Collaboration Endpoint software version 9.7
APRIL 2019

Administrator guide

for Cisco Webex DX70 and DX80

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
► https://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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

2

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

3

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Chapter 1

Introduction

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

4

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.

User documentation

This guide provides you with the information required to administrate the video system.

The guide primarilly addresses capabilities and configurations of on-premise registered video systems (CUCM, VCS), but a sub-set of the capabilities and configurations also applies to devices that are registered to our cloud service (Cisco Webex).

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

Documentation on the Cisco web site

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

- ► https://www.cisco.com/go/dx-docs

Documentation for cloud registered devices

For more information about devices that are registered to the Cisco Webex cloud service, visit:

- ► https://help.webex.com

Cisco Project Workplace

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

- ► https://www.cisco.com/go/projectworkplace

Software

Download software for the endpoint from the Cisco web site:

- ► https://software.cisco.com/download/home

We recommend reading the Software release notes (CE9):

- ► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

Converting to CE software

Until September 2016 DX80 and DX70 were shipped with *Android based software*. Before converting 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.

What's new in CE9

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 9 (CE9) compared to CE8.

The following products are new in CE9:

- CE9.0 – Room Kit
- CE9.1 – Codec Plus, and Room 55
- CE9.2 – Room 70
- CE9.4 – Codec Pro, Room 70 G2, and Room 55 Dual
- CE9.6 – Room Kit Mini

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

► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

New features and improvements in CE9.7

Connect to xAPI over a WebSocket

(All products)

You can now connect to the xAPI over WebSocket. The communication channel over WebSocket is open both ways until it is explicitly closed. This means that the server can send data to the client as soon as the new data is available, and there is no need for re-authentication for every request. This improves speed significantly compared to HTTP.

Each message contains a complete JSON document and nothing else. Many programming languages have good library support for WebSocket and JSON-RPC.

WebSocket is not enabled by default. Note that WebSocket is tied to HTTP and HTTP or HTTPS must be enabled before you can use WebSocket.

For more information, see ► xAPI over WebSocket guide.

Graphical sound mixer available on Audio Console

(Codec Pro, MX700, MX800, Room 70 G2, Room 70D G2, SX80)

The Audio Console now has a graphical sound mixer. It has 8 user-definable parametric equalizer settings. A setting consists of up to 6 sections, each of which has its own filter type, gain, center/crossover frequency and Q value. Each section is shown with its own color and the effect of altering any of the parameters immediately becomes visible in the graph.

For more information, see the *Customization guide* for CE9.7 at ► https://www.cisco.com/go/in-room-control-docs

Ambient noise reporting

(Codec Plus, Codec Pro, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit, Room Kit Mini)

The Room series devices can be configured to report the stationary ambient noise level in the room. The reported value is an A-weighted decibel value (dBA), which reflects the response of the human ear. Based on reported noise, facility management or a building manager can intervene to troubleshoot the issue.

All signal processing related to this feature is local and the only data transmitted is the calculated noise level.

Support for multiple SRG-120DH/PTZ-12 cameras *(Codec Plus)*

You can now connect up to three SRG-120DH/PTZ-12 cameras to a Codec Plus using an HDMI and an Ethernet switch.

Other updates

- 1080p support for Room Kit Mini when it is used as a USB camera. *(Room Kit Mini)*
- You can turn video off and on during calls. *(All products)*
- A system administrator can prevent the use of HTTP and only allow HTTPS Post and HTTPS Put requests. *(All products)*

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

6

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

New features and improvements in CE9.6

New product

- Cisco Webex Room Kit Mini

HDCP support

(Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)

The room device's second HDMI input (Connector 3) can be configured to support HDCP (High-bandwidth Digital Content Protection) protected content. This allows customers to re-purpose the screen by connecting devices such as a Google Chromecast, an Apple TV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the connector is configured to support HDCP, it is reserved for this type of content. This means that you cannot share any content from this specific connector while in a call, not even non-protected content from a laptop.

Remove default buttons from the user interface

(All products)

If you don't need all of the default buttons on the user interface, you can remove the ones that you don't need. This makes it possible to fully customize the user interface. The configuration only removes the buttons, not the functionality as such, and the custom In-Room Control panels can still be exposed.

For more information, see the *Customization guide* at
► https://www.cisco.com/go/in-room-control-docs

HTTP Post and Put requests *(All products)*

This feature makes it possible to send arbitrary HTTP(S) Post and Put requests from a device to an HTTP(S) server.

By using macros, you can send data to an HTTP(S) server whenever you want. You can choose what data to send, and structure them as you like. This way you can adapt the data to an already established service.

Security measures:

- The HTTP(S) Post/Put feature is disabled by default.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent Post and Put requests is limited.

Support for 3rd party USB controllers

(Codec Plus, Codec Pro, DX70, DX80, Room 55, Room 55 Dual, Room 70, Room 70 G2, Room Kit)

You can use a 3rd party USB input device to control certain functions on a room device. A Bluetooth remote control with a USB dongle and a USB keyboard are examples of such input devices. You can setup the desired features through macros.

This feature is meant to complement the functionality of the Touch 10 or the DX user interfaces. It is not meant to replace the Touch 10 and DX user interfaces.

For more information, see the *Customization guide* at
► https://www.cisco.com/go/in-room-control-docs

Content priority *(All products)*

You can now configure your device to prioritize bandwidth usage for either Main Video Channel or Presentation Channel.

```
xConfiguration Video Presentation Priority:
<Equal, High>
```

Equal is the default configuration and means 50 / 50 bandwidth division. Selecting "High" divides the bandwidth 25 / 75 in favor of the presentation channel.

Other updates *(All products)*

- You can start and control recording meetings from the device's user interface, provided that recording is supported by your infrastructure.
- Edit contact's information on Uls.
- SIP calls now display the SIP Session ID field in the logs to help identify calls.
- Ability to use ICE over MRA to locate the best path for media.

New features and improvements in CE9.5

Presentation source composition

(All products except SX10, DX70, DX80)

With using two or more content sources and sending them as one image, you can create a new experience for sharing in meetings.

This gives users more flexibility with what they present to remote sites. You can configure the presentation composition through in-room controls together with macros or an external controller.

The maximum number of different sources is determined by the device in use:

- *SX20, MX200 G2, MX300 G2, and Room Kit:* two sources
- *Codec Plus, Room 55, Room 55 Dual, and Room 70:* three sources
- *SX80, MX700, MX800, Codec Pro, and Room 70 G2:* four sources

You can only compose content that has been shared through a cable.

Audio Console on the web interface

(SX80, Codec Pro)

The new Audio Console is natively available on the web interface. The audio console gives you simplified tools to route audio from an input to an output. The Audio Console replaces the old java-based CE Console that is no longer maintained.

When you access the Audio Console for the first time you will see the default system audio routes. The Audio Console is controlled by an underlying macro, which is saved and started once you select Choose to overwrite the current device configurations.

For more information, see the *Customization guide* at
► https://www.cisco.com/go/in-room-control-docs

Classroom set-up

(SX80, MX700, MX800, Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)

The Classroom template uses macros to tailor a room set-up that works well for presenting and teaching scenarios. The template provides easy setup, management, and use of the room.

The Classroom set-up works similarly to the Briefing Room set-up (which is available for SX80, Codec Pro, MX700, MX800, and Room 70 G2), but it doesn't require three screens.

Support for Korean keyboard *(All products)*

Korean keyboard input is supported on Touch 10 when the user interface language is set to Korean.

Remote monitoring of screen status *(SX20, SX80)*

The remote monitoring of screen status that has been available for the Webex Room series and SX10, is now available for SX20 and SX80.

The codec can wake up the screen from standby mode, or put the screen to standby when the codec enters standby. The input source can also be changed automatically when a call is received.

CEC is disabled on the video system by default and must be enabled in the Video Output Connector [n] CEC Mode setting. Your screen must support CEC for remote monitoring to work.

Welcome banner *(All products)*

You can set up a welcome banner that users see after they sign in to the video system's web interface or command line interface. The banner can for example contain information you need in order to get started, or things you must be aware of when setting up the system.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

8

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

New features and improvements in CE9.4

New products

- Cisco Webex Codec Pro
- Cisco Webex Room 55 Dual
- Cisco Webex Room 70 G2

Rebranding from Cisco Spark to Cisco Webex

(All products)

Cisco Spark has changed its name to Cisco Webex, and the user interface elements that displayed *Spark* are changed to *Webex*. In the activation flow you now see Cisco Webex as a registration option instead of Cisco Spark.

The following products have gotten new names:

- Cisco Spark Room Kit is now Cisco Webex Room Kit
- Cisco Spark Room Kit Plus is now Cisco Webex Room Kit Plus
- Cisco Spark Codec Plus is now Cisco Webex Codec Plus
- Cisco Spark Quad Camera is now Cisco Quad Camera
- Cisco Spark Room 55 are now Cisco Webex Room 55
- Cisco Spark Room 70 are now Cisco Webex Room 70
- Cisco DX70 is now Cisco Webex DX70
- Cisco DX80 is now Cisco Webex DX80

The maximum number of Proximity clients is increased

(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)

A Cisco Webex Room Series device can have up to 30 paired clients simultaneously when the Proximity service *ContentShare ToClients* is disabled. If *ContentShare ToClients* is enabled, the limit of paired clients is 7 which is the same as in earlier software versions.

Support for content sharing using H.263 in a call between Cisco Webex Room Series and legacy MXP devices

(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)

Support for H.263 content sharing between MXP and Cisco Webex Room Series is now available. The Room Series previously had a limitation where it could not receive or share content in a separate content channel. Sharing content from a Room Series device to an MXP device would in earlier versions compose the presentation into the main video stream.

This is only supported in certain scenarios:

- Direct H.323 calls (IP dialing) between a Room Series device and an MXP device.
- MXP registered on VCS on H.323 and a Room Series device registered to the same VCS on either SIP or H.323. Note that making an H.323 to SIP call on a VCS requires that an interworking option key is installed on the VCS.

See the CE9 release notes for information on other limitations related to this feature.

CUCM provisioning of the admin settings lockdown configuration *(All products)*

The admin settings lockdown configuration, that was introduced in CE9.2.1, can now be provisioned from CUCM. You can lock a selection of the settings on the settings menu on all of your devices simultaneously when you configure them through CUCM.

Your CUCM may require a new device package in order to expose the new fields for this configuration.

Enable backlight compensation from the user interface *(DX70, DX80)*

A new setting on the DX70 and DX80 main menu enables and disables backlight compensation. This is a fixed setting that increases (on) or decreases (off) the sensors brightness levels in order to compensate for sunlight or other bright light sources behind the user. The backlight compensation sets the sensor to a fixed level and it is not auto adjusted to the backlight.

Changed default HTTP mode from HTTP+HTTPS to HTTPS *(All products)*

The default value of *NetworkServices HTTP Mode* is changed from HTTP+HTTPS to HTTPS. This is to increase the security of the room devices on default configuration. Upgrading from earlier software versions will not automatically change the default value and it will stay on HTTP+HTTPS to avoid breaking current HTTP implementations.

The change is seen on new systems running CE9.4.0 or later, or if the device is factory reset on CE9.4.0. The HTTP requests are redirect to HTTPS and on the first visit to the device's web interface, the device displays an "Insecure connection warning". To proceed to the web interface, you need to create an exception in your browser. This is a one-time operation unless you access the web interface with a different browser that has never visited the device web interface or if the device is factory reset.

In-Room Control update *(All products)*

You can add buttons for as many panels as you want on the home screen as well as on the in-call screen of the user interface.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

9

New features and improvements in CE9.3

Backup and restore settings and custom elements *(All products)*

You can include custom elements as well as configurations in a backup file bundle (zip). You can choose which of the following elements to include in the bundle:

- Branding images
- Macros
- Favorites
- Sign-in banner
- In-room control panels
- Configurations (all or a sub-set)

In previous software versions, you could only backup the configurations.

The backup file can either be restored manually from the video system's web interface, or you can generalize the backup bundle so that it can be provisioned across multiple video systems, for example using Cisco UCM or TMS.

You will find the backup and restore functionality under *Maintenance > Backup and Restore* on the video system's web interface.

Provisioning of custom elements *(All products)*

The backup bundle, as described above, can be provisioned to many video systems using Cisco UCM or TMS. It is important that device specific information is removed when creating a backup bundle intended for multiple video systems. If you include device specific information in such a bundle, you may end up with multiple video systems that cannot be reached.

By provisioning a non-system specific backup bundle, you can for example, copy a video system's setup with macros, branding elements, and in-room control panels across multiple video systems.

Currently, provisioning via Cisco UCM will not restore any configurations, only the other custom elements; TMS will restore everything that is included in the backup bundle.

See the release note for more details about provisioning.

In-Room Control updates *(All products)*

The following functionality is added to the in-room control feature:

- You can add buttons for up to 20 panels in total. The buttons appear on the home screen or the in-call screen of the user interface depending on the panel type.
- As before, there are three types of in-room control panels: global panels (always available), in-call panels (available only when in call), and out-of-call panels (only available when not in a call). The entry point for the global panel has been removed from the status bar (top right corner of the user interface). Buttons to open global panels are added to both the home screen and the in-call screen instead, together with the buttons for the out-of-call only and in-call only panels, respectively.
- You can make standalone trigger-buttons, which are buttons that trigger an event directly, without opening a panel on the user interface.

Also the following features are added in the in-room control editor:

- Some new icons are available.
- A set of colors to choose from for the in-room-control buttons.
- Double click text elements to edit text directly.
- Drag and drop in-room control XML files into the editor.

For a full description of in-room controls, see the *Customization guide* at
► https://www.cisco.com/go/in-room-control-docs

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

10

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Support for ISDN Link *(All products)*

ISDN Link with software version IL1.1.7 is supported for all video systems that supports CE9.3.0.

As before, when using automatic pairing (which allows the ISDN Link to be automatically discovered by the video system) IPv6 must be enabled on the video system.

One Button to Push snooze *(All products)*

You are able to snooze an One Button to Push (OBTP) meeting reminder for 5 minutes. The snooze time cannot be changed. The reminder typically appears if you are in a call and a scheduled meeting is about to start. You can snooze the reminder for 5 minutes each time it appears until the meeting has ended.

Adjust the call rate before making a call

(All products)

As soon as you start typing in the *Search or dial* field, you can open a dialog and select a custom call rate. In earlier releases this was available only when selecting an entry from the Directory.

If you don't select a custom call rate, you get the rate set in the *Conference DefaultCall Rate* setting.

Select ring-tone and adjust ring-tone volume

(All products)

You can select a ring-tone and adjust the ring-tone volume from the settings menu on the user interface. In the previous releases this was done from the web interface.

Resume a postponed upgrade *(All products)*

When you get a notification about software upgrade, you can choose *Upgrade now* or *Postpone.* If you postpone the upgrade, you can resume the upgrade from the *Settings > About this device* menu on the user interface when you are ready; you don't have to wait for 6 hours like you had to before.

If you don't manually resume the upgrade, the upgrade will start automatically after 6 hours.

Prevent system information from being exposed in the user interface *(All products)*

You can prevent important system information from being exposed in the user interface, for example:

- IP addresses (video system, touch controller, UCM/VCS registrar)
- MAC address
- Serial number
- Software version

To enable this feature the following must be done:

- A passphrase must be set for all users with administrator rights
- *UserInterface SettingsMenu Mode* must be set to Locked
- *UserInterface Security Mode* must be set to Strong

This feature also means that the IP address is not displayed on the screen when you disconnect a Touch controller.

Mirrored self-view *(DX70, DX80)*

You can configure the video system to show the self-view image the way other people see you, or as you would see yourself in a mirror. Use the *Video Selfview Mirrored* setting. Mirrored self-view used to be available only for Cisco DX devices running Android software.

Mirroring only applies to the self-view image, and has no effect on the video that is sent to the far end.

Accessibility: Flashing screen on incoming calls

(All products)

You can configure the video system so that the screen and Touch controller flashes red / light grey when the system receives an incoming call. This feature is mainly targeting hearing impaired users, making it easier for them to notice an incoming call.

The feature is disabled by default, and must be enabled by the *Accessibility IncomingCallNotification* setting.

Screen status monitoring and control *(SX10)*

SX10 now has the same CEC (Consumer Electronics Control) behavior as the video systems in the Room series.

The video system will use CEC to set the screen in standby when the system itself enters standby, and wake up the screen and select the correct video input when the video system itself wakes up from standby. CEC information from the screen is included in the video system's status. Of course, the screen must also support CEC and send the relevant information to the video system.

CEC is disabled on the video system by default, and must be enabled in the *Video Output Connector [1] CEC Mode* setting.

One common API guide *(All products)*

We have gathered all API information in **one** API guide, that covers all products. This is in contrast to earlier releases were we have had one API guide per product.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

11

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

New features and improvements in CE9.2

New product

- Cisco Webex Room 70 (formerly Cisco Spark Room 70)

Macro framework *(All products except SX10)*

The macro framework allows users and integrators to write JavaScript macros in order to automate scenarios and customize endpoint behavior so that it suites an individual customer's requirements.

The combination of macros and powerful features such as listening for events/status changes, automating execution of commands and configurations, and providing local control functionality for the In-Room control feature, provides many possibilities for custom setups.

Minor behavioral changes, such as having the video system in Do Not Disturb for an infinite amount of time, can be easily realized by macros. Some other examples are: Reset configurations automatically, make a call at a certain time of the day, and issue alert or help messages depending on status changes.

The macro editor, which also provides several example macros, is available from the video system's web interface.

HDCP support *(Room 55)*

The video system's second HDMI input (Connector 3) can be configured to support HDCP (High-bandwidth Digital Content Protection) protected content. This allows customers to re-purpose the video system's screen by connecting devices such as a Google ChromeCast, an AppleTV, or an HDTV decoder. This type of content cannot be shared while in a call.

When the connector is configured to support HDCP, it is reserved for this type of content. This means that you cannot share any content from this specific connector while in a call, not even non-protected content from a laptop.

Branding and halfwake customization

(All products except SX10)

You can upload your own text and images to customize the appearance of the screen and user interface in both the halfwake state and the awake state.

In the *Halfwake* state you can:

- Add a background brand image to the screen and user interface.
- Add a small logo in the bottom right corner of the screen and user interface.

In the *Awake* state you can:

- Add a small logo in the bottom right corner of the screen and user interface.
- Add a label or message in the bottom left corner of the screen (not the user interface).

Source composition *(All products except SX10, DX70, DX80)*

You can compose up to four input sources (depending on how many input sources are available on the codec) into one image. This is the image that will be sent in the main video stream to the far end in a call. Source composition can only be enabled via the API, so we recommend creating a user interface extension combined with a macro to control the compositions on demand.

This feature replaces some of the functionality that was provided by the TC Console application for TC software.

HTTP Proxy support *(All products)*

You can set up the video system to go through a HTTP Proxy when registering it to Cisco's cloud service, Cisco Spark.

