

Software version TE6.0  
NOVEMBER 2012

## ADMINISTRATOR GUIDE

CISCO TELEPRESENCE SYSTEMS  
EX60 AND EX90



Thank you for choosing Cisco!

Your Cisco TelePresence System EX90/EX60 has been designed to give you many years of safe, reliable operation.

This part of the EX90/EX60 documentation is aimed at administrators working with the setup of the system.

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

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

The user documentation can be found on our web site. Go to:

► <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

<b>Introduction.....</b>	<b>3</b>	<b>Advanced settings.....</b>	<b>34</b>
What's new in this version .....	5	Overview of the advanced settings .....	35
EX90 system overview.....	8	Audio settings .....	37
EX60 system overview.....	9	Cameras settings.....	39
User interfaces.....	10	Conference settings .....	41
How to use the Touch controller.....	11	FacilityService settings .....	44
How to use the web interface .....	12	Network settings.....	45
<b>Using the web interface.....</b>	<b>13</b>	NetworkServices settings.....	51
Starting the web interface .....	14	Phonebook settings .....	54
Changing the system/codec password .....	15	Provisioning settings .....	55
The interactive menu .....	16	RTP settings.....	57
The system information page .....	17	SIP settings .....	58
Log files .....	18	Standby settings .....	61
XML files .....	19	SystemUnit settings .....	62
Advanced configuration.....	20	Time settings .....	63
Choosing a wallpaper .....	21	UserInterface settings.....	64
Sign in banner .....	22	Video settings.....	65
Placing a call .....	23	Experimental settings .....	71
Controlling and monitoring a call .....	24	<b>Setting passwords.....</b>	<b>72</b>
Local layout control.....	25	Setting the system password .....	73
Capturing snapshots.....	26	Setting the menu password.....	74
Adding option keys .....	28	<b>Appendices.....</b>	<b>75</b>
Certificate management .....	29	Audio outputs and microphones.....	76
User administration .....	30	Optimal definition profiles .....	77
Restarting the system.....	32	ClearPath – Packet loss resilience .....	78
Factory reset.....	33	EX90 dimensions .....	79
		EX60 dimensions – wall mounting and arm mounting .....	80
		Factory reset.....	81
		Technical specifications.....	82
		Supported RFCs .....	85
		User documentation on the Cisco web site.....	86
		<b>Cisco contacts .....</b>	<b>87</b>

## CHAPTER 1

# INTRODUCTION



This document provides you with the information required to administer your product.

How to install the product is described in the *Installation guides*. The initial configurations required to get the system up and running on the Cisco Unified Communications Manager (CUCM) is described in the *Getting Started with TE6.0 and CUCM 9.0* guide.

#### Products covered in this guide

- Cisco TelePresence System EX60
- Cisco TelePresence System EX90

## User documentation

The user documentation for the Cisco TelePresence EX series includes several guides suitable for various user groups:

- Installation guides
- Getting started guide (not for TE6.0)
- Administering endpoints on CUCM (not for TE6.0)
- Getting Started with TE6.0 and CUCM 9.0 (TE6.0 only)
- Administrator guide
- Quick reference guides
- User guides
- Knowledge base articles
- Video conference room primer
- Video conference room acoustics guidelines
- 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/ex-docs>

Guidance how to find the documents 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>



## What's new in this version

This section provides an overview of the new features in the TE6.0 software version.



The TE6.0 software version only applies to EX Series endpoints *registered on a Cisco Unified Communications Manager (CUCM)*.

TE6.0 does not support all non-CUCM features from earlier TC software releases. Full non-CUCM feature parity with TC software will be introduced in TC6.0 and beyond.

### Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (TE6). Go to:

► [http://www.cisco.com/en/US/products/ps11327/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11327/tsd_products_support_series_home.html)

### Software download

For software download go to:

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

A new release key is *not* required in order to upgrade from software version TC5.x to TE6.0.

### New features and improvements

#### 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 TE6.0 this feature is extended to also include secure (encrypted) connections. The encryption indicator is shown on the Touch user interface during a call.

This feature requires that security mode is installed and configured on CUCM. Read the *Getting Started with TE6.0 and CUCM 9.0* guide to find how to set up this feature.

#### Voice mail support and message waiting indication

Endpoints registered to a Cisco Unified Communications Manager (CUCM) can be assigned a voice mail profile. When receiving a *Busy* or *No Answer* signal from such an endpoint, the call is forwarded to voice mail.

A message waiting notification appears on the Touch controller. By tapping the Messages icon a call is placed directly to the voice mail and you can retrieve your messages.

#### Shared lines support

When registered to a Cisco Unified Communications Manager (CUCM) the endpoint may be part of a shared line. This means that several devices in the same partition share the same directory number. The different devices sharing the same number receive status from the other appearances on the line.

For example, you can set up a shared line so that many devices share the same number and the first available operator picks up the call (help desk). Assisted call handling, where an administrator manages the calls (forward, barge) for an executive is another example. Also multiple devices belonging to one person can share the same line, thus allowing him/her to pick up a call on one device and resume it on another (single number reach).

You can find information about how to set up shared lines in the CUCM user documentation (Cisco Unified Communications Manager System Guide).

#### Ad-hoc conferencing in CUCM

Endpoints registered on Cisco Unified Communications Manager (CUCM) version 8.6.2 or later can use the Touch panel to invoke an ad-hoc conference. This requires that a conference bridge is added as an MCU on CUCM. Any endpoint can participate in the conference, regardless of where they are registered.

When configured, CUCM ad-hoc conferencing will be dominant over embedded MultiSite. If the number of participants drops to two, the conference will de-escalate to a point to point call.

#### Support for call forwarding (Call Forward All)

Call forwarding diverts calls to a specified number. When Call Forward All is activated, all incoming calls are diverted.

The target destination for diverted calls can be set from the Touch controller, or provisioned by the Cisco Unified Communications Manager (CUCM).

You can find information about call forwarding in the CUCM user documentation (Cisco Unified Communications Manager System Guide).

#### 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.

#### Audio-driven microphone mute indication

When in a call, you will be notified if you start speaking while your microphone is muted. The notification – *Your microphone is muted* – will be displayed on the main display.

### Bluetooth headset support

The Bluetooth version 2.1 headset profile is supported. The following functions are included: answer, volume up, volume down and hang up. A Bluetooth headset icon appears in the audio selector on the Touch controller when a headset is paired with the video system. Only one headset can be paired at a time.

### Support for Medianet

- **The Mediatrace diagnostics tool**

Mediatrace is a software feature that discovers the routers and switches (layer 2 and 3 devices) along the path of an IP flow. It is a diagnostic tool that 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.

- **Metadata**

The Metadata component allows applications to convey information to the network, for example by marking the video traffic traversing the network. The metadata adds information to the flow. Network managers use this information to prioritize and allocate bandwidth efficiently.

### CTI/JTAPI support (remote expert solution support)

A Cisco Unified Communications Manager (CUCM) exposes call control of endpoints via a Java Telephony API (JTAPI). For the EX Series Cisco's JTAPI enables custom applications to monitor device availability and control calls remotely. The following features are supported: call, answer, disconnect, hold, resume, blind transfer, consultative transfer and consultative conference.

Endpoints registered to a Cisco Unified Communications Manager (CUCM) 9.0 or later support the Cisco Remote Expert Smart Solution (version 1.8).

### Refined Touch user interface

- New home menu and call scene for easier call control
- New layout control
- Missed calls and message waiting indicators
- Tabbed view for calls on hold and improved call transfer handling
- Swipe feature to second view of conference participant list
- New dial pad, soft keyboard and improved text selector
- Encryption and call duration indicators

Also see the illustration below.

### New languages supported on Touch

- Dutch
- Italian
- Korean
- Portuguese-Brazilian



## New settings

- Conference [1..1] BFCP Mode
- NetworkServices CTMS Mode
- SIP Profile [1..1] Mailbox
- SIP Profile [1..1] Line
- SIP ListenPort
- SystemUnit Bluetooth Mode
- UserInterface TouchPanel DomainAutocomplete
- Video Input HDMI [1] RGBQuantizationRange (only EX90)
- Video Input DVI [n] RGBQuantizationRange

## Settings that are removed

- Audio Microphones Mute Enabled
- Cameras Camera [1..1] Mirror
- Cameras Camera [1..1] Flip
- Cameras Camera [1..1] IrSensor
- Conference [1..1] IncomingMultisiteCall Mode
- Conference [1..1] FarEndControl SignalCapability
- Conference [1..1] VideoBandwidth Mode
- Conference [1..1] VideoBandwidth MainChannel Weight
- Conference [1..1] VideoBandwidth PresentationChannel Weight
- Conference [1..1] Presentation Policy
- Conference [1..1] Multipoint Mode
- H323 NAT Address
- H323 NAT Mode
- H323 Profile [1..1] Authentication LoginName
- H323 Profile [1..1] Authentication Mode
- H323 Profile [1..1] Authentication Password
- H323 Profile [1..1] CallSetup Mode
- H323 Profile [1..1] Gatekeeper Address
- H323 Profile [1..1] Gatekeeper Discovery
- H323 Profile [1..1] H323Alias E164
- H323 Profile [1..1] H323Alias ID
- H323 Profile [1..1] PortAllocation

- Network [1..1] RemoteAccess Allow
- NetworkServices H323 Mode
- NetworkServices MultiWay Mode
- NetworkServices MultiWay Address
- NetworkServices MultiWay Protocol
- NetworkServices SSH AllowPublicKey
- NetworkServices HTTPS OCSP URL
- NetworkServices HTTPS OCSP Mode
- Security Audit Server Address
- Security Audit Server Port
- Security Audit OnError Action
- Security Audit Logging Mode
- Security Session ShowLastLogon
- Security Session InactivityTimeout
- SerialPort Mode
- SerialPort BaudRate
- SerialPort LoginRequired
- Standby Control
- Standby WakeupAction
- Standby BootAction
- Standby StandbyAction
- Video Layout Scaling
- Video Layout ScaleToFrame
- Video Layout ScaleToFrameThreshold
- Video Layout LocalLayoutFamily
- Video Layout RemoteLayoutFamily
- Video OSD MyContactsExpanded
- Video OSD LoginRequired
- Video OSD Mode
- Video OSD AutoSelectPresentationSource
- Video OSD TodaysBookings
- Video OSD Output
- Video OSD InputMethod InputLanguage
- Video OSD InputMethod Cyrillic
- Video Monitors

## Settings that are modified

- Audio Volume  
Renamed to Audio Volume Speaker
- Audio VolumeHandset  
Renamed to Audio Volume Handset
- Audio VolumeHeadset  
Renamed to Audio Volume Headset
- Conference [1..1] DefaultCallProtocol  
**OLD:** <H323/Sip>  
**NEW:** <Sip>
- Network [1..1] IPv6 Assignment  
**OLD:** <Static/Autoconf>  
**NEW:** <Static/DHCPv6/Autoconf>
- Network [1..1] DNS Server [1..n] Address  
Maximum number of DNS servers reduced from 5 to 3
- Provisioning Mode  
**OLD:** <Off/TMS/VCS/CallWay/CUCM/Auto>  
**NEW:** <Off/CUCM>
- SIP Profile [1..1] Type  
**OLD:** <Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel>  
**NEW:** <Cisco>
- SystemUnit MenuLanguage  
Added: Dutch, Italian, Korean, Portuguese-Brazilian
- Video Wallpaper  
Removed: Growing, Summersky

## EX90 system overview

The system is delivered with:

- EX90 unit
- Touch controller with cable
- Handset with cable
- DVI-D to DVI-I cable (recommended for optimal PC image quality)
- VGA to DVI-I cable
- Stereo audio cable 3.5 mm
- Ethernet cable
- AC adapter and power cable

The camera can be tilted and used as a document camera.



EX90, front view

Touch controller



EX90, rear view  
(without rear cover)

Detach the rear side cover when connecting cables.

When finished, snap on the rear cover.



A handset can be attached to the Touch controller.



## EX60 system overview

The system is delivered with:

- EX60 unit
- Touch controller with cable
- Handset with cable
- DVI-D to DVI-I cable (recommended for optimal PC image quality)
- VGA to DVI-I cable
- Stereo audio cable 3.5 mm
- Ethernet cable
- AC adapter and power cable

The camera can be tilted and used as a document camera.



EX60, front view

Touch controller



EX60, rear view  
(without rear cover)

Detach the rear side cover when connecting cables.

When finished, snap on the rear cover.



A handset can be attached to the Touch controller.

## User interfaces

The principal operating device for your Cisco TelePresence System EX90 or EX60 system is a Touch controller.

Additionally, you can configure your system via its web interface, provided that it is already connected to a network and you know the IP address.

On the next pages we briefly describe how to use the Touch controller and how to navigate and use the web interface.



Touch controller



Web interface

## How to use the Touch controller

The basic function of the Touch controller is illustrated below.  
The Touch controller and its use are described in full detail in the User Guide for your video system.

