Thank you for choosing Cisco!

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

This part of the product documentation is aimed at administrators working with the setup and configuration of the video 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 http://www.cisco.com/go/dx-docs

How to use this guide

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

---

Table of contents

- **Introduction** ................................................................. 4
  - User documentation and software .................................. 5
  - What's new in CE8.3...................................................... 6
  - DX70 and DX80 at a glance .......................................... 10
  - Power On and Off ......................................................... 11
  - LED indicators .............................................................. 12
  - How to administer the video system................................ 13

- **Configuration** ......................................................................................... 17
  - User administration .......................................................... 18
  - Change the system passphrase ......................................... 19
  - Set a PIN code for the on-screen Settings menu ............... 20
  - System configuration ......................................................... 21
  - Add a sign in banner ......................................................... 22
  - Manage the service certificates of the video system .......... 23
  - Manage the list of trusted certificate authorities (CAs) ...... 24
  - Set up secure audit logging ............................................. 25
  - Manage pre-installed certificates for CUCM via Expressway provisioning .................................................. 26
  - Delete CUCM trust lists ................................................... 27
  - Change the persistency mode .......................................... 28
  - Set strong security mode ............................................... 29
  - Set up Intelligent Proximity for content sharing ............... 30
  - Adjust the video quality to call rate ratio ........................ 35
  - Packet loss resilience - ClearPath ................................... 36
  - Choose wallpaper ........................................................... 37
  - Choose a ringtone and set the ringtone volume ............... 38
  - Manage local contacts ..................................................... 39

- **Peripherals** ....................................................................................... 40
  - Connect a computer ......................................................... 41
  - Extend the number of input sources ............................... 42

- **Maintenance** .................................................................................... 43
  - Upgrade the system software ............................................. 44
  - Add option keys ................................................................ 46
  - System status ................................................................... 47
  - Run diagnostics .................................................................. 48
  - Download log files ............................................................ 49
  - Create a remote support user ............................................ 50
  - Backup or restore a configuration .................................... 51
System settings ........................................................................................................................................ 57
Overview of the system settings ........................................................................................................ 58
Audio settings ........................................................................................................................................ 62
Conference settings ............................................................................................................................. 65
FacilityService settings ......................................................................................................................... 69
H323 settings ......................................................................................................................................... 70
Logging settings ..................................................................................................................................... 73
Network settings .................................................................................................................................... 74
NetworkServices settings ....................................................................................................................... 81
Peripherals settings ............................................................................................................................... 86
Phonebook settings ............................................................................................................................... 87
Provisioning settings ............................................................................................................................. 88
Proximity settings ................................................................................................................................. 91
RoomReset settings ............................................................................................................................... 92
RTP settings ........................................................................................................................................... 93
Security settings ..................................................................................................................................... 94
SerialPort settings ................................................................................................................................. 96
SIP settings ............................................................................................................................................ 97
Standby settings ................................................................................................................................... 101
SystemUnit settings .............................................................................................................................. 102
Time settings .......................................................................................................................................... 103
UserInterface settings ............................................................................................................................ 106
UserManagement settings ..................................................................................................................... 108
Video settings ......................................................................................................................................... 110
Experimental settings ............................................................................................................................ 117

Appendices ........................................................................................................................................... 118
The user interface .................................................................................................................................. 119
Set up remote monitoring ....................................................................................................................... 120
Access call information while using the web interface ......................................................................... 121
Place a call using the web interface ..................................................................................................... 122
Share content using the web interface ................................................................................................. 124
Local layout control ............................................................................................................................... 125
Control a far end camera ....................................................................................................................... 126
Add in-room controls to the user interface .......................................................................................... 127
Manage startup scripts .......................................................................................................................... 128
Access the video system’s XML files ..................................................................................................... 129
Execute API commands and configurations from the web interface .................................................. 130
Serial interface ..................................................................................................................................... 131
Technical specification ........................................................................................................................ 134
Supported RFCs ..................................................................................................................................... 134
User documentation on the Cisco web site ......................................................................................... 135
Cisco contacts ....................................................................................................................................... 136
Chapter 1

Introduction
User documentation and software

Products covered in this guide
- Cisco TelePresence DX70
- Cisco TelePresence DX80

From Collaboration Software version 8.2 (CE8.2) all DX80 and DX70 units can run CE software, which is the same software that runs on the Cisco TelePresence SX and MX Series.

Note that Cisco DX650 is not, and will not be, supported by CE software.

This guide does not cover information on Cisco Spark registered systems. For more information on Cisco Spark room systems, visit:

► https://help.webex.com/community/cisco-cloud-collab-mgmt

Software migration to CE software
Cisco DX80 and Cisco DX70 were originally shipped with Android based software. Before migrating to CE software, it is important to carefully consider the conversion requirements and the functionality changes compared to Android based software; otherwise migration can leave you with a non-functional deployment that requires you to convert back.

Refer to the software release notes, and the Upgrade the system software chapter for further details.

User documentation
This guide provides you with the information required to administrate the endpoint. How to install the endpoint is covered in the Installation guide, and the required initial configurations are described in the Getting started guide.

Refer to the User documentation on the Cisco web site appendix for more information about the guides for this endpoint.

Downloading the user documentation
Visit the Cisco web site regularly for updated versions of the guides:

► http://www.cisco.com/go/dx-docs

Cisco Project Workplace
Explore the Cisco Project Workplace to find inspiration and guidelines when preparing an office or meeting room for video conferencing:

► http://www.cisco.com/go/projectworkplace

Software
Download software for the endpoint from the Cisco web site:

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

We recommend reading the Software release notes (CE8):

What’s new in CE8.3

This chapter provides an overview of the new and changed system settings, and the new features and improvements in the Cisco Collaboration Endpoint software version 8.3 (CE8.3).

For more details, we recommend reading the Software release notes:

New features and improvements in CE8.3

Wi-Fi
DX70 and DX80 video systems that are shipped with a built-in Wi-Fi adapter, can connect to the network either via Ethernet or Wi-Fi.

The video system supports the following standards for Wi-Fi:
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

In addition to open networks (not secured), the following security protocols are supported:
- WPA-PSK (AES)
- WPA2-PSK (AES)

The video system cannot connect to both Ethernet and Wi-Fi at the same time. If connected, Ethernet takes precedence over Wi-Fi, and you must disconnect the Ethernet cable in order to use Wi-Fi.

Intelligent Proximity for content sharing
In alignment with the other video systems running CE software, DX70 and DX80 now support Cisco Proximity. Cisco Proximity allows you to automatically pair your smartphone, tablet, or laptop with the video system when the device comes within range. This feature is disabled by default, but you can enable it from the web interface or xAPI.

DX70 and DX80 support the same services as other video systems with CE software:
- Content sharing to mobile clients (only when in a call due to privacy concerns)
- Content sharing from desktop clients
- Basic call control from mobile clients

Cisco recommends only one video system with Proximity enabled per room. More systems may cause unstable pairing conditions. The maximum number of simultaneous Proximity connections is three.

The Cisco Proximity clients for smartphones and tablets (Android and iOS), and laptops (Windows and OS X) can be downloaded from ► http://proximity.cisco.com. Clients for smartphones and tablets are also available through Google Play (Android) and Apple App Store (iOS).
More Cisco UCM features

Multiple Cisco UCM features, which are already supported by the other video systems that are running CE software, are enabled:

- Voicemail
- Shared lines
- Extension mobility
- Forward all calls
- Consultative add and transfer
  - Allows you to consult with the person you intend to add or transfer to before completing the action
- Multiple calls on hold, and merge calls

IEEE 802.1x authentication for devices connected to the computer network port

IEEE 802.1x authentication is enabled on the computer network port of DX70 and DX80. This means that devices connected to this port can authenticate using this protocol.

In-Room Controls

With In-Room Control you can customize the video system's user interface to allow control of peripherals in your room, for example lights and blinds. You get a consistent user experience when the video system and other peripherals in the room are controlled from the same device.

You may experience low resolution graphics in the first release. Also see the Release Note.

For more information about setting up the In-Room Control feature, refer to the user guide: [http://www.cisco.com/go/in-room-control-docs](http://www.cisco.com/go/in-room-control-docs)

Control of an external video switch with additional input sources

You can customize our touch user interfaces to include input sources that are connected to third-party external video switches. These external input sources will appear and behave just as a video source that is connected directly to the video system. You don’t have to swap cables or change the physical input source manually.

The number of external input sources you can create depends on how many inputs the video switches allow. Cisco recommends maximum 50 sources.

The video switch must be supported by a third-party control system, for example from Crestron or AMX, which can interact with the video system’s xAPI. It is the control system, not the video system, that controls the video switch.

For more information about how to customize the user interface, and how to use the xAPI to set up this feature, refer to the user guide: [http://www.cisco.com/go/in-room-control-docs](http://www.cisco.com/go/in-room-control-docs)

ActiveControl in CMS 2.1 hosted conferences

ActiveControl is a SIP-only feature that has been supported for a while for video systems in Cisco TelePresence Server hosted conferences.

From CE8.3 ActiveControl is also supported in CMS 2.1 hosted conferences. It is enabled by default on the video system, and can be used as long as it is supported by the infrastructure as well (auto-negotiation).

New ActiveControl functionality:

- When the video system is muted from the server side, the mute indicator is shown on screen and the microphone’s mute LED is lit.
- Best effort encryption is used by default.
- An automatic layout is introduced as default. Who is shown in the automatic layout is based on recent active speakers.
- Recording status indicator shown on screen.
- ActiveControl functionality available from the Call Control page on the web interface, for example participant list, participant mute indicator, and drop participant button.

Media channel details available in the xAPI

Media channels contains information about audio, video and data for ongoing calls. You can monitor the channel rate, packet loss, jitter, video frame rate, and more from the xAPI.

Sign in to the xAPI as an admin user and run xStatus MediaChannels to see the media channel details. You can also check the media channel status on the Status page in the web interface.
HTTP feedback in JSON format

HTTP feedback can be sent in JSON (JavaScript Object Notation) format for third-party feedback interpreters, as an alternative to XML (eXtensible Markup Language).

TMS uses XML by default, and does not support JSON formatted feedback.

Configurable network speed

You can configure the Ethernet link speed from the web interface or the xAPI. This is in alignment with other video systems running CE software.

You can choose to autonegotiate the link speed (default), or force it to:

- 10 Mbps half-duplex
- 10 Mbps full-duplex
- 100 Mbps half-duplex
- 100 Mbps full-duplex
- 1 Gbps full-duplex

In general, we recommend not to change from the default value, where the video system negotiates with the network to set the speed automatically.

Keypad for DTMF tones available on the web interface

We have added a keypad to the Call Control page of the web interface. The keypad is available when in call, and can be used to send DTMF tones to the far end when required.

New languages

We have added support for EnglishUK and SpanishLatin to the on-screen display and user interfaces.
System configuration changes in CE8.3

New configurations
Network [1] Speed
NetworkServices WIFI Allowed
NetworkServices WIFI Enabled
Peripherals Profile ControlSystems
Proximity Mode
Proximity Services CallControl
Proximity Services ContentShare FromClients
Proximity Services ContentShare ToClients
Standby AudioMotionDetection

Configurations that are removed
SIP Ice OfferTcpCandidates
Moved to Experimental

Configurations that are modified
H323 Encryption KeySize
  OLD: Default value: Max1024bit
  NEW: Default value: Min1024bit
Logging External Server Port
  OLD: Default value: 0
  NEW: Default value: 514
Network [1] *
  OLD: User role: Admin
  NEW: User role: Admin, User
UserInterface/Language
  Change: EnglishUK and SpanishLatin added to value space
UserInterface OSD Output
  OLD: 1 / 2 / 3 / Auto
  Default value: 1
  NEW: Auto
  Default value: Auto
Video Monitors
  OLD: Auto / Dual / DualPresentationOnly / Single
  NEW: Single
Video Selfview Default OnMonitorRole
  OLD: Current / First / Fourth / Second / Third
  Default value: Current
  NEW: First
  Default value: First
DX70 and DX80 at a glance

The Cisco DX70 and DX80 are all-in-one units designed to video-enable small collaboration spaces. They are high quality featuring high-definition (HD) video, unified communications features, a display for your laptop, and expanded capabilities.

Features and benefits

- A dedicated, always-on 1080p HD video communication system
- A high-quality audio system for speakerphone
- A 23-inch (DX80) or 14-inch (DX70) 16:9 screen that provides an engaging experience for video calls
- A multitouch capacitive touchscreen that provides an elegant and powerful user interface
- A self-provisioning device that is simple for users to take out of the box and start using quickly
- Ability for administrators to use Cisco Expressway for the secure connection of their remote workers
- Registers with Cisco Unified Communications Manager (UCM), Cisco TelePresence Video Communication Server (VCS), and Cisco Spark
Power On and Off

Power On/Off with the Power button
The power button, with LED indicator, is placed on the front as shown in the illustration.

![Power button with LED indicator](image)

**Switch on**
The video system does not start automatically. Press the power button gently, and hold for a few seconds.
The LED is lit while the video system starts up.

**Switch off**
Press the power button gently and hold until the light goes out.

**Enter/exit standby mode**
Press the power button briefly. It takes a few seconds before the unit enters standby.

Power Off or restart the system remotely
Sign in to the web interface and navigate to Maintenance > Restart.

**Restart the system**
Click Restart device... and confirm your choice.
It takes a few minutes before the system is ready for use.

**Power Off the system**
Click Shutdown device... and confirm your choice.

- You cannot power the system on again remotely.

**Restart and standby using the Touch interface**

**Restart the system**
1. Select the settings icon (cogwheel) on the home screen.
2. Select System Information > Restart.
3. Select Restart again to confirm your choice.

**Enter/exit standby mode**
1. Select the settings icon (cogwheel) on the home screen.
2. Select Standby.
LED indicators

**Status LED**

The status LED is a circle around the power button. The normal LED color is white. A red light indicates hardware failure.

*Normal operation (not standby):*
  - Steady light.

*In standby mode:*
  - The LED pulsates slowly.

*No network connection:*
  - The LED repeatedly flashes twice.

*During startup (boot):*
  - The LED flashes.

**Camera LED**

The camera LED is just above the camera lens.

*Incoming call:*
  - The LED flashes.

*In call:*
  - Steady light.
How to administer the video system  (page 1 of 4)

In general, we recommend you to use the web interface to administer and maintain the video system, as described in this administrator guide.

Alternatively, you can access the API of the video system by other methods:
- HTTP or HTTPS (also used by the web interface)
- SSH
- Telnet
- Serial interface (RS-232)

If you want more information about the different access methods, and how to use the API, refer to the API guide for the video system.

Tip
If the configuration or status is available in the API, the web interface setting or status translates into an API configuration or status as follows:

Set $X > Y > Z$ to Value (web)
is the same as
xConfiguration $X \ Y \ Z$: Value (API)

Check $X > Y > Z$ status (web)
is the same as
xStatus $X \ Y \ Z$ (API)

For example:

Set SystemUnit > Name to MySystem
is the same as
xConfiguration SystemUnit Name: MySystem

Check SystemUnit > Software > Version status
is the same as
xStatus SystemUnit Software Version

More settings and status are available in the web interface than in the API.

<table>
<thead>
<tr>
<th>Access method</th>
<th>Notes</th>
<th>How to enable/disable the methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP/HTTPS</td>
<td>• Used by the web interface of the video system</td>
<td>NetworkServices &gt; HTTP &gt; Mode</td>
</tr>
<tr>
<td></td>
<td>• Non-secure (HTTP) or secure (HTTPS) communication</td>
<td>Restart the video system for changes to take effect</td>
</tr>
<tr>
<td></td>
<td>• HTTP: Enabled by default</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• HTTPS: Enabled by default</td>
<td></td>
</tr>
<tr>
<td>Telnet</td>
<td>• Non-secure TCP/IP connection</td>
<td>NetworkServices &gt; Telnet &gt; Mode</td>
</tr>
<tr>
<td></td>
<td>• Disabled by default</td>
<td>You do not need to restart the video system. It may take some time for changes to take effect</td>
</tr>
<tr>
<td>SSH</td>
<td>• Secure TCP/IP connection</td>
<td>NetworkServices &gt; SSH &gt; Mode</td>
</tr>
<tr>
<td></td>
<td>• Enabled by default</td>
<td>You do not need to restart the video system. It may take some time for changes to take effect</td>
</tr>
<tr>
<td>Serial interface (RS-232)</td>
<td>• Connect to the video system with a cable. IP-address, DNS, or a network is not required</td>
<td>SerialPort &gt; Mode</td>
</tr>
<tr>
<td></td>
<td>• Enabled by default</td>
<td>Restart the video system for changes to take effect</td>
</tr>
<tr>
<td></td>
<td>• For security reasons, you are asked to sign in by default (SerialPort &gt; LoginRequired)</td>
<td></td>
</tr>
</tbody>
</table>

⚠️ If all access methods are disabled (set to Off), you can no longer configure the video system. You are not able to re-enable (set to On) any of the access methods, and you must factory reset the video system to recover.
The web interface of the video system

The web interface is the administration portal for the video system. You can connect from a computer and administer the system remotely. It provides full configuration access and offers tools and mechanisms for maintenance.

**Note:** The web interface requires that HTTP or HTTPS is enabled (refer to NetworkServices > HTTP > Mode setting).

We recommend that you use the latest release of one of the major web browsers.

---

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

**How to find the IP address**
1. Select the settings icon (cogwheel) on the home screen.
2. Select System Information.

**Sign in**
Enter user name and passphrase for the endpoint and click Sign In.

The system is delivered with a default user named admin with no passphrase. Leave the Passphrase field blank when signing in for the first time.

It is mandatory to set a password for the admin user.

**Sign out**
Hover the mouse over the user name and choose Signout from the drop-down list.
How to administer the video system (page 3 of 4)

How the web interface is organized

The web interface is organized in sub-pages. A user that is signed in, sees only the pages that he has access rights for.

Read more about user administration, user roles and access rights in the ► User administration chapter.
How to administer the video system (page 4 of 4)

Settings available on-screen

You have access to the following information and settings on-screen:
- System information
- Warnings and error messages
- Restart of the video system
- Basic settings for language, time zone, network and provisioning (service activation)
- Extended logging
- Factory reset

Access system information and settings

1. Select the settings icon (cogwheel) on the home screen.
2. Select System Information to find system information, potential issues, and a Restart button.
3. Then, select Settings for system adjustments and basic configurations.
   You may be prompted for a PIN code to open this menu.
   Consult the Set a PIN code for the on-screen Settings menu section for more details.

Consult the Getting Started Guide for your video system for more details.
Chapter 2

Configuration
User administration

You have to sign in to get access to the web and command line interfaces. You can assign different roles to users, to determine what they should have access to.

The default user account
The video system comes with a default administrator user account with full access rights. The user name is admin and no passphrase is initially set.

It is mandatory to set a passphrase for the admin user.

Read how to set the passphrase in the ►Change the system passphrase chapter.

Create a new user account
1. Sign in to the web interface, and navigate to Security > Users.
2. Click Add new user...
3. Fill in the Username, Passphrase and Repeat passphrase input fields.
   As a default, the user has to change the passphrase when he signs in for the first time.
   Fill in the Client Certificate DN (Distinguished Name) field only if you use client certificates for authentication.
4. Check the appropriate Roles check boxes.
   If you assign the ADMIN role to a user, enter your own passphrase in the Your passphrase input field for verification.
5. Set the Status to Active to activate the user.
6. Click Create User.
   Use the Back button to leave without making any changes.

Edit an existing user account
If you make changes to a user that holds the Admin role, you must always enter your own passphrase in the Your passphrase input field for verification.

