Cisco TelePresence MX200

ADMINISTRATOR GUIDE

- MX200

Software version TC4.2
JULY 2011

Thank you for choosing Cisco!

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

This part of the product documentation is aimed at administrators working with the setup of the MX200.

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

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

The user documentation can be found on
‣ http://www.cisco.com/go/telepresence/docs.

How to use this guide

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

Table of contents

Chapter 1

Introduction

Intellectual property rights

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

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

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

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

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

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

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

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

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

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

Products covered in this guide

- Cisco TelePresence MX200

User documentation

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

- Video conference room primer
- Video conference room acoustics guidelines
- Installation guide for Cisco TelePresence MX200
- Getting started guide for the Cisco TelePresence systems
- Software release notes for the TC software
- User guide for the TelePresence systems (with Touch controller)
- Quick reference guides for the TelePresence systems
- Administrator guide for Cisco TelePresence MX200
- Regulatory compliance and safety information guide
- Legal & license information for products using TC software

Downloading the user documentation

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

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

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

Software

You can download the software for your product from the Cisco web site, go to:

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

Cisco contacts

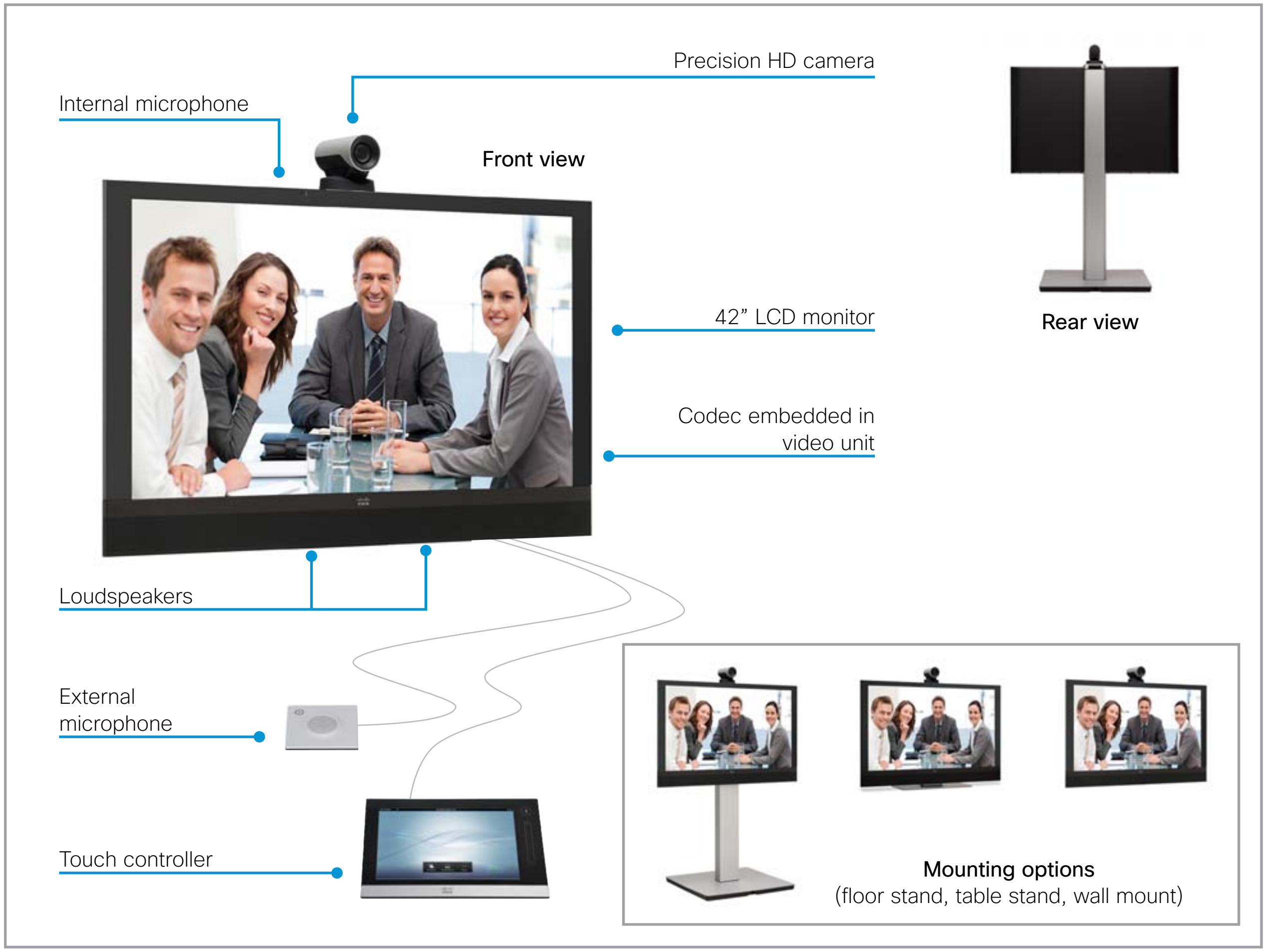
On our web site you will find an overview of the worldwide Cisco contacts.

Go to: ▸ http://www.cisco.com/web/siteassets/contacts

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

Cisco TelePresence MX200 at a glance

The Cisco TelePresence® MX200 makes telepresence more accessible to teams everywhere with ready-to-use simplicity and high quality. This highly integrated telepresence system is easy to install, so you can quickly transform any meeting space into a video-enabled team room. Whether you are just getting started with video communications or implementing a large-scale deployment, the Cisco TelePresence MX200 delivers high quality performance in a simple and intuitive way.



Features and benefits

- The system is easy to install–one piece plus floor stand, table stand, or wall mount brackets (VESA mount).
- The system is self-configuring with Cisco TelePresence Management Suite (TMS), or Cisco Callway provisioning. All you need is to authenticate your endpoint to the network.
- PrecisionHD camera with pan, tilt, and 4x optical zoom helps ensure optimal framing and video clarity.
- Dedicated camera presets provide flexibility and easy viewing for any meeting scenario.
- The 8-inch Touch interface offers simple control.
- Video resolutions of 1080p30 and 720p60 bring premium telepresence experience to any meeting room or office.
- The high-quality 42-inch display with 1920 x 1080 resolution enables clear images.
- You can easily connect and share your PC content at WXGA and 720p30 resolution and frame rate.
- The system supports H.323 and Session Initiation Protocol (SIP) with bandwidth up to 6 Mbps point-to-point.
- Two front speakers provide superior audio quality.
- The system is standards-based.
- Capabilities for large conferences and transparent escalation from point-to-point to multipoint calls using the Cisco TelePresence Multiway™ technology.

Chapter 2

The web interface

Connecting to the video conference system

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

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

This section describes the web interface functions and how you can use them for system configuration and maintenance.

Starting to use the web interface

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

   To find the IP address, open the System Information page on the Touch controller. Tap the icons *More > Settings*, select *System Information* and find the *IPv4 Address* or *IPv6 Address*.

2. Enter your user name and password 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).

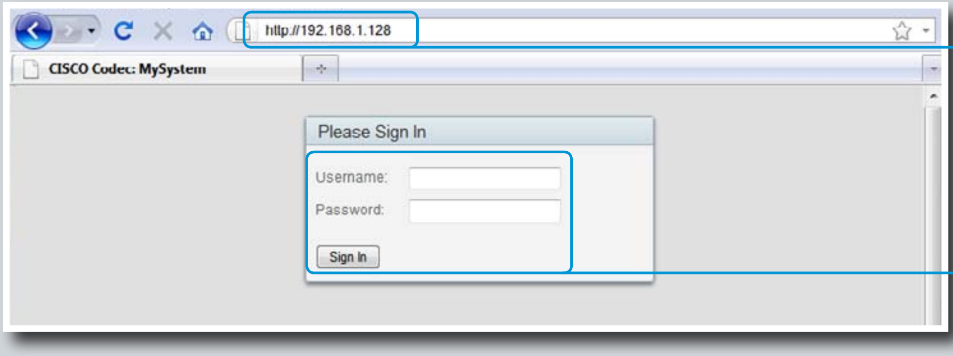
3. To sign out, click your user name and select *Sign out* from the drop down menu.

About password protection

You sign in to the web interface with the same user name and password as for the video conference system.

NOTE: We strongly recommend that you set a password for the admin user to restrict access to system configuration.

Read more about password protection in the ▸ Setting passwords appendices in this guide.

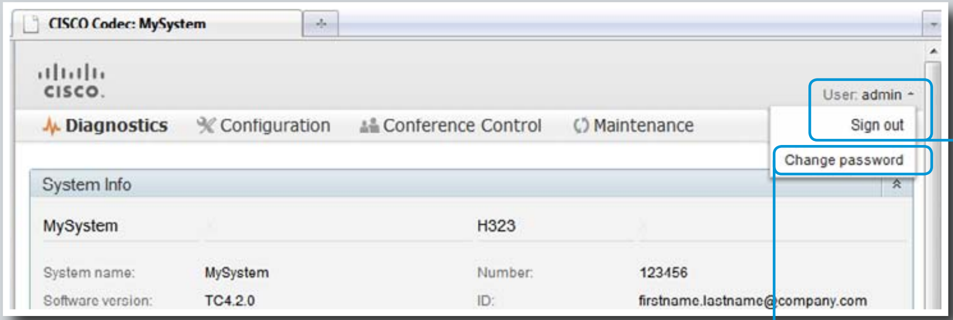


1. Connect

Enter the IP address of the video system.

2. Sign in

Enter the user name and password and press *Sign in*.



MySystem H323

System name: MySystem Number: 123456
Software version: TC4.2.0 ID: firstname.lastname@company.com

3. Sign out

Click on your user name and select *Sign out*.

Change your password

Click on your user name and select *Change password*.

The interactive menus

When you have signed in to the system the main menu appears near the top of the page.

When you hover the mouse over a menu item, the names of the related sub-menus appear. When you click a sub-menu name the corresponding web page opens. These web pages are described on the following pages.

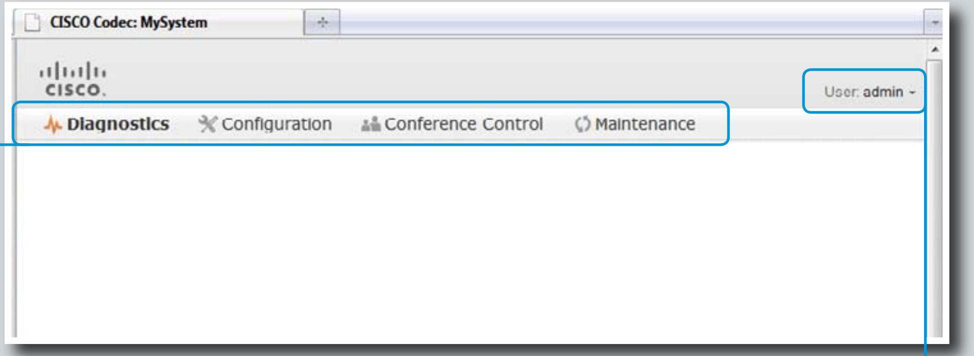
Menu availability and user roles

A user account possesses one or more user roles. Three user roles are defined: ADMIN, AUDIT and USER. Note that the default admin user holds all three roles. [1]

The table below shows which menus are available for users holding the different roles.

	ADMIN	AUDIT	USER
Diagnostics			
System Information	✓	✓	✓
Logs	✓		
XML Files	✓		
Snapshot (not available for MX200)	✓		
Configuration			
Advanced Configuration	✓	✓	
Wallpaper	✓	✓	
Sign In Banner	✓		
Conference Control			
Call			✓
Maintenance			
Upgrade Software	✓		
Certificate Management	✓		
Audit Certificate		✓	
User Administration	✓		
Change Password	✓	✓	✓
Restart			✓

[1] You can read more about user administration and user roles in the ▸ User administration section.



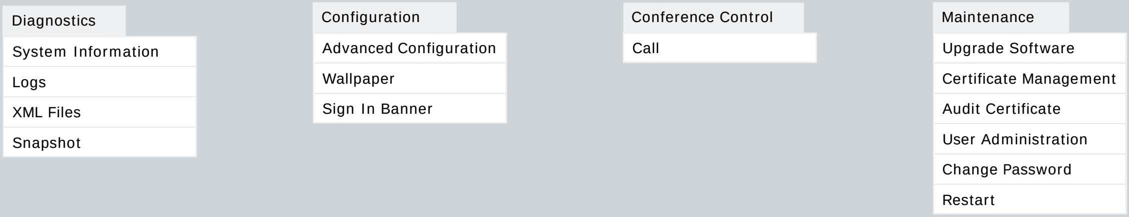
Main menu

- Diagnostics
- Configuration
- Conference Control
- Maintenance

The signed in user

Click on your user name to change your password or sign out.

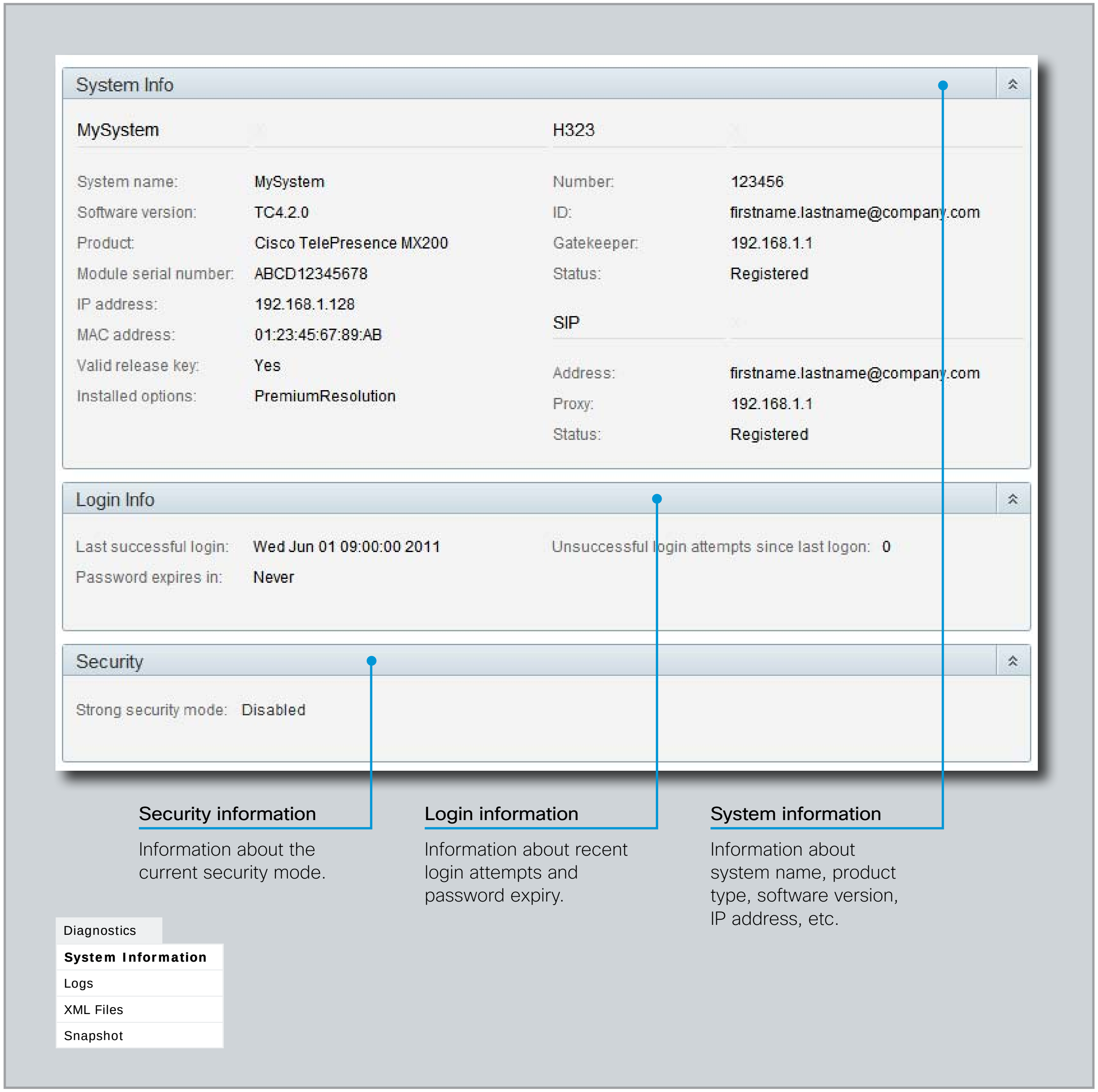
When you hover the mouse over a main menu item, the related sub-menus are shown. [2]



[2] The illustration lists all the sub-menus. A user *not* possessing all user roles will only see the sub-set relevant for his type of user.

