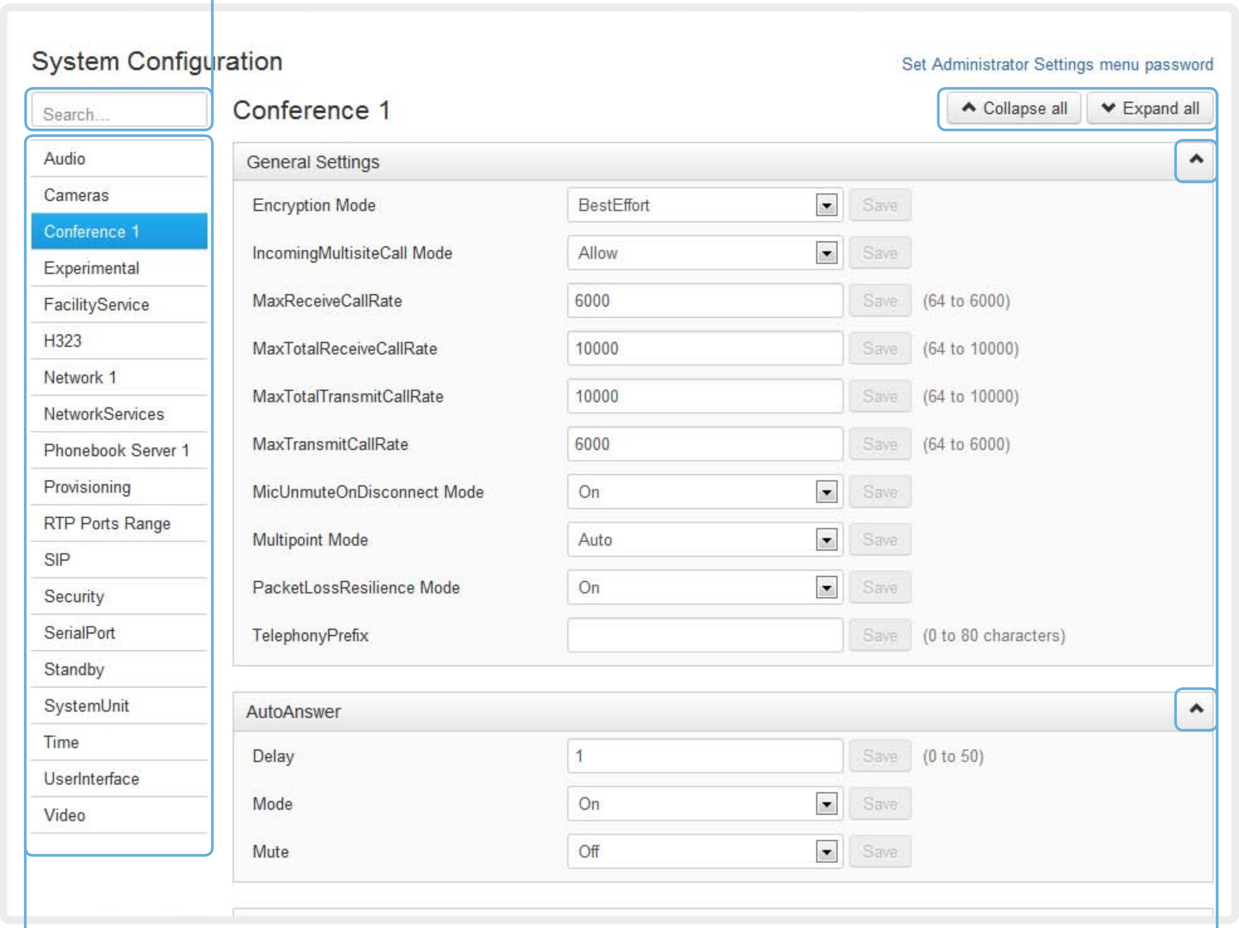
The system settings are grouped in several categories. When you choose a category in the left pane all related settings appear to the right.

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

Navigate to: Configuration > System Configuration

Searching for settings

Enter as many letters as needed in the search field. All settings containing these letters will be highlighted.



Conference 1

General Settings

Encryption Mode	BestEffort	
IncomingMultisiteCall Mode	Allow	
MaxReceiveCallRate	6000	(64 to 6000)
MaxTotalReceiveCallRate	10000	(64 to 10000)
MaxTotalTransmitCallRate	10000	(64 to 10000)
MaxTransmitCallRate	6000	(64 to 6000)
MicUnmuteOnDisconnect Mode	On	
Multipoint Mode	Auto	
PacketLossResilience Mode	On	
TelephonyPrefix		(0 to 80 characters)

AutoAnswer

Delay	1	(0 to 50)
Mode	On	
Mute	Off	

Selecting a category

The system settings are structured in several categories. Choose a category to display the related settings.

Expanding and collapsing lists

Use the buttons to expand and collapse all or individual lists.

Changing system settings

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

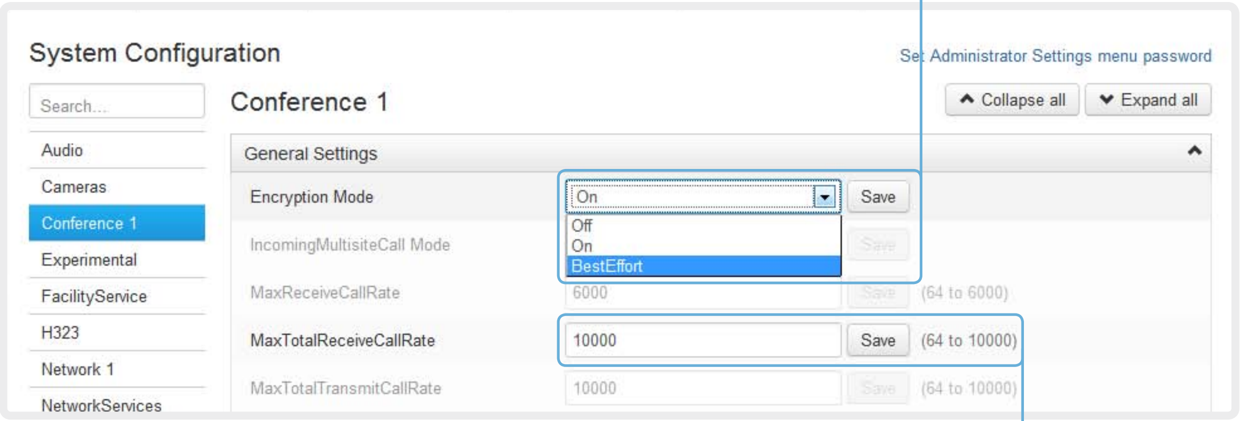
Different settings may require different user credentials. In order to be sure that an administrator is able to change all system settings, the user must possess all user roles.

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.

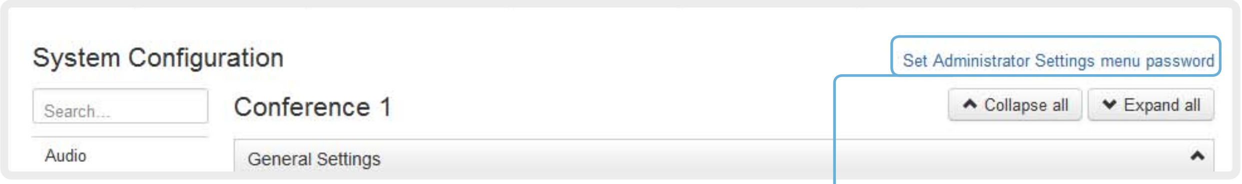
Setting the Administrator Settings menu password

When starting up the video conference system for the first time anyone can access the Administrator Settings menu with the Touch controller because the menu password is not set.

⚠ We strongly recommend that you define a menu password, because the Administrator Settings may severely affect the behavior of the video conference system.

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

Navigate to: Configuration > System Configuration

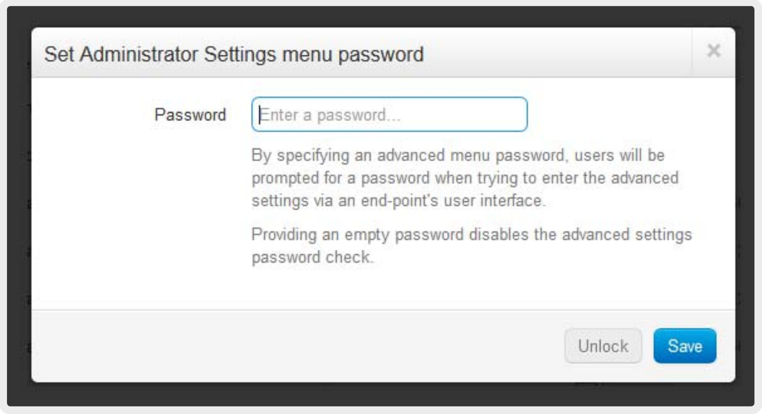


Changing the menu password

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

Enter a new password in the text input field and click *Save* to store it.

Use the *Unlock* button to clear the existing password.



By specifying an advanced menu password, users will be prompted for a password when trying to enter the advanced settings via an end-point's user interface.

Providing an empty password disables the advanced settings password check.

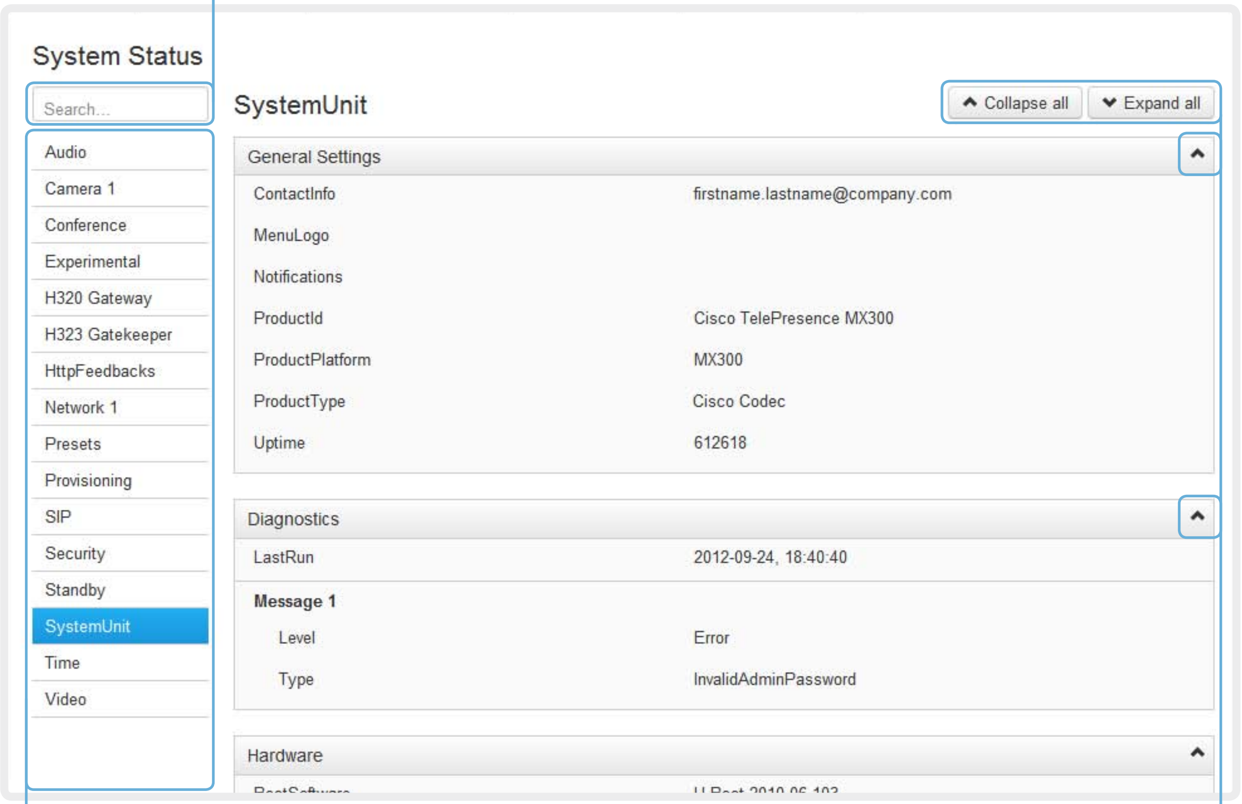
System status

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

Searching for status entries

Enter as many letters as needed in the search field. All entries containing these letters will be highlighted.



General Settings

ContactInfo	firstname.lastname@company.com
MenuLogo	
Notifications	
ProductId	Cisco TelePresence MX300
ProductPlatform	MX300
ProductType	Cisco Codec
Uptime	612618

Diagnostics

LastRun	2012-09-24, 18:40:40
Message 1	
Level	Error
Type	InvalidAdminPassword

Selecting a category

The system status is structured in several categories. Choose a category to display the related status information.

Expanding and collapsing lists

Use the buttons to expand and collapse all or individual lists.

