Thank you for choosing Cisco!

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

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

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

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

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

[http://www.cisco.com/go/telepresence/docs](http://www.cisco.com/go/telepresence/docs)

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

Go to: [http://www.cisco.com/web/siteassets/contacts](http://www.cisco.com/web/siteassets/contacts)

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

---

**Table of contents**

<table>
<thead>
<tr>
<th>Introduction</th>
<th>Using the web interface</th>
<th>Advanced configuration</th>
<th>Appendices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction .................................................................</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Intellectual property rights ........................................</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User documentation .......................................................</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>What’s new in this version ..............................................</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software release notes ..................................................</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software download ..........................................................</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User documentation ........................................................</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New features and improvements .......................................</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX90 system overview ....................................................</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EX60 system overview ....................................................</td>
<td>8</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Using the web interface ..........................................................**

- The web interface ......................................................... 9
- Connect to the EX90/EX60 ............................................... 10
- Password protection ..................................................... 10
- Menu options .............................................................. 11
- The system information page .......................................... 12
- Making calls from the web interface ................................. 13
- User management .......................................................... 14
- User roles ........................................................................ 14
- The default user account ............................................... 14
- Security mode ............................................................... 14
- Changing your password ............................................... 16
- Custom wallpaper .......................................................... 17
- File format and picture size ............................................ 17
- Upload the custom wallpaper file .................................. 17
- Activate the new wallpaper ........................................... 17
- Adding a logon banner .................................................. 18
- Uploading certificates ................................................... 19
- Audit certificate ............................................................ 20
- About audit logging ...................................................... 20
- Upload the audit certificate list ..................................... 20
- Log files ......................................................................... 21
- Viewing XML files ........................................................ 22
- Software upgrade .......................................................... 23
- Advanced configuration ................................................. 24
- Restarting the system ..................................................... 25

**The Advanced Configuration ......................................................**

- Description of the advanced configuration settings ........... 26
- The Audio settings .......................................................... 27
- The Cameras settings ....................................................... 31
- The Conference settings .................................................. 32
- The H323 settings .......................................................... 33
- The Network settings ...................................................... 36
- The NetworkServices settings ....................................... 37
- The Phonebook settings ................................................ 42
- The Provisioning settings .............................................. 44
- The Security settings ..................................................... 45
- The SerialPort settings .................................................. 46
- The SIP settings ............................................................ 47
- The Standby settings ..................................................... 48
- The SystemUnit settings ............................................... 49
- The Time settings ........................................................ 49
- The Video settings ....................................................... 50
- The Experimental settings ............................................ 56

**Appendices ...........................................................................**

- Password protection ..................................................... 58
- Change your codec password ........................................ 59
- Set the Administrator settings password ....................... 59
- Change the user passwords ............................................ 59
- Set a root password ...................................................... 59
- Optimal definition profiles .......................................... 60
- ClearPath — Packet loss resilience .................................. 61
- Dimensions of the EX90 ............................................ 62
- Wall mounting or arm mounting the EX60 ..................... 63
- Technical specifications ................................................. 64
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, EXPRESSED OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco’s trademarks can be found at www.cisco.com/go/trademarks. 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.

Patent information

The products described in this manual is covered by the following patents:


An updated list of the patents applying can be found on our web site.
Go to: ▶️ www.tandberg.com/tandberg_pm.jsp

User documentation

The user documentation for the Cisco TelePresence EX series:

• Quick Reference Guides
• User guides
• Administrator guide
• Regulatory compliance and safety information guide
• Legal and license information for products using TC software

Other user documentation you might find useful:

• Video conference room primer
• Video conference room acoustics guidelines

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. In the right pane select TelePresence Personal Endpoints > TelePresence Desktop > Cisco TelePresence System EX Series.
What's new in this version

This section provides an overview of the new and changed advanced configuration settings and new features in the TC4.1 software version.

New features and improvements

Cisco TelePresence Touch for EX Series

The Cisco TelePresence Touch is a touch based user interface that supports Cisco's vision for a natural user experience.

You can make video calls, share content, and access some advanced feature - all with a simple tap of the finger.

New graphical user interface

A new and improved GUI (Graphical User Interface) has been developed for the Cisco TelePresence Touch controller. Existing users of EX60 and EX90 will experience a new user interface when upgrading to TC4.1.0.

Some of the new features of the new GUI includes:

- Overall usability and responsiveness.
- Far end camera control on MultiSite (MultiSite is not supported on EX60).
- EMC resilience mode.
- All in one “search and dial” mechanism.
- Provisioning of system settings and phonebook is supported. Provisioning of software upgrade is not supported in this release.

The Administrator Settings menu on the Touch controller can be password protected. This is done from a command line interface with an API (Application Programmer Interface) command. The password protection options are described in the EX Series Administrator Guide.
Introduction

The advanced configurations

NOTE: Many of the system configurations are available in the Administrator Settings menu on the touch controller. To access all the system configurations you must use the web interface. Go to: Using the web interface section to see a description of the web interface.

New settings

Video Input Source [1..2]/[1..3] Type
- Note that EX60 has two and EX90 has three video input sources.

Settings that have changed

Cameras Camera 1 Focus Mode (EX90 only)
- Renamed argument “ContinuousAuto”

Provisioning Mode
- Added argument “VCS”

Settings that have been removed

SystemUnit MenuType
SystemUnit Type

Experimental settings

The Experimental settings are beta settings. These settings can be used ‘as is’, and are not fully documented.

NOTE: The Experimental settings are likely to change.

New settings

Experimental NetworkServices UPnP Mode
Experimental NetworkServices UPnP Timeout
Experimental SystemUnit MenuType
EX90 system overview

The system is delivered with:

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

Detach the rear side cover when connecting cables.
When finished, snap on the rear cover.

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

A handset can be mounted to the touch screen controller.
EX60 System Overview

The system is delivered with:

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

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

A handset can be mounted to the touch screen controller.

Detach the rear side cover when connecting cables.
When finished, snap on the rear cover.
The Cisco TelePresence System EX90/EX60 can be configured using the touch screen controller and from the web interface. The touch screen controller and its use are described in the EX90 and EX60 User Guides. For full access to the configurable parameters, the web interface must be used—the touch screen controller provides access to a limited set of parameters only.

CHAPTER 2
USING THE WEB INTERFACE
The web interface

The web interface allows for remote administration of the system.

Connect to the EX90/EX60

Open a web browser and enter the IP address of the codec.

How to find the IP address:

- To find the IP address, open the System Information page on the touch screen controller. Tap the Settings icon, select System Information and find the IP Address.

Password protection

The web interface can be password protected. It uses the same user name and password as defined for the codec that is integrated in the EX90/EX60.

Read more about password protection in the Password Protection section in this guide.
Menu options

You will find the interactive menus on the left-hand side of the web interface. When you click a menu option, a corresponding web page will open.

The role of the logged in user determines which menu options are available. You can read more about user roles in the User management section.

The user name of the signed in user is always displayed in the upper right corner.

The table below shows which menu options are available for users having ADMIN, AUDIT or USER roles. Note that the default admin user holds all three roles.