User interface features *(All products)*

- The Settings panel is restructured.
- The Settings panel in the user interface can be protected by the video system's admin password. If the password is blank, anyone can access the Settings and factory reset the system.
- If you select the Russian language on the user interface, you can choose between a Russian keyboard and a keyboard with a Latin character set.
- Arabic and Hebrew languages are added to the user interface. Also localized keyboards are included.
- Basic IEEE 802.1x settings are added to the Settings panel in the user interface.

Cisco TelePresence Precision 60 Camera support *(Codec Plus, Room 70)*

You can connect Cisco TelePresence Precision 60 cameras to Codec Plus. Note that you need a switch for the camera control cables if you have more than one camera. The People Count feature is not supported if Precision 60 is the only camera type connected to the codec.

Cisco Spark Quad Camera support *(SX80)*

You can connect a Cisco Spark Quad Camera to the SX80. Note that the Quad Camera uses only one of the codec's HDMI inputs, while the SpeakerTrack 60 camera uses two. The People Count feature (in call) is also available when using the Quad Camera.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

12

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Support for the Snap to Whiteboard feature

(SX80, MX700, MX800, Codec Plus, Room Kit, Room 55, Room 70)

The Snap to Whiteboard feature is now available for all products that have a camera with speaker track functionality: SX80 with Cisco TelePresence Speaker Track 60 camera or Cisco Spark Quad Camera, MX700/MX800 with dual camera, Room Kit, Room Kit Plus, Room 55 and Room 70.

When the video system detects a person that is speaking close to the whiteboard, the camera view will switch to the whiteboard area. The wizard in the Settings panel on the Touch 10 user interface helps you to set up the feature and define where the whiteboard area is.

Briefing Room mode *(SX80, MX700, MX800)*

The Briefing Room feature, which was introduced already in TC software, has been reworked. The in-room control framework is used for creating the associated user interface elements.

For MX700 and MX800, Briefing Room is supported only for dual camera systems. Also, you need a Precision 60 camera, and a total of three screens.

For SX80, Briefing Room is supported when a speaker track camera, a Precision 60 camera, and three screens are connected. The speaker track camera can be either Cisco TelePresence SpeakerTrack 60 or Cisco Spark Quad Camera.

USB to Serial port support

(Codec Plus, Room Kit, Room 55, Room 70)

You can connect a USB (Type A) to serial (D-sub 9) adapter to access the video systems API. Cisco recommends the UC232R-10 USB to RS232 (FTDI) adapter.

Mute and unmute remote participants in a CMS hosted conference - Active Control *(All products)*

When a video system is enabled for Active Control in a CMS (2.1 or later) conference you can mute and unmute remote participants from the participant list on the user interface (the feature must also be enabled on the CMS).

A video system that is running software version CE9.2 will not be unmuted directly. When you try to unmute such a video system remotely, a message will show up on its screen requesting the user to unmute the audio locally.

API commands for Custom input prompt

(All products)

API commands are introduced to allow for an input prompt in the user interface: xCommand UserInterface Message TextInput *. When issuing the display command a prompt with your custom text, a text input field for the user, and a submit button, shows up on the user interface. For example, you can prompt a user to leave feedback after an ended call. You can specify what type of input you want from the user: single line text, numeric, password, or PIN code.

The prompt can only be enabled via the API, so it is recommended to combine it with macros and either a custom user interface panel or an auto-triggered event.

Certificate upload via API *(All products)*

ASCII PEM formatted certificates can be installed directly using multiline API commands (xCommand Security Certificates CA Add, or xCommand Security Certificates Services Add). You can also upload certificates to a video system from its web interface, as before.

API commands for user management *(All products)*

You can create and manage user accounts directly using API commands (xCommand UserManagement User *). As before, you can also do this from the video system's user interface.

Preview mode for In-Room Controls *(All products)*

The In-Room Control editor has a new preview mode. A virtual touch interface shows how the design looks. The user interface is interactive so that you can test the functionality. It produces real events on the video system, which can trigger any functionality you have created with a third-party control system. A console in the right pane displays both the widget values when interacted with, and control system feedback messages.

Intelligent Proximity changes *(All products)*

A Proximity indicator is displayed on the screen (middle right) to inform that one or more clients are paired to the system with Cisco Proximity. The old indicator (top left), which was always shown when Proximity was enabled, has been removed.

You can no longer disable the Proximity services from the user interface.

The ultrasound settings have moved from Peripherals Pairing Ultrasound to Audio Ultrasound.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

13

Automatic factory reset when changing the call service – device activation *(All products)*

The video system will automatically factory reset and restart when using the user interface to change the device activation method, for example from VCS to Cisco UCM. This will prevent conflicting configurations when provisioning the video system to a new service.

Changing the provisioning from the API will not automatically factory reset the video system.

Support for separate RTP port ranges for audio and other media *(All products)*

You can configure the video system so that audio uses a different RTP port range than other media. The two ranges cannot overlap. As default, all media use the same RTP port range.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

14

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

New features and improvements in CE9.1

New products

· Cisco Webex Codec Plus (formerly Cisco Spark Codec Plus)

· Cisco Webex Room 55 (formerly Cisco Spark Room 55)

Dual Screen experience and Active Control for CMS based meetings

(SX80, MX700, MX800, Codec Plus, Room Kit, Room 55)

Dual screen video systems can utilize both screens for video in a CMS based meeting. The video system receives two transcoded video streams and one content stream from the CMS, and utilizes both screens to render the streams.

With Active Control enabled, you get a participant list that shows all meeting participants and their current activity status, such as mute, sharing and active speaker indication. You can change the layout seamlessly from the touch interface by using the layout selection panels.

New wake-up experience *(All products)*

SX10, DX70, DX80: The wake-up experience has an additional standby state: *Halfwake*. In *Halfwake* state, the video system shows a simple on-screen interaction guide when it is not in use.

Other products: The wake-up experience has two additional standby states: *Halfwake* and *Standby with motion detection*. When automatic wake-up is enabled, the video system detects presence using ultrasound (motion detection) or when pairing to a Cisco Proximity client. The video system wakes up with a greeting before going into the *Halfwake* state, which has a simple on-screen interaction guide.

Bluetooth headset support *(DX70, DX80)*

A Bluetooth headset can be used with the video system. The headset must support HFP (Hands Free Protocol). The user can enable Bluetooth and set the video system in Bluetooth pairing mode from the user interface.

Support for the EAP authentication framework for wireless networks

(DX70, DX80, Codec Plus, Room Kit, Room 55)

In addition to WPA-PSK and WPA2-PSK, the video system now supports the WPA-EAP authentication framework for Wi-Fi connections. In total the following methods are supported:

· Open
· WPA-PSK (AES)
· WPA2-PSK (AES)
· EAP-TLS
· EAP-TTLS
· EAP-FAST
· PEAP
· EAP-MSCHAPv2
· EAP-GTC

Additions for Room Analytics

(All products except SX10, DX70, DX80)

Detect people presence in the room: The video system has the capability to find whether there are people present in the room. The feature is based on ultrasound, and it does not keep record of who was in the room, only whether or not the room is in use.

People count (only for Room Kit, Codec Plus, Room 55)**:** The video system counts the number of people in the room when in a call, and when displaying the self-view picture. You can configure the video system to also count the number of people outside of call, but the video system cannot count the number of people when it is in standby. It does not keep record of who was in the room, only the number of faces that were detected.

Network port 2 can be disabled *(DX70, DX80)*

You can connect a computer to the network through the video system's second network port. Then you only need one network wall socket to support both the video system and the computer.

For security reasons, we recommend that you disable this network port if the video system is used in a public environment. This way, you prevent someone from connecting a computer to your network through the video system.

New features and improvements in CE9.0

New product

- Cisco Webex Room Kit (formerly Cisco Spark Room Kit)

Updated user interface *(All products)*

The user interfaces on the Touch 10, on screen, and on integrated touch screens have been updated. The main menu items on the home screen have been replaced with more prominent activities.

Some of the settings have been removed from the Touch 10 advanced settings menu to align with the on-screen display menu.

Wakeup on motion detection *(All products)*

Wakeup on motion detection senses when a person walks into the conference room and the video system wakes up automatically. You need to enable the following setting for this feature to work:

xConfiguration Standby WakeupOnMotionDetection

You can't manually set the video system in standby when this feature is enabled.

Updated In-Room Control editor *(All products)*

The In-Room Control editor is updated with a new look, improved logic and usability for producing a control interface more efficiently. In addition, a new directional pad widget and an In-Room Control simulator is added.

Added language support *(All products)*

We have added support for Potuguese (Portugal) to the on-screen display and Touch controller menus.

Other changes *(All products)*

- Support for HTTPS client certificates has been added.
- Unplugging the presentation cable stops the presentation sharing instantly.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

16

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

System configuration changes in CE9.7

New configurations

HttpClient AllowHTTP *(All products)*

Logging Debug Wifi *(Codec Plus, Codec Pro, DX70, DX80, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

Logging Internal Mode *(All products)*

NetworkServices Websocket *(All products)*

Phonebook Server [1] Pagination *(All products)*

RoomAnalytics AmbientNoiseEstimation Mode *(Codec Plus, Codec Pro, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2)*

UserInterface Features Call VideoMute *(Codec Plus, Codec Pro, MX200 G2, MX300 G2, MX700, MX800, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, SX10, SX20, SX80)*

UserInterface Features Whiteboard Start *(DX70, DX80)*

UserInterface Phonebook Mode *(All products)*

UserInterface SettingsMenu Visibility *(All products)*

UserInterface UsbPromotion *(Room Kit Mini)*

Configurations that are modified

Audio Input Line [1..4] VideoAssociation VideoInputSource *(MX700, MX800, SX80)*

　　OLD: 1/2/3/4/5

　　NEW: 1/2/3/4

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(Codec Pro, Room 70 G2)*

　　OLD: 1/2/3/4/5

　　NEW: 1/2/3/4/5/6

Audio Input Microphone [1..8] VideoAssociation VideoInputSource *(MX700, MX800, SX80)*

　　OLD: 1/2/3/4/5

　　NEW: 1/2/3/4

CallHistory Mode *(All products)*

　　OLD: Public: False

　　NEW: Public: True

Conference Multipoint Mode *(Codec Pro, Codec Plus, MX200 G2, MX300 G2, MX700, MX800, Room Kit, Room Kit Mini, Room 55, Room 55D, Room 70, Room 70 G2, SX20, SX80)*

　　OLD: Public: False

　　NEW: Public: True

Logging External Mode *(All products)*

　　OLD: Public: False

　　NEW: Public: True

Logging External Protocol *(All products)*

　　OLD: Public: False

　　NEW: Public: True

Logging External Server Address *(All products)*

　　OLD: Public: False

　　NEW: Public: True

Logging External Server Port *(All products)*

　　OLD: Public: False

　　NEW: Public: True

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

17

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

SIP ANAT *(All products)*

OLD: Public: False

NEW: Public: True

Video Input Connector [6] CameraControl Mode *(Codec Pro, Room 70 G2)*

OLD: Default: On

NEW: Default: Off

OLD: On

NEW: On/Off

Video Presentation Priority *(All products)*

OLD: Public: False

NEW: Public: True

OLD: Equal/High

NEW: Equal/High/Low

Configurations that are removed

RoomAnalytics PeopleCountOutOfCall *(MX700, MX800)*

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

18

System configuration changes in CE9.6

New configurations

Audio Input Microphone [1..8] Channel *(Codec Pro, Room 70 G2)*

Audio Input HDMI [n] Level *(Codec Plus, Room 55, Room 70 G2, Room Kit)*

Audio Input HDMI [n] Mode *(Room 70 G2, Room Kit)*

Audio Input HDMI [2..5] VideoAssociation MuteOnInactiveVideo *(Room 70 G2)*

Audio Microphones PhantomPower *(Codec Plus, MX200 G2, MX300 G2, Room 55, Room Kit, SX20)*

Audio Output ConnectorSetup *(Codec Pro, Room 70 G2)*

Audio Output HDMI [n] Level *(MX700, MX800)*

Audio Output HDMI [n] Mode *(Codec Plus, MX700, MX800)*

Audio Output InternalSpeaker Mode *(MX700, MX800, Room 55 Dual, Room 70)*

Audio Output Line [1..6] Equalizer ID *(Room 70 G2)*

Audio Output Line [1..6] Equalizer Mode *(Room 70 G2)*

HttpClient AllowInsecureHTTPS *(All products)*

HttpClient Mode *(All products)*

NetworkServices NTP Server [1..3] Key *(All products)*

NetworkServices NTP Server [1..3] KeyId *(All products)*

NetworkServices NTP Server [1..3] KeyAlgorithm *(All products)*

Peripherals InputDevice Mode *(DX70, DX80)*

UserInterface Branding AwakeBranding Colors *(All products)*

UserInterface Features Call End *(All products)*

UserInterface Features Call MidCallControls *(All products)*

UserInterface Features Call Start *(All products)*

UserInterface Features HideAll *(All products)*

UserInterface Features Share Start *(All products)*

Video Input Connector [n] HDCP Mode *(Codec Plus, Codec Pro, Room 55 Dual, Room 70, Room 70 G2)*

Video Output Connector [2] CEC Mode *(Room 70 Single)*

Video Presentation Priority *(All products)*

Configurations that are modified

Audio Output ARC [1] Mode *(Codec Pro, Room 70 G2)*

> OLD: Default: Auto
> NEW: Default: On
> OLD: Value space: Off / On / Auto
> NEW: Value space: Off / On

Audio Output HDMI [1..3] Mode *(Codec Pro, Room 70 G2)*

> OLD: Default: Auto *(Codec Pro)*
> NEW: Default: On *(Codec Pro)*
> OLD: Default, HDMI [2..3]: Auto *(Room 70G2 Single)*
> NEW: Default, HDMI [2..3]: Off *(Room 70G2 Single)*
> OLD: Default, HDMI [3]: Auto *(Room 70G2 Dual)*
> NEW: Default, HDMI [3]: Off *(Room 70G2 Dual)*
> OLD: Value space: Off / On / Auto *(Codec Pro, Room 70 G2)*
> NEW: Value space: Off / On *(Codec Pro, Room 70 G2)*

Audio Output InternalSpeaker Mode *(Room 55, Room 70 G2, Room Kit)*

> OLD: Default: Auto *(Room 70 G2)*
> NEW: Default: On *(Room 70 G2)*
> OLD: Value space: Off / On / Auto *(Room 70 G2)*
> NEW: Value space: Off / On / UltrasoundOnly *(Room 70 G2)*
> OLD: Value space: Off / On *(Room 55, Room Kit)*
> NEW: Value space: Off / On / UltrasoundOnly *(Room 55, Room Kit)*

Audio Ultrasound MaxVolume *(SX20)*

> OLD: Default: 70
> NEW: Default: 60

Provisioning Mode *(All products)*

> OLD: Value space: Auto / CUCM / Edge / Off / TMS / VCS / Spark
> NEW: Value space: Auto / CUCM / Edge / Off / TMS / VCS / Webex

Provisioning Mode *(Room 55 Dual)*

> OLD: Default: Off
> NEW: Default: On

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

19

Standby WakeupOnMotionDetection *(Room 55 Dual)*

    OLD: Default: Off

    NEW: Default: On

Configurations that are removed

Conference MultiStream Mode *(MX200 G2, MX300 G2, SX20)*

SIP PreferredIPMedia *(All products)*

System configuration changes in CE9.5

New configurations

Audio Input ARC [n] Mode *(Codec Pro, Room 70 G2)*

Audio Output ARC [1] Delay DelayMs *(Codec Pro, Room 70 G2)*

Audio Output ARC [1] Delay Mode *(Codec Pro, Room 70 G2)*

Audio Output ARC [1] Mode *(Codec Pro, Room 70 G2)*

Audio Output InternalSpeaker Mode *(Room 70 G2)*

Audio Output Line [1] Mode *(Codec Plus, Room 55)*

Audio Output Line [1] OutputType *(Codec Plus, Room 55*

NetworkServices SSH HostKeyAlgorithm *(All products)*

Peripherals InputDevice Mode *(Codec Plus, Codec Pro, Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2)*

RoomAnalytics PeopleCountOutOfCall *(SX80)*

Configurations that are removed

Audio Output InternalSpeaker Mode *(Codec Pro)*

Cameras SpeakerTrack ConnectorDetection CameraLeft *(Room 70 G2)*

Cameras SpeakerTrack ConnectorDetection CameraRight *(Room 70 G2)*

Cameras SpeakerTrack ConnectorDetection Mode *(Room 70 G2)*

Cameras SpeakerTrack TrackingMode *(Room 70 G2)*

Provisioning RoomType ClassroomEnabled *(SX80, MX700, MX800, Codec Pro, Room 70 G2)*

Configurations that are modified

Audio Input Microphone[1..8] Equalizer ID *(Codec Pro, Room 70 G2)*

    OLD: Value space: Integer (1..14)

    NEW: Value space: Integer (1..8)

Audio Ultrasound MaxVolume *(SX80, MX700, MX800, Codec Pro, Room 70 G2)*

    OLD: Default value: 70 *(SX80, Codec Pro, MX700, MX800, Room 70 G2)*

    NEW: Default value: 60 *(SX80, Codec Pro, Room 70 G2)*

    NEW: Default value: 66 *(MX700, MX800)*

    OLD: Value space: Integer (0..90) *(Room 70 G2)*

    NEW: Value space: Integer (0..80) *(Room 70 G2)*

Cameras PresenterTrack Connector *(Codec Plus, Codec Pro, Room 70, Room 70 G2)*

    OLD: Default value: 1 *(Codec Pro, Room 70 G2)*

    NEW: Default value: 6 *(Codec Pro, Room 70 G2)*

    OLD: Value space: Integer (1..5) *(Codec Plus, Codec Pro, Room 70, Room 70 G2)*

    NEW: Value space: Integer (1..3) *(Codec Plus, Room 70)*

    NEW: Value space: Integer (1..6) *(Codec Pro, Room 70 G2)*

Video Input Connector [3,4,5] PreferredResolution *(Codec Pro, Room 70 G2)*

    OLD: Default value: 3840_2160_30

    NEW: Default value: 1920_1080_60

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

21

System configuration changes in CE9.4

New configurations

Audio Input HDMI [1..2] Mode *(Room 55)*

Audio Input HDMI [1..2] VideoAssociation MuteOnInactiveVideo *(Room 55)*

Audio Output Line [1] OutputType *(Room 70)*

Cameras Camera [1] Backlight DefaultMode *(DX70, DX80)*

Cameras Camera [1..2] Mirror *(MX700, MX800)*

Conference FarendMessage Mode *(All products)*

SIP MinimumTLSVersion *(All products)*

Configurations that are removed

NetworkServices HTTP Proxy Allowed *(All products)*

Video Output Connector [2] CEC Mode *(DX70, DX80)*

Video Output Connector [2] Location HorizontalOffset *(DX70, DX80)*

Video Output Connector [2] Location VerticalOffset *(DX70, DX80)*

Video Output Connector [2] OverscanLevel *(DX70, DX80)*

Video Output Connector [2] Resolution *(DX70, DX80)*

Video Output Connector [2] RGBQuantizationRange *(DX70, DX80)*

Configurations that are modified

Audio Output Line [1] OutputType *(Room Kit)*
  OLD: Default value: LineOut
  NEW: Default value: Loudspeaker
  OLD: Value space: LineOut / Subwoofer
  NEW: Value space: LineOut / Loudspeaker / Recorder / Subwoofer