The system information page

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



System Info

MySystem

System name: MySystem
Software version: TC4.2.0
Product: Cisco TelePresence MX200
Module serial number: ABCD12345678
IP address: 192.168.1.128
MAC address: 01:23:45:67:89:AB
Valid release key: Yes
Installed options: PremiumResolution

H323

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

SIP

Address: firstname.lastname@company.com
Proxy: 192.168.1.1
Status: Registered

Login Info

Last successful login: Wed Jun 01 09:00:00 2011
Password expires in: Never
Unsuccessful login attempts since last logon: 0

Security

Strong security mode: Disabled

Security information

Information about the current security mode.

Login information

Information about recent login attempts and password expiry.

System information

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

Log files

The log files are Cisco specific debug files which may be requested by the Cisco support organization if you need technical support.

Current log files

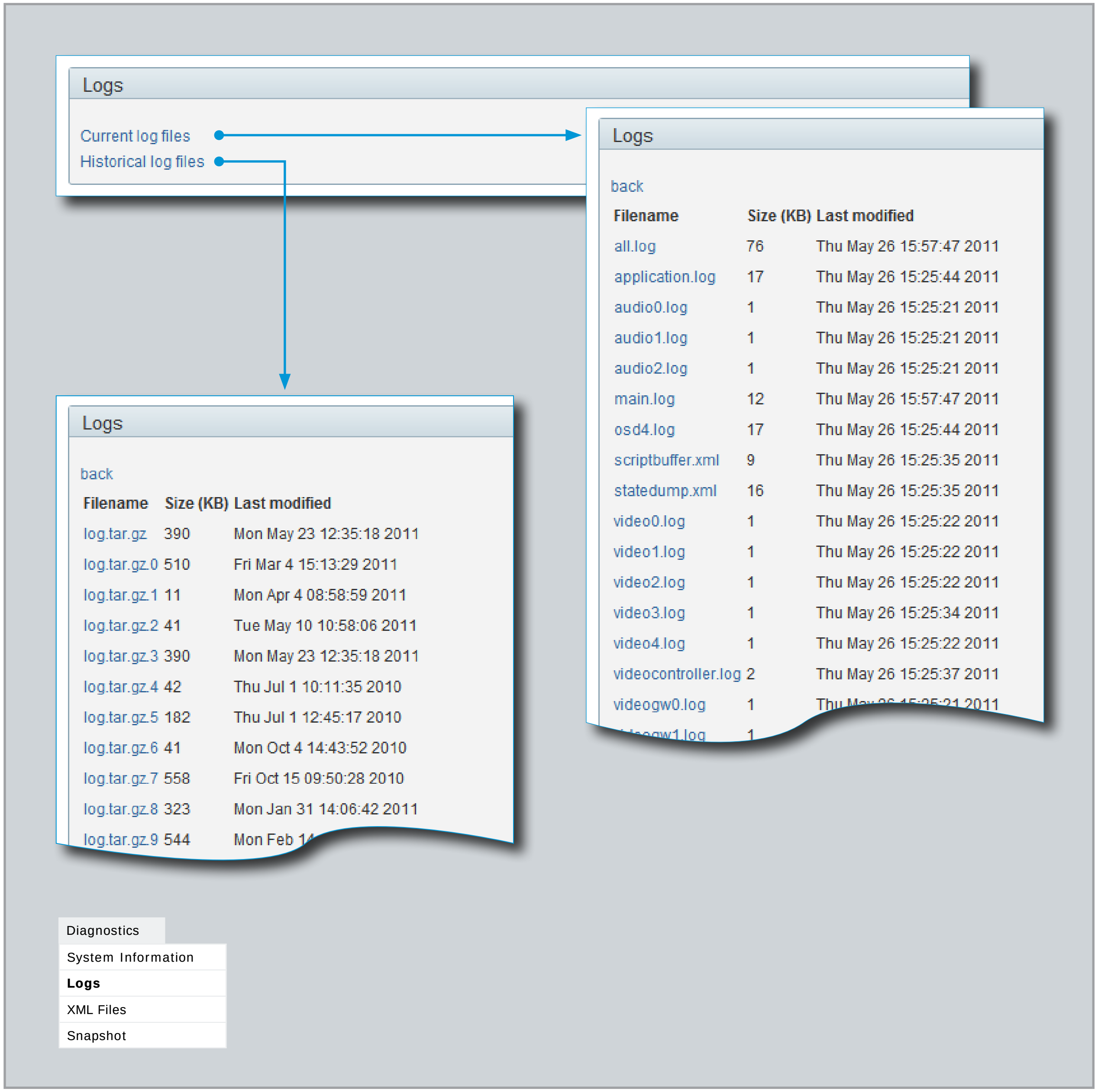
The current log files are time stamped event log files.

Select *Current log files,* and click on a log file to view or save the file (left or right click depending on your browser). Follow the instructions in the dialog box to save or open the file.

Historical log files

These are time stamped historical log files.

Select *Historical log files*, and click on a log file to view or save the file (left or right click depending on your browser). Follow the instructions in the dialog box to save or open the file.



Logs

Current log files
Historical log files

Logs

back

Filename	Size (KB)	Last modified
all.log	76	Thu May 26 15:57:47 2011
application.log	17	Thu May 26 15:25:44 2011
audio0.log	1	Thu May 26 15:25:21 2011
audio1.log	1	Thu May 26 15:25:21 2011
audio2.log	1	Thu May 26 15:25:21 2011
main.log	12	Thu May 26 15:57:47 2011
osd4.log	17	Thu May 26 15:25:44 2011
scriptbuffer.xml	9	Thu May 26 15:25:35 2011
statedump.xml	16	Thu May 26 15:25:35 2011
video0.log	1	Thu May 26 15:25:22 2011
video1.log	1	Thu May 26 15:25:22 2011
video2.log	1	Thu May 26 15:25:22 2011
video3.log	1	Thu May 26 15:25:34 2011
video4.log	1	Thu May 26 15:25:22 2011
videocontroller.log	2	Thu May 26 15:25:37 2011
videogw0.log	1	Thu May 26 15:25:21 2011
videogw1.log	1	

Logs

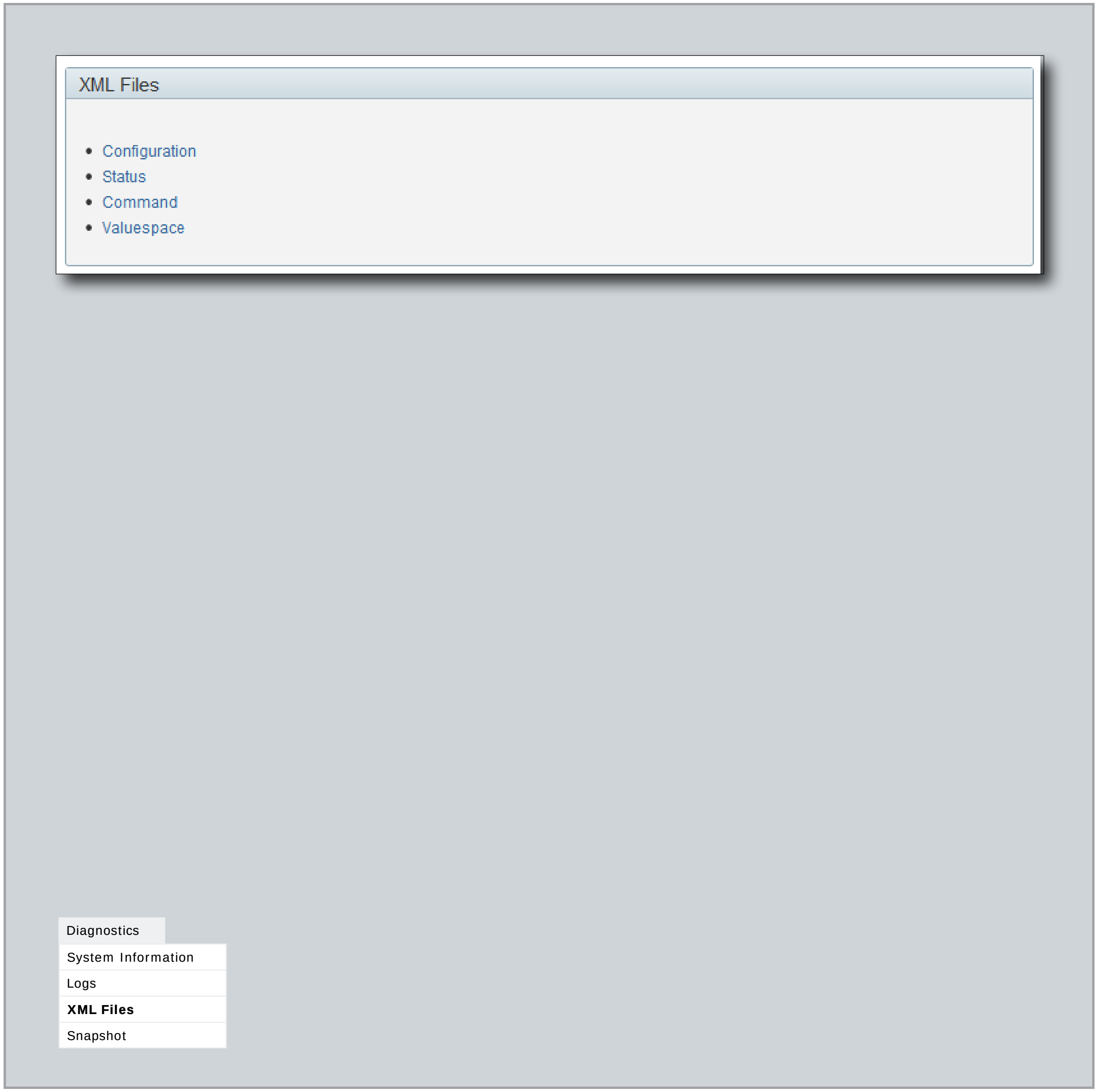
back

Filename	Size (KB)	Last modified
log.tar.gz	390	Mon May 23 12:35:18 2011
log.tar.gz.0	510	Fri Mar 4 15:13:29 2011
log.tar.gz.1	11	Mon Apr 4 08:58:59 2011
log.tar.gz.2	41	Tue May 10 10:58:06 2011
log.tar.gz.3	390	Mon May 23 12:35:18 2011
log.tar.gz.4	42	Thu Jul 1 10:11:35 2010
log.tar.gz.5	182	Thu Jul 1 12:45:17 2010
log.tar.gz.6	41	Mon Oct 4 14:43:52 2010
log.tar.gz.7	558	Fri Oct 15 09:50:28 2010
log.tar.gz.8	323	Mon Jan 31 14:06:42 2011
log.tar.gz.9	544	Mon Feb 14

XML files

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

- Select *Configuration* to see an overview of the system settings, which are controlled from the web interface or from the API (Application Programmer Interface).
- The *Status* information is constantly updated by the system to reflect system and process changes. The status information is normally monitored from the API.
- Select *Command* to see an overview of the commands available to instruct the system to perform an action. The commands are issued from the API.
- Select *Valuespace* to see an overview of the value spaces.



XML Files

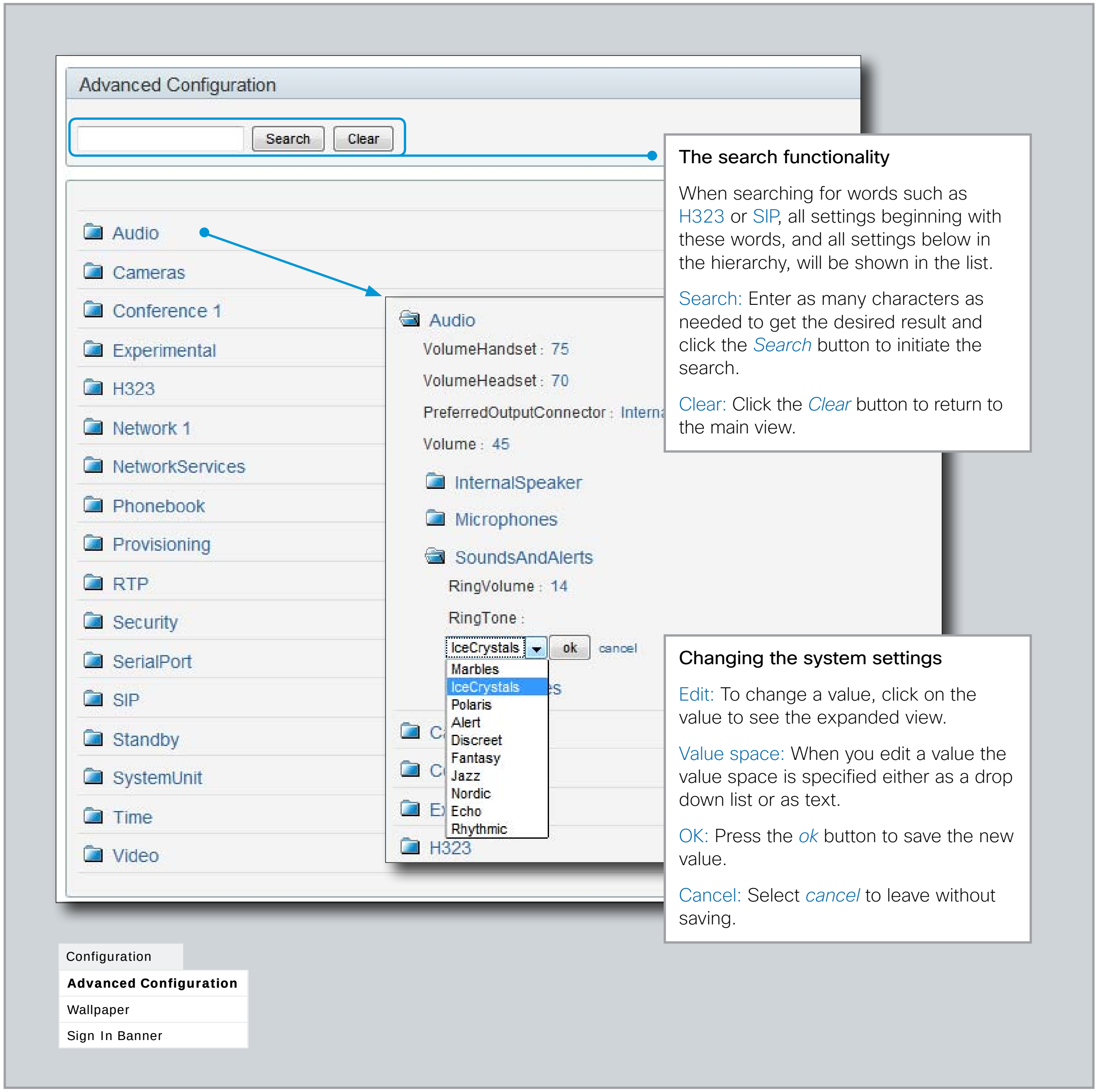
- Configuration
- Status
- Command
- Valuespace

Advanced configuration

The web interface allows for remote administration of the system.

The system settings are structured in a hierarchy, and you can navigate to each setting. Click a folder to open or close it, and change a value as explained to the right.

Each system setting is further described in the ▸ Advanced settings chapter.



Audio

VolumeHandset : 75

VolumeHeadset : 70

PreferredOutputConnector : Interna

Volume : 45

RingVolume : 14

RingTone :

The search functionality

When searching for words such as H323 or SIP, all settings beginning with these words, and all settings below in the hierarchy, will be shown in the list.

Search: Enter as many characters as needed to get the desired result and click the *Search* button to initiate the search.

Clear: Click the *Clear* button to return to the main view.

Changing the system settings

Edit: To change a value, click on the value to see the expanded view.