<table>
<thead>
<tr>
<th>Menu Option</th>
<th>ADMIN</th>
<th>AUDIT</th>
<th>USER</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Information</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Call</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapshot (not applicable for EX90/EX60)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Users</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Change Password</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wallpaper</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Logon Banner</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Upload Certificates</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Audit Certificate</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Logs</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>XML Files</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Upgrade Software</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Configuration</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Restart</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Sign Out</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

The signed in user

Interactive menus

Click on the menu items to access the pages. Which menu options are available depends on the role of the logged in user.
The system information page

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

System information

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.
Using the web interface

Making calls 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.

Make 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 Call rate in the drop down list.

The call status page

The call status page appear when you make a call. Please allow for approximately 30 seconds after the call is up before checking call details.

You will find the following information on the call status page:

- Remote number
- Status: Connected
- Direction: Incoming/Outgoing
- Protocol: H323/SIP
- Transmit and receive call rate
- Encryption
- Audio: transmit and receive protocols
- Video: transmit and receive protocols and resolutions
- Presentation: transmit and receive protocols and resolutions
User management

From this page you can manage the user accounts of your video system. You can create a new user, edit the details of an existing user, and delete a user. You need ADMIN rights to perform these tasks.

User roles

You must assign one or more user roles to a user account. Three user roles, which possess different system rights, are defined:

- **ADMIN**: A user with ADMIN rights can create a new user and change all settings, except the security audit configurations. 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.

The roles ADMIN, USER and AUDIT have non-overlapping rights, but a user can be created with one or more roles to combine the rights of more than one role.

**NOTE**: It is very important that at least one user has ADMIN rights at all times.

The default user account

The system comes with a default user account. The user name is admin with no password set. The admin user possesses USER, ADMIN and AUDIT roles.

It is highly recommended to set a password for this user.

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 login.
User management, continued...

If you have ADMIN rights you can manage users as described below.

Create 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.
3. Set the Status to Active to activate the user.
4. Press Save to save the changes.

Edit 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.

Deactivate 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.

Delete a user account
1. Select the name of the user to open the Editing user window.
2. Press Delete.
   NOTE: Do not delete all users with ADMIN rights.
Changing your password

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

NOTE: It is highly recommended to set a password for all users with ADMIN rights.
The password is a string with 0-255 characters.

Change 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.
2. Press **Change password** to change the password.
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 screen controller. When you choose a new predefined wallpaper on the touch screen, it will appear on both screens and replace your custom wall paper.

File format and picture size

The picture file format for the custom wallpaper is PNG. The maximum size is $1920 \times 1200$ pixels.

Upload the custom wallpaper file

1. Press Browse... and locate the wallpaper file (.PNG)
2. Press Upload to save the file to the codec.
3. Refresh the web page to see the wallpaper you just uploaded.

Activate the new wallpaper

1. Move to the Advanced configuration page and enter wallpaper in the search field. From the drop down list, select Custom. The new wallpaper will be displayed on screen.
2. If the new wallpaper does not show on screen, you may have to toggle once between Wallpaper: None and Custom to put the change into effect.
Adding a logon banner

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

The message will be shown, whether the user signs in using the menu system, the web interface or the command line interface.

Add a logon banner

1. Enter the text message, which you want to present to the user prior to signing in, in the Logon Banner text area.
2. Press Submit Changes to activate the message.
Using the web interface

Certificates

Using the web interface

Certificates

Uploading certificates
The SSL certificate is a text file which verifies the authenticity of your codec. 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 codec to trust.

Upload 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.
• Press Browse... and locate the HTTPS certificate file (.PEM format).
• Press Browse... and locate the Private key file (.PEM format).
• Enter the Passphrase.
• Press Upload to upload the certificate to the codec.

Upload 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.
• Press Browse... and locate the file with the Trusted CA list (.PEM format).
• Press Upload to upload the certificate to the codec.
Audit certificate

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

Audit logging is disabled by default, and must be enabled using the on screen menu, the web interface or the command line interface.

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.
• Press Browse... and locate the file with the audit list file (.PEM format).
• Press Upload to upload the certificate to the codec.

Enable secure audit logging

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

1. Navigate to Advanced Configuration > Security > Audit > Server and enter the IP address of the audit server.
2. Navigate to Advanced Configuration > Security > Audit > Logging > Mode and set it to ExternalSecure.
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

Time stamped event log files. Select **Current log files** and click on a text file to view the file. Right click on a file and follow the instructions in the dialog box to save the file.

Historical log files

Time stamped historical log files. Select **Historical log files**, click on a file and follow the instructions in the dialog box to save the file.
Viewing 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.
- The **Directory** file will be described later.
- Select **Valuespace** to see an overview of the value spaces.
- The **Documentation** file will be described later.
Software upgrade

From this page you can do software upgrades and add a release key and option keys.

Software versions

EX90/EX60 are using the 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).

Software download

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 any of 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 options available are:
- Premium resolution
- Multisite (only EX90)
- Dual display (only EX90)
Contact your Cisco representative to obtain the option key(s).

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 valid procedure will be:
1. Enter the release key and press Add.
The key format: "1TC001-1-0C22E348" (each system will have a unique key).
2. Enter the option key and press Add.
The key format: "1N000-1-AA7A4A09" (each system will have a unique key).
3. If you have more than one option key, add the remaining keys.

Upgrade the software on the codec

4. 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).
5. Press Browse... and select the .PKG file.
6. Press the Upgrade button to start the installation.
7. 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.
Advanced configuration

The web interface allows for remote administration of the system.

The Advanced configuration defines the system settings and are structured in a hierarchy, making up a database of system settings.

The system settings are further explained in the Advanced configuration chapter in this guide.

The search functionality

When searching for words such as H323 or SIP, all settings beginning with these words, included all settings below in the hierarchy, will show 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.

Change the system settings

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

Value space: The value space is specified, either as a drop down list or as text, when you edit a value.

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

Cancel: Select cancel to leave without saving.
Restarting the system

To restart the system, press Restart now.

Restarting the system takes a few minutes.
The EX90/EX60 can be configured via the touch screen controller or via its web interface. For full access to the configurable parameters, the web interface must be used—the touch screen controller provides access to a limited set of parameters only.

CHAPTER 3
THE ADVANCED CONFIGURATION
Description of the advanced configuration 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.

Open a web browser and enter the IP address of the EX90/EX60. To find the IP address, open the System Information page on the touch screen controller. Tap the **Settings** icon, select **System Information** and find the **IP Address**.
The Network Services settings

- Network Services H323 Mode
- Network Services HTTP Mode
- Network Services HTTPS Mode
- Network Services HTTPS VerifyClientCertificate
- Network Services HTTPS VerifyServerCertificate
- Network Services NTP Address
- Network Services NTP Mode
- Network Services SIP Mode
- Network Services SNMP CommunityName
- Network Services SNMP Host [1..3] Address
- Network Services SNMP Mode
- Network Services SNMP SystemContact
- Network Services SNMP SystemLocation
- Network Services SSH AllowPublicKey
- Network Services SSH Mode
- Network Services Telnet Mode

The Phonebook settings

- Phonebook Server [1..1] ID
- Phonebook Server [1..1] Type
- Phonebook Server [1..1] URL

The Provisioning settings

- Provisioning ExternalManager Address
- Provisioning ExternalManager Domain
- Provisioning ExternalManager Path
- Provisioning ExternalManager Protocol
- Provisioning HttpMethod
- Provisioning LoginName
- Provisioning Mode
- Provisioning Password