### Basic operating principles



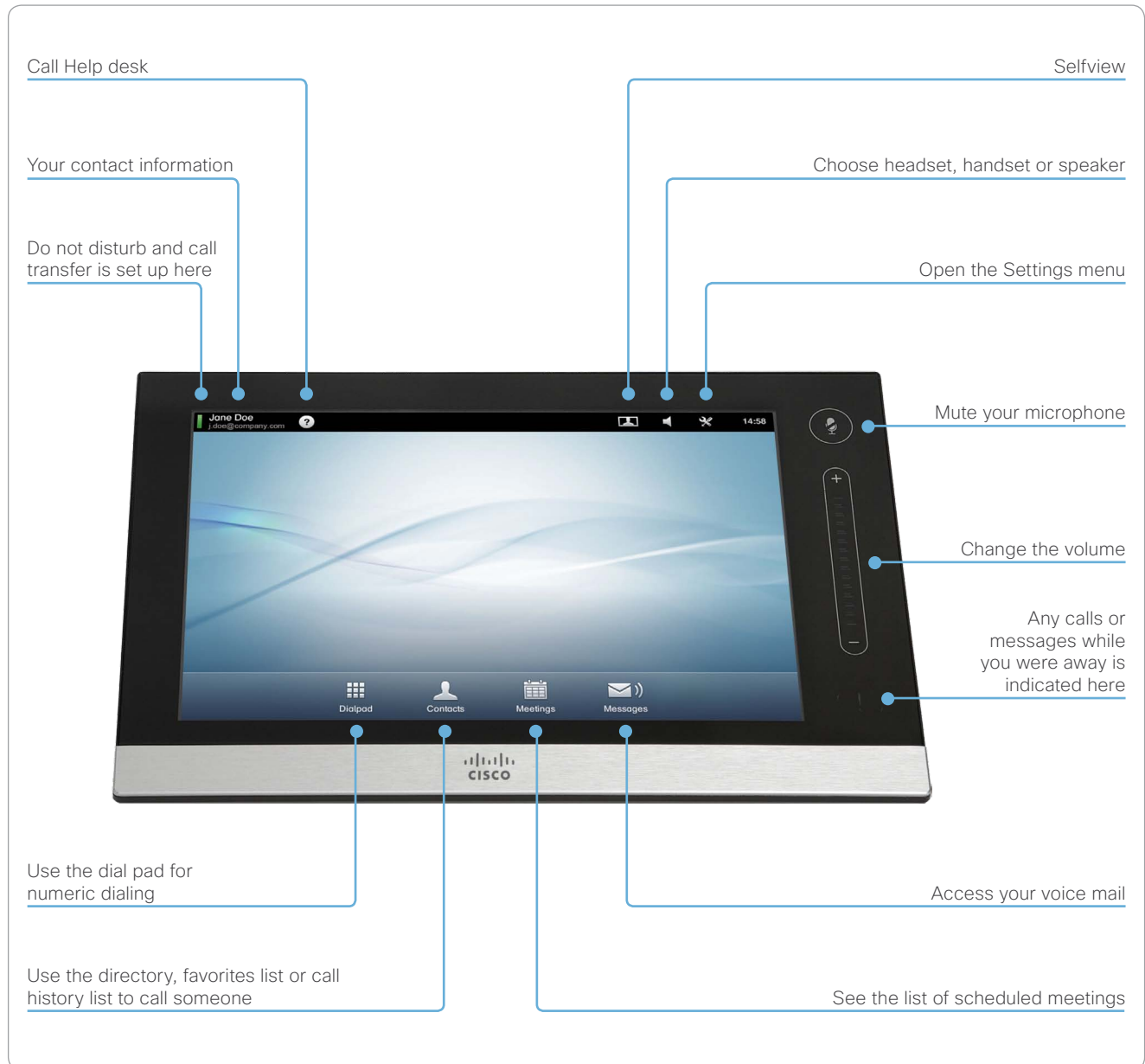
Tap the touch screen to wake up the system, if needed.



Tap a button to activate its function.



Scroll in lists as shown.



## How to use the web interface

The basic principles of navigating your video conference system's web interface and setting parameters are illustrated below.

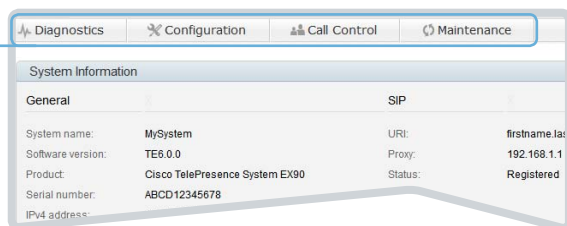
You open the web interface by entering your system's IP address in the address bar of a web browser; then you sign in.

Recommended browsers: Internet Explorer 8 and Mozilla Firefox 3.x.

The [Web interface](#) chapter describes how the web interface is organized, and the [Advanced settings](#) chapter describes the configurations it provides access to.

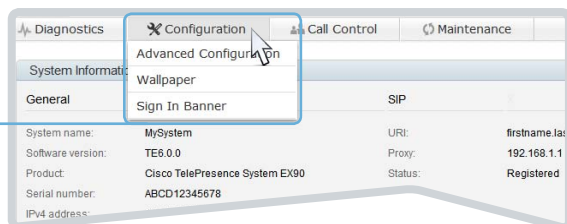
### The main menu

The main menu opens when you have signed in to the system.



### The Configuration sub-menu

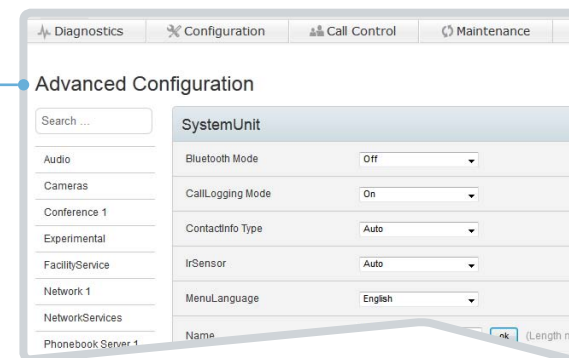
A sub-menu opens when hovering the mouse over the main menu item.



### The Advanced Configuration page

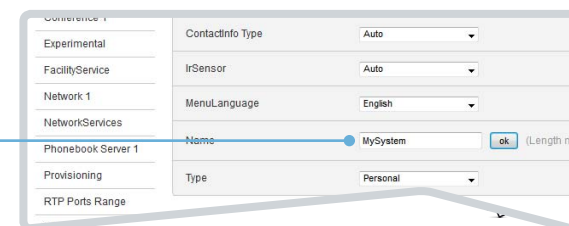
When clicking a sub-menu item the corresponding page opens.

You can change the system settings from the Advanced configuration page.



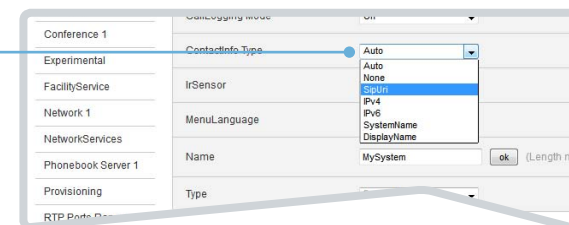
### Input text

Enter text in the input field, and click **ok** to save the change.



### Choose a value

Click the arrow to open the drop down list. Choose a value. The chosen value will be automatically saved.



## CHAPTER 2

### USING THE WEB INTERFACE

The Cisco TelePresence System EX90/EX60 can be configured using the Touch controller or the web interface.

The Touch controller and its use are described in the EX90 and EX60 User Guides.

For full access to the configurable parameters, the web interface must be used – the Touch controller provides access to a limited set of parameters only.



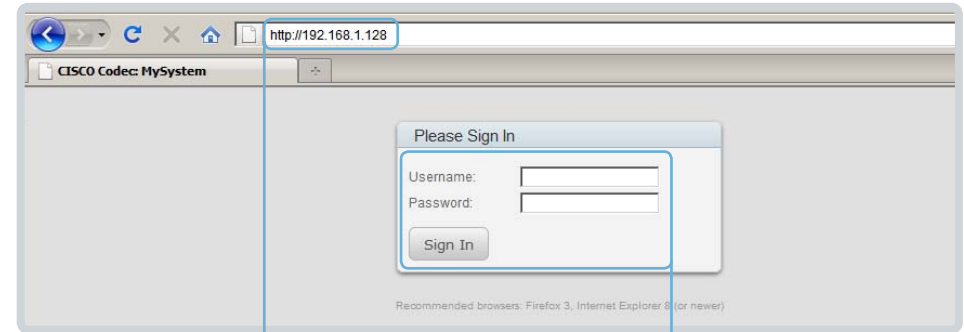


## Starting the web interface

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

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

On the following pages we describe how to use the web interface for system configuration and maintenance.



### 1. Connect to the video system

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



Tap [Settings](#) (⚙) > [System Information](#) on the Touch controller to find the system's IP address (IPv4 or IPv6).

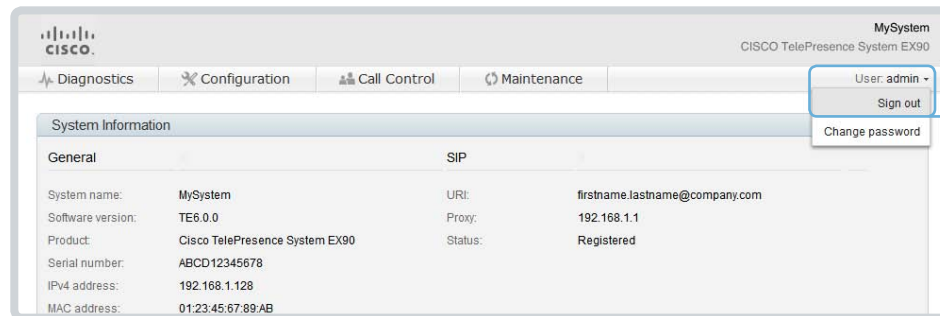
### 2. Sign in

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.



### Sign out

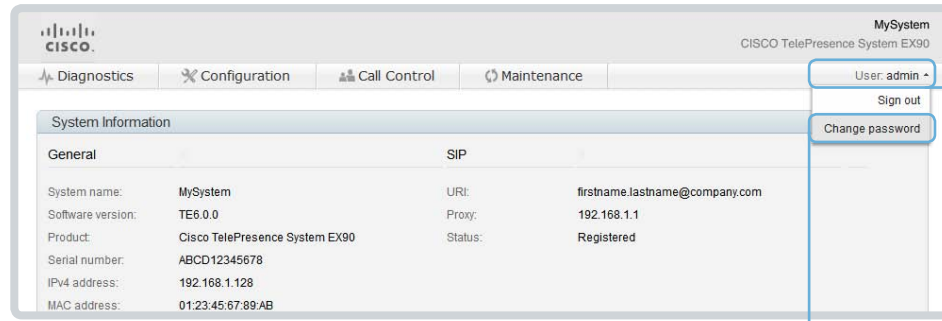
Click on your user name and choose [Sign out](#) in the drop down menu.

## Changing the system/codec 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 Information	
<b>General</b>	<b>SIP</b>
System name: MySystem	URI: firstname.lastname@company.com
Software version: TE6.0.0	Proxy: 192.168.1.1
Product: Cisco TelePresence System EX90	Status: Registered
Serial number: ABCD12345678	
IPv4 address: 192.168.1.128	
MAC address: 01:23:45:67:89:AB	

1. Click your user name

2. Open the Change Password dialog box

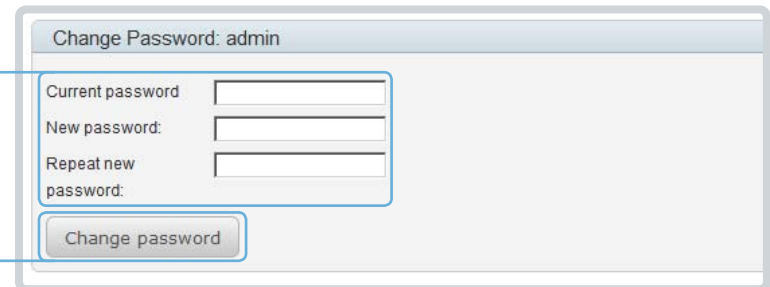
Choose [Change password](#) in the drop down menu.

### 3. Enter passwords

Enter your current and new passwords as requested. If the password currently is not set, leave the [Current password](#) field blank.

### 4. Set the new password

Click [Change password](#) for the change to take effect.



## The interactive menu

The web interface provides access to tasks and configurations which are grouped in four categories. They are available from the main menu.

The sub-pages for the different tasks are described on the following pages.