Audio Ultrasound MaxVolume *(MX200 G2, MX300 G2, Codec Plus, Room 55, Room 70)*
  OLD: Default value: 60 *(MX200 G2, MX300 G2)*
  OLD: Default value: 70 *(Codec Plus, Room 55, Room 70)*
  NEW: Default value: 50 *(MX200 G2, MX300 G2)*
  NEW: Default value: 60 *(Codec Plus, Room 70)*
  NEW: Default value: 64 *(Room 55)*
  OLD: Value space: Integer (0..80) *(MX200 G2, MX300 G2)*
  OLD: Value space: Integer (0..90) *(Room 55, Room 70)*
  NEW: Value space: Integer (0..70) *(MX200 G2, MX300 G2)*
  NEW: Value space: Integer (0..80) *(Room 70)*
  NEW: Value space: Integer (0..84) *(Room 55)*

Network [1] DNS DNSSEC Mode *(All products)*
  OLD: User role: ADMIN, USER
  NEW: User role: ADMIN

Network [1] Speed *(All products)*
  OLD: User role: ADMIN, USER
  NEW: User role: ADMIN, INTEGRATOR

NetworkServices HTTP Mode *(All products)*
  OLD: Default value: HTTP+HTTPS
  NEW: Default value: HTTPS

NetworkServices SNMP CommunityName *(All products)*
  OLD: User role: ADMIN
  NEW: User role: ADMIN, INTEGRATOR

NetworkServices SNMP Host [1..3] Address *(All products)*
  OLD: User role: ADMIN
  NEW: User role: ADMIN, INTEGRATOR

NetworkServices SNMP Mode *(All products)*
  OLD: User role: ADMIN
  NEW: User role: ADMIN, INTEGRATOR

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

22

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

NetworkServices SNMP SystemContact *(All products)*

OLD: User role: ADMIN

NEW: User role: ADMIN, INTEGRATOR

NetworkServices SNMP SystemLocation *(All products)*

OLD: User role: ADMIN

NEW: User role: ADMIN, INTEGRATOR

UserInterface ContactInfo Type *(SX10, DX70, DX80)*

OLD: Value space: Auto / DisplayName / IPv4 / IPv6 / None / SipUri / SystemName

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

Video Output Connector [1] CEC Mode *(SX10)*

OLD: Default value: Off

NEW: Default value: On

Video Output Connector [3] Resolution *(SX80)*

OLD: User role: ADMIN, INTEGRATOR

NEW: User role: ADMIN, INTEGRATOR, USER

System configuration changes in CE9.3

New configurations

Audio KeyClickDetector Attenuate *(Codec Plus, Room Kit, Room 55, Room 70)*

Audio KeyClickDetector Enabled *(Codec Plus, Room Kit, Room 55, Room 70)*

Cameras Camera [1..3] AssignedSerialNumber *(Codec Plus, Room 70)*

Cameras Camera [3] Backlight DefaultMode *(Codec Plus, Room 70)*

Cameras Camera [3] Brightness DefaultLevel *(Codec Plus, Room 70)*

Cameras Camera [3] Brightness Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Focus Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Gamma Level *(Codec Plus, Room 70)*

Cameras Camera [3] Gamma Mode *(Codec Plus, Room 70)*

Cameras Camera [3] Mirror *(Codec Plus, Room 70)*

Cameras Camera [3] Whitebalance Level *(Codec Plus, Room 70)*

Cameras Camera [3] Whitebalance Mode *(Codec Plus, Room 70)*

Network [1] DNS DNSSEC Mode *(All products)*

NetworkServices HTTP Proxy PACUrl *(All products)*

SystemUnit CrashReporting Advanced *(All products)*

SystemUnit CrashReporting Mode *(All products)*

SystemUnit CrashReporting URL *(All products)*

UserInterface Accessibility IncomingCallNotification *(All products)*

UserInterface Security Mode *(All products)*

Video Selfview Mirrored *(DX70, DX80)*

Configurations that are removed

Provisioning HttpMethod *(All products)*

Configurations that are modified

NetworkServices HTTP Proxy Allowed *(All products)*
> OLD: Default value: True
> NEW: Default value: False

NetworkServices HTTP Proxy Mode *(All products)*
> OLD: Value space: Manual/Off
> NEW: Value space: Manual/Off/PACUrl/WPAD

Proximity Mode *(Room 70)*
> OLD: Default value: Off
> NEW: Default value: On

Security Session MaxSessionsPerUser *(All products)*
> OLD: Default value: 0
> NEW: Default value: 20
> OLD: Value space: Integer (0..100)
> NEW: Value space: Integer (1..20)

Security Session MaxTotalSessions *(All products)*
> OLD: Default value: 0
> NEW: Default value: 20
> OLD: Value space: Integer (0..100)
> NEW: Value space: Integer (1..20)

Standby WakeupOnMotionDetection *(Room 70)*
> OLD: Default value: Off
> NEW: Default value: On

Video Input Connector[2] Name *(Room 55)*
> OLD: Default value: "PC 1 (HDMI)"
> NEW: Default value: ""

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

24

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Video Input Connector[3] Name *(Room 55)*

OLD: Default value: "PC 2 (HDMI)"

NEW: Default value: ""

Video Input Connector[1] CEC Mode *(Room 70)*

OLD: Value space: Off/On

NEW: Value space: On

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

25

System configuration changes in CE9.2

New configurations

Audio Input HDMI[n] Mode *(Codec Plus)*

Audio Input HDMI[n] VideoAssociation MuteOnInactiveVideo *(Codec Plus, Room Kit)*

Audio Output InternalSpeaker Mode *(Room 55)*

Audio Ultrasound MaxVolume *(All products)*

    Replacing Peripherals Pairing Ultrasound Volume MaxLevel

Audio Ultrasound Mode *(All products)*

    Replacing Peripherals Pairing Ultrasound Volume Model

Cameras Camera[1..2] Focus Mode *(MX700, MX800)*

    Added for the integrated cameras

Cameras SpeakerTrack Whiteboard Mode *(Codec Plus, Room Kit, Room 55)*

Macros AutoStart *(All products except SX10)*

Macros Mode *(All products except SX10)*

NetworkServices HTTP Proxy Allowed *(All products)*

NetworkServices HTTP Proxy LoginName *(All products)*

NetworkServices HTTP Proxy Mode *(All products)*

NetworkServices HTTP Proxy Password *(All products*

NetworkServices HTTP Proxy Url *(All products)*

RTP Video Ports Range Start *(All products)*

RTP Video Ports Range Stop *(All products)*

Security Session FailedLoginsLockoutTime *(All products)*

Security Session MaxFailedLogins *(All products)*

UserInterface CustomMessage *(All products)*

UserInterface OSD HalfwakeMessage *(All products)*

UserInterface SettingsMenu Mode *(All products)*

Video Input Connector[n] HDCP Mode *(Room 55)*

Configurations that are removed

Conference MultiStream Mode *(SX10, DX70, DX80)*

Peripherals Pairing Ultrasound Volume MaxLevel *(All products)*

    Replaced by Audio Ultrasound MaxVolume

Peripherals Pairing Ultrasound Volume Mode *(All products)*

    Replaced by Audio Ultrasound Mode

Configurations that are modified

Audio Input MicrophoneMode *(DX70, DX80)*

    OLD: User role: ADMIN
    NEW: User role: ADMIN, INTEGRATOR

Audio Input Microphone[n] Level *(Room Kit, Room 55)*

    OLD: Value space: 0..36
    NEW: Value space: 0..26

Cameras Camera[n] Focus Mode *(SX80, MX700, MX800, Codec Plus)*

    OLD: Value space: Auto/Manual
    NEW: Value space: Auto/AutoLimited/Manual

Cameras SpeakerTrack Closeup *(SX80, MX700, MX800, Room Kit, Codec Plus, Room 55)*

    OLD: User role: ADMIN, INTEGRATOR
    NEW: User role: ADMIN, INTEGRATOR, USER

Cameras SpeakerTrack Whiteboard Mode *(SX80, MX700, MX800)*

    OLD: User role: ADMIN, INTEGRATOR
    NEW: User role: ADMIN, INTEGRATOR, USER

Security Audit Logging Mode *(All products)*

    OLD: Default value: Off
    NEW: Default value: Internal

UserInterface Language *(All products)*

    NEW: Arabic and Hebrew added to valuespace

UserInterface OSD Output *(Room Kit)*

OLD: Default value: 1

NEW: Default value: Auto

Video Input Connector[2] Name *(Codec Plus, Room 55)*

OLD: Default value: PC (HDMI1)

NEW: Default value: PC 1 (HDMI)

Video Input Connector[3] Name *(Codec Plus, Room 55)*

OLD: Default value: PC (HDMI2)

NEW: Default value: PC 2 (HDMI)

Video Output Connector[1] Resolution *(MX200G2, MX300G2, DX70, DX80, Room 55)*

OLD: User role: ADMIN, INTEGRATOR

NEW: User role: ADMIN, INTEGRATOR, USER

Video Selfview OnCall Mode *(Room Kit)*

OLD: Default value: Off

NEW: Default value: On

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

27

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

System configuration changes in CE9.1

New configurations

Bluetooth Allowed *(DX70, DX80)*

Bluetooth Enabled *(DX70, DX80)*

Cameras Camera Framerate *(Room Kit)*

NetworkPort [2] Mode *(DX70, DX80)*

RoomAnalytics PeopleCountOutOfCall *(Codec Plus, Room Kit)*

RoomAnalytics PeoplePresenceDetector *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, Codec Plus, Room Kit)*

Video Input Connector [n] CEC Mode *(Codec Plus, Room Kit)*

Configurations that are removed

None

Configurations that are modified

Conference DefaultCall Rate *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, Codec Plus, Room Kit)*
>   OLD: Default value: 3072
>   NEW: Default value: 6000

Conference MultiStream Mode *(SX80, MX700, MX800, Codec Plus, Room Kit)*
>   OLD: Default value: Off
>   NEW: Default value: Auto
>   OLD: Valuespace: Off
>   NEW: Valuespace: Auto/Off

Network[1] IEEE8021X Password *(All products)*
>   OLD: Valuespace: String(0, 32)
>   NEW: Valuespace: String(0, 50)

NetworkServices Wifi Enabled *(DX70, DX80)*
>   OLD: Default value: False
>   NEW: Default value: True

Peripherals Profile TouchPanels *(SX80, Codec Plus, Room Kit)*
>   OLD: Default value: NotSet
>   NEW: Default value: Minimum1

Standby WakeupOnMotionDetection *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800, Codec Plus, Room Kit)*
>   OLD: Default value: Off
>   NEW: Default value: On

Video Input Connector [n] PresentationSelection *(All products)*
>   OLD: Valuespace: AutoShare/Manual/OnConnect *(SX10, SX20, SX80, MX200 G2, MX300 G2,, MX700, MX800, Codec Plus, Room Kit)*
>   OLD: Valuespace: AutoShare/Desktop/Hidden/Manual/OnConnect *(DX70, DX80)*
>   NEW: Valuespace: AutoShare/Desktop/Manual/OnConnect *(All products)*

Video Output Connector [1..2] MonitorRole *(Room Kit, Codec Plus)*
>   OLD: Default value: Connector [1]: First; Connector [2]: Second
>   NEW: Default value: Auto

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

28

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

System configuration changes in CE9.0

New configurations

Cameras SpeakerTrack Closeup *(SX80, MX700, MX800)*

NetworkServices HTTPS Server MinimumTLSVersion *(All products)*

NetworkServices HTTPS StrictTransportSecurity *(All products)*

Peripherals Pairing CiscoTouchPanels EmcResilience *(SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Standby WakeupOnMotionDetection *(All products)*

Configurations that are removed

UserInterface UserPreferences *(All products)*

Audio Microphones PhantomVoltage *(SX20, MX200 G2, MX300 G2)*

Conference VideoBandwidth PresentationChannel Weight *(All products)*

Standby AudioMotionDetection *(All products)*

Video Layout DisableDisconnectedLocalOutputs *(SX20, MX200 G2, MX300 G2, DX70, DX80)*

Configurations that are modified

Cameras Camera [n] * *(SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*
> OLD: User role: ADMIN, USER
> NEW: User role: ADMIN, INTEGRATOR

Cameras PresenterTrack * *(SX80, MX700, MX800)*
> OLD: User role: ADMIN, USER
> NEW: User role: ADMIN, INTEGRATOR

Cameras SpeakerTrack * *(SX80, MX700, MX800)*
> OLD: User role: ADMIN, USER
> NEW: User role: ADMIN, INTEGRATOR

Conference MultiStream Mode *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*
> OLD: Value space: Auto/Off
> NEW: Value space: Off

NetworkServices Wifi Allowed *(DX70, DX80)*
> Renamed from NetworkServices WIFI Allowed
> OLD: User role: ADMIN
> NEW: User role: ADMIN, USER

NetworkServices Wifi Enabled *(DX70, DX80)*
> Renamed from NetworkServices WIFI Enabled
> OLD: User role: ADMIN
> NEW: User role: ADMIN, USER

UserInterface Language *(All products)*
> NEW: Portuguese added to value space

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

29

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Configurations with the new INTEGRATOR user role

A new user role – INTEGRATOR – is introduced in CE9.0. It has been added to the following configurations:

Audio DefaultVolume *(All products)*

Audio Input HDMI [n] * *(SX80, MX700, MX800)*

Audio Input Line [n] * *(SX20, SX80, MX700, MX800)*

Audio Input Microphone [n] * *(SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Audio MicrophoneReinforcement * *(SX80, MX700, MX800)*

Audio Microphones Mute Enabled *(All products)*

Audio Output HDMI [n] * *(SX80)*

Audio Output Line [n] * *(SX10, SX20, SX80, MX700, MX800)*

Audio SoundsAndAlerts * *(All products)*

CallHistory Mode *(All products)*

Cameras Camera [n] * *(SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Cameras PowerLine Frequency *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Cameras PresenterTrack * *(SX80, MX700, MX800)*

Cameras SpeakerTrack * *(SX80, MX700, MX800)*

Conference DefaultCall Rate *(All products)*

Conference DoNotDisturb DefaultTimeout *(All products)*

FacilityService * *(All products)*

GPIO Pin [n] Mode *(SX80, MX700, MX800)*

Peripherals Pairing Ultrasound Volume MaxLevel *(All products)*

Peripherals Pairing Ultrasound Volume Mode *(All products)*

Peripherals Profile * *(SX10, SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

SerialPort BaudRate *(SX20, SX80, MX700, MX800)*

SerialPort Mode *(All products)*

Standby * *(SX10, SX20, SX80, MX200 G2, MX300 G2, DX70, DX80)*

Standby BootAction *(MX700, MX800)*

Standby Control *(MX700, MX800)*

Standby Delay *(MX700, MX800)*

Standby StandbyAction *(MX700, MX800)*

Standby WakeupAction *(MX700, MX800)*

Standby WakeupOnMotionDetection *(MX700, MX800)*

SystemUnit Name *(All products)*

Time Zone *(All products)*

UserInterface OSD Output *(All products)*

UserInterface Wallpaper *(All products)*

Video ActiveSpeaker DefaultPIPPosition *(All products)*

Video Input Connector [n] * *(SX10, DX70, DX80)*

Video Input Connector [n] CameraControl CameraId *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] CameraControl Mode *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] InputSourceType *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] Name *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] OptimalDefinition Profile *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] PresentationSelection *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] Quality *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] RGBQuantizationRange *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Input Connector [n] Visibility *(SX20, SX80, MX200 G2, MX300 G2, MX700, MX800)*

Video Monitors *(All products)*

Video Output Connector [n] * *(SX80, MX700, MX800)*

Video Output Connector [n] CEC Mode *(SX10, SX20, MX200 G2, MX300 G2, DX70, DX80)*

Video Output Connector [n] Location HorizontalOffset *(SX20, MX200 G2, MX300 G2, DX70, DX80)*

Video Output Connector [n] Location VerticalOffset *(SX20, MX200 G2, MX300 G2, DX70, DX80)*

Video Output Connector [n] MonitorRole *(SX20)*

Video Output Connector [n] Resolution *(SX10, SX20, MX200 G2, MX300 G2, DX70, DX80)*

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

30

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Video Output Connector [n] RGBQuantizationRange *(SX10, SX20, MX200 G2, MX300 G2, DX70, DX80)*

Video Presentation DefaultPIPPosition *(All products)*

Video Selfview Default * *(All products)*

Video Selfview OnCall * *(All products)*

<path> * means that the change applies to all configurations starting with *<path>*.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

31

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

DX70 and DX80 at a glance

The Cisco Webex 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
- Support for wireless Bluetooth headset, Bluetooth headset with USB dongle, and USB headset
- 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 Webex
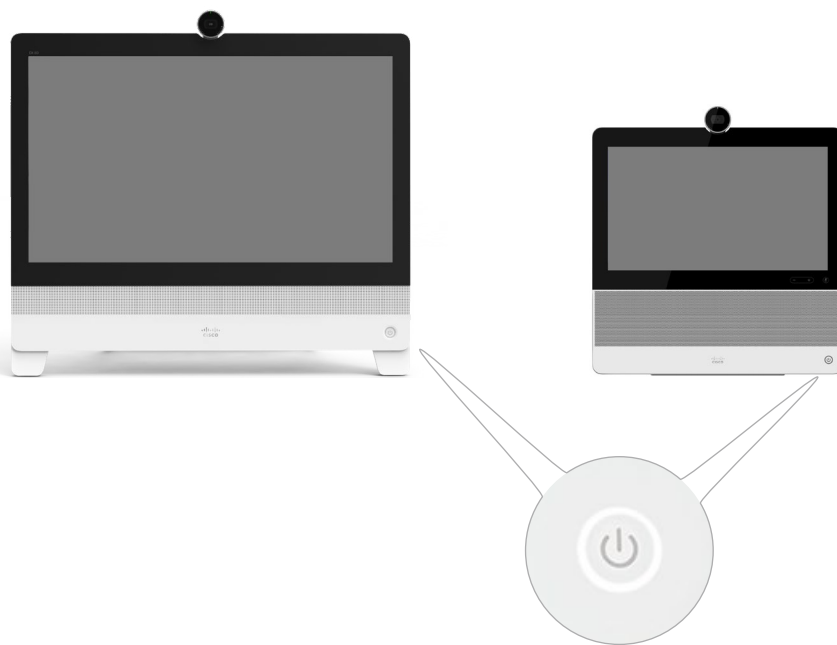
Cisco Webex DX70

Cisco Webex DX80

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

32

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 LEDs
encircling the button

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.