Value space: When you edit a value the value space is specified either as a drop down list or as text.

OK: Press the *ok* button to save the new value.

Cancel: Select *cancel* to leave without saving.

Custom wallpaper

If you want the company logo or a custom picture to be displayed on the main screen, you may use a custom wallpaper.

NOTE: The custom wall paper applies to the main screen only and will not appear on the Touch controller. When you choose a new predefined wallpaper on the Touch controller, it will replace your custom wall paper.

File format and picture size

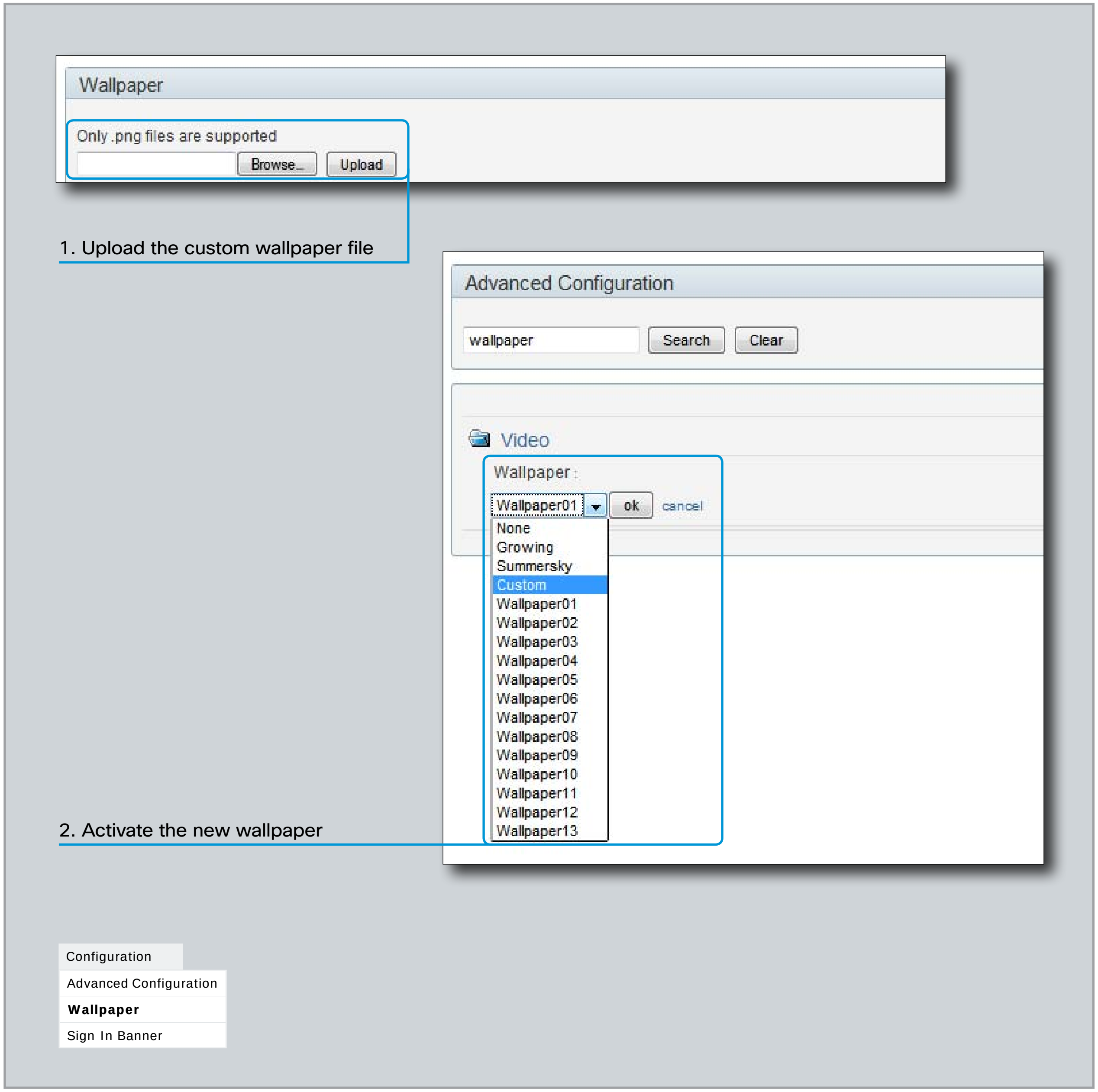
The picture file format for the custom wallpaper is PNG. The maximum size is 1920 × 1280 pixels.

Uploading the custom wallpaper file

1. Press *Browse...* and locate the wallpaper file (.PNG)
2. Press *Upload* to save the file to the codec.

Activating the new wallpaper

1. Go to the *Configuration* tab and open the the *Advanced Configuration* page. Enter `wallpaper` in the search field. From the drop down list, select *Custom*. The new wallpaper will be displayed on screen.



1. Upload the custom wallpaper file

2. Activate the new wallpaper

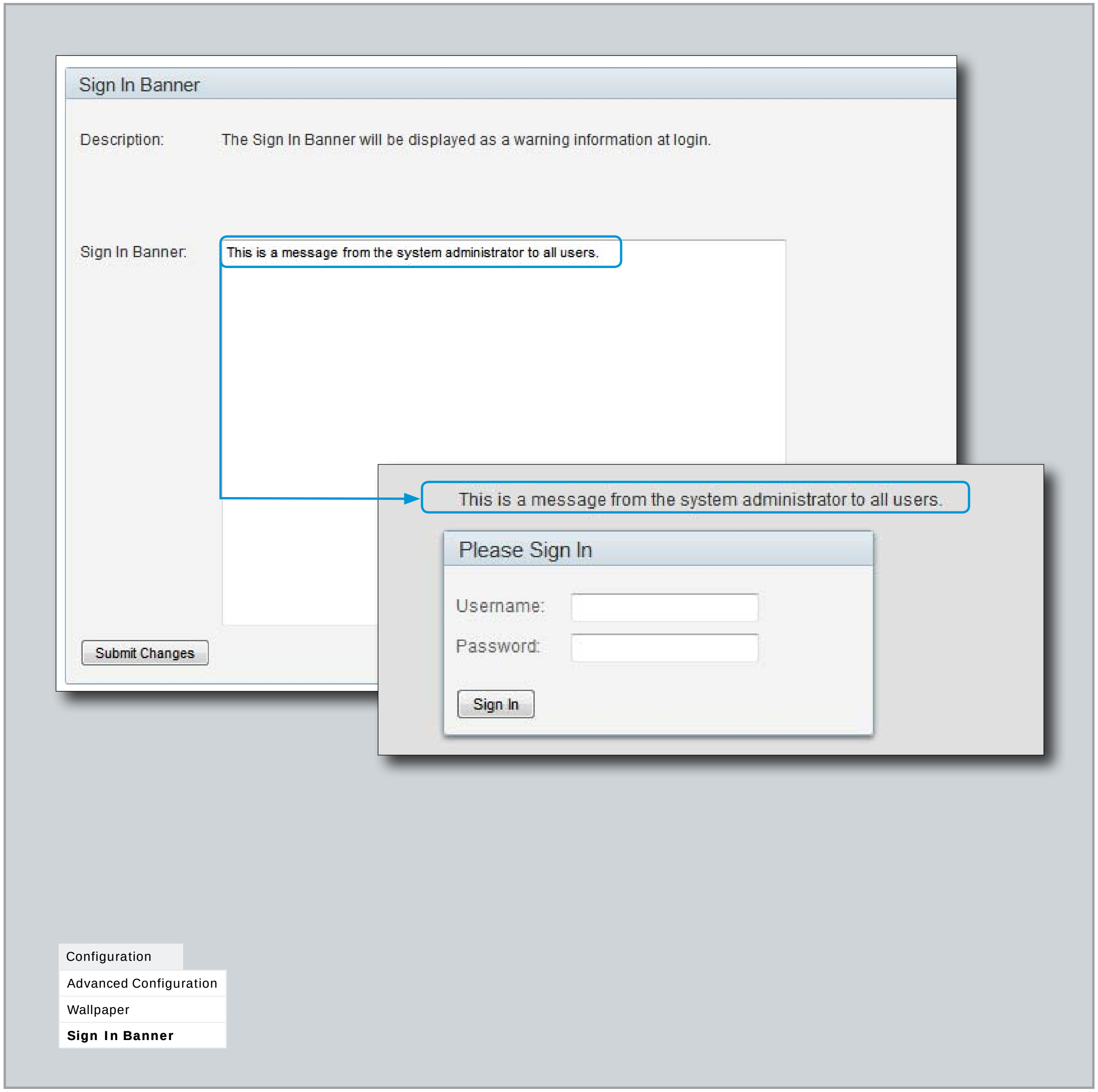
Sign in banner

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 using the menu system, the web interface or the command line interface.

Adding a sign in banner

1. Enter the text message, which you want to present to the user prior to signing in, in the *Sign In Banner* text area.
2. Press *Submit Changes* to activate the message.



Sign In Banner

Description: The Sign In Banner will be displayed as a warning information at login.

Sign In Banner: This is a message from the system administrator to all users.

This is a message from the system administrator to all users.

Please Sign In

Username:

Password:

Making a call from the web interface

Sometimes, e.g. when you are configuring the system from a remote location, it is convenient to be able to make calls from the video system to ensure everything works as expected.

Making a call

Input field: Enter one or more characters in the input field until the name you want to call appears in the dynamic search list or, enter the complete name or number.

Dial: Press *Dial* to initiate the call.

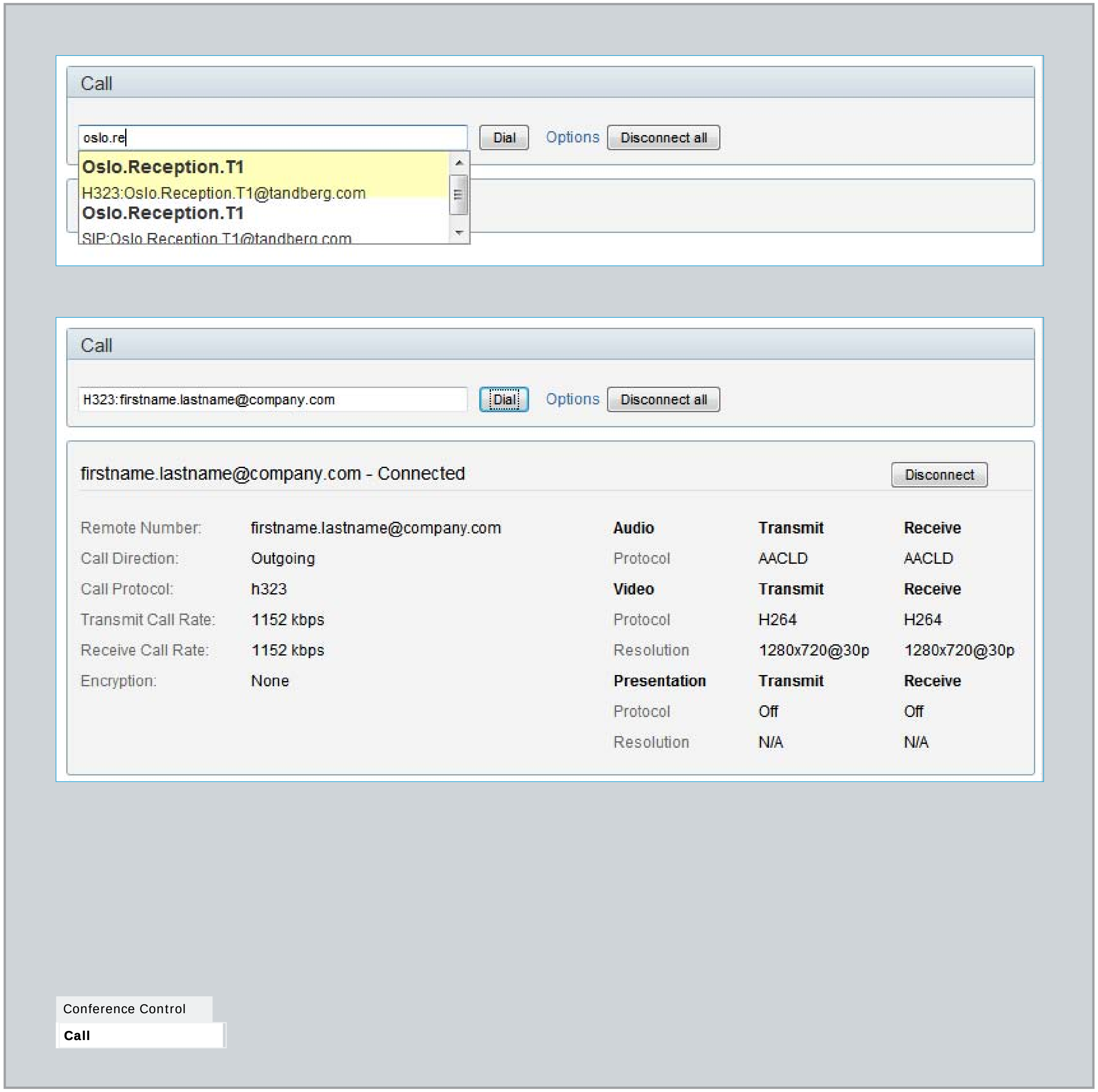
Disconnect all: Press *Disconnect all* to end all calls.

Options: Click *Options* to change the bit rate for this call. Select the bit rate you want in the *Call rate* drop down list.

The call status page

You will find the following information on the call status page when you are in a call:

- Remote number
- Call direction: Incoming/Outgoing
- Call protocol: H323/SIP
- Transmit and receive call rate
- Encryption
- Audio: Transmit and receive protocols
- Video: Transmit protocol and resolution, and receive protocol and resolution
- Presentation: Transmit protocol and resolution, and receive protocol and resolution



Oslo.Reception.T1
H323:Oslo.Reception.T1@tandberg.com
Oslo.Reception.T1
SIP:Oslo.Reception.T1@tandberg.com

H323:firstname.lastname@company.com

firstname.lastname@company.com - Connected

Remote Number:	firstname.lastname@company.com	**Audio**	**Transmit**	**Receive**
Call Direction:	Outgoing	Protocol	AACLD	AACLD
Call Protocol:	h323	**Video**	**Transmit**	**Receive**
Transmit Call Rate:	1152 kbps	Protocol	H264	H264
Receive Call Rate:	1152 kbps	Resolution	1280x720@30p	1280x720@30p
Encryption:	None	**Presentation**	**Transmit**	**Receive**
		Protocol	Off	Off
		Resolution	N/A	N/A

Upgrading the system software

From the Upgrade Software page you can initiate software upgrades and add a release key and option keys.

Software versions

This video conference system is using TC software.

NOTE: 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 (TC4).

Go to: ▸ http://www.cisco.com/en/US/products/ps11422/tsd_products_support_series_home.html

Downloading new software

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

Release key

The release key is required to be able to use the released software.

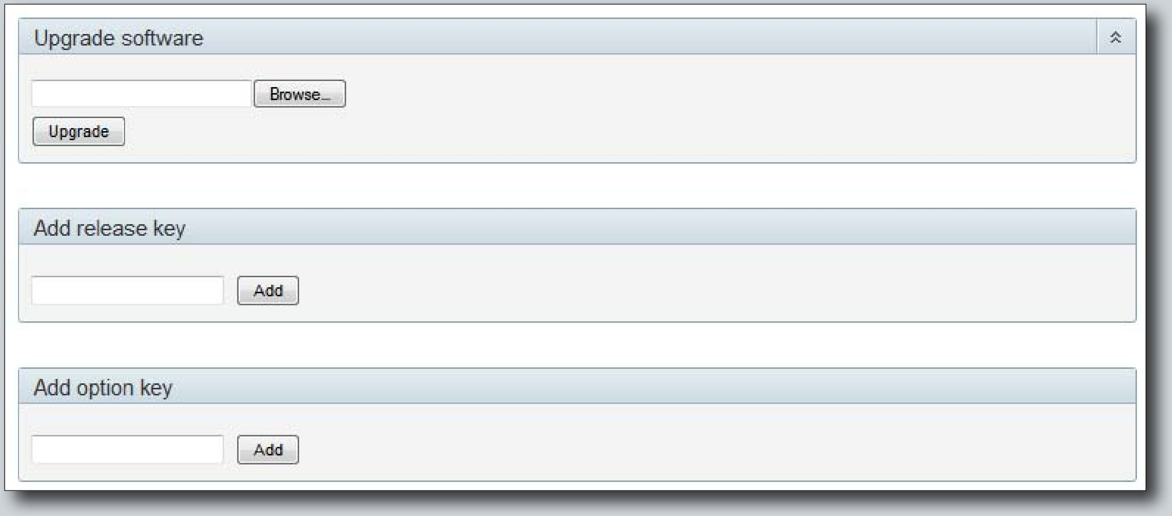
Contact your Cisco representative to obtain the release key.