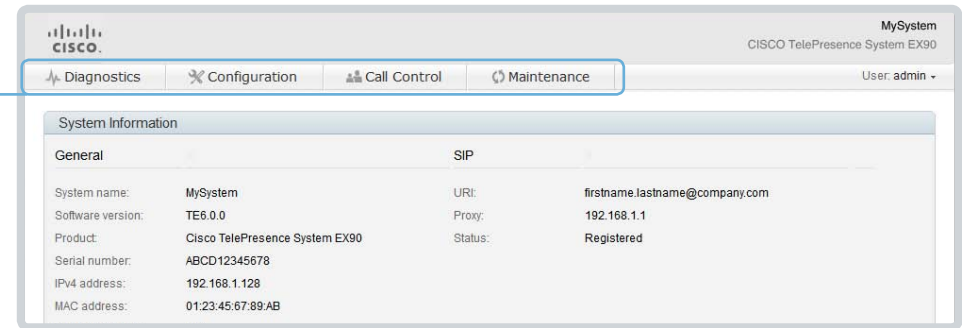


Only users with full access rights are allowed to perform all the tasks and configurations.

You can read more about user administration and access rights in the ► [User administration](#) section.

### Main menu

- Diagnostics
- Configuration
- Call Control
- Maintenance



#### Diagnostics

System Information  
Log Files  
XML Files

#### Configuration

Advanced Configuration  
Wallpaper  
Sign In Banner

#### Call Control

#### Maintenance

Software Upgrade  
Certificate Management  
User Administration  
Restart  
Factory Reset

### Open the sub-pages

When you hover the mouse over a main menu item, the titles of related sub-pages appear. \*

Click a sub-page's title to open it. If there are no related sub-pages, click the main menu item itself.

\* The illustration lists all the sub-menus. A user with limited access rights will not be able to access all the items.

## The system information page

You can find an overview of your video system set-up on the System Information page.

Diagnostics > System Information

System Information	
<b>General</b>	<b>SIP</b>
System name: <b>MySystem</b>	URI: <b>firstname.lastname@company.com</b>
Software version: <b>TE6.0.0</b>	Proxy: <b>192.168.1.1</b>
Product: <b>Cisco TelePresence System EX90</b>	Status: <b>Registered</b>
Serial number: <b>ABCD12345678</b>	
IPv4 address: <b>192.168.1.128</b>	
MAC address: <b>01:23:45:67:89:AB</b>	
Valid release key: <b>Yes</b>	
Installed options: <b>PremiumResolution</b>	
<b>Sign In Information</b>	
Last successful sign in: <b>Wed Oct 10 09:00:00 2012</b>	Unsuccessful authorization attempts since last sign in: <b>0</b>
Password expires in: <b>Never</b>	

### System information

Information about system name, product type, software version, IP address, etc.

### Sign in information

Information about recent sign in attempts and password expiry.

## 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.

Click on a log file and follow the instructions in the dialog box to save or open the file (left or right click depending on your browser).

You can also download all log files as a bundle; click the corresponding link on the web page and follow the instructions.

### Diagnostics > Log Files

#### Current Logs

File Name	Size	Last Modified
<a href="#">arm0-system.log</a>	9 KB	2012-10-09 14:55
<a href="#">arm1-system.log</a>	10 KB	2012-10-15 13:05
<a href="#">arm2-system.log</a>	10 KB	2012-10-09 14:55
<a href="#">console</a>	3 KB	2012-10-10 13:09
<a href="#">dmesg</a>	12 KB	2012-10-09 14:53
<a href="#">endeavour-system.log</a>	7 KB	2012-10-15 06:48
<a href="#">eventlog/all.log</a>	94 KB	2012-10-15 14:52
<a href="#">eventlog/identification.log</a>	75 KB	2012-10-15 14:52

<a href="#">kern.log</a>	22 KB	2012-10-09 14:54
<a href="#">lastlog</a>	0 KB	2012-10-09 14:53
<a href="#">messages.log</a>	14 KB	2012-10-15 13:19
<a href="#">wtmp</a>	1 KB	2012-10-09 14:55

[Download all log files as bundle \(tar.gz format\)](#)

#### Historical Logs

File Name	Size	Last Modified
<a href="#">log.0.tar.gz</a>	32 KB	2011-07-19 13:12
<a href="#">log.1.tar.gz</a>	97 KB	2011-10-06 13:53
<a href="#">log.2.tar.gz</a>	39 KB	2011-10-06 15:01
<a href="#">log.3.tar.gz</a>	466 KB	2011-10-20 19:52
<a href="#">log.4.tar.gz</a>	86 KB	2011-11-03 15:29
<a href="#">log.5.tar.gz</a>	110 KB	2011-11-09 11:06
<a href="#">log.6.tar.gz</a>	73 KB	2011-12-03 04:19
<a href="#">log.7.tar.gz</a>	208 KB	2012-05-02 17:09
<a href="#">log.8.tar.gz</a>	38 KB	2012-10-04 13:07
<a href="#">log.9.tar.gz</a>	223 KB	2012-10-09 14:52
<a href="#">log.tar.gz</a>	223 KB	2012-10-09 14:52

[Download all log files as bundle \(tar.gz format\)](#)



## XML files

The XML files are structured in a hierarchy building up a database of information about the codec.

Click the file names to open the corresponding file.

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

### Diagnostics > XML Files

XML Files

These XML files are a part of the codec's API, and can be used by external services to inspect the state and configuration of the codec.

The files are protected using Basic Authentication, thus you may be prompted for a user name and password.

File Name	Description
<a href="#">configuration.xml</a>	Configuration settings
<a href="#">status.xml</a>	Endpoint status parameters
<a href="#">command.xml</a>	Available API commands
<a href="#">valuespace.xml</a>	Value spaces of the XML files

## Advanced configuration

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

Each system setting is further described in the [Advanced settings](#) chapter.

Configuration > Advanced Configuration

### Advanced Configuration

Search functionality

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

Search ...

- Audio
- Cameras
- Conference 1
- Experimental
- FacilityService
- Network 1
- NetworkServices
- Phonebook: Server 1
- Provisioning
- RTP Ports Range
- SIP
- Standby
- SystemUnit**
- Time
- UserInterface
- TouchPanel
- Video

Categories

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

### SystemUnit

Bluetooth Mode: Off

CallLogging Mode: On

ContactInfo Type: Auto

IrSensor

MenuLanguage

Name: MySystem ok (Length must be from 0 to 50)

Type: Personal

### Changing system settings

The value space for a setting is specified either as a drop down list or with explanatory text following a text input field.

*Drop down list:* Click the down arrow to open the drop down list. Then choose the preferred value.

*Text input field:* Enter a new value in the field and click [ok](#) to save the new value.

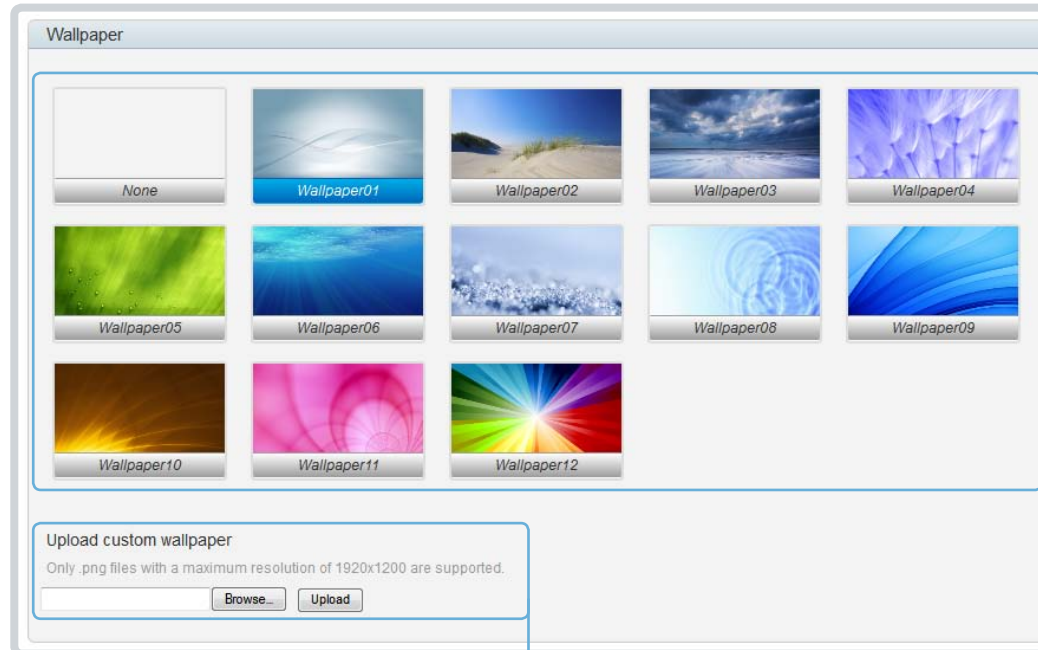
## Choosing a wallpaper

You can choose between a set of predefined wallpapers as background on your display.

If you want the company logo or another custom picture to be displayed on the main display, you may also upload and use a custom wallpaper.

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

### Configuration > Wallpaper



#### Upload a custom wallpaper file

1. Click [Browse...](#) and locate your custom wallpaper image file.  
The file format must be .png and the maximum image size is 1920 × 1200 pixels.
2. Click [Upload](#) to save the file on the video system.  
The custom wallpaper is chosen automatically upon upload.

#### Choose a wallpaper

Choose a wallpaper from the list.  
If you have uploaded a custom wallpaper, it will also appear in the list.  
The chosen wallpaper is highlighted.

## Sign in banner

If a system administrator wants to provide initial information to all users, he can create a sign in banner. A sign in banner is a message that is displayed to the user before signing in.

The message will be shown when the user signs in to the web interface or the command line interface.

Configuration > Sign In Banner

Sign In Banner

This is information that will be shown to all users before they sign in.

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

Save Sign In Banner

**1. Enter text for the sign in banner**

Enter the message which you want to present to the user prior to signing in.

**2. Activate the sign in banner**

Click [Save Sign In Banner](#) to activate it.

**An active sign in banner**

The sign in banner is displayed here.

## Placing a call

You can use the Call Control page of the web interface to initiate a call.

Only point-to-point video calls (a call involving only two parties) are supported. You cannot use the web interface to initiate multi-party conferences.



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; not the PC running the web interface.

## Calling someone

Enter one or more characters in the address input field until the name you want to call appears in the dynamic search list or, enter the complete name or number. Then click [Dial](#).

Click [End all](#) to disconnect the call.




## Sharing contents


Click the [Start Presentation](#) button to start sharing contents with the remote participant.


Normally a PC is used as presentation source, but other options may be available depending on your system setup.


To stop the content sharing, click the [Stop Presentation](#) button that is visible while sharing content.


Call Control

Volume:   Mute Internal 




☐ Live snapshots
  Camera Control





 Start Presentation


Participants

participant@company.com


 Dial


6000 kbps 

SIP 

 End all

Layout family:

Equal 




participant@company.com

participant@company.com

Call rate: 6000 kbps

Protocol: sip



[Show details](#)

Address input field

D14726.08 EX Series Administrator Guide TE6.0, NOVEMBER 2012.

23

www.cisco.com — Copyright © 2010–2012 Cisco Systems, Inc. All rights reserved.



## Controlling and monitoring a call

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

- **Adjusting the sound volume**

Use **+** and **-** on the volume control bar to adjust the sound volume (not the keyboard **+** and **-** keys).

- **Muting the microphone**

Use the **Mute** button when you want to deactivate the microphone for privacy reasons.

When the microphone is muted, the **Unmute** button that re-activates the microphone appears.

- **Using the in-built microphone/speaker, handset or headset**

Use the audio selector drop down list to choose whether to use the built-in microphone and loudspeakers, the handset on the Touch controller, or a headset.

- **Controlling the camera**

First, click the **Camera Control** button. Then, in the window that opens, choose a camera preset or use **+** and **-** to adjust the zoom.

Note that zoom control is available only on the EX90.

- **Changing the call rate**

When you load the Call Control page, the default call bit rate is shown in the **Call bit rate** field. If preferred, you can choose another bit rate from the drop down list.

You can not change these setting during a call.

- **The call protocol**

When you load the Call Control page, the default call protocol is shown in the **Call protocol** field. This software version (TE6.0) supports only the SIP call protocol.

- **Call details**

Click **Show details** while in a call to provide information on call rate, encryption, as well as important video and audio parameters. **Hide details** removes the information.

Call Control

Volume control

Microphone mute

Audio selector

Call Control

Volume:

Mute Internal

Live snapshots

Camera Control

Start Presentation

Participants

participant@company.com

Dial 6000 kbps SIP

End all

Layout family: Equal

participant@company.com

participant@company.com

Transmit Call Rate: 6000 kbps

Receive Call Rate: 6000 kbps

Encryption: A

Audio	Transmit	Receive	Video	Transmit	Receive
Protocol	AACLD	AACLD	Protocol	H264	H264
Channel rate	125 kbps	128 kbps	Channel rate	5783 kbps	5844 kbps
Resolution	-	-	Resolution	1920x1088@30	1280x720@60
Jitter	0 ms	0 ms	Jitter	1 ms	2 ms
Loss	0 %	0 %	Loss	0 %	0 %

Hide details

Show/hide call details

Call bit rate

Call protocol

Camera Control

Main Source Camera 1

Presets

No presets stored

+

Q

-

Camera control

D14726.08 EX Series Administrator Guide TE6.0, NOVEMBER 2012.