Restart and standby using the user interface

Restart the system

1. Select the contact information in the upper left corner of the user interface.

2. Select *Settings*, followed by *Restart*.

3. Select *Restart* again to confirm your choice.

Enter/exit standby mode

1. Select the contact information in the upper left corner of the user interface.

2. Select *Standby*.

Power Off or restart the system remotely

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

Restart the system

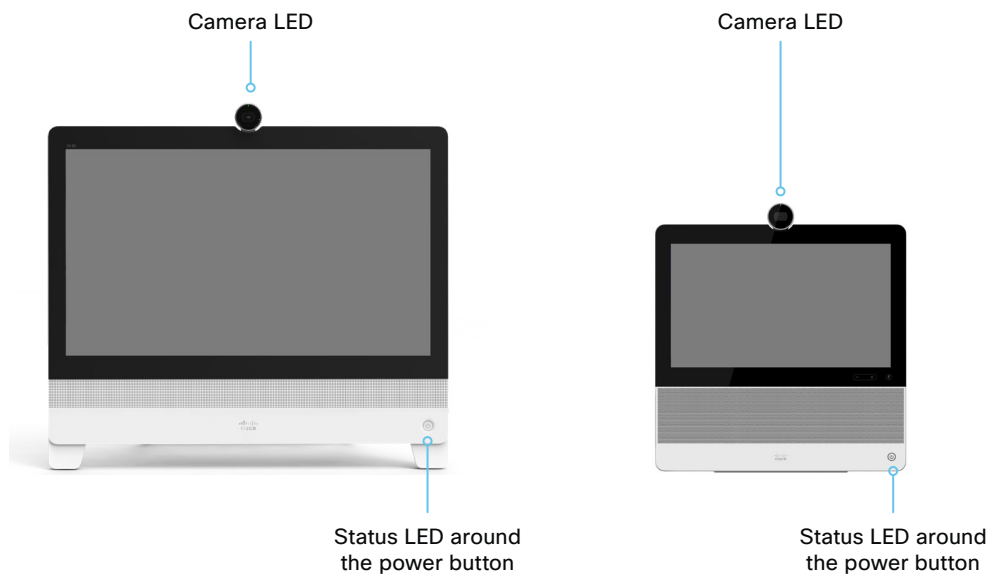Click *Restart device...* and confirm your choice.

It takes a few minutes before the system is ready for use.

Power Off the system

Click *Shutdown device...* and confirm your choice.

> ℹ️ You cannot power the system on again remotely; you have to use the power button.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

33

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

LED indicators

Camera LED

Camera LED

Status LED around
the power button

Status LED around
the power button

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 statuses are available in the web interface than in the API.

Access method	Notes	How to enable/disable the methods
HTTP/HTTPS	• Used by the web interface of the video system • Non-secure (HTTP) or secure (HTTPS) communication • HTTPS: *Enabled* by default • HTTP: *Enabled* by default only for video systems that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the video system has not been factory reset after the upgrade.	*NetworkServices > HTTP > Mode* Restart the video system for changes to take effect
Telnet	• Non-secure TCP/IP connection • *Disabled* by default	*NetworkServices > Telnet > Mode* You do not need to restart the video system. It may take some time for changes to take effect
SSH	• Secure TCP/IP connection • *Enabled* by default	*NetworkServices > SSH > Mode* You do not need to restart the video system. It may take some time for changes to take effect
Serial interface (RS-232)	• Connect to the video system with a cable. IP-address, DNS, or a network is not required • *Enabled* by default • For security reasons, you are asked to sign in by default (*SerialPort > LoginRequired*)	*SerialPort > Mode* Restart the video system for changes to take effect

⚠ 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

35

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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).

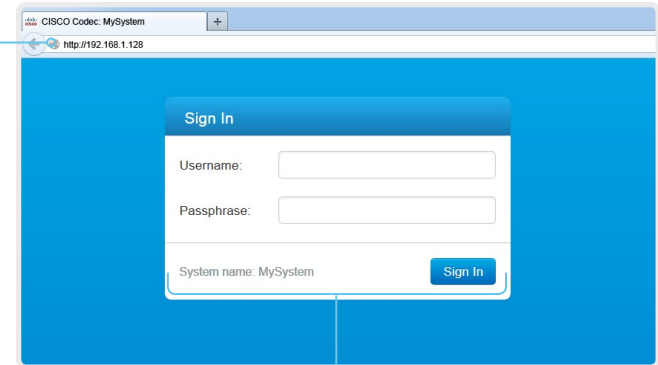We recommend that you use the latest release of one of the major web browsers.

Connect to the video system

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

ℹ️ **How to find the IP address**

1. Select the contact information in the upper left corner of the user interface.
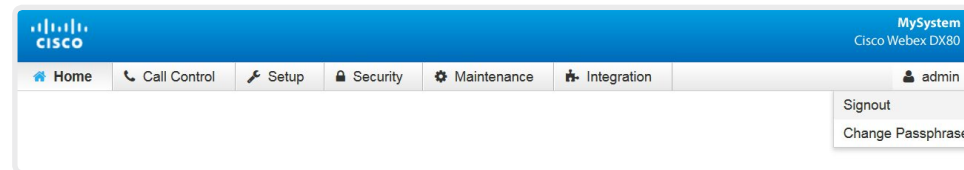2. Select *Settings*, followed by *About this device*.

Sign in

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

ℹ️ 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

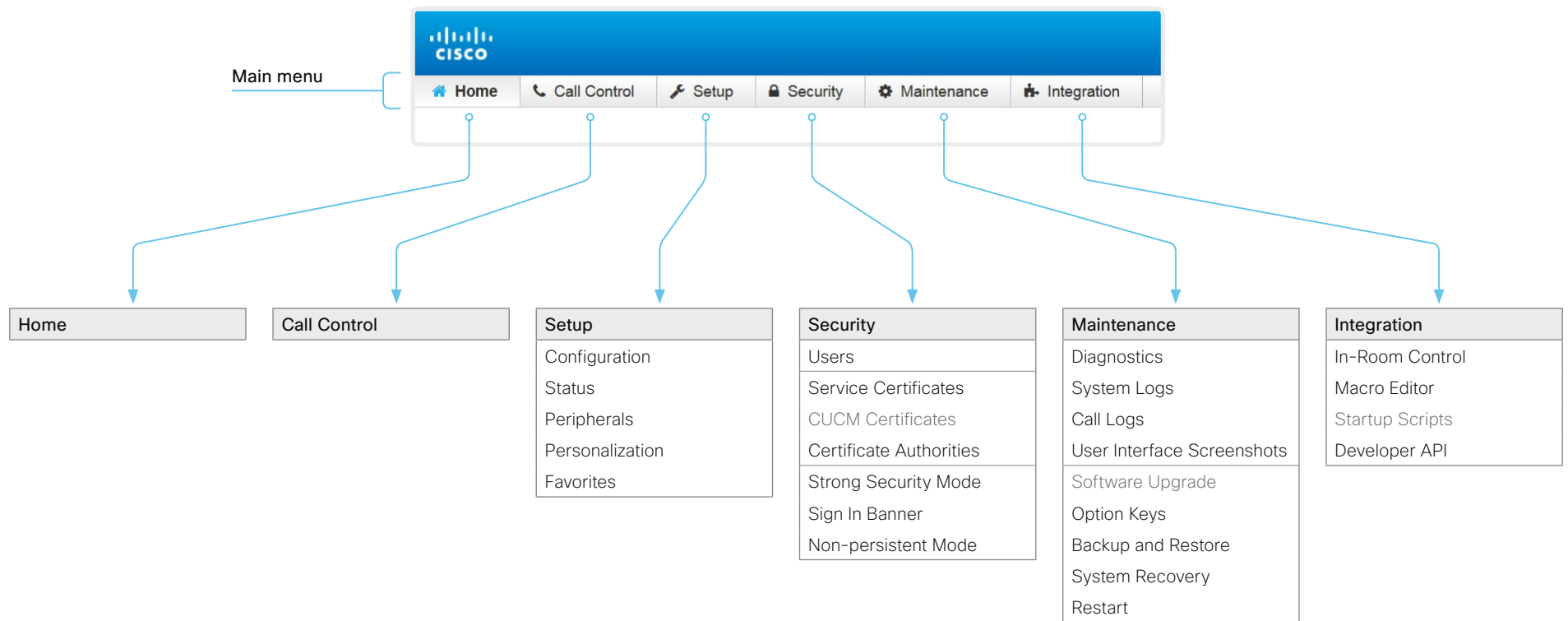Hover the mouse over the user name and choose *Signout* from the drop-down list.

How to administer the video system (page 3 of 4)

How the web interface is organized

The web interface is organized in sub-pages. All sub-pages shown below are available if the video system is registerd to an on-premise service (CUCM, VCS); the pages shown in grey color are not available if the video system is registered to the Cisco cloud service (Cisco Webex).

In both cases, 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.

Main menu

🏠 Home	📞 Call Control	🔧 Setup	🔒 Security	⚙ Maintenance	👥 Integration

Home	Call Control	Setup	Security	Maintenance	Integration
		Configuration	Users	Diagnostics	In-Room Control
		Status	Service Certificates	System Logs	Macro Editor
		Peripherals	CUCM Certificates	Call Logs	Startup Scripts
		Personalization	Certificate Authorities	User Interface Screenshots	Developer API
		Favorites	Strong Security Mode	Software Upgrade	
			Sign In Banner	Option Keys	
			Non-persistent Mode	Backup and Restore	
				System Recovery	
				Restart	

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

37

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Settings and system information on the user interface

You have access to system information, and some basic configurations and system tests on the video system's user interface.

System-critical settings and functions, such as network settings, service activation, and factory reset, may be protected by a passphrase, refer to the ▶ Restrict the access to the Settings menu chapter.

Some of the settings and tests are also part of the *Setup assistant* that is launched when the video system is powered up for the first time. The Setup assistant is described in the *Getting Started Guide* for systems running CE software.

Access Settings

1. Select the contact information in the upper left corner of the user interface.

2. Select *Settings*.

   A padlock symbol 🔒 indicates that a setting is protected (locked down).

3. Select the setting you want to change, or the test you want to run.

   If a setting is locked down, an authentication window pops up, and you have to sign in with ADMIN credentials to proceed.

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 **Acitve** 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 *Edit 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.

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.

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

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

INTEGRATOR: A user with this role has access to settings, commands and status that are required to set up advanced AV scenarios, and to integrate our video systems with 3rd party equipment. Such a user can also create in-room controls.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

40

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 your passphrase

1. Sign in to the web interface, hover the mouse over the user name, and choose *Change Passphrase* in the drop down list.

2. Enter the current passphrase and new passphrase in the input fields, and click *Change passphrase*.

   The passphrase format is a string with 0–64 characters.

ℹ️ If the passphrase currently is not set, leave the *Current passphrase* field blank.
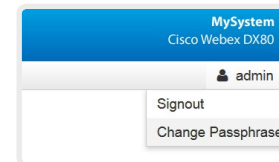
Change another user's passphrase

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

41

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Restrict the access to the Settings menu

By default, any user has access to the Settings menu on the user interface.

We recommend that you restrict the access to prevent unauthorized users from changing the configuration of the video system.

Lock down the Settings menu

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

2. Go to *UserInterface > SettingsMenu > Mode*, and select **Locked**.

3. Click *Save* for the change to take effect.

   Now a user has to sign in with ADMIN credentials to get access to the system-critical settings on the user interface.
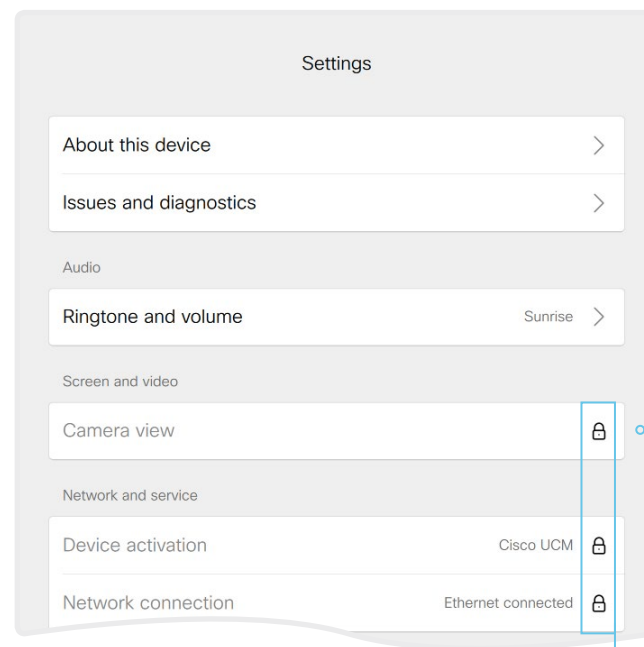
Unlock the Settings menu

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

2. Go to *UserInterface > SettingsMenu > Mode*, and select **Unlocked**.

3. Click *Save* for the change to take effect.

   Now any user has access to the complete Settings menu on the user interface.
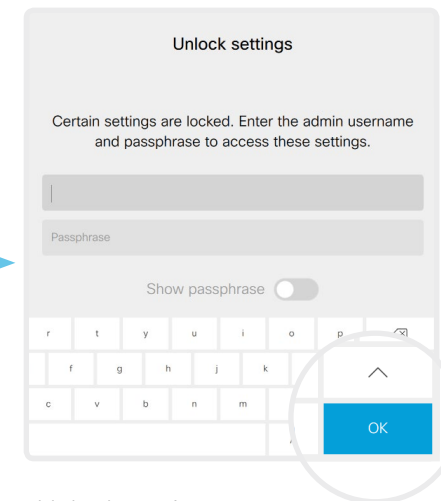
The Settings menu on the user interface

If the menu is locked down, you must sign in to access the system-critical settings.

Select the contact information in the upper left corner of the user interface followed by *Settings*, in order to open the Settings menu.

Locked down settings

Locked down settings are marked with a padlock.

Unlock settings

If you click on the padlock, you are asked to sign in with an ADMIN user.

Once signed in, you can access all settings until you close the Settings menu.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

42

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

System configuration

Sign in to the web interface, and navigate to *Setup > Configuration*.
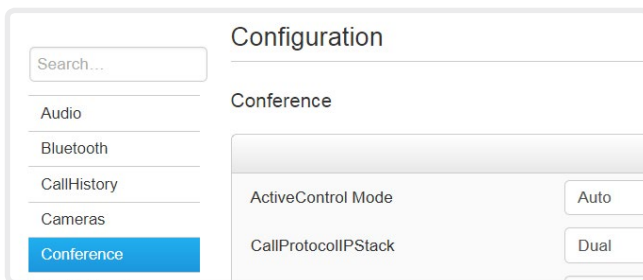
Find a system setting

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.
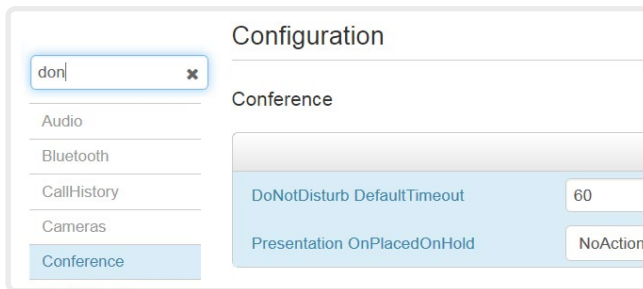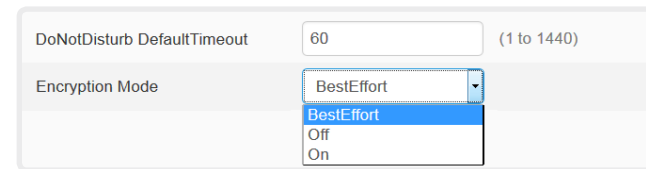
Select a category and navigate to settings

The system settings are grouped in categories. Choose a category in the left pane to show the associated settings.
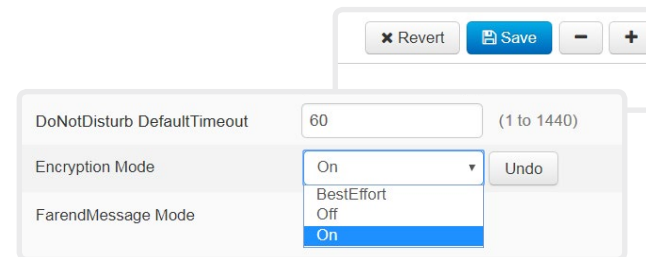
Change a system setting

Check the value space

A settings'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 *Revert* buttons if you do not want to make any changes.

Categories with unsaved changes are marked with an edit symbol ( ).

About system settings

All system settings can be changed from the web interface.

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

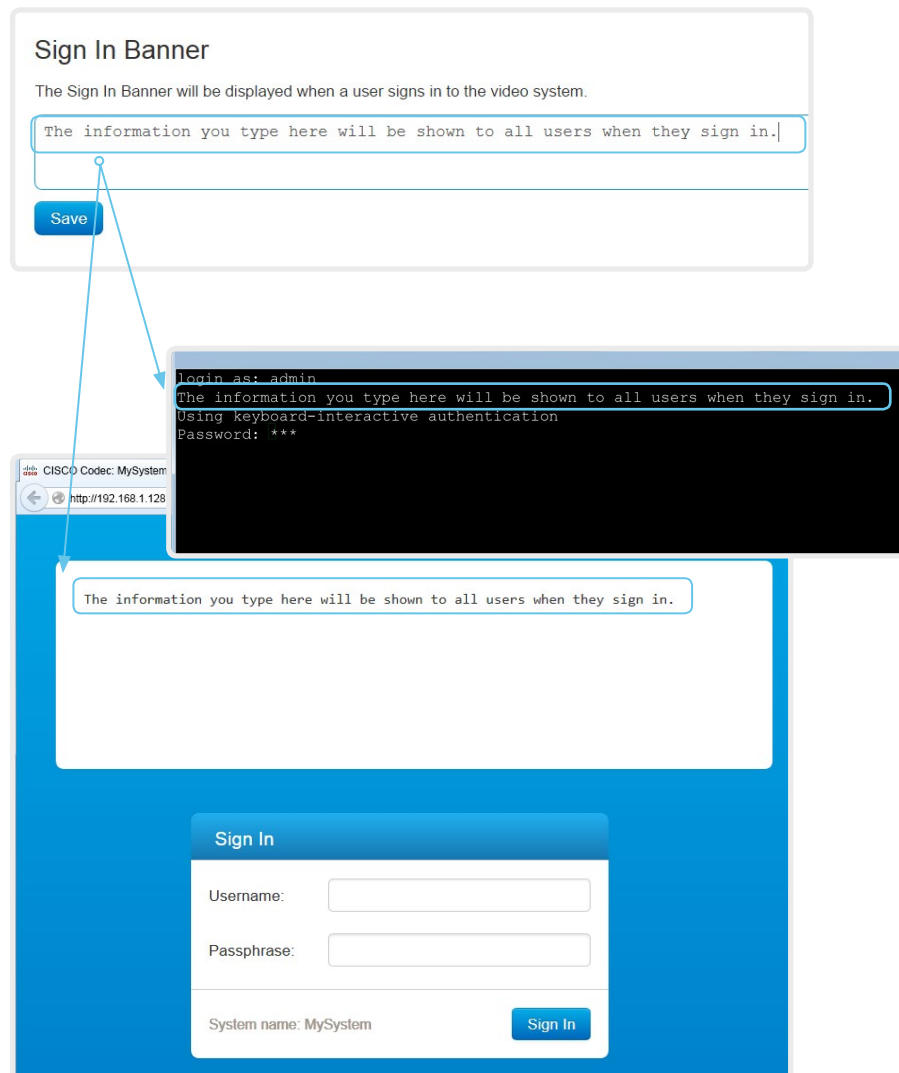Different settings may require different user credentials. In order to be sure that an administrator is able to change all system settings, an administrator user must possess all user roles.