Change the user privileges
1. Sign in to the web interface, and navigate to Security > Users.
2. Click the appropriate user in the list.
3. Choose user roles, set the status to Active or Inactive, and decide if the user has to change the passphrase on the next sign in.
   Fill in the Client Certificate DN (Distinguished Name) field only if you use certificate login on HTTPS.
4. Click Update User to save the changes.
   Use the Back button to leave without making any changes.

Change the passphrase
1. Sign in to the web interface, and navigate to Security > Users.
2. Click the appropriate user in the list.
3. Enter the new passphrase in the appropriate input fields.
4. Click Change Passphrase to save the change.
   Use the Back button to leave without making any changes.

Delete the user account
1. Sign in to the web interface, and navigate to Security > Users.
2. Click the appropriate user in the list.
3. Click Delete user... and confirm when prompted.

About user roles
A user account may hold one or a combination of user roles. A user account with full access rights, like the default admin user, should possess the ADMIN, USER and AUDIT roles.

These are the user roles:

ADMIN: A user with this role can create new users, change most settings, make calls, and search the contact lists. The user cannot upload audit certificates and change the security audit settings.

USER: A user with this role can make calls and search the contact lists. The user can modify a few settings, for example adjust the ringtone volume and set the time and date format.

ROOMCONTROL: A user with this role can create in-room controls. The user has access to the In-room control editor and corresponding developement tools.

AUDIT: A user with this role can change the security audit settings and upload audit certificates.
Change the system passphrase

You need to know the system passphrase in order to:

- Sign in to the web interface
- Sign in and use the command line interfaces

The default user account

The video system is delivered with a default user account with full access rights. The user name is admin, and initially, no passphrase is set.

It is mandatory to set a passphrase for the default admin user in order to restrict access to system configuration. It is also mandatory to set a passphrase for any other user with ADMIN rights.

A warning, saying that the system passphrase is not set, is shown on screen until a passphrase is set for the admin user.

Other user accounts

You can create many user accounts for the video system.

Read more about how to create and manage user accounts in the User administration chapter.

Change another user’s passphrase

If you have administrator access rights, you can change the password of any user.

1. Sign in to the web interface, and navigate to Security > Users.
2. Click the appropriate user in the list.
3. Enter the new passphrase in the Passphrase and Repeat passphrase input fields.
   If the user holds the Admin role, you must enter your own passphrase in the Your passphrase input field for verification.
4. Click Change Passphrase to save the change.
   Use the Back button to leave without making any changes.
Set a PIN code for the on-screen Settings menu

We recommend that you set a PIN code for the on-screen Settings menu, to prevent unauthorized users from changing the configuration of the video system.

Set a PIN code
1. Sign in to the web interface, and navigate to Security > Access PIN.
2. Enter a PIN code in the input field, and click Set PIN. The PIN can only contain numbers.

Clear the PIN code
1. Sign in to the web interface, and navigate to Security > Access PIN.
2. Click Clear PIN.
## System configuration

Sign in to the web interface, and navigate to **Setup > Configuration**.

### Find a system setting

#### Search for settings

Enter as many letters as needed in the search field. All settings that contain these letters are shown in the right pane. Settings that have these letters in their value space are also shown.

### Change a system setting

#### Check the value space

A setting's value space is specified either by text following the input field or in a drop-down list that opens when you click the arrow.

#### Change a value

1. Choose the preferred value from the drop-down list, or enter new text in the input field.
2. Click **Save** for the change to take effect.

Use the **Undo** or **Cancel** buttons if you do not want to make any changes.

### About system settings

All system settings can be changed from the web interface.

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

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

You can read more about user administration and user roles in the ► **User administration** chapter.

Categories with unsaved changes are marked with an edit symbol (✓).
Add a sign in banner

Sign in to the web interface, and navigate to Security > Sign In Banner.

1. Enter the message that you want to present to the user when he signs in.
2. Click Save to activate the banner.

About sign in banner

If a system administrator wants to provide initial information to all users, he can create a sign in banner. The message is shown when the user signs in to the web interface or the command line interface.
Manage the service certificates of the video system

You need the following files:

- Certificate (file format: .PEM)
- Private key, either as a separate file or included in the same file as the certificate (file format: .PEM format)
- Passphrase (required only if the private key is encrypted)

The certificate and the private key will be stored in the same file on the video system.

About the service certificates of the video system

Certificate validation may be required when using TLS (Transport Layer Security).

A server or client may require that the video system presents a valid certificate to them before communication can be set up.

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

Certificates are used for the following services: HTTPS server, SIP, IEEE 802.1X and audit logging.

You can store many certificates on the video system, but only one certificate can be enabled for each service at a time.

If authentication fails, the connection will not be established.
Manage the list of trusted certificate authorities (CAs)

Sign in to the web interface, navigate to Security > Certificate Authorities, and open the Custom CAs tab.

You need the following file:
- CA certificate list (file format: .PEM).

View or delete a certificate
Use the corresponding button to view or delete a certificate.

Upload a list of certificate authorities

1. Click Browse... and find the file containing a list of CA certificates on your computer (file format: .PEM).
2. Click Add certificate authority... to store the new CA certificates on the video system.

About trusted CAs
Certificate validation may be required when using TLS (Transport Layer Security).

The video system may be set up to require that a server or client presents its certificate to the video system before communication can be set up.

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

In order to verify the signature of the certificates, a list of trusted CAs must reside on the video system.

The list must include all CAs needed in order to verify certificates for both audit logging and other connections.

If authentication fails, the connection will not be established.
Set up secure audit logging

Sign in to the web interface, navigate to Setup > Configuration.

1. Open the Security category.
2. Find the Audit > Server settings, and enter the Address of the audit server. If you set PortAssignment to Manual, you must also enter a Port number for the audit server.
   
   Click Save for the changes to take effect.
3. Set Audit > Logging > Mode to ExternalSecure.
   Click Save for the change to take effect.

The certificate authority (CA) that verifies the certificate of the audit server must be in the video system's list of trusted certificate authorities. Otherwise, logs will not be sent to the external server.

Refer to the Manage the list of trusted certificate authorities (CAs) chapter how to update the list.

About secure audit logging

When audit logging is enabled, all sign in activity and configuration changes on the video system are recorded.

Use the Security > Audit > Logging > Mode setting to enable audit logging. Audit logging is disabled by default.

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

The signature of the audit server is verified using the same CA list as other servers/clients.

If the audit server authentication fails, no audit logs are sent to the external server.
Manage pre-installed certificates for CUCM via Expressway provisioning

Sign in to the web interface, navigate to Security > Certificate Authorities, and open the Preinstalled CAs tab.

About pre-installed certificates

The pre-installed certificates in this list are only used when the video system is provisioned by Cisco Unified Communications Manager (CUCM) via Expressway (Edge).

Only Cisco Expressway infrastructure certificates are checked against this list. If the validation of the Cisco Expressway infrastructure certificate fails, the video system will not be provisioned and registered.

Factory resetting the video system does not delete the list of pre-installed certificates.

View or disable certificates

Use the Details... and Disable buttons respectively, to view or disable certificates.

The certificates and certificate issuers in the illustration are examples. Your system has other certificates.

As an alternative to using the pre-installed certificates, you can append the certificates you need to the certificate list manually.

Refer to the Manage the list of trusted certificate authorities (CAs) chapter how to update the list of trusted certificates.
Delete CUCM trust lists

The information in this chapter is only relevant for video systems that are registered to a Cisco Unified Communications Manager (CUCM).

Sign in to the web interface, navigate to Security > CUCM Certificates.

Delete the CUCM trust lists

Click Delete CTL/ITL to remove the trust lists.

As a general rule, you should not delete old CTL (Certificate Trust List) and ITL (Initial Trust List) files. In these cases, you must still delete them:

• When you change the CUCM IP address.
• When you move the endpoint between CUCM clusters.
• When you need to re-generate or change the CUCM certificate.

Overview of trust list fingerprints and certificates

The trust lists’ fingerprints and an overview of the certificates in the lists are displayed on the web page.

This information may be useful for troubleshooting.

More information about trust lists

For more information about CUCM and trust lists, read the Deployment guide for TelePresence endpoints on CUCM that is available on the Cisco web site.
Change the persistency mode

Sign in to the web interface and navigate to Security > Non-persistent Mode.

Check the persistency status
The active radio buttons show the current persistency status of the video system.
Alternatively, you can navigate to Setup > Status > Security > Persistency to see the status.

Change the persistency settings
All persistency settings are set to Persistent by default. You only have to change the settings to make them Non-persistent.

1. Click the radio buttons to set the persistency for configurations, call history, internal logging, local phonebook (local directory and favorites) and IP connectivity (DHCP) information.
2. Click Save and reboot...
   The video system restarts automatically. After the restart, the behavior changes according to the new persistency settings.

Logs, configurations, and other data that was stored before you switched to Non-persistent mode, are NOT cleared or deleted.

Persistency mode
Configurations, call history, internal logs, local phonebook (local directory and favorites list), and IP connectivity information are stored by default. Because all persistency settings are set to Persistent, a system restart does not delete this information.

Generally, we recommend you NOT to change the persistency settings. Only change to Non-persistent mode if you have to prevent users from being able to see or traceback to any logged information from the previous session.

In Non-persistent mode, the following information is lost or cleared each time the system restarts:

- System configuration changes
- Information about placed and received calls (call history)
- Internal log files
- Changes to the local contacts or favorites list
- All IP related information (DHCP) from the last session

Information that was stored before changing to Non-persistent mode is not automatically cleared or deleted. You must factory reset the video system to delete such information.

There is more information about performing a factory reset in the Factory reset the video system chapter.
Set strong security mode

Sign in to the web interface, navigate to Security > Strong Security Mode.

Set strong security mode

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

1. If you want to use strong security mode, click Enable Strong Security Mode... and confirm your choice in the dialog box that appears. The video system restarts automatically.

2. Change the passphrase when you are prompted. The new passphrase must meet the strict criteria as described. How to change the system passphrase is described in the ► Change the system passphrase chapter.

Return to normal mode

Click Disable Strong Security Mode... in order to restore the video system to normal mode. Confirm your choice in the dialog box that appears. The video system restarts automatically.

About strong security mode

Use strong security mode only when compliance with DoD JITC regulations is required.

Strong security mode sets very strict passphrase requirements, and requires all users to change their passphrase on the next sign in.
Set up Intelligent Proximity for content sharing (page 1 of 5)

Cisco Proximity allows users to see, control, capture and share content directly on their own mobile devices (smartphone, tablet, or laptop), when the device is near a video system.

The mobile device can automatically pair with the video system when it comes within range of ultrasound transmitted by the video system.

The number of simultaneous Proximity connections depends on the type of video system. The client warns new users if the maximum number of connections has been reached.

<table>
<thead>
<tr>
<th>Video system</th>
<th>Maximum number of connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>SX80</td>
<td>10</td>
</tr>
<tr>
<td>SX20</td>
<td>7</td>
</tr>
<tr>
<td>SX10</td>
<td>7</td>
</tr>
<tr>
<td>MX700, MX800</td>
<td>10</td>
</tr>
<tr>
<td>MX200 G2, MX300 G2</td>
<td>7</td>
</tr>
<tr>
<td>DX70, DX80</td>
<td>3</td>
</tr>
</tbody>
</table>

Proximity services

Place calls and control the video system:
- Dial, mute, adjust volume, hang up
- Available on smartphones and tablets (iOS and Android)

View shared content on a mobile device:
- View shared content, review previous slides, save selected slides
- Available on smartphones and tablets (iOS and Android)
- For DX70 and DX80, this service is available only when in a call

Wireless share from a desktop client:
- Share content without connecting a presentation cable
- Available on laptops (OS X and Windows)
Set up Intelligent Proximity for content sharing (page 2 of 5)

Install a Cisco Proximity client

Where to find the clients
You can download the Cisco Proximity clients for smartphones and tablets (Android and iOS), and laptops (Windows and OS X) free of charge from http://proximity.cisco.com
Clients for smartphones and tablets are also available directly through Google Play (Android) and Apple App Store (iOS).

End-user license agreement

Supported operating systems
- iOS 7 and above
- Android 4.0 and above
- Mac OS X 10.9 and above
- Windows 7 and above
  The tile based interface introduced with Windows 8 is not supported.
Set up Intelligent Proximity for content sharing (page 3 of 5)

Ultrasound emission
Cisco video systems emit ultrasound as part of the Proximity feature.

Use the Proximity > Mode setting to switch the Proximity feature - and thereby also ultrasound emission - On and Off.

Most people are exposed to ultrasound more or less daily in many environments, including industry, commercial applications and home appliances.

Even if airborne ultrasound may cause subjective effects for some individuals, it is very unlikely that any effects will occur for levels below 75 dB.

**SX10N and MX Series:**
- The ultrasound sound pressure level is below 75 dB at a distance of 50 cm or more from the loudspeaker.

**DX70 and DX80:**
- The ultrasound sound pressure level is below 75 dB at a distance of 20 cm or more from the loudspeaker.

**SX10, SX20, SX80, or an MX Series:**
- We strongly recommend you to switch off ultrasound emission if you use a headset with these video systems (set Proximity > Mode to Off). Then you cannot use the Proximity feature.

Since these systems don't have dedicated headset outputs, we are not able to control the sound pressure level from the connected headsets.

Headsets
**DX70, DX80, and SX10N:**
You can always use a headset with these systems because:
- DX70 and DX80 have dedicated headset outputs, on which we never emit ultrasound.
- SX10N has a built-in loudspeaker for ultrasound, so ultrasound is never emitted on the HDMI and loudspeaker outputs.

**SX10, SX20, SX80, or an MX Series:**
- We strongly recommend you to switch off ultrasound emission if you use a headset with these video systems (set Proximity > Mode to Off). Then you cannot use the Proximity feature.

Since these systems don't have dedicated headset outputs, we are not able to control the sound pressure level from the connected headsets.
Enable Proximity services

1. Sign in to the web interface, and navigate to Setup > Configuration.

2. Go to Proximity > Mode, and switch Proximity On.
   The video system starts sending ultrasound pairing messages.

3. Enable the services you want to allow. Only Wireless share from a mobile device is enabled by default.
   In order to fully utilise the Proximity functionality, we recommend that you enable all services.

Place calls and control the video system:

• Go to Proximity > Services > CallControl and choose Enabled.

View shared content on a mobile device:

• Go to Proximity > Services > ContentShare > FromClients and choose Enabled.

Wireless share from a desktop client:

• Go to Proximity > Services > ContentShare > ToClients and choose Enabled.

Temporarily disable the Proximity services

In sessions or meetings where you want to prevent devices in the room from receiving content, you can use the video system's user interface to temporarily disable the Proximity services.

The video system will continue to transmit ultrasound pairing messages during such sessions. This ensures that clients will know about a nearby video system, and can give the user an explanation why he cannot connect.

1. Select the settings icon (cogwheel) on the home screen to open the dropdown panel.

2. Switch Proximity on or off with the toggle button.

The Proximity indicator

You will see a Proximity indicator on the display when Proximity is switched On, and at least one Proximity service is enabled.

The Proximity indicator has two states:

- Proximity services are available for use.

- Proximity services are temporarily disabled. Use the toggle button in the settings dropdown panel to make them available again.

About Proximity

The Proximity feature is switched Off by default, because the DX products are often deployed in open offices with several systems close to each other. In such environments, pairing could be unstable. In general, Proximity should be switched On only on one system per room.

When Proximity is switched On, the video system transmits ultrasound pairing messages.

The ultrasound pairing messages are received by nearby devices with Proximity clients, and triggers the authentication and authorization of the device.

Provided that you have verified that Proximity is suitable in your environment, Cisco recommends - for the best user experience - that Proximity always is switched On.

In order to get full access to Proximity, the Proximity services (Proximity > Services > ...) must be Enabled as well.
Set up Intelligent Proximity for content sharing (page 5 of 5)

About privacy
In the Cisco Privacy statement and the Cisco Proximity Supplement you find information about data collection in the clients and privacy concerns that needs to be considered when deploying this feature in the organization. Refer to:

You can use the video system’s user interface to temporarily disable the Proximity services. This is useful in sessions or meetings where you want to prevent mobile devices in the room from receiving content.

Also note that the mobile devices in the room only can receive and view content when the video system is in a call.

Basic troubleshooting

Cannot detect devices with Proximity clients
• Some Windows laptops are not able to record sound in the ultrasound frequency range (20kHz-22kHz). This can be due to frequency limitations with the sound card, sound driver or the internal microphone of the particular device. Refer to the Support forum for more information.

Audio artifacts
• If you can hear audio artifacts, like humming or clipping noise, decrease the maximum ultrasound volume (Peripherals > Pairing > Ultrasound > Volume > MaxLevel).

Cannot share content from a laptop
• For content sharing to work, the video system and the laptop must be on the same network. For this reason Proximity sharing might fail if your video system is connected to your company network via Expressway, and your laptop is connected via VPN (VPN client dependent).

Additional resources
Cisco Intelligent Proximity site:
► https://www.cisco.com/go/proximity
Support forum:
► https://www.cisco.com/go/proximity-support
Adjust the video quality to call rate ratio

Optimal definition profile
The optimal definition profile should reflect the lighting conditions in the video conferencing room and the quality of the camera (video input source). The better the lighting conditions and the better the quality of the camera, the higher the profile should be used. In good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate. Generally, the Medium profile is recommended. However, if the lighting conditions are very good, we recommend that you test the endpoint on the various Optimal Definition Profile settings before deciding on a profile. The High profile may be set in order to increase the resolution for a given call rate.

Video input quality settings
The Video Input Connector n Quality setting must be set to Motion for the optimal definition settings to take any effect. With the video input quality set to Sharpness, the endpoint will transmit the highest resolution possible, regardless of frame rate.

Sign in to the web interface and navigate to Setup > Configuration.

1. Go to Video > Input > Connector n > Quality and set the video quality parameter to Motion (skip this step for Connector 1 (internal camera)).

2. Go to Video > Input > Connector n > OptimalDefinition > Profile and choose the preferred optimal definition profile.
Packet loss resilience - ClearPath

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

ClearPath is a Cisco proprietary protocol. All endpoints running CE software support ClearPath.

If the involved endpoints and infrastructure elements support ClearPath, all packet loss resilience mechanisms are used in point-to-point connections (including hosted conferences).
Choose wallpaper

Sign in to the web interface, and navigate to Setup > Personalization.

Choose wallpaper

Choose a wallpaper from the list.
The active wallpaper is highlighted.

Upload a custom wallpaper

Overwrites any old custom wallpaper.

1. Click Browse... and locate the custom wallpaper image file.
2. Click Upload to save the file on the video system.

Supported file formats: BMP, GIF, JPEG, PNG
Maximum file size: 4 MByte

The custom wallpaper is automatically activated once uploaded.

About a custom wallpaper

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

You can only store one custom wallpaper on the video system at a time; a new custom wallpaper overwrites the old one.

When you use a custom wallpaper, these items are removed from the main display:
• The large clock
• The list of upcoming meetings

Delete the custom wallpaper

Delete fully removes the custom wallpaper from the video system.

You have to upload it anew if you want to use it again.
Choose a ringtone and set the ringtone volume

Sign in to the web interface, and navigate to Setup > Personalization.

Change the ringtone
1. Choose a ringtone from the drop-down list.
2. Click Save to make it the active ringtone.

Set the ringtone volume
Use the slide bar to adjust the ringtone volume.

About ringtones
A set of ringtones are installed on the video system. Use the web interface to choose a ringtone, and set the ringtone volume.

You can play back the chosen ringtone from the web interface. Note that the ringtone will be played back on the video system itself, and not on the computer running the web interface.

Play back the ringtone
Click the play button (►) to play back the ringtone.
Use the stop button (■) to end the playback.
Manage local contacts

Sign in to the web interface and navigate to Setup > Local Contacts.