The Security settings

- Security Audit Logging Mode
- Security Audit OnError Action
- Security Audit Server Address
- Security Audit Server Port
- Security Session InactivityTimeout

The Serial Port settings

- SerialPort BaudRate
- SerialPort LoginRequired
- SerialPort Mode
### The SIP settings

- SIP Profile [1..1] Authentication [1..1] LoginName ........................................ 47
- SIP Profile [1..1] Authentication [1..1] Password ........................................... 47
- SIP Profile [1..1] DefaultTransport ................................................................. 47
- SIP Profile [1..1] Outbound ........................................................................... 47
- SIP Profile [1..1] Proxy [1..4] Address .............................................................. 47
- SIP Profile [1..1] Proxy [1..4] Discovery ............................................................ 47
- SIP Profile [1..1] TisVerify ............................................................................ 47
- SIP Profile [1..1] Type .................................................................................. 47
- SIP Profile [1..1] URI .................................................................................. 47

### The Standby settings

- Standby BootAction .................................................................................... 48
- Standby Control ......................................................................................... 48
- Standby Delay ............................................................................................ 48
- Standby StandbyAction ............................................................................... 48
- Standby WakeupAction ............................................................................... 48

### The SystemUnit settings

- SystemUnit CallLogging Mode ...................................................................... 49
- SystemUnit ContactInfo Type ....................................................................... 49
- SystemUnit IrSensor Mode .......................................................................... 49
- SystemUnit MenuLanguage .......................................................................... 49
- SystemUnit Name ........................................................................................ 49

### The Time settings

- Time DateFormat .......................................................................................... 50
- Time TimeFormat .......................................................................................... 50
- Time Zone....................................................................................................... 50

### The Video settings

- Video ControlPanel Brightness ...................................................................... 50
- Video DefaultPresentationSource ................................................................. 50
- Video Input DVI [2] [1] Type ......................................................................... 50
- Video Input Source [1..3] [1..2] CameraControl Camerald .................................. 50
- Video Input Source [1..3] [1..2] CameraControl Mode ..................................... 50
- Video Input Source [1..3] [1..2] Name .............................................................. 50
- Video Input Source [1..3] [1..2] OptimalDefinition Profile .................................. 50
- Video Input Source [1..3] [1..2] OptimalDefinition Threshold60fps ............... 50
- Video Input Source [1..3] [1..2] Quality ........................................................... 50
- Video Input Source [1..3] [1..2] Type ............................................................... 50
- Video Input Source 1 Connector ................................................................... 50
- Video Input Source 2 Connector ................................................................... 50
- Video Input Source 3 Connector ................................................................... 50
- Video Layout LocalLayoutFamily ................................................................... 50
- Video Layout RemoteLayoutFamily ............................................................... 50
- Video Layout ScaleToFrame .......................................................................... 50
- Video Layout ScaleToFrameThreshold ......................................................... 50
- Video Layout Scaling .................................................................................... 50
- Video MainVideoSource ............................................................................... 50
- Video Monitors ............................................................................................. 50
- Video OSD InputMethod Cyrillic ..................................................................... 50
- Video OSD InputMethod InputLanguage ....................................................... 50
- Video OSD LoginRequired ........................................................................... 50
- Video OSD Mode .......................................................................................... 50
- Video OSD MyContactsExpanded .................................................................. 50
- Video OSD Output .......................................................................................... 50
- Video OSD TodaysBookings .......................................................................... 50
- Video Output HDMI [1] MonitorRole ............................................................. 50
- Video Output HDMI [1] OverscanLevel .......................................................... 50
- Video Output HDMI [1] Resolution ............................................................... 50
- Video Output LCD [2] [1] Blue ...................................................................... 50
- Video Output LCD [2] [1] Brightness .............................................................. 50
- Video Output LCD [2] [1] Red........................................................................ 50
- Video Output LCD [2] [1] Resolution ............................................................ 50
- Video Selfview .............................................................................................. 50
- Video Wallpaper ............................................................................................ 50
## Advanced configuration

### The Experimental settings

- Experimental Audio Panning MaxAngle .......................................................... 56
- Experimental Audio Panning Mode ................................................................. 56
- Experimental Audio Panning MonitorLeft ..................................................... 56
- Experimental Audio Panning MonitorRight .................................................. 56
- Experimental CapsetFilter ........................................................................... 57
- Experimental Conference [1..1] PacketLossResilience ForwardErrorCorrection ........ 56
- Experimental NetworkServices UPnP Mode .................................................. 57
- Experimental NetworkServices UPnP Timeout .............................................. 57
- Experimental SoftwareUpgrade Mode .......................................................... 56
- Experimental SoftwareUpgrade ServerAddress .......................................... 56
- Experimental SystemUnit MenuType ............................................................ 57
- Experimental Video OSD AlertOnIncomingCall ............................................. 56
The Audio settings

Audio Volume Handset
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 Volume Handset: 70

Audio Volume Headset
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 Volume Headset: 70

Audio Preferred Output Connector
Select the preferred connector for the audio out. When the handset is in use the audio out goes to the handset, and when hung up the audio out goes to the preferred output connector.
Requires user role: ADMIN
Value space: <None/HDMI/Internal/BlueTooth/Handset/Headset>
  None: The default audio output is the internal speaker.
  HDMI: The audio out goes to the HDMI audio channel.
  Internal: The audio out goes to the internal loudspeaker. NOTE: Requires the "Audio Internal Speaker Mode" to be enabled.
  BlueTooth: The audio out goes to the Bluetooth device (for future use).
  Handset: The audio out goes to the handset.
  Headset: The audio out goes to the headset.
Example: Audio Preferred Output Connector: Internal

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

Audio Internal Speaker 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 Internal Speaker Mode: On

Audio Sounds And Alerts Ring Volume
Sets the ring tone volume for an incoming call. The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Volume 0 = Off.
Requires user role: USER
Value space: <0..100>
  Range: Select a value from 0 to 100.
Example: Audio Sounds And Alerts Ring Volume: 50

Audio Sounds And Alerts Ring Tone
Selects the ringtone for incoming calls.
Requires user role: USER
Value space: <Marbles/IceCrystals/Polaris/Alert/Discreet/Fantasy/Jazz/Nordic/Echo/Rhythmic>
  Select a tone from the list of ringtones.
Example: Audio Sounds And Alerts Ring Tone: Jazz

Audio Sounds And Alerts Key Tones Mode
Not applicable in this version.
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/60Hz**: Set to 50 Hz or 60 Hz.

Example: Cameras PowerLine Frequency: Auto

**Cameras Camera [1..1] Backlight**
The backlight functionality compensates for lights 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] Mirror**
Not applicable in this version.

**Cameras Camera [1..1] Flip**
Not applicable in this version.

**Cameras Camera [1..1] IrSensor**
Not applicable in this version.

**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] 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] Whitebalance Mode**
Set the camera whitebalance mode.

Requires user role: ADMIN

Value space: <Auto/Manual>
- **Auto**: When set to Auto, the camera will continuously adjust the whitebalance depending on the camera view.
- **Manual**: Set to Manual to enable 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
Cameras Camera [1..1] Focus Mode
Set the camera focus mode. When moving the camera, the system will use auto focus for a few seconds to set the right focus of the new camera position.

Requires user role: ADMIN

Value space: <Auto/Manual/ContinuousAuto>

- **Auto**: The focus will be updated throughout the call. 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.
- **ContinuousAuto**: The focus is updated throughout the call, without being turned off. NOTE: Applies to EX90 only.