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

43

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

Sign In Banner

The Sign In Banner will be displayed when a user signs in to the video system.

The information you type here will be shown to all users when they sign in.

Save

```
login as: admin
The information you type here will be shown to all users when they sign in.
Using keyboard-interactive authentication
Password: ***
```

CISCO Codec: MySystem

http://192.168.1.128

The information you type here will be shown to all users when they sign in.

Sign In

Username: _____

Passphrase: _____

System name: MySystem   Sign In

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.

The maximum size is: 4 kByte

Welcome banner versus sign in banner

Sign in banner:

- The banner is shown *before* the user signs in to the web interface or the command line interface.

Welcome banner:

- The banner is shown *after* the user has signed in to the web interface or the command line interface.

Add a welcome banner

Adding a Welcome banner is only available using API commands; we don't provide a dedicated user interface for it.

API commands

    xCommand SystemUnit WelcomeBanner Set

This is a multiline command. Anything you input after you issue the command, is input to the command (including line breaks). Finish the input with a separate line containing just a period ending with a line break.

There are also a few more welcome banner commands, refer to the API-guide for more details.

    xCommand SystemUnit WelcomeBanner Clear
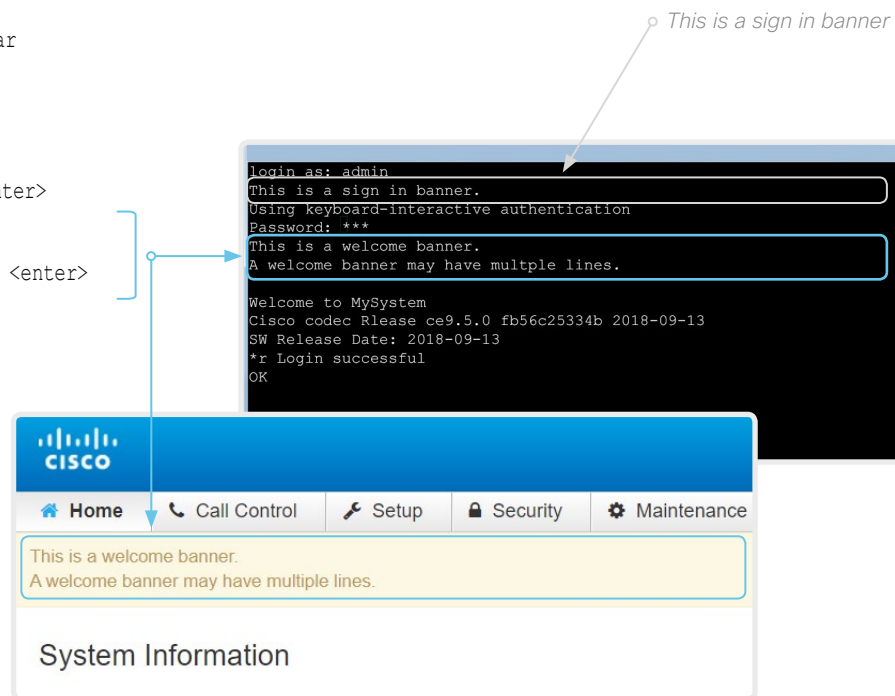
    xCommand SystemUnit WelcomeBanner Get

Example

xCommand SystemUnit WelcomeBanner Set <enter>

This is a welcome banner. <enter>

A welcome banner may have multiple lines. <enter>

. <enter>

This is a sign in banner

```
login as: admin
This is a sign in banner.
Using keyboard-interactive authentication
Password: ***
This is a welcome banner.
A welcome banner may have multple lines.

Welcome to MySystem
Cisco codec Rlease ce9.5.0 fb56c25334b 2018-09-13
SW Release Date: 2018-09-13
*r Login successful
OK
```

| 🏠 Home | 📞 Call Control | 🔧 Setup | 🔒 Security | ⚙ Maintenance |

This is a welcome banner.
A welcome banner may have multiple lines.

System Information

About welcome banner

You can set up a welcome banner that users see after they sign in to the video system's web interface or command line interface. The banner can have multiple lines.

The banner can for example contain information you need in order to get started, or things you must be aware of when setting up the system.

The maximum size is: 4 kByte

Welcome banner versus sign in banner

Sign in banner:

- The banner is shown *before* the user signs in to the web interface or the command line interface.

Welcome banner:

- The banner is shown *after* the user has signed in to the web interface or the command line interface.

Manage the service certificates of the video system

Sign in to the web interface and navigate to *Security > Service Certificates*.

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.

Enable or disable, view or delete a certificate

Use the On and Off buttons to enable or disable a certificate for the different services.

Use the corresponding button to view or delete a certificate.

Add a certificate

1. Browse to find the Certificate file and Private key file (optional) on your computer.

2. Fill in the *Passphrase* if required.

3. Click *Add certificate...* to store the certificate on the video system.

Service Certificates

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

Add Certificate

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

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

Add certificate...

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

46

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.
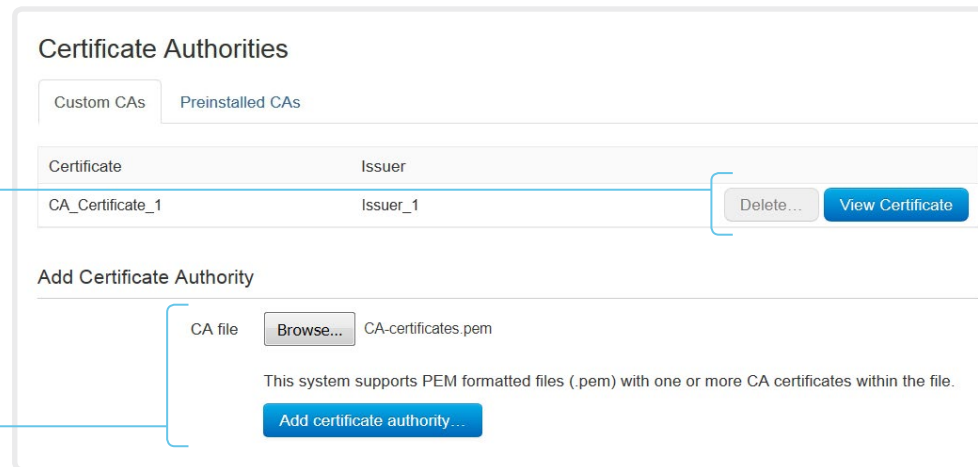
You need the following file:

- CA certificate list (file format: .PEM).

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.

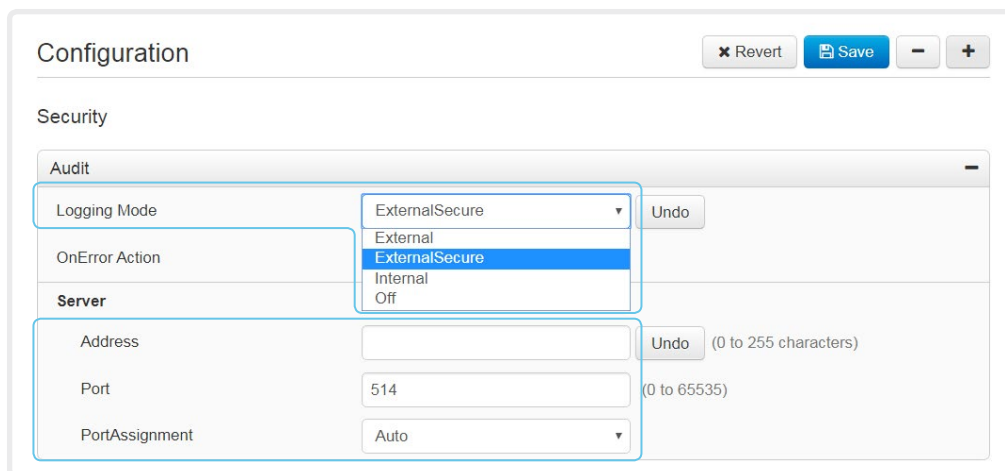If authentication fails, the connection will not be established.

View or delete a certificate

Use the corresponding button to view or delete a certificate.

Certificate Authorities

| Custom CAs | Preinstalled CAs |

Certificate	Issuer		
CA_Certificate_1	Issuer_1	Delete...	View Certificate

Add Certificate Authority

CA file   [Browse...]   CA-certificates.pem

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

[Add certificate authority...]

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

Upload a list of certificate authorities

1. Browse to 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.

⚠ Previously stored certificates are not deleted automatically.

The entries in a new file with CA certificates are appended to the existing list.

Set up secure audit logging

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

⚠ 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.

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.

3. Set *Audit > Logging > Mode* to **ExternalSecure**.

4. Click *Save* for the change to take effect.

Configuration		✖ Revert	🖫 Save	−	+

Security

Audit			−
Logging Mode	ExternalSecure ▼	Undo	
	External		
	ExternalSecure		
OnError Action	Internal		
	Off		
Server			
Address		Undo	(0 to 255 characters)
Port	514		(0 to 65535)
PortAssignment	Auto ▼		

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

48

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

Certificate Authorities

Custom CAs | Preinstalled CAs

This CA list is used for Cisco UCM via Expressway (Edge) provisioning only.

Configure provisioning now.

These certificates are used to validate the servers contacted over the Internet when the endpoint uses Cisco UCM via Expressway provisioning.

Certificate	Issuer			Disable All
Certificate_01	Issuer_1	Details...	✔	Disable
Certificate_02	Issuer_2	Details...	✔	Disable
Certificate_03	Issuer_3	Details...	✔	Disable

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

View or disable certificates

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

ℹ 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*, and then open the *Security* category to see the *Persistency* status.

Change the persistency settings

All persistency settings are set to **Persistent** by default. You only have to change these settings if you want 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 reveived 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.

Strong Security Mode

Strong Security Mode is **not** enabled.

Strong Security Mode is required to adhere to U.S. Department of Defense JITC regulations.

It will introduce the following:

- All users and administrators must change their passphrase and PIN on the next signin
- New passphrases must meet the following criteria:
  - Minimum 15 characters
  - Minimum 2 uppercase alphabetic characters
  - Minimum 2 lowercase alphabetic characters
  - Minimum 2 numerical characters
  - Minimum 2 non-alphanumeric (special) characters
  - No more than 2 consecutive characters may be the same
  - Must be different from the last 10 previous passphrases used
  - Not more than 2 characters from the previous passphrase can be in the same position
- Passphrases must be changed at least every 60 days
- Passphrases cannot be changed more than once per 24 hours
- 3 failed signins will lock the user account until an administrator re-activates the account

[Enable Strong Security Mode...]

Strong Security Mode

Strong Security Mode is enabled.

[Disable Strong Security Mode...]

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

52

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.

Ultrasound

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.

Video system	Maximum number of connections
Room Kit, Room 55, Room 55 Dual, Room 70, Room 70 G2	30 / 7 *
Codec Plus, Codec Pro	30 / 7 *
SX80	10
SX10, SX20	7
MX700, MX800	10
MX200 G2, MX300 G2	7
DX70, DX80	3

* 30 connections when the *View shared content on a mobile device* Proximity service is disabled; 7 connections when this service is enabled.

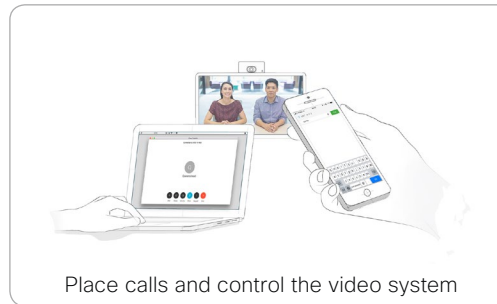## Proximity services

Place calls and control the video system:

· Dial, mute, adjust volume, hang up
· Available on laptops (OS X and Windows), 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 laptop:

· Share content without connecting a presentation cable
· Available on laptops (OS X and Windows)

Place calls and control the video system

View shared content on a mobile device

Wireless share from a mobile device

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

53

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.
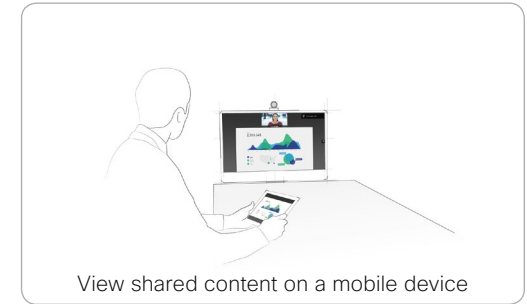
Set up Intelligent Proximity for content sharing (page 2 of 5)

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 ► https://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

Read the end-user license agreement carefully,
► https://www.cisco.com/c/en/us/td/docs/general/warranty/English/EU1KEN_.html

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.

Room 70, Room 70 G2, Room 55, Room 55 Dual, Room Kit, Room Kit Plus, 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.

Codec Plus, Codec Pro, SX10, SX20, and SX80:

- We cannot foresee the ultrasound sound pressure level on these video systems, because they emit ultrasound on third-party loudspeakers.

   The volume control on the loudspeaker itself, and the *Audio > Ultrasound > MaxVolume* setting affect the ultrasound sound pressure level; the volume control on the remote control or Touch controller does not have any effect.

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 plays ultrasound on the built-in loudspeakers. Ultrasound is never emitted on the HDMI or audio outputs.

Room 70, Room 70 G2, Room 55, Room 55 Dual, Room Kit, Room Kit Plus, Codec Plus, Codec Pro, SX10, SX20, SX80, and MX Series:

- These systems are not designed for headset use.
- 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.

Set up Intelligent Proximity for content sharing (page 4 of 5)

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.

   Enable the services you want to allow. Only *Wireless share from a desktop client* 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 > ToClients* and choose **Enabled**.

   Wireless share from a desktop client:

   - Go to *Proximity > Services > ContentShare > FromClients* and choose **Enabled**.

The Proximity indicator

You can see the Proximity indicator on the screen as long as at least one Proximity client is paired with the system.

The indicator doesn't disappear immediately when the last client unpairs. It may take a few minutes.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

56

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:
► https://www.cisco.com/web/siteassets/legal/privacy.html

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 (20 kHz–22 kHz). 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.
- Check *Settings > Issues and diagnostics* on the user interface, or *Maintenance > Diagnostics* on the web interface of the video system. If there are no ultrasound related Issues listed ("Unable to verify the ultrasound signal"), ultrasound pairing messages are emitted by the video system as they should. Refer to the Proximity *Support forum* for further assistance with the client detection issues.

Audio artifacts

- If you can hear audio artifacts, like humming or clipping noise, decrease the maximum ultrasound volume (*Audio > Ultrasound > MaxVolume*).

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 Proximity site:
► https://proximity.cisco.com

Support forum:
► https://www.cisco.com/go/proximity-support

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

57

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Adjust the video quality to call rate ratio

Video input quality settings

When encoding and transmitting video there is a trade-off between high resolution (sharpness) and high frame rate (motion).

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.

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.

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.

Some typical resolutions used for different optimal definition profiles, call rates and transmit frame rates are shown in the table. The resolution and frame rate must be supported by both the calling and called systems.

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 (integrated camera).

2. Go to *Video > Input > Connector n > OptimalDefinition > Profile* and choose the preferred optimal definition profile.

Resolutions and frame rate [w×h@fps] obtained for different optimal definition profiles and call rates			
Call rate [kbps]	H.264, maximum 30 fps		
	Normal	*Medium*	*High*
128	320×180@30	512×288@20	512×288@30
160	512×288@20	512×288@30	640×360@30
256	512x288@30	640x360@30	768x448@30
384	640x360@30	768x448@30	768x448@30
512	768x448@30	1024x576@30	1024x576@30
576	768×448@30	1024×576@30	1280×720@30
768	1024×576@30	1280×720@30	1280×720@30
1152	1280x720@30	1280x720@30	1280x720@30
1472	1280x720@30	1280x720@30	1920x1080@30
1920	1280x720@30	1920x1080@30	1920x1080@30
2560	1920x1080@30	1920x1080@30	1920x1080@30
3072	1920×1080@30	1920×1080@30	1920×1080@30

# Add corporate branding to the screen <small>(page 1 of 2)</small>

Sign in to the web interface, and navigate to *Setup > Personalization*, and open the *Branding* tab.

From this page you can add your own branding elements (background brand image, logo, custom message) to the video system.

Branding in the awake state

In the awake state you can:

- Add a logo in the bottom right corner
- Add a short message (text only) in the bottom left corner

Custom text
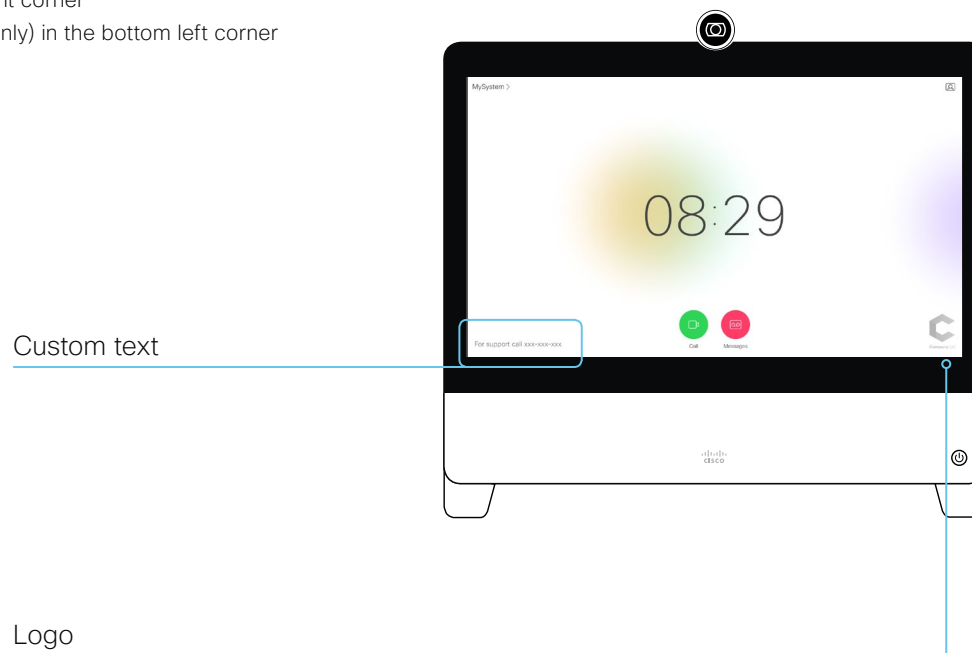
Logo

We recommend:

- A black logo (the video system will add a white overlay with 40% opacity so that the logo and the other user interface elements go well together)
- PNG-format with transparent background
- Minimum 272×272 pixels (it will be scaled automatically)

About Branding

The Branding feature, as describe in this chapter, allows you to customize the screen appearence without compromising the overall Cisco user experience.