Import/Export contacts from file

Click Export to save the local contacts in a file; and click Import to bring in contacts from a file.

The current local contacts are discarded when you import new contacts from a file.

Add or edit a contact

1. Click Add contact to make a new local contact, or click a contact’s name followed by Edit contact.
2. Fill in or update the form that pops up.
   Choose a folder in the folder drop down list in order to store the contact in a sub-folder.
   Click Add contact method and fill in the new input fields if you want to store more than one contact method for the contact (for example video address, telephone and mobile number).
3. Click Save to store the local contact.

Delete a contact

1. Click a contacts name followed by Edit contact.
2. Click Delete to remove the local contact.

Where to find the local contacts

On-screen: Select Call > Directory > Local contacts. The local contacts are listed alphabetically without regard to the folder hierarchy.

Web interface: Click Call Control, and open the Local tab in the Contacts section.

Favorites list

The Favorites list is only available on-screen. It is not available on the web interface.

Select Call > Favorites to find the list. You can add both Local contacts and other Directory entries to the Favorites list.

Also, a directory entry that is marked as a favorite is automatically copied to the Local contacts folder.

Add a contact to the Favorites list

On-screen: Navigate to the contact, and then •••. Click Mark as Favorite.

Web interface: Navigate to Setup > Local Contacts. Click the star next to the contact.

Add a sub-folder

1. Click Add folder to make a new sub-folder, or click one of the listed sub-folders followed by Edit folder to change an existing sub-folder.
2. Fill in or update the form that pops up.
3. Click Save to create or update the folder.

Delete a sub-folder

1. Click Edit folder.
2. Click Delete to remove the folder and all its contacts and sub-folders. Confirm your choice in the dialog that pops up.
Chapter 3

Peripherals
Connect a computer

Connect a computer to the HDMI input port in order to use the video system as screen for the computer, and to share content with conference participants.

Flip the connector cover up to uncover the connector panel.

DX70

DX80

HDMI input for computer
(Input Connector 2)
Extend the number of input sources

You can customize our touch user interfaces to include input sources that are connected to a third-party external video switch. The sources will appear and behave as any other video source that is connected directly to the video system.

Consult the In-Room Control guide for full details about how to extend the user interface, and how to use the video system’s API to set it up. Go to:

► http://www.cisco.com/go/in-room-control-docs

Architecture

You need a Cisco video system with a touch interface, a third-party control system, for example Crestron or AMX, and a third-party video switch. It is the control system, not the video system, that controls the video switch.

When you program the control system you must use the video system’s API (events and commands)* in order to connect with the video switch and the controls on the touch interface. This way you can synchronize what is shown and done on the user interface with the actual state of the input sources.

* You need a user that holds the ROOMCONTROL or ADMIN user roles in order to access the API commands that you need when programming the control system.
Chapter 4

Maintenance
Upgrade the system software  (page 1 of 2)

Convert between Android-based software and CE software

From Collaboration Software version 8.2 (CE8.2) all DX80 and DX70 units can run CE software, which is the same software that runs on the Cisco TelePresence SX and MX Series.

Cisco DX80 and Cisco DX70 were originally shipped with Android based software, but will later on be shipped with CE software.

Before converting to CE software, it is important to carefully consider the conversion requirements and the functionality changes compared to Android based software.

The CE software on DX devices does not support the following features in CE8.3:

- Bluetooth headset
- 3rd party app installation
- Keyboard control, keyboard and mouse redirect

Refer to the Software Release Notes for further information.

Find a detailed description about how to convert from Android-based software and CE software, and vice versa, in the Cisco DX70 and DX80 Convert between CE and Android based software guide available under Install and Upgrade Guides at http://www.cisco.com/go/dx-docs
Upgrade the system software (page 2 of 2)

Note: You can only upgrade to another CE software version using this procedure, for example from CE8.2.x to CE8.2.y.
If you want to convert between Android-based software, and CE software, refer to the previous page.

Sign in to the web interface and navigate to Maintenance > Software Upgrade.

Download new software
For software download, go to the Cisco Download Software web page:
Then navigate to your product.
The format of the file name is “sS2040ce8_3_x.pkg”. Each software version has a unique file name.

Install new software
Download the appropriate software package and store it on your computer. This is a .pkg file.
1. Click Browse... and find the .pkg file that contains the new software.
The software version will be detected and shown.
2. Click Install software to start the installation process.
The complete installation normally take no longer than 15 minutes. You can follow the progress on the web page. The video system restarts automatically after the installation.
You must sign in anew in order to continue working with the web interface after the restart.

About software versions
This video conference system is using CE software. The version described in this document is CE8.3.x.
Add option keys

Sign in to the web interface and navigate to Maintenance > Option Keys.

You see a list of all option keys, also the ones that are not installed on your video system.

Contact your Cisco representative for information about how to get option keys for the uninstalled options.

About option keys

Your video system may or may not have one or more software options installed. In order to activate the optional functionality the corresponding option key must be present on the video system.

Each video system has unique option keys.

Option keys are not deleted when performing a software upgrade or factory reset, so they need to be added only once.

Add option key

1. Enter an Option Key in the text input field.
2. Click Add option key.

If you want to add more than one option key, repeat these steps for all keys.

The video system’s serial number

You need the video system’s serial number when ordering an option key.

Contact your Cisco representative to obtain option keys.

You need to provide the serial number to get option keys.
System status

System information overview
Sign in to the web interface to see the System Information page.
This page shows the product type, system name and basic information about the hardware, software, installed options and network address. Registration status for the video networks (SIP and H.323) is included, as well as the number/URI to use when making a call to the system.

Detailed system status
Sign in to the web interface, and navigate to Setup > Status in order to find more detailed status information.

Search for a status entry
Enter as many letters as needed in the search field. All entries that contain these letters are shown in the right pane. Entries that have these letters in their value space are also shown.

Select a category and navigate to the correct status
The system status is grouped in categories. Choose a category in the left pane to show the related status to the right.

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

Sign in to the web interface and navigate to *Maintenance > Diagnostics*.

The diagnostics page lists the status for some common sources of errors*. Errors and critical issues are clearly marked in red color; warnings are yellow.

---

* The messages shown in the illustration serve as examples. Your system may show other information.
Download log files

Sign in to the web interface and navigate to Maintenance > System Logs.

Download all log files

Click Download logs archive... and follow the instructions.

An anonymized call history is included in the log files by default.

Use the drop down list if you want to exclude the call history from the log files, or if you want to include the full call history (non-anonymous caller/callee).

Open/save one log file

Click the file name to open the log file in the web browser; right click to save the file on the computer.

Start extended logging

Click Start extended logging...

Extended logging lasts for 3 or 10 minutes, depending on whether full capture of network traffic is included or not.

Click Stop extended logging if you want to stop the extended logging before it times out.

As default, the network traffic is not captured. Use the drop down menu if you want to include partial or full capture of network traffic.

Refresh a log file list

Click the refresh button for Current logs or Historical logs to update the corresponding lists.

About log files

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

The current log files are time stamped event log files.

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

Extended logging mode

Extended logging mode may be switched on to help diagnose network issues and problems during call setup. While in this mode more information is stored in the log files.

Extended logging uses more of the video system’s resources, and may cause the video system to under-perform. Only use extended logging mode when you are troubleshooting an issue.
Create a remote support user

Sign in to the web interface, navigate to **Maintenance > System Recovery** and select the **Remote Support User** tab.

⚠️ The remote support user should only be enabled for troubleshooting reasons when instructed by Cisco TAC.

Create remote support user

1. Click **Create user**.
2. Open a case with Cisco TAC.
3. Copy the text in the **Token** field and send it to Cisco TAC.
4. Cisco TAC will generate a **password**.

The remote support user is valid for seven days, or until it is deleted.

Delete remote support user

Click **Delete user**.

About the remote support user

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

The remote support user is granted read access to the system and has access to a limited set of commands that can aid troubleshooting.

You will need assistance from Cisco Technical Assistance Center (TAC) to acquire the password for the remote support user.
Backup or restore a configuration

Sign in to the web interface and navigate to Maintenance > Backup and Restore.

Show the current configuration
Click Preview backup to display the current settings on-screen.

Back up the current configuration
Click Take backup to store the configuration as a text file.

Restore configuration from backup
1. Click Browse... and find the backup file with the configuration you want to restore.
2. Click Restore to reconfigure the system as defined in the file. Some settings require that you restart the video system before they take effect.

About configuration backup
All the system settings, which are available on the System configuration page, can be listed on-screen or stored as a backup text file.

The backup text file can be loaded back onto the system, thereby restoring the configuration.
Revert to the previously used software image

Sign in to the web interface and navigate to Maintenance > System Recovery.

Note: You can only revert to another CE software version using this procedure, for example from CE8.3.y to CE8.2.x.

If you want to convert back to Android-based software, refer to the Upgrade the system software chapter.

We recommend you to back up the log files and configuration of the video system before you swap to the previously used software image.

Back up log files and system configuration
1. Select the Backup tab.
2. Click Download Logs and follow the instructions to save the log files on your computer.
3. Click Download Configuration Backup and follow the instructions to save the configuration file on your computer.

Revert to the previously used software image
Only administrators, or when in contact with Cisco technical support, should perform this procedure.
1. Select the Software Recovery Swap tab.
2. Click Switch to software: cex.y.z..., where x.y.z indicates the software version.
3. Click Yes to confirm your choice, or Cancel if you have changed your mind.

Wait while the system resets. The system restarts automatically when finished. This procedure may take a few minutes.

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

If the system has not been factory reset since the last software upgrade, the previously used software image still resides on the system. You do not have to download the software again.
If there is a severe problem with the video system, the last resort may be to reset it to its default factory settings. It is not possible to undo a factory reset.

Always consider reverting to the previously used software image before performing a factory reset. In many situations this will recover the system. Read about software swapping in the Revert to the previously used software image chapter.

We recommend that you use the web interface to factory reset the video system. If the web interface is not available, use the reset button for DX80 and the mute and volume buttons for DX70.

A factory reset implies:
- Call logs are deleted.
- Passphrases are reset to default.
- All system parameters are reset to default values.
- All files that have been uploaded to the system are deleted. This includes, but is not limited to, custom wallpaper, certificates, local contacts and favorites lists.
- The previous (inactive) software image is deleted.
- Option keys are not affected.

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

Back up log files and system configuration

Sign in to the web interface and navigate to Maintenance > System Recovery.

1. Select the Backup tab.
2. Click Download Logs and follow the instructions to save the log files on your computer.
3. Click Download Configuration Backup and follow the instructions to save the configuration file on your computer.

We recommend that you back up the log files and configuration of the video system before you perform a factory reset; otherwise these data will be lost.
Factory reset the video system (page 2 of 3)

We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.

Factory reset DX80 using the mute and volume buttons

Follow these steps to factory reset a DX80 on boot up. If the video system is on, press and hold the power button until the system shuts down before you continue.

1. Locate the Mute and Volume up buttons.
2. Press and hold the Volume Up button and power on the device.
3. Release the Volume Up button when the Mute button is lit red, then press the Mute button.

Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

When the system has been successfully reset to factory settings, the Setup assistant starts and you will see the Welcome screen. Refer to the DX80 Getting Started guide for details.

Factory reset DX80 using the reset button

To use this method, the DX80 must be up and running.

1. Flip the connector cover up to uncover the connector panel at the rear of the video system.
2. Use the tip of a pen (or similar) to press the recessed reset button. Hold the button for 1-2 seconds, until a notification Resetting to factory settings shows on screen.
3. Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

When the system has been successfully reset to factory settings, the Setup assistant starts and you will see the Welcome screen. Refer to the DX80 Getting Started guide for details.
We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.

Factory reset DX70 using the mute and volume buttons

Follow these steps to factory reset a DX70 on boot up. If the video system is on, press and hold the power button until the system shuts down before you continue.

1. Locate the Mute and Volume up buttons (LEDs).
2. Press the power button, and pay attention to the Mute button.
3. When the Mute button has blinked twice, press the Volume up button, immediately followed by pressing and holding the Mute button for approximately 4 seconds. During this process the Mute button turns red for a few seconds.

Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

When the system has been successfully reset to factory settings, the Setup assistant starts with the Welcome screen. Refer to the DX70 Getting Started guide for details.
Capture user interface screenshots

Sign in to the web interface and navigate to Maintenance > User Interface Screenshots.

Capture a screenshot

Click Take screenshot of OSD to capture a screenshot of the on-screen display.

The screenshot displays in the area below the buttons. It may take up to 30 seconds before the screenshot is ready.

All captured snapshots are included in the list above the buttons. Click the screenshot ID to display the image.

Delete screenshots

If you want to delete all screenshots, click Remove all.

To delete just one screenshot, click the × button for that screenshot.

About user interface screenshots

You can capture screenshots of the on-screen display (menus, indicators and messages on the main display).
Chapter 5

System settings
Overview of the system settings

In the following pages you will find a complete list of the system settings which are configured from the Setup > Configuration page on the web interface.

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

How to find the IP address

1. Select the settings icon (cogwheel) on the home screen.
2. Select System Information.
## H323 Call Setup Mode
- H323 Authentication Password .......................... 70
- H323 Call Setup Mode ........................................... 70
- H323 Encryption KeySize ........................................ 71
- H323 Gatekeeper Address ........................................ 71
- H323 H323Alias E164 ......................................... 71
- H323 H323Alias ID ............................................. 71
- H323 NAT Address ........................................... 72
- H323 NAT Mode ............................................. 71
- H323 Port Allocation .......................................... 72

## Logging settings
- Logging External Protocol ...................................... 73
- Logging External Server Address ......................... 73
- Logging External Server Port ................................ 73
- Logging Mode ................................................... 73

## Network settings
- Network [1] IPv6 Address ....................................... 74
- Network [1] IPv4 Assignment .................................. 74
- Network [1] IPv4 Address ....................................... 74
- Network [1] IPv4 Gateway ...................................... 74
- Network [1] IPv4 SubnetMask .................................. 74
- Network [1] IPv6 Address ....................................... 77
- Network [1] IPv6 Assignment .................................. 77
- Network [1] IPv6 Gateway ...................................... 77
- Network [1] IPv6 Options ...................................... 77
- Network [1] MTU ............................................... 77
- Network [1] QoS Diffserv Audio ............................ 78
- Network [1] QoS Diffserv Data .............................. 78
- Network [1] QoS Diffserv ICMPv6 ......................... 79
- Network [1] QoS Diffserv NTP ................................ 79
- Network [1] QoS Diffserv signalling ....................... 78
- Network [1] QoS Diffserv Video ............................ 78
- Network [1] QoS Mode ......................................... 77
- Network [1] Speed ............................................ 79
- Network [1] Traffic Control Mode ......................... 80
- Network [1] VLAN Voice Mode ............................. 80
- Network [1] VLAN Voice VlanId ............................ 80

## NetworkServices settings
- NetworkServices CDP Mode ................................... 81
- NetworkServices DNS Domain Name .................. 81
- NetworkServices DNS Server [1..3] Address .......... 81
- NetworkServices EIES8021X AnonymouseIdenty .... 85
- NetworkServices EIES8021X Eap Md5 .................. 75
- NetworkServices EIES8021X Eap Peap ................. 75
- NetworkServices EIES8021X Eap Tls .................... 75
- NetworkServices EIES8021X Eap Tlts ................. 75
- NetworkServices EIES8021X Identity ................. 75
- NetworkServices EIES8021X Mode ..................... 74
- NetworkServices EIES8021X Password ............... 75
- NetworkServices EIES8021X TlsVerify ............... 74
- NetworkServices EIES8021X UseClientCertificate ... 74
- NetworkServices IPStack ...................................... 76
- NetworkServices NTP Server [1..3] Address .......... 82
- NetworkServices NTP Mode ................................... 82
- NetworkServices NTP Server [1..3] Address .......... 82
- NetworkServices SIP Mode .................................... 82
- NetworkServices SNMP CommunityName ............. 83
- NetworkServices SNMP Host [1..3] Address .......... 83
- NetworkServices SNMP Mode ................................ 83
- NetworkServices SNMP SystemContact ............... 83
- NetworkServices SNMP SystemLocation .............. 83
- NetworkServices SSH AllowPublicKey ................. 84
- NetworkServices SSH Mode .................................. 84
- NetworkServices Telnet Mode ....................... 84
- NetworkServices Welcome Text ......................... 84
- NetworkServices WIFI Allowed ......................... 84
- NetworkServices WIFI Enabled ......................... 85
- NetworkServices XMILAPI Mode ......................... 85

## Peripherals settings
- Peripherals Pairing Ultrasound Volume MaxLevel ... 86
- Peripherals Pairing Ultrasound Volume Mode ....... 86
- Peripherals Profile ControlSystems .................... 86
<table>
<thead>
<tr>
<th>Settings</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security settings</td>
<td>94</td>
</tr>
<tr>
<td>Provisioning settings</td>
<td>88</td>
</tr>
<tr>
<td>Phonebook settings</td>
<td>87</td>
</tr>
<tr>
<td>SerialPort settings</td>
<td>96</td>
</tr>
<tr>
<td>SIP settings</td>
<td>97</td>
</tr>
<tr>
<td>Time settings</td>
<td>103</td>
</tr>
<tr>
<td>Standby settings</td>
<td>101</td>
</tr>
<tr>
<td>SystemUnit settings</td>
<td>102</td>
</tr>
<tr>
<td>RTP settings</td>
<td>93</td>
</tr>
</tbody>
</table>

**Security settings**
- Security Audit Logging Mode
- Security Audit OnError Action
- Security Audit Server Address
- Security Audit Server Port
- Security Audit Server PortAssignment
- Security Session InactivityTimeout
- Security Session MaxSessionsPerUser
- Security Session MaxTotalSessions
- Security Session ShowLastLogon

**Provisioning settings**
- Provisioning Connectivity
- Provisioning ExternalManager Address
- Provisioning ExternalManager AlternateAddress
- Provisioning ExternalManager Domain
- Provisioning ExternalManager Path
- Provisioning ExternalManager Protocol
- Provisioning HttpMethod
- Provisioning LoginName
- Provisioning Mode
- Provisioning Password

**Phonebook settings**
- Phonebook Server [1] ID
- Phonebook Server [1] Type
- Phonebook Server [1] URL

**SerialPort settings**
- SerialPort LoginRequired
- SerialPort Mode

**SIP settings**
- SIP ANAT
- SIP Authentication Password
- SIP Authentication UserName
- SIP DefaultTransport
- SIP DisplayName
- SIP Ice DefaultCandidate
- SIP Ice Mode
- SIP Line
- SIP ListenPort
- SIP Mailbox
- SIP PreferredIPMedia
- SIP PreferredIPSignaling
- SIP Proxy [1..4] Address
- SIP TlsVerify
- SIP Turn DiscoverMode
- SIP Turn DropRfH
- SIP Turn Password
- SIP Turn Server
- SIP Turn UserName
- SIP Type
- SIP URI

**Time settings**
- Time DateFormat
- Time TimeFormat
- Time Zone
UserInterface settings ................................................................. 106
  UserInterface ContactInfo Type ............................................. 106
  UserInterface KeyTones Mode ............................................... 106
  UserInterface Language ......................................................... 106
  UserInterface OSD EncryptionIndicator ................................. 106
  UserInterface OSD Output ..................................................... 107
  UserInterface UserPreferences ............................................. 107
  UserInterface Wallpaper ..................................................... 107

UserManagement settings ...................................................... 108
  UserManagement LDAP Admin Filter ..................................... 109
  UserManagement LDAP Admin Group .................................... 109
  UserManagement LDAP Attribute .......................................... 109
  UserManagement LDAP Encryption ....................................... 108
  UserManagement LDAP MinimumTLSVersion .......................... 108
  UserManagement LDAP Mode ............................................... 108
  UserManagement LDAP Server Address ................................ 108
  UserManagement LDAP Server Port ...................................... 108
  UserManagement LDAP VerifyServerCertificate ..................... 109

Video settings ........................................................................ 110
  Video ActiveSpeaker DefaultPIPPosition ............................... 110
  Video DefaultLayoutFamily Local .......................................... 110
  Video DefaultLayoutFamily Remote ....................................... 111
  Video DefaultMainSource ................................................... 111
  Video Input Connector [1..2] CameraControl CameraId .......... 111
  Video Input Connector [1..2] CameraControl Mode ................. 111
  Video Input Connector [1..2] InputSourceType ....................... 111
  Video Input Connector [1..2] Name ....................................... 112
  Video Input Connector [1..2] OptimalDefinition Profile .......... 112
  Video Input Connector [1..2] Visibility .................................. 113
  Video Input Connector [2] PresentationSelection ................... 113
  Video Input Connector [2] Quality ........................................ 112
  Video Input Connector [2] RGBQuantizationRange .................. 113
  Video Layout DisableDisconnectedLocalOutputs ................... 114
  Video Monitors .................................................................. 114
  Video Output Connector [1..2] Resolution ............................. 114
  Video Output Connector [1] Brightness ................................ 114
  Video Output Connector [1] Whitebalance Level .................... 114
  Video Output Connector [2] CEC Mode ................................ 114
  Video Output Connector [2] Location HorizontalOffset .......... 114

Video Output Connector [2] Location VerticalOffset ................ 114
Video Output Connector [2] OverscanLevel .............................. 114
Video Output Connector [2] RGBQuantizationRange .................. 114
Video Presentation DefaultPIPPosition ................................... 115
Video Presentation DefaultSource .......................................... 115
Video Selfview Default FullscreenMode .................................. 115
Video Selfview Default Mode ................................................. 115
Video Selfview Default OnMonitorRole ................................... 115
Video Selfview Default PIPPosition ......................................... 116
Video Selfview OnCall Duration ............................................. 116
Video Selfview OnCall Mode .................................................. 116

Experimental settings .................................................................. 117
Audio settings

Audio DefaultVolume

Define the default volume for the speakers. The volume is set to this value when you switch on or restart the video system. Use the controls on the video system to change the volume while it is running. You may also use API commands (xCommand Audio Volume) to change the volume while the video system is running, and to reset to default value.