Example: Cameras Camera 1 Focus Mode: Auto

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

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] 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 from 64 to 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 from 64 to 6000 kbps.

Example: Conference 1 MaxReceiveCallRate: 6000

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 should be unmuted automatically when all calls are disconnected. In a meeting room or other shared resource 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: 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 mode. 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: Set to On when you want 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: When set to Off the far end can not access any of the features above on your system.
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: Enter a value from 64 to 6000 kbps.

Example: Conference 1 DefaultCall Rate: 768

Conference [1..1] VideoBandwidth Mode
Set the conference video bandwidth mode.

Requires user role: ADMIN

Value space: <Dynamic/Static>

Dynamic: The available transmit video 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: 10.0.0.1".
  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] 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"
The Network settings

**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] 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] 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] MTU**
Set the Ethernet MTU (Maximum Transmission Unit).
Requires user role: ADMIN
- **Value space:** `<400..1500>`
  - **Range:** Select a value from 400 to 1500 bytes.

**Example:** Network 1 MTU: 1500

**Network [1..1] VLAN Voice Mode**
Set the VLAN voice mode.
Requires user role: ADMIN
- **Value space:** `<Tagged/Untagged>`
  - **Tagged:** The voice packets in the VLAN network are tagged with VlanId and Priority.
  - **Untagged:** The voice packets in the VLAN network are untagged.

**Example:** Network 1 VLAN Voice Mode: Untagged

**Network [1..1] VLAN VlanId**
Set the VLAN voice ID.
Requires user role: ADMIN
- **Value space:** `<0..4096>`
  - **Range:** Select a value from 0 to 4096.

**Example:** Network 1 VLAN VlanId: 0

**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

**Network [1] VLAN Data Mode**
Set the VLAN data mode.
Requires user role: ADMIN
- **Value space:** `<Tagged/Untagged>`
  - **Tagged:** The data packets in the VLAN network are tagged with Data VlanId and Data Priority.
  - **Untagged:** The data packets in the VLAN network are untagged.

**Example:** Network 1 VLAN Data Mode: Untagged

**Network [1] VLAN Data VlanId**
Set the VLAN data ID.
Requires user role: ADMIN
- **Value space:** `<0..4096>`
  - **Range:** Select a value from 0 to 4096.

**Example:** Network 1 VLAN Data VlanId: 0
### Network [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] 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.  

### 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] IPv4 Address
Enter the static IP 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 IP 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 IP 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] 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] 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] 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] 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 AnonymousIdentity
The 802.1X Anonymous ID string is to be used as unencrypted identity with EAP (Extensible Authentication Protocol) types that support different tunneled identity, like EAP-PEAP and EAP-TTLS. If set, the anonymous ID will be used for the initial (unencrypted) EAP Identity Request.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: Network 1 IEEE8021X AnonymousIdentity: ""

Network [1..1] IEEE8021X Identity
The 802.1X Identity is the user name needed for 802.1X authentication.

Requires user role: ADMIN

Value space: <S: 0, 64>

Format: String with a maximum of 64 characters.

Example: Network 1 IEEE8021X Identity: ""

Network [1..1] IEEE8021X Password
The 802.1X Password is the password needed for 802.1X authentication.

Requires user role: ADMIN

Value space: <S: 0, 32>

Format: String with a maximum of 32 characters.

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

Network [1..1] IEEE8021X Eap Md5
Set the Md5 (Message-Digest Algorithm 5) mode. This is a Challenge Handshake Authentication Protocol that relies on a shared secret. Md5 is a Weak security.

Requires user role: ADMIN

Value space: <On/Off>

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

Example: Network 1 IEEE8021X Eap Md5: On

Network [1..1] IEEE8021X Eap TTLS
Set the TTLS (Tunneled Transport Layer Security) mode. Authenticates LAN clients without the need for client certificates. Developed by Funk Software and Certicom. Usually supported by Agere Systems, Proxim and Avaya.

Requires user role: ADMIN

Value space: <On/Off>

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

Example: Network 1 IEEE8021X Eap TTLS: On

Network [1..1] IEEE8021X Eap 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] 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 addresses or IP range.

Example: Network 1 RemoteAccess Allow: "192.168.1.231, 192.168.1.182"
The NetworkServices settings

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

Requires user role: ADMIN

Value space: <On/Off>
- **On:** The Telnet protocol is enabled.
- **Off:** The Telnet protocol is disabled. This is the factory setting.

Example: NetworkServices Telnet Mode: Off

**NetworkServices 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 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 list of trusted CA's 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 list of trusted CA's are uploaded to the system in advance.
- **Off:** Do not verify client certificates.

Example: NetworkServices HTTPS VerifyClientCertificate: Off

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

Requires user role: ADMIN

Value space: <Off/Readonly/ReadWrite>
- **Off:** Disable the SNMP network service.
- **ReadOnly:** Enable the SNMP network service for queries only.
- **ReadWrite:** Enable the SNMP network service for both queries and commands.

Example: NetworkServices SNMP Mode: ReadWrite
**NetworkServices SNMP CommunityName**

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

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: NetworkServices SNMP CommunityName: "public"

---

**NetworkServices SNMP SystemContact**

Enter the name of the Network Services SNMP System Contact.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: NetworkServices SNMP SystemContact: ""  

---

**NetworkServices SNMP SystemLocation**

Enter the name of the Network Services SNMP System Location.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: NetworkServices SNMP SystemLocation: ""  

---

**NetworkServices SNMP Host [1..3] Address**

Enter the address of up to three SNMP Managers. 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 H323 Mode**

Determine whether the system should be able to place and receive H.323 calls. 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 SIP Mode**

Determine whether the system should be able to place and receive SIP calls. 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 NTP Mode**

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

Requires user role: ADMIN

Value space: <Auto/Manual>

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

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: \( <OFF/TMS/VCS/Callway> \)
  - 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.
- 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 provisioning server supports GET.
  - POST: Select POST when the provisioning server supports POST.
  - Example: Provisioning HttpMethod: POST
Provisioning External Manager 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 External Manager 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 Network Services HTTP Mode setting.
HTTPS: Set to HTTPS to enable secure management. Requires HTTPS to be enabled in the Network Services HTTPS Mode setting.

Example: Provisioning ExternalManager Protocol: HTTP

Provisioning External Manager 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 External Manager 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 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 sends 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 InactivityTimeout
Determine how long the system will accept inactivity from the user before he is automatically logged out.

Requires user role: AUDIT

Value space: <0..10000>

Range: Select a value from 0 to 10000 seconds. 0 means the 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 port on the codec. The default value is 38400.


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 port at the codec.

Requires user role: ADMIN

Value space: <On/Off>

On: Login is required when connecting to the codec through COM port.