24

www.cisco.com — Copyright © 2010–2012 Cisco Systems, Inc. All rights reserved.

## Local layout control




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


The term layout is used to describe the various ways a video conversation appear on screen. Different types of meetings will require different layouts.

Each layout will typically specify a screen layout well suited when you are not in a meeting or you are in a meeting with one, two or three parties; when the meeting does or does not involve a second video stream for presentations; when the screen aspect ratio is 4:3 or 16:9.


Call Control


Call Control


Volume:   Internal 







☐ Live snapshots


Camera Control 



Start Presentation 

Participants

Dial or search   6000 kbps  SIP 

Layout family: Equal 

No calls connected

### Choose a layout

Choose your preferred layout in the drop down menu. \*

You may change the layout while in a call.

### \*) Layout families

*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.

*Equal:* All videos have equal size, as long as there is space enough on the screen.

*Prominent:* The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. The pictures will not overlap. Transitions between active speakers are voice switched.

*Overlay:* 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.

## 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, for example 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, and must be enabled using the Touch controller.

- Tap [Settings](#) (⚙️) > [Administrator](#) > [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.

Call Control


Volume: 


 Mute

Internal 







☒ Live snapshots


 Camera Control

 Start Presentation

Participants


participant@company.com  6000 kbps SIP 

Layout family: Equal 




participant@company.com

participant@company.com



Call rate: 6000 kbps

Protocol: sip



Show details

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

D14726.08 EX Series Administrator Guide TE6.0, NOVEMBER 2012.

26

www.cisco.com — Copyright © 2010–2012 Cisco Systems, Inc. All rights reserved.

## Upgrading the system software

The TE6.0 software version only applies to EX Series endpoints registered on a Cisco Unified Communications Manager (CUCM).

You can upgrade from software version TC5.x to TE6.0 without adding a new release key.



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

### Software release notes and upgrade files

For a complete overview of the news and changes, we recommend reading the Software Release Notes (TE6). Go to:

► [http://www.cisco.com/en/US/products/ps11327/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps11327/tsd_products_support_series_home.html)

### Downloading new software

For software download, go to:

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

#### Maintenance > Software Upgrade

#### Upgrade Software

Current software version: TE6.0.0

#### Add Option Key

Option keys allow for extended functionality of the codec. Contact your Cisco representative for information about available keys and to obtain required option key(s). Option keys are based on the unique serial number of the codec. The serial number for this codec is ...

#### Upgrading the system software

- Before you can start the upgrade you must download the software upgrade file.  
Each software version has a unique file name, and the format is "s52110te6\_0\_0.pkg".
- Click [Browse...](#) and find the .PKG file.
- Click [Upgrade](#) to start the installation.
- Allow the installation process to complete. It may take up to 30 minutes. You can follow the progress on the web page.  
The system restarts automatically after the installation.  
If you want to continue working with the web interface you must sign in anew.

## Adding option keys

Option keys allow for extended functionality of the system. The keys are required to activate the optional functionality. You may have several option keys in your system.

The available options are:

- Premium resolution
- MultiSite (only EX90)
- Dual display (only EX90)

Contact your Cisco representative to obtain the required option key(s).

### Maintenance > Software Upgrade

#### Upgrade Software

Current software version: TE6.0.0

#### Add Option Key

Option keys allow for extended functionality of the codec. Contact your Cisco representative for information about available keys and to obtain required option key(s). Option keys are based on the unique serial number of the codec. The serial number for this codec is ...

#### Adding option keys

- i. Enter the *Option Key* and click *Add*.  
Each system has a unique key, and the key format is:  
"1N000-1-AA7A4A09".
- ii. If you have more than one option key, repeat step i for all of them.
- iii. When all option keys are added, restart the system to activate the new options.

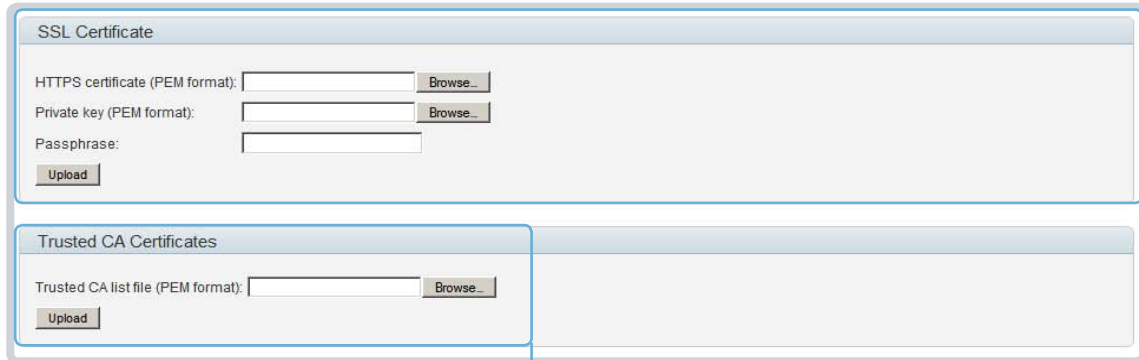


## Certificate management

The SSL certificate is a text file which verifies the authenticity of your video conference system. The certificate may be issued by a certificate authority (CA). Other parties can check this certificate before setting up communication with you.

The list of trusted CA certificates is a list containing the SSL certificates of all parties that you want your system to trust.

### Maintenance > Certificate Management



#### Uploading the trusted CA certificates list

To install the trusted CA certificates list, you will need the following:

- Trusted CA list file ( .PEM format).

Contact your system administrator to obtain the required file.

1. Click [Browse...](#) and find the file with the Trusted CA list ( .PEM format).
2. Click [Upload](#) to store the certificate list on your system.

#### Uploading the SSL certificate

To install the SSL certificate, you will need the following:

- HTTPS certificate ( .PEM format)
- Private key ( .PEM format)
- Passphrase (optional)

Contact your system administrator to obtain the required files.

1. Click [Browse...](#) and locate the HTTPS certificate file ( .PEM format).
2. Click [Browse...](#) and find the Private key file ( .PEM format).
3. Enter the [Passphrase](#).
4. Click [Upload](#) to store the certificate on your system

## 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 user name *admin* and no password set. The admin user has full access rights, and **it is highly recommended to set a password for the default user.**

Read more about passwords in the [▶ Setting passwords](#) chapter.

### About user roles

Three user roles with *non-overlapping rights* are defined. \*

Any user must hold one or a combination of these *user roles*. An administrator user account with full access rights, like the default *admin* user, must possess all the three roles.

#### <sup>1)</sup>User roles

**ADMIN:** A user holding this role can create new users and change most settings.

**USER:** A user holding this role can make calls, search the phone book. The user can modify a few settings, e.g. adjusting the audio volume and changing the menu language.

**AUDIT:** This user role is reserved for security audit configurations.

#### Maintenance > User Administration

User Management		
User	Roles	Status
admin	Admin, User, Audit	Active
user1	User	Active
Create new user		

#### Default user account

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

## Creating a new user account

1. Click [Create new user](#).
2. Fill in the Username, Password and PIN code, and choose the user role(s) for this user account.  
  
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.

## Editing user details

1. Choose 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



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

1. Choose the name of an existing user to open the Editing user window.
2. Set the [Status](#) to **Inactive**.
3. Click [Save](#) to save the changes.

## Deleting a user account



Always keep at least one user with ADMIN rights.

1. Choose the name of the user to open the Editing user window.
2. Click [Delete](#).

Maintenance > User Administration

### User Management

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

Create new user

### Editing user: user1

Password:   
 PIN:  (Used if login-required h  
 DN Subject:

Roles: ☐ Admin  
☒ User  
☐ Audit

Status: ☒ Active  
☐ Inactive

☐ Require password change on next user logon  
☐ Require PIN change on next user logon

Save Delete Cancel

### Create new user

Username:   
 Password:   
 PIN:  (Used if login-required h  
 DN Subject:

Roles: ☐ Admin  
☐ User  
☐ Audit

Status: ☐ Active  
☒ Inactive

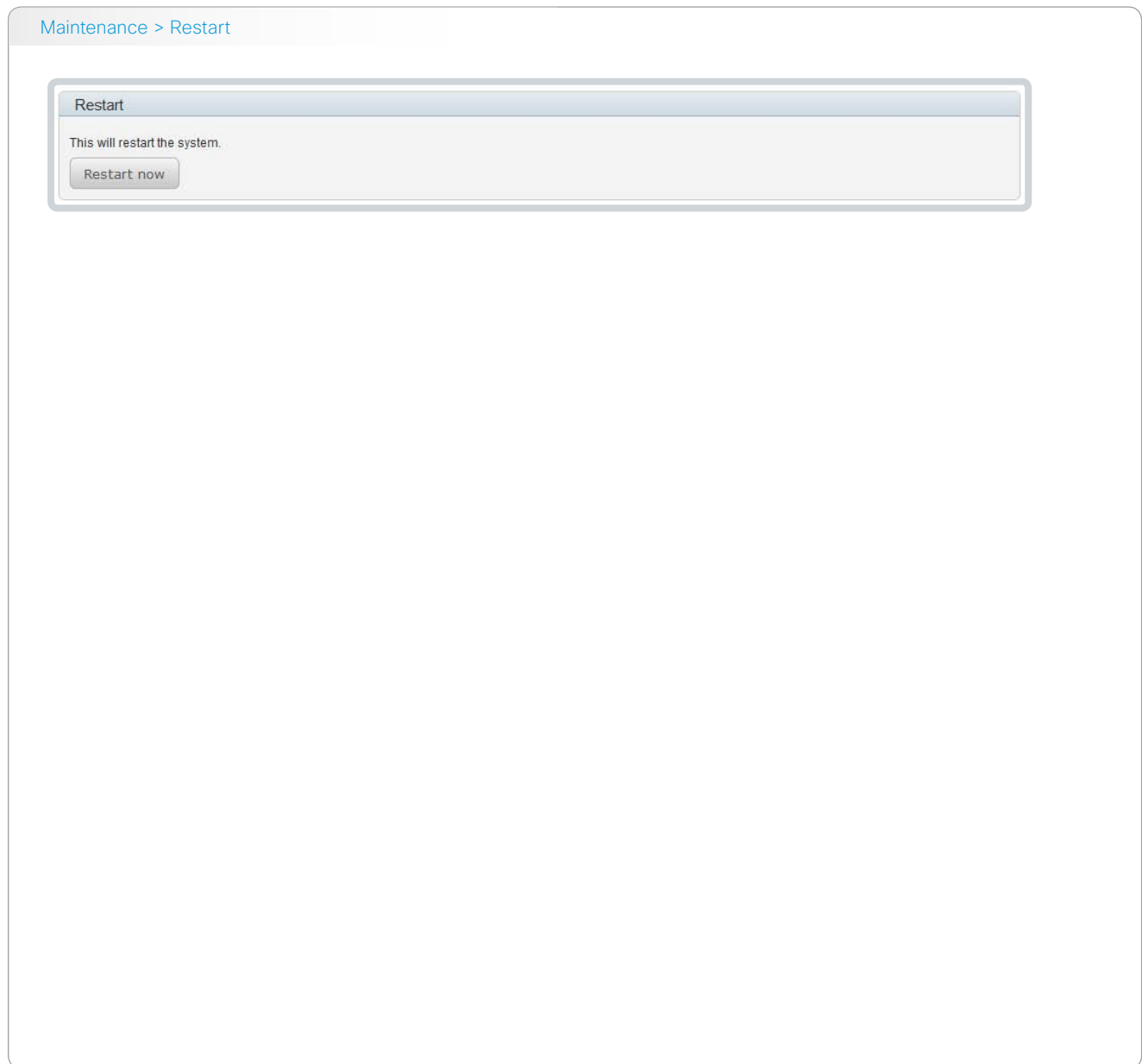
☒ Require password change on next user logon  
☒ Require PIN change on next user logon

Save Cancel

## Restarting the system

To restart the system, click [Restart now](#).

Restarting the system takes a few minutes.



## Factory reset

When factory resetting the video system the following happens:

- The call logs are deleted.
- All system parameters are reset to default values.
- All files that have been uploaded to the system are deleted.
- Release key(s) and option key(s) are preserved.
- Automatic restart of the system.




It is not possible to undo a factory reset.

### Maintenance > Factory Reset

Factory Reset

This will reset the codec to factory default settings, followed by an automatic reboot of the codec.  
The call logs will be deleted and all system parameters will be reset to default values. All files that have been uploaded to the codec will be deleted. Release keys and option keys will **not** be affected.

 A factory reset cannot be undone.

☒ I want to reset the codec back to factory settings!