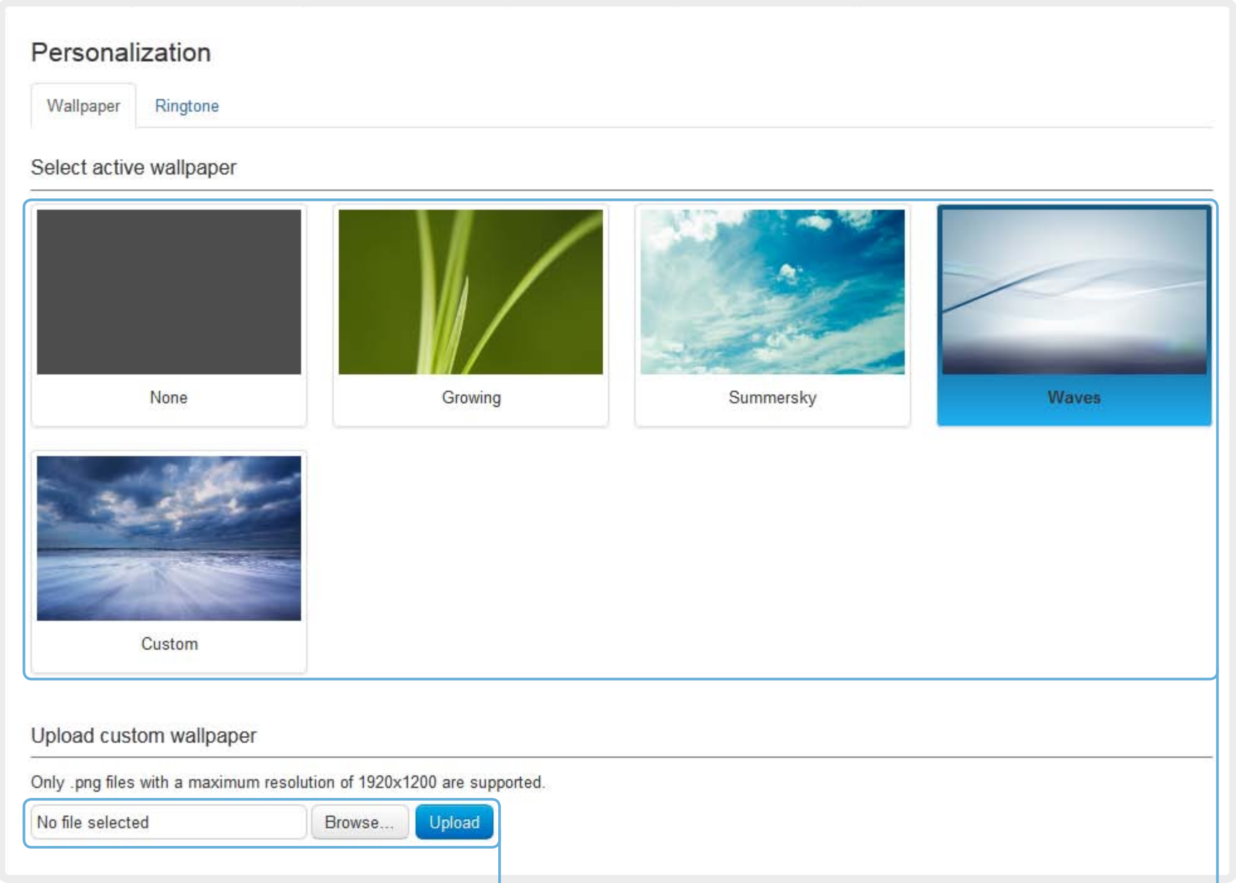
Choosing a wallpaper

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 to be displayed on the main display, you may upload and use a custom wallpaper.

The custom wallpaper applies to only the main display and will not appear on the Touch controller.

Navigate to: Configuration > Personalization : Wallpaper tab



Personalization

Wallpaper | Ringtone

Select active wallpaper

Upload custom wallpaper

Only .png files with a maximum resolution of 1920x1200 are supported.

Uploading a custom wallpaper file

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

The file format must be .png and the maximum image size is 1920 × 1200 pixels.

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

Choosing a wallpaper

Choose a wallpaper from the list.

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

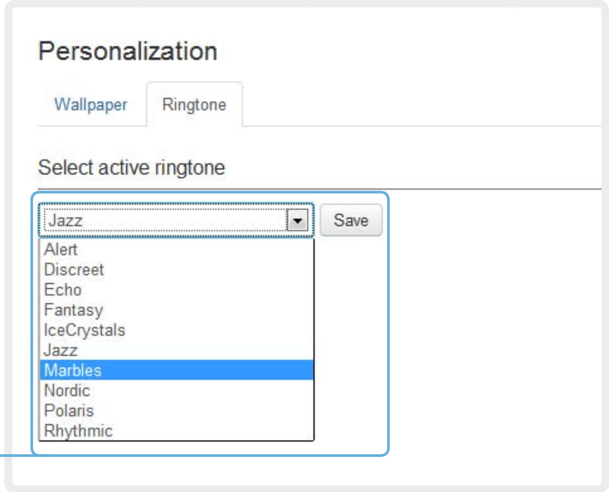
The chosen wallpaper is highlighted.

Choosing a ringtone

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

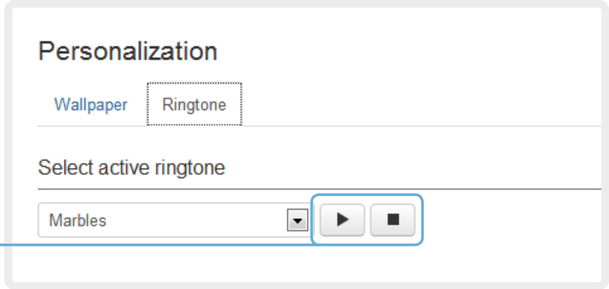
Even if the web interface is used to initiate the playback it is the video system that plays back the ringtone; it is not the PC running the web interface.

Navigate to: Configuration > Personalization : Ringtone tab



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.

You must save the ringtone before it can be played back.

Peripherals overview

This page shows an overview of the video input and video output configuration, as well as information about any camera(s), Touch controller or ISDN Link that is connected to your video system.

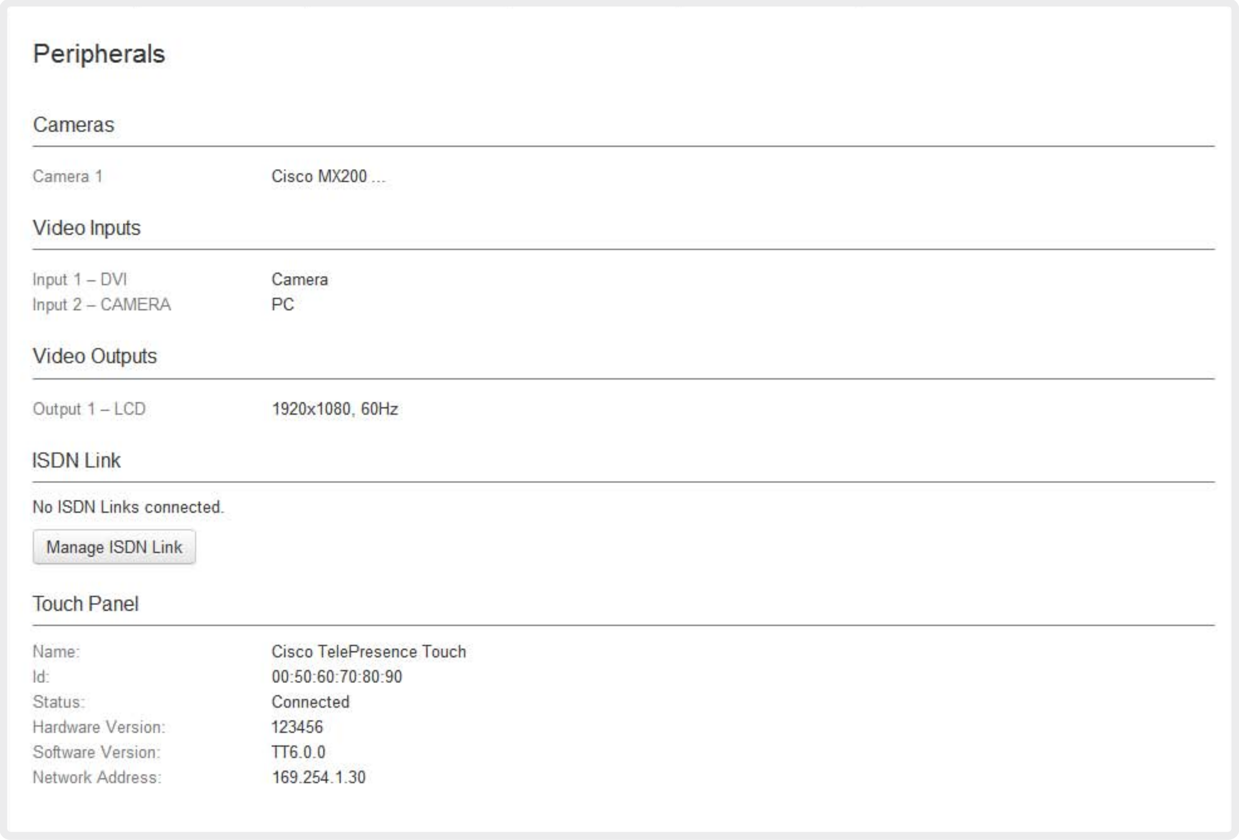
The illustration to the right is an example; your system may have different peripherals and video input/output configurations.

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

Navigate to: Configuration > Peripherals



Peripherals

Cameras

Camera 1	Cisco MX200 ...

Video Inputs

Input 1 – DVI	Camera
Input 2 – CAMERA	PC

Video Outputs

Output 1 – LCD	1920x1080, 60Hz

ISDN Link

No ISDN Links connected.

Touch Panel

Name:	Cisco TelePresence Touch
Id:	00:50:60:70:80:90
Status:	Connected
Hardware Version:	123456
Software Version:	TT6.0.0
Network Address:	169.254.1.30

User administration

From this page you can manage the user accounts of your video conference system. You can create new user accounts, edit the details of existing users, and delete users.

The default user account

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

⚠ It is highly recommended 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:

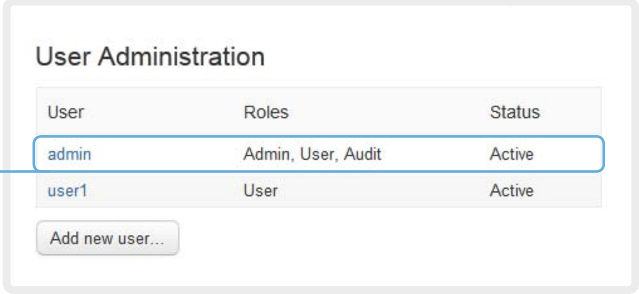
- ADMIN: A user holding this role can create new users and change most settings. The user neither can upload audit certificates nor change the security audit settings.
- USER: A user holding this role can make calls and search the phone book. The user can modify a few settings, e.g. adjusting the audio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



User Administration

User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active

User administration, continued

Creating a new user account

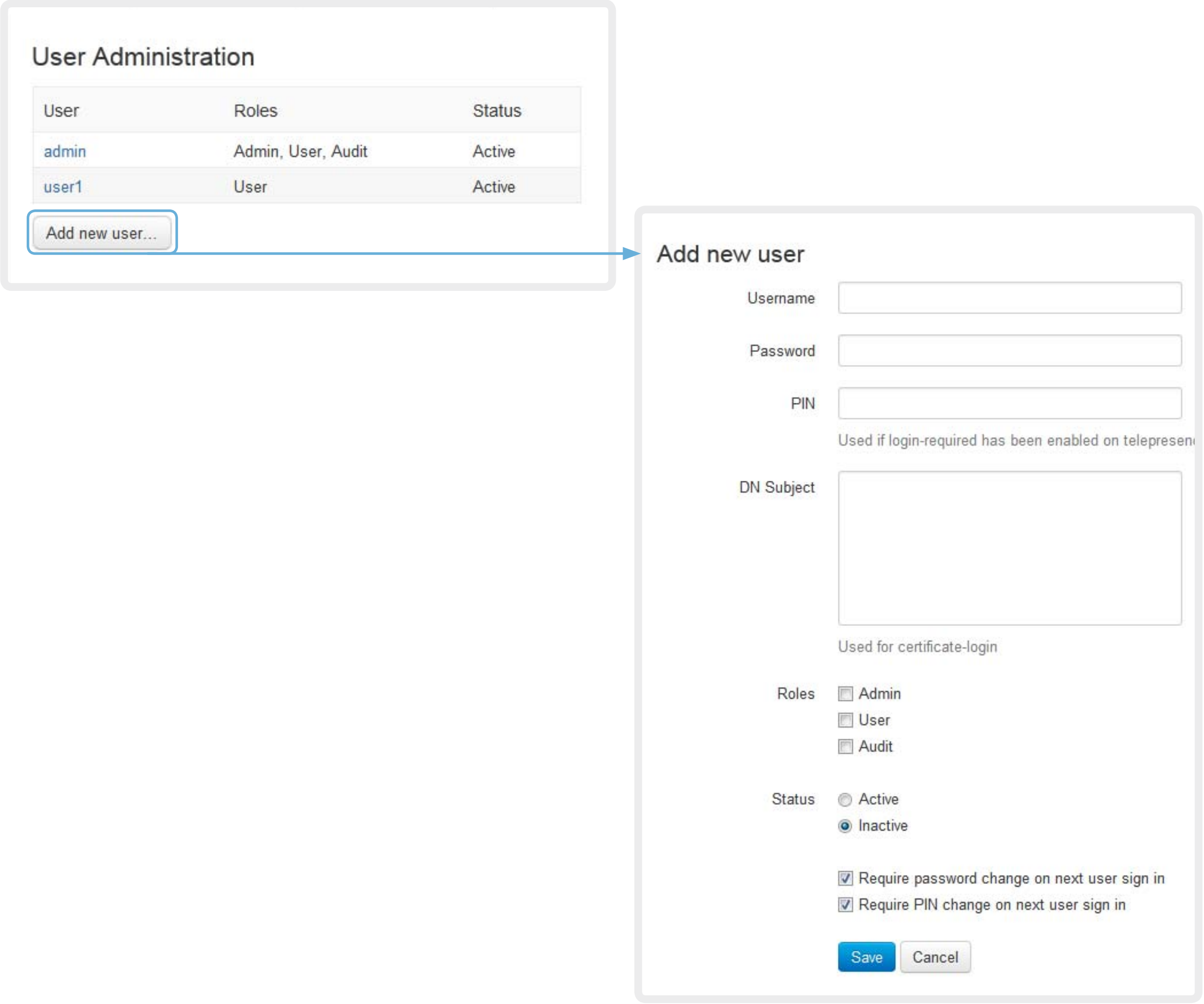
Follow these steps in order to create a new user account:

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 Distinguished Name (DN) Subject field unless you want to use certificate login on https.
3. Set the Status to **Active** to activate the user.
4. Click *Save* to save the changes.