Option key

An option key is required to activate any optional functionality, and you may have several option keys in your system. The available options are:

- Premium resolution

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



1. Add the release and option keys

Contact your Cisco representative to obtain the required key(s). If you will add both a release key and one or more option keys, the correct procedure will be:

i. Enter the *release key* and press *Add*.
Key format: "1TC001-1-0C22E348" (each system will have a unique key).

ii. Enter the *option key* and press *Add*.
Key format: "1N000-1-AA7A4A09" (each system will have a unique key).

iii. If you have more than one option key, add the remaining keys.

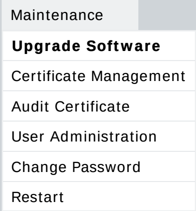
2. Upgrade the software on the codec

i. Before you can start the upgrade you must download the software upgrade file. The file format: "s52000tc4_0_0.pkg" (each software version has a unique file name).

ii. Press *Browse...* and select the .PKG file.

iii. Press the *Upgrade* button to start the installation.

iv. Leave the system to allow the installation process to complete. You can follow the progress on this page. When the upgrade is successfully completed a message will appear. The installation process may take up to 30 minutes.



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.

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. Press *Browse...* and locate the HTTPS certificate file (.PEM format).
2. Press *Browse...* and locate the Private key file (.PEM format).
3. Enter the *Passphrase*.
4. Press *Upload* to upload the certificate to your system.

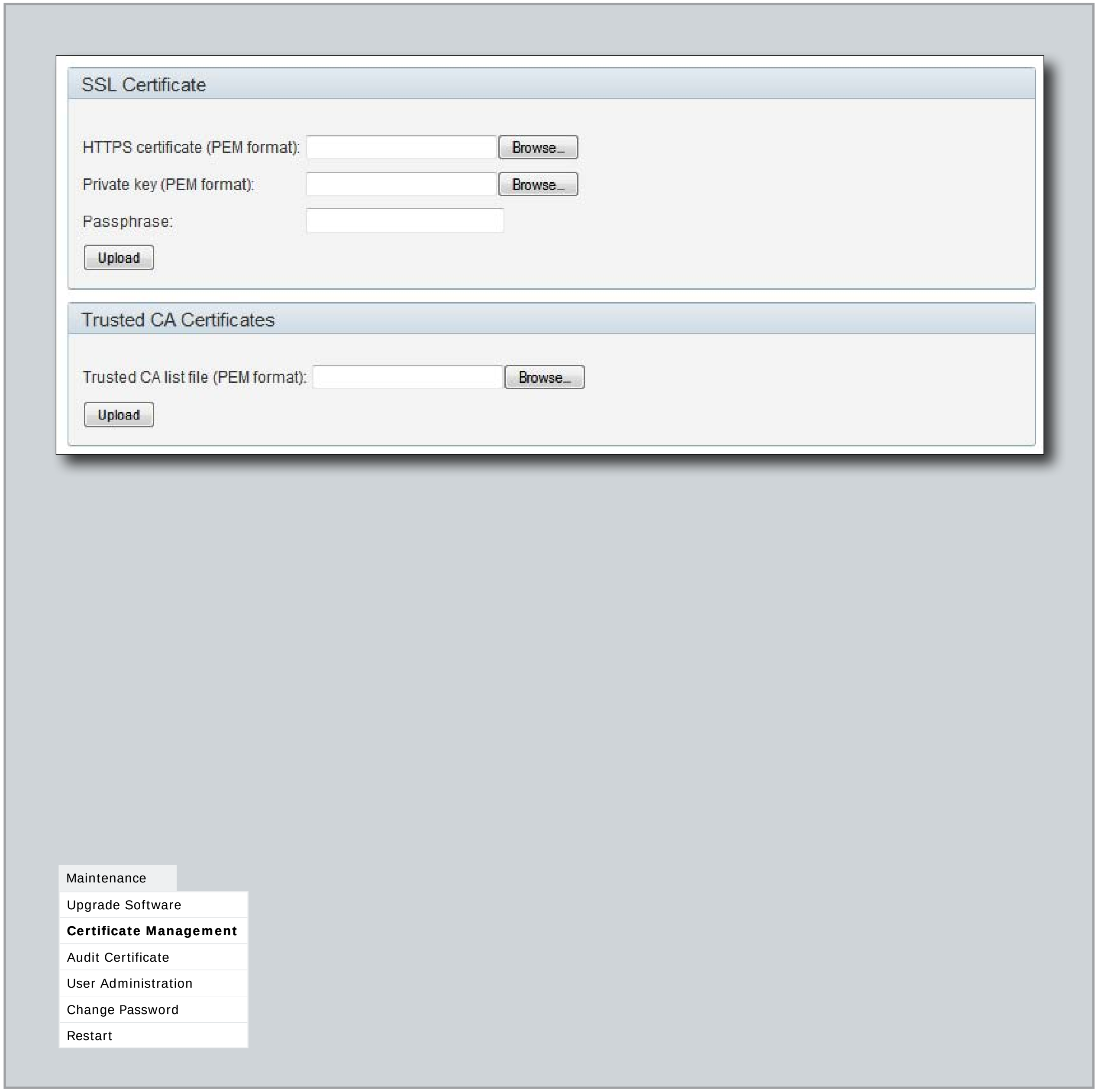
Uploading the trusted CA certificates list

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. Press *Browse...* and locate the file with the Trusted CA list (.PEM format).
2. Press *Upload* to upload the certificate list to your system.



The audit certificate list

If you want to use the ExternalSecure audit logging mode, you must upload a list of trusted audit certificates to the video conference system. This list covers all audit servers that your system shall trust.

In the ExternalSecure audit logging mode audit logging information will only be sent to entities holding a valid audit certificate.

NOTE: You should always upload the audit certificate list before enabling secure audit logging.

About audit logging

Audit logging records all login activity and configuration changes on the system.

Audit logging is disabled by default. You can enable audit logging using the on-screen menu or the web interface.

1. Upload the audit certificate list

To install the audit certificate, you will need:

- Audit list file (.PEM format)

Contact your system administrator to obtain the required file.

i. Press *Browse...* and locate the file with the audit list file (.PEM format).

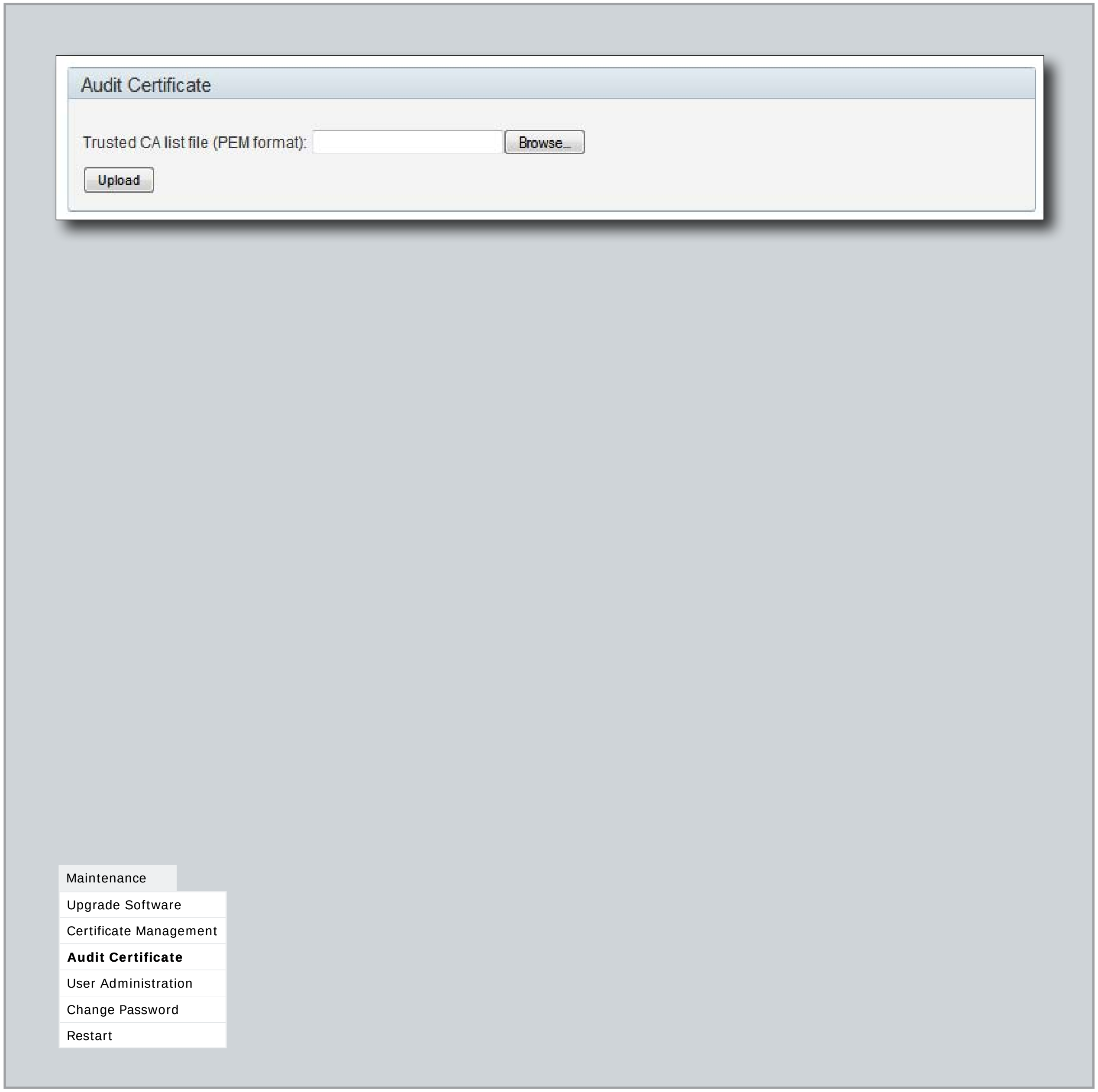
ii. Press *Upload* to upload the certificate to your system.

2. Enable secure audit logging

When you have uploaded the audit certificate list you must enable secure audit logging:

i. Navigate to *Advanced Configuration > Security > Audit > Server* and enter the IP address and Port number of the audit server.

ii. Navigate to *Advanced Configuration > Security > Audit > Logging > Mode* and set it to ExternalSecure.



User administration

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

The default user account

The system comes with a default administrator user account with username admin and no password set. The admin user has full access rights, and it is highly recommended to set a password for this user.

Read more about passwords in the ▸ Set passwords appendices in this guide.

About user roles

A user account must possess one or a combination of several user roles. Three user roles exist, representing different rights:

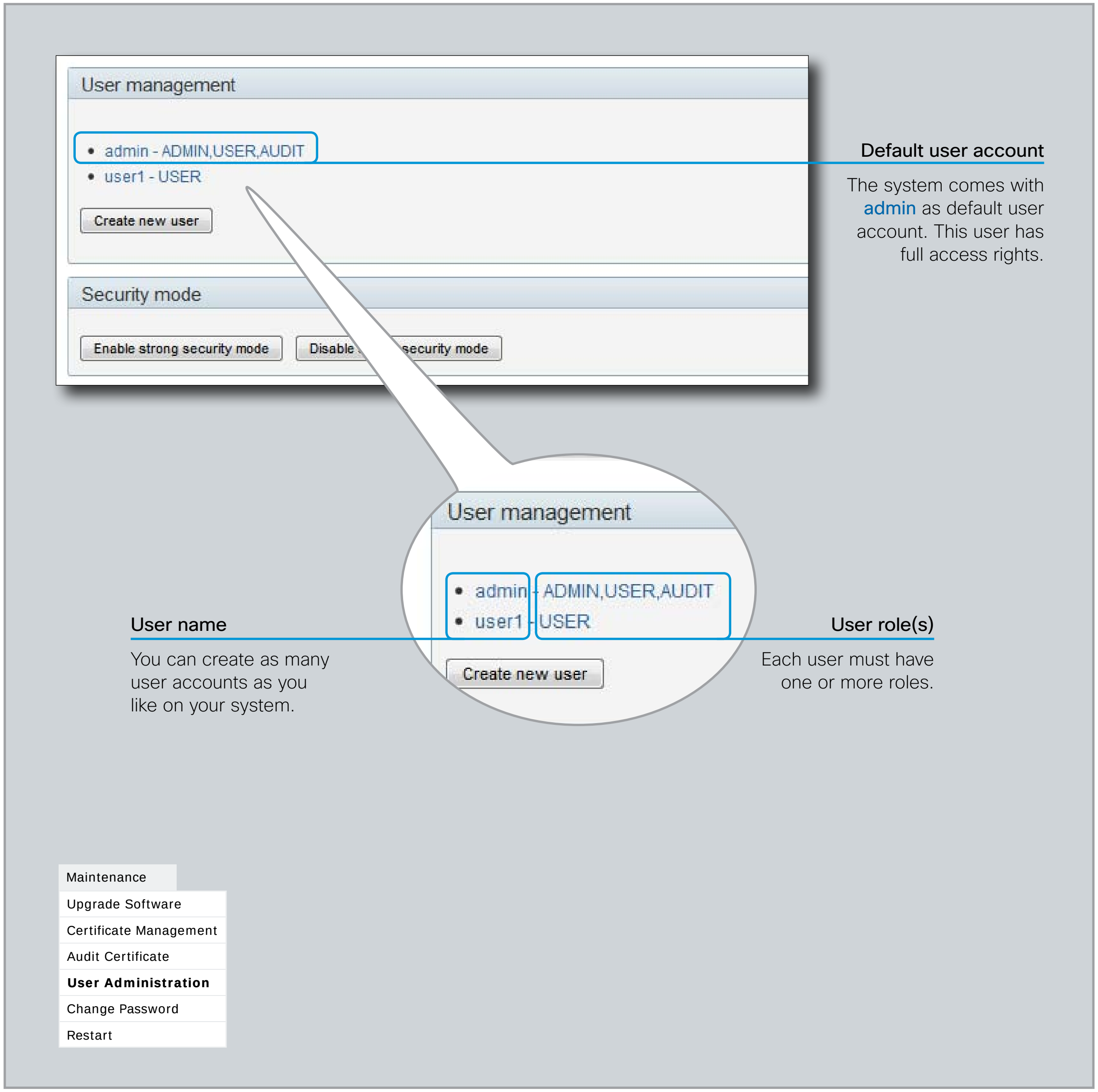
- **ADMIN**: A user with admin rights can create new users and change all settings, except the security audit settings. This user cannot upload audit certificates.
- **USER**: A user with user rights can make calls and search the phonebook.
- **AUDIT**: A user with audit rights can change the security audit configurations and upload audit certificates.

It is important to note that these roles have non-overlapping rights.

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

Security mode

You can enable/disable the strong security mode from this page. Strong security mode sets very strict password requirements, and requires all users to change their password on next sign in.



Default user account

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

User name

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

User role(s)

Each user must have one or more roles.

Creating a new user account

1. Press *Create new user*.
2. Fill in the Username, Password and PIN code, and select the user role(s) for this user account.

   As a default the user have 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. Press *Save* to save the changes.