Perform a factory reset

#### Perform a factory reset

Read the provided information carefully before you restore the factory settings.

Check the *I want to reset...* check box, and click *Perform a factory reset*.

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

## CHAPTER 3

### ADVANCED SETTINGS

The Cisco TelePresence System EX90/EX60 can be configured using the Touch controller or the web interface.

For full access to the configurable parameters, the web interface must be used – the Touch controller provides access to a limited set of parameters only.



## Overview of the advanced settings

In the following pages you will find a complete list of the system settings which are configured from the Advanced configuration page on the web interface. The examples shows either the default value or an example of a value.

Open a web browser and enter the IP address of the EX90/EX60; then sign in.



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

<b>Audio settings</b> .....	<b>37</b>	<b>FacilityService settings</b> .....	<b>44</b>
Audio InternalSpeaker Mode.....	37	FacilityService Service [1..5] CallType .....	44
Audio PreferredOutputConnector.....	37	FacilityService Service [1..5] Name.....	44
Audio SoundsAndAlerts KeyTones Mode .....	38	FacilityService Service [1..5] Number .....	44
Audio SoundsAndAlerts RingTone.....	38	FacilityService Service [1..5] Type .....	44
Audio SoundsAndAlerts RingVolume.....	37		
Audio Volume Handset.....	37	<b>Network settings</b> .....	<b>45</b>
Audio Volume Headset .....	37	Network [1..1] Assignment.....	45
Audio Volume Speaker.....	37	Network [1..1] DNS Domain Name.....	46
		Network [1..1] DNS Server [1..3] Address.....	46
<b>Cameras settings</b> .....	<b>39</b>	Network [1..1] IEEE8021x AnonymousIdentity .....	48
Cameras Camera [1..1] Backlight .....	40	Network [1..1] IEEE8021x Eap Md5.....	48
Cameras Camera [1..1] Brightness Level .....	39	Network [1..1] IEEE8021x Eap Peap.....	49
Cameras Camera [1..1] Brightness Mode.....	39	Network [1..1] IEEE8021x Eap Tls .....	49
Cameras Camera [1..1] Focus Mode .....	39	Network [1..1] IEEE8021x Eap Ttls.....	48
Cameras Camera [1..1] FrameRate.....	40	Network [1..1] IEEE8021x Identity .....	48
Cameras Camera [1..1] Gamma Level.....	40	Network [1..1] IEEE8021x Mode.....	47
Cameras Camera [1..1] Gamma Mode .....	40	Network [1..1] IEEE8021x Password .....	48
Cameras Camera [1..1] Whitebalance Level.....	39	Network [1..1] IEEE8021x TlsVerify .....	48
Cameras Camera [1..1] Whitebalance Mode.....	39	Network [1..1] IEEE8021x UseClientCertificate.....	48
Cameras PowerLine Frequency.....	39	Network [1..1] IPStack.....	45
		Network [1..1] IPv4 Address .....	45
<b>Conference settings</b> .....	<b>41</b>	Network [1..1] IPv4 Gateway.....	45
Conference [1..1] AutoAnswer Delay.....	41	Network [1..1] IPv4 SubnetMask.....	45
Conference [1..1] AutoAnswer Mode.....	41	Network [1..1] IPv6 Address .....	46
Conference [1..1] AutoAnswer Mute.....	41	Network [1..1] IPv6 Assignment.....	45
Conference [1..1] BFCP Mode .....	42	Network [1..1] IPv6 DHCPOptions .....	46
Conference [1..1] DefaultCall Protocol.....	42	Network [1..1] IPv6 Gateway.....	46
Conference [1..1] DefaultCall Rate.....	42	Network [1..1] MTU .....	49
Conference [1..1] DoNotDisturb Mode .....	41	Network [1..1] QoS Diffserv Audio.....	46
Conference [1..1] Encryption Mode .....	42	Network [1..1] QoS Diffserv Data.....	47
Conference [1..1] FarEndControl Mode .....	42	Network [1..1] QoS Diffserv Signalling.....	47
Conference [1..1] IX Mode .....	42	Network [1..1] QoS Diffserv Video.....	47
Conference [1..1] MaxReceiveCallRate .....	42	Network [1..1] QoS Mode .....	46
Conference [1..1] MaxTransmitCallRate .....	42	Network [1..1] Speed .....	49
Conference [1..1] MicUnmuteOnDisconnect Mode.....	41	Network [1..1] TrafficControl Mode.....	49
Conference [1..1] PacketLossResilience Mode .....	43	Network [1..1] VLAN Voice Mode .....	49
Conference [1..1] TelephonyPrefix.....	43	Network [1..1] VLAN Voice VlanId.....	50



<b>NetworkServices settings.....</b>	<b>51</b>	<b>SIP settings.....</b>	<b>58</b>	<b>Video settings.....</b>	<b>65</b>
NetworkServices CTMS Mode .....	53	SIP ANAT .....	60	Video AllowWebSnapshots.....	68
NetworkServices HTTP Mode .....	53	SIP ListenPort .....	59	Video ControlPanel Brightness .....	68
NetworkServices HTTPS Mode.....	51	SIP OCSP DefaultResponder.....	60	Video DefaultPresentationSource.....	67
NetworkServices HTTPS VerifyClientCertificate .....	51	SIP OCSP Mode.....	60	Video Input DVI [1] RGBQuantizationRange.....	68
NetworkServices HTTPS VerifyServerCertificate .....	51	SIP PreferredIPMedia.....	60	Video Input DVI [1] Type .....	68
NetworkServices NTP Address .....	52	SIP PreferredIPSignaling.....	60	Video Input HDMI [1] RGBQuantizationRange .....	67
NetworkServices NTP Mode .....	52	SIP Profile [1..1] Authentication [1..1] LoginName .....	59	Video Input Source [1..3]/[1..2] CameraControl Camerald ..	66
NetworkServices SIP Mode.....	52	SIP Profile [1..1] Authentication [1..1] Password .....	59	Video Input Source [1..3]/[1..2] CameraControl Mode .....	65
NetworkServices SNMP CommunityName .....	51	SIP Profile [1..1] DefaultTransport .....	58	Video Input Source [1..3]/[1..2] Name.....	65
NetworkServices SNMP Host [1..3] Address .....	52	SIP Profile [1..1] DisplayName.....	58	Video Input Source [1..3]/[1..2] OptimalDefinition Profile.....	66
NetworkServices SNMP Mode .....	51	SIP Profile [1..1] Line.....	59	Video Input Source [1..3]/[1..2] OptimalDefinition	
NetworkServices SNMP SystemContact.....	51	SIP Profile [1..1] Mailbox .....	59	Threshold60fps.....	67
NetworkServices SNMP SystemLocation .....	52	SIP Profile [1..1] Outbound.....	58	Video Input Source [1..3]/[1..2] Quality .....	67
NetworkServices SSH Mode .....	53	SIP Profile [1..1] Proxy [1..4] Address.....	59	Video Input Source [1..3]/[1..2] Type .....	65
NetworkServices Telnet Mode.....	53	SIP Profile [1..1] Proxy [1..4] Discovery .....	59	Video Input Source [1] Connector .....	65
<b>Phonebook settings .....</b>	<b>54</b>	SIP Profile [1..1] TlsVerify .....	58	Video Input Source [2] Connector.....	65
Phonebook Server [1..1] ID.....	54	SIP Profile [1..1] Type.....	58	Video Input Source [3] Connector.....	65
Phonebook Server [1..1] Type .....	54	SIP Profile [1..1] URI .....	58	Video MainVideoSource .....	68
Phonebook Server [1..1] URL .....	54	<b>Standby settings .....</b>	<b>61</b>	Video Output HDMI [1] CEC Mode .....	69
<b>Provisioning settings.....</b>	<b>55</b>	Standby Delay .....	61	Video Output HDMI [1] MonitorRole .....	69
Provisioning Connectivity.....	55	<b>SystemUnit settings .....</b>	<b>62</b>	Video Output HDMI [1] OverscanLevel.....	69
Provisioning ExternalManager Address .....	56	SystemUnit Bluetooth Mode .....	62	Video Output HDMI [1] Resolution.....	69
Provisioning ExternalManager Domain .....	56	SystemUnit CallLogging Mode .....	62	Video Output Internal [3]/[2] MonitorRole .....	70
Provisioning ExternalManager Path .....	56	SystemUnit ContactInfo Type .....	62	Video Output LCD [2]/[1] Blue .....	70
Provisioning ExternalManager Protocol .....	56	SystemUnit IrSensor.....	62	Video Output LCD [2]/[1] Brightness .....	70
Provisioning HttpMethod .....	55	SystemUnit MenuLanguage.....	62	Video Output LCD [2]/[1] Green.....	70
Provisioning LoginName .....	55	SystemUnit MenuLanguage.....	62	Video Output LCD [2]/[1] MonitorRole .....	69
Provisioning Mode .....	55	SystemUnit Name .....	62	Video Output LCD [2]/[1] Red .....	70
Provisioning Password.....	55	SystemUnit Type.....	62	Video Output LCD [2]/[1] Resolution.....	69
<b>RTP settings.....</b>	<b>57</b>	<b>Time settings .....</b>	<b>63</b>	Video Selfview .....	70
RTP Ports Range Start.....	57	Time DateFormat .....	63	Video Wallpaper.....	70
RTP Ports Range Stop .....	57	Time TimeFormat.....	63	<b>Experimental settings .....</b>	<b>71</b>
		Time Zone.....	63		
		<b>UserInterface settings.....</b>	<b>64</b>		
		UserInterface TouchPanel DefaultPanel .....	64		
		UserInterface TouchPanel DomainAutocomplete .....	64		

## Audio settings

### Audio InternalSpeaker Mode

Set the internal loudspeaker mode.

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* The internal speakers are enabled.

*Off:* The internal speakers are disabled.

**Example:** Audio InternalSpeaker Mode: On

### Audio Volume Handset

Adjust the handset 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 Handset: 70

### Audio Volume Headset

Adjust the headset 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 Headset: 70

### Audio Volume Speaker

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

### Audio PreferredOutputConnector

Select the preferred connector for the audio output. When the handset is in use the audio goes to the handset, and when hung up the audio out goes to the preferred output connector.

**Requires user role:** ADMIN

**Value space:** <None/HDMI/Internal/Bluetooth/Handset/Headset>

*None:* The default audio output is the internal speaker.

*HDMI:* The audio output goes to the HDMI audio channel.

*Internal:* The audio output goes to the internal loudspeaker. NOTE: Requires the Audio InternalSpeaker Mode setting is enabled.

*Bluetooth:* The audio output goes to the Bluetooth headset.

*Handset:* The audio output goes to the handset.

*Headset:* The audio output goes to the (wired) headset.

**Example:** Audio PreferredOutputConnector: Internal

### 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 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 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:** <On/Off>

*On:* You will hear key tones when you type.

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

**Example:** Audio SoundsAndAlerts KeyTones Mode: Off

## 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] 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] 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

### 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, and for EX90 also after zooming the camera. 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] 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:** <On/Off>

*On:* Turn on the camera backlight compensation.

*Off:* Turn off the camera backlight compensation.

**Example:** Cameras Camera 1 Backlight: Off

### 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] 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

## Conference settings

### Conference [1..1] AutoAnswer Mode

Set the auto answer mode.

**Requires user role:** ADMIN

**Value space:** <On/Off>

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

*Off:* An incoming call must be answered manually by tapping the Accept key on the Touch controller.

**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:** <On/Off>

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

*Off:* The incoming call will not be muted.

**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:** <On/Off>

*On:* Unmute the microphones after the call is disconnected.

*Off:* If muted during a call, let the microphones remain muted 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:** <On/Off/Timed>

*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.

*Off:* The incoming calls will come through as normal.

*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] 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:** <On/Off>

*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.

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

**Example:** Conference 1 FarEndControl Mode: On

### Conference [1..1] IX Mode

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

### 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:** <BestEffort>

*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 multi-point calls:* In order to have encrypted multi-party 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:** <Sip>

*Sip:* Select SIP to ensure that calls are set up as SIP calls.

**Example:** Conference 1 DefaultCall Protocol: Sip

### 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 call rate to be used when placing or receiving 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 call rate to be used when placing or receiving 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] BFCP Mode

The Binary Floor Control Protocol (BFCP) is defined in IETF RFC 4582 and can be used in SIP calls. BFCP is a protocol for controlling the access to the media resources in a conference, in this case content sharing data. The media from content sharing is usually video output from a laptop or from a document camera. When using BFCP the content sharing data will be transmitted as a separate video channel (dual stream). This is recommended for better quality.

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* Enable the use of BFCP, i.e. allow content sharing data to be transmitted in a separate video channel.

*Off:* Disable the use of BFCP, i.e. the main video and the content sharing data must share the capacity of one video channel.

**Example:** Conference BFCP Mode: On



### 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] PacketLossResilience Mode

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

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* Enable the packet loss resilience.

*Off:* Disable the packet loss resilience.