Navigate to: Configuration > User Administration



User Administration

User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active

Add new user

Username

Password

PIN

Used if login-required has been enabled on telepresen

DN Subject

Used for certificate-login

Roles
□ Admin
□ User
□ Audit

Status
○ Active
● Inactive

☑ Require password change on next user sign in
☑ Require PIN change on next user sign in

User administration, continued

Editing user details

Follow these steps in order to edit an existing user account:

1. Click the name of an existing user to open the Editing user window.
2. Edit the details.
3. Click *Save* to save the changes or *Cancel* to go back one step without storing the information.

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. Open the Editing user window by clicking the name of the user.
2. Set the Status to **Inactive**.
3. Click *Save* to save the changes.

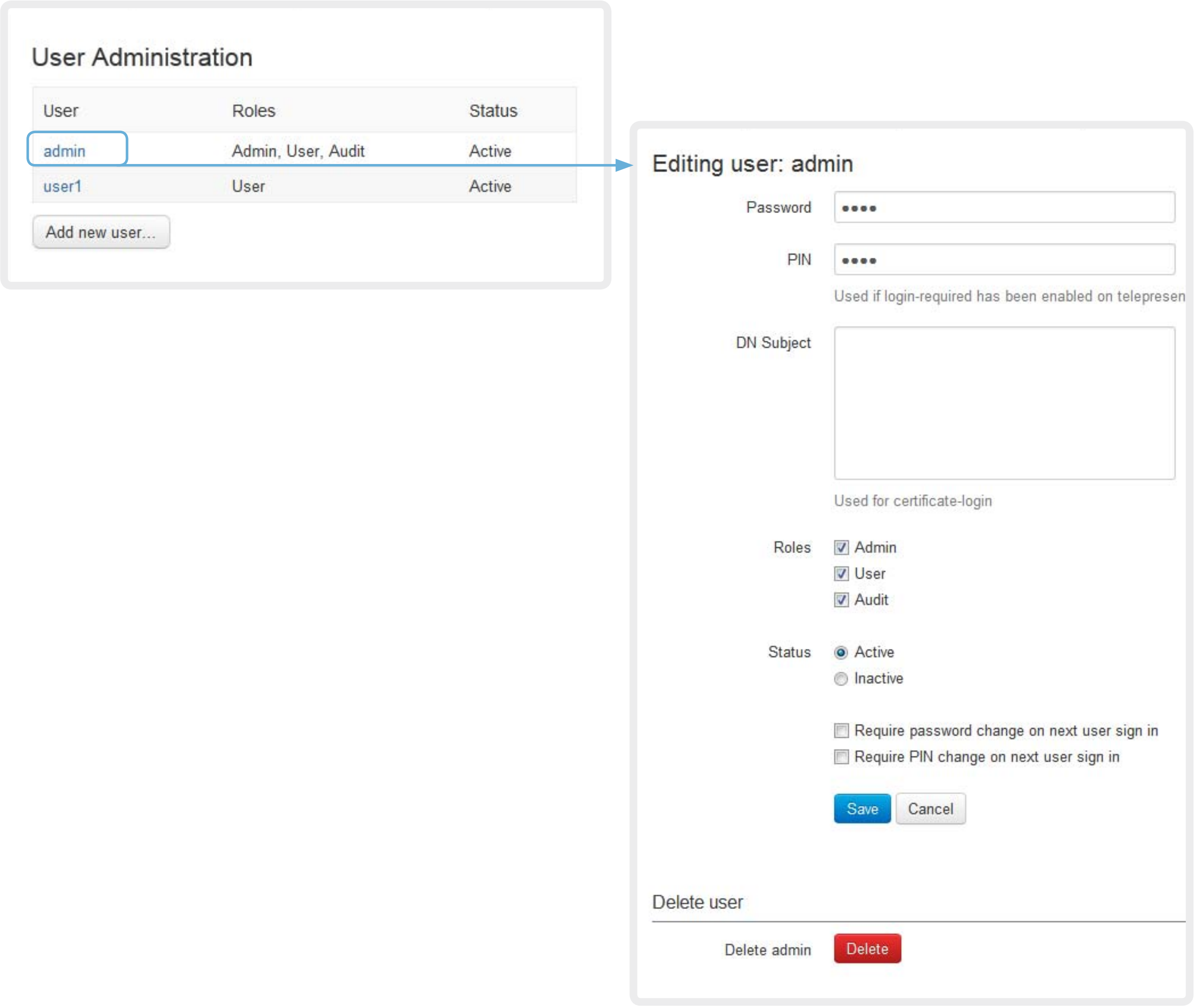
Deleting a user account

Follow these steps in order to delete a user account:

⚠ Always keep at least one user with ADMIN rights.

1. Open the Editing user window by clicking the name of the user.
2. Click *Delete*.

Navigate to: Configuration > User Administration



User Administration

User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active

Editing user: admin

Password: ••••

PIN: ••••

Used if login-required has been enabled on telepresen

DN Subject:

Used for certificate-login

Roles: ☑ Admin ☑ User ☑ Audit

Status: ● Active ○ Inactive

□ Require password change on next user sign in

□ Require PIN change on next user sign in

Delete user

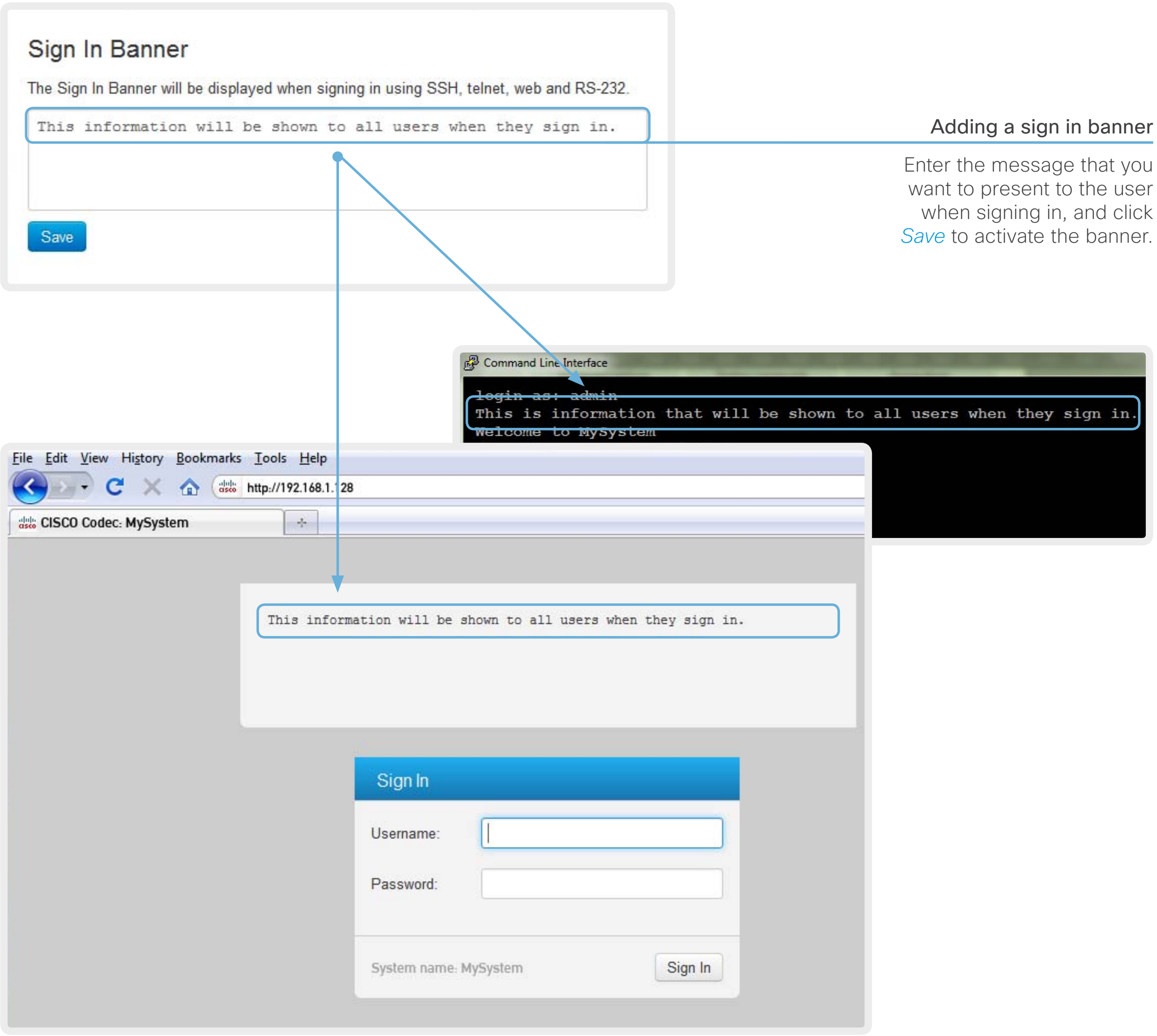
Delete admin

Adding a sign in banner

A sign in banner is a message that is displayed to the user when signing in.

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



Sign In Banner

The Sign In Banner will be displayed when signing in using SSH, telnet, web and RS-232.

```
This information will be shown to all users when they sign in.
```

Save

Command Line Interface

```
login as: admin
This is information that will be shown to all users when they sign in.
Welcome to MySystem
```

```
This information will be shown to all users when they sign in.
```

Sign In

Username:

Password:

System name: MySystem

Sign In

Adding a sign in banner

Enter the message that you want to present to the user when signing in, and click *Save* to activate the banner.

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.

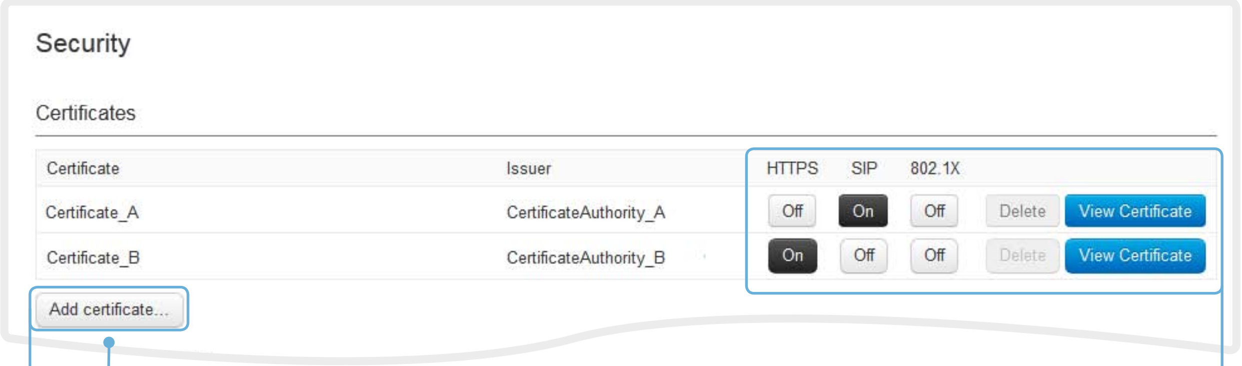
The video system's certificates are text files that verify the authenticity of the system. These certificates may be issued by a certificate authority (CA).