Off: The user can access the codec through COM 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] 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] Type
Enables SIP extensions and special behavior for a vendor or provider.
Requires user role: ADMIN
Value space: <Standard/Alcatel/Avaya/Cisco/Microsoft/Nortel/Experimental/Siemens>
- Standard: Should be used when registering to standard SIP proxy like OpenSer.
- Alcatel: Must be used when registering to a Alcatel-Lucent OmniPCX Enterprise R7 or later.
- Avaya: Must be used when registering to a Avaya Communication Manager.
- Cisco: Must be used when registering to a Cisco CallManager version 5 or later.
- Microsoft: Must be used when registering to a Microsoft LCS or OCS server.
- Nortel: Must be used when registering to a Nortel MCS 5100 or MCS 5200 PBX.
- Experimental: Can be used if auto is not working. NOTE: This mode is for testing purposes only.
Example: SIP Profile 1 Type: Standard

SIP Profile [1..1] Outbound
Requires user role: ADMIN
Value space: <On/Off>
- On: Set up multiple outbound connections to servers in the Proxy Address list.
- Off: Connect to the single proxy configured first in Proxy Address list.
Example: SIP Profile 1 Outbound: Off

SIP Profile [1..1] Proxy [1..4] Discovery
Select if the SIP Proxy address is to be obtained manually or by using Dynamic Host Configuration Protocol (DHCP).
Requires user role: ADMIN
Value space: <Auto/Manual>
- Manual: When Manual is selected, the manually configured SIP Proxy address will be used.
- Auto: When Auto is selected, the SIP Proxy address is obtained using Dynamic Host Configuration Protocol (DHCP).
Example: SIP Profile 1 Proxy 1 Discovery: Manual
**Advanced configuration**

### 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] 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:** \(<S: 0, 50>\)

**Format:** String with a maximum of 50 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:** \(<S: 0, 50>\)

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

**Example:** SIP Profile 1 Authentication 1 Password:

---

## 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 WakeupAction

Not applicable in this version.

### Standby BootAction

Not applicable in this version.

### Standby StandbyAction

Not applicable in this version.
The SystemUnit settings

**SystemUnit Name**

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

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

**Requires user role:** ADMIN

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

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

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

**SystemUnit MenuLanguage**

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

**Requires user role:** USER

**Value space:** <English>

**Example:** SystemUnit MenuLanguage: English

**SystemUnit IrSensor Mode**

Not applicable in this version.

**SystemUnit ContactInfo Type**

Not applicable in this version.

**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 GUI or using the xHistory command.

**Requires user role:** ADMIN

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

- **On:** Enable logging.
- **Off:** Disable logging.

**Example:** SystemUnit CallLogging Mode: On

---

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 (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-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, Berlink, Bern, Rome, Stockholm, Vienna) / GMT+01:00 (Brussels, Copenhagen, Madrid, Paris) / GMT+01:00 (Paris) / GMT+01:00 (Garajev, 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

---

**Video**

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

Requires user role: **ADMIN**

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

- **On:** Set to On when you want selfview to be displayed on screen.
- **Off:** Set to Off when you do not want selfview to be displayed on screen.

Example: Video Selfview: On

**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/>`

- **Wallpaper01 to Wallpaper12:** 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.

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

**MainVideoSource**
Not applicable in this version.
Video DefaultPresentationSource

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

Define which video input source shall be used as the default presentation source (e.g. when you tap View followed by Present on the touch screen). The input source is configured to a video input connector.

Requires user role: USER

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

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

Example: Video DefaultPresentationSource: 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 Input Source [1..3]/[1..2] Name

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

Enter a name for the video input source.

Requires user role: ADMIN

Value space: <S: 0, 50>

Format: String with a maximum of 50 characters.

Example: Video Input Source 1 Name: ""

Video Input Source 1 Connector

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

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

Requires user role: ADMIN

Value space: <HDMI>/<DVI>

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

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

Example: Video Input Source 1 Connector: HDMI

Video Input Source 2 Connector

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

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

Requires user role: ADMIN

Value space: <DVI>/<CAMERA>

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

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

Example: Video Input Source 2 Connector: DVI

Video Input Source 3 Connector

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

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

Requires user role: ADMIN

Value space: <CAMERA>

CAMERA (EX90): Select CAMERA when you want to use the camera as input source 3.

Example: Video Input Source 3 Connector: CAMERA

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

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

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

Requires user role: ADMIN

Value space: <camera/PC/DVD/document _ camera/other>

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.

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

Example: Video Input Source 1 Type: Camera
Video Input Source [1..3]/[1..2] Quality

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

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

Requires user role: ADMIN

Value space: <Motion/Sharpness>

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

Example: Video Input Source 1 Quality: Motion

Video Input Source [1..3]/[1..2] CameraControl Mode

Not applicable in this version.

Video Input Source [1..3]/[1..2] CameraControl CameraId

Not applicable in this version.

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

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

Adjust how rapidly the system will increase the transmitted resolution when increasing the bandwidth.

- **Requires that the Video Input Source Quality is set to Motion**.
- **NOTE**: The default transmit frame rate is set to 30 fps which is recommended for normal light conditions. In good light conditions you can also consider to allow 60 fps. To do this you need to enable 60 Hz capture frequency on the camera, which is done with the Cameras Camera 1 FrameRate setting (Cameras Camera 1 FrameRate: 60Hz).

Normal: Use this setting for normal to poorly lit environment. If the source is a camera with 1920x1080p60, the system will transmit 720p60 at about 2.2 Mb/sec and above when the Video Input Source [1..3]/[1..2] OptimalDefinition Threshold60fps is set to 1280_720 or lower.

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 720p60 at about 1.9 Mb/sec and above when the Video Input Source [1..3]/[1..2] OptimalDefinition Threshold60fps is set to 1280_720 or lower.

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 720p60 at about 1.1 Mb/sec and above when the Video Input Source [1..3]/[1..2] OptimalDefinition Threshold60fps is set to 1280_720 or lower.

Requires user role: ADMIN

Value space: <Normal/Medium/High>

Ref: Table 1 and Table 2.

Example: Video Input Source 1 OptimalDefinition Profile: Normal

<table>
<thead>
<tr>
<th>Table 1: Optimal definition, for systems supporting 1080p</th>
</tr>
</thead>
<tbody>
<tr>
<td>w288p30</td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Optimal definition, for systems supporting 720p60</th>
</tr>
</thead>
<tbody>
<tr>
<td>w144p60</td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>
Video Input Source [1..3]/[1..2] Optimal Definition Threshold 60fps

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

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

NOTE: The default transmit frame rate is set to 30 fps which is recommended for normal light conditions. In good light conditions you can also consider to allow 60 fps. To do this you need to enable 60 Hz capture frequency on the camera, which is done with the Cameras Camera 1 FrameRate setting (Cameras Camera 1 FrameRate: 60Hz).

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 60 fps.

Example: Video Input Source 1 Optimal Definition Threshold 60fps: 1280 _ 720

Video Input DVI [2][1] Type

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

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

Requires user role: USER

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 2 Type: AutoDetect

Video Output HDMI [1] Resolution

NOTE: Applies to EX90.

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

Requires user role: ADMIN

Value space: <Auto/640 _ 480 _ 60/800 _ 600 _ 60/1024 _ 768 _ 60/1280 _ 1024 _ 60/1280 _ 720 _ 60/1920 _ 1080 _ 60/1280 _ 768 _ 60/1360 _ 768 _ 60/1600 _ 1200 >

- Auto: The system will automatically try to set the optimal resolution based on negotiation with the connected monitor.
- Range: 640x480@60, 800x600@60, 1024x768@60, 1280x1024@60, 1280x720@60, 1920x1080@60, 1280x768@60, 1360x768@60, 1366x768@60, 1600x1200@60, 1920x1200@60

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

Video Output HDMI [1] MonitorRole

NOTE: Applies to EX90.