**Example:** Conference 1 PacketLossResilience Mode: On

## 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 help desk 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

## Network settings

### Network [1..1] IPStack

Select which internet protocols the system will support.

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

**Requires user role:** ADMIN

**Value space:** <IPv4/IPv6>

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

*IPv6:* IP version 6 is used for the SIP 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, e.g. 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 auto configuration of the IPv6 network interface. See RFC4862 for a detailed description. The options, e.g. 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 Gateway: 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 you must configure the Diffserv sub menu settings (Audio, Data, Signalling and Video).

**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] 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:** <On/Off>

*On:* The 802.1X authentication is enabled.

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

**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:** 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 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 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 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:** <On/Off>

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

*Off:* The EAP-MD5 protocol is disabled.

**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:** <On/Off>

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

*Off:* The EAP-TTLS protocol is disabled.

**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:** <On/Off>

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

*Off:* The EAP-PEAP protocol is disabled.

**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. 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:* Auto negotiate link speed.

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

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

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

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

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

**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:** <On/Off>

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

*Off:* Transmit video packets at link speed.

**Example:** Network 1 TrafficControl: On

## Network [1..1] VLAN Voice Mode

Set the VLAN voice mode.

**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. The VLAN Voice Mode automatically will be set to Auto when the GUI is used to set the Provisioning Mode to CUCM.

*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 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:** <On/Off>

*On:* The HTTPS protocol is enabled.

*Off:* The HTTPS protocol is disabled.

**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:** <On/Off>

*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.

*Off:* Do not verify server certificates.

**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:** <On/Off>

*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.

*Off:* Do not verify client certificates.

**Example:** NetworkServices HTTPS VerifyClientCertificate: Off

### 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 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 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.), e.g. 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 SIP Mode

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

**Requires user role:** ADMIN

**Value space:** <On/Off>

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

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

**Example:** NetworkServices SIP Mode: On

### 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:** <Off/Auto/Manual>

*Off:* The system will not use an NTP server.

*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.

*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 CTMS Mode

This setting determines whether or not to allow multiparty conferences controlled by a Cisco TelePresence Multipoint Switch (CTMS). CTMS must be version 1.8 or later. Encrypted conferences are not supported.

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* Multiparty conferencing via CTMS is allowed.

*Off:* Multiparty conferencing via CTMS is prohibited.

**Example:** NetworkServices CTMS Mode: On

### NetworkServices Telnet Mode

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

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* The Telnet protocol is enabled.

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

**Example:** NetworkServices Telnet Mode: Off

### 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:** <On/Off>

*On:* The HTTP protocol is enabled.

*Off:* The HTTP protocol is disabled.

**Example:** NetworkServices HTTP Mode: On

### 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:** <On/Off>

*On:* The SSH protocol is enabled.

*Off:* The SSH protocol is disabled.

**Example:** NetworkServices SSH Mode: On

## 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 phone book server type.

**Requires user role:** ADMIN

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

*VCS:* Select VCS if the phone book is located on the Cisco TelePresence Video Communication Server.

*TMS:* Select TMS if the phone book is located on the Cisco TelePresence Management Suite server.

*Callway:* Select Callway if the phone book 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 phone book 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 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 whether to use a provisioning system or not. Contact your provisioning system provider/representative for more information.

**Requires user role:** ADMIN

**Value space:** <Off/CUCM>

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

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

**Example:** Provisioning Mode: CUCM

### Provisioning LoginName

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

**Requires user role:** ADMIN

**Value space:** <S: 0, 80>

*Format:* String with a maximum of 80 characters.

**Example:** Provisioning LoginName: ""

### Provisioning Password

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

**Requires user role:** ADMIN

**Value space:** <S: 0, 64>

*Format:* String with a maximum of 64 characters.

**Example:** Provisioning Password: ""

### Provisioning HttpMethod

Select the HTTP method to be used for the provisioning.

**Requires user role:** ADMIN

**Value space:** <GET/POST>

*GET:* Select GET when the provisioning server supports GET.

*POST:* Select POST when the provisioning server supports POST.

**Example:** Provisioning HttpMethod: POST

### 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 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.

The DHCP server can be set up to provide the external manager address automatically (DHCP Option 150). 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

Not applicable in this software version.

## Provisioning ExternalManager Domain

Not applicable in this software version.

## RTP settings

### RTP Ports Range Start

Specify the first port in the range of RTP ports.

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.

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

## SIP settings

### 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] DefaultTransport

Select the transport protocol to be used over the LAN.

**Requires user role:** ADMIN

**Value space:** <UDP/TCP/Tls/Auto>

*UDP:* The system will always use UDP as the default transport method.

*TCP:* The system will always use TCP 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:** <On/Off>

*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.

*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.

**Example:** SIP Profile 1 TlsVerify: Off

### SIP Profile [1..1] Type

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

**Requires user role:** ADMIN

**Value space:** <Cisco>

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

**Example:** SIP Profile 1 Type: Cisco

### 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:** <On/Off>

*On:* Set up multiple outbound connections to servers in the Proxy Address list.

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

**Example:** SIP Profile 1 Outbound: Off

### 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] 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 invalid IP addresses (192.0.1234.0) will be rejected.

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

### 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] Mailbox

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

**Requires user role:** ADMIN

**Value space:** <S: 0, 255>

*Format:* String with a maximum of 255 characters.

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

### SIP Profile [1..1] Line

When registered to a Cisco Unified Communications Manager (CUCM) the endpoint may be part of a shared line. This means that several devices share the same directory number. The different devices sharing the same number receive status from the other appearances on the line as defined in RFC 4235.

Note that shared lines are set up by CUCM, not by the endpoint. Therefore do not change this setting manually; CUCM pushes this information to the endpoint when required.

**Requires user role:** ADMIN

**Value space:** <Shared/Private>

*Shared:* The system is part of a shared line and is therefore sharing its directory number with other devices.

*Private:* This system is not part of a shared line (default).

**Example:** SIP Profile 1 Line: Private

### 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 ANAT**

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

**SIP PreferredIPMedia**

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

**SIP PreferredIPSignaling**

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

**SIP OCSP Mode**

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

**SIP OCSP DefaultResponder**

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

## Standby settings

### Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode.

**Requires user role:** ADMIN

**Value space:** <1..480>

*Range:* Select a value from 1 to 480 minutes.

**Example:** Standby Delay: 10

## SystemUnit settings

### SystemUnit Name

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

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

**Requires user role:** ADMIN

**Value space:** <S: 0, 50>

*Format:* String with a maximum of 50 characters.

**Example:** SystemUnit Name: "Meeting Room"

### SystemUnit MenuLanguage

Select the language to be used in the menus on screen.

**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 Type

Select whether the video system is for personal use or to be used in a multi-user environment. It is highly recommended to use the default setting.

**Requires user role:** ADMIN

**Value space:** <Personal/Shared>

*Personal:* Set to Personal when the system is for personal use.

*Shared:* Set to Shared when the system is used in a multi-user environment.

**Example:** SystemUnit Type: Personal

### SystemUnit IrSensor

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

### SystemUnit Bluetooth Mode

The video system has a Bluetooth interface that can be used for short range voice transmission. You can connect a Bluetooth wireless headset to the video system via this interface. Only one headset can be used at a time.

The Bluetooth version 2.1 headset profile is supported. The following functions are included: answer, volume up, volume down and hang up.

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* The Bluetooth radio interface is switched on and can be used to communicate with a Bluetooth wireless headset.

*Off:* The Bluetooth radio interface is switched off and a Bluetooth wireless headset cannot be used.

**Example:** SystemUnit Bluetooth Mode: Off

### SystemUnit ContactInfo Type

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

### 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:** <On/Off>

*On:* Enable logging.

*Off:* Disable logging.

**Example:** SystemUnit CallLogging Mode: On



## 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 or the list of scheduled meetings on the Touch controller as default.

**Requires user role:** USER

**Value space:** <ContactList/MeetingList>

*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.

**Example:** UserInterface TouchPanel DefaultPanel: ContactList

### UserInterface TouchPanel DomainAutocomplete

When you are typing text in an address input field in order to call someone the string defined in this setting is automatically appended as soon as you tap "@".

For example, if you want to call "name@company.com" and you have defined the DomainAutocomplete string to be "company.com", you just have to enter "name" followed by "@" on the Touch controller in order to call the person. The domain-part of the address is automatically appended.

If you ignore the auto-completion and continue by typing another domain name, the auto-completion is overridden.

**Requires user role:** ADMIN

**Value space:** <S: 0, 256>

*Format:* String with a maximum of 256 characters.

**Example:** UserInterface TouchPanel DomainAutocomplete: "company.com"

## Video settings

### Video Input Source [1..3]/[1..2] Name

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

Enter a name for the video input source.

**Requires user role:** ADMIN

**Value space:** <S: 0, 50>

*Format:* String with a maximum of 50 characters.

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

### Video Input Source [1] Connector

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

**Requires user role:** ADMIN

**Value space:** <HDMI>/<DVI>

*HDMI (EX90):* Select HDMI when you want to use the HDMI as the video input source 1.

*DVI (EX60):* Select DVI when you want to use the DVI as the video input source 1.

**Example:** Video Input Source 1 Connector: HDMI

### Video Input Source [2] Connector

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

**Requires user role:** ADMIN

**Value space:** <DVI>/<CAMERA>

*DVI (EX90):* Select DVI when you want to use the DVI-I as input source 2.

*CAMERA (EX60):* Select CAMERA when you want to use the camera as input source 2.

**Example:** Video Input Source 2 Connector: DVI

### Video Input Source [3] Connector

NOTE: Applies to only EX90.

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

**Requires user role:** ADMIN

**Value space:** <CAMERA>

*CAMERA:* Select CAMERA when you want to use the camera as input source 3.

**Example:** Video Input Source 3 Connector: CAMERA

### Video Input Source [1..3]/[1..2] Type

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

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

**Requires user role:** ADMIN

**Value space:** <other/camera/PC/DVD/document\_camera>

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

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

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

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

*Document\_Camera:* Select Document\_Camera when you have a document camera connected to the selected video input.

**Example:** Video Input Source 1 Type: PC

### Video Input Source [1..3]/[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 the value is fixed for all input sources.

**Value space:** <On/Off>

*On:* Enable camera control.

*Off:* Disable camera control.

## Video Input Source [1..3]/[1..2] CameraControl Cameramd

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

**Value space:** <1>

*Range:* Indicates the ID of the camera.

## Video Input Source [1..3]/[1..2] OptimalDefinition Profile

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

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..3]/[1..2] OptimalDefinition Threshold60fps

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

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/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.

*Never:* Do not set a threshold for transmitting 60fps.

**Example:** Video Input Source 2 OptimalDefinition Threshold60fps: 1280\_720

## Video Input Source [1..3]/[1..2] Quality

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

When encoding and transmitting video there will be a trade-off between high resolution and high frame rate. For some video sources it is more important to transmit high frame rate than high resolution and vice versa. The Quality setting specifies whether to give priority to high frame rate or to high resolution for a given source.

**Requires user role:** ADMIN

**Value space:** <Motion/Sharpness>

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

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

**Example:** Video Input Source 2 Quality: Motion

## Video DefaultPresentationSource

NOTE: EX90 has Video Input Source [1..3] and EX60 has Video Input Source [1..2].

Define which video input source shall be used as the default presentation source (when you tap Presentation followed by Present on the Touch controller). The input source is configured to a video input connector.

**Requires user role:** USER

**Value space:** <1/2/3>/<1/2>

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

**Example:** Video DefaultPresentationSource: 1

## Video Input HDMI [1] RGBQuantizationRange

NOTE: Applies to only EX90.

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

**Requires user role:** ADMIN

**Value space:** <Auto/Full/Limited>

*Auto:* RGB quantization range is automatically selected based on the RGB Quantization Range bits (Q0, Q1) in the AVI infoframe. If no AVI infoframe is available, RGB quantization range is selected based on video format according to CEA-861-E.

*Full:* Full quantization range. The R, G, B quantization range includes all code values (0 - 255). This is defined in CEA-861-E.

*Limited:* Limited Quantization Range. R, G, B quantization range that excludes some code values at the extremes (16 - 235). This is defined in CEA-861-E.

**Example:** Video Input HDMI 1 RGBQuantizationRange: Auto

## 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 DVI 1 RGBQuantizationRange: Full

## Video Input DVI [1] Type

NOTE: EX90 has the DVI 2 input connector and EX60 has the DVI 1 input connector.

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 MainVideoSource

Define which video input source shall be used as the main video source. This value is fixed in this product.

**Value space:** EX90: <3>, EX60: <2>

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

## 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:** <On/Off>

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

*Off:* Capturing web snapshots is not allowed.

**Example:** Video AllowWebSnapshots: Off

## Video Output HDMI [1] CEC Mode

NOTE: Applies to only EX90.