The certificate 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.

Navigate to: Configuration > Security

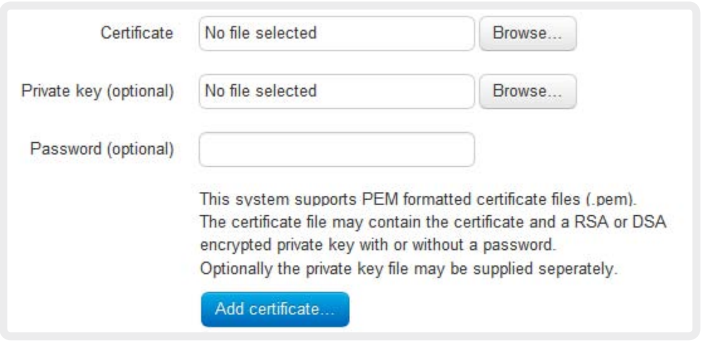


Security

Certificates

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

Add certificate...



Certificate	No file selected	Browse...
Private key (optional)	No file selected	Browse...
Password (optional)		

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

Add certificate...

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.

Adding a certificate

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

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).

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.

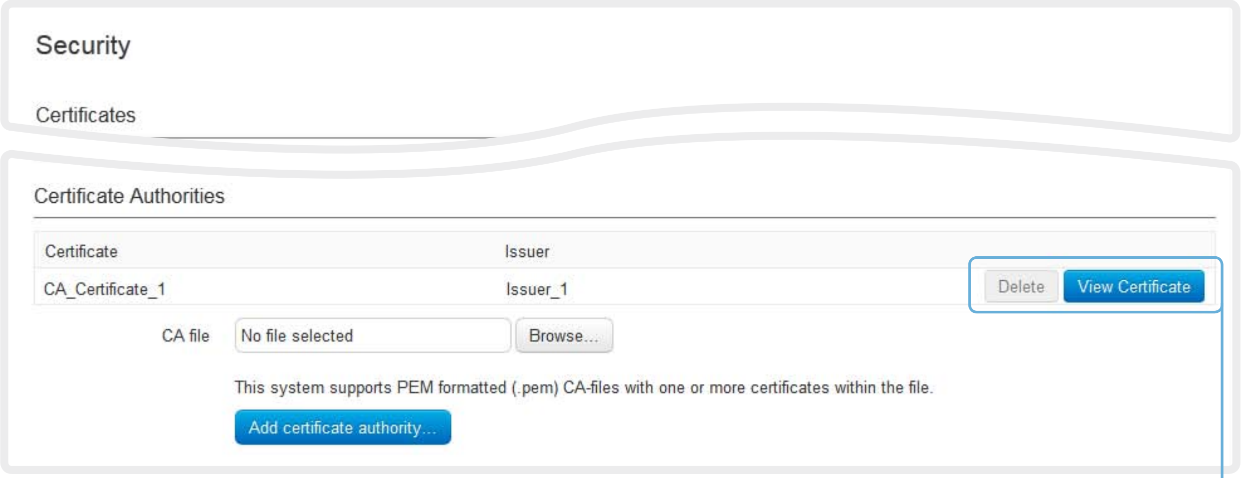
The certificates are text files that verify the authenticity of the server or client. The certificates must be signed by a trusted certificate authority (CA).

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 CAs to verify certificates for as well HTTPS, SIP and IEEE 802.1X connections.

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

Navigate to: Configuration > Security



Security

Certificates

Certificate Authorities

Certificate	Issuer
CA_Certificate_1	Issuer_1

CA file: No file selected

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

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 *Show CAs...* to list the existing CA certificates.

ii. Click *Add Certificate Authority...*.

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

iv. Click *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).

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 web interface.

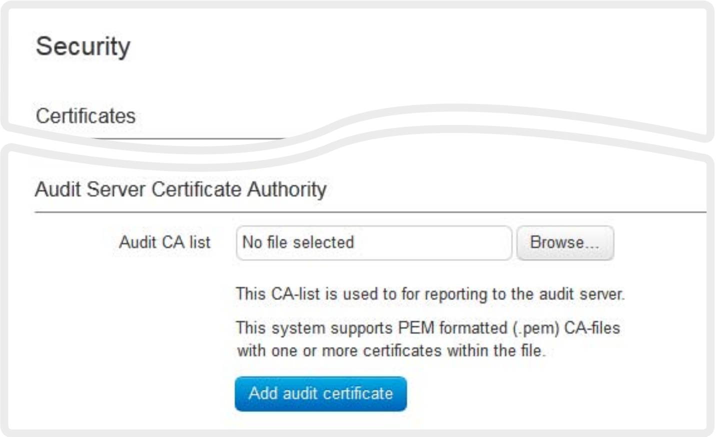
In ExternalSecure audit logging mode the video system sends encrypted audit logs to an external audit server (syslog server), which identity must be verified by a signed certificate.

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 / Configuration > System Configuration



Audit CA list: No file selected

This CA-list is used to for reporting to the audit server.

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

1. Upload a list of audit server certificates

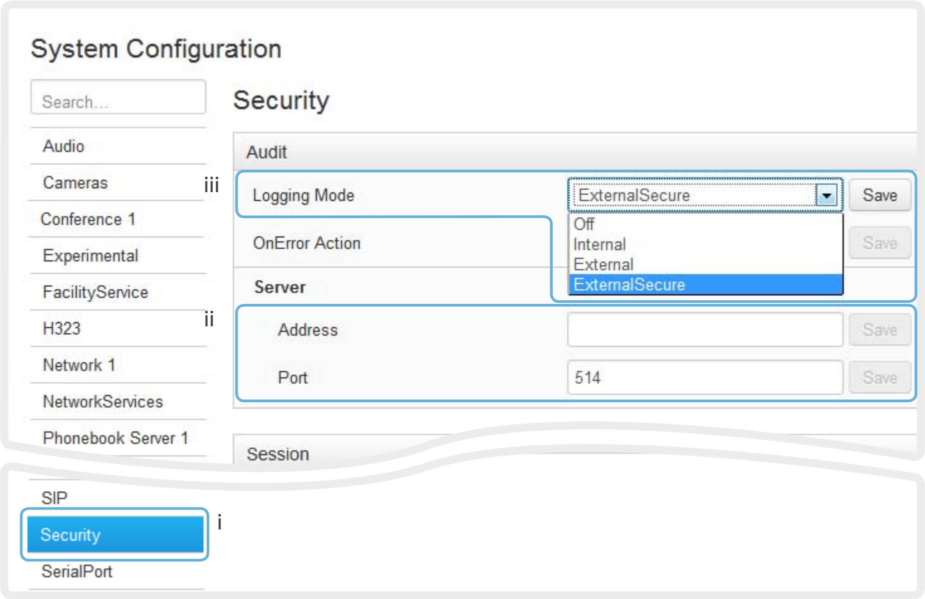
⚠ The entries in a new file with CA certificates will overwrite the existing list, that is, any previously stored audit certificates will be lost when you add a new file.

i. Click *Add audit server certificate authority...*.

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

iii. 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).



Logging Mode: ExternalSecure

Address:

Port: 514

2. Enable secure audit logging

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

ii. Enter the *Address* and *Port* number of 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.

Setting strong security mode

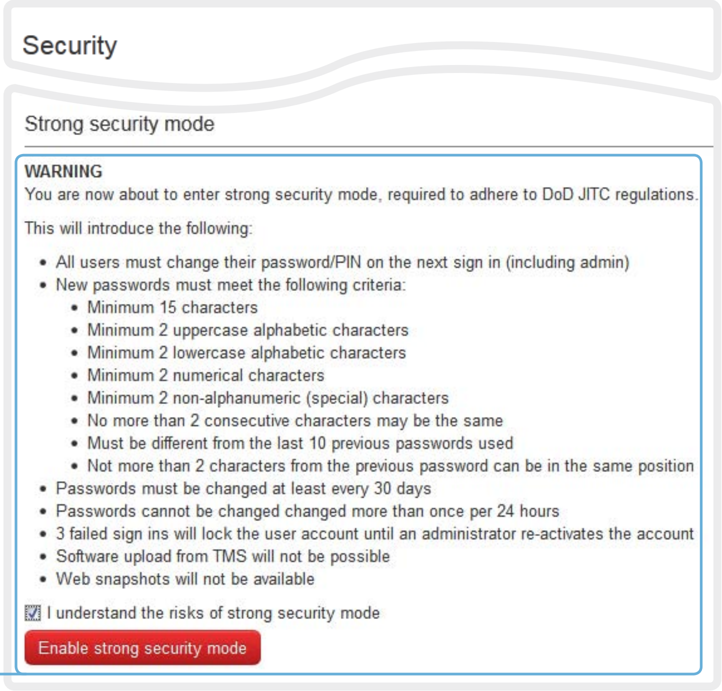
Strong security mode should be used only when compliance with DoD JITC regulations is required.

⚠ Read the warning 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



Security

Strong security mode

WARNING

You are now about to enter strong security mode, required to adhere to DoD JITC regulations.

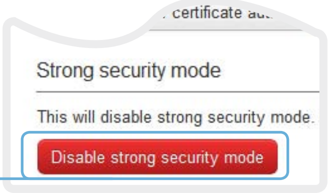
This will introduce the following:

- All users must change their password/PIN on the next sign in (including admin)
- New passwords must meet the following criteria:
  - Minimum 15 characters
  - Minimum 2 uppercase alphabetic characters
  - Minimum 2 lowercase alphabetic characters
  - Minimum 2 numerical characters
  - Minimum 2 non-alphanumeric (special) characters
  - No more than 2 consecutive characters may be the same
  - Must be different from the last 10 previous passwords used
  - Not more than 2 characters from the previous password can be in the same position
- Passwords must be changed at least every 30 days
- Passwords cannot be changed changed more than once per 24 hours
- 3 failed sign ins will lock the user account until an administrator re-activates the account
- Software upload from TMS will not be possible
- Web snapshots will not be available

☑ I understand the risks of strong security mode

Setting strong security mode

1. Click *Configure strong security mode...* and read the warning carefully before continuing.
2. If you want to use strong security mode, check the *I understand the risks of strong security mode* check box and click *Enable strong security mode*.
3. Change the password to meet the strict criteria shown in the warning. How to change the system password: see the ▶ Setting passwords section.
4. Restart the codec for the change to take effect.



Strong security mode

This will disable strong security mode.

Return to normal mode

1. When in strong security mode, the system can be restored to normal mode by clicking *Configure strong security mode...* followed by *Disable strong security mode*.
2. Restart the codec for the change to take effect.

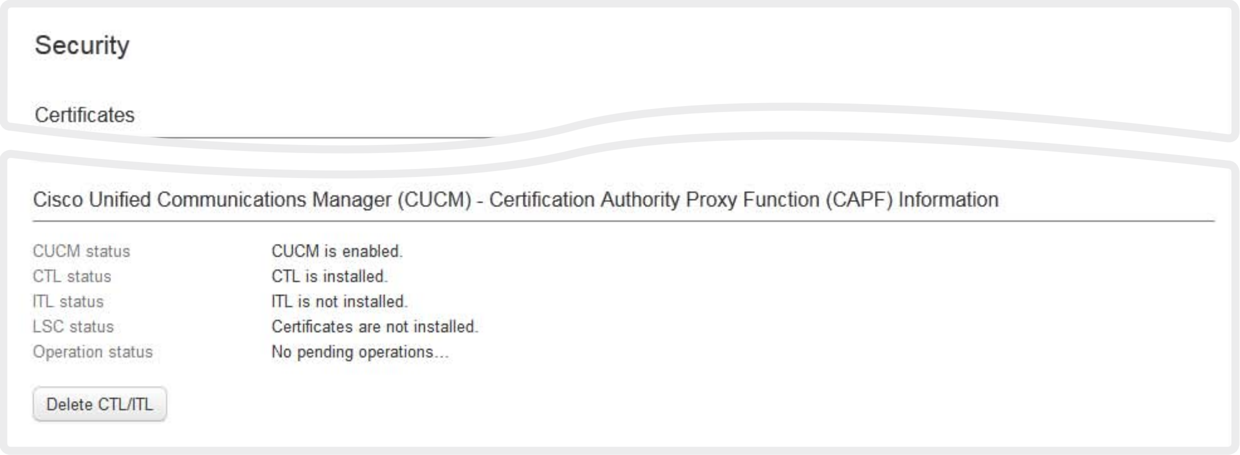
Deleting trust lists (CUCM only)

The Cisco Unified Communications Manager (CUCM) and Certification Authority Proxy Function (CAPF) information that is shown on the Security page is only relevant for video systems that are registered to CUCM.

The web interface can be used to delete an existing Certificate Trust List (CTL) that is stored on the video system. Normally, you will not delete the old CTL file, but there are a few cases when you will need to delete it.

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

Navigate to: Configuration > Security



Security

Certificates

Cisco Unified Communications Manager (CUCM) - Certification Authority Proxy Function (CAPF) Information

CUCM status	CUCM is enabled.
CTL status	CTL is installed.
ITL status	ITL is not installed.
LSC status	Certificates are not installed.
Operation status	No pending operations...