Requires user role: ADMIN, USER
Default value: 50

Value space: Integer (0..100)

Select a value between 1 and 100. This corresponds to the dB range from -34.5 dB to 15 dB, in steps of 0.5 dB). If set to 0 the audio is switched off.

Audio Microphones Mute Enabled

Define the microphone mute behaviour on the video system.

Requires user role: ADMIN
Default value: True

Value space: True/InCallOnly

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

Audio SoundsAndAlerts RingTone

Define which ringtone to use for incoming calls.

Requires user role: ADMIN, USER
Default value: Sunrise

Value space: Sunrise/Mischief/Ripples/Reflections/Vibes/Delight/Evolve/Playful/Ascent/Calculation/Mellow/Ringer

Select a ringtone from the list.

Audio SoundsAndAlerts RingVolume

Define the ring volume for incoming calls.

Requires user role: ADMIN, USER
Default value: 50

Value space: Integer (0..100)

The value goes in steps of 5 from 0 to 100 (from -34.5 dB to 15 dB). Volume 0 = Off.
Audio Input Microphone Mode

This setting only applies to DX80.

The DX80 has microphones in both legs. If you set the microphone mode to Focused, the microphones can be combined to focus sound sensitivity. As a result, the noise in the room is suppressed, and you can be heard better when sitting right in front of the video system. The voice of people not sitting right in front of the system will be suppressed.

If you set the microphone mode to Wide, the system behaves like any other system. The voice of people sitting beside you will be heard, and also more noise from the room.

We recommend that you use Focused mode when you are the only speaker. Use Wide mode when several speakers are in front of the system.

Requires user role: ADMIN
Default value: Wide

Value space: Focused/Wide
- Focused: Focused sound sensitivity, suppressing sound from sources that are not right in front of the video system.
- Wide: Default microphone operation with normal sound sensitivity.
CallHistory settings

CallHistory Mode

Determine whether or not information about calls that are placed or received are stored, including missed calls and calls that are not answered (call history). This determines whether or not the calls appear in the Recents list in the user interfaces.

Requires user role: ADMIN
Default value: On
Value space: Off/On

- Off: New entries are not added to the call history.
- On: New entries are stored in the call history list.
Conference settings

Conference ActiveControl Mode
Active control is a feature that allows conference participants to administer a conference on Cisco TelePresence Server or Cisco Meeting Server using the video system’s interfaces. Each user can see the participant list, change video layout, disconnect participants, etc. from the interface. The active control feature is enabled by default, provided that it is supported by the infrastructure (Cisco Unified Communications Manager (CUCM) version 9.1.2 or newer, Cisco TelePresence Video Communication Server (VCS) version X8.1 or newer, Cisco Media Server (CMS) version 2.1 or newer). Change this setting if you want to disable the active control features.

Requires user role: ADMIN
Default value: Auto
Value space: Auto/Off
- Auto: Active control is enabled when supported by the infrastructure.
- Off: Active control is disabled.

Conference AutoAnswer Mode
Define the auto answer mode. Use the Conference AutoAnswer Delay setting if you want the system to wait a number of seconds before answering the call, and use the Conference AutoAnswer Mute setting if you want your microphone to be muted when the call is answered.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
- Off: You must answer incoming calls manually by tapping Answer.
- On: The system automatically answers incoming calls, except if you are already in a call. You must always answer or decline incoming calls manually when you are already engaged in a call.

Conference AutoAnswer Mute
Define if the microphone shall be muted when an incoming call is automatically answered.

Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
- Off: The incoming call will not be muted.
- On: The incoming call will be muted when automatically answered.

Conference AutoAnswer Delay
Define how long (in seconds) an incoming call has to wait before it is answered automatically by the system. Requires that AutoAnswer Mode is switched on.

Requires user role: ADMIN
Default value: 0
Value space: Integer (0..50)
- The auto answer delay (seconds).

Conference CallProtocolIPStack
Select if the system should enable IPv4, IPv6, or dual IP stack on the call protocol (SIP).

Requires user role: ADMIN
Default value: Dual
Value space: Dual/IPv4/IPv6
- Dual: Enables both IPv4 and IPv6 for the call protocol.
- IPv4: When set to IPv4, the call protocol will use IPv4.
- IPv6: When set to IPv6, the call protocol will use IPv6.
Conference Default Call Rate
Define the Default Call Rate to be used when placing calls from the system.

Requires user role: ADMIN
Default value: 3072

Value space: Integer (64..3072)

The default call rate (kbps).

Conference Do Not Disturb Default Timeout
This setting determines the default duration of a Do Not Disturb session, i.e. the period when incoming calls are rejected and registered as missed calls. The session can be terminated earlier by using the user interface. The default value is 60 minutes.

Requires user role: ADMIN
Default value: 60

Value space: Integer (1..1440)

The number of minutes (maximum 1440 minutes = 24 hours) before the Do Not Disturb session times out automatically.

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

NOTE: If the Encryption Option Key is not installed on the video system, the encryption mode is always Off.

Requires user role: ADMIN
Default value: BestEffort

Value space: Off/On/BestEffort

Off: The system will not use encryption.
On: The system will only allow calls that are encrypted.
BestEffort: The system will use encryption whenever possible.

> In Point to point calls: If the far end system supports encryption (AES-128), the call will be encrypted. If not, the call will proceed without encryption.
> In MultiSite calls: In order to have encrypted MultiSite conferences, all sites must support encryption. If not, the conference will be unencrypted.

Conference Far End Control 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
Default value: On

Value space: Off/On

Off: The far end is not allowed to select your video sources or to control your local camera (pan, tilt, zoom).
On: Allows the far end to be able to select your video sources and control your local camera (pan, tilt, zoom). You will still be able to control your camera and select your video sources as normal.

Conference Far End Control Signal Capability
Define the far end control (H.224) signal capability mode.

Requires user role: ADMIN
Default value: On

Value space: Off/On

Off: Disable the far end control signal capability.
On: Enable the far end control signal capability.

Conference Max Receive Call Rate
Define the maximum receive bit rate to be used when placing or receiving calls.

Note that this is the maximum bit rate for each individual call; use the Conference Max Total Receive Call Rate setting to set the aggregated maximum for all simultaneous active calls.

Requires user role: ADMIN
Default value: 3072

Value space: Integer (64..3072)

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

Requires user role: ADMIN
Default value: 3072
Value space: Integer (64..3072)
   The maximum transmit call rate (kbps).

Conference MaxTotalReceiveCallRate
Define the maximum overall receive bit rate allowed. This product does not support multiple simultaneous calls, so the total receive call rate will be the same as the receive bit rate for one call (ref. Conference MaxReceiveCallRate setting).

Requires user role: ADMIN
Default value: 3072
Value space: Integer (64..3072)
   The maximum receive call rate (kbps).

Conference MaxTotalTransmitCallRate
Define the maximum overall transmit bit rate allowed. This product does not support multiple simultaneous calls, so the total transmit call rate will be the same as the transmit bit rate for one call (ref. Conference MaxTransmitCallRate setting).

Requires user role: ADMIN
Default value: 3072
Value space: Integer (64..3072)
   The maximum transmit call rate (kbps).

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

Requires user role: ADMIN
Default value: On
Value space: Off/On
   Off: If muted during a call, let the microphones remain muted after the call is disconnected.
   On: Unmute the microphones after the call is disconnected.

Conference Presentation OnPlacedOnHold
Define whether or not to continue sharing a presentation after the remote site has put you on hold.

Requires user role: ADMIN
Default value: NoAction
Value space: Stop/NoAction
   Stop: The video system stops the presentation sharing when the remote site puts you on hold. The presentation will not continue when the call is resumed.
   NoAction: The video system will not stop the presentation sharing when put on hold. The presentation will not be shared while you are on hold, but it will continue automatically when the call is resumed.

Conference VideoBandwidth Mode
Define the conference video bandwidth mode.

Requires user role: ADMIN
Default value: Dynamic
Value space: Dynamic/Static
   Dynamic: The available transmit bandwidth for the video channels are distributed among the currently active channels. If there is no presentation, the main video channels will use the bandwidth of the presentation channel.
   Static: The available transmit bandwidth is assigned to each video channel, even if it is not active.
Conference Video Bandwidth Presentation Channel Weight

The available transmit video bandwidth is distributed on the main channel and presentation channel according to "Main Channel Weight" and "Presentation Channel 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
Default value: 5
Value space: Integer (1..9)
Set the bandwidth weight for the presentation channel.
FacilityService settings

FacilityService Service [1..5] Type
Not applicable in this software version.

FacilityService Service [1..5] Name
Not applicable in this software version.

FacilityService Service [1..5] Number
Not applicable in this software version.

FacilityService Service [1..5] CallType
Not applicable in this software version.
H323 settings

H323 Authentication Mode
Define the authentication mode for the H.323 profile.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: The system will not try to authenticate itself to a H.323 Gatekeeper, but will still try a normal registration.
  On: If an H.323 Gatekeeper indicates that it requires authentication, the system will try to authenticate itself to the gatekeeper. Requires the H323 Authentication LoginName and H323 Authentication Password settings to be defined on both the codec and the Gatekeeper.

H323 Authentication LoginName
The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN
Default value: **
Value space: String (0, 50)
  The authentication login name.

H323 Authentication Password
The system sends the H323 Authentication Login Name and the H323 Authentication Password to an H.323 Gatekeeper for authentication. The authentication is a one way authentication from the codec to the H.323 Gatekeeper, i.e. the system is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the system will still try to register. Requires the H.323 Authentication Mode to be enabled.

Requires user role: ADMIN
Default value: **
Value space: String (0, 50)
  The authentication password.

H323 CallSetup Mode
Defines whether to use a Gatekeeper or Direct calling when establishing H.323 calls. Direct H.323 calls can be made also when H323 CallSetup Mode is set to Gatekeeper.

Requires user role: ADMIN
Default value: Gatekeeper
Value space: Direct/Gatekeeper
  Direct: You can only make an H.323 call by dialing an IP address directly.
  Gatekeeper: The system uses a Gatekeeper to make an H.323 call. When choosing this option, the H323 Gatekeeper Address must also be configured.
**H323 Encryption KeySize**

Define the minimum or maximum key size for the Diffie-Hellman key exchange method, which is used when establishing the Advanced Encryption Standard (AES) encryption key.

Requires user role: ADMIN
Default value: Min1024bit

Value space: Min1024bit/Max1024bit/Min2048bit
  - Min1024bit: The minimum size is 1024 bit.
  - Max1024bit: The maximum size is 1024 bit.
  - Min2048bit: The minimum size is 2048 bit.

**H323 Gatekeeper Address**

Define the IP address of the Gatekeeper. Requires H323 CallSetup Mode to be set to Gatekeeper.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 255)
  - A valid IPv4 address, IPv6 address or DNS name.

**H323 H323Alias E164**

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

Requires user role: ADMIN
Default value: ""

Value space: String (0, 30)
  - The H.323 Alias E.164 address. Valid characters are 0-9, *, and #.

**H323 H323Alias ID**

Define the H.323 Alias ID, which is used to address the system on a H.323 Gatekeeper and will be displayed in the call lists.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 49)
  - The H.323 Alias ID. Example: "firstname.lastname@company.com", "My H.323 Alias ID"

**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
Default value: Off

Value space: Auto/Off/On
  - Auto: The system will determine if the H323 NAT Address or the real IP address should be used in signaling. This makes it possible to place calls to endpoints on the LAN as well as endpoints on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.
  - Off: The system will signal the real IP address.
  - On: The system will signal the configured H323 NAT Address instead of its real IP address in Q.931 and H.245. The NAT server address will be shown in the startup-menu as: "My IP Address: 10.0.2.1". If the H323 NAT Address is wrong or not set, H.323 calls cannot be set up.
H323 NAT Address

Define the external/global IP address to the router with NAT support. Packets sent to the router will then be routed to the system. Note that NAT cannot be used when registered to a gatekeeper.

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

* Port 1720
* Port 5555–6555
* Port 2326–2487

Requires user role: ADMIN
Default value: ""
Value space: String (0, 64)
   A valid IPv4 address or IPv6 address.

H323 Port Allocation

This setting affects the H.245 port numbers used for H.323 call signaling.

Requires user role: ADMIN
Default value: Dynamic
Value space: Dynamic/Static
   Dynamic: The system will allocate which ports to use when opening a TCP connection. The reason for doing this is to avoid using the same ports for subsequent calls, as some firewalls consider this as a sign of attack. When Dynamic is selected, the H.323 ports used are from 11000 to 20999. Once 20999 is reached they restart again at 11000. The ports are automatically selected by the system within the given range. Firewall administrators should not try to deduce which ports are used when, as the allocation schema within the mentioned range may change without any further notice.
   Static: When set to Static the ports are given within a static predefined range [5555–6555].
Logging settings

Logging External Mode
Determine whether or not to use a remote syslog server for logging.
Requires user role: ADMIN
Default value: Off
Value space: Off/On
   Off: Disable logging to a remote syslog server.
   On: Enable logging to a remote syslog server.

Logging External Protocol
Determine which protocol to use toward the remote logging server. You can use either the syslog protocol over TLS (Transport Layer Security), or the syslog protocol in plaintext. For details about the syslog protocol, see RFC 5424.
Requires user role: ADMIN
Default value: SyslogTLS
Value space: Syslog/SyslogTLS
   Syslog: Syslog protocol in plain text.
   SyslogTLS: Syslog protocol over TLS.

Logging External Server Address
The address of the remote syslog server.
Requires user role: ADMIN
Default value: ""
Value space: String (0..255)
   A valid IPv4 address, IPv6 address or DNS name.

Logging External Server Port
The port that the remote syslog server listens for messages on. If set to 0, which is the default, the video system will use the standard syslog port. The standard syslog port is 514 for syslog, and 6514 for syslog over TLS.
Requires user role: ADMIN
Default value: 514
Value space: Integer (0..65535)
   The number of the port that the remote syslog server is using. 0 means that the video system uses the standard syslog port.

Logging Mode
Define the logging mode for the video system (syslog service). When disabled, the syslog service does not start, and most of the event logs are not generated. The Historical Logs and Call Logs are not affected.
Requires user role: ADMIN
Default value: On
Value space: Off/On
   Off: Disable the system logging service.
   On: Enable the system logging service.
Network settings

Network [1] DNS Domain Name
The 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, USER
Default value: ""
Value space: String (0, 64)
The DNS domain name.

Define the network addresses for DNS servers. Up to three addresses may be specified. If the network addresses are unknown, contact your administrator or Internet Service Provider.

Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 64)
A valid IPv4 address or IPv6 address.

Network [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, USER
Default value: Off
Value space: Off/On
Off: The 802.1X authentication is disabled (default).
On: The 802.1X authentication is enabled.

Network [1] IEEE8021X TlsVerify
Verification of the server-side certificate of an IEEE802.1x connection against the certificates in the local CA-list when TLS is used. The CA-list must be uploaded to the video system. This can be done from the web interface.
This setting takes effect only when Network [1] IEEE8021X Eap Tls is enabled (On).

Requires user role: ADMIN, USER
Default value: Off
Value space: Off/On
Off: When set to Off, TLS connections are allowed without verifying the server-side X.509 certificate against the local CA-list. This should typically be selected if no CA-list has been uploaded to the codec.
On: When set to On, the server-side X.509 certificate will be validated against the local CA-list for all TLS connections. Only servers with a valid certificate will be allowed.

Authentication using a private key/certificate pair during an IEEE802.1x connection. The authentication X.509 certificate must be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN, USER
Default value: Off
Value space: Off/On
Off: When set to Off client-side authentication is not used (only server-side).
On: When set to On the client (video system) will perform a mutual authentication TLS handshake with the server.
Network [1] IEEE8021X Identity
Define the user name for 802.1X authentication.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 64)
   The user name for 802.1X authentication.

Network [1] IEEE8021X Password
Define the password for 802.1X authentication.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 32)
   The password for 802.1X authentication.

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, USER
Default value: ""
Value space: String (0, 64)
   The 802.1X Anonymous ID string.

Define 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, USER
Default value: On
Value space: Off/On
   Off: The EAP-MD5 protocol is disabled.
   On: The EAP-MD5 protocol is enabled (default).

Network [1] IEEE8021X Eap Ttls
Define 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, USER
Default value: On
Value space: Off/On
   Off: The EAP-TTLS protocol is disabled.
   On: The EAP-TTLS protocol is enabled (default).

Network [1] IEEE8021X Eap Tls
Enable or disable the use of EAP-TLS (Transport Layer Security) for IEEE802.1x connections. The EAP-TLS protocol, defined in RFC 5216, is considered one of the most secure EAP standards. LAN clients are authenticated using client certificates.
Requires user role: ADMIN, USER
Default value: On
Value space: Off/On
   Off: The EAP-TLS protocol is disabled.
   On: The EAP-TLS protocol is enabled (default).
Cisco DX70 and DX80

Network [1] IEEE8021X Eap Peap

Define 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, USER
Default value: On
Value space: Off/On
  Off: The EAP-PEAP protocol is disabled.
  On: The EAP-PEAP protocol is enabled (default).

Network [1] IPStack

Select if the system should use IPv4, IPv6, or dual IP stack, on the network interface. NOTE: After changing this setting you may have to wait up to 30 seconds before it takes effect.