Editing user details

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

Deactivating a user account

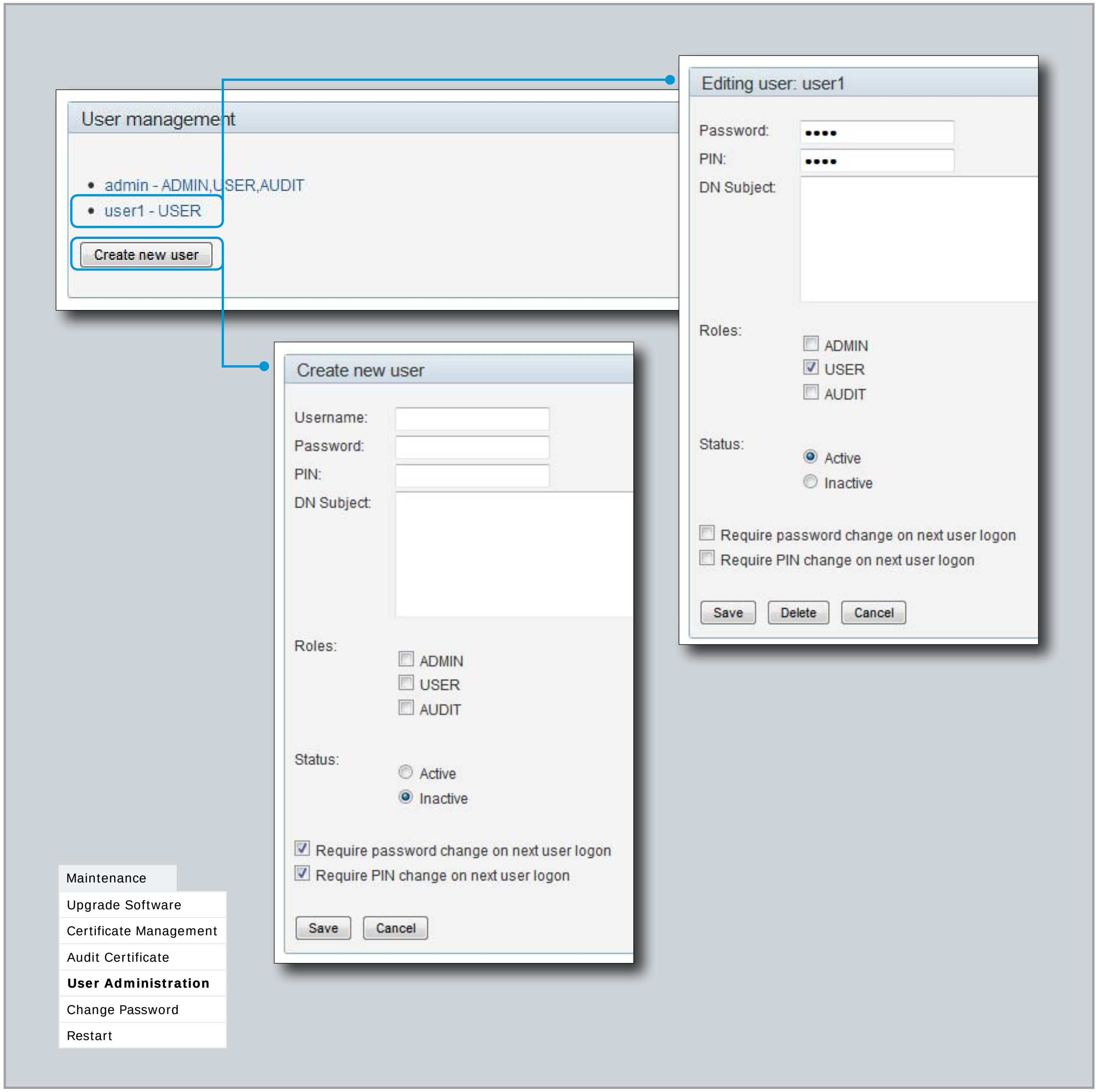
1. Select the name of an existing user to open the Editing user window.
2. Set the *Status* to **Inactive**.
3. Press *Save* to save the changes.

NOTE: Always keep at least one user with ADMIN rights Active.

Deleting a user account

1. Select the name of the user to open the Editing user window.
2. Press *Delete*.

NOTE: Always keep at least one user with ADMIN rights.



User management

- admin - ADMIN,USER,AUDIT
- user1 - USER

Create new user

Editing user: user1

Password: ••••
PIN: ••••
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:
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

Changing your password

When you are signed in, you can change your password. In the example to the right, the admin user is signed in.

Remember, it is highly recommended to set a password for all users holding ADMIN rights.

The password is a string with 0–64 characters.

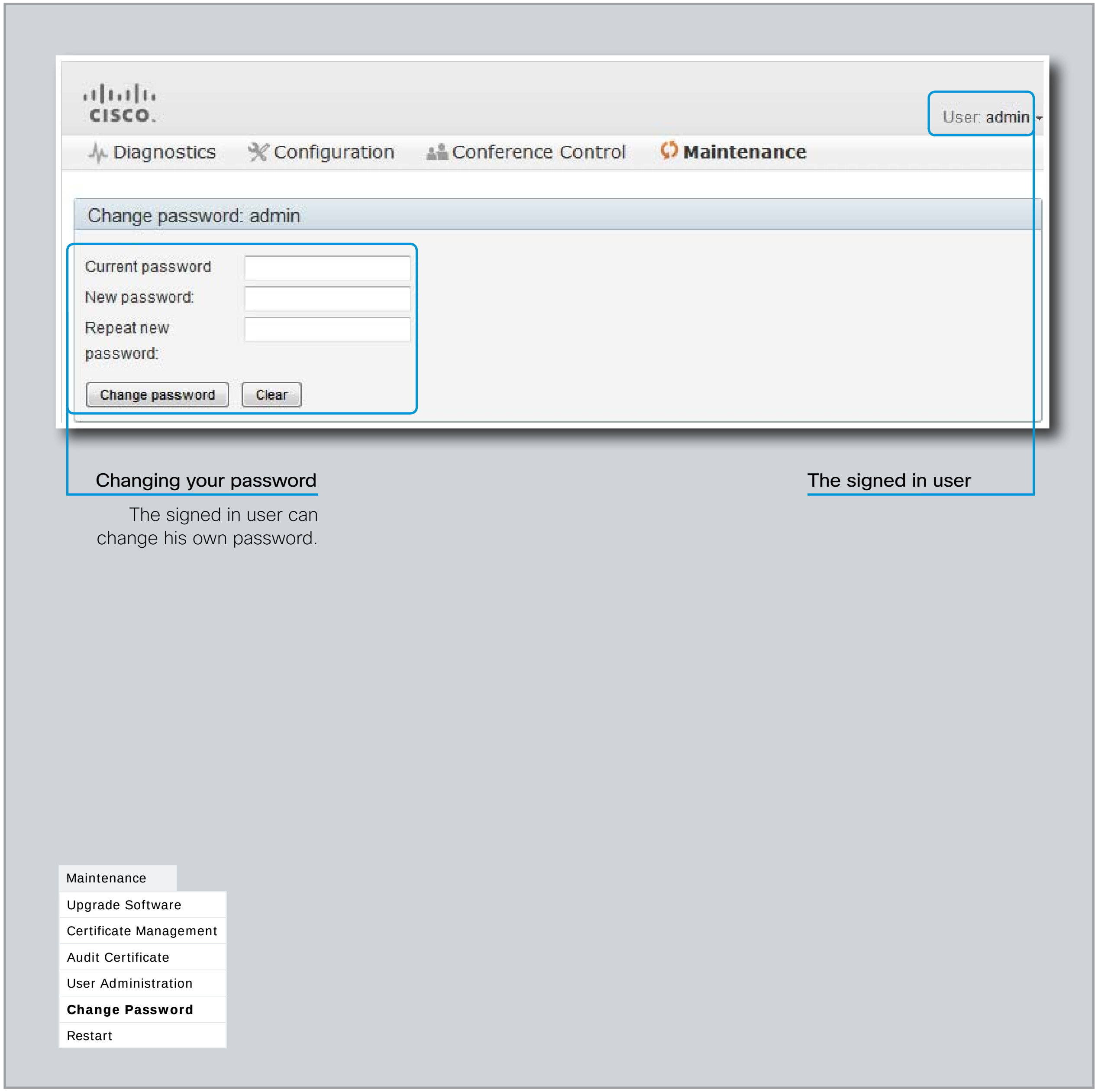
Changing your password

1. Enter your current password, your new password, and repeat the new password in the input fields.

   If no password is set, leave the current password input field empty.

   If you want to remove a password, leave the new password input fields empty (not recommended for users with ADMIN rights).

2. Click *Change password* to change the password.



Changing your password

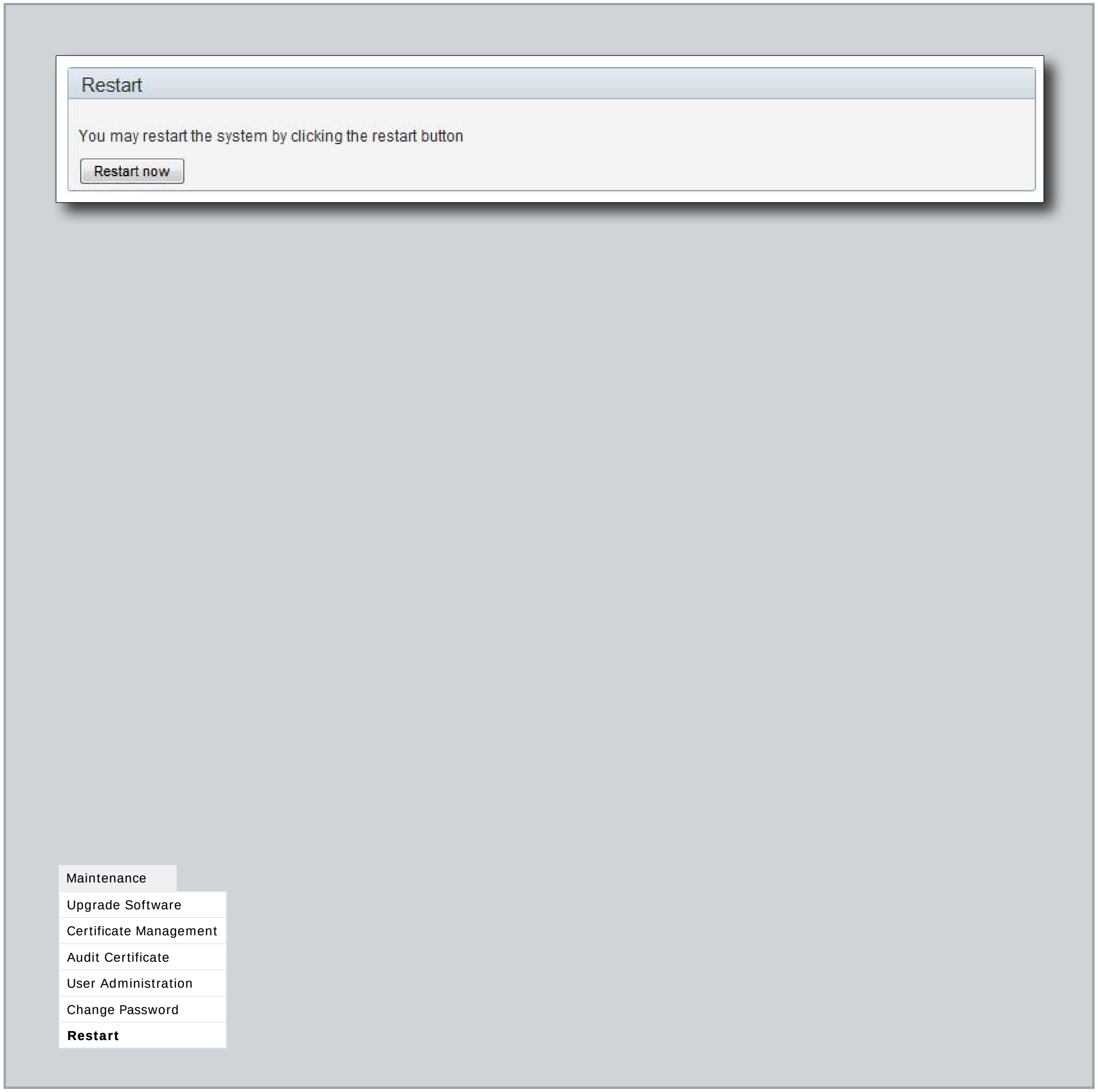
The signed in user can change his own password.

The signed in user

Restarting the system

To restart the system, press *Restart now*.

Restarting the system takes a few minutes.



Restart

You may restart the system by clicking the restart button

Chapter 3

The advanced settings

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 show either the default value or an example of a value.

Find the IP address of your system

Tap *More > Settings* on the Touch controller, select *System Information* and find the *IPv4 Address* or *IPv6 Address* of your system.

Open the web interface

Open a web browser and enter your video conference system's IP address in the address bar; then sign in.

Overview of the advanced settings

The Audio settings

Audio PreferredOutputConnector

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

Requires user role: ADMIN

Value space: `<None/Internal>`

None: The default audio output is the internal speaker.

Internal: The audio out goes to the internal loudspeaker. NOTE: Requires the " Audio InternalSpeaker Mode" to be enabled.

Example: `Audio PreferredOutputConnector: Internal`

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 Microphones Mute Enabled

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

Requires user role: ADMIN

Value space: `<True/InCallOnly>`

True: Muting of audio is always available.

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

Example: `Audio Microphones Mute Enabled: True`

Audio SoundsAndAlerts KeyTones Mode

Not applicable in this version.

Audio SoundsAndAlerts RingTone

Select the ring tone for incoming calls.

Requires user role: USER

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

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

Example: `Audio SoundsAndAlerts RingTone: Jazz`

Audio SoundsAndAlerts RingVolume

Sets the ring tone 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 VolumeHandset

Set the volume on the handset.

Requires user role: ADMIN

Value space: `<0..100>`

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

Example: `Audio VolumeHandset: 70`

Audio VolumeHeadset

Set the volume on the headset.

Requires user role: ADMIN

Value space: `<0..100>`

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

Example: `Audio VolumeHeadset: 70`

Audio Volume

Set the volume on the loudspeaker.

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). Value 0 = Off.

Example: `Audio Volume: 70`

The Cameras settings

Cameras PowerLine Frequency

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

Requires user role: ADMIN

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

Auto: Set to Auto to enable power frequency auto detection in the camera.
50Hz: Set to 50 Hz.
60Hz: Set to 60 Hz.

Example: `Cameras PowerLine Frequency: Auto`

Cameras Camera [1..1] Backlight

The backlight functionality compensates for light shining directly at the camera (usually the sun entering the window) to avoid a too dark image from the room.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Turn on the camera backlight.
Off: Turn off the camera backlight.

Example: `Cameras Camera 1 Backlight: Off`

Cameras Camera [1..1] Brightness Mode

Set the camera brightness mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: The camera brightness is automatically set by the system.
Manual: Enable manual control of the camera brightness, e.g. the level of the brightness level setting will be used for the camera.

Example: `Cameras Camera 1 Brightness Mode: Auto`

Cameras Camera [1..1] Brightness Level

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

Requires user role: ADMIN

Value space: `<1..31>`

Range: Select a value from 1 to 31.

Example: `Cameras Camera 1 Brightness Level: 1`

Cameras Camera [1..1] Flip

Not applicable in this version.

Cameras Camera [1..1] Focus Mode

Set the camera focus mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: When set to Auto the focus will be updated throughout the call. When moving the camera, the system will use auto focus for a few seconds to set the right focus of the new camera position. After a few seconds auto focus is turned off to prevent continuous focus adjustments of the camera.
Manual: Turn the autofocus off and adjust the camera focus manually.

Example: `Cameras Camera 1 Focus Mode: Auto`

Cameras Camera [1..1] FrameRate

Set the frame rate frequency.

Requires user role: ADMIN

Value space: `<60Hz/30Hz>`

60Hz: Set the frame rate to 60 Hz.
30Hz: Set the frame rate to 30 Hz.

Example: `Cameras Camera 1 FrameRate: 30Hz`

Cameras Camera [1..1] Gamma Mode

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

Requires user role: ADMIN

Value space: `<Auto/Manual>`

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

Example: `Cameras Camera 1 Gamma Mode: Auto`

Cameras Camera [1..1] Gamma Level

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

Requires user role: ADMIN

Value space: `<0..7>`

Range: Select a value from 0 to 7.

Example: `Cameras Camera 1 Gamma Level: 0`

Cameras Camera [1..1] IrSensor

Not applicable in this version.