Troubleshooting

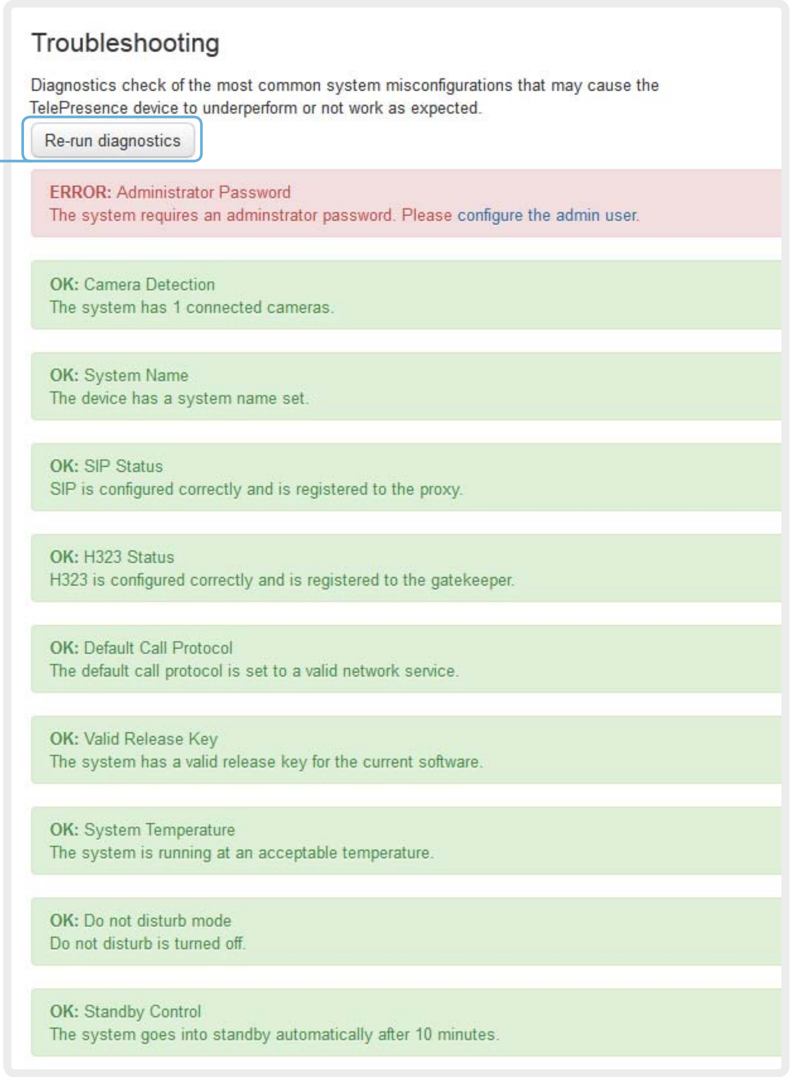
The troubleshooting page lists the status for some common sources of errors. The list may be different for different products and installations.

Errors are clearly marked in red color, and 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.



Troubleshooting

Diagnostics check of the most common system misconfigurations that may cause the TelePresence device to underperform or not work as expected.

ERROR: Administrator Password
The system requires an adminstrator password. Please configure the admin user.

OK: Camera Detection
The system has 1 connected cameras.

OK: System Name
The device has a system name set.

OK: SIP Status
SIP is configured correctly and is registered to the proxy.

OK: H323 Status
H323 is configured correctly and is registered to the gatekeeper.

OK: Default Call Protocol
The default call protocol is set to a valid network service.

OK: Valid Release Key
The system has a valid release key for the current software.

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

OK: Do not disturb mode
Do not disturb is turned off.

OK: Standby Control
The system goes into standby automatically after 10 minutes.

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.

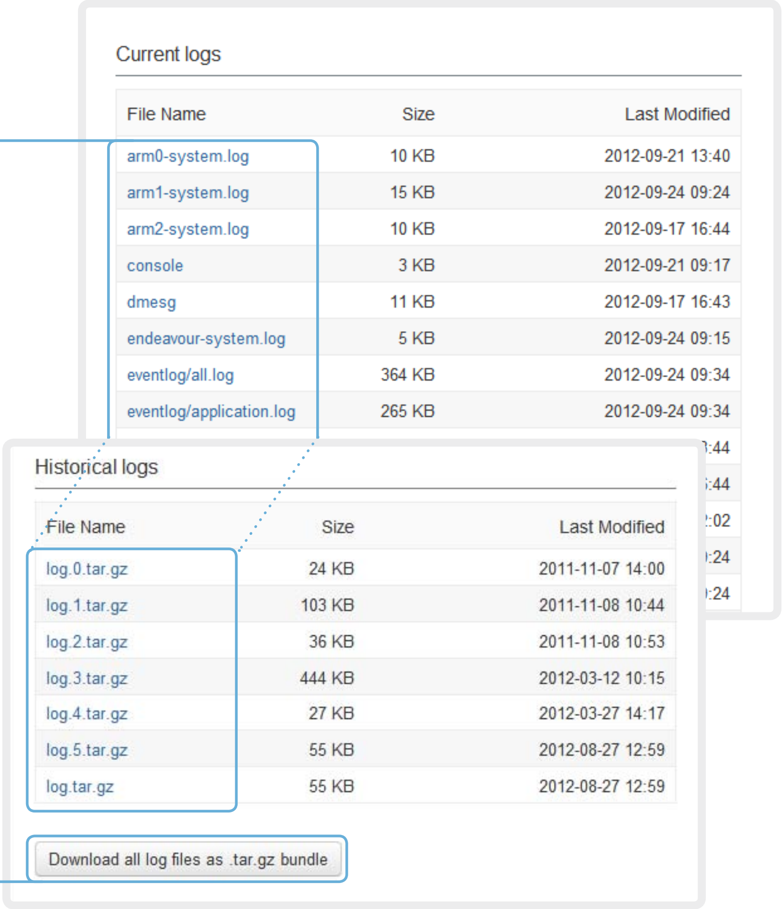
The *current log files* are time stamped event log files.

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

Navigate to: Diagnostics > Log Files

Downloading one file

Click the file name and follow the instructions to save or open the file (left or right click depending on your browser).



Current logs

File Name	Size	Last Modified
arm0-system.log	10 KB	2012-09-21 13:40
arm1-system.log	15 KB	2012-09-24 09:24
arm2-system.log	10 KB	2012-09-17 16:44
console	3 KB	2012-09-21 09:17
dmesg	11 KB	2012-09-17 16:43
endeavour-system.log	5 KB	2012-09-24 09:15
eventlog/all.log	364 KB	2012-09-24 09:34
eventlog/application.log	265 KB	2012-09-24 09:34
		:44
		:44
		:02
		:24
		:24

Historical logs

File Name	Size	Last Modified
log.0.tar.gz	24 KB	2011-11-07 14:00
log.1.tar.gz	103 KB	2011-11-08 10:44
log.2.tar.gz	36 KB	2011-11-08 10:53
log.3.tar.gz	444 KB	2012-03-12 10:15
log.4.tar.gz	27 KB	2012-03-27 14:17
log.5.tar.gz	55 KB	2012-08-27 12:59
log.tar.gz	55 KB	2012-08-27 12:59

Downloading all files

Click *Download all log files as .tar.gz bundle* and follow the instructions.

Upgrading the system software

This video conference system is using TC software. The version described in this document is TC6.0.

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 (TC6).

Go to: ► http://www.cisco.com/en/US/products/ps11776/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 file name is something like “s52000tc6_0_0.pkg” (each software version has a unique file name).

Release key and option keys

The *release key* is required to be able to use the software. A new release key is required for every major software release (e.g. when upgrading from TC5.x or older to TC6.x).

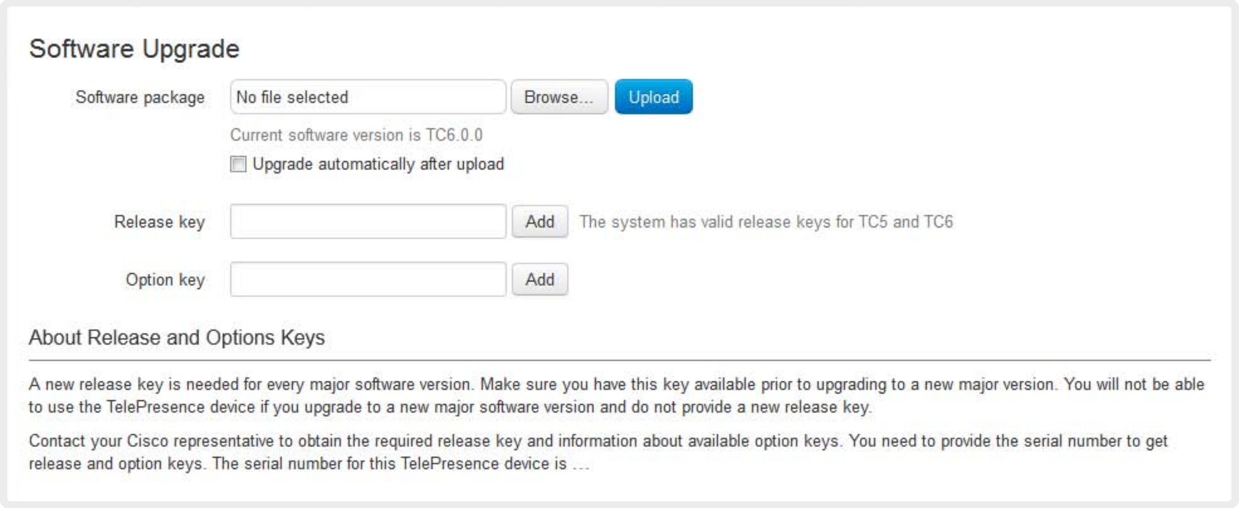
An *option key* is required to activate optional functionality. You may have several option keys in your system.

The available options are:

- Premium resolution

Contact your Cisco representative to obtain the required release key and option keys.

Navigate to: Maintenance > Software Upgrade



Software Upgrade

Software package: No file selected [Browse...] [Upload]

Current software version is TC6.0.0

□ Upgrade automatically after upload

Release key: [Add] The system has valid release keys for TC5 and TC6

Option key: [Add]

About Release and Options Keys

A new release key is needed for every major software version. Make sure you have this key available prior to upgrading to a new major version. You will not be able to use the TelePresence device if you upgrade to a new major software version and do not provide a new release key.

Contact your Cisco representative to obtain the required release key and information about available option keys. You need to provide the serial number to get release and option keys. The serial number for this TelePresence device is ...

1. Add the release and option keys

Contact your Cisco representative to obtain the required key(s). Then perform the following steps:

i. Enter the *Release key* in the appropriate text input field and click *Add*.

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

If you have more than one option key, repeat step ii for all of them.

Each system has unique keys.

Release key format: “1TC005-1-0C22E348”
Option key format: “1N000-1-AA7A4A09”

2. Install new software

Download the appropriate software package from the Cisco Software Download web page (see link to the left) before you start the software upgrade as described in these steps:

i. Click *Browse...* and find the .pkg file containing 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 reboots automatically after the installation.

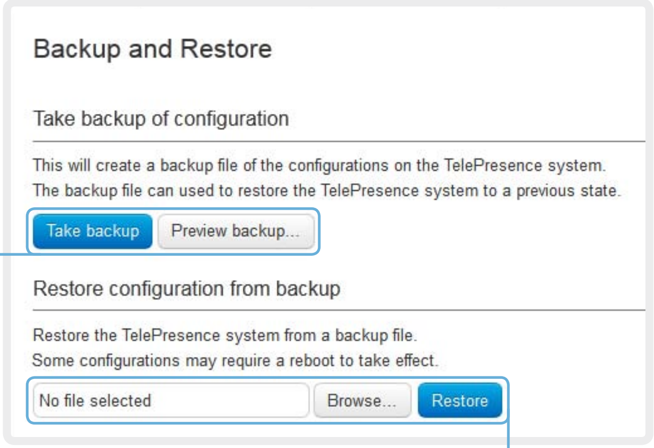
You must sign in anew in order to continue working with the web interface after the reboot.

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 old configuration.

Navigate to: Maintenance > Backup and Restore



Backup and Restore

Take backup of configuration

This will create a backup file of the configurations on the TelePresence system.
The backup file can used to restore the TelePresence system to a previous state.

Restore configuration from backup

Restore the TelePresence system from a backup file.
Some configurations may require a reboot to take effect.

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 (.tsh).