Requires user role: ADMIN, USER
Default value: Dual
Value space: Dual/IPv4/IPv6
  Dual: When set to Dual, the network interface can operate on both IP versions at the same time, and can have both an IPv4 and an IPv6 address at the same time.
  IPv4: When set to IPv4, the system will use IPv4 on the network interface.
  IPv6: When set to IPv6, the system will use IPv6 on the network interface.

Network [1] IPv4 Assignment

Define how the system will obtain its IPv4 address, subnet mask and gateway address. This setting only applies to systems on IPv4 networks.

Requires user role: ADMIN, USER
Default value: DHCP
Value space: Static/DHCP
  Static: The addresses must be configured manually using the Network IPv4 Address, Network IPv4 Gateway and Network IPv4 SubnetMask settings (static addresses).
  DHCP: The system addresses are automatically assigned by the DHCP server.

Network [1] IPv4 Address

Define the static IPv4 network address for the system. Applicable only when Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER
Default value: **
Value space: String (0, 64)
  A valid IPv4 address.

Network [1] IPv4 Gateway

Define the IPv4 network gateway address. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER
Default value: **
Value space: String (0, 64)
  A valid IPv4 address.

Network [1] IPv4 SubnetMask

Define the IPv4 network subnet mask. Applicable only when the Network IPv4 Assignment is set to Static.

Requires user role: ADMIN, USER
Default value: **
Value space: String (0, 64)
  A valid IPv4 address.
Network [1] IPv6 Assignment

Define how the system will obtain its IPv6 address and the default gateway address. This setting only applies to systems on IPv6 networks.

Requires user role: ADMIN, USER
Default value: Autoconf

Value space: Static/DHCPv6/Autoconf
  - Static: The codec and gateway IP addresses must be configured manually using the Network IPv6 Address and Network IPv6 Gateway settings. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.
  - DHCPv6: All IPv6 addresses, including options, will be obtained from a DHCPv6 server. See RFC 3315 for a detailed description. The Network IPv6 DHCPOptions setting will be ignored.
  - Autoconf: Enable IPv6 stateless autoconfiguration of the IPv6 network interface. See RFC 4862 for a detailed description. The options, for example NTP and DNS server addresses, must either be set manually or obtained from a DHCPv6 server. The Network IPv6 DHCPOptions setting determines which method to use.

Network [1] IPv6 Address

Define the static IPv6 network address for the system. Applicable only when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER
Default value: ""

Value space: String (0, 64)
  - A valid IPv6 address including a network mask. Example: 2001:DB8::/48


Define the IPv6 network gateway address. This setting is only applicable when the Network IPv6 Assignment is set to Static.

Requires user role: ADMIN, USER
Default value: ""

Value space: String (0, 64)
  - A valid IPv6 address.

Network [1] IPv6 DHCPOptions

Retrieve a set of DHCP options, for example NTP and DNS server addresses, from a DHCPv6 server.

Requires user role: ADMIN, USER
Default value: On

Value space: Off/On
  - Off: Disable the retrieval of DHCP options from a DHCPv6 server.
  - On: Enable the retrieval of a selected set of DHCP options from a DHCPv6 server.

Network [1] MTU

Define the Ethernet MTU (Maximum Transmission Unit) size. The MTU size must be supported by your network infrastructure. The minimum size is 576 for IPv4 and 1280 for IPv6.

Requires user role: ADMIN, USER
Default value: 1500

Value space: Integer (576..1500)
  - Set a value for the MTU (bytes).

Network [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, USER
Default value: Diffserv

Value space: Off/Diffserv
  - Off: No QoS method is used.
  - Diffserv: When you set the QoS Mode to Diffserv, the Network QoS Diffserv Audio, Network QoS Diffserv Video, Network QoS Diffserv Data, Network QoS Diffserv Signalling, Network QoS Diffserv ICMPv6 and Network QoS Diffserv NTP settings are used to prioritize packets.
Network [1] QoS Diffserv Audio
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority Audio packets should have in the IP network.
The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Audio is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
Set the priority of the audio packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Video
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority Video packets should have in the IP network. The packets on the presentation channel (shared content) are also in the Video packet category. The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Video is CS4, which equals the decimal value 32. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
Set the priority of the video packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Data
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority Data packets should have in the IP network.
The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for Data is 0, which means best effort. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
Set the priority of the data packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv Signalling
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority Signalling packets that are deemed critical (time-sensitive) for the real-time operation should have in the IP network.
The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended class for Signalling is CS3, which equals the decimal value 24. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
Set the priority of the signalling packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).
Network [1] QoS Diffserv ICMPv6
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority ICMPv6 packets should have in the IP network.
The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for ICMPv6 is 0, which means best effort. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
set the priority of the ICMPv6 packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Network [1] QoS Diffserv NTP
This setting will only take effect if Network QoS Mode is set to Diffserv.
Define which priority NTP packets should have in the IP network.
The priority for the packets ranges from 0 to 63 - the higher the number, the higher the priority. The recommended value for NTP is 0, which means best effort. If in doubt, contact your network administrator.
The priority set here might be overridden when packets are leaving the network controlled by the local network administrator.
Requires user role: ADMIN, USER
Default value: 0
Value space: Integer (0..63)
set the priority of the NTP packets in the IP network - the higher the number, the higher the priority. The default value is 0 (best effort).

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the codec from SSH/Telnet/HTTP/HTTPS. Multiple IP addresses are separated by a white space.
A network mask (IP range) is specified by <ip address>/N, where N is 1-32 for IPv4, and N is 1-128 for IPv6. The /N is a common indication of a network mask where the first N bits are set. Thus 192.168.0.0/24 would match any address starting with 192.168.0, since these are the first 24 bits in the address.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 255)
a valid IPv4 address or IPv6 address.

Network [1] Speed
Define the Ethernet link speed. We recommend not to change from the default value, which negotiates with the network to set the speed automatically. If you do not use autonegotiation, make sure that the speed you choose is supported by the closest switch in your network infrastructure.
Requires user role: ADMIN, USER
Default value: Auto
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.
Network [1] Traffic Control Mode
Define the network traffic control mode to decide how to control the video packets transmission speed.

Requires user role: ADMIN, USER
Default value: On
Value space: Off/On
  - Off: Transmit video packets at link speed.
  - On: Transmit video packets at maximum 20 Mbps. Can be used to smooth out bursts in the outgoing network traffic.

Network [1] VLAN Voice Mode
Define the VLAN voice mode. The VLAN Voice Mode will be set to Auto automatically if you have Cisco UCM (Cisco Unified Communications Manager) as provisioning infrastructure. Note that Auto mode will NOT work if the Network Services CDP Mode setting is Off.

Requires user role: ADMIN, USER
Default value: Auto
Value space: Auto/Manual/Off
  - Auto: The Cisco Discovery Protocol (CDP), if available, assigns an id to the voice VLAN. If CDP is not available, VLAN is not enabled.
  - Manual: The VLAN ID is set manually using the Network VLAN Voice VlanId setting. If CDP is available, the manually set value will be overruled by the value assigned by CDP.
  - Off: VLAN is not enabled.

Network [1] VLAN Voice VlanId
Define the VLAN voice ID. This setting will only take effect if Network VLAN Voice Mode is set to Manual.

Requires user role: ADMIN, USER
Default value: 1
Value space: Integer (1..4094)
  - Set the VLAN voice ID.
NetworkServices settings

NetworkServices CDP Mode
Enable or disable the CDP (Cisco Discovery Protocol) daemon. Enabling CDP will make the endpoint report certain statistics and device identifiers to a CDP-enabled switch. If CDP is disabled, the Network VLAN Voice Mode: Auto setting will not work.
Requires user role: ADMIN
Default value: On
Value space: Off/On
  Off: The CDP daemon is disabled.
  On: The CDP daemon is enabled.

NetworkServices H323 Mode
Define whether the system should be able to place and receive H.323 calls or not.
Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: Disable the possibility to place and receive H.323 calls.
  On: Enable the possibility to place and receive H.323 calls (default).

NetworkServices HTTP Mode
Define whether or not to allow access to the video system using the HTTP or HTTPS (HTTP Secure) protocols. Note that the video system's web interface use HTTP or HTTPS. If this setting is switched Off, you cannot use the web interface.
If you need extra security (encryption and decryption of requests, and pages that are returned by the web server), allow only HTTPS.
Requires user role: ADMIN
Default value: HTTP+HTTPS
Value space: Off/HTTP+HTTPS/HTTPS
  Off: Access to the video system not allowed via HTTP or HTTPS.
  HTTP+HTTPS: Access to the video system allowed via both HTTP and HTTPS.
  HTTPS: Access to the video system allowed via HTTPS, but not via HTTP.

NetworkServices HTTPS VerifyServerCertificate
When the video system connects to an external HTTPS server (like a phone book server or an external manager), this server will present a certificate to the video system to identify itself.
Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: Do not verify server certificates.
  On: Requires the system to verify that the server certificate is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.
NetworkServices HTTPS VerifyClientCertificate

When the video system connects to a HTTPS client (like a web browser), the client can be asked to present a certificate to the video system to identify itself.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: Do not verify client certificates.
  On: Requires the client to present a certificate that is signed by a trusted Certificate Authority (CA). This requires that a list of trusted CAs are uploaded to the system in advance.

NetworkServices HTTPS OCSP Mode

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

For any outgoing HTTPS connection, the OCSP responder is queried of the status. If the corresponding certificate has been revoked, then the HTTPS connection will not be used.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: Disable OCSP support.
  On: Enable OCSP support.

NetworkServices HTTPS OCSP URL

Define the URL of the OCSP responder (server) that will be used to check the certificate status.

Requires user role: ADMIN
Default value: ""
Value space: String (0, 255)
  A valid URL.

NetworkServices NTP Mode

The Network Time Protocol (NTP) is used to synchronize the system's time and date to a reference time server. The time server will be queried regularly for time updates.

Requires user role: ADMIN
Default value: Auto
Value space: Auto/Manual/Off
  Auto: The system will use an NTP server for time reference. As default, the server address will be obtained from the network's DHCP server. If a DHCP server is not used, or if the DHCP server does not provide an NTP server address, the NTP server address that is specified in the NetworkServices NTP Server [n] Address setting will be used.
  Manual: The system will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.
  Off: The system will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

NetworkServices NTP Server [1..3] Address

The address of the NTP server that will be used when NetworkServices NTP Mode is set to Manual, and when NetworkServices NTP Mode is set to Auto and no address is supplied by a DHCP server.

Requires user role: ADMIN
Default value: 0.tandberg.pool.ntp.org
Value space: String (0, 255)
  A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SIP Mode

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

Requires user role: ADMIN
Default value: On
Value space: Off/On
  Off: Disable the possibility to place and receive SIP calls.
  On: Enable the possibility to place and receive SIP calls (default).
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
Default value: ReadOnly
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.

NetworkServices SNMP Host [1..3] Address

Define the address of up to three SNMP Managers.
The system's SNMP Agent (in the codec) responds to requests from SNMP Managers (a PC program etc.), for example about system location and system contact. SNMP traps are not supported.

Requires user role: ADMIN
Default value: *
Value space: String (0, 255)
  A valid IPv4 address, IPv6 address or DNS name.

NetworkServices SNMP CommunityName

Define 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
Default value: *
Value space: String (0, 50)
  The SNMP community name.

NetworkServices SNMP SystemContact

Define the name of the Network Services SNMP System Contact.

Requires user role: ADMIN
Default value: *
Value space: String (0, 50)
  The name of the SNMP system contact.

NetworkServices SNMP SystemLocation

Define the name of the Network Services SNMP System Location.

Requires user role: ADMIN
Default value: *
Value space: String (0, 50)
  The name of the SNMP system location.
NetworkServices SSH Mode
SSH (or Secure Shell) protocol can provide secure encrypted communication between the codec and your local computer.
Requires user role: ADMIN
Default value: On
Value space: Off/On
   Off: The SSH protocol is disabled.
   On: The SSH protocol is enabled.

NetworkServices SSH AllowPublicKey
Secure Shell (SSH) public key authentication can be used to access the codec.
Requires user role: ADMIN
Default value: On
Value space: Off/On
   Off: The SSH public key is not allowed.
   On: The SSH public key is allowed.

NetworkServices TelNet Mode
Telnet is a network protocol used on the Internet or Local Area Network (LAN) connections.
Requires user role: ADMIN
Default value: Off
Value space: Off/On
   Off: The Telnet protocol is disabled. This is the factory setting.
   On: The Telnet protocol is enabled.

NetworkServices WelcomeText
Choose which information the user should see when logging on to the codec through Telnet/SSH.
Requires user role: ADMIN
Default value: On
Value space: Off/On
   Off: The welcome text is: Login successful
   On: The welcome text is: Welcome to <system name>; Software version; Software release date; Login successful.

NetworkServices WIFI Allowed
DX video systems that have a built-in Wi-Fi adapter, can connect to the network either via Ethernet or Wi-Fi. They cannot connect to both at the same time. The systems support the following standards: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n. The following security types are supported: WPA-PSK TKIP, WPA2-PSK AES, and open (not secured).
Both Ethernet and Wi-Fi are allowed by default. Use this setting if you want to prohibit the use of Wi-Fi.
Some DX video systems ship without the built-in Wi-Fi adapter (the PID, which you find on the rating label at the rear of the video system, are CP-DX80-NR-K9=, or CP-DX70-W-NR-K9= for these units). These systems do not get the option to configure Wi-Fi at all.
Requires user role: ADMIN
Default value: True
Value space: False/True
   False: Wi-Fi cannot be used. You must connect to the network via Ethernet.
   True: Both Ethernet and Wi-Fi are allowed.
NetworkServices WIFI Enabled

Provided that the video system is allowed to connect to the network via Wi-Fi (see the NetworkServices WIFI Allowed setting), you can use this setting to enable and disable Wi-Fi.

You cannot use Ethernet and Wi-Fi at the same time. If you try to configure Wi-Fi while an Ethernet cable is connected, you must unplug the Ethernet cable to proceed. If you connect an Ethernet cable while connected to Wi-Fi, Ethernet will take precedence. If you unplug the Ethernet cable, the video system will automatically connect to the last connected Wi-Fi network, if available.

Requires user role: ADMIN
Default value: False

Value space: False/True
- False: Wi-Fi is disabled.
- True: Wi-Fi is enabled.

NetworkServices XMLAPI Mode

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

Requires user role: ADMIN
Default value: On

Value space: Off/On
- Off: The XML API is disabled.
- On: The XML API is enabled (default).
Peripherals settings

Peripherals Pairing Ultrasound Volume Mode
This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN
Default value: Dynamic
Value space: Dynamic/Static
Dynamic: The video system adjusts the ultrasound volume dynamically. The volume may vary up to the maximum level as defined in the Peripherals Pairing Ultrasound Volume MaxLevel setting.
Static: Use only if advised by Cisco.

Peripherals Pairing Ultrasound Volume MaxLevel
This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message. Refer to the Peripherals Pairing Ultrasound Volume Mode setting.

Requires user role: ADMIN
Default value: DX80: 70  DX70: 60
Value space: DX80: Integer (0..90)  DX70: Integer (0..60)
Select a value in the specified range. If set to 0, the ultrasound is switched off.

Peripherals Profile ControlSystems
Define if a third-party control system, for example Crestron or AMX, is expected to be connected to the video system. This information is used by the video system’s diagnostics service. If the number of connected control systems does not match this setting, the diagnostics service will report it as an inconsistency. Note that only one third-party control system is supported.

If set to 1, the control system must send heart beats to the video system using xCommand Peripherals Pair and HeartBeat commands. Failing to do so will cause the in-room control extensions to show a warning that the video system has lost connectivity to the control system.

Requires user role: ADMIN
Default value: NotSet
Value space: 1/NotSet
1: One third-party control system should be connected to the video system.
NotSet: No check for a third-party control system is performed.
Phonebook settings

Phonebook Server [1] ID
Define a name for the external phone book.
Requires user role: ADMIN
Default value: ""
Value space: String (0, 64)
  The name for the external phone book.

Phonebook Server [1] Type
Select the phonebook server type.
Requires user role: ADMIN
Default value: Off
Value space: Off/CUCM/Spark/TMS/VCS
  Off: Do not use a phonebook.
  CUCM: The phonebook is located on the Cisco Unified Communications Manager.
  Spark: The phonebook is located on Spark.
  TMS: The phonebook is located on the Cisco TelePresence Management Suite server.
  VCS: The phonebook is located on the Cisco TelePresence Video Communication Server.

Phonebook Server [1] URL
Define the address (URL) to the external phone book server.
Requires user role: ADMIN
Default value: ""
Value space: String (0, 255)
  A valid address (URL) to the phone book server.
Provisioning settings

Provisioning Connectivity
This setting controls how the device discovers whether it should request an internal or external configuration from the provisioning server.

Requires user role: ADMIN, USER
Default value: Auto

Value space: Internal/External/Auto
  Internal: Request internal configuration.
  External: Request external configuration.
  Auto: Automatically discover using NAPTR queries whether internal or external configurations should be requested. If the NAPTR responses have the "e" flag, external configurations will be requested. Otherwise internal configurations will be requested.

Provisioning Mode
It is possible to configure a video system using a provisioning system (external manager). This allows video conferencing network administrators to manage many video systems simultaneously. With this setting you choose which type of provisioning system to use. Provisioning can also be switched off. Contact your provisioning system provider/representative for more information.

Requires user role: ADMIN, USER
Default value: Auto

Value space: Off/Auto/CUCM/Edge/Spark/TMS/VCS
  Off: The video system is not configured by a provisioning system.
  Auto: Automatically select the provisioning server.
  CUCM: Push configurations to the video system from CUCM (Cisco Unified Communications Manager).
  Edge: Push configurations to the video system from CUCM (Cisco Unified Communications Manager). The system connects to CUCM via the Collaboration Edge infrastructure.
  Spark: Push configurations to the video system from Spark.
  TMS: Push configurations to the video system from TMS (Cisco TelePresence Management System).
  VCS: Push configurations to the video system from VCS (Cisco TelePresence Video Communication Server).

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

Requires user role: ADMIN, USER
Default value: ""

Value space: String (0, 80)
A valid username.
Provisioning Password
This is the password part of the credentials used to authenticate the video system with the provisioning server. This setting must be used when required by the provisioning server.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 64)
A valid password.

Provisioning HttpMethod
Select the HTTP method to be used for the provisioning.
Requires user role: ADMIN, USER
Default value: POST
Value space: GET/POST
GET: Select GET when the provisioning server supports GET.
POST: Select POST when the provisioning server supports POST.

Provisioning ExternalManager Address
Define the IP Address or DNS name of the external manager / provisioning system. If an External Manager Address (and Path) is configured, the system will send a message to this address when starting up. When receiving this message the external manager / provisioning system can return configurations/commands to the unit as a result.
When using CUCM or TMS provisioning, the DHCP server can be set up to provide the external manager address automatically (DHCP Option 242 for TMS, and DHCP Option 150 for CUCM). An address set in the Provisioning ExternalManager Address setting will override the address provided by DHCP.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 64)
A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager AlternateAddress
Only applicable when the endpoint is provisioned by Cisco Unified Communication Manager (CUCM) and an alternate CUCM is available for redundancy. Define the address of the alternate CUCM. If the main CUCM is not available, the endpoint will be provisioned by the alternate CUCM. When the main CUCM is available again, the endpoint will be provisioned by this CUCM.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 64)
A valid IPv4 address, IPv6 address or DNS name.

Provisioning ExternalManager Protocol
Define whether to use the HTTP (unsecure communication) or HTTPS (secure communication) protocol when sending requests to the external manager / provisioning system.
The chosen protocol must be enabled in the NetworkServices HTTP Mode setting.
Requires user role: ADMIN, USER
Default value: HTTP
Value space: HTTPS/HTTP
HTTPS: Send requests via HTTPS.
HTTP: Send requests via HTTP.