We recommend that you use this feature rather than our legacy Custom wallpaper feature, which prevents the use of functionality such as One Button to Push.

You cannot use the Branding feature and a Custom wallpaper at the same time.

If your video system is set up with a Custom wallpaper, you must click *Disable the custom wallpaper* before adding branding elements.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

59

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Add corporate branding to the screen (page 2 of 2)

Branding in the halfwake state

In halfwake state you can:

- Add a background brand image
- Add a logo in the bottom right corner
- Customize or remove the message at the center of the screen. This is the message that informs the user how to start using the video system

    In general, we recommend that you keep the standard message. Change the message only if you have to adapt it to a different scenario, for example if you have a third party user interface.
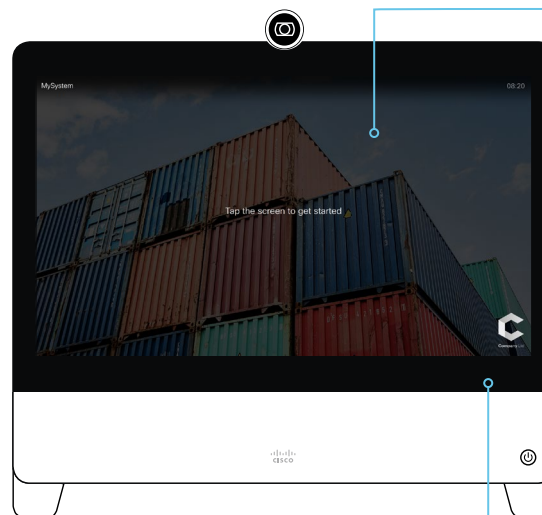
Background brand image

- When the video system wakes up, the image is shown in full color; after a few seconds the image is automatically dimmed (transparent black overlay)
- Image format: PNG or JPEG
- Recommended size: 1920 × 1080 pixels

Logo

We recommend:

- A white logo (so that it goes well with the dark background brand image)
- PNG-format with transparent background
- Minimum 272×272 pixels

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

60

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Add a custom wallpaper

Sign in to the web interface, and navigate to *Setup > Personalization*, and open the *Custom wallpaper* tab.

Personalization

Branding	Custom wallpaper	Ringtones

Custom wallpaper

The default experience is not compatible with custom wallpaper. The custom wallpaper disables the background image in all screen states, and disables the "One Button to Push" functionality, meeting info, and default usage prompts.

Custom 🗑

Upload custom wallpaper

Only BMP, GIF, JPEG and PNG files smaller than 16 megapixels are supported. Custom wallpapers do not apply to touch panels.

Browse...   No file selected.   Upload

Upload a custom wallpaper

Overwrites any old custom wallpaper.

1. Browse to find 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: 16 megapixels

The custom wallpaper is automatically activated once uploaded.

Delete the custom wallpaper

Delete fully removes the custom wallpaper from the video system.

You have to upload it anew if you want use it again.

About a custom wallpaper

If you want a custom picture as background on your screen, you may upload and use a *custom wallpaper*. A custom wallpaper will not appear on the Touch controller.

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

We recommend that you use our new Branding feature rather than this legacy Custom wallpaper feature. You will get a better overall Cisco user experience, and avoid loosing functionality such as One Button To Push and meeting information. See the ► Add corporate branding to the screen chapter.

You cannot use the Branding feature and a Custom wallpaper at the same time.

If your video system is set up with branding elements you must click *Continue without branding* before adding a custom wallpaper.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

61

Choose a ringtone and set the ringtone volume

Sign in to the web interface, and navigate to *Setup > Personalization*, and open the *Ringtones* tab.

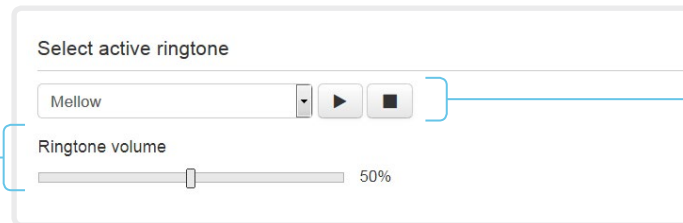**Change the ringtone**

1. Choose a ringtone from the drop-down list.

2. Click *Save* to make it the active ringtone.
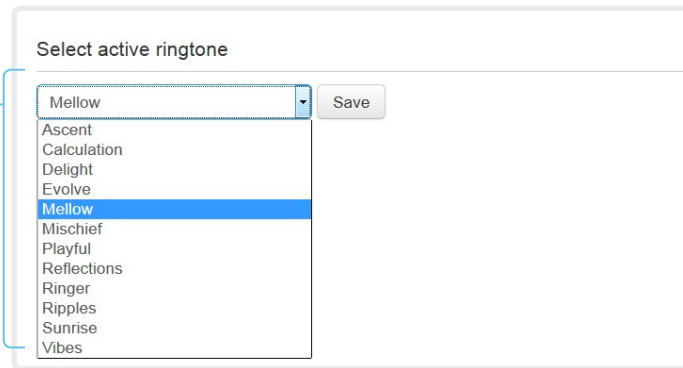
Set the ringtone volume

Use the slide bar to adjust the ringtone volume.

Play back the ringtone

Click the play button (►) to play back the ringtone.

Use the stop button (■) to end the playback.

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 choosen 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.

Manage the Favorites list

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

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.

Favorites

| Search contacts | ✕ | + Add folder | + Add contact | ⊕ Import | ⊕ Export |

| ‹ Back | Favorites | | Edit folder |

Name	Number	
📁 Meeting Rooms		
📁 Sales and Support Offices		
Andrea Carter	andrea@company.com	
Carlos Jiminez	carlos@company.com	
Maria Bartelli	maria@company.com	
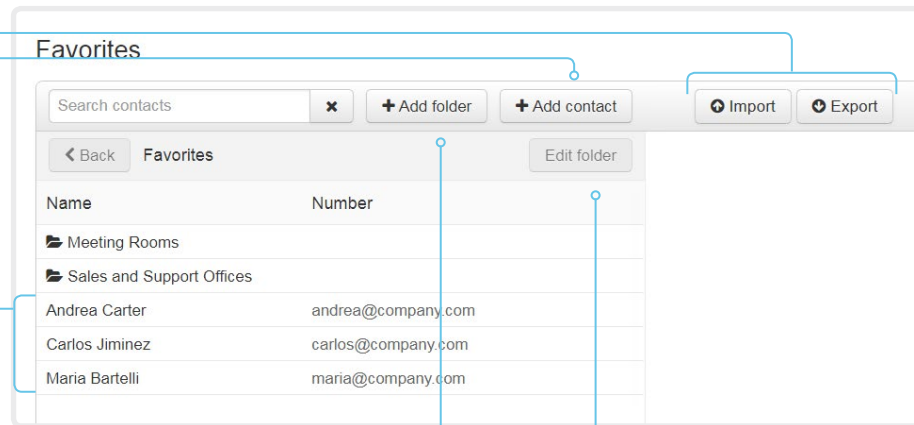
Add or edit a sub-folder

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 a folder's name followed by *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.

Manage Favorites using the video system's user interface

Add a contact in the Favorites list

1. Select *Call* on the home screen.

2. Select the contact you want to add.

3. Select the three dots that appear under the *Call* button on the contact card.

4. Select *Mark as favorite*.

The contact you add will be placed in the top folder. You cannot select or create a sub-folder.

Remove a contact from the Favorites list

1. Select *Call* on the home screen.

2. Select the *Favorites* tab.

3. Select the contact you want to remove.

4. Select the three dots that appear under the *Call* button on the contact card.

5. Select *Unmark as favorite*.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

63

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Set up accessibility features

Flashing screen for incoming calls

To make it easier for the hearing impaired users to notice when someone is calling, the screen can be setup to flash red and gray on incoming calls.

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

2. Go to *UserInterface > Accessibility > IncomingCallNotification* and select **AmplifiedVisuals**.
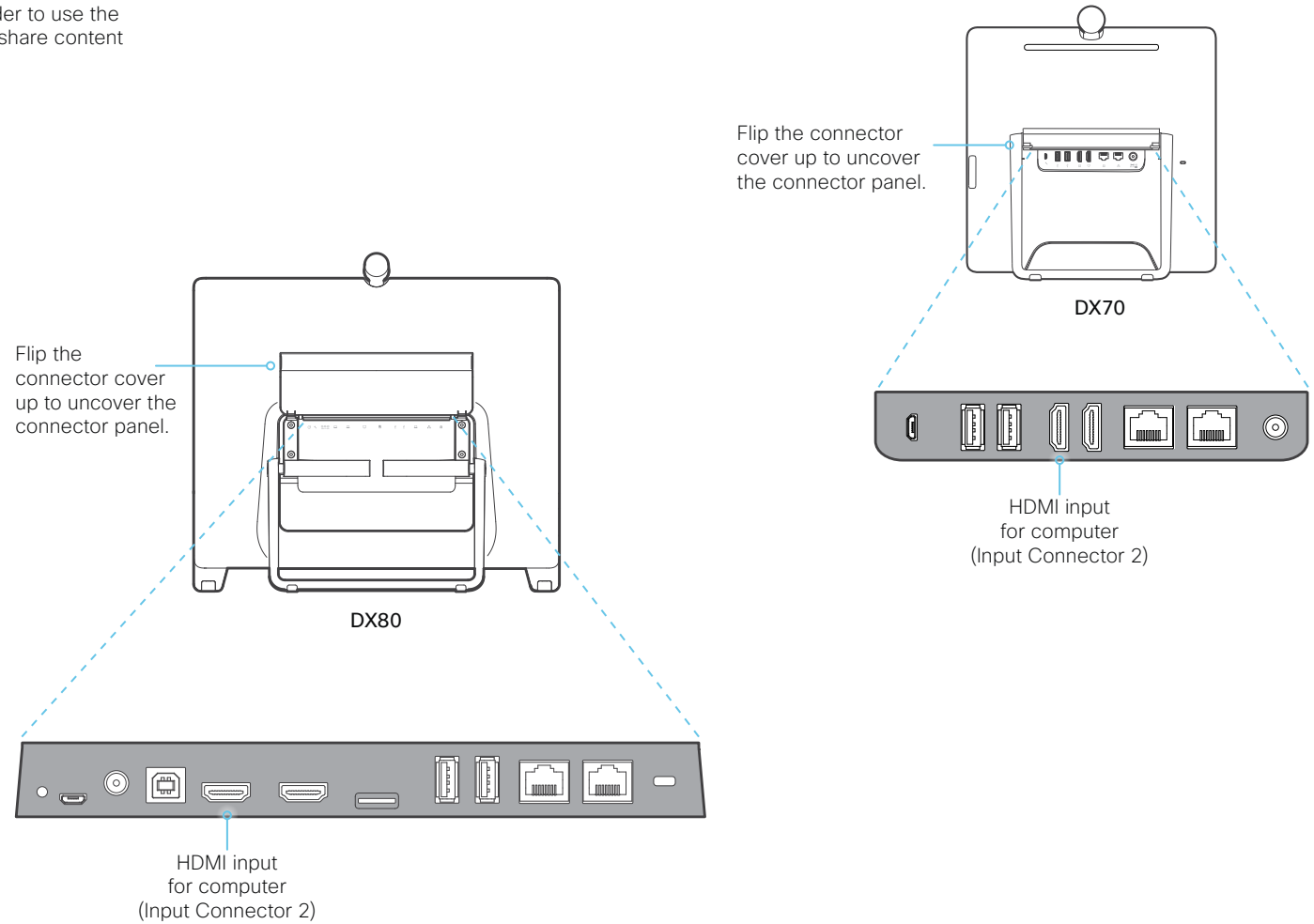
3. Click *Save*.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

64

Chapter 3

Peripherals

    65

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

HDMI input
for computer
(Input Connector 2)

Flip the connector cover up to uncover the connector panel.

DX80

HDMI input
for computer
(Input Connector 2)

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

66

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.
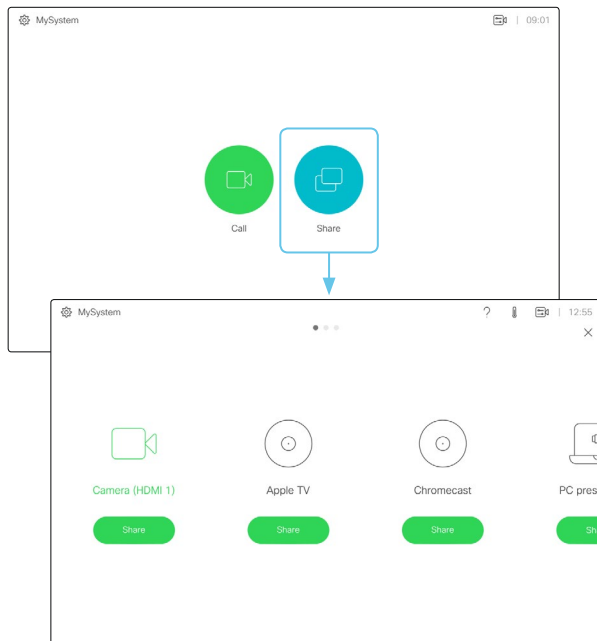
User interface with multiple external input sources (example)

Consult the *Customization 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:

▶ https://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.
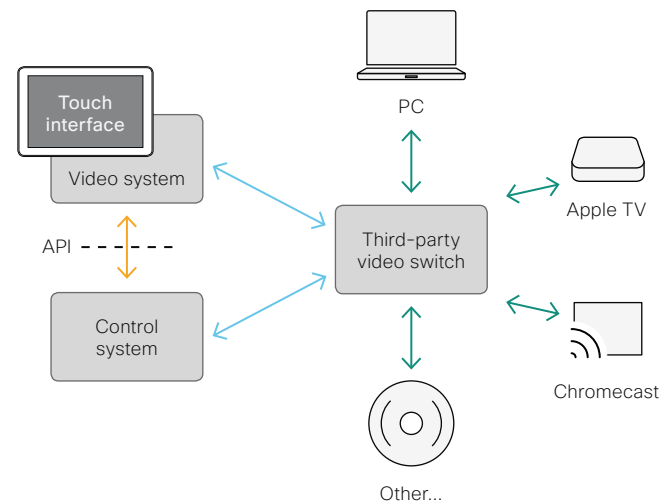
---

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

67

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Bluetooth headset

Bluetooth headset is supported on DX70 and DX80.

- Bluetooth profiles supported:
  - HFP (Hands-Free Profile)
  - A2DP (Advanced Audio Distribution Profile)
  - The headset must support both HFP and A2DP or HFP-only. Headsets with A2DP-only is not supported.
- Bluetooth headset is supported directly with the embedded Bluetooth radio or using a USB Bluetooth dongle.
- Multiple headsets can be paired to the video system, but only one can be connected at a time.
- The range is up to 10 m (30 ft). If you move outside the range when in a call, the audio will switch to the speakers on the video system.
- Most headsets have built in volume controls. When in a call, the volume of the headset and video system is synchronized. When not in a call, the volume buttons on the headset and video system operates independently.

Supported Bluetooth features:

- Answer incoming calls
- Reject incoming calls
- Hang up calls
- Volume up and down
- Some headsets have mute control. This operates independently from the mute control on on video system.

USB Bluetooth dongle

- Using the USB Bluetooth dongle is advisable as it gives better audio quality.
- When using a USB Bluetooth dongle the headset is detected as a USB headset.
- There will be no synchronization of headset volume and video system volume when using a dongle.
- We have tested Jabra Link 360, Plantronics BT300 and Plantronics BT600; though others might work as well.

Pairing a Bluetooth headset

1. Activate Bluetooth pairing on the headset. Refer to the instruction manual for the headset if in doubt.

2. Select the contact information in the upper left corner of the user interface. Select *Settings*, followed by *Bluetooth*. If Bluetooth is disabled, turn it on. Bluetooth is enabled by default.

3. The video system will scan for devices. Upon successful discovery the Bluetooth headset should be displayed in the device list.

4. Select the device and pairing begins. It may take a few seconds for the pairing to complete.

5. If the pairing is successful the video system will now list the headset as connected. The pairing is now completed.

Status bar

USB socket
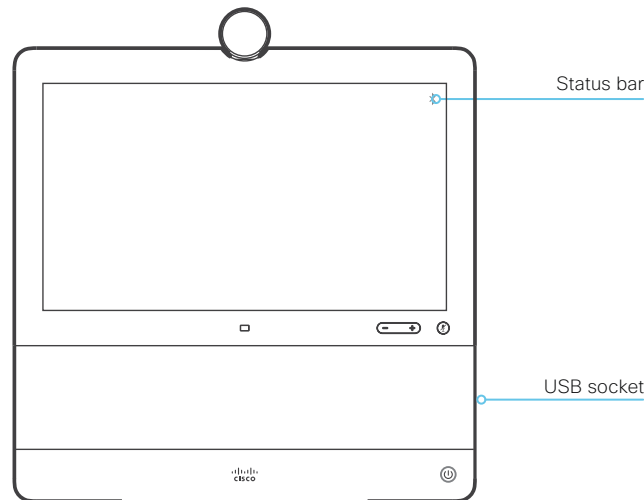
Switch between devices

You can switch between the speaker on the video system and the devices that are connected via Bluetooth or USB.

Select the icon (📞 / 🎧 / 🎧 / 🔊 / ᚼ) in the status bar of the user interface, and choose from the available devices.

🔊 Speakers

🎧 Analog headset (DX70 only)

🎧 USB headset

📞 USB handset

ᚼ Bluetooth device

You may use Bluetooth pairing directly to the video system, or use a USB dongle

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

68

Connect the ISDN Link

The ISDN Link enables a video system to use ISDN lines for connectivity, and enables both video calls and telephone calls over the PSTN (Public Switched Telephone Network).