Restoring an earlier configuration

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

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

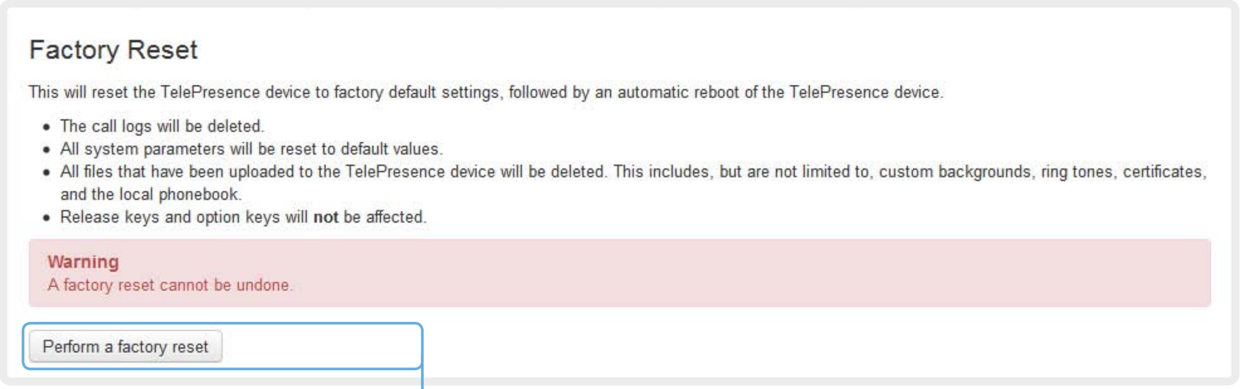
Factory reset

When performing a factory reset the call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the system will be deleted. Release keys and option keys will be preserved.

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

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

Navigate to: Maintenance > Factory Reset



Factory Reset

This will reset the TelePresence device to factory default settings, followed by an automatic reboot of the TelePresence device.

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the TelePresence device will be deleted. This includes, but are not limited to, custom backgrounds, ring tones, certificates, and the local phonebook.
- Release keys and option keys will **not** be affected.

Warning
A factory reset cannot be undone.

Perform a factory reset

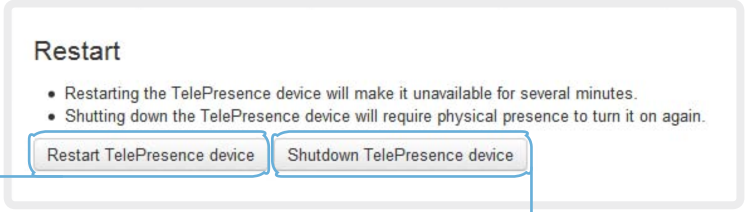
1. Read the provided information carefully before you restore the factory settings by clicking *Perform a factory reset*.
2. Click *Reset* to confirm your choice, or *Cancel* if you have changed your mind.

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

Restarting the system

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

Navigate to: Maintenance > Restart



Restart

- Restarting the TelePresence device will make it unavailable for several minutes.
- Shutting down the TelePresence device will require physical presence to turn it on again.

Restarting the system

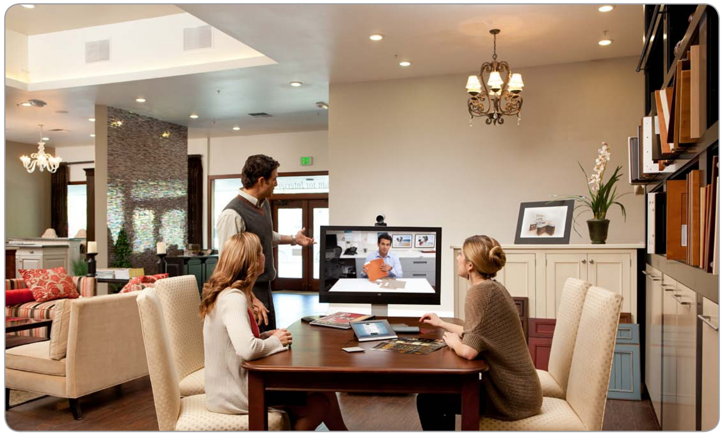
Click *Restart TelePresence device* to restart the system.

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.



Chapter 3

System settings

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.

ⓘ Tap *Settings (✖) > System Information* on the Touch controller to find the system's IP address (IPv4 or IPv6).

Audio settings

Audio InternalSpeaker Mode

Set the internal loudspeaker mode.

Requires user role: ADMIN

Value space: <Off/On>

Off: The internal speakers are disabled.

On: The internal speakers are enabled.

Example: `Audio InternalSpeaker Mode: On`

Audio Microphones Mute Enabled

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

Requires user role: ADMIN

Value space: <True/InCallOnly>

True: Muting of audio is always available.

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

Example: `Audio Microphones Mute Enabled: True`

Audio SoundsAndAlerts KeyTones Mode

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

Requires user role: USER

Value space: <Off/On>

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

On: You will hear key tones when you type.

Example: `Audio SoundsAndAlerts KeyTones Mode: Off`

Audio SoundsAndAlerts RingTone

Select the ring tone for incoming calls.

Requires user role: USER

Value space: <Marbles/IceCrystals/Polaris/Alert/Discreet/Fantasy/Jazz/Nordic/Echo/Rhythmic>

Range: Select a tone from the list of ring tones.

Example: `Audio SoundsAndAlerts RingTone: Jazz`

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 Volume

Adjust the speaker volume.

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`

Cameras settings

Cameras PowerLine Frequency

Applies to cameras supporting PowerLine frequency anti-flickering, i.e. PrecisionHD 1080p cameras.

Requires user role: ADMIN

Value space: <50Hz/60Hz>

50Hz: Set to 50 Hz.

60Hz: Set to 60 Hz.

Example: `Cameras PowerLine Frequency: 50Hz`

Cameras Camera [1..1] Backlight

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

Requires user role: ADMIN

Value space: <Off/On>

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Example: `Cameras Camera 1 Backlight: Off`

Cameras Camera [1..1] Brightness Mode

Set the camera brightness mode.

Requires user role: ADMIN

Value space: <Auto/Manual>

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

Manual: Enable manual control of the camera brightness. The brightness level is set using the Cameras Camera Brightness Level setting.

Example: `Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1..1] Brightness Level

Set the brightness level. NOTE: 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..1] Flip

Not applicable in this version.

Cameras Camera [1..1] Focus Mode

Set the camera focus mode.

Requires user role: ADMIN

Value space: <Auto/Manual>

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

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

Example: `Cameras Camera 1 Focus Mode: Auto`

Cameras Camera [1..1] FrameRate

Set the frame rate.

Requires user role: ADMIN

Value space: <60Hz/30Hz>

60Hz: Set the frame rate to 60 Hz.

30Hz: Set the frame rate to 30 Hz.

Example: `Cameras Camera 1 FrameRate: 30Hz`

Cameras Camera [1..1] Gamma Mode

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

Requires user role: ADMIN

Value space: <Auto/Manual>

Auto: Auto is the default and the recommended setting.

Manual: In severe light conditions, you may switch mode to manual and specify explicitly which gamma table to use by setting the Gamma Level.

Example: `Cameras Camera 1 Gamma Mode: Auto`

Cameras Camera [1..1] Gamma Level

By setting the Gamma Level you can select which gamma correction table to use. This setting may be useful in difficult lighting conditions, where changes to the brightness setting does not provide satisfactory results. NOTE: 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..1] IrSensor

Not applicable in this version.

Cameras Camera [1..1] Mirror

Not applicable in this version.

Cameras Camera [1..1] 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..1] Whitebalance Level

Set the whitebalance level. NOTE: 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`

Conference settings

Conference [1..1] TelephonyPrefix

Enter the prefix to be used for telephony calls.

Requires user role: ADMIN

Value space: <S: 0, 80>

Format: String with a maximum of 80 characters.

Example: `Conference 1 TelephonyPrefix: "520"`

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 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. NOTE: 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. NOTE: 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`

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 if there should be an alert on 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. The calls received while in Do Not Disturb mode will be shown as missed calls.

Timed: Select this option only if using the API to switch Do Not Disturb mode on and off.

Example: `Conference 1 DoNotDisturb Mode: Off`

Conference [1..1] DoNotDisturb DefaultTimeout

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

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.

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: <H323/Sip/H320>

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: 768`

Conference [1..1] MaxTransmitCallRate

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

Requires user role: ADMIN

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxTransmitCallRate: 6000`

Conference [1..1] MaxReceiveCallRate

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

Requires user role: ADMIN

Value space: <64..6000>

Range: Select a value between 64 and 6000 kbps.

Example: `Conference 1 MaxReceiveCallRate: 6000`

Conference [1..1] MaxTotalTransmitCallRate

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

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

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

Requires user role: ADMIN

Value space: <64..10000>

Range: Select a value between 64 and 10000.

Example: `Conference 1 MaxTotalTransmitCallRate: 9000`

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: 9000`

Conference [1..1] VideoBandwidth Mode

Set the conference video bandwidth mode.

Requires user role: ADMIN

Value space: <Dynamic/Static>

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

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

Example: `Conference 1 VideoBandwidth Mode: Dynamic`

Conference [1..1] VideoBandwidth MainChannel Weight

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

Requires user role: ADMIN

Value space: <1..10>

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth MainChannel Weight: 5`

Conference [1..1] VideoBandwidth PresentationChannel Weight

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

Requires user role: ADMIN

Value space: <1..10>

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth PresentationChannel Weight: 5`

Conference [1..1] PacketLossResilience Mode

Set the packetloss resilience mode. This configuration will only take effect for calls initiated after the configuration is set.

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable the packetloss resilience.

On: Enable the packetloss resilience.

Example: `Conference 1 PacketLossResilience Mode: On`

Conference [1..1] Presentation Policy

Control how the presentation service is to be performed.

Requires user role: ADMIN

Value space: <LocalRemote/LocalOnly>

LocalRemote: The presentation will be shown locally and sent to remote side.

LocalOnly: The presentation will only be shown locally.

Example: `Conference 1 Presentation Policy: LocalRemote`

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 multipoint video conferences. MultiWay requires that your video network includes an external Multipoint control unit (MCU), which let you set up conferences with many participants.

Requires user role: ADMIN

Value space: <Auto/Off/MultiWay>

Auto: Use MultiWay for multipoint conferences if the MultiWay service is available. If not, the multipoint mode is set to Off automatically.

Off: Multipoint conferences are not allowed.

MultiWay: Use MultiWay for multipoint conferences. The Multipoint Mode will be set to Off automatically if the MultiWay service is unavailable, for example when a server address is not specified in the NetworkServices MultiWay Address setting.

Example: `Conference 1 Multipoint Mode: Auto`

Conference [1..1] IncomingMultisiteCall Mode

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

Requires user role: ADMIN

Value space: <Allow/Deny>

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

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

Example: `Conference 1 IncomingMultisiteCall Mode: Allow`

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.

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

Set the name of 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, and its Name is used on the facility service call button.

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

Set the number 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.

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.

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`

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 "NAT Address" or the real IP-address should be used in signalling. This is done to make it possible to place calls to endpoints on the LAN as well as endpoints on the WAN.

Off: The system will signal the real IP Address.

On: The system will signal the configured "NAT Address" instead of its own 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".

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.

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

* Port 1720

* Port 5555-5574

* Port 2326-2485

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

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. NOTE: 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. NOTE: 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: ""`

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. NOTE: 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. NOTE: 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: Only the valid IP address format is accepted. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

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"`

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`

Network settings

Network [1..1] IPStack

Select which internet protocols the system will support.

NOTE: Restart the system after changing this setting.

Requires user role: ADMIN

Value space: <IPv4/IPv6>

IPv4: IP version 4 is used for the SIP and H323 calls.

IPv6: IP version 6 is used for the SIP and H323 calls.

Example: `Network 1 IPStack: IPv4`

Network [1..1] 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 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: Only the valid IPv4 address format is accepted.

Example: `Network 1 IPv4 Address: "192.0.2.0"`

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: Only the valid IPv4 address format is accepted.

Example: `Network 1 IPv4 Gateway: "192.0.2.0"`

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: Only the valid IPv4 address format is accepted.

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 RFC3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC4862 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`

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: Only the valid IPv6 address format is accepted.

Example: `Network 1 IPv6 Address: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"`

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: Only the valid IPv6 address format is accepted.

Example: `Network 1 IPv6 Gateway: "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff"`

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] 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: String with a maximum of 64 characters.

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

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

Note: 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

Note: 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

Note: 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`

Network [1..1] QoS Diffserv Signalling

Note: 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

Note: 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

Note: 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`

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 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: `xConfiguration 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.

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`

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 RFC5216, 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.

NOTE: If running older software versions than TC6.0, restart the system for any change to this setting to take effect.

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`

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: Off`

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`

NetworkServices settings

NetworkServices XMLAPI Mode

Not applicable in this version.

NetworkServices MultiWay Address

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

Multiway™ can be used in the following situations:

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

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

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

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: String with a maximum of 255 characters.

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 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.

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

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 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.

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

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`

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: String with a maximum of 64 characters.

Example: `NetworkServices NTP Address: "1.ntp.tandberg.com"`

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 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: String with a maximum of 64 characters.

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"`

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 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 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: Mulitparty conferencing via CTMS is prohibited.