Provisioning ExternalManager Path
Define the Path to the external manager / provisioning system. This setting is required when several management services reside on the same server, i.e. share the same External Manager address.
Requires user role: ADMIN, USER
Default value: ""
Value space: String (0, 255)
A valid path to the external manager or provisioning system.
Provisioning ExternalManager Domain

Define the SIP domain for the VCS provisioning server.

Requires user role: ADMIN, USER
Default value: ""

Value space: String (0, 64)
  A valid domain name.
Proximity settings

Proximity Mode
Determine whether the video system will emit ultrasound pairing messages or not.
When the video system emits ultrasound, Proximity clients can detect that they are close to the video system. In order to use a client, at least one of the Proximity services must be enabled (refer to the Proximity Services settings). In general, Cisco recommends enabling all the Proximity services.

Requires user role: ADMIN, USER
Default value: Off
Value space: Off/On
- Off: The video system does not emit ultrasound, and Proximity services cannot be used.
- On: The video system emits ultrasound, and Proximity clients can detect that they are close to the video system. Enabled Proximity services can be used.

Proximity Services CallControl
Enable or disable basic call control features on Proximity clients. When this setting is enabled, you are able to control a call using a Proximity client (for example dial, mute, adjust volume and hang up). This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER
Default value: Disabled
Value space: Enabled/Disabled
- Enabled: Call control from a Proximity client is enabled.
- Disabled: Call control from a Proximity client is disabled.

Proximity Services ContentShare FromClients
Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the video system, e.g. share your laptop screen. This service is supported by laptops (OS X and Windows). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER
Default value: Enabled
Value space: Enabled/Disabled
- Enabled: Content sharing from a Proximity client is enabled.
- Disabled: Content sharing from a Proximity client is disabled.

Proximity Services ContentShare ToClients
Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the video system. You can zoom in on details, view previous content and take snapshots. This service is supported by mobile devices (iOS and Android). Proximity Mode must be On for this setting to take any effect.

Requires user role: ADMIN, USER
Default value: Disabled
Value space: Enabled/Disabled
- Enabled: Content sharing to a Proximity client is enabled.
- Disabled: Content sharing to a Proximity client is disabled.
RoomReset settings

RoomReset Control
Not applicable.
RTP settings

RTP Ports Range Start
Define the first port in the range of RTP ports.
As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

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

Requires user role: ADMIN
Default value: 2326

Value space: Integer (1024..65438)
Set the first port in the range of RTP ports.

RTP Ports Range Stop
Define the last port in the range of RTP ports.
As default, the system is using the UDP ports in the range 2326 to 2487 for RTP and RTCP media data. Each media channel is using two adjacent ports for RTP and RTCP. The default number of ports required in the UDP port range is based on the number of simultaneous calls that the endpoint is capable of.

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

Requires user role: ADMIN
Default value: 2486

Value space: Integer (1120..65535)
Set the last port in the range of RTP ports.
Security settings

Security Audit Logging Mode
Define where to record or transmit the audit logs. The audit logs are sent to a syslog server. When using the External/ExternalSecure modes and setting the port assignment to manual in the Security Audit Server PortAssignment setting, you must also enter the address and port number for the audit server in the Security Audit Server Address and Security Audit Server Port settings.

Requires user role: AUDIT
Default value: Off
Value space: Off/Internal/External/ExternalSecure
- Off: No audit logging is performed.
- Internal: The system records the audit logs to internal logs, and rotates logs when they are full.
- External: The system sends the audit logs to an external syslog server. The syslog server must support UDP.
- ExternalSecure: The system sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the codec using the web interface. The common_name parameter of a certificate in the CA list must match the IP address of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

Security Audit OnError Action
Define what happens when the connection to the syslog server is lost. This setting is only relevant when Security Audit Logging Mode is set to ExternalSecure.

Requires user role: AUDIT
Default value: Ignore
Value space: Halt/Ignore
- Halt: If a halt condition is detected the system codec is rebooted and only the auditor is allowed to operate the unit until the halt condition has passed. When the halt condition has passed the audit logs are re-spooled to the syslog server. Halt conditions are: A network breach (no physical link), no syslog server running (or incorrect address or port to the syslog server), TLS authentication failed (if in use), local backup (re-spooling) log full.
- Ignore: The system will continue its normal operation, and rotate internal logs when full. When the connection is restored it will again send its audit logs to the syslog server.

Security Audit Server Address
The audit logs are sent to a syslog server. Define the IP address of the syslog server. Only valid IPv4 or IPv6 address formats are accepted. Host names are not supported. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure.

Requires user role: AUDIT
Default value: **
Value space: String (0, 255)
A valid IPv4 address or IPv6 address
Security Audit Server Port

The audit logs are sent to a syslog server. Define the port of the syslog server that the system shall send its audit logs to. This setting is only relevant when Security Audit Server PortAssignment is set to Manual.

Requires user role: AUDIT
Default value: 514
Value space: Integer (0..65535)
Set the audit server port.

Security Audit Server PortAssignment

The audit logs are sent to a syslog server. You can define how the port number of the external syslog server will be assigned. This setting is only relevant when Security Audit Logging Mode is set to External or ExternalSecure. To see which port number is used you can check the Security Audit Server Port status. Navigate to Configuration > System status on the web interface or, if on a command line interface, run the command xStatus Security Audit Server Port.

Requires user role: AUDIT
Default value: Auto
Value space: Auto/Manual
- Auto: Will use UDP port number 514 when the Security Audit Logging Mode is set to External. Will use TCP port number 6514 when the Security Audit Logging Mode is set to ExternalSecure.
- Manual: Will use the port value defined in the Security Audit Server Port setting.

Security Session InactivityTimeout

Define how long the system will accept inactivity from the user before he is automatically logged out from a web, Telnet, or SSH session.

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

Requires user role: ADMIN
Default value: 0
Value space: Integer (0..10000)
Set the inactivity timeout (minutes); or select 0 when inactivity should not enforce automatic logout.

Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user. 0, which is the default value, means no hard limit. Sessions consume resources, so there will be some limitation, but this may vary based on different criteria.

Requires user role: ADMIN
Default value: 0
Value space: Integer (0..100)
The maximum number of sessions per user. 0 means no hard limit.

Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total. 0, which is the default value, means no hard limit. Sessions consume resources, so there will be some limitation, but this may vary based on different criteria.

Requires user role: ADMIN
Default value: 0
Value space: Integer (0..100)
The maximum number of sessions in total. 0 means no hard limit.

Security Session ShowLastLogon

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

Requires user role: ADMIN
Default value: Off
Value space: Off/On
- Off: Do not show information about the last session.
- On: Show information about the last session.
SerialPort settings

SerialPort Mode
Enable/disable the serial port (connection via Micro USB to USB cable). The serial port uses 115200 bps, 8 data bits, no parity and 1 stop bit.

Requires user role: ADMIN
Default value: On
Value space: Off/On
  Off: Disable the serial port.
  On: Enable the serial port.

SerialPort LoginRequired
Define if login shall be required when connecting to the serial port.

Requires user role: ADMIN
Default value: On
Value space: Off/On
  Off: The user can access the codec via the serial port without any login.
  On: Login is required when connecting to the codec via the serial port.
SIP settings

SIP ANAT
ANAT (Alternative Network Address Types) enables media negotiation for multiple addresses and address types, as specified in RFC 4091.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
  Off: Disable ANAT.
  On: Enable ANAT.

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

Requires user role: ADMIN
Default value: ""
Value space: String (0, 128)
  A valid username.

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

Requires user role: ADMIN
Default value: ""
Value space: String (0, 128)
  A valid password.

SIP DefaultTransport
Select the transport protocol to be used over the LAN.

Requires user role: ADMIN
Default value: Auto
Value space: TCP/UDP/Tls/Auto
  TCP: The system will always use TCP as the default transport method.
  UDP: The system will always use UDP as the default transport method.
  Tls: The system will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the video system. If no such CA-list is available on the system then anonymous Diffie Hellman will be used.
  Auto: The system will try to connect using transport protocols in the following order: TLS, TCP, UDP.

SIP DisplayName
When configured the incoming call will report the display name instead of the SIP URI.

Requires user role: ADMIN
Default value: ""
Value space: String (0, 550)
  The name to be displayed instead of the SIP URI.
SIP Ice Mode

ICE (Interactive Connectivity Establishment, RFC 5245) is a NAT traversal solution that the video systems can use to discover the optimized media path. Thus the shortest route for audio and video is always secured between the video systems.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/Off/On
  Auto: ICE is enabled if a TURN server is provided, otherwise ICE is disabled.
  Off: ICE is disabled.
  On: ICE is enabled.

SIP Ice DefaultCandidate

The ICE protocol needs some time to reach a conclusion about which media route to use (up to the first 5 seconds of a call). During this period media for the video system will be sent to the Default Candidate as defined in this setting.

Requires user role: ADMIN
Default value: Host

Value space: Host/Rflx/Relay
  Host: Send media to the video system’s private IP address.
  Rflx: Send media to the video system’s public IP address, as seen by the TURN server.
  Relay: Send media to the IP address and port allocated on the TURN server.

SIP Line

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

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

Requires user role: ADMIN
Default value: Private

Value space: Private/Shared
  Shared: The system is part of a shared line and is therefore sharing its directory number with other devices.
  Private: This system is not part of a shared line (default).

SIP ListenPort

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the endpoint will only be reachable through the SIP registrar (CUCM or VCS). It is recommended to leave this setting at its default value.

Requires user role: ADMIN
Default value: On

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

SIP Mailbox

When registered to a Cisco Unified Communications Manager (CUCM) you may be offered the option of having a private voice mailbox.

Requires user role: ADMIN
Default value: **

Value space: String (0, 255>)
  A valid number or address. Leave the string empty if you do not have a voice mailbox.
SIP PreferredIPMedia

Define the preferred IP version for sending and receiving media (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version.

Requires user role: ADMIN
Default value: IPv4

Value space: IPv4/IPv6
  IPv4: The preferred IP version for media is IPv4.
  IPv6: The preferred IP version for media is IPv6.

SIP PreferredIPSignaling

Define the preferred IP version for signaling (audio, video, data). Only applicable when both Network IPStack and Conference CallProtocolIPStack are set to Dual, and the network does not have a mechanism for choosing the preferred IP version. It also determines the priority of the A/AAAA lookups in DNS, so that the preferred IP version is used for registration.

Requires user role: ADMIN
Default value: IPv4

Value space: IPv4/IPv6
  IPv4: The preferred IP version for signaling is IPv4.

SIP 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.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 255)
  A valid IPv4 address, IPv6 address or DNS name.

SIP TlsVerify

For TLS connections a SIP CA-list can be uploaded to the video system. This can be done from the web interface.

Requires user role: ADMIN
Default value: Off

Value space: Off/On
  Off: Set to Off to allow TLS connections without verifying them. The TLS connections are allowed to be set up without verifying the x.509 certificate received from the server against the local CA-list. This should typically be selected if no SIP CA-list has been uploaded.
  On: Set to On to verify TLS connections. Only TLS connections to servers, whose x.509 certificate is validated against the CA-list, will be allowed.

SIP Turn DiscoverMode

Define the discover mode to enable/disable the application to search for available Turn servers in DNS. Before making calls, the system will test if port allocation is possible.

Requires user role: ADMIN
Default value: On

Value space: Off/On
  Off: Set to Off to disable discovery mode.
  On: When set to On, the system will search for available Turn servers in DNS, and before making calls the system will test if port allocation is possible.

SIP Turn DropRflx

DropRflx will make the endpoint force media through the Turn relay, unless the remote endpoint is on the same network.

Requires user role: ADMIN
Default value: Off

Value space: Off/On
  Off: Disable DropRflx.
  On: The system will force media through the Turn relay when the remote endpoint is on another network.
SIP Turn Server

Define the address of the TURN (Traversal Using Relay NAT) server. It is used as a media relay fallback and it is also used to discover the endpoint's own public IP address.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 255)
The preferred format is DNS SRV record (e.g. _turn._udp.<domain>), or it can be a valid IPv4 or IPv6 address.

SIP Turn UserName

Define the user name needed for accessing the TURN server.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 128)
A valid user name.

SIP Turn Password

Define the password needed for accessing the TURN server.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 128)
A valid password.

SIP Type

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

Requires user role: ADMIN
Default value: Standard

Value space: Standard/Cisco
  Standard: Use this when registering to standard SIP Proxy (tested with Cisco TelePresence VCS and Broadsoft)
  Cisco: Use this when registering to Cisco Unified Communication Manager.

SIP URI

The SIP URI (Uniform Resource Identifier) is the address that is used to identify the video system. The URI is registered and used by the SIP services to route inbound calls to the system. The SIP URI syntax is defined in RFC 3261.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 255)
An address (URI) that is compliant with the SIP URI syntax.
Standby settings

Standby AudioMotionDetection
The video system is able to automatically discover that people are in its proximity. Given that this feature is switched on, the video system wakes up from standby when someone is detected.

Requires user role: ADMIN
Default value: Off

Value space: Off/On
  - Off: Detection of people in proximity of the video system is switched off.
  - On: Detection of people in proximity of the video system is switched on.

Standby Control
Define whether the system should go into standby mode or not.

Requires user role: ADMIN
Default value: On

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

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

Requires user role: ADMIN
Default value: 10

Value space: Integer (1..480)
  - Set the standby delay (minutes).
SystemUnit settings

SystemUnit Name
Define the system name. The system name will be sent as the hostname in a DHCP request and when the codec is acting as an SNMP Agent.

Requires user role: ADMIN
Default value: ""

Value space: String (0, 50)
  Define the system name.
Time settings

Time TimeFormat
Define the time format.
Requires user role: ADMIN, USER
Default value: 24H
Value space: 24H/12H
  - 24H: Set the time format to 24 hours.
  - 12H: Set the time format to 12 hours (AM/PM).

Time Date Format
Define the date format.
Requires user role: ADMIN, USER
Default value: DD_MM_YY
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
Time Zone

Define the time zone for the geographical location of the video system. The information in the value space is from the tz database, also called the IANA Time Zone Database.

Requires user role: ADMIN, USER

Default value: Etc/UTC

Value space: Africa/Abidjan, Africa/Accra, Africa/Addis_Ababa, Africa/Algiers, Africa/Asmara, Africa/Asmera, Africa/Bamako, Africa/Bangui, Africa/Banjul, Africa/Bissau, Africa/B sostyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/E l_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Liberiville, Africa/Lome, Africa/Luanda, Africa/Lubumbashi, Africa/Lusaka, Africa/Malabo, Africa/Maputo, Africa/Maseru, Africa/Mbabane, Africa/Mogadishu, Africa/Monrovia, Africa/Nairobi, Africa/Ndjamena, Africa/Niamey, Africa/Nouakchott, Africa/Ouagadougou, Africa/Porto-Nov, Africa/Sao_Tome, Africa/Timbuktu, Africa/Tripoli, Africa/Tunis, Africa/Windhoek, America/Adak, America/Anchorage, America/Anguilla, America/Antigua, America/Araguaina, America/Argentina/Buenos_Aires, America/Argentina/Catamarca, America/Argentina/ComodRivadavia, America/Argentina/Cordoba, America/Argentina/Jujuy, America/Argentina/La_Rioja, America/Argentina/Mendoza, America/Argentina/Rio_Gallegos, America/Argentina/Salta, America/Argentina/San_Juan, America/Argentina/San_Luis, America/Argentina/Tucuman, America/Argentina/Ushuaia, America/Aruba, America/Asuncion, America/Atikokan, America/Atka, America/Bahia, America/Bahia_Banderas, America/Barbados, America/Belem, America/Beijing, America/Blanc-Sablon, America/Boa_Vista, America/Bogota, America/Boise, America/Buenos_Aires, America/Cambridge_Bay, America/Campo_Grande, America/Cancun, America/Caracas, America/Catamarca, America/Cayenne, America/Cayman, America/Chicago, America/Chihuahua, America/Coral_Harbour, America/Cordoba, America/Costa_Rica, America/Creston, America/Cuiaba, America/Curacao, America/Danmarkshavn, America/Dawson, America/Dawson_Creek, America/Denver, America/Detroit, America/Dominica, America/Edmonton, America/Eirunep, America/El_Salvador, America/Ensenada, America/Fort_Nelson, America/Fort_Wayne, America/Fortaleza, America/Glace_Bay, America/Godthab, America/Goose_Bay, America/Grand_Turk, America/Grenada, America/Guadeloupe, America/Guatemala, America/Guayaquil, America/Guyana, America/Halifax, America/Havana, America/Hermosillo, America/Indiana/Indianapolis, America/Indiana/Knox, America/Indiana/Marengo, America/Indiana/Petersburg, America/Indiana/Tell_City, America/Indiana/Vevay, America/Indiana/Vincennes, America/Indiana/Winamac, America/Indianapolis, America/Inuvik, America/Iqaluit, America/Jamaica, America/Jujuy, America/Junee, America/Kentucky/Louisville, America/Kentucky/Monticello, America/Knox_IN, America/Kralendijk, America/La_Paz, America/Lima, America/Los_Angeles, America/Louisville, America/Lower_Princes, America/Maceio, America/Managua, America/Manaus, America/Marigot, America/Martinique, America/Matamoros, America/Mazatlan, America/Mendoza, America/Menominee, America/Merida, America/Metaltatla, America/Mexico_City, America/Miquelon, America/Moncton, America/Monterrey, America/Montevideo, America/Montreal, America/Montserrat, America/Nassau, America/New_York, America/Nipigon, America/Nome, America/Noronha, America/North_Dakota/Beulah, America/North_Dakota/Center, America/North_Dakota/New_Salem, America/Ojinaga, America/Panama, America/Pangnirtung, America/Paramaribo, America/Phoenix, America/Port-au-Prince, America/Port_of_Spain, America/Porto_Acre, America/Porto_Velho, America/Puerto_Rico, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarém, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbyland, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yukon, America/Yellowknife, Antarctica/Casely, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Baghdad, Asia/Bahrain, Asia/Baku, Asia/Bangkok, Asia/Barnaul, Asia/Beirut, Asia/Bishkek, Asia/Brunei, Asia/Calcutta, Asia/Chita, Asia/Chobi, Asia/Chongqing, Asia/Chungking, Asia/Colombo, Asia/Dacca, Asia/Damascus, Asia/Dhaka, Asia/Dili, Asia/Dubai, Asia/Dushanbe, Asia/Gaza, Asia/Harbin, Asia/Hebron, Asia/Ho_Chi_Minh, Asia/Hong_Kong, Asia/Hovd, Asia/Irkutsk, Asia/Istanbul, Asia/Jakarta, Asia/Jayapura, Asia/Jerusalem, Asia/Kabal, Asia/Kamchatka, Asia/Karachi, Asia/Kashgar, Asia/Kathmandu, Asia/Katmandu, Asia/Khandyga, Asia/Kolkata, Asia/Krasnoyarsk, Asia/Kuala_Lumpur, Asia/Kuching, Asia/Kuwait, Asia/Macao, Asia/Macau, Asia/Magadan, Asia/Makassar, Asia/Manila, Asia/Muscat, Asia/Nicosia, Asia/Novokuznetsk, Asia/Novosibirsk, Asia/Nov, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Kandad, Asia/Seoul, Asia/Shanghai, Asia/Singapore, Asia/Srednekolymsk, Asia/Taipei, Asia/Tashkent, Asia/Tbilisi, Asia/Tehran, Asia/Tel_Aviv, Asia/Thimbu, Asia/Thimphu, Asia/Tokyo, Asia/Tomsk, Asia/Ujung_Pandang, Asia/Ulanbaatar, Asia/Ulan_Bator, Asia/Urumqi, Asia/Ust-Nera, Asia/Vientiane, Asia/Vladivostok, Asia/Yakutsk, Asia/Yekaterinburg, Asia/Yerevan, Atlantic/Azores, Atlantic/Bermuda, Atlantic/Canary, Atlantic/Cape_Verde, Atlantic/Paerou, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adealde, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman Island, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perah, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CEST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, CET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+11, Etc/GMT+2, Etc/GMT+3, Etc/
Select a time zone from the list.
UserInterface settings

UserInterface ContactInfo Type
Choose which type of contact information to show on the Home screen, and when you tap the Settings icon.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/None/IPv4/IPv6/SipUri/SystemName/DisplayName
- Auto: Show the address which another system can dial to reach this system. The address depends on the system registration.
- None: Do not show any contact information.
- IPv4: Show the system’s IPv4 address.
- IPv6: Show the system’s IPv6 address.
- SipUri: Show the system’s SIP URI (refer to the SIP URI setting).
- SystemName: Show the system’s name (refer to the SystemUnit Name setting).
- DisplayName: Show the system’s display name (refer to the SIP DisplayName setting).