ISDN Link support ISDN BRI, ISDN PRI and V.35. ISDN can be used in addition to regular IP connectivity for SIP or H.323 calls, or without any IP infrastructure.

ISDN Link is managed from the video systems web interface. Sign in to the web interface, and navigate to *Setup > Peripherals*.

Requirements:

- The ISDN Link must be running IL1.1.7 software or later
- The video system (codec) must be running CE9.3 software or later. The ISDN Link must be re-paired with the video system after the video system has been converted from TC software to CE software.
- The video endpoint must have IPv6 enabled in the web interface or API in order to communicate with the ISDN Link
- Observe the network topology in the ISDN Link Installation Guide in order to guarantee a successful installation
- The video system and ISDN Link must be on the same subnet. If the endpoint or ISDN Link are assigned new IP addresses they will only remain paired as long as they are kept in the same subnet.

Limitations:

- Video systems that are registered to the Cisco Webex cloud service are not able to use ISDN Link.

Setup and configuration

When converting the video system from TC (TC6 or later) to CE software (CE9.3 or later) the ISDN Link will automatically be unpaired due to security reasons.

More information about ISDN Link (Release Notes, Installation Guide, Administrator Guide, API Guide, Compliance and Safety guide) is found here: ► https://www.cisco.com/go/isdnlink-docs

Setup with LAN and direct connection between the video system and ISDN Link

This is the recommended setup. But there are other options, so see the user documentation for additional examples: ► https://www.cisco.com/go/isdnlink-docs

PC/Laptop for system management

LAN

Video system (represented by an SX80 codec)

ISDN Link, rear panel

BRI 1–4   PRI   NET   LAN port   Video system port   Power

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

69

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Chapter 4

Maintenance

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

70
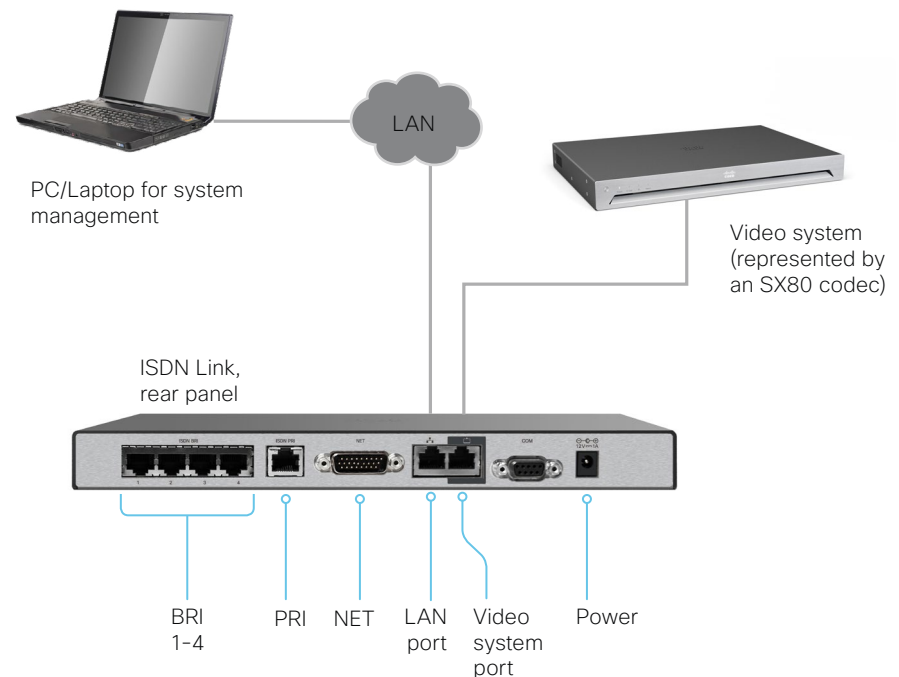
Upgrade the system software (page 1 of 2)

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.

DX80 and DX70 were originally shipped with *Android based software*, but are now shipping 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 CE9.1:

· 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 Webex DX70 and DX80 Convert between CE and Android based software* guide available under *Install and Upgrade Guides* at
► https://www.cisco.com/go/dx-docs

Upgrading from CE8 to CE9

The MultiStream feature with Cisco TelePresence Server is deprecated in CE9.

Also, some features that were available from the touch interface in CE8, are not available in the first CE9 releases. Read the release notes for details before you upgrade.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

71

Upgrade the system software (page 2 of 2)

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

Each software version has a unique file name. Go to the Cisco Download Software web page, and select your product:
► https://software.cisco.com/download/home

The format of the file name:

"s52040ce9_7_x-yyy.pkg"

Where "x" represents the dot release number, and "yyy" represents a unique identifier of the software.

Install new software

Download the appropriate software package and store it on your computer. This is a .pkg file. Don't change the file name.

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.

Software release notes

For a complete overview of the news and changes, we recommend reading the Software Release Notes (CE9).

Go to: ► https://www.cisco.com/c/en/us/support/collaboration-endpoints/desktop-collaboration-experience-dx600-series/tsd-products-support-series-home.html

Install new software

| Software | Browse... | No file selected. |

Detected version ○ Please select a file

[Install software]

Check new software version

When you have selected a file, the software version is shown here

Software download

Go to the Cisco Download Software web page, and select your product: ► https://software.cisco.com/download/home

The SX, MX and DX series can be upgraded from the web interface using PKG files.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

72

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

The video system's serial number

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

Add an 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.

Serial number ....

Option key

Contact your Cisco representative to obtain option keys.
You need to provide the serial number to get option keys.

Add option key

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.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

74

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

Run diagnostics

Click *Re-run diagnostics* to ensure that the list is up to date.

Leave standby mode

Click *Wake up the system* to wake up a video system that is in standby mode.

Diagnostics

Wake up the system   Re-run diagnostics

Diagnostics help identify issues that may cause the system to fail or not work as expected.

CRITICAL: Passphrases
There is one or more users without a passphrase set. Please set a passphrase for all users.

WARNING: System Name
The system has not been configured with a name. Please configure a system name. Note that changing the name of the system requires a reboot.

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

OK: Standby Control
The system goes into standby automatically after 10 minutes. Standby can be configured through the standby configuration.

---

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

75

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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).

Download logs archive...	▼
No call history	
Full call history	
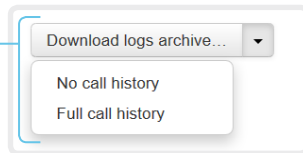
Open/save one log file

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.

Start extended logging...	▼
Include a limited packet capture	
Include a full packet capture	

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.

Current Logs	↻

Historical Logs	↻

Refresh a log file list

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

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.

The system does not have an active Remote Support User.

[Create user] [Delete user]

This user is valid until
2018-10-05 16:50:18

Token

bgD9FjGyIUNn0TB71KcmT1FPnx6uY0vTFy9kpiUa5zl+b
TQek1PaSpsQJNEMfzThgbvK4J7pgOyt4lmCyvxWPGipJQ
GL0ynjvHBvhfqYEsSWwCSSZxQ1wP6bUPQzOSgztZnkOG7
e9CpAoRNg+mZMqEG1lsswKPZ7HYu1vyVTH/XuPzU7Nues
9pwzLc8BFgBt1xV0fKeoeOmMX+it1Ecamln41nXlScgOt
yPSXiFWLdKAJsqHJQHZ0PCxxYcnEUYnNpAoJiD39edLy4
etY+/SAtwBIiohrgF9JLW9FfNEF+IyD1wUmYkPoEirBj7
N3Zvpivlv1Z7+NUalQW9qWTj4Ag==

The system has an active Remote Support User.

[Create user] [Delete user]

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

77

Backup and restore configurations and custom elements

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

You can include custom elements as well as configurations in a backup file (zip-format). You can choose which of the following elements to include in the bundle:

- Branding images
- Macros
- Favorites
- Sign-in banner
- In-room control panels
- Configurations/settings (all or a sub-set)

The backup file can either be restored manually from the video system's web interface, or you can generalize the backup bundle so that it can be provisioned across multiple video systems, for example using Cisco UCM or TMS (see the **next** chapters).

Create a backup file

1. Open the *Create backup* tab.

2. Select the elements you want to include in the backup file.

   Elements that currently don't exist on the video system are greyed out.

3. Select which settings - if any - you want to include in the backup file. Note the following:
   - As default, all settings are included in the backup file.
   - You can remove one or more settings manually by deleting them from the list on the web page.
   - If you want to remove all settings that are specific to one video system, click *Remove system-specific configurations*.

     This is useful if you are going to restore the backup bundle on other video systems.

4. Click *Download backup* to store the elements in a zip-file on your computer.

Restore a backup file

1. Choose the *Restore backup* tab.

2. Click *Browse...* and find the backup file you want to restore.

   All settings and elements in the backup file will be applied.

3. Click *Upload file* to apply the backup.

   Some settings may require that you restart the video system before they take effect.

Additional information

Restoring macros

If a backup file that contains macros is restored on a video system the following applies:

- The macro runtime is started or restarted.
- The macros are automatically activated (started).

Restoring branding images

If a backup bundle contains branding images, the *UserInterface Wallpaper* setting is automatically set to **Auto.**

This means that the branding images will automatically be displayed, possibly replacing a custom wallpaper.

The backup file

The backup file is a zip-file that contains several files. It is important that the files are at the top level within the zip-file, and not include in a folder.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

78

CUCM provisioning of custom elements

A backup file, as described in the ► Backup and restore configurations and custom elements chapter, can be used as a *customization template* for multiple video systems.

The customization template (backup file) may be hosted on either:

- the CUCM TFTP file service, or
- a custom web server that can be reached by the video systems on HTTP or HTTPS.

When a video system get information from CUCM (Cisco Unified Communications Manager) about the name and location of a customization template, the video system will contact the server, download the file, and restore the custom elements.

ⓘ Configurations will not be restored on the video system, even if they are part of the backup file that you use as a customization template.

Upload a customization template to the TFTP file server

1. Sign in to *Cisco Unified OS Administration.*

2. Navigate to *Software Upgrades > TFTP File Management*.

3. Click *Upload File*. Enter the name and path of the customization template in the input field.

4. Click *Upload File*.

Add customization provisioning information for each video system

1. Sign in to *Cisco Unified CM Administration.*

2. Navigate to *Device > Phone*.

3. Fill in the **Customization Provisioning** fields in the product specific configuration section of the relevant devices:

   - *Customization File:* The customization template file name (for example: backup.zip) *

   - *Customization Hash Type:* **SHA512**

   - *Cutomization Hash:* The SHA512 checksum for the customization template.

   If these fields are not present, you must install a newer Device Package on CUCM.

4. Click *Save* and *Apply Config* to push the configuration to the video systems.

_____

* If not using the TFTP Service, you must enter the complete URI for the customization template: `<hostname>:<portnumber>/<path-and-filename>`

For example:
- http://host:6970/backup.zip, or
- https://host:6971/backup.zip

SHA512 checksum

Tip! You can find the SHA512 checksum of a file by restoring it to a video system using its web interface.

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

2. Choose the *Restore backup* tab.

3. Click *Browse...* and find the file you want to calculate the checksum for.

   Then you can see the SHA512 checksum at the bottom of the page.

CUCM documentation

► https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html

TMS provisioning of custom elements

A backup file, as described in the ► Backup and restore configurations and custom elements chapter, can be used as a *customization template* for multiple video systems.

The backup file must be hosted on a custom web server that can be reached by the video systems on HTTP or HTTPS.

When a video system get information from TMS (TelePresence Management Suite) about the name and location of the backup file, the video system will contact the server, download the file, and restore the custom elements.

Create and apply a configuration template

1. Create a configurations template.

2. Add a custom command containing the following XML string in the configuration template:

```
<Command>
  <Provisioning>
    <Service>
      <Fetch>
        <URL>web-server-address</URL>
        <Checksum>checksum</Checksum>
        <Origin>origin</Origin>
      </Fetch>
    </Service>
  </Provisioning>
</Command>
```

where

web-server-address: The URI to the backup file (for example, http://host/backup.zip).

checksum: The SHA512 checksum of the backup file.

origin: **Provisioning** [*]

3. Select the video systems you want to push the configuration template to, and click *Set on systems*.

Read the ► Cisco TMS administrator guide for details how to create TMS configurations templates and make custom commands.

SHA512 checksum

Tip! You can find the SHA512 checksum of a file by restoring it to a video system using its web interface.

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

2. Choose the *Restore backup* tab.

3. Click *Browse...* and find the file you want to calculate the checksum for.

   Then you can see the SHA512 checksum at the bottom of the page.

---

[*] If not setting this parameter to **Provisioning**, also configurations that are part of the backup file will be pushed to the video system. If the backup file contains configurations that are specific to one video system, for example static IP addresses, system name, and contact information, you may and up with video systems that you cannot reach.

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, configurations, and custom elements of the video system before you swap to the previously used software image.

Back up log files, configurations and custom elements

1. Select the *Backup* tab.

2. Click *Download logs* and follow the instructions to save the log files on your computer.

3. Click *Download backup* and follow the instructions to save the backup bundle 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

81

Factory reset the video system (page 1 of 4)

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 or user interface to factory reset the video system. If these interfaces are not available, use the reset pin-hole 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, 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.

We recommend that you back up the log files, configurations, and custom elements of the video system before you perform a factory reset; otherwise these data will be lost.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

82

Factory reset the video system (page 2 of 4)

Factory reset using the web interface

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

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

1. Select the *Factory Reset* tab, and read the provided information carefully.

2. Click *Perform a factory reset…*.

3. Click *Yes* to confirm your choice, or *Cancel* if you have changed your mind.

4. Wait while the video system reverts to the default factory settings. When finished, the video system restarts automatically. This may take a few minutes.
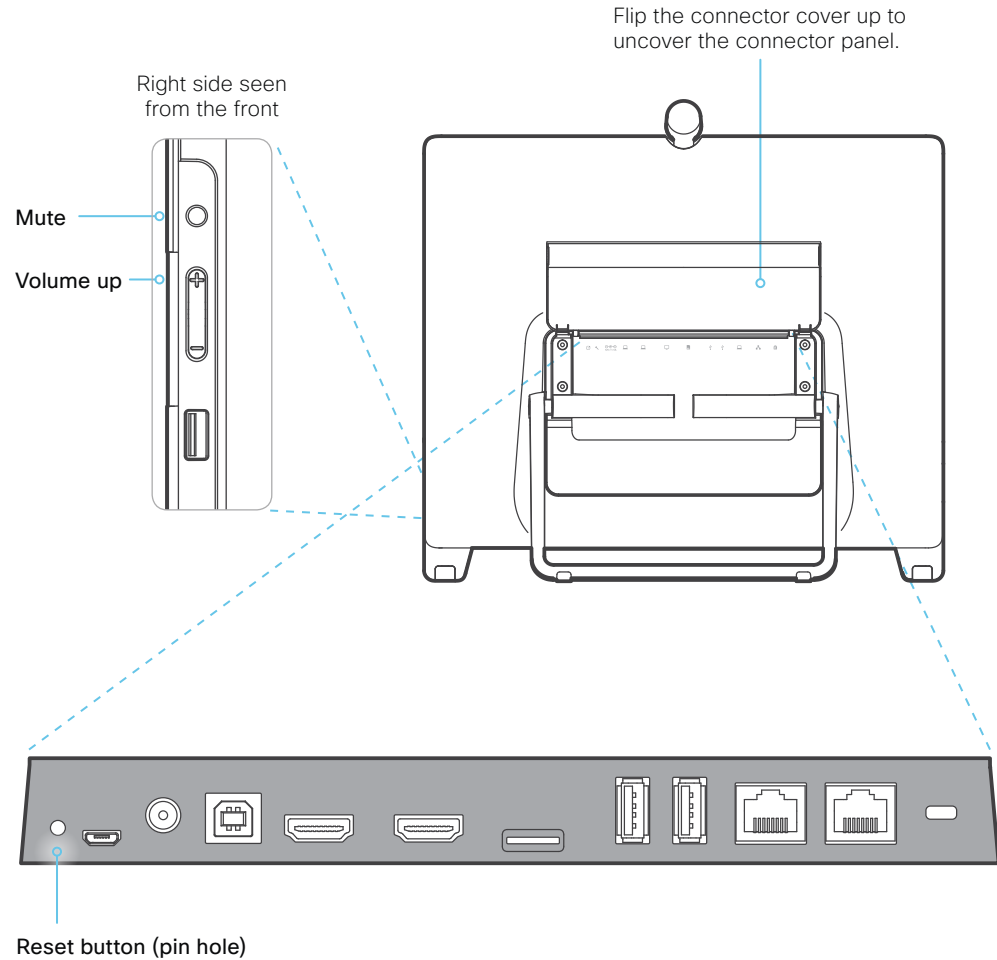
   When the system has been successfully reset to factory settings, the Setup assistant starts with the *Welcome* screen.

Factory reset from the user interface

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

1. Select the contact information in the upper left corner of the user interface.

2. Select *Settings*.

3. Select *Factory reset*.

4. Select *Reset* to confirm your choice, or *Back* if you have changed your mind.

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

   When the system has been successfully reset to factory settings, the Setup assistant starts with the *Welcome* screen.

Back up log files, configurations, and custom elements

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

Back up log files, configurations, and custom element

1. Select the *Backup* tab.

2. Click *Download logs* and follow the instructions to save the log files on your computer.

3. Click *Download backup* and follow the instructions to save the backup bundle on your computer.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

83

Factory reset the video system (page 3 of 4)

We recommend that you back up the log files and configuration of the video system before you continue with the factory reset.
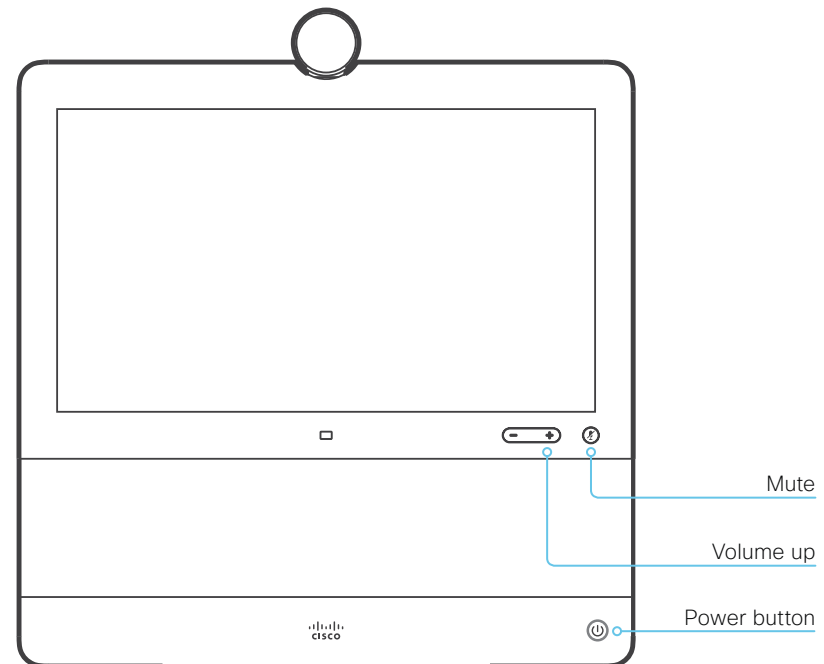
Factory reset DX80 using the mute and volume buttons

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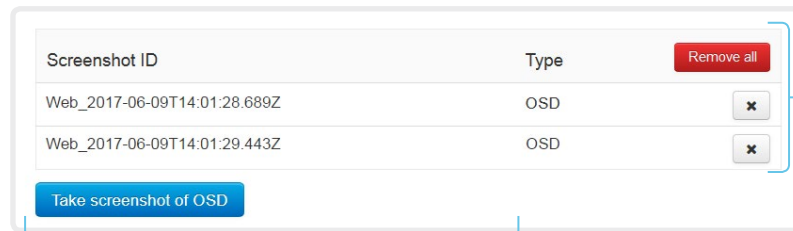
   Wait while the video system reverts to the default factory settings. The video system restarts automatically when finished. This may take a few minutes.