On: Mulitparty 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`

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"
```

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>

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 called 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.

Example: `Provisioning Mode: TMS`

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`

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 IP address format or DNS name; a compact string with a maximum of 64 characters.

Example: `Provisioning ExternalManager Address: ""`

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"`

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`

Security settings

Security Audit Logging Mode

Determine where to record or transmit the audit logs. When using the External or ExternalSecure modes, you also must enter the address and port number for the audit server in the Security Audit Server Address and Security Audit Server Port settings.

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

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 audit server (syslog server). The audit server must support TCP.

ExternalSecure: The system sends encrypted audit logs to an external audit server (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 audit server.

Example: `Security Audit Logging Mode: Off`

Security Audit Server Address

Enter the IP-address of the audit 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.

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

Requires user role: AUDIT

Value space: <S: 0, 64>

Format: Valid IPv4 or IPv6 address formats.

Example: `Security Audit Server Address: ""`

Security Audit Server Port

Enter the port of the audit server that the system shall send its audit logs to. The default port is 514. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

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

Requires user role: AUDIT

Value space: <0..65535>

Range: Select a value from 0 to 65535.

Example: `Security Audit Server Port: 514`

Security Audit OnError Action

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

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

Requires user role: AUDIT

Value space: <Halt/Ignore>

Halt: If a halt condition is detected the system 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 audit server. Halt conditions are: A network breach (no physical link), no audit server running (or wrong audit server address or port), 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 audit server.

Example: `Security Audit OnError Action: Ignore`

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`

SerialPort settings

SerialPort Mode

Enable/disable the serial 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`

SIP settings

SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off the endpoint must be registered with a SIP registrar to be reachable.

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 Profile [1..1] URI

The SIP URI or number is used to address the system. This is the URI that is registered and used by the SIP services to route inbound calls to the system. A Uniform Resource Identifier (URI) is a compact string of characters used to identify or name a resource.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters.

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.

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`

SIP Profile [1..1] Outbound

The client initiated connections mechanism for firewall traversal, connection reuse and redundancy. The current version supports http://tools.ietf.org/html/draft-ietf-sip-outbound-20.

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 Outbound is enabled, multiple proxies can be addressed.

Requires user role: ADMIN

Value space: <S: 0, 255>

Format: Compact string with a maximum of 255 characters. An IP address that contains letters (192.a.2.0) or unvalid IP addresses (192.0.1234.0) will be rejected.

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.

Requires user role: ADMIN

Value space: <Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel>

Standard: To be used when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)

Alcatel: To be used when registering to Alcatel-Lucent OmniPCX Enterprise. NOTE: This mode is not fully supported.

Avaya: To be used when registering to Avaya Communication Manager. NOTE: This mode is not fully supported.

Cisco: To be used when registering to Cisco Unified Communication Manager.

Microsoft: To be used when registering to Microsoft LCS or OCS. NOTE: This mode is not fully supported.

Nortel: To be used when registering to Nortel MCS 5100 or MCS 5200 PBX. NOTE: This mode is not fully supported.

Example: `SIP Profile 1 Type: Standard`

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. NOTE: 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. NOTE: 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`

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 on the Touch controller.

Requires user role: USER

Value space: <English/ChineseSimplified/Danish/Dutch/Finnish/French/German/Italian/Japanese/Korean/Norwegian/Portuguese-Brazilian/Russian/Spanish/Swedish>

Example: `SystemUnit MenuLanguage: English`

SystemUnit ContactInfo Type

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

Requires user role: ADMIN

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

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

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

IPv4: Show the IPv4 address as contact information.

IPv6: Show the IPv6 address as contact information.

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

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

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

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

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

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

Example: `SystemUnit ContactInfo Type: Auto`

SystemUnit CallLogging Mode

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

Requires user role: ADMIN

Value space: <Off/On>

Off: Disable logging.

On: Enable logging.

Example: `SystemUnit CallLogging Mode: On`

SystemUnit IrSensor

Not fully supported in this software version. Do not change this setting; it is included only for testing.

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)/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+03:00 (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 (Irkutsk, Ulaan Bataar)/GMT+09:00 (Osaka, Sapporo, Tokyo)/GMT+09:00 (Seoul)/GMT+09:00 (Yakutsk)/GMT+09:30 (Darwin)/GMT+09:30 (Adelaide)/GMT+10:00 (Guam, Port Moresby)/GMT+10:00 (Brisbane)/GMT+10:00 (Vladivostok)/GMT+10:00 (Hobart)/GMT+10:00 (Canberra, Melbourne, Sydney)/GMT+11:00 (Magadan, Solomon Is., New Caledonia)/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`

UserInterface settings

UserInterface TouchPanel DefaultPanel

Select whether to display the list of contacts, the list of scheduled meetings, or a dial pad on the Touch controller as default.

Requires user role: USER

Value space: <ContactList/MeetingList/Dialpad>

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

Example: `UserInterface TouchPanel DefaultPanel: ContactList`

Video settings

Video Input Source [1..2] 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: <DVI>

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

Example: `Video Input Source 1 Connector: DVI`

Video Input Source [2] Connector

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

Requires user role: ADMIN

Value space: <CAMERA>

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

Example: `Video Input Source 2 Connector: CAMERA`

Video Input Source [1..2] 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..2] PresentationSelection

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.

This setting is used to define whether to display the presentation source on the local video system's display automatically or not. To share the presentation with the far end always requires additional action (tap Start Presenting on the Touch controller).

Default values: source 1 = Automatic, source 2 (camera) = Hidden

Requires user role: ADMIN

Value space: <Manual/Automatic/Hidden>

Manual: The content on the input source will not be presented on the local video system's display before you select it. Use the Touch controller to choose which input source to present.

Automatic: Any content on the input source will be presented on the local video system's display automatically. If there is active content on more than one input source (which is set to Automatic) the most recent one will be used.

Hidden: The input source is not expected to be used as a presentation source.

Example: `Video Input Source 1 PresentationSelection: Automatic`

Video Input Source [1..2] CameraControl Mode

Indicates whether or not camera control is enabled for the selected video input source when the video input is active. In this product this value is fixed for all input sources.

Value space: <Off/On>

Off: Disable camera control.

On: Enable camera control.

Video Input Source [1..2] CameraControl CameraId

Indicates the ID of the camera. This value is fixed in this product.

Value space: <1>

Range: Indicates the ID of the camera.

Video Input Source [1..2] 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.

In order to allow a transmit frame rate of 60 fps, you must enable 60 Hz capture frequency on the camera with the Cameras Camera 1 FrameRate setting.

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

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 2 OptimalDefinition Profile: Normal`

Video Input Source [1..2] OptimalDefinition Threshold60fps

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

In order to allow a transmit frame rate of 60 fps, you must enable 60 Hz capture frequency on the camera with the Cameras Camera 1 FrameRate setting.

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 2 OptimalDefinition Threshold60fps: 1280_720`

Video Input Source [1..2] Quality

When encoding and transmitting video there will be a trade-off between high resolution and high framerate. For some video sources it is more important to transmit high framerate 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 framerate. 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 2 Quality: Motion`

Video MainVideoSource

Define which video input source shall be used as the main video source. The video input source is configured with the "Video Input Source [1..n] Connector" setting.

Requires user role: USER

Value space: <1/2>

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

Example: `Video MainVideoSource: 2`

Video DefaultPresentationSource

Not applicable in this version.

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

Video Input DVI [1] RGBQuantizationRange

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 1 RGBQuantizationRange: Full`

Video Input DVI [1] Type

The official DVI standard supports both digital and analog signals. In most cases the default AutoDetect setting can detect whether the signal is analog RGB or digital. However, in some rare cases when DVI-I cables are used (these cables can carry both the analog and digital signals) the auto detection fails. This setting makes it possible to override the AutoDetect and select the correct DVI video input.

Requires user role: ADMIN

Value space: <AutoDetect/Digital/AnalogRGB/AnalogYPbPr>

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.

Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.

AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Example: `Video Input DVI 1 Type: AutoDetect`

Video ControlPanel Brightness

Set the brightness level for the Touch controller.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100.

Example: `Video ControlPanel Brightness: 100`

Video Layout Scaling

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

Requires user role: ADMIN

Value space: <Off/On>

Off: No adjustment of the aspect ratio.

On: Let the system automatically adjust aspect ratio.

Example: `Video Layout Scaling: On`

Video Layout ScaleToFrame

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

Requires user role: ADMIN

Value space: <Manual/MaintainAspectRatio/StretchToFit>

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

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

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

Example: `Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

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

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

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 as from TC6.0.

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 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 Selfview FullscreenMode settings respectively.

This setting obsoletes the Video Selfview setting as from TC6.0.

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`

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 role set for the output in the Video Output Internal MonitorRole setting.

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 LCD/Internal MonitorRole set to First.

Second: The self view picture will be shown on outputs with the Video Output LCD/Internal 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 PIP ActiveSpeaker DefaultValue Position

Determine the position on screen of the active speaker picture-in-picture (PiP). The setting only takes effect when using a video layout where the active speaker is a PiP, i.e. the Overlay layout, or possibly a Custom layout (see the Video Layout LocalLayoutFamily setting). The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN

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

Current: The position of the active speaker PiP will be kept unchanged when leaving a call.

UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.

UpperCenter: The active speaker PiP will appear in the upper center position.

UpperRight: The active speaker PiP will appear in the upper right corner of the screen.

CenterLeft: The active speaker PiP will appear in the center left position.

CentreRight: The active speaker PiP will appear in the center right position.

LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.

LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

Example: `Video PIP ActiveSpeaker DefaultValue Position: Current`

Video PIP Presentation DefaultValue Position

Determine the position on screen of the presentation picture-in-picture (PiP). The setting only takes effect when the presentation is explicitly minimized to a PiP, for example using the Touch controller. The setting takes effect from the next call onwards; if changed during a call, it will have no effect on the current call.

Requires user role: ADMIN

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

Current: The position of the presentation PiP will be kept unchanged when leaving a call.

UpperLeft: The presentation PiP will appear in the upper left corner of the screen.

UpperCenter: The presentation PiP will appear in the upper center position.

UpperRight: The presentation PiP will appear in the upper right corner of the screen.

CenterLeft: The presentation PiP will appear in the center left position.

CentreRight: The presentation PiP will appear in the center right position.

LowerLeft: The presentation PiP will appear in the lower left corner of the screen.

LowerRight: The presentation PiP will appear in the lower right corner of the screen.

Example: `Video PIP Presentation DefaultValue Position: Current`

Video Layout LocalLayoutFamily

Select which video layout family to use locally.

Requires user role: ADMIN

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

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

FullScreen: 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.

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 RemoteLayoutFamily

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

Requires user role: ADMIN

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

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