UserInterface KeyTones Mode
You can configure the system to make a keyboard click sound effect (key tone) when typing text or numbers.

Requires user role: ADMIN, USER
Default value: Off

Value space: Off/On
- Off: There is no key tone sound effect.
- On: The key tone sound effect is turned on.

UserInterface Language
Select the language to be used in menus and messages on the screen.

Requires user role: ADMIN, USER
Default value: English

Value space: Arabic/Catalan/ChineseSimplified/ChineseTraditional/Czech/Danish/Dutch/English/EnglishUK/Finnish/French/FrenchCanadian/German/Hebrew/Hungarian/Italian/Japanese/Korean/Norwegian/Polish/PortugueseBrazilian/Russian/Spanish/SpanishLatin/Swedish/Turkish
Select a language from the list.

UserInterface OSD EncryptionIndicator
Define for how long the encryption indicator (a padlock) is shown on screen. The icon for encrypted calls is a locked padlock, and the icon for non-encrypted calls is a crossed out locked padlock.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/AlwaysOn/AlwaysOff
- Auto: If the call is encrypted, a “Call is encrypted” notification is shown for 5 seconds, while the encryption indicator icon is shown for the duration of the call. If the call is not encrypted, a “Call is not encrypted” notification is shown for 5 seconds. Also the encryption indicator icon disappears from screen after 5 seconds.
- AlwaysOn: The encryption indicator is displayed on screen during the entire call.
- AlwaysOff: The encryption indicator is never displayed on screen.
UserInterface OSD Output
Define on which monitor the on-screen information and indicators (OSD) should be displayed.
Requires user role: ADMIN
Default value: Auto
Value space: Auto
  Auto: The system sends the on-screen information and indicators to the system's integrated display.

UserInterface Wallpaper
Select a background image (wallpaper) for the video screen when idle.
You may upload a custom wallpaper to the video system using the web interface. The following file formats are supported: BMP, GIF, JPEG, PNG. The maximum file size is 4 MByte. When you use a custom wallpaper, the clock and the list of upcoming meetings are removed from the main display.
Requires user role: ADMIN, USER
Default value: Auto
Value space: Auto/Custom/None
  Auto: Use the default wallpaper.
  None: There is no background image on the screen.
  Custom: Use the custom wallpaper as background image on the screen. If no custom wallpaper is uploaded to the system, the setting will revert to the default value.

UserInterface UserPreferences
Not applicable.
UserManagement settings

UserManagement LDAP Mode
The video system supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate user names and passwords. Use this setting to configure whether or not to use LDAP authentication. Our implementation is tested for the Microsoft Active Directory (AD) service.

Requires user role: ADMIN
Default value: Off
Value space: Off/On
- Off: LDAP authentication is not allowed.
- On: Use LDAP authentication.

UserManagement LDAP Server Address
Set the IP address or hostname of the LDAP server.

Requires user role: ADMIN
Default value: ""
Value space: String (0, 255)
- A valid IPv4 address, IPv6 address or hostname.

UserManagement LDAP Server Port
Set the port to connect to the LDAP server on. If set to 0, use the default for the selected protocol (see the UserManagement LDAP Encryption setting).

Requires user role: ADMIN
Default value: 0
Value space: Integer (0..65535)
- The LDAP server port number.

UserManagement LDAP Encryption
Define how to secure the communication between the video system and the LDAP server. You can override the port number by using the UserManagement LDAP Server Port setting.

Requires user role: ADMIN
Default value: LDAPS
Value space: LDAPS/None/STARTTLS
- LDAPS: Connect to the LDAP server on port 636 over TLS (Transport Layer Security).
- None: Connect to LDAP server on port 389 with no encryption.
- STARTTLS: Connect to LDAP server on port 389, then send STARTTLS to enable TLS encryption.

UserManagement LDAP MinimumTLSVersion
Set the lowest version of the TLS (Transport Layer Security) protocol that is allowed.

Requires user role: ADMIN
Default value: TLSv1.2
Value space: TLSv1.0/TLSv1.1/TLSv1.2
- TLSv1.0: Support TLS version 1.0 or higher.
- TLSv1.1: Support TLS version 1.1 or higher.
- TLSv1.2: Support TLS version 1.2 or higher.
UserManagement LDAP VerifyServerCertificate

When the video system connects to an LDAP server, the server will identify itself to the video system by presenting its certificate. Use this setting to determine whether or not the video system will verify the server certificate.

Requires user role: ADMIN
Default value: On

Value space: Off/On
   Off: The video system will not verify the LDAP server’s certificate.
   On: The video system must verify that the LDAP server’s certificate is signed by a trusted Certificate Authority (CA). The CA must be on the list of trusted CAs that are uploaded to the system in advance. Use the video system’s web interface to manage the list of trusted CAs (see more details in the administrator guide).

UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges. If set, this setting takes precedence over the UserManagement LDAP Admin Group setting.

Requires user role: ADMIN
Default value: "*

Value space: String (0, 1024)
   Refer to the LDAP specification for the syntax of this string. Example: ",(CN=adminuser)"

UserManagement LDAP Attribute

The attribute used to map to the provided username. If not set, sAMAccountName is used.

Requires user role: ADMIN
Default value: "*

Value space: String (0, 255)
   The attribute name.

UserManagement LDAP Admin Group

Members of this AD (Active Directory) group will be given administrator access. This setting is a shorthand for saying (memberOf:1.2.840.113556.1.4.1941:=<group name>). If UserManagement LDAP Admin Filter is set, this setting is ignored.

Requires user role: ADMIN
Default value: "*

Value space: String (0, 255)
   The distinguishing name of the AD group. Example: "CN=admin_group, OU=company groups, DC=company, DC=com"
Video settings

**Video ActiveSpeaker DefaultPIPPosition**

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

Requires user role: ADMIN
Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight
- Current: The position of the active speaker PiP will be kept unchanged when leaving a call.
- UpperLeft: The active speaker PiP will appear in the upper left corner of the screen.
- UpperCenter: The active speaker PiP will appear in the upper center position.
- UpperRight: The active speaker PiP will appear in the upper right corner of the screen.
- CenterLeft: The active speaker PiP will appear in the center left position.
- CentreRight: The active speaker PiP will appear in the center right position.
- LowerLeft: The active speaker PiP will appear in the lower left corner of the screen.
- LowerRight: The active speaker PiP will appear in the lower right corner of the screen.

**Video DefaultLayoutFamily Local**

Select which video layout family to use locally.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single>
- Auto: The default layout family, as given in the layout database provided by the system, will be used as the local layout.
- Equal: The Equal layout family will be used as the local layout. All videos have equal size, as long as there is space enough on the screen.
- Prominent: The Prominent layout family will be used as the local layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.
- Overlay: The Overlay layout family will be used as the local layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.
- Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.
Video DefaultLayoutFamily Remote
Select which video layout family to be used for the remote participants.

Requires user role: ADMIN
Default value: Auto

Value space: Auto/Equal/Prominent/Overlay/Single
- Auto: The default layout family, as given by the local layout database, will be used as the remote layout.
- Equal: The Equal layout family will be used as the remote layout. All videos have equal size, as long as there is space enough on the screen.
- Prominent: The Prominent layout family will be used as the remote layout. The active speaker, or the presentation if present, will be a large picture, while the other participants will be small pictures. Transitions between active speakers are voice switched.
- Overlay: The Overlay layout family will be used as the remote layout. The active speaker, or the presentation if present, will be shown in full screen, while the other participants will be small pictures-in-picture (PiP). Transitions between active speakers are voice switched.
- Single: The active speaker, or the presentation if present, will be shown in full screen. The other participants are not shown. Transitions between active speakers are voice switched.

Video Input Connector [1..2] CameraControl Mode
Define whether a camera can be controlled or not. This value is fixed for both Connector 1 (integrated camera) and Connector 2 (HDMI), and cannot be changed.

Requires user role: ADMIN
Default value: Off

Value space: Off
- Off: Disable camera control.

Video Input Connector [1..2] CameraControl CameraId
The camera ID is a unique identifier of the cameras that are connected to the video input.

Requires user role: ADMIN
Default value: 1

Value space: 1
- The camera ID is fixed and cannot be changed.

Video Input Connector [1..2] InputSourceType
Select which type of input source is connected to the video input.
Note that Connector 1 is the system’s integrated camera.

Requires user role: ADMIN
Default value: Connector 1: camera   Connector 2: desktop

Value space: Connector 1: camera   Connector 2: camera/desktop/document_camera/mediaplayer/PC/whiteboard/other
- camera: Use this when a camera is connected to the video input.
- desktop: Use this when the video system’s monitor is the main screen for the PC / laptop that is connected to this input. The Video Input Connector [n] PresentationSelection setting must then also be set to desktop.
- document_camera: Use this when a document camera is connected to the video input.
- mediaplayer: Use this when a media player is connected to the video input.
- PC: Use this when a computer is connected to the video input.
- whiteboard: Use this when a whiteboard camera is connected to the video input.
- other: Use this when the other options do not match.

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

Requires user role: ADMIN, USER
Default value: 1

Value space: 1
- Set the source to be used as the main video source.
Video Input Connector [1..2] Name

Define a name for the video input connector.

Requires user role: ADMIN
Default value: ""
Value space: String (0, 50)
   Name for the video input connector.

Video Input Connector [2] Quality

When encoding and transmitting video there is 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. This setting specifies whether to give priority to high frame rate or to high resolution.

Requires user role: ADMIN
Default value: Sharpness
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.

Video Input Connector [1..2] OptimalDefinition Profile

This setting will only take effect if the corresponding Video Input Connector [n] Quality setting is set to Motion.

The optimal definition profile reflects the lighting conditions in the video conferencing room and the quality of the camera. The better lighting conditions and the better quality of the camera, the higher the profile. In good lighting conditions, the video encoder will provide better quality (higher resolution or frame rate) for a given call rate. Generally, the Normal or Medium profiles are recommended. However, when the lighting conditions are very good, the High profile can be set in order to increase the resolution for a given call rate. The resolution must be supported by both the calling and called systems.

Requires user role: ADMIN
Default value: Medium
Value space: Normal/Medium/High
   Normal: Use this profile for a normally to poorly lit environment. Resolutions will be set rather conservative.
   Medium: Requires good and stable lighting conditions and a good quality video input. For some call rates this leads to higher resolution.
   High: Requires nearly optimal video conferencing lighting conditions and a good quality video input in order to achieve a good overall experience. Rather high resolutions will be used.
Video Input Connector [2] PresentationSelection

Define how the video system will behave when you connect a presentation source to the video input.

If the video system is in standby mode, it will wake up when you connect a presentation source. Sharing the presentation with the far end requires additional action (select Share on the user interface) except when this setting is set to AutoShare.

Requires user role: ADMIN
Default value: Desktop
Value space: AutoShare/Desktop/Manual/OnConnect

AutoShare: While in a call, the content on the video input will automatically be presented to the far end as well as on the local screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). You do not have to select Share on the user interface. If a presentation source is already connected when you make or answer a call, you have to manually select Share on the user interface.

Desktop: The content on the video input will be presented on the screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). This applies both when idle and in a call. Also, the content on the video input will stay on the screen when you leave the call, provided that it was the active input at the time of leaving.

Manual: The content on the video input will not be presented on the screen until you select Share from the user interface.

OnConnect: The content on the video input will be presented on screen when you connect the cable, or when the source is activated otherwise (for example when a connected computer wakes up from sleep mode). Otherwise, the behavior is the same as in manual mode.

Video Input Connector [2] RGBQuantizationRange

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

Requires user role: ADMIN
Default value: Auto
Value space: Auto/Full/Limited

Auto: RGB quantization range is automatically selected based on video format according to CEA-861-E. CE video formats will use limited quantization range levels. IT video formats will use full quantization range levels.

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

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

Video Input Connector [1..2] Visibility

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

Note that Connector 1 is the system’s integrated camera, which is not available as a presentation source.

The default value is IfSignal for Video Input Connector 2 Visibility (the HDMI connector).

Requires user role: ADMIN
Default value: Connector 1: Never Connector 2: Always Connector 3: OnConnect
Value space: Connector 1: Never Connector 2, 3: Never/Always/IfSignal

Never: When the input source is not expected to be used as a presentation source, set to Never.
Always: When set to Always, the menu selection for the video input connector will always be visible on the graphical user interface.
IfSignal: When set to IfSignal, the menu selection for the video input connector will only be visible when something is connected to the video input.
Video Layout DisableDisconnectedLocalOutputs

This setting is fixed to On.
Default value: On

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

Video Monitors

Define the monitor layout mode. Note that this video system supports only one monitor, so this value is fixed and cannot be changed.

Requires user role: ADMIN
Default value: Single

Value space: Single
Single: The layout is shown on the video system's monitor.

Video Output Connector [1] Brightness

Define the brightness level for the video system's integrated display.

Requires user role: ADMIN, USER
Default value: 80

Value space: Integer (0..100)
Range: The value must be between 0 and 100.

Video Output Connector [2] CEC Mode

The HDMI output (Output Connector 2) is for future use.

Video Output Connector [2] Location VerticalOffset

The HDMI output (Output Connector 2) is for future use.

Video Output Connector [2] OverscanLevel

The HDMI output (Output Connector 2) is for future use.

Video Output Connector [1..2] Resolution

Connector 1: The resolution and refresh rate for the integrated display. This value is fixed and cannot be changed.
Connector 2: The HDMI output (Output Connector 2) is for future use.
Default value: Connector 1: 1920_1080_60

Value space: Connector 1: 1920_1080_60
1920_1080_60: The resolution is 1920 x 1080, and the refresh rate is 60 Hz.

Video Output Connector [2] RGBQuantizationRange

The HDMI output (Output Connector 2) is for future use.

Video Output Connector [1] Whitebalance Level

The integrated display's color temperature (white balance) is adjustable from 4000 K (warm) to 9000 K (cool).

Requires user role: ADMIN, USER
Default value: 6500

Value space: Integer (4000..9000)
The color temperature in Kelvin.
Video Presentation DefaultPIPPosition

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

Requires user role: ADMIN
Default value: Current

Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight
  - Current: The position of the presentation PiP will be kept unchanged when leaving a call.
  - UpperLeft: The presentation PiP will appear in the upper left corner of the screen.
  - UpperCenter: The presentation PiP will appear in the upper center position.
  - UpperRight: The presentation PiP will appear in the upper right corner of the screen.
  - CenterLeft: The presentation PiP will appear in the center left position.
  - CenterRight: The presentation PiP will appear in the center right position.
  - LowerLeft: The presentation PiP will appear in the lower left corner of the screen.
  - LowerRight: The presentation PiP will appear in the lower right corner of the screen.

Video Selfview Default Mode

Define if the main video source (self-view) shall be displayed on screen after a call. The position and size of the self-view window is determined by the Video Selfview Default PIPPosition and the Video Selfview Default FullscreenMode settings respectively.

Requires user role: ADMIN
Default value: Current

Value space: Off/Current/On
  - Off: self-view is switched off when leaving a call.
  - Current: self-view is left as is, i.e. if it was on during the call, it remains on after the call; if it was off during the call, it remains off after the call.
  - On: self-view is switched on when leaving a call.

Video Selfview Default FullscreenMode

Define if the main video source (self-view) shall be shown in full screen or as a small picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting).

Requires user role: ADMIN
Default value: Current

Value space: Off/Current/On
  - Off: self-view will be shown as a PiP.
  - Current: The size of the self-view picture will be kept unchanged when leaving a call, i.e. if it was a PiP during the call, it remains a PiP after the call; if it was fullscreen during the call, it remains fullscreen after the call.
  - On: The self-view picture will be shown in fullscreen.

Video Selfview Default OnMonitorRole

Define which monitor to display the main video source (self-view) on after a call. Note that this video system has only one monitor, so this value is fixed and cannot be changed.

Requires user role: ADMIN
Default value: First

Value space: First
  - First: The self-view picture will be shown on the integrated screen.

Video Presentation DefaultSource

Define which video input source to use as a default presentation source. This setting may be used by the API and 3rd party user interfaces. It is not relevant when using the user interfaces provided by Cisco.

Requires user role: ADMIN, USER
Default value: 2

Value space: 2
  - The video input source to use as default presentation source.
Video Selfview Default PiPPosition

Define the position on screen of the small self-view picture-in-picture (PiP) after a call. The setting only takes effect when self-view is switched on (see the Video Selfview Default Mode setting) and fullscreen view is switched off (see the Video Selfview Default FullscreenMode setting).

Requires user role: ADMIN
Default value: Current
Value space: Current/UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight
  Current: The position of the self-view PiP will be kept unchanged when leaving a call.
  UpperLeft: The self-view PiP will appear in the upper left corner of the screen.
  UpperCenter: The self-view PiP will appear in the upper center position.
  UpperRight: The self-view PiP will appear in the upper right corner of the screen.
  CenterLeft: The self-view PiP will appear in the center left position.
  CentreRight: The self-view PiP will appear in the center right position.
  LowerLeft: The self-view PiP will appear in the lower left corner of the screen.
  LowerRight: The self-view PiP will appear in the lower right corner of the screen.

Video Selfview OnCall Mode

This setting is used to switch on self-view for a short while when setting up a call. The Video Selfview OnCall Duration setting determines for how long it remains on. This applies when self-view in general is switched off.

Requires user role: ADMIN
Default value: On
Value space: Off/On
  Off: self-view is not shown automatically during call setup.
  On: self-view is shown automatically during call setup.

Video Selfview OnCall Duration

This setting only has an effect when the Video Selfview OnCall Mode setting is switched on. In this case, the number of seconds set here determines for how long self-view is shown before it is automatically switched off.

Requires user role: ADMIN
Default value: 10
Value space: Integer (1..60)
  Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.
Experimental settings

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

The user interface and its use are described in full detail in the User guide for the video system.

Access the System Information and Settings menu, Restart the video system, activate and deactivate Standby and Do not disturb modes, adjust the brightness of the screen.

Indicates whether or not the Proximity feature is available.

System name or contact information

Tap Call to invoke the contacts including Favorites, Directory and Recents lists, and to open the Search or Dial field.

Tap Messages to invoke the voice mail system, if available.

On the right side of the unit:
- USB and mini-jack sockets for headset
- Microphone: mute/unmute
- Loudspeaker volume control
- Selfview: on/off
- Entry icon for in-room controls, if available (your system may have a different entry icon).
- Time of day
- Microphone mute indicator
- On the right side of the unit:
  - Microphone mute button
  - Loudspeaker volume controls
  - USB socket for headset
Set up remote monitoring

Requirement:
- RemoteMonitoring option

Remote monitoring is useful when you want to control the video system from another location.