Cameras Camera [1..1] Mirror

Not applicable in this version.

Cameras Camera [1..1] Whitebalance Mode

Set the camera whitebalance mode.

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: The camera will continuously adjust the whitebalance depending on the camera view.
Manual: Enables manual control of the camera whitebalance, e.g. the level of the whitebalance level setting will be used for the camera.

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`

The Conference settings

Conference [1..1] TelephonyPrefix

Enter the prefix to be used for telephony calls.

Requires user role: ADMIN

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

Format: String with a maximum of 80 characters.

Example: `Conference 1 TelephonyPrefix: "520"`

Conference [1..1] IncomingMultisiteCall Mode

Set the incoming Multisite call mode. The MultiSite feature allows participants from more than two locations to join a meeting – by video and/or telephone.

Requires user role: ADMIN

Value space: `<Allow/Deny>`

Allow: Accept incoming calls to an already active call/conference. The incoming call will be added to the MCU conference.
Deny: The system will not accept incoming calls when you are in a call. The calling side will receive a busy signal.

Example: `Conference 1 IncomingMultisiteCall Mode: Allow`

Conference [1..1] AutoAnswer Mode

Set the AutoAnswer mode.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable AutoAnswer to let the system automatically answer all incoming calls.
Off: The incoming calls must be answered manually by pressing the green 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 the AutoAnswer Mode to be enabled.

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 the AutoAnswer Mode to be enabled.

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

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Un-mute the microphones after the call is disconnected.

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

Example: `Conference 1 MicUnmuteOnDisconnect: On`

Conference [1..1] DoNotDisturb Mode

Determine if there should be an alert on incoming calls.

Requires user role: USER

Value space: `<On/Off>`

On: All incoming calls will be rejected, with no alert. The calling side will receive a busy signal when trying to call the codec. A message will display on screen, telling that Do not disturb is turned on, together with an option to turn off the Do not disturb. When turning off the Do not disturb mode you will see a list of the calls that have been rejected.

Off: The incoming calls will be alerted.

Example: `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] FarEndControl SignalCapability

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the far end control signal capability.

Off: Disable the far end control signal capability.

Example: `Conference 1 FarEndControl SignalCapability: On`

Conference [1..1] Encryption Mode

Set the conference encryption mode. A padlock with the text " Encryption On" or " Encryption Off" displays on screen for a few seconds when the conference starts.

Requires user role: ADMIN

Value space: `<BestEffort/On/Off>`

BestEffort: The system will use encryption whenever possible.

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

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

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

Off: The system will not use encryption.

Example: `Conference 1 Encryption Mode: BestEffort`

Conference [1..1] DefaultCall Protocol

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

Requires user role: ADMIN

Value space: `<H323/Sip>`

H.323: Select H.323 to ensure that calls are set up as H.323 calls.

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

Example: `Conference 1 DefaultCall Protocol: H323`

Conference [1..1] DefaultCall Rate

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

Requires user role: ADMIN

Value space: `<64..6000>`

Range: Select a value between 64 and 6000 kbps

Example: `Conference 1 DefaultCall Rate: 768`

Conference [1..1] MaxTransmitCallRate

Specify the maximum transmit 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] VideoBandwidth Mode

Set the conference video bandwidth mode.

Requires user role: ADMIN

Value space: `<Dynamic/Static>`

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

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

Example: `Conference 1 VideoBandwidth Mode: Dynamic`

Conference [1..1] VideoBandwidth MainChannel Weight

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

Requires user role: ADMIN

Value space: `<1..10>`

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth MainChannel Weight: 5`

Conference [1..1] VideoBandwidth PresentationChannel Weight

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

Requires user role: ADMIN

Value space: `<1..10>`

Range: 1 to 10.

Example: `Conference 1 VideoBandwidth PresentationChannel Weight: 5`

Conference [1..1] PacketLossResilience Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the packetloss resilience.

Off: Disable the packetloss resilience.

Example: `Conference 1 PacketLossResilience Mode: On`

The H323 settings

H323 NAT Mode

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

Requires user role: ADMIN

Value space: `<Auto/On/Off>`

Auto: The system will determine if the " NAT Address" or the real IP-address should be used within signalling. This is done to make it possible to place calls to endpoints on the LAN as well as endpoints on the WAN.
On: The system will signal the configured " NAT Address" in place of its own IP-address within Q.931 and H.245. The NAT Server Address will be shown in the startup-menu as: " My IP Address: 10.0.2.1".
Off: The system will signal the real IP Address.

Example: `H323 NAT Mode: Off`

H323 NAT Address

Enter the external/global IP-address to the router with NAT support. Packets sent to the router will then be routed to the system.

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

* Port 1720

* Port 5555-5574

* Port 2326-2485

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

Example: `H323 NAT Address: ""`

H323 Profile [1..1] Authentication Mode

Set the authenticatin mode for the H.323 profile.

Requires user role: ADMIN

Value space: `<On/Off>`

On: If the H.323 Gatekeeper Authentication Mode is set to On and a H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. NOTE: Requires the Authentication LoginName and Authentication Password to be defined on both the codec and the Gatekeeper.
Off: If the H.323 Gatekeeper Authentication Mode is set to Off the system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.

Example: `H323 Profile 1 Authentication Mode: Off`

H323 Profile [1..1] Authentication LoginName

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

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

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

H323 Profile [1..1] Authentication Password

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

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

Example: `H323 Profile 1 Authentication Password:`

H323 Profile [1..1] CallSetup Mode

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

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

Requires user role: ADMIN

Value space: `<Direct/Gatekeeper>`

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

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

Example: `H323 Profile 1 CallSetup Mode: Gatekeeper`

H323 Profile [1..1] Gatekeeper Discovery

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

Requires user role: ADMIN

Value space: `<Manual/Auto>`

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

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

Example: `H323 Profile 1 Gatekeeper Discovery: Manual`

H323 Profile [1..1] Gatekeeper Address

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

Requires user role: ADMIN

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

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

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

H323 Profile [1..1] H323Alias E164

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

Requires user role: ADMIN

Value space: `<S: 0, 30>`

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

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

H323 Profile [1..1] H323Alias ID

Lets you specify the H.323 Alias ID which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists. Example: " firstname.surname@company.com", " My H.323 Alias ID"

Requires user role: ADMIN

Value space: `<S: 0, 49>`

Format: String with a maximum of 49 characters

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

H323 Profile [1..1] PortAllocation

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

Requires user role: ADMIN

Value space: `<Dynamic/Static>`

Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. For RTP and RTCP media data, the system is using UDP ports in the range 2326 to 2487. Each media channel is using two adjacent ports, ie 2330 and 2331 for RTP and RTCP respectively. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.

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

Example: `H323 Profile 1 PortAllocation: Dynamic`

The Network settings

Network [1..1] Assignment

Define whether to use DHCP or Static IPv4 assignment.

Requires user role: ADMIN

Value space: `<Static/DHCP>`

Static: Set the network assignment to Static and configure the static IPv4 settings (IP Address, SubnetMask and Gateway).

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

Example: `Network 1 Assignment: DHCP`

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..5] Address

Define the network addresses for DNS servers. Up to 5 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] IPStack

Select which internet protocols the system will support.

Requires user role: ADMIN

Value space: `<IPv4/IPv6>`

IPv4: IP version 4 is supported.

IPv6: IP version 6 is supported. The IPv4 settings (IP Address, IP Subnet Mask and Gateway) will be disabled.

Example: `Network 1 IPStack: IPv4`

Network [1..1] IPv4 Address

Enter the static IPv4 network address for the system. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

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

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

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

Network [1..1] IPv4 Gateway

Define the IPv4 network gateway. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

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

Format: Compact string with a maximum of 64 characters.

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

Network [1..1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Only applicable if the Network Assignment is set to Static.

Requires user role: ADMIN

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

Format: Compact string with a maximum of 64 characters.

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

Network [1..1] IPv6 Address

Enter the static IPv6 network address for the system. Only applicable if the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

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

Format: The IPv6 address of host name.

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

Network [1..1] IPv6 Gateway

Define the IPv6 network gateway address. Only applicable if the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN

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

Format: The IPv6 address of host name.

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

Network [1..1] IPv6 Assignment

Define whether to use Autoconf or Static IPv6 assignment.

Requires user role: ADMIN

Value space: `<Static/Autoconf>`

Static: Set the network assignment to Static and configure the static IPv6 settings (IP Address and Gateway).

Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC4862 for a detailed description.

Example: `Network 1 IPv6 Assignment: Autoconf`

Network [1..1] IPv6 DHCPOptions

Retrieves a set of DHCP options from a DHCPv6 server.

Requires user role: ADMIN

Value space: `<On/Off>`

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

Off: Set to Off when IPv6 Assignment is set to Static.

Example: `Network 1 IPv6 Gateway: On`

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

The Diffserv Audio defines which priority Audio packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Audio: A recommended value is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Audio: 0`

Network [1..1] QoS Diffserv Data

The Diffserv Data defines which priority Data packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Data: A recommended value is Diffserv Code Point (DSCP) AF23, which equals the value 22. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Data: 0`

Network [1..1] QoS Diffserv Signalling

The Diffserv Signalling defines which priority Signalling packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Signalling: A recommended value is Diffserv Code Point (DSCP) AF31, which equals the value 26. If in doubt, contact your network administrator.

Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Signalling: 0`

Network [1..1] QoS Diffserv Video

The Diffserv Video defines which priority Video packets should have in an IP network. Enter a priority, which ranges from 0 to 63 for the packets. The higher the number, the higher the priority. These priorities might be overridden when packets are leaving the network controlled by the local network administrator. NOTE: Requires the Network QoS Mode to be set to Diffserv.

Requires user role: ADMIN

Value space: `<0..63>`

Video: A recommended value is Diffserv Code Point (DSCP) AF41, which equals the value 34. If in doubt, contact your network administrator.
Range: Select a value from 0 to 63.

Example: `Network 1 QoS Diffserv Video: 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 Identity

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

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X Identity: ""`

Network [1..1] IEEE8021X Password

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

Requires user role: ADMIN

Value space: `<S: 0, 32>`

Format: String with a maximum of 32 characters.

Example: `Network 1 IEEE8021X Password: "***"`

Network [1..1] IEEE8021X AnonymousIdentity

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

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

Example: `Network 1 IEEE8021X AnonymousIdentity: ""`

Network [1..1] IEEE8021X Eap Md5

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

Requires user role: ADMIN

Value space: `<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 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] 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] MTU

Set the Ethernet MTU (Maximum Transmission Unit).

Requires user role: ADMIN

Value space: `<576..1500>`

Range: Select a value from 576 to 1500 bytes.

Example: `Network 1 MTU: 1500`

Network [1..1] Speed

Set the Ethernet link speed.

Requires user role: ADMIN

Value space: `<Auto/10half/10full/100half/100full/1000full>`

Auto: Autonegotiate link speed.
10half: Force link to 10 Mbps half-duplex.
10full: Force link to 10 Mbps full-duplex.
100half: Force link to 100 Mbps half-duplex.
100full: Force link to 100 Mbps full-duplex.
1000full: Force link to 1 Gbps full-duplex.

Example: `Network 1 Speed: Auto`

Network [1..1] TrafficControl Mode

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

Requires user role: ADMIN

Value space: `<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] RemoteAccess Allow

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

Requires user role: ADMIN

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

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

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

Network [1..1] VLAN Data Mode

Set the VLAN data mode.

Requires user role: ADMIN

Value space: `<Manual/Off>`

Manual: The data packets in the VLAN network are manually tagged with VlanId and Priority.
Off: The data packets in the VLAN network are untagged.

Example: `Network 1 VLAN Data Mode: Off`

Network [1..1] VLAN Data VlanId

Set the VLAN data ID.

Requires user role: ADMIN

Value space: `<1..4094>`

Range: Select a value from 1 to 4094.

Example: `Network 1 VLAN Data VlanId: 1`

Network [1..1] VLAN Data Priority

Set the VLAN data priority.

Requires user role: ADMIN

Value space: `<0..7>`

Range: Select a value from 0 to 7.

Example: `Network 1 VLAN Data Priority: 0`

Network [1..1] VLAN Voice Mode

Set the VLAN voice mode.

Requires user role: ADMIN

Value space: `<Manual/Off>`

Manual: The voice packets in the VLAN network are manually tagged with VlanId and Priority.
Off: The voice packets in the VLAN network are untagged.

Example: `Network 1 VLAN Voice Mode: Off`

Network [1..1] VLAN Voice VlanId

Set the VLAN voice ID.

Requires user role: ADMIN

Value space: `<1..4094>`

Range: Select a value from 1 to 4094.

Example: `Network 1 VLAN Voice VlanId: 1`

Network [1..1] VLAN Voice Priority

Set the VLAN voice priority.

Requires user role: ADMIN

Value space: `<0..7>`

Range: Select a value from 0 to 7.

Example: `Network 1 VLAN Voice Priority: 0`

The NetworkServices settings

NetworkServices Multiway Address

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

Multiway™ can be used in the following situations:

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

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

Requirements: The Codec C20 must be running TC3.0 (or later), Codec C90/C60/C40 must be running TC4.0 (or later), EX90/EX60/MX200 must be running TC4.2 (or later), Video Communication Server (VCS) version X5 (or later) and Codian MCU version 3.1 (or later). Endpoints invited to join the Multiway™ conference must support the H.323 routeToMC facility message if in an H.323 call, or SIP REFER message if in a SIP call.

Requires user role: ADMIN

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

Format: String with a maximum of 255 characters.

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

NetworkServices Multiway Protocol

Determine the protocol to be used for Multiway calls. NOTE: Requires a restart of the codec.

Requires user role: ADMIN

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

Auto: The system will select the protocol for Multiway calls.
H323: The H323 protocol will be used for Multiway calls.
Sip: The SIP protocol will be used for Multiway calls.

Example: `NetworkServices Multiway Protocol: Auto`

NetworkServices H323 Mode

Determine whether the system should be able to place and receive H.323 calls or not. NOTE: Requires a restart of the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

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

Example: `NetworkServices H323 Mode: On`

NetworkServices HTTP Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: The HTTP protocol is enabled.
Off: The HTTP protocol is disabled.

Example: `NetworkServices HTTP Mode: On`

NetworkServices HTTPS Mode

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

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 system connects to an external HTTPS server (like a phonebook server or an external manager), this server will present a certificate to the 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 system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the 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 HTTPS OCSP Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable OCSP support.
Off: Disable OCSP support.

Example: `NetworkServices HTTPS OCSP Mode: Off`

NetworkServices HTTPS OCSP URL

Specify the URL of an OCSP server.

Requires user role: ADMIN

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

Format: String with a maximum of 255 characters.

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

NetworkServices NTP Mode

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

Requires user role: ADMIN

Value space: `<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 SIP Mode

Determine whether the system should be able to place and receive SIP calls or not. NOTE: Requires a restart of the codec.

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 SNMP Mode

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

Requires user role: ADMIN

Value space: `<Off/ReadOnly/ReadWrite>`

Off: Disable the SNMP network service.

ReadOnly: Enable the SNMP network service for queries only.

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

Example: `NetworkServices SNMP Mode: ReadWrite`

NetworkServices SNMP Host [1..3] Address

Enter the address of up to three SNMP Managers. All traps will then be sent to the hosts listed.

The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.). SNMP Traps are generated by the SNMP Agent to inform the SNMP Manager about important events. Can be used to send event created messages to the SNMP agent about different events like: system reboot, system dialling, system disconnecting, MCU call, packet loss etc. Traps can be sent to multiple SNMP Trap Hosts.

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

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

NetworkServices SNMP CommunityName

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

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP CommunityName: "public"`

NetworkServices SNMP SystemContact

Enter the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemContact: ""`

NetworkServices SNMP SystemLocation

Enter the name of the Network Services SNMP System Location.

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

Example: `NetworkServices SNMP SystemLocation: ""`

NetworkServices SSH Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: The SSH protocol is enabled.

Off: The SSH protocol is disabled.

Example: `NetworkServices SSH Mode: On`

NetworkServices SSH AllowPublicKey

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: The SSH public key is allowed.

Off: The SSH public key is not allowed.