The HDMI monitor role describes what video stream will be shown on the monitor connected to the video output HDMI connector. Applicable only if the "Video > Monitors" configuration is set to dual.

Requires user role: ADMIN

Value space: <First/Second/PresentationOnly>

- 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.

Example: Video Output HDMI 1 MonitorRole: First

Video Output HDMI [1] OverscanLevel

NOTE: Applies to EX90.

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

Requires user role: ADMIN

Value space: <Medium/High/None>

- Medium: The system will not use the outer 3% of the output resolution.
- High: The system will not use the outer 6% of the output resolution.
- None: The system will use all of the output resolution.

Example: Video Output HDMI 1 OverscanLevel: None
### Advanced configuration

#### Video Output LCD [2]/[1] Resolution
NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the screen resolution.

**Requires user role:** ADMIN

**Value space:** `<1920 _ 1200 _ 60>`

**Range:** The screen resolution is 1920 x 1200 60 Hz.

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

#### Video Output LCD [2]/[1] MonitorRole
NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the LCD monitor role. 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.
- **InternalSettings:** Internal settings from the touch controller will be used.

**Example:** Video Output LCD 2 MonitorRole: InternalSetup

#### Video Output LCD [2]/[1] Brightness
NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the brightness level for the monitor.

**Requires user role:** ADMIN

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

**Range:** Select a value from 0 to 100.

**Example:** Video Output LCD 2 Brightness: 50

#### Video Output LCD [2]/[1] Red
NOTE: EX90 has the LCD 2 connector and EX60 has the LCD 1 connector.

Set the Red color level for the monitor.

**Requires user role:** ADMIN

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

**Range:** Select a value from 0 to 100.

**Example:** Video Output LCD 2 Red: 50

### 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 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 Video Layout RemoteLayoutFamily: Auto

Video OSD Mode

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 LoginRequired

Not applicable in this version.

Video OSD InputMethod InputLanguage

Not applicable in this version.

Video OSD InputMethod Cyrillic

Not applicable in this version.
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 Video OSD AlertOnIncomingCall

Not applicable in this version.

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 Audio Panning Mode

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

Requires user role: ADMIN
Value space: <Auto/Off>

Example: Experimental Audio Panning Mode: Off

Experimental SoftwareUpgrade 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: <Auto/Manual>

Example: Experimental SoftwareUpgrade Mode: Auto

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: 60

Experimental Audio Panning MonitorLeft

Requires user role: ADMIN
Value space: <1..5>

Example: Experimental Audio Panning MonitorLeft: 1

Experimental Audio Panning MonitorRight

Requires user role: ADMIN
Value space: <0..5>

Example: Experimental Audio Panning MonitorRight: 1

Experimental SoftwareUpgrade ServerAddress

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, 255>

Example: Experimental SoftwareUpgrade ServerAddress: "http://csupdate.tandberg.com/getswlist.py"
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 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
The appendices section provides you with additional information that you may find useful as a system administrator for the EX90/EX60.

CHAPTER 4

APPENDICES
Password protection

The Codec is password protected. You always need to enter a username to log in.

The same username and password is used for the web and command line interfaces.

- The default username is admin with no password set.
  
  **NOTE:** We recommend that you set a password for the admin user - see how to Change your codec password to the right.

- New user accounts with username and password can be created using the web interface.

  Read more about user rights and how to add, edit and delete a user account in the User management section.

You can also protect the File system of the codec by setting a password for the root user. The root user is disabled by default.

**NOTE:** When a new administrator password has been defined make sure you keep a copy of the password in a safe place. Contact your Cisco representative if you have forgotten the password.

---

Password settings

### Change your codec password

A user, including the default admin user, can change his codec password using the web interface or the command line interface.

If a password is not currently set, use the procedure below with a blank current password.

#### Change the password using the web interface:

1. Log in to the web interface with your username and current password.
2. Go to the Change password page.
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 0-255 characters.
4. Click *Save*.

#### Change the password using the command line interface:

1. Connect to the codec through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Log in to the codec with your username and current password.
3. Run the following API command and when prompted enter the current password, the new password, and confirm the new password:

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

### Set the Administrator settings password

You can set a password to restrict access to the Administrator Settings on the touch controller.

Open a command line interface, for example PuTTY, and run the following command:

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

### Change the user passwords

All users can change their own codec password as described to the right.

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

1. Log in to the web interface with username and password.
2. Go to the *Users* page.
3. Select the appropriate user from the list.
4. Enter a new password and PIN code.
5. Click *Save*.

### Set a root password

If you log in to the command line interface as root, you can access the codec’s file system.

The root user is disabled by default.

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

1. Connect to the codec through the network or the serial data port, using a command line interface (SSH or Telnet).
2. Log in to the codec with the username (admin) and password. You need ADMIN rights.
3. Run the following API command:

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

   **NOTE:** The root password is not the same as the administrator 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 configuration section. Go to Advanced configuration.

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>
<thead>
<tr>
<th>Table 1: Optimal definition for systems supporting 1080p</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2: Optimal definition for systems supporting 720p60</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Normal</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
</tbody>
</table>
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.
Dimensions of the EX90

The illustration shows the EX90 dimensions.

All dimensions are in mm.

EX90 weight: 11 kg (24.2 lb)
Wall mounting or arm mounting the EX60

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

When choosing a mounting solution, consider the mounting pattern, the EX60 dimensions and obstructions.

**NOTE:** Not all VESA compatible products will easily fit with the EX60.

**Dimensions of the EX60**

All dimensions are in mm.

EX60 weight: 5.85 kg (12.9 lb).
### Technical specifications

The EX90/EX60 units are delivered with a fully integrated codec, display, camera, microphone and loudspeakers, and a touch screen controller with a detachable wideband handset.