The HDMI outputs support Consumer Electronics Control (CEC). When set to on (off is default), and the monitor connected to the HDMI output is CEC compatible and CEC is configured, the system will use CEC to set the monitor in standby when the system enters standby. Likewise the system will wake up the monitor when the system wakes up from standby. Please note that the different manufacturers uses different marketing names for CEC: Anynet+ (Samsung); Aquos Link (Sharp); BRAVIA Sync (Sony); HDMI-CEC (Hitachi); Kuro Link (Pioneer); CE-Link and Regza Link (Toshiba); RIHD (Onkyo); SimpLink (LG); HDAVI Control, EZ-Sync, VIERA Link (Panasonic); EasyLink (Philips); and NetCommand for HDMI (Mitsubishi).

**Requires user role:** ADMIN

**Value space:** <On/Off>

*On:* Enable CEC control.

*Off:* Disable CEC control.

**Example:** Video Output HDMI 1 CEC Mode: Off

## Video Output HDMI [1] MonitorRole

NOTE: Applies to only EX90, and only when the Dual Display option is installed.

Define which video stream to show on the monitor connected to the HDMI output connector. The value is fixed for this product.

**Value space:** <Second>

*Second:* Show the presentation, if present, on the monitor connected to the HDMI output.

## Video Output HDMI [1] OverscanLevel

NOTE: Applies to only EX90.

Some TVs or other monitors may not display the whole image sent out on the systems video output, but cuts the outer parts of the image. In this case this setting can be used to let the system not use the outer parts of video resolution. The video will be scaled in this case.

**Requires user role:** ADMIN

**Value space:** <Medium/High/None>

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

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

*None:* The system will use all of the output resolution.

**Example:** Video Output HDMI 1 OverscanLevel: None

## Video Output HDMI [1] Resolution

NOTE: Applies to only EX90.

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

**Requires user role:** ADMIN

**Value space:** <Auto/640\_480\_60/800\_600\_60/1024\_768\_60/1280\_1024\_60/1280\_720\_60/1920\_1080\_60/1280\_768\_60/1360\_768\_60/1366\_768\_60/1600\_1200\_60/1920\_1200\_60>

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

*Range:* 640x480@60p, 800x600@60p, 1024x768@60p, 1280x1024@60p, 1280x720@60p, 1920x1080@60p, 1280x768@60p, 1360x768@60p, 1366x768@60p, 1600x1200@60p, 1920x1200@60p

**Example:** Video Output HDMI 1 Resolution: 1920 \_ 1080 \_ 60

## Video Output LCD [2]/[1] Resolution

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the screen resolution.

**Requires user role:** ADMIN

**Value space:** EX90: <1920\_1200\_60> EX60: <1920\_1080\_60>

*Range:* The screen resolution is 1920 x 1200 60 Hz for EX90 and 1920 x 1080 60 Hz for EX60.

**Example:** Video Output LCD 2 Resolution: 1920 \_ 1200 \_ 60

## Video Output LCD [2]/[1] MonitorRole

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the LCD monitor role. The value is fixed for this product.

**Value space:** <InternalSetup>

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



### Video Output LCD [2]/[1] Brightness

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

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 [2]/[1] Red

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

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 [2]/[1] Green

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

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 [2]/[1] Blue

NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

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 [3]/[2] MonitorRole

NOTE: EX90 has Internal 3 and EX60 has Internal 2.

Determine the role of the internal monitor and choose where to show the video stream and presentation. The value is fixed for this product.

**Value space:** <First>

*First:* Show the main video stream and presentation on the internal monitor. For EX90, the presentation may be shown on a second monitor connected to the HDMI output (see the Video Output HDMI 1 MonitorRole setting).

### Video Selfview

Determine if the main video source (self view) shall be displayed on screen.

**Requires user role:** USER

**Value space:** <On/Off>

*On:* Display self view on screen.

*Off:* Do not display self view on screen.

**Example:** Video Selfview: On

### Video WallPaper

Select a background image (wallpaper) for the video screen when idle. A corresponding background image will be applied to the Touch controller.

**Requires user role:** USER

**Value space:** <None/Custom/Wallpaper01/Wallpaper02/Wallpaper03/Wallpaper04/Wallpaper05/Wallpaper06/Wallpaper07/Wallpaper08/Wallpaper09/Wallpaper10/Wallpaper11/Wallpaper12>

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

*Wallpaper01 to Wallpaper12:* The chosen background image is shown on both the video screen and the Touch controller.

*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.

**Example:** Video Wallpaper: Wallpaper01

## 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 and command line interfaces 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 contact your Cisco representative 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 choose [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 on 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 system.**

You have to issue a command from the command line interface to set the menu password; neither the Touch controller nor the web interface can be used.

### Setting the menu password

1. Connect to the system through the network or its serial data port (if available) and open a command line interface (SSH or Telnet).  
See below how to find the system's IP address.
2. Sign in to the system with user name and password. The user needs ADMIN rights.
3. Type the following command:

```
xCommand SystemUnit MenuPassword Set Password:  
<password>
```

The password format is a string with 0-255 characters.



To find the system's IP address tap [Settings \(⌘\)](#) > [System Information](#) on the Touch controller.

## APPENDICES

The appendices section provides you with additional information that you may find useful as a system administrator for the EX60/EX90.





## Audio outputs and microphones

The EX90/EX60 offers the choice of four audio outputs:

- Built-in loudspeaker
- Headset (wired)
- Bluetooth headset (wireless)
- Handset on Touch controller

Available microphone options depends on the chosen audio output.

### Microphone input / external microphone

The microphone input at the rear of the video system may only be used for one of the following options:

- Headset microphone
- Cisco TelePresence Table Microphone 20 (external microphone)







Other microphone types are not supported.

Note that the video system's internal microphone is disabled when a headset microphone or an external microphone is connected.

### Headset output / external loudspeakers

The headset output is for headsets only. You should not connect external loudspeakers to the headset output.

## Choosing audio output and microphone

To select an audio output, tap the [Audio output selector](#) (, , , ) and choose **Speaker**, **Headset**, **Bluetooth** or **Handset**.



### Speaker

As a default, the built-in loudspeaker is used together with the internal microphone.

If an external microphone is connected, the internal microphone is disabled and the external microphone will be used instead.



### Headset (wired)

Connect the headset to the headset output at the rear of the system. If the headset has an in-built microphone, connect it to the microphone input.

If the headset comes without a microphone, either the internal microphone or, if connected, the external microphone is used.

If you have connected both a wired headset and a Bluetooth headset, only the Bluetooth headset will be available in the selector.



### Bluetooth headset (wireless)

Use the Touch controller to pair the headset with the video system (tap [Settings](#) (✕) > [Bluetooth Headset](#) and set-up the connection).

The headset's microphone will be used.



### Handset

The handset is automatically selected when you lift it off the hook.

Only the microphone in the handset is enabled. Neither the internal microphone nor an external microphone can be used.

Note that only the available options are shown, i.e. if you have not connected a headset (neither wired nor wireless), and you have not lifted the handset off the hook, only Speaker is present in the selector.





## 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 Advanced 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 Advanced 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 Advanced 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 [Advanced 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.

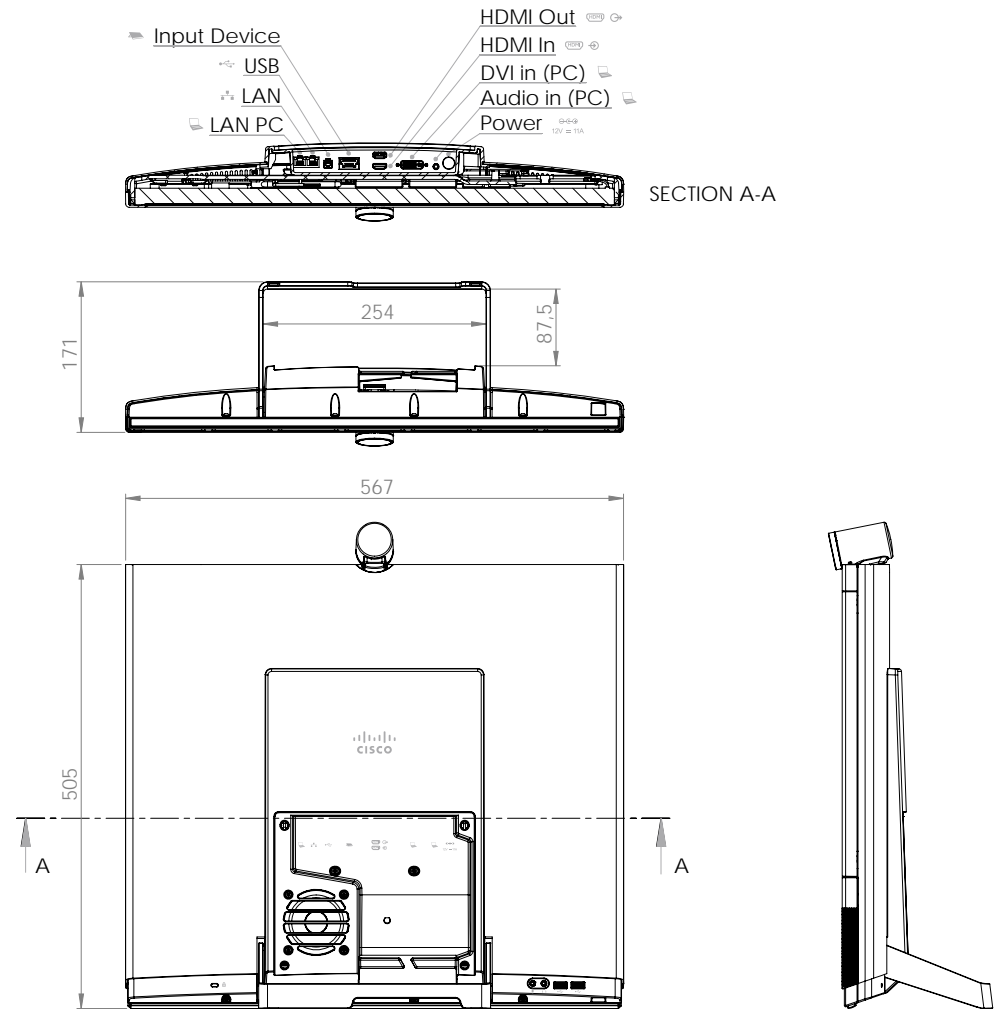
Go to Advanced configuration (on the web interface):

- Navigate to [Conference 1 > PacketLossResilience > Mode](#)

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

## EX90 dimensions

The illustration shows the EX90 dimensions.

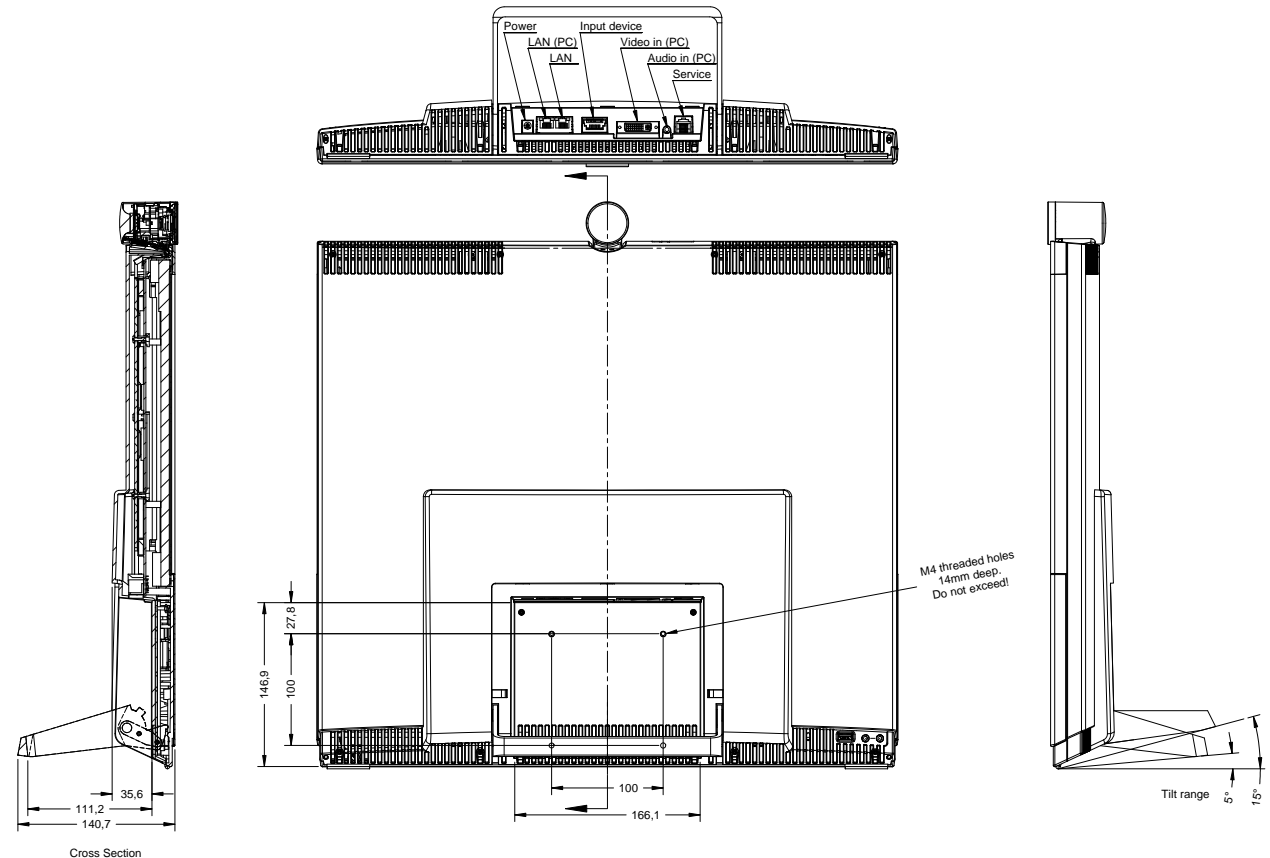


All dimensions are in mm.  
 EX90 weight: 11 kg (24.2lb)

## EX60 dimensions - wall mounting and arm mounting

The EX60 can be attached to a variety of 100 mm × 100 mm VESA compatible wall mounts and arms.