Example: `NetworkServices SSH AllowPublicKey: On`

NetworkServices Telnet Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: The Telnet protocol is enabled.

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

Example: `NetworkServices Telnet Mode: Off`

The Phonebook settings

Phonebook Server [1..1] ID

Enter a name for the external phonebook.

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

Example: `Phonebook Server 1 ID: ""`

Phonebook Server [1..1] Type

Select the phonebook server type.

Requires user role: ADMIN

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

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

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

Callway: Select Callway if the phonebook is to be provided by the Callway subscription service. Contact your Callway provider for more information.

Example: `Phonebook Server 1 Type: TMS`

Phonebook Server [1..1] URL

Enter the address (URL) to the external phonebook 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"`

The Provisioning settings

Provisioning Mode

Provides the possibility of managing the codec (endpoint) by using an external manager/ management system.

Requires user role: ADMIN

Value space: `<Off/TMS/VCS/CallWay/Auto>`

Off: The system will not try to register to any management system.
TMS: If set to TMS (Cisco TelePresence Management System) the system will try to register with a TMS server. Contact your Cisco representative for more information.
VCS: If set to VCS (Cisco TelePresence Video Communication Server) the system will try to register with a VCS. Contact your Cisco representative for more information.
Callway: If set to Callway the system will try to register with the Callway subscription provider. Contact your Callway provider for more information.
Auto: The provisioning server will automatically be selected by the system.

Example: `Provisioning Mode: TMS`

Provisioning LoginName

Enter the user id provided by the provisioning server. This is the user name part of the credentials used to authenticate towards the HTTP server when using HTTP provisioning.

Requires user role: ADMIN

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

Format: String with a maximum of 80 characters.

Example: `Provisioning LoginName: ""`

Provisioning Password

Enter the password provided by the provisioning server. This is the password part of the credentials used to authenticate towards the HTTP server when using HTTP provisioning.

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 provisiong server supports GET.
POST: Select POST when the provisiong server supports POST.

Example: `Provisioning HttpMethod: POST`

Provisioning ExternalManager Address

Enter the IP Address to the External Manager/Management system. If an External Manager address and a path is configured, the system will post an HTTP message to this address when starting up. When receiving this HTTP posting the External Manager (typically a management system) can return configurations/commands to the unit as a result. If the DHCP Option 242 is returned in the DHCP response from the DHCP server the system will interpret this as the External Manager address to use.

Requires user role: ADMIN

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

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

Example: `Provisioning ExternalManager Address: ""`

Provisioning ExternalManager Protocol

Determine whether or not to use secure management.

Requires user role: ADMIN

Value space: `<HTTP/HTTPS>`

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

Example: `Provisioning ExternalManager Protocol: HTTP`

Provisioning ExternalManager Path

Set the path to the External Manager/Management system. If an External Manager address and a path is configured, the system will post an HTTP message to this address when starting up. When receiving this HTTP posting the External Manager (typically a management system) can return configurations/commands to the unit as a result. If the DHCP Option 242 is returned in the DHCP response from the DHCP server the system will interpret this as the External Manager address to use.

Requires user role: ADMIN

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

Format: String with a maximum of 255 characters.

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

Provisioning ExternalManager Domain

Enter the SIP domain for the provisioning server.

Requires user role: ADMIN

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

Format: String with a maximum of 64 characters.

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

The RTP settings

RTP Ports Range Start

Specify the first port in the range of RTP ports. See also the " H323 Profile [1..1] PortAllocation" command.

Requires user role: USER

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. See also the " H323 Profile [1..1] PortAllocation" command.

Requires user role: USER

Value space: `<1056..65535>`

Range: Select a value from 1056 to 65535.

Example: `RTP Ports Range Stop: 2486`

The Security settings

Security Audit Server Address

Enter the external/global IP-address to the audit syslog server.

Requires user role: AUDIT

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

Format: String with a maximum of 64 characters.

Example: `Security Audit Server Address: ""`

Security Audit Server Port

Enter the port of the syslog server that the system shall send its audit logs to. A user with AUDIT rights is required to change this setting.

Requires user role: AUDIT

Value space: `<0..65535>`

Range: Select a value from 0 to 65535.

Example: `Security Audit Server Port: 514`

Security Audit OnError Action

Describes what actions will be taken if connection to the syslog server is lost. A user with AUDIT rights is required to change this setting.

Requires user role: AUDIT

Value space: `<Halt/Ignore>`

Halt: If the connection to the syslog server is lost for more than a few seconds, the system will reboot and try to establish connection. If connection is restored, the audit logs are respooled to the syslog server, and the system starts up again.

Ignore: The system will continue its normal operation, and rotate internal logs when full. When connection is restored it will again send its audit logs to the syslog server.

Example: `Security Audit OnError Action: Ignore`

Security Audit Logging Mode

Describes where the audit logs are recorded or transmitted. A user with AUDIT rights is required to change this setting.

Requires user role: AUDIT

Value space: `<Off/Internal/External/ExternalSecure>`

Off: No audit logging is performed.

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

External: The system sends the audit logs to an external audit server.

ExternalSecure: The system sends the audit logs to an external audit server that is verified by the Audit CA list.

Example: `Security Audit Logging Mode: Off`

Security Session ShowLastLogon

When logging in to the system using SSH or Telnet you will see the UserId, time and date of the last session that did a successful login.

Requires user role: ADMIN

Value space: `<Off/On>`

On: Set to On to enable the possibility to show information about the last session.

Off: Set to Off to disable the possibility to show information about the last session.

Example: `Security Session ShowLastLogon: Off`

Security Session InactivityTimeout

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

Requires user role: ADMIN

Value space: `<0..10000>`

Range: Select a value from 0 to 10000 seconds. 0 means that inactivity will not enforce automatically logout.

Example: `Security Session InactivityTimeout: 0`

The SerialPort settings

SerialPort Mode

Set the COM 1 serial port to be enabled/disabled.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable the COM 1 serial port.
Off: Disable the COM 1 serial port.

Example: `SerialPort Mode: On`

SerialPort BaudRate

Specify the baud rate (data transmission rate, bits per second) for the COM 1 port on the codec. The default value is 38400.

Connection parameters for the COM port: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

Requires user role: ADMIN

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

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

Example: `SerialPort BaudRate: 38400`

SerialPort LoginRequired

Determine if login shall be required when connecting to the COM 1 port at the codec.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Login is required when connecting to the codec through COM 1 port.
Off: The user can access the codec through COM 1 port without any login.

Example: `SerialPort LoginRequired: On`

The 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] Authentication [1..1] LoginName

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

Requires user role: ADMIN

Value space: `<S: 0, 128>`

Format: String with a maximum of 128 characters.

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

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

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

Requires user role: ADMIN

Value space: `<S: 0, 128>`

Format: String with a maximum of 128 characters.

Example: `SIP Profile 1 Authentication 1 Password:`

SIP Profile [1..1] DefaultTransport

Select the transport protocol to be used over the LAN.

Requires user role: ADMIN

Value space: `<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 using the web interface. 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 using the web interface.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Set to On to verify TLS connections. Only TLS connections to servers, whom 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] 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] Address

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

Requires user role: ADMIN

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

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

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

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

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

Requires user role: ADMIN

Value space: `<Auto/Manual>`

Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).
Manual: When Manual is selected, the manually configured SIP Proxy address will be used.

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

SIP Profile [1..1] Type

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

Requires user role: ADMIN

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

Standard: To be used when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)
Alcatel: To be used when registering to Alcatel-Lucent OmniPCX Enterprise. NOTE: This mode is not fully supported.
Avaya: To be used when registering to Avaya Communication Manager. NOTE: This mode is not fully supported.
Cisco: To be used when registering to Cisco Unified Communication Manager.
Microsoft: To be used when registering to Microsoft LCS or OCS. NOTE: This mode is not fully supported.
Nortel: To be used when registering to Nortel MCS 5100 or MCS 5200 PBX. NOTE: This mode is not fully supported.

Example: `SIP Profile 1 Type: Standard`

The Standby settings

Standby Control

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enter standby mode when the Standby Delay has timed out. NOTE: Requires the Standby Delay to be set to an appropriate value.
Off: The system will not enter standby mode.

Example: `Standby Control: On`

Standby Delay

Define how long (in minutes) the system shall be in idle mode before it goes into standby mode. NOTE: Requires the Standby Control to be enabled.

Requires user role: ADMIN

Value space: `<1..480>`

Range: Select a value from 1 to 480 minutes.

Example: `Standby Delay: 10`

Standby BootAction

Define the camera position after a restart of the codec.

Requires user role: ADMIN

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

None: No action.
Preset1 to Preset15: After a reboot the camera position will be set to the position defined by the selected preset.
RestoreCameraPosition: After a reboot the camera position will be set to the position it had before the last boot.
DefaultCameraPosition: After a reboot the camera position will be set to the factory default position.

Example: `Standby BootAction: DefaultCameraPosition`

Standby StandbyAction

Define the camera position when going into standby mode.

Requires user role: ADMIN

Value space: `<None/PrivacyPosition>`

None: No action.
PrivacyPosition: Turns the camera to a sideways position for privacy.

Example: `Standby StandbyAction: PrivacyPosition`

Standby WakeupAction

Define the camera position when leaving standby mode.

Requires user role: ADMIN

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

None: No action.
Preset1 to Preset15: When leaving standby the camera position will be set to the position defined by the selected preset.
RestoreCameraPosition: When leaving standby the camera position will be set to the position it had before entering standby.
DefaultCameraPosition: When leaving standby the camera position will be set to the factory default position.

Example: `Standby WakeupAction: RestoreCameraPosition`

The SystemUnit settings

SystemUnit MenuType

Systems having a Cisco TelePresence Touch Controller will use the Touch controller to control the system, and should select Indicators as menu type. Systems having a Cisco Remote Control will use the remote control to control the system, and should select Full as menu type.

Requires user role: ADMIN

Value space: `<Indicators/Full>`

Indicators: Systems having a Cisco Touch controller will use the Touch menus and should select Indicators as menu type.

Full: Systems having a Cisco Remote Control will use the on-screen menus and should select Full as menu type.

Example: `SystemUnit MenuType: Indicators`

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>`

Example: `SystemUnit MenuLanguage: English`

SystemUnit ContactInfo Type

Not applicable in this version.

SystemUnit Type

Select whether the video system is for personal use or to be used in a multiuser environment. It is highly recommended not 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 multiuser environment.

Example: `SystemUnit Type: Personal`

SystemUnit CallLogging Mode

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable logging.

Off: Disable logging.

Example: `SystemUnit CallLogging Mode: On`

SystemUnit IrSensor

Not applicable in this version.

The 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`

The Video settings

Video Input Source [1..2] Name

Enter a name for the video input source.

Requires user role: ADMIN

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

Format: String with a maximum of 50 characters.

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

Video Input Source [1] Connector

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

Requires user role: ADMIN

Value space: `<DVI>`

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

Example: `Video Input Source 1 Connector: DVI`

Video Input Source [2] Connector

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

Requires user role: ADMIN

Value space: `<CAMERA>`

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

Example: `Video Input Source 2 Connector: CAMERA`

Video Input Source [1..2] Type

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

Requires user role: ADMIN

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

Other: Select Other when some other type of equipment is connected to the selected video input.
Camera: Select Camera when you have a camera connected to the selected video input.
PC: Select PC when you have a PC connected to the selected video input.
DVD: Select DVD when you have a DVD player connected to the selected video input.
Document_Camera: Select Document_Camera when you have a document camera connected to the selected video input.

Example: `Video Input Source 1 Type: PC`

Video Input Source [1..2] CameraControl Mode

Set the camera control mode for the camera associated with the video source.

Requires user role: ADMIN

Value space: `<On/Off>`

On: Enable camera control.
Off: Disable camera control.

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

Video Input Source [1..2] CameraControl CameraId

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

Requires user role: ADMIN

Value space: `<1..5>`

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

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

Video Input Source [1..2] OptimalDefinition Profile

Adjust how rapidly the system will increase the transmitted resolution when increasing the bandwidth. NOTE: Requires that the Video Input Source Quality is set to Motion.

Normal: Use this setting for normal to poorly lit environment. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 2.2Mb/sec and above with this setting set to normal.

Medium: Requires better than normal and consistent lighting and good quality video inputs. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 1.4Mb/sec and above with this setting set to medium.

High: Requires good lighting conditions for a good overall experience and good quality video inputs. If the source is a camera with 1920x1080p60, the system will transmit 1920x720p60 at about 1.1Mb/sec and above with this setting set to high.

Requires user role: ADMIN

Value space: `<Normal/Medium/High>`

Ref: Table 1 and Table 2.

Example: `Video Input Source 1 OptimalDefinition Profile: Normal`

Table 1: Optimal definition for systems supporting 1080p

	w288p30	*w448p30*	*w576p30*	*720p30*	*1080p30*
Normal	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s	2560 kbit/s
Medium	128 kbit/s	384 kbit/s	512 kbit/s	1152 kbit/s	1920 kbit/s
High	128 kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1472 kbit/s

Table 2: Optimal definition for systems supporting 720p60

	w144p60	*w288p60*	*w448p60*	*w576p60*	*720p60*
Normal	128 kbit/s	512 kbit/s	1152 kbit/s	1472 kbit/s	2240 kbit/s
Medium	128 kbit/s	384 kbit/s	768 kbit/s	1152 kbit/s	1920 kbit/s
High	128 kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s

Video Input Source [1..2] OptimalDefinition Threshold60fps

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

Requires user role: ADMIN

Value space: `<512_288/768_448/1024_576/1280_720/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 1 OptimalDefinition Threshold60fps: 1280_720`

Video Input Source [1..2] Quality

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

Requires user role: ADMIN

Value space: `<Motion/Sharpness>`

Motion: Gives the highest possible framerate. Used when there is a need for higher frame rates, typically when a large number of participants are present or when there is a lot of motion in the picture.
Sharpness: Gives the highest possible resolution. Used when you want the highest quality of detailed images and graphics.

Example: `Video Input Source 1 Quality: Motion`

Video DefaultPresentationSource

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>`

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

Example: `Video DefaultPresentationSource: 2`

Video Input DVI [1] Type

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

Requires user role: ADMIN

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

AutoDetect: Set to AutoDetect to automatically detect if the signal is analog RGB or digital.
Digital: Set to Digital to force the DVI video input to Digital when using DVI-I cables with both analog and digital pins and AutoDetect fails.
AnalogRGB: Set to AnalogRGB to force the DVI video input to AnalogRGB when using DVI-I cables with both analog and digital pins and AutoDetect fails.
AnalogYPbPr: Set to AnalogYPbPr to force the DVI video input to AnalogYPbPr, as the component (YPbPr) signal cannot be auto detected.

Example: `Video Input DVI 1 Type: AutoDetect`

Video ControlPanel Brightness

Set the brightness level for the touch screen.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Range: Select a value from 0 to 100.

Example: `Video ControlPanel Brightness: 100`

Video Layout Scaling

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

Requires user role: ADMIN

Value space: `<On/Off>`

On: Let the system automatically adjust aspect ratio.
Off: No adjustment of the aspect ratio.

Example: `Video Layout Scaling: On`

Video Layout ScaleToFrame

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

Requires user role: ADMIN

Value space: `<Manual/MaintainAspectRatio/StretchToFit>`

Manual: If the difference in aspect ratio between the video input source and the target image frame is less than the ScaleToFrameThreshold configuration (in percent), the image is stretched to fit. If not, the system will maintain the original aspect ratio.
MaintainAspectRatio: Will maintain the aspect ratio of the input source, and fill in black in the rest of the frame (letter boxing or pillar boxing).
StretchToFit: Will stretch (horizontally or vertically) the input source to fit into the image frame. NOTE: The general limitation is that you cannot upscale in one direction and at the same time downscale in the other direction. In such situations the codec will apply letterboxing.

Example: `Video Layout ScaleToFrame: MaintainAspectRatio`

Video Layout ScaleToFrameThreshold

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

Requires user role: ADMIN

Value space: `<0..100>`

Range: Select a value from 0 to 100 percent.

Example: `Video Layout ScaleToFrameThreshold: 5`

Video Layout LocalLayoutFamily

Select which video layout family to be used locally.