#### Technical specifications for EX90

<table>
<thead>
<tr>
<th>PRODUCT COMPATIBILITY</th>
<th>AUDIO SYSTEM</th>
<th>OPERATING TEMPERATURE AND HUMIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully compatible with standards-compliant telepresence and video systems</td>
<td>Two stereo front speakers</td>
<td>Ambient temperature: 32° F to 95° F (0° C to 35° C)</td>
</tr>
<tr>
<td>SOFTWARE COMPATIBILITY</td>
<td>Integrated full-range microphone</td>
<td>Relative Humidity (RH): 10 to 90%</td>
</tr>
<tr>
<td>Cisco TelePresence Software Version TC3.1 or later</td>
<td>One 3.5-mm line-in jack for PC or other audio source</td>
<td>Storage and transport temperature at RH 10-90% (non-condensing): -20° C to 60° C (-4° F to 140° F)</td>
</tr>
<tr>
<td>COMPONENTS</td>
<td>Two 3.5-mm jack for headset</td>
<td></td>
</tr>
<tr>
<td>Fully integrated unit including codec, display, camera, microphone and loudspeakers</td>
<td>Wideband handset</td>
<td></td>
</tr>
<tr>
<td>Cables including: DVI-I-to-VGA cable, DVI-D cable, 3.5 mm jack audio cable, LAN cable, power adapter, and power cable</td>
<td>Bluetooth-ready</td>
<td></td>
</tr>
<tr>
<td>Fully integrated unit including codec, display, camera, microphone and loudspeakers</td>
<td>Integrated subwoofer</td>
<td></td>
</tr>
<tr>
<td>Cables including: DVI-I-to-VGA cable, DVI-D cable, 3.5 mm jack audio cable, LAN cable, power adapter, and power cable</td>
<td>Support for Performance Mic 20</td>
<td></td>
</tr>
<tr>
<td>DISPLAY</td>
<td>USER INTERFACE</td>
<td></td>
</tr>
<tr>
<td>24 in. LCD monitor</td>
<td>HDMI audio input/output</td>
<td></td>
</tr>
<tr>
<td>Resolution: 1920 x 1200 (16:9)</td>
<td>EX90 MAIN UNIT DIMENSIONS</td>
<td></td>
</tr>
<tr>
<td>Contrast ratio: 1000:1</td>
<td>Height: 54.5 cm (21.4&quot;)</td>
<td></td>
</tr>
<tr>
<td>Viewing angle: 160°</td>
<td>Length: 56.7 cm (22.3&quot;)</td>
<td></td>
</tr>
<tr>
<td>Response time: 5 ms</td>
<td>Depth: 17.3 cm (6.8&quot;)</td>
<td></td>
</tr>
<tr>
<td>Brightness: 300 cd/m²</td>
<td>Weight: 11 kg (24.2 lb)</td>
<td></td>
</tr>
<tr>
<td>5° - 15° tilt</td>
<td>TOUCH SCREEN DIMENSIONS</td>
<td></td>
</tr>
<tr>
<td>PC AND SECOND SOURCE VIDEO INPUTS</td>
<td>Height: 4.4 cm (1.7&quot;)</td>
<td></td>
</tr>
<tr>
<td>DVI-I</td>
<td>7.7 cm (3.0&quot;) with handset</td>
<td></td>
</tr>
<tr>
<td>HDMI In</td>
<td>Length: 22.8 cm (9.0&quot;)</td>
<td></td>
</tr>
<tr>
<td>SVGA (800 x 600) to WUXGA (1920 x 1200)</td>
<td>29.0 cm (11.4&quot;) with handset</td>
<td></td>
</tr>
<tr>
<td>CAMERA</td>
<td>Depth: 14.5 cm (5.7&quot;)</td>
<td></td>
</tr>
<tr>
<td>Cisco TelePresence PrecisionHD design</td>
<td>18.7 cm (7.4&quot;) with headset</td>
<td></td>
</tr>
<tr>
<td>Resolutions: 1080p30 and 720p60</td>
<td>Weight: 0.64 kg (1.4 lb), 0.94 kg (2.1 lb) with headset</td>
<td></td>
</tr>
<tr>
<td>Auto focus</td>
<td>Cable length: 120 cm (47&quot;)</td>
<td></td>
</tr>
<tr>
<td>Integrated privacy shutter</td>
<td>POWER</td>
<td></td>
</tr>
<tr>
<td>Document camera mode</td>
<td>Autosensing power supply</td>
<td></td>
</tr>
<tr>
<td>Multicoated all-glass optics</td>
<td>100-240 VAC, 50/60 Hz</td>
<td></td>
</tr>
<tr>
<td>1/3-in., 2.1 megapixel CMOS sensor</td>
<td>150 watts max</td>
<td></td>
</tr>
<tr>
<td>Horizontal field of view: 45°-65°</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vertical field of view: 40°-27°</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Focus distance 0.3-∞</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optical, motorized zoom</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Cables including:**
- DVI-I-to-VGA cable
- DVI-D cable
- 3.5 mm jack audio cable
- LAN cable
- Power adapter
- Power cable

**24 in. LCD monitor**
- Resolution: 1920 x 1200 (16:9)
- Contrast ratio: 1000:1
- Viewing angle: 160°
- Response time: 5 ms
- Brightness: 300 cd/m²
- 5° - 15° tilt

**Language support**
- English

**EX90 main unit dimensions**
- Height: 54.5 cm (21.4")
- Length: 56.7 cm (22.3")
- Depth: 17.3 cm (6.8")
- Weight: 11 kg (24.2 lb)

**Touch screen dimensions**
- Height: 4.4 cm (1.7")
- 7.7 cm (3.0") with handset
- Length: 22.8 cm (9.0")
- 29.0 cm (11.4") with handset
- Depth: 14.5 cm (5.7")
- 18.7 cm (7.4") with headset
- Weight: 0.64 kg (1.4 lb), 0.94 kg (2.1 lb) with headset
- Cable length: 120 cm (47")

**Power**
- Autosensing power supply
- 100-240 VAC, 50/60 Hz
- 150 watts max

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

**Approvals**
- **EU/EEC**
  - Directive 2006/95/EC (Low Voltage Directive)
  - Standard EN 60950-1
  - 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

- **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.
## Technical specifications for EX90, continued...

### BANDWIDTH
H.323/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 488@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 720@30 fps (SXGA)
- 1280 x 720@30 fps (720p30)
- 1280 x 768@30 fps (WXGA)
- 1920 x 1080@30 fps (1080p30)*
- 1920 x 1200@25fps (WUXGA)*
- 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)*
- 1024x576@60 fps (w576p60)*
- 1280x720@60 fps (720p60)*
  - Requires premium resolution option

### AUDIO FEATURES
- CD-quality 20 kHz stereo
- Acoustic echo canceling
- Automatic gain control
- Automatic noise reduction
- Adaptive lip synchronization

### DUAL STREAM
- H.239 (H.323) dual stream
- BFCP (SIP) dual stream
- Supports resolutions up to 1080p in both main stream and dual stream simultaneously

### PROTOCOLS
- H.323
- SIP

### NETWORK INTERFACES
- Internal 2-port Ethernet switch
- 1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for PC
- 1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for LAN

### OTHER INTERFACES
- Bluetooth for future applications
- 2x USB device for future applications

### IP NETWORK FEATURES
- Domain Name System (DNS) lookup for service configuration
- Differentiated Services (QoS)
- IP adaptive bandwidth management (including flow control)
- Auto gatekeeper discovery
- Dynamic playout and lip-sync buffering
- H.245 DTMF tones in H.323
- Date and time support with Network Time Protocol (NTP)
- Packet loss based downspeeding
- DNS-based URI dialing
- TCP/IP
- Dynamic Host Configuration Protocol (DHCP)
- IEEE 802.1x network authentication
- IPv6 802.1q VLAN

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

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

### SECURITY FEATURES
- Management via Secure HTTP (HTTPS) and Secure Shell (SSH) protocol
- IP administration password
- Menu administration password
- Disable IP services
- Network settings protection

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

### SYSTEM MANAGEMENT
- Support for the Cisco TelePresence Management Suite
- Total management through embedded Simple Network Management Protocol (SNMP), Telnet, SSH, XML, and Simple Object Access Protocol (SOAP)
- Remote software upload: Through web server, Secure Copy Protocol, HTTP, and HTTPS
- DATE(TM) PRODUCT RELIABILITY/MTBF
- The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:
  - Power On Hours (POH) > 69 000 hours.
  - Useful Life Cycle > 6 years.
- ISO 9001 certificate is available upon request