When choosing a mounting solution, consider the mounting pattern, the EX60 dimensions and obstructions; not all VESA compatible products will easily fit with the EX60.



All dimensions are in mm.

EX60 weight: 5.85 kg (12.9 lb)

## Factory reset

You can use the video system's power button, the Touch controller or the web interface to reset the system to its default factory settings.

When factory resetting the video system the following happens:

- The call logs will be deleted.
- All system parameters will be reset to default values.
- All files that have been uploaded to the system will be deleted.
- The Release and Option keys will be preserved.
- Automatic restart of the system.



It is not possible to undo a factory reset.

### Touch

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

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

The system will confirm 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 check the *I want to reset...* check box
4. Click *Perform a factory reset*.

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

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

### Power button

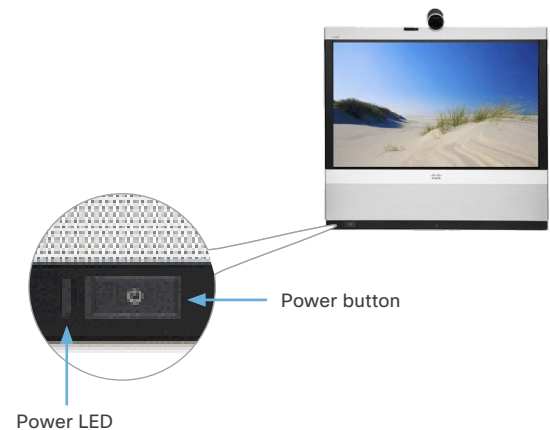
1. Power down the system by pressing gently and holding the power button until the system shuts down (the power LED turns off).
2. Press gently and hold the power button for 10 seconds. During this period the power LED will remain off.
3. Within four seconds after the LED starts blinking, press the power button twice.

When the LED lights continuously, the system will revert to the default factory settings and automatically restart.

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



If you failed to press the power button twice within the four seconds, the system will not revert to the default factory settings, and you will not see the confirmation message. If this happens, go back to step 1 and try again.



## Technical specifications

The EX90/EX60 units are delivered with a fully integrated codec, display, camera, microphone and loudspeakers, and a Touch controller with a detachable wide band handset.



When running software version TE6.0 the following limitations apply:

- Only the SIP call protocol is supported
- Only registration to CUCM is supported

This implies that TE6.0 does not support all non-CUCM features from earlier TC software releases. Full non-CUCM feature parity with TC software will be introduced in TC6.0 and beyond.

### PRODUCT COMPATIBILITY

- Fully compatible with standards-compliant telepresence and video systems

### SOFTWARE COMPATIBILITY

#### EX90:

- Cisco TelePresence Software Version TC3.1 or later, and TE6.0

#### EX60:

- Cisco TelePresence Software Version TC4.0 or later, and TE6.0

### COMPONENTS

- Fully integrated unit including codec, display, camera, microphone and loudspeakers
- Cables including: VGA-to-DVI-I cable, DVI-D cable, 3.5 mm jack audio cable, LAN cable, power adapter, and power cable

### DISPLAY

#### EX90:

- 24 in. LCD monitor
- Resolution: 1920 × 1200 (16:10)
- Contrast ratio: 1000:1
- Viewing angle: 160°
- Response time: 5 ms
- Brightness: 300 cd/m<sup>2</sup>
- 5° - 15° tilt

#### EX60:

- 21.5 in. LCD monitor (with LED backlight)
- Resolution: 1920 × 1080 (16:9)
- Contrast ratio: 1000:1
- Viewing angle: 170°
- Response time: 5 ms
- Brightness: 225 cd/m<sup>2</sup>

### CAMERA

- Cisco TelePresence PrecisionHD design
- Resolutions: 1080p30 and 720p60
- Auto focus
- Integrated privacy shutter
- Document camera mode
- Multicoated all-glass optics
- 1/3-in., 2.1 megapixel CMOS sensor

#### EX90:

- Horizontal field of view: 45°-65°
- Vertical field of view: 40°-27°
- Focus distance 0.3-infinity
- Optical, motorized zoom

#### EX60:

- Horizontal field of view: 50°
- Vertical field of view: 29°
- Focus distance 0.1-infinity

### AUDIO SYSTEM

- Two stereo front speakers
- Integrated full-range microphone
- One 3.5 mm line-in jack for PC or other audio source
- Two 3.5 mm jack for headset
- Wideband handset
- Bluetooth module 2.1 + EDR

#### Only EX90:

- Integrated subwoofer
- Support for Cisco TelePresence Table Microphone 20
- HDMI audio input/output

### PC AND SECOND SOURCE VIDEO INPUT

#### EX90:

- DVI-I
- HDMI In

#### EX60:

- DVI-I

### SUPPORTED PC INPUT RESOLUTIONS

#### EX90:

- SVGA (800 × 600) to WUXGA (1920 × 1200)

#### EX60:

- SVGA (800 × 600) to 1080p (1920 × 1080)

### USER INTERFACE

- Cisco TelePresence Touch 8 controller
- Eight-inch projected capacitive touch screen
- Resolution: 800 × 480

### LANGUAGE SUPPORT

- Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese-Brazilian, Russian, Simplified Chinese, Spanish, Swedish

### POWER

- Autosensing power supply
- 100-240 VAC, 50/60 Hz

#### EX90:

- 150 W max

#### EX90 with Touch 8:

- In video call: 110 W
- In standby: 58 W

#### EX60:

- 75 W max

#### EX60 with Touch 8:

- In video call: 46 W
- In standby: 31 W

## OPERATING TEMPERATURE AND HUMIDITY

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

## MAIN UNIT DIMENSIONS

### EX90:

- Height: 54.5 cm (21.4 in.)
- Length: 56.7 cm (22.3 in.)
- Depth: 17.3 cm (6.8 in.)
- Weight: 11.0 kg (24.2 lb)

### EX60:

- Height: 50.8 cm (20.0 in.)
- Length: 52.0 cm (20.5 in.)
- Depth: 13.8 cm (5.4 in.)
- Weight: 5.85 kg (12.9 lb)

## TOUCH SCREEN DIMENSIONS

### Without handset:

- Height: 4.4 cm (1.7 in.)
- Length: 22.8 cm (9.0 in.)
- Depth: 14.5 cm (5.7 in.)
- Weight: 0.64 kg (1.4 lb)
- Cable length: 120 cm (47 in.)

### With handset:

- Height: 7.7 cm (3.0 in.)
- Length: 29.0 cm (11.4 in.)
- Depth: 18.7 cm (7.4 in.)
- Weight: 0.94 kg (2.1 lb)
- Cable length: 120 cm (47 in.)

## BANDWIDTH

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

## AUDIO STANDARDS

- G.711, G.722, G.722.1, 64/128 kbps MPEG4 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

### EX90:

- Supports resolutions up to 1080p in both main stream and dual stream simultaneously

### EX60:

- Supports resolutions up to 720p in both main stream and dual stream simultaneously

## 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 × 144@30 fps (QCIF)
- 352 × 288@30 fps (CIF)
- 512 × 288@30 fps (w288p)
- 576 × 448@30 fps (448p)
- 768 × 448@30 fps (w448p)
- 704 × 576@30 fps (4CIF)
- 1024 × 576@30 fps (w576p)
- 640 × 480@30 fps (VGA)
- 800 × 600@30 fps (SVGA)
- 1024 × 768@30 fps (XGA)
- 1280 × 1024@30 fps (SXGA)
- 1280 × 720@30 fps (720p30)
- 1280 × 768@30 fps (WXGA)
- 1920 × 1080@30 fps (1080p30)\*
- 1440 × 900@30 fps (WXGA+)\*
- 1472 × 1080@30 fps (SXGA+)\*
- 1680 × 1050@30 fps (WSXGA+)\*
- 1600 × 1200@30 fps (UXGA)\*
- 512 × 288@60 fps (w288p60)\*
- 768 × 448@60 fps (w448p60)\*
- 1024 × 576@60 fps (w576p60)\*
- 1280 × 720@60 fps (720p60)\*

### Only EX90:

- 1920 × 1200@25fps (WUXGA)\*

\* Requires premium resolution option

## PROTOCOLS

- H.323
- SIP

## NETWORK INTERFACES

- Internal 2-port Ethernet switch
- 1 × LAN/Ethernet (RJ-45) 10/100/1000 Mbit for PC
- 1 × LAN/Ethernet (RJ-45) 10/100/1000 Mbit for LAN

## OTHER INTERFACES

- Bluetooth

### EX90:

- 2 × USB device for future applications

### EX60:

- 1 × USB device for future applications

## IP NETWORK FEATURES

- Domain Name System (DNS) lookup for service configuration
- Differentiated Services (QoS)
- IP adaptive bandwidth management (including flow control)
- Auto gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 DTMF tones in H.323
- Date and time support 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 (CoS)
- ClearPath

## 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, autoconfiguration (stateless address autoconfiguration) and DHCPv6

## FIREWALL TRAVERSAL

- Cisco TelePresence Expressway Technology
- H.460.18 and H.460.19 Firewall Traversal

#### EMBEDDED ENCRYPTION

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

#### SECURITY FEATURES

- Management via Secure HTTP (HTTPS) and Secure Shell (SSH) protocol
- IP administration password
- Administrator menu 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)

#### Only EX90:

- Four-way embedded SIP/H.323 MultiPoint, reference MultiSite

#### MULTISITE

(embedded multipoint switch)

#### Only EX90:

- 4-way 720p30 Continuous Presence (CP) MultiSite
- Full individual audio and video transcoding
- Individual layouts for each participant (CP layout without self view feature)
- H.323/SIP/VoIP in the same conference
- Best Impression (Automatic CP layouts)
- H.264, encryption and dual stream from any site
- IP downspeeding
- Dial in/Dial out

#### SUPPORTED INFRASTRUCTURE

- Cisco Unified Communications Manager 8.6.2 and newer
- Cisco TelePresence Video Communication Server (Cisco VCS)
- Cisco WebEx TelePresence Server

#### SYSTEM MANAGEMENT

- Support for the Cisco TelePresence Management Suite
- 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 (SCP), 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

#### MTBF PRODUCT RELIABILITY/MTBF

The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:

- Power On Hours (POH) > 69 000 hours.
- Useful Life Cycle > 6 years.

ISO 9001 certificate is available upon request

#### APPROVALS

##### EU/EEC

Directive 2006/95/EC (Low Voltage Directive)

- Standard EN 60950-1

Directive 2004/108/EC (EMC Directive)

- Standard EN 55022, Class A
- Standard EN 55024
- Standard EN 61000-3-2/-3-3

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.

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

November 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 2396 Uniform Resource Identifiers (URI): Generic Syntax
- RFC 2429 RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)
- 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 3047 RTP Payload Format for ITU-T Recommendation G.722.1
- 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 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 4028 Session Timers in SIP
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4235 An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol
- draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4583 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- draft-ietf-bfcpbis-rfc4583bis-00 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4587 RTP Payload Format for H.261 Video Streams
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5104 Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)
- RFC 5168 XML Schema for Media Control
- RFC 5589: SIP Call Control Transfer
- RFC 5626 Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)
- 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 EX Series, this is the path you have to follow:

*TelePresence >*

*TelePresence Endpoints - Personal >*

*TelePresence Desktop >*

*Cisco TelePresence Systems EX Series*

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

► <http://www.cisco.com/go/ex-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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

TANDBERG is now a part of Cisco. TANDBERG® is a registered trademark belonging to Tandberg ASA.

### Cisco contacts

On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ► <http://www.cisco.com/web/siteassets/contacts>

Corporate Headquarters  
Cisco Systems, Inc.  
170 West Tasman Dr.  
San Jose, CA 95134 USA