Requires user role: ADMIN

Value space: `<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>`

Auto: The default layout family, as given by the layout database, will be used as the local layout. For more information about the layout database, see the command: xCommand Video Layout LoadDb.
FullScreen: The FullScreen layout family will be used as the local layout.
Equal: The Equal layout family will be used as the local layout.
PresentationSmallSpeaker: The PresentationSmallSpeaker layout family will be used as the local layout.
PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the local layout.

Example: `Video Layout LocalLayoutFamily: Auto`

Video Layout RemoteLayoutFamily

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

Requires user role: ADMIN

Value space: `<Auto/FullScreen/Equal/PresentationSmallSpeaker/PresentationLargeSpeaker>`

Auto: The default layout family, as given by the local layout database, will be used as the remote layout. For more information about the layout database, see the command: xCommand Video Layout LoadDb.
FullScreen: The FullScreen layout family will be used as the remote layout.
Equal: The Equal layout family will be used as the remote layout.
PresentationSmallSpeaker: The PresentationSmallSpeaker layout family will be used as the remote layout.
PresentationLargeSpeaker: The PresentationLargeSpeaker layout family will be used as the remote layout.

Example: `Video Layout RemoteLayoutFamily: Auto`

Video MainVideoSource

Define which video input source shall be used as the main video source. The video input source is configured with the " Video Input Source [1..2] Connector" setting.

Requires user role: USER

Value space: `<1..2>`

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

Example: `Video MainVideoSource: 1`

Video Monitors

Set the monitor layout mode.

Requires user role: ADMIN

Value space: `<Single/Dual/DualPresentationOnly>`

Single: The same layout is shown on all monitors.
Dual: The layout is distributed on two monitors.
DualPresentationOnly: All participants in the call will be shown on the first monitor, while the presentation (if any) will be shown on the second monitor.

Example: `Video Monitors: Single`

Video OSD Mode

Not applicable in this version.

Video OSD AutoSelectPresentationSource

Not applicable in this version.

Video OSD TodaysBookings

Not applicable in this version.

Video OSD MyContactsExpanded

Not applicable in this version.

Video OSD Output

Not applicable in this version.

Video OSD InputMethod InputLanguage

Not applicable in this version.

Video OSD InputMethod Cyrillic

Not applicable in this version.

Video OSD LoginRequired

Not applicable in this version.

Video Output LCD [1] Resolution

Set the screen resolution.

Requires user role: ADMIN

Value space: `<1920_1080_60>`

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

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

Video Output LCD [1] MonitorRole

Set the LCD monitor role.

It is highly recommended to use the default setting. NOTE: The settings made here will be overruled by the touch controller.

Requires user role: ADMIN

Value space: `<First/Second/PresentationOnly/InternalSetup>`

First: Show main video stream.
Second: Show presentation video stream if active, or other participants.
PresentationOnly: Show presentation video stream if active, and nothing else.
InternalSetup: Internal setup from the touch controller will be used.

Example: `Video Output LCD 1 MonitorRole: InternalSetup`

Video Output LCD [1] Brightness

Set the brightness level for the monitor.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Brightness: 50`

Video Output LCD [1] Red

Set the Red color level for the monitor.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Red: 50`

Video Output LCD [1] Green

Set the Green color level for the monitor.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Green: 50`

Video Output LCD [1] Blue

Set the Blue color level for the monitor.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Range: Select a value from 0 to 100.

Example: `Video Output LCD 1 Blue: 50`

Video Output Internal [2] MonitorRole

Determine the role of the internal monitor and select where to show the video stream and presentation.

It is highly recommended to use the default setting.

Requires user role: ADMIN

Value space: `<First/Second/PresentationOnly>`

First: Show the main video stream.

Second: Show presentation video stream if active, or other participants.

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

Example: `Video Output Internal 2: First`

Video Selfview

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

Requires user role: USER

Value space: `<On/Off>`

On: Display selfview on screen.

Off: Do not display selfview on screen.

Example: `Video Selfview: On`

Video WallPaper

Determine which background picture to show on the touch screen and main screen when idle. It is recommended to use Wallpaper01 to Wallpaper12.

Requires user role: USER

Value space: `<None/Growing/Summersky/Custom/Wallpaper01/Wallpaper02/Wallpaper03/Wallpaper04/Wallpaper05/Wallpaper06/Wallpaper07/Wallpaper08/Wallpaper09/Wallpaper10/Wallpaper11/Wallpaper12/Wallpaper13>`

Wallpaper01 to Wallpaper13: Select one of the predefined wallpapers to be displayed on the main screen and touch screen. The wallpaper will be shown on both screens.

None: No wallpaper will be displayed on the main screen. NOTE: When you change the wallpaper on the touch screen, it will also set the wallpaper for the main screen.

Summersky, Growing: Select one of the predefined wallpapers to be displayed on the main screen. It will not be displayed on the touch screen. NOTE: When you change the wallpaper on the touch screen, it will also change the wallpaper for the main screen.

Custom: The custom wallpaper will only show on the main screen, not the touch screen. It must be uploaded to the codec from the web interface before selecting Custom. The maximum supported resolution is 1920x1280.

1) On the video system: Find the IP address of the codec. Open the menu on screen and go to Home > Settings > System information to find the IP Address.

2) On your computer: Open a web browser and enter the IP address of the codec. Select " Wallpaper" from the menu, browse for the file, and press the " Upload" button.

3) On the web interface: Log in and go to Advanced Configuration > Video > Wallpaper and select Custom. Give it a few seconds to display the new picture. If the picture does not show, toggle once between " None" and " Custom" wallpaper to make the change take effect. NOTE: When you change the wallpaper on the touch screen, it will also change the wallpaper for the main screen.

Example: `Video Wallpaper: Wallpaper01`

The Experimental settings

The Experimental settings are beta preview features and can be used 'as is'. They are not fully documented.

NOTE: The Experimental settings are likely to change without further notice.

Experimental Audio Panning Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Off/Auto>`

Example: `Experimental Audio Panning Mode: Off`

Experimental Audio Panning MaxAngle

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<0..90>`

Example: `Experimental Audio Panning MaxAngle: 0`

Experimental Audio Panning MonitorLeft

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<1/2/3/4/5>`

Example: `Experimental Audio Panning MonitorLeft: 1`

Experimental Audio Panning MonitorRight

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<1/2/3/4/5>`

Example: `Experimental Audio Panning MonitorRight: 1`

Experimental CapsetFilter

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<S: 0, 100>`

Example: `Experimental CapsetFilter: ""`

Experimental CapsetReduction

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Auto/Reduced>`

Example: `Experimental CapsetReduction: Auto`

Experimental Conference [1..1] PacketLossResilience ForwardErrorCorrection

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Will enable ForwardErrorCorrection (RFC5109) mechanism as part of the PacketLossResilience mechanism. Default value is On.

On: Forward error correction will be used as part of the PacketLossResilience mechanism.

Off: Forward error correction will NOT be used as part of the PacketLossResilience mechanism.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental Conference 1 PacketLossResilience ForwardErrorCorrection: On`

Experimental Conference [1..1] PacketLossResilience RateAdaption

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Will use the a RateAdaption algorithm adapted to the PacketLossResilience mechanism. Default value is On.

On: RateAdaption will be used as part of the PacketLossResilience mechanism.

Off: RateAdaption will NOT be used as part of the PacketLossResilience mechanism.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental Conference 1 PacketLossResilience RateAdaption: On`

Experimental Conference [1..1] ReceiverBasedDownspeeding

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental Conference 1 ReceiverBasedDownspeeding: Off`

Experimental NetworkServices UPnP Mode

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental NetworkServices UPnP Mode: Off`

Experimental NetworkServices UPnP Timeout

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<0..3600>`

Example: `Experimental NetworkServices UPnP Timeout: 0`

Experimental SystemUnit MenuType

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<Indicators/Full>`

Example: `Experimental SystemUnit MenuType: Full`

Experimental SystemUnit SoftwareUpgrade RequireAuthentication

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental SystemUnit SoftwareUpgrade RequireAuthentication: Off`

Experimental Video OSD AlertOnIncomingCall

NOTE: This Experimental command can be used 'as is' and will not be further documented. The Experimental settings WILL change.

Requires user role: ADMIN

Value space: `<On/Off>`

Example: `Experimental Video OSD AlertOnIncomingCall: On`

Appendices

Setting the system password

You need a username and password to sign in to the web and command line interfaces of your system.

The video conference system is delivered with a default user account with username admin and no password set. This user has full access rights to the system.

NOTE: We strongly recommend that you set a password for the admin user 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.

Changing your 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 username and current password.
2. Go to the *Maintenance* tab and select *Change Password*.
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

Read more about creating more user accounts in the ▸ User management section.

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

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

Setting the Administrator settings menu password

When starting up the system for the first time the Administrator Settings menu password is not set.

NOTE: We strongly recommend that you define a password to protect the Administrator Settings menu on the Touch controller, since these settings affect the behavior of the video conference system.

You need to use a command line interface to set the Administrator Settings menu password; you neither can use the Touch controller nor the web interface.

Setting the Administrator Settings menu password

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Type the following command:

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

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

Setting a root password

You can also protect the file system of your video system by setting a password for the root user. The root user is disabled by default. You have to use the command line interface to enable the root user and set a root password.

Setting a root password

Perform the following steps to activate the root user and set a password for it:

1. Connect to the system through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Sign in to the system with username and password. The user needs ADMIN rights.
3. Type the following command:

   ```
   systemtools rootsettings on <password>
   ```

NOTE: The root password is not the same as the system (admin) password.

Optimal definition profiles

Under ideal lighting conditions the bandwidth requirements can be substantially reduced with the optimal definitions profiles.

Generally, we recommend the Optimal Definition set at Normal.

If lighting conditions are good we recommend that you test the endpoint on the various Optimal Definition settings before deciding on a profile.

Go to Advanced Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Profile* and select the optimal definition profile.

You can set a resolution threshold below which the maximum frame rate will be 30 fps.

Go to Advanced Configuration on the web interface and navigate to *Video > Input > Source [1..n] > OptimalDefinition > Threshold60fps* and select a threshold.

The video input quality settings must be set to Motion for the Optimal Definition to work. 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* and set the video quality parameter.

You can read more about the video settings in the ▸ Advanced settings chapter.

High (720p60)

Typically used in dedicated video conferencing rooms. Requires good lighting conditions for a good overall experience.

Under ideal conditions the bandwidth requirements can be reduced by up to 50%.

Medium (w576p60)

Typically used in rooms with better than normal, and consistent lighting.

The bandwidth requirements can be reduced by up to 25%.

Normal (w448p60)

This setting is typically used in office environments where the environment is normal to poorly lit.

Generally, we recommend the Optimal Definition set at Normal.

Table 1: Optimal definition for systems supporting 1080p

	w288p30	*w448p30*	*w576p30*	*720p30*	*1080p30*
Normal	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s	2560 kbit/s
Medium	128 kbit/s	384 kbit/s	512 kbit/s	1152 kbit/s	1920 kbit/s
High	128 kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1472 kbit/s

Table 2: Optimal definition for systems supporting 720p60

	w144p60	*w288p60*	*w448p60*	*w576p60*	*720p60*
Normal	128 kbit/s	512 kbit/s	1152 kbit/s	1472 kbit/s	2240 kbit/s
Medium	128 kbit/s	384 kbit/s	768 kbit/s	1152 kbit/s	1920 kbit/s
High	128 kbit/s	256 kbit/s	512 kbit/s	768 kbit/s	1152 kbit/s

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.

To configure ClearPath select *Advanced Configuration* on the web interface and navigate to *Conference 1 > PacketLossResilience > Mode*. Select **Off** to disable ClearPath and select **On** to enable ClearPath.

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

Technical specification for Cisco TelePresence MX200

PRODUCT SPECIFICATION

Product compatibility

Fully compatible with standards-compliant telepresence and video systems

Software compatibility

Cisco TelePresence Software Version TC4.2 or later

Components

Fully integrated unit including:

- Codec
- Display
- Camera
- Integrated microphone and loudspeakers
- Cisco TelePresence Performance Mic 20
- Cables including: DVI-I-to-VGA cable, 3.5-mm jack audio cable, LAN cable, and power cable

Display

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

PC and second-source video input

DVI-I

Supported PC input resolutions

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

Camera

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

Audio system

- Integrated full-range speaker and subwoofer
- Integrated full-range microphone
- Bluetooth-ready
- Support for two Cisco TelePresence Performance Mic 20 (one standard plus one optional)
- RCA PC audio input
- RCA audio output

User interface

Cisco TelePresence Touch

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

Language support

English

Physical dimensions

42-inch main unit with floor stand:
Height: 1429 mm / 56.3 in.
Width: 1026 mm / 40.4 in.
Depth: 602 mm / 23.7 in.
Weight: 40.2 kg / 89 lb

42-inch main unit with table stand:
Height: 781 mm / 30.7 in.
Width: 1026 mm / 40.4 in.
Depth: 259 mm /10.2 in.
Weight: 31.5 kg / 69 lb

42-inch main unit with wall mount:
Height: 757 mm / 29.8 in.
Width: 1026 mm / 40.4 in.
Depth: 169 mm / 6.7 in.
Weight: 30 kg / 66 lb

Power

- Autosensing power supply
- 100–240 VAC, 50/60 Hz
- 75 watts maximum

Temperature range

Operating temperature and humidity:

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

Approvals and compliance

EU/EEC

Directive 2006/95/EC (Low Voltage Directive)

- Standard EN 60950-1

Directive 2004/108/EC (EMC Directive)

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

Warning: This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

USA

Approved according to UL 60950-1

Complies with FCC15B Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

Approved according to CAN/CSA C22.2 No. 60950-1

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada

VIDEO AND AUDIO SPECIFICATIONS

Bandwidth

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

Video standards

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

Video features

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

Live video resolutions (encode/decode)

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

* Requires premium resolution option

Audio standards

- G.711
- G.722
- G.722.1
- 64/128 kbps 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
- Support for resolutions up to 720p30 in both main stream and dual stream simultaneously

NETWORK, SECURITY AND MANAGEMENT SPECIFICATIONS

Protocols

- H.323
- SIP

Network interfaces

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

Other interfaces

- Bluetooth for future applications
- RJ-45 for service

IP network features

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

Firewall traversal

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

Embedded encryption

- H.323 and SIP point-to-point
- Standards-based: H.235v2 and v3 and Advanced Encryption Standard (AES)
- Automatic key generation and exchange
- Support in dual stream

Security features

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

Cisco TelePresence Multiway™

- Multiway™ conferencing enables video endpoint users to introduce a 3rd party into an existing call utilizing a Cisco TelePresence MCU

System management

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

Directory services

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

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

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

July 2011

User documentation on the Cisco web site

User documentation for Cisco TelePresence products can be found on ▸ http://www.cisco.com/go/telepresence/docs.

Depending on which product you have got, select the following in the right pane:

MX200:

TelePresence Endpoints - Multipurpose
> Cisco TelePresence MX200 Series

Profile Series:

TelePresence Endpoints - Multipurpose
> Cisco TelePresence System Profile Series

EX Series:

TelePresence Endpoints - Personal
> TelePresence Desktop
> Cisco TelePresence System EX Series

Codec C Series:

TelePresence Solutions Platform
> TelePresence Integrator Products
> Cisco TelePresence System Integrator C Series

Quick Set C20:

TelePresence Solutions Platform
> TelePresence Quick Set
> Cisco TelePresence System Quick Set C Series

Document categories

For each product you will find the documents under the following categories:

User guides:

Maintain and Operate | End-User Guides

Quick reference guides:

Maintain and Operate | End-User Guides

Installation guides:

Install and Upgrade | Install and Upgrade Guides

Getting started guide:

Install and Upgrade | Install and Upgrade Guides

Administrator guides:

Maintain and Operate | Maintain and Operate Guides

API reference guides:

Reference Guides | Command references

Physical interface guides:

Maintain and Operate | End-User Guides

Regulatory compliance and safety information:

Install and Upgrade | Install and Upgrade Guides

TC software release notes:

Release and General Information | Release Notes

TC software licensing information:

Release and General Information | Licensing Information

Video conferencing room guidelines:

Design | Design Guides

NOTE: All products do not have all types of user documentation.