February 2011
Technical specifications for EX60

<table>
<thead>
<tr>
<th>PRODUCT COMPATIBILITY</th>
<th>AUDIO SYSTEM</th>
<th>OPERATING TEMPERATURE AND HUMIDITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully compatible with standards-compliant telepresence and video systems</td>
<td>Two stereo front speakers</td>
<td>Ambient temperature: 32° F to 95° F (0° C to 35° C)</td>
</tr>
<tr>
<td>SOFTWARE COMPATIBILITY</td>
<td>Integrated full-range microphone</td>
<td>Relative Humidity (RH): 10 to 90%</td>
</tr>
<tr>
<td>Cisco TelePresence Software Version TC4.0 or later</td>
<td>One 3.5-mm line-in jack for PC or other audio source</td>
<td>Storage and transport temperature at RH 10-90% (non-condensing): -20° C to 60° C (-4° F to 140° F)</td>
</tr>
<tr>
<td>COMPONENTS</td>
<td>Two 3.5-mm jack for headset</td>
<td>APPROVALS</td>
</tr>
<tr>
<td>Fully integrated unit including codec, display, camera, microphone and loudspeakers</td>
<td>Wideband handset</td>
<td>EU/EEC</td>
</tr>
<tr>
<td>Cables including: DVI-I-to-VGA cable, DVI-D cable, 3.5 mm jack audio cable, LAN cable, power adapter, and power cable</td>
<td>Bluetooth-ready</td>
<td>Directive 2006/95/EC (Low Voltage Directive)</td>
</tr>
<tr>
<td>DISPLAY</td>
<td>USER INTERFACE</td>
<td>– Standard EN 60950-1</td>
</tr>
<tr>
<td>Resolution: 1920 x 1080 (16:9)</td>
<td>Eight-inch projected capacitive touch screen</td>
<td>– Standard EN 55022, Class A</td>
</tr>
<tr>
<td>Contrast ratio: 1000:1</td>
<td>Resolution: 480 x 800</td>
<td>– Standard EN 55024</td>
</tr>
<tr>
<td>Viewing angle: 170°</td>
<td></td>
<td>– Standard EN 61000-3-2/-3-3</td>
</tr>
<tr>
<td>Response time: 5 ms</td>
<td>LANGUAGE SUPPORT</td>
<td>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.</td>
</tr>
<tr>
<td>Brightness: 225 cd/m²</td>
<td>English</td>
<td>USA</td>
</tr>
<tr>
<td>PC AND SECOND SOURCE VIDEO INPUTS</td>
<td>TOUCH SCREEN DIMENSIONS</td>
<td>Approved according to UL 60950-1</td>
</tr>
<tr>
<td>DVI-I</td>
<td>Height: 4.4 cm (1.7&quot;)</td>
<td>Complies with FCC15B Class A</td>
</tr>
<tr>
<td>SUPPORTED PC INPUT RESOLUTIONS</td>
<td>7.7 cm (3.0&quot;) with handset</td>
<td>Canada</td>
</tr>
<tr>
<td>SVGA (800 x 600) to 1080p (1920 x 1080)</td>
<td>Length: 22.6 cm (9.0&quot;)</td>
<td>Approved according to CAN/CSA C22.2 No. 60950-1</td>
</tr>
<tr>
<td>CAMERA</td>
<td>29.0 cm (11.4&quot;) with handset</td>
<td>This Class A digital apparatus complies with Canadian ICES-003.</td>
</tr>
<tr>
<td>Cisco TelePresence PrecisionHD design</td>
<td>Depth: 14.5 cm (5.7&quot;)</td>
<td>Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.</td>
</tr>
<tr>
<td>Resolutions: 1080p30 and 720p60</td>
<td>Weight: 0.64 kg (1.4 lb)</td>
<td></td>
</tr>
<tr>
<td>Auto focus</td>
<td>18.7 cm (7.4&quot;) with handset</td>
<td></td>
</tr>
<tr>
<td>Integrated privacy shutter</td>
<td>Weight: 0.94 kg (2.1 lb) with handset</td>
<td></td>
</tr>
<tr>
<td>Document camera mode</td>
<td>Cable length: 120 cm (47&quot;)</td>
<td></td>
</tr>
<tr>
<td>Multicoated all-glass optics</td>
<td>TOUCH SCREEN DIMENSIONS</td>
<td></td>
</tr>
<tr>
<td>1/3-in., 2.1 megapixel CMOS sensor</td>
<td>Height: 4.4 cm (1.7&quot;)</td>
<td></td>
</tr>
<tr>
<td>Horizontal field of view: 50°</td>
<td>7.7 cm (3.0&quot;) with handset</td>
<td></td>
</tr>
<tr>
<td>Vertical field of view: 29°</td>
<td>Length: 22.6 cm (9.0&quot;)</td>
<td></td>
</tr>
<tr>
<td>Focus distance 0.1-infinity</td>
<td>29.0 cm (11.4&quot;) with handset</td>
<td></td>
</tr>
<tr>
<td>POWER</td>
<td>Autosensing power supply</td>
<td>100-240 VAC, 50/60 Hz</td>
</tr>
<tr>
<td>100-240 VAC, 50/60 Hz</td>
<td>75 watts max</td>
<td></td>
</tr>
</tbody>
</table>
### Technical specifications for EX60, continued...

#### BANDWIDTH
H.323/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)
- 704 x 576@30 fps (w576p)
- 768 x 576@30 fps (w576p)
- 800 x 600@30 fps (SVGA)
- 1024 x 576@30 fps (w576p)
- 1280 x 768@30 fps (WXGA)
- 1280 x 720@30 fps (720p60)*
- 1024 x 768@30 fps (XGA)
- 800 x 576@30 fps (w576p)
- 720 x 576@30 fps (w576p)
- 640 x 480@30 fps (VGA)
- 640 x 480@30 fps (VGA)
- 1024 x 768@30 fps (XGA)
- 1280 x 768@30 fps (WXGA)
- 1280 x 720@30 fps (720p30)
- 1280 x 768@30 fps (WXGA)
- 1024 x 1080@30 fps (1080p30)*
- 1440 x 900@30 fps (WXGA+)*
- 1680 x 1050@30 fps (WXGA+)*
- 1600 x 1200@30 fps (UXGA)*
- 1280 x 720@60 fps (720p60)*
- 1024 x 576@60 fps (w576p60)*
- 768 x 448@60 fps (w448p60)*
- 2304x1760@60 fps (1080p30)*
- 1920 x 1080@30 fps (1080p30)*

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

#### PROTOCOLS
- H.323
- SIP

#### NETWORK INTERFACES
- Internal 2-port Ethernet switch
- 1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for PC
- 1 x LAN/Ethernet (RJ-45) 10/100/1000 Mbit for LAN

#### OTHER INTERFACES
- Bluetooth for future applications
- 1x USB device for future applications

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

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

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

#### SECURITY FEATURES
- Management via Secure HTTP (HTTPS) and Secure Shell (SSH) protocol
- IP administration password
- Menu administration password
- Disable IP services
- Network settings protection

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

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

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

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

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

### MTBF PRODUCT RELIABILITY/MTBF
The predicted reliability is expressed in the expected random Mean Time Between Failures (MTBF) for the electronic components based on the Power On Hours:
- Power On Hours (POH) > 69 000 hours.
- Useful Life Cycle > 6 years.
- ISO 9001 certificate is available upon request

February 2011
On our web site you will find an overview of the worldwide Cisco contacts.

Go to: [http://www.cisco.com/web/siteassets/contacts](http://www.cisco.com/web/siteassets/contacts)

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

---

**Disclaimer**

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.