FullScreen: 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. It is recommended not to use this value 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 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: This value is not supported.

DualPresentationOnly: This value is not supported.

Example: `Video Monitors: Single`

Video OSD Mode

Not applicable in this version.

Video OSD MenuStartupMode

Not applicable in this version.

Video OSD VirtualKeyboard

Not applicable in this version.

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

Not applicable in this version.

Video OSD AutoSelectPresentationSource

Not applicable in this version.

Video OSD TodaysBookings

Not applicable in this version.

Video OSD MyContactsExpanded

Not applicable in this version.

Video OSD Output

Not applicable in this version.

Video OSD InputMethod InputLanguage

Not applicable in this version.

Video OSD InputMethod Cyrillic

Not applicable in this version.

Video OSD LoginRequired

Not applicable in this version.

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 Touch controller.

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 Output LCD [1] Resolution

Set the screen resolution.

Requires user role: ADMIN

Value space: <1920_1080_60>

Range: The screen resolution is 1920 x 1080 60 Hz.

Example: `Video Output LCD 1 Resolution: 1920_1080_60`

Video Output LCD [1] MonitorRole

Set the LCD monitor role.

Set the LCD monitor role. Do not change this setting manually; keep the default setting.

Value space: <InternalSetup>

InternalSetup: The internal setup as defined by the Touch controller will be used.

Video Output LCD [1] Brightness

Set the brightness level for the monitor.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Brightness: 50`

Video Output LCD [1] Red

Set the Red color level for the monitor.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Red: 50`

Video Output LCD [1] Green

Set the Green color level for the monitor.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Green: 50`

Video Output LCD [1] Blue

Set the Blue color level for the monitor.

Requires user role: ADMIN

Value space: <0..100>

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Blue: 50`

Video Output Internal [2] MonitorRole

Determine the role of the internal monitor and select where to show the video stream and presentation. Do not change this setting manually; keep the default setting.

Value space: <First>

First: Show the main video stream and presentation on the internal monitor.

Video WallPaper

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

Requires user role: USER

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

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 maximum supported resolution is 1920x1200.

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

Example: `Video Wallpaper: Summersky`

Experimental settings

The Experimental settings are for testing only and should not be used unless agreed with Cisco. These settings are not documented and WILL change in later releases.

Chapter 4

Setting passwords

Setting the system password

You need to sign in to be able to use the web interface of your system.

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.

⚠ **We strongly recommend that you set a password for the admin user, and to any other user with similar credentials, to restrict access to system configuration.**

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.

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*.

Setting the menu password

When starting up the video conference system for the first time anyone can access the Administrator Settings menu with the Touch controller 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.**

You should use the web interface to set the menu password; the Touch controller cannot be used.

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.

ⓘ To find the system's IP address tap *Settings (✖) > System Information* on the Touch controller.

Appendices

Cisco VCS provisioning

When using Cisco VCS (Video Communication Server) provisioning, a template containing all the settings that can be provisioned must be uploaded to Cisco TMS (TelePresence Management System). This is called the *Cisco TMS provisioning configuration template*.

All the system settings for your video system are included in this template. All settings except *SystemUnit Name* and *SIP Profile [1..1] URI* can be automatically provisioned to the video system.

The settings are described in the ► System settings chapter in this guide. Examples showing either the default value or an example value are included.

Downloading the provisioning configuration template

You can download the templates here:

► http://www.cisco.com/en/US/products/ps11776/prod_release_notes_list.html

For each software release there is one provisioning configuration template for every video system model. Take care to download 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.

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

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 System Configuration (on the web interface):

- Navigate to *Conference 1 > PacketLossResilience > Mode*

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

Factory resetting

If you have to reset your video system to its default factory settings, we recommend that you use either the Touch controller or the web interface. If neither of these methods are available, you can use the video system's reset button.

When factory resetting the video system the following happens:

- 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 local phone book.
- Release keys and option keys will **not** be affected.
- The system restarts automatically after the reset.

⚠ It is not possible to undo a factory reset.

If you want to backup your current configuration before you factory reset the unit, open a web browser and follow these steps:

- Enter the IP address of the video system in the address bar and sign in.
- Navigate to *Maintenance > Backup and Restore*.
- Click *Take backup* and follow the instructions to save the file on your computer.

Touch

1. Tap gently on the Touch screen if the unit is in sleep mode.
2. Navigate to *Settings (🛠) > Administrator Settings > Reset.*
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.

Web

ⓘ Tap *Settings (🛠) > System Information* on the Touch controller 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 > Factory Reset*.
3. Read the provided information carefully before you click *Perform a factory reset*.
4. If you are sure you want to perform a factory reset, click the red *Reset* button.

   The system reverts to the default factory settings and restarts automatically. This will take a few minutes.

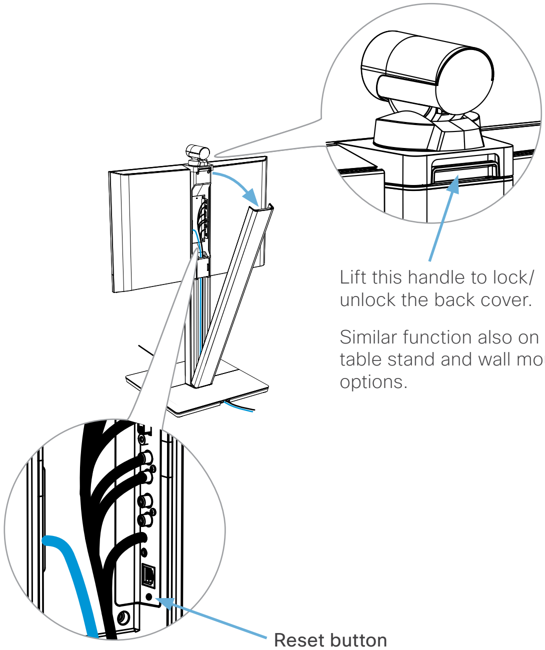
   The system confirms the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.

Reset button

1. Remove the video system's back cover.
2. Use the tip of a pen (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.

   The system reverts to the default factory settings and restarts automatically. This will take a few minutes.

   The system confirms the factory reset by displaying a notification on the main screen when up and running again. The notification disappears after approximately 10 seconds.



Lift this handle to lock/ unlock the back cover.

Similar function also on table stand and wall mount options.

Reset button

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

Factory resetting the Touch 8” controller

You must use the New message indicator and Mute buttons to reset the Touch 8” controller to its default factory settings.

When factory resetting the Touch controller the logs will be cleared, and the configuration and pairing information are lost.

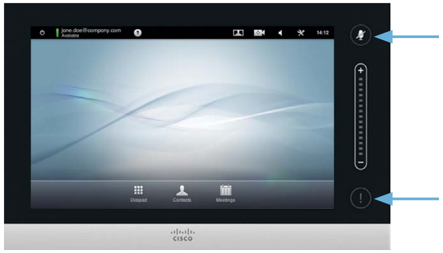
The Touch controller restarts after the reset and receives a new configuration automatically from the video system.

⚠ It is not possible to undo a factory reset.

Touch

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.

Technical specification for MX300/MX200

PRODUCT SPECIFICATION

Product compatibility

Fully compatible with standards-compliant telepresence and video systems

Software compatibility

MX200: Cisco TelePresence Software Version TC4.2 or later

MX300: Cisco TelePresence Software Version TC5.0 or later

Components

Fully integrated unit including:

- Codec
- Display
- Camera
- Integrated microphone and loudspeakers

Cisco TelePresence Table Mic 20 microphone (MX200 comes standard with one microphone; MX300 comes standard with two microphones)

Cables: VGA-to-DVI-I cable, 3.5 mm jack audio cable, LAN cable, and power cable

Display

- LCD monitor:
  42” (MX200), 55” (MX300)
- Resolution: 1920 x 1200 (16:9)
- Contrast ratio: 2500:1
- Viewing angle: 178°
- Response time:
  8 ms (MX200), 10 ms (MX300)
- Brightness: 550 cd/m^2

PC and second-source video input

DVI-I

Supported PC input resolutions

SVGA (800 x 600) to 1080p (1920 x 1080)

Camera

- PrecisionHD camera: 1080p 4x zoom
- Resolutions: 1080p30 and 720p60
- Auto-focus
- Wide-angle 72-degree horizontal field of view
- 4x optical zoom
- Pan +/–100 degrees
- Tilt +/–25 degrees

Audio system

- Integrated full-range speaker and woofer
- Integrated full-range microphone
- Bluetooth-ready
- Support for two Cisco TelePresence Table Mic 20 microphones
- RCA PC audio input
- RCA audio output

User interface

Cisco TelePresence Touch

- Eight-inch projected capacitive touch screen
- Resolution: 800 x 480

Language support

- Danish
- English
- Finnish
- French
- German
- Japanese
- Russian
- Simplified Chinese
- Spanish
- Swedish

Physical dimensions

MX200 with floor stand:
Height: 1429 mm / 56.3 in.
Width: 1026 mm / 40.4 in.
Depth: 602 mm / 23.7 in.
Weight: 40.2 kg / 89 lb

MX200 with table stand:
Height: 781 mm / 30.7 in.
Width: 1026 mm / 40.4 in.
Depth: 259 mm /10.2 in.
Weight: 31.5 kg / 69 lb

MX200 with wall mount:
Height: 757 mm / 29.8 in.
Width: 1026 mm / 40.4 in.
Depth: 169 mm / 6.7 in.
Weight: 30 kg / 66 lb

MX300 with floor stand:
Height: 1523 mm / 60.0 in.
Width: 1280 mm / 50.4 in.
Depth: 671 mm / 26.4 in.
Weight: 51.3 kg / 113 lb

MX300 with wall mount:
Height: 942 mm / 37.1 in.
Width: 1280 mm / 50.4 in.
Depth: 217 mm / 8.5 in.
Weight: 34.4 kg / 76 lb

Power

- Autosensing power supply
- 100–240 VAC, 50/60 Hz
- 250 W maximum

Temperature range

Operating temperature and humidity:

- Ambient temperature: 32 to 95°F (0 to 35°C)
- Relative humidity (RH): 10 to 90%
- Storage and transport temperature at RH 10–90% (noncondensing): –4 to 140°F (–20 to 60°C)

Approvals and compliance

EU/EEC

- Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN 60950-1
- Directive 2004/108/EC (EMC Directive)
  - Standard EN 55022, Class A
  - Standard EN 55024
  - Standard EN 61000-3-2/-3-3

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

VIDEO AND AUDIO SPECIFICATIONS

Bandwidth

- H.323 and SIP up to 6 Mbps point-to-point

Video standards

- H.261
- H.263
- H.263+
- H.264

Video features

- Widescreen: 16:9
- Advanced screen layouts
- Intelligent video management
- Local auto-layout

Live video resolutions (encode/decode)

- 176 x 144 @ 30 fps (QCIF)
- 352 x 288 @ 30 fps (CIF)
- 512 x 288 @ 30 fps (w288p)
- 576 x 448 @ 30 fps (448p)
- 768 x 448 @ 30 fps (w448p)
- 704 x 576 @ 30 fps (4CIF)
- 1024 x 576 @ 30 fps (w576p)
- 640 x 480 @ 30 fps (VGA)
- 800 x 600 @ 30 fps (SVGA)
- 1024 x 768 @ 30 fps (XGA)
- 1280 x 1024 @ 30 fps (SXGA)
- 1280 x 720 @ 30 fps (720p30)
- 1280 x 768 @ 30 fps (WXGA)
- 1920 x 1080 @ 30 fps (1080p30)*
- 1440 x 900 @ 30 fps (WXGA+)*
- 1680 x 1050 @ 30 fps (WSXGA+)*
- 1600 x 1200 @ 30 fps (UXGA)*
- 512 x 288 @ 60 fps (w288p60)*
- 768 x 448 @ 60 fps (w448p60)*
- 1024 x 576 @ 60 fps (w576p60)*
- 1280 x 720 @ 60 fps (720p60)

* Requires premium resolution option

Audio standards

- G.711
- G.722
- G.722.1
- 64/128 kbps MPEG-4 AAC-LD
- AAC-LD stereo

Audio features

- CD-quality 20 kHz stereo
- Acoustic echo canceling
- Automatic gain control
- Automatic noise reduction
- Active lip synchronization

Dual stream

- H.239 (H.323) dual stream
- BFCP (SIP) dual stream
- Support for resolutions up to 720p30 in both main stream and dual stream simultaneously

NETWORK, SECURITY AND MANAGEMENT SPECIFICATIONS

Protocols

- H.323
- SIP

Network interfaces

- One LAN or Ethernet (RJ-45) 10/100/1000 Mbps for LAN

Other interfaces

- Bluetooth for future applications
- RJ-45 for maintenance

IP network features

- Domain Name System (DNS) lookup for service configuration
- Differentiated Services (quality of service (QoS))
- IP adaptive bandwidth management (including flow control)
- Auto-gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 dual-tone multifrequency (DTMF) tones in H.323
- Date and time support with Network Time Protocol (NTP)
- Packet loss based downspeeding
- DNS based URI dialing
- TCP/IP
- Dynamic Host Configuration Protocol (DHCP)
- IEEE 802.1x network authentication
- IEEE 802.1q VLAN
- IEEE 802.1p QoS and class of service

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)

Firewall traversal

- Cisco TelePresence Expressway technology
- H.460.18 and H.460.19 firewall traversal

Embedded encryption

- H.323 and SIP point-to-point
- Standards-based: H.235v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Support in dual stream

Security features

- Management through Secure HTTP (HTTPS) and Secure Shell (SSH) Protocol
- IP administration password
- Menu administration password
- Disable IP services
- Network settings protection

Multipoint support

- 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)

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

System management

- Support for the Cisco TelePresence Management Suite (Cisco TMS)
- Total management through embedded Simple Network Management Protocol (SNMP), Telnet, SSH, XML, and Simple Object Access Protocol (SOAP)
- Remote software upload: Through web server, Secure Copy Protocol, HTTP, and HTTPS

Directory services

- Support for local directories (My Contacts)
- Corporate directory
- Unlimited entries using server directory supporting
- Lightweight Directory Access Protocol (LDAP) and H.350
- Unlimited number for corporate directory (available with Cisco TelePresence Management Suite)
- Local directory: 200 numbers
- Received calls with date and time
- Placed calls with date and time
- Missed calls with date and time

All specifications are subject to change without notice, system specifics may vary.

All images in these materials are for representational purposes only, actual products may differ.

February 2012

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 1889 RTP: A Transport Protocol for Real-time Applications
- 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 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 4145 TCP-Based Media Transport in the SDP
- 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 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 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification
- RFC 6184 RTP Payload Format for H.264 Video

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. For the MX Series, this is the path you have to follow:

TelePresence >
TelePresence Endpoints - Multipurpose >
Cisco TelePresence MX Series

Alternatively, you can use the following short-link to find the documentation for the MX Series:

- ► http://www.cisco.com/go/mx-docs

The documents are organized in the following categories:

Installation guides:

Install and Upgrade > Install and Upgrade Guides

Getting started guide:

Install and Upgrade > Install and Upgrade Guides
Maintain and Operate > Maintain and Operate Guides

Administrator guides:

Maintain and Operate > Maintain and Operate Guides

User guides and Quick reference guides:

Maintain and Operate > End-User Guides

Knowledge base articles and frequently asked questions:

Troubleshoot and Alerts > Troubleshooting Guides

CAD drawings:

Reference Guides > Technical References

Video conferencing room guidelines:

Design > Design Guides

Software licensing information:

Software Downloads, Release and General Information > Licensing Information

Regulatory compliance and safety information:

Install and Upgrade > Install and Upgrade Guides

Software release notes:

Software Downloads, Release and General Information > Release Notes

Intellectual property rights

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