Snapshots from input sources appear in the web interface, so you can check the camera view and control the camera without being in the room.

If enabled, snapshots are refreshed automatically approximately every 5 seconds.

Check whether or not the video system has the RemoteMonitoring option

1. Sign in to the web interface.
2. Check the Home page to see if RemoteMonitoring is on the list of installed options.
   - If not on the list, remote monitoring is not available.

Enable remote monitoring

Install the RemoteMonitoring option key. How to install option keys are described in the ➤ Add option keys chapter.

PLEASE BE AWARE THAT IF YOU ENABLE THE REMOTE MONITORING OPTION YOU MUST MAKE SURE THAT YOU COMPLY WITH LOCAL LAWS AND REGULATIONS WITH REGARD TO PRIVACY AND PROVIDE ADEQUATE NOTICE TO USERS OF THE SYSTEM THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS YOUR RESPONSIBILITY TO COMPLY WITH PRIVACY REGULATIONS WHEN USING THE SYSTEM AND CISCO DISCLAIMS ALL LIABILITY FOR ANY UNLAWFUL USE OF THIS FEATURE.

About snapshots

Local input sources

Snapshots of the local input sources of the video system appear on the Call Control page.

Snapshots appear both when the video system is idle, and when in a call.

Far end snapshots

When in call, you may also see snapshots from the far end camera. It does not matter whether or not the far end video system has the RemoteMonitoring option.

Far end snapshots are not displayed if the call is encrypted.
Access call information while using the web interface

Open the Call Information window
Click the Call state indicator to open the Call Information window manually.
As default, the Call Information window pops up automatically when the video system receives a call.

Switch incoming call notifications on or off
Click Ignore incoming call notices, to decide whether or not the Call Information window should pop up automatically when the video system receives a call.
When the check box is checked, the Call Information window will not open automatically.

Open the Call Control page
Click Open Call Control to go straight to the Call Control page.

About the call state indicator
The call state indicator shows whether the system is in a call or not. You may also be notified about incoming calls.
The call state indicator is available on all pages except the Call Control page.

Control the call(s)
Relevant control buttons appear in the Call Information window. Use the buttons to:
- Show call details
- Put the call on hold
- Answer the call
- Disconnect the call
Place a call using the web interface (page 1 of 2)

Sign in to the web interface and navigate to **Call Control**.

**Place a call**

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

1. Navigate the **Local**, **Directory** or **Recents** lists to find the correct entry; or enter one or more characters in the **Search or Dial** field*. Click the correct contact name.
2. Click **Call** in the contact card.

Alternatively, enter the complete URI or number in the **Search and Dial** field. Then click the **Call** button that appears next to the URI or number.

**Send DTMF tones**

Click to open a key pad that you can use if your application requires DTMF (dual-tone multi-frequency) signaling.

**Show/hide call details**

Click the information button to show details about the call. Click the button again to hide the information.

**Hold and resume a call**

Use the **Hold** button next to a participant’s name to put that participant on hold.

To resume the call, use the **Resume** button that is present when a participant is on hold.

**End a call**

If you want to terminate a call, click **Disconnect all** or the **End** button.
Place a call using the web interface (page 2 of 2)

Sign in to the web interface and navigate to Call Control.

Calling more than one

Calling more than one using a conference bridge (CUCM ad hoc conferencing) is not supported from the web interface, even if it is supported by the video system itself.

Adjust the volume

Mute the microphone

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

Click Microphone: Off to unmute.

Volume down

Volume up
Share content using the web interface

Sign in to the web interface and navigate to Call Control.

Share content

1. Click Start Presentation. Then the text changes to Stop Presentation.

Stop content sharing:
Click the Stop Presentation button that is present while sharing.

About content sharing
You can connect a presentation source, most often a PC, to the HDMI computer connector at the back of the video system.

While in a call you can share content with the other participant in the call (far end).

If you are not in a call, the content is shown locally.
Local layout control

Sign in to the web interface and navigate to Call Control.

Change the layout
Click Layout, and choose your preferred layout in the window that opens.

The set of layouts to choose from depends on the system configurations.

You may change the layout both when idle and in a call.

About layouts
The term layout is used to describe the various ways the video and presentation can appear on the screen. Different types of meetings may require different layouts.
Control a far end camera

Sign in to the web interface and navigate to Call Control.

Prerequisites

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

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

Control the remote participant’s camera

1. Click the camera icon to open the remote camera control window.

2. Use the left and right arrows to pan the camera; the up and down arrows to tilt it; and + and - to zoom in and out.

If you are not allowed to control the far end camera, the controls will not appear in the image.

If the call is encrypted, the far end snapshot behind the controls are not displayed.
Add in-room controls to the user interface

You can customize the user interface to allow control of peripherals in a meeting room, for example lights and blinds. This allows for the powerful combination of a control system’s functionality and the video system’s user-friendly user interface.

Consult the In-Room Control guide for full details about how to design an in-room control panel using the In-Room Control editor, and how to use the video system’s API to program the in-room controls. Go to:

► http://www.cisco.com/go/in-room-control-docs

Architecture

You need a Cisco video system with a touch interface, and a third-party control system, for example Crestron or AMX, with hardware drivers for the peripherals. It is the control system, not the video system, that controls the peripherals.

When you program the control system you must use the video system’s API (events and commands) in order to connect with the controls on the video system’s user interface.

An easy to use drag-and-drop editor, which you should use to compose the custom in-room control panel, comes free of charge with the video system’s software.

The In-Room Control editor

You can use the In-Room Control editor to compose your custom in-room control panels for the video system’s user interface.

Sign in’ to the web interface, and navigate to Integration > In-Room Control.

• Click Launch Editor to launch the editor directly from the video system’s web interface.

You can push a new in-room control panel to the video system, and see the result immediately on the Touch controller.

• Click Download Editor to download a stand-alone version that you can use to work offline.

* You need a user that holds the ROOMCONTROL or ADMIN user roles in order to access the In-Room Control editor and the API commands that you need when programming the control system.
Manage startup scripts

Sign in to the web interface, and navigate to Integration > Startup Scripts.

About startup scripts

A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure.

A few commands and configurations cannot be placed in a startup script, for example xCommand SystemUnit Boot. It is not possible to save a script that contains illegal commands and configurations.

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

List of startup scripts

You can create one or more startup scripts.

A green dot appears next to an active startup script; a red ring appears next to an inactive startup script.

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

Create a startup script

1. Click Create new...
2. Enter a name for the startup script in the title input field.
3. Enter the commands (xConfiguration or xCommand) in the command input area. Start each command on a new line.
4. Click Save.
5. Click On to activate the startup script.

If you want to use an existing script as a starting point for editing, select that script and click Copy.

Run a startup script immediately

1. Select the startup script from the list.
2. Click Run.

Both active and inactive startup scripts can be run immediately.

Activate or deactivate a startup script

1. Select the startup script from the list.
2. Click On to activate, or Off to deactivate a script.

Active startup scripts will run every time the video system starts up.

Delete a startup script

1. Select the startup script from the list.
2. Click Delete.
Access the video system’s XML files

Sign in to the web interface and navigate to Integration > Developer API.

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

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

Open an XML file

Click the file name to open the XML file.

About the API

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

Sign in to the web interface and navigate to Integration > Developer API.

Commands (xCommand) and configurations (xConfiguration) can be executed from the web interface. Syntax and semantics are explained in the API guide for the video system.

Execute API commands and configurations

1. Enter a command (xCommand or xConfiguration), or a sequence of commands, in the text area.
2. Click Execute to issue the command(s).

About the API

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

Use the micro USB connector for direct communication with the video system. You need a micro USB to USB cable. If the computer doesn’t auto-install a serial port driver, you need to install a serial port driver on the computer manually.

Use a terminal emulator (SSH client) to connect to the serial interface. For the most common computer types (PC, MAC) and operating systems, PuTTY or Tera Term will work.

The serial connection can be used without an IP-address, DNS, or a network.

Parameters:
• Baud rate: 115200 bps
• Data bits: 8
• Parity: None
• Stop bit: 1

Video system settings

Serial communication is enabled by default. Use the following configuration to change the behavior:

SerialPort > Mode

For security reasons, you are asked to sign in before using the serial interface. Use the following setting to change the behavior:

SerialPort > LoginRequired

Restart the video system when you have made changes to the serial port settings.

If your video system is provisioned by CUCM, the serial port settings should be configured from CUCM.
SOFTWARE COMPATIBILITY
• Collaboration Endpoint Software Version 8.2 or later

PRODUCT DELIVERED WITH:
• DX80 or DX70 system with integrated HD camera and microphone
• Network cable
• HDMI/USB cable (DX80 only)
• Power adapter and regional power cable

INTEGRATED HD CAMERA
• -5° to 70° from the display
• 63° horizontal field of view
• 38° vertical field of view
• Resolution: 1080p30
• F 2.2
• Instant focus based on face detection
• Privacy shutter

USER INTERFACE
• On-screen graphical user interface

LANGUAGE SUPPORT
(cependant, software version)
• Arabic, Catalan, Chinese—Simplified, Chinese—Traditional, Czech, Danish, Dutch, English, English—UK, Finnish, French, French—Canadian, German, Hebrew, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese—Brazilian, Russian, Spanish, Spanish—Latin, Swedish, Turkish

SYSTEM MANAGEMENT
• Total management through embedded SNMP, Telnet, SSH, XML, and SOAP
• Remote software upload using web server, HTTP, and HTTPS
• On-screen menu system

DIRECTORY SERVICES
• Support for local directories (Favorites)
• Corporate directory (through Cisco Unified Communications Manager and Cisco TelePresence Management Suite)
• Server directory supporting LDAP and H.350 (requires Cisco TelePresence Management Suite)
• Call history with received, placed and missed calls with date and time

POWER
• Rated: 60W maximum
• Low-power standby mode

OPERATING TEMPERATURE AND HUMIDITY
• Ambient temperature: 0°C to 40°C (32°F to 95°F)
• Relative humidity (RH): 10 to 90%

STORAGE AND TRANSPORT TEMPERATURE
• -20°C to 60°C (-4°F to 140°F) at RH 10-90% (noncondensing)

DX80 SYSTEM DIMENSIONS
• Width: 22.2 in. (56.5 cm)
• Height: 20.2 in. (51.2 cm)
• Depth: 3.5 in. (8.9 cm)
• Weight: 15.65 lb (7.1 kg)

DX70 SYSTEM DIMENSIONS
• Width: 13.91 in. (35.31 cm)
• Height: 14.84 in. (37.71 cm)
• Depth: 2.45 in. (6.23 cm)
• Weight: 7.5 lb (3.4 kg)

APPROVALS AND COMPLIANCE
• Directive 2014/35/EU (Low-Voltage Directive)
• Directive 2014/30/EU (EMC Directive) – Class A
• Directive 2011/65/EU (RoHS)
• Directive 2002/96/EC (WEEE)
• NRTL approved (Product Safety)
• FCC CFR 47 Part 15B (EMC) – Class B
• FCC Listed (Radio Equipment)

AIRTEC APPROVED
Please check Product Approval Status Database www.ciscofax.com for approval documents per country.

BANDWIDTH
• Up to 3Mbps

MINIMUM BANDWIDTH FOR RESOLUTION AND FRAME RATE
• 720p30 from 768kbps
• 1080p30 from 1472kbps

FIREWALL TRAVERSAL
• Cisco TelePresence Expressway technology

VIDEO STANDARDS
• H.263
• H.263+
• H.264
• AVC (H.264/MPEG-4 Part 10 Advanced Video Coding)

VIDEO INPUT
One HDMI video input. Supports formats up to maximum 1920 x 1080 @ 60 fps (HD1080p60), including:
• 640 x 480
• 720 x 480
• 800 x 600
• 1024 x 768
• 1280 x 720
• 1366 x 768
• 1920 x 1080

Extended Display Identification Data (EDID)

VIDEO OUTPUT
One HDMI output. (reserved for future use) Supports format:
• 1920 x 1080 @ 60fps (1080p60)

VESA Monitor Power Management
Extended Display Identification Data (EDID)

* HDMI version 1.3
Technical specification (page 2 of 2)

LIVE VIDEO RESOLUTIONS (ENCODE/DECODE)
Supports encode/decode video formats up to maximum 1920 × 1080@30 fps (HD1080p30), including:
• 176 × 144 @ 30 fps (QCIF) (decode only)
• 352 × 288 @ 30 fps (CIF)
• 512 × 288 @ 30 fps (w288p)
• 576 × 448 @ 30 fps (448p)
• 640 × 480 @ 30 fps (VGA)
• 704 × 576 @ 30 fps (4CIF)
• 768 × 448 @ 30 fps (w448p)
• 800 × 600 @ 30 fps (SVGA)
• 1024 × 576 @ 30 fps (w576p)
• 1024 × 768 @ 30 fps (XGA)
• 1280 × 720 @ 30 fps (HD720p)
• 1280 × 768 @ 30 fps (WXGA)
• 1440 × 900 @ 30 fps (WXGA+)
• 1680 × 1050 @ 30 fps (WSXGA+)
• 1920 × 1080 @ 30 fps (HD1080p)

AUDIO FEATURES
• Up to 48 kHz sampling rate
• High quality 20 kHz audio
• Acoustic echo cancellers
• Automatic gain control
• Automatic noise reduction
• Active lip synchronization

AUDIO STANDARDS
• 64 kbps AAC-LD
• OPUS
• G.722
• G.722.1
• G.711mu
• G.711a
• G.729AB

AUDIO INPUTS
• Internal microphone array
• One HDMI audio-in

AUDIO OUTPUTS
• One line out, mini-jack (DX70)
• One HDMI (digital main audio)

DUAL STREAM
• H.239 (H.323) dual stream
• BFCP (SIP) dual stream
• Support for resolutions up to 1080p (1920 x 1080)

MULTIPOINT SUPPORT
• Cisco ad-hoc conferencing (requires Cisco Unified Communications Manager, Cisco TelePresence Server and Cisco TelePresence Conductor)

PROTOCOLS
• SIP and H.323

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

IP NETWORK FEATURES
• DNS lookup for service configuration
• Differentiated Services (QoS)
• IP adaptive bandwidth management (including flow control)
• Auto-gatekeeper discovery
• Dynamic playout and lip-sync buffering
• H.245 dual-tone multifrequency (DTMF) tones in H.323
• Date and time support via NTP
• Packet loss based downspeeding
• URI dialing
• TCP/IP
• DHCP
• IEEE 802.1x network authentication
• IEEE 802.1q Virtual LAN
• IEEE 802.1p CoS and class of service
• Cisco ClearPath

IPV6 NETWORK SUPPORT
• Dual stack IPv4 and IPv6 for H.323 and SIP
• Dual stack IPv4 and IPv6 for DHCP, SSH, HTTP, HTTPS, DNS, DiffServ
• Support for static IP address assignment, stateless autoconfiguration and DHCPv6

SUPPORTED INFRASTRUCTURE
• Cisco Unified Communications Manager 8.6.2 and later
• Cisco TelePresence Video Communication Server (Cisco VCS)

SECURITY FEATURES
• Management using web interface (HTTPS/HTTP) and SSH
• Password protected IP administration
• Password protected administration menu
• Disable IP services
• Network settings protection

NETWORK INTERFACES
• Internal 2-port Cisco Ethernet switch (RJ-45) 10/100/1000BASE-T (only auto-negotiation)

OTHER INTERFACES
• Three USB ports
• One MicroSD card slot for future use
• One Micro USB port for maintenance

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.
December 2016
Supported RFCs

The RFC (Request for Comments) series contains technical and organizational documents about the Internet, including the technical specifications and policy documents produced by the Internet Engineering Task Force (IETF).

- RFC 2190 RTP Payload Format for H.263 Video Streams
- RFC 2460 Internet protocol, version 6 (IPv6) specification
- RFC 2617 Digest Authentication
- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 2976 The SIP INFO Method
- RFC 3016 RTP Payload Format for MPEG-4 Audio/Visual Streams
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3262 Reliability of Provisional Responses in SIP
- RFC 3263 Locating SIP Servers
- RFC 3264 An Offer/Answer Model with SDP
- RFC 3311 UPDATE method
- RFC 3361 DHCP Option for SIP Servers
- RFC 3388 Grouping of Media Lines in the Session Description Protocol (SDP)
- RFC 3420 Internet Media Type message/sipfrag
- RFC 3515 Refer method
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3551 RTP Profile for Audio and Video Conferences with Minimal Control
- RFC 3581 Symmetric Response Routing
- RFC 3605 RTCP attribute in SDP
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- RFC 3840 Indicating User Agent Capabilities in SIP
- RFC 3890 A Transport Independent Bandwidth Modifier for SDP
- RFC 3891 The SIP “Replaces” Header
- RFC 3892 Referred-By Mechanism
- RFC 3960 Early Media
- RFC 3986 Uniform Resource Identifier (URI); Generic Syntax
- RFC 4028 Session Timers in SIP
- RFC 4091 The Alternative Network Address Types (ANAT) Semantics for the Session Description Protocol (SDP) Grouping Framework
- RFC 4092 Usage of the Session Description Protocol (SDP) Alternative Network Address Types (ANAT) Semantics in the Session Initiation Protocol (SIP)
- RFC 4145 TCP-Based Media Transport in the SDP
- RFC 4235 An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)
- RFC 4566 SDP: Session Description Protocol
- RFC 4568 SDP: Security Descriptions for Media Streams
- RFC 4574 The Session Description Protocol (SDP) Label Attribute
- RFC 4582 The Binary Floor Control Protocol draft-ietf-bfcpcbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4583 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams draft-ietf-bfcpcbis-rfc4583bis-00 Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams
- RFC 4585 Extended RTP Profile for RTCP-Based Feedback
- RFC 4629 RTP Payload Format for ITU-T Rec. H.263 Video
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 4796 The SDP Content Attribute
- RFC 4862 IPv6 stateless address autoconfiguration
- RFC 5104 Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)
- RFC 5168 XML Schema for Media Control
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5389 Session Traversal Utilities for NAT (STUN)
- RFC 5577 RTP Payload Format for ITU-T Recommendation G.722.1
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5768 Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)
- RFC 6156 TRAP Using Relays around NAT (TURN): Extension for IPv6
- RFC 6184 RTP Payload Format for H.264 Video
- RFC 6550 IP QoS Control: A Framework for Controlling Quality of Service in the Internet
- RFC 7002 RTP Payload Format for ITU-T Rec. H.264 Video
User documentation on the Cisco web site

User documentation for the Cisco TelePresence products is available at ► http://www.cisco.com/go/telepresence/docs

Choose a product category in the right pane until you find the correct product. This is the path you have to follow:

Collaboration Desk Endpoints >       
  DX Series >                      
    DX Series

Alternatively, use the following short-link to find the documentation: ► http://www.cisco.com/go/dx-docs

The documents are organized in the following categories:

Install and Upgrade > Install and Upgrade Guides
  • Installation guides: How to install the product
  • Getting started guide: Initial configurations required to get the system up and running
  • RCSI guide: Regulatory compliance and safety information

Maintain and Operate > Maintain and Operate Guides
  • Administrator guide: Information required to administer your product
  • Deployment guide for TelePresence endpoints on CUCM: Tasks to perform to start using the video system with the Cisco Unified Communications Manager (CUCM)

Maintain and Operate > End-User Guides
  • User guides: How to use the product

Reference Guides > Command references
  • API reference guides: Reference guide for the Application Programmer Interface (API)

Software Downloads, Release and General Information > Licensing Information
  • Open source documentation: Licenses and notices for open source software used in this product

Software Downloads, Release and General Information > Release Notes
  • Software release notes
Cisco contacts

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

Go to: http://www.cisco.com/go/offices

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