   When the system has been successfully reset to factory settings, the Setup assistant starts and you will see the *Welcome* screen.

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.

Flip the connector cover up to uncover the connector panel.

Right side seen from the front

Mute

Volume up

Reset button (pin hole)

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

84

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Factory reset the video system (page 4 of 4)

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.

Mute

Volume up

Power button

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

85

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Capture user interface screenshots

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

About user interface screenshots

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

Delete screenshots

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

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

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

86

Chapter 5

System settings

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

87

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.

ℹ **How to find the IP address**

1. Select the contact information in the upper left corner of the user interface.

2. Select *Settings*, followed by *About this device*.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

88

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

90

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

91

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

92

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 user interface 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, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

> Range: 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 Input MicrophoneMode

This setting applies only 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, INTEGRATOR

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.

Audio Microphones Mute Enabled

Define the microphone mute behavior on the video system.

Requires user role: ADMIN, INTEGRATOR

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, INTEGRATOR, 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, INTEGRATOR, USER

Default value: 50

Value space: Integer (0..100)

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

93

Audio Ultrasound Mode

This setting applies to the Intelligent Proximity feature. Keep the setting at its default value.

Requires user role: ADMIN, INTEGRATOR
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 Audio Ultrasound Volume MaxVolume setting.
Static: Use only if advised by Cisco.

Audio Ultrasound MaxVolume

This setting applies to the Intelligent Proximity feature. Set the maximum volume of the ultrasound pairing message.

Requires user role: ADMIN, INTEGRATOR
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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

94

Bluetooth settings

Bluetooth Allowed

The video system has a built-in Bluetooth module. As a default, the user can turn it on or off using the user interface. With this setting, the administrator can disable Bluetooth configuration, so that it cannot be set up from the user interface.

Requires user role: ADMIN

Default value: True

Value space: False/True

False: Bluetooth is switched off by the administrator, and the user cannot turn it on from the user interface.

True: Bluetooth is allowed. The user can turn it on or off from the user interface.

Bluetooth Enabled

Provided that Bluetooth connections are allowed (see the Bluetooth Allowed setting), you can use this setting to enable and disable Bluetooth. The video system supports the HFP (Hands-Free Profile) and A2DP (Advanced Audio Distribution Profile) profiles. Headsets that only supports A2DP cannot be used.

Requires user role: ADMIN

Default value: False

Value space: False/True

False: Bluetooth is disabled, and no Bluetooth devices can pair with the video system.

True: Bluetooth is enabled, and you can pair and use a Bluetooth headset.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

95

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, INTEGRATOR

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

96

Cameras settings

Cameras Camera [n] Backlight DefaultMode

n: 1..1

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

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

    Off: Turn off the camera backlight compensation.

    On: Turn on the camera backlight compensation.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

97

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 can answer incoming calls manually by tapping Answer.

On: The system automatically answers incoming calls, except if you are already in a call. You can 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, H323).

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

98

Conference DefaultCall Protocol

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

Requires user role: ADMIN

Default value: Auto

Value space: Auto/H320/H323/Sip/Spark

Auto: Enables auto-selection of the call protocol based on which protocols are available. If multiple protocols are available, the order of priority is: 1) SIP; 2) H323; 3) H320. If the system cannot register, the auto-selection chooses H323.

H320: All calls are set up as H.320 calls (only applicable if used with Cisco TelePresence ISDN Link).

H323: All calls are set up as H.323 calls.

Sip: All calls are set up as SIP calls.

Spark: Reserved for Webex registered systems. Do not use.

Conference DefaultCall Rate

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

Requires user role: ADMIN, INTEGRATOR

Default value: 3072

Value space: Integer (64..3072)

The default call rate (kbps).

Conference DoNotDisturb DefaultTimeout

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

Requires user role: ADMIN, INTEGRATOR

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 FarEndControl Mode

Lets you decide if the remote side (far end) should be allowed to select your video sources and control your local camera (pan, tilt, zoom).

Requires user role: ADMIN

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

99

Conference FarEndControl SignalCapability

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 FarEndMessage Mode

Toggle whether it is allowed to send data between two codecs in a point-to-point call, for use with control systems or macros. Works with SIP calls only. This setting will enable/disable the use of the xCommand Call FarEndMessage Send command.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

    Off: It is not possible to send messages between two codecs.

    On: It is possible to send messages between two codecs in a point-to-point call.

Conference MaxReceiveCallRate

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 MaxTotalReceiveCallRate 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 transmitt 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).

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

100

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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: NoAction/Stop

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.

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.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

101

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

FacilityService settings

FacilityService Service [n] Type

n: 1..5

Up to five different facility services can be supported simultaneously. With this setting you can select what kind of services they are. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Helpdesk

Value space: Catering/Concierge/Emergency/Helpdesk/Security/Transportation/Other

Catering: Select this option for catering services.

Concierge: Select this option for concierge services.

Emergency: Select this option for emergency services.

Helpdesk: Select this option for helpdesk services.

Security: Select this option for security services.

Transportation: Select this option for transportation services.

Other: Select this option for services not covered by the other options.

FacilityService Service [n] Name

n: 1..5

Define the name of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. The name will show on the facility service call button, which appears when you tap the question mark icon in the top bar. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Service 1: "Live Support"   Other services: ""

Value space: String (0, 1024)

The name of the facility service.

FacilityService Service [n] Number

n: 1..5

Define the number (URI or phone number) of the facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 1024)

The number (URI or phone number) of the facility service.

FacilityService Service [n] CallType

n: 1..5

Define the call type for each facility service. Up to five different facility services are supported. A facility service is not available unless both the FacilityService Service [n] Name and the FacilityService Service [n] Number settings are properly set. Facility services are available from the user interface.

Requires user role: ADMIN, INTEGRATOR

Default value: Video

Value space: Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

102

H323 settings

H323 Authentication Mode

Define the authenticatin 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: Max1024bit/Min1024bit/Min2048bit

Max1024bit: The maximum size is 1024 bit.

Min1024bit: The minimum 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

104

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 PortAllocation

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].

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

105

HttpClient settings

HttpClient Mode

Allow or prohibit communication with an external HTTP(S) server using HTTP(S) requests and responses.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

    Off: The video system cannot communicate with an external HTTP(S) server.

    On: The video system is allowed to communicate with an external HTTP(S) server.

HttpClient AllowHTTP

The HttpClient Mode setting is used to allow or prohibit communication with an external HTTP(S) server. The Mode setting does not distinguish between HTTP and HTTPS. You must use the HttpClient AllowHTTP setting to further allow or prohibit the use of HTTP.

Requires user role: ADMIN

Default value: True

Value space: False/True

    False: The video system can communicate only over HTTPS.

    True: The video system can communicate over both HTTPS and HTTP.

HttpClient AllowInsecureHTTPS

You can choose whether or not to allow the video system to communicate with a server over HTTPS without checking the server's certificate first.

Even if the video system is allowed to skip the certificate validation process, it doesn't automatically do it. You must specifically set the AllowInsecureHTTPS parameter in each xCommand HttpClient command for data to be exchanged with the server without certificate validation.

Requires user role: ADMIN

Default value: False

Value space: False/True

    False: The video system always checks that the HTTPS server has a valid certificate. No communication with the server takes place if the certificate validation fails.

    True: The video system is allowed to skip the certificate validation process before communicating with the server.

Logging settings

Logging Debug Wifi

When this option in enabled, the video system logs more information about the set-up and maintenance of the Wi-Fi connection between the video system and the access point. This may be useful when you are troubleshooting Wi-Fi connection issues. We recommend that this setting is Off if the Wi-Fi connection is working as expected.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: Logging only basic Wi-Fi information.

On: Logging a large amount of information about the Wi-Fi connection.

Logging External Mode

Determine whether or not to store the system logs on a remote syslog server. This setting has no effect if the Logging Mode setting is set to Off.

You must enter the address of the remote server in the Logging External Server Address setting. Unless otherwise specified in the Logging External Server Port setting, the standard syslog port is used.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: System logs will not be stored on the remote syslog server.

On: System logs will be stored on the 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, 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

107

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Logging Internal Mode

Determine whether or not to store the system logs on the video system (local files). These are the files that you get when you download the log bundles from the video system. This setting has no effect if the Logging Mode setting is set to Off.

Requires user role: ADMIN

Default value: On

Value space: Off/On

   Off: System logs will not be stored on the video system.

   On: System logs will be stored on the video system.

Logging Mode

Define the logging mode for the video system (syslog service). When disabled, the syslog service does not start, and most of the systema and audit 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.

Macros settings

Macros Mode

Macros allow you to write snippets of JavaScript code that can automate parts of your video endpoint, thus creating custom behavior. Use of macros is disabled by default, but the first time you open the Macro Editor you will be asked whether to enable use of macros on the codec. Use this setting when you want to manually enable, or to permanently disable the use of macros on the codec. You can disable the use of macros within the Macro Editor. But this will not permanently disable macros from running, because every time the codec is reset the macros will be re-enabled automatically.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

    Off: Permanently disable the use of macros on this video system.

    On: Enable the use of macros on this video system.

Macros AutoStart

All the macros run in a single process on the video endpoint, called the macro runtime. It should be running by default, but you can choose to stop and start it manually. If you restart the video system, the runtime will automatically start again if auto start is enabled.

Requires user role: ADMIN

Default value: On

Value space: Off/On

    Off: The macro runtime will not start automatically after a restart of the video system.

    On: The macro runtime will start automatically after a restart of the video system.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

109

Network settings

Network [n] DNS DNSSEC Mode

n: 1..1

Domain Name System Security extensions (DNSSEC) is a set of extensions to DNS. It is used to authenticate DNS replies for zones that are signed. It will still allow unsigned zones.

Requires user role: ADMIN
Default value: Off

Value space: Off/On
    Off: Disable Domain Name System Security Extensions.
    On: Enable Domain Name System Security Extensions.

Network [n] DNS Domain Name

n: 1..1

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.

Network [n] DNS Server [m] Address

n: 1..1

m: 1..3

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 [n] IEEE8021X Mode

n: 1..1

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.
    On: The 802.1X authentication is enabled.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

110

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Network [n] IEEE8021X TlsVerify

n: 1..1

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.

Network [n] IEEE8021X UseClientCertificate

n: 1..1

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 [n] IEEE8021X Identity

n: 1..1

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 [n] IEEE8021X Password

n: 1..1

Define the password for 802.1X authentication.

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

Value space: String (0, 50)
The password for 802.1X authentication.

Network [n] IEEE8021X AnonymousIdentity

n: 1..1

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.

Network [n] IEEE8021X Eap Md5

n: 1..1

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.

Network [n] IEEE8021X Eap Ttls

n: 1..1

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.

Network [n] IEEE8021X Eap Tls

n: 1..1

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.

Network [n] IEEE8021X Eap Peap

n: 1..1

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.

Network [n] IPStack

n: 1..1

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

112

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Network [n] IPv4 Assignment

n: 1..1

Define how the system will obtain its IPv4 address, subnet mask and gateway address.

When using DHCP for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

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 [n] IPv4 Address

n: 1..1

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 [n] IPv4 Gateway

n: 1..1

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 [n] IPv4 SubnetMask

n: 1..1

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 [n] IPv6 Assignment

n: 1..1

Define how the system will obtain its IPv6 address and the default gateway address.

When using DHCPv6 for address assignment, "01" appended by the MAC address is used as client identifier in DHCP requests.

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 [n] IPv6 Address

n: 1..1

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

Network [n] IPv6 Gateway

n: 1..1

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 [n] IPv6 DHCPOptions

n: 1..1

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 [n] MTU

n: 1..1

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 [n] QoS Mode

n: 1..1

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

114

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Network [n] QoS Diffserv Audio

n: 1..1

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. 0 means "best effort".

Network [n] QoS Diffserv Video

n: 1..1

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. 0 means "best effort".

Network [n] QoS Diffserv Data

n: 1..1

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. 0 means "best effort".

Network [n] QoS Diffserv Signalling

n: 1..1

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. 0 means "best effort".

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

115

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Network [n] QoS Diffserv ICMPv6

n: 1..1

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. 0 means "best effort".

Network [n] QoS Diffserv NTP

n: 1..1

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. 0 means "best effort".

Network [n] RemoteAccess Allow

n: 1..1

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 [n] Speed

n: 1..1

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 auto-negotiation, make sure that the speed you choose is supported by the closest switch in your network infrastructure.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/10half/10full/100half/100full/1000full

Auto: Auto-negotiate link speed.

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

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

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

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

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

Network [n] TrafficControl Mode

n: 1..1

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 [n] VLAN Voice Mode

n: 1..1

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 NetworkServices 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 [n] VLAN Voice VlanId

n: 1..1

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.

NetworkPort settings

NetworkPort [n] Mode

n: 2..2

The video system has two network ports. The first network port is for connecting the video system to Ethernet LAN. The second network port (also called the computer network port) allows you to connect a computer to the Ethernet LAN via the video system. In this way, you only need one network wall socket to support both the video system and the computer.

If the video system is used in a public environment we recommend that you disable this network port, to prevent people from connecting a computer to your network through the video system.

You have to restart the video system for any change to this setting to take effect.

Requires user role: ADMIN

Default value: On

Value space: Off/On

Off: The computer network port is disabled.

On: The computer network port is available for use.

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.

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.

For additional security (encryption and decryption of requests and pages that are returned by the web server), allow only HTTPS.

Note: The default value is HTTP+HTTPS for video systems that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the video system has not been factory reset after the upgrade.

Requires user role: ADMIN

Default value: HTTPS (changed from HTTP+HTTPS to HTTPS in CE9.4)

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 HTTP Proxy LoginName

This is the user name part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 80)

    The authentication login name.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

119

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

NetworkServices HTTP Proxy Password

This is the password part of the credentials for authentication towards the HTTP proxy. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0, 64)

   The authentication password.

NetworkServices HTTP Proxy Mode

The HTTP proxy for Cisco Webex can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

Requires user role: ADMIN, USER

Default value: Off

Value space: Manual/Off/PACUrl/WPAD

   Manual: Enter the address of the proxy server in the NetworkServices HTTP Proxy URL setting. Optionally, also add the HTTP proxy login name and password in the NetworkServices HTTP Proxy LoginName/Password settings.

   Off: The HTTP proxy mode is turned off.

   PACUrl: The HTTP proxy is auto-configured. You must enter the URL for the PAC (Proxy Auto Configuration) script in the NetworkServices HTTP Proxy PACUrl setting.

   WPAD: With WPAD (Web Proxy Auto Discovery) the HTTP proxy is fully automated and auto-configured.

NetworkServices HTTP Proxy Url

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

   The URL of the HTTP proxy server.

NetworkServices HTTP Proxy PACUrl

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

Requires user role: ADMIN, USER

Default value: ""

Value space: String (0..255)

   The URL of the PAC (Proxy Auto Configuration) script.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

120

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

NetworkServices HTTPS Server MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.1

Value space: TLSv1.1/TLSv1.2

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

NetworkServices HTTPS StrictTransportSecurity

The HTTP Strict Transport Security header lets a web site inform the browser that it should never load the site using HTTP and should automatically convert all attempts to access the site using HTTP to HTTPS requests instead.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

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 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

121

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

NetworkServices NTP Server [n] Address

n: 1..3

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 NTP Server [n] Key

n: 1..3

To make sure that the NTP information comes from a trusted source, the video system must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 2045)

The key, which is part of the ID/key pair that the NTP source uses.

NetworkServices NTP Server [n] KeyId

n: 1..3

To make sure that the NTP information comes from a trusted source, the video system must know the ID/key pair that the NTP source uses. Use the NetworkServices NTP Server [n] Key and NetworkServices NTP Server [n] KeyId settings for the key and ID respectively.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 10)

The ID, which is part of the ID/key pair that the NTP source uses.

NetworkServices NTP Server [n] KeyAlgorithn

n: 1..3

Choose the authentication hash function that the NTP server uses, and that the video system must use to authenticate the time messages.

Requires user role: ADMIN

Default value: ""

Value space: None/SHA1/SHA256

None: The NTP server doesn't use a hash function.

SHA1: The NTP server uses the SHA-1 hash function.

SHA256: The NTP server uses the SHA-256 hash function (from the SHA-2 family of hash functions).

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.

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, INTEGRATOR

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 [n] Address

n: 1..3

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, INTEGRATOR

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, INTEGRATOR

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, INTEGRATOR

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, INTEGRATOR

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 HostKeyAlgorithm

Choose the cryptographic algorithm that shall be used for the SSH host key. Choices are RSA (Rivest–Shamir–Adleman) with 2048 bits keysize, ECDSA (Elliptic Curve Digital Signature Algorithm) with NIST curve P–384, and EdDSA (Edwards–curve Digital Signature Algorithm) with ed25519 signature schema.

Requires user role: ADMIN

Default value: RSA

Value space: ECDSA/RSA/ed25519

ECDSA: Use the ECDSA algorithm (nist–384p).

RSA: Use the RSA algorithm (2048 bits).

ed25519: Use the ed25519 algorithm.

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 Websocket

It is possible to interact with the API of the video system over the WebSocket protocol, both the insecure and secure versions (ws and wss). A WebSocket is tied to HTTP, so that also HTTP or HTTPS must be enabled before you can use WebSockets (see the NetworkServices HTTP Mode setting).

Requires user role: ADMIN

Default value: Off

Value space: FollowHTTPService/Off

FollowHTTPService: Communication over the WebSocket protocol is allowed when HTTP or HTTPS is enabled.

Off: Communication over the WebSocket protocol is not allowed.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

124

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

NetworkServices Wifi Allowed

Video systems that have a built-in Wi-Fi adapter, can connect to the network either via Ethernet or Wi-Fi. Both Ethernet and Wi-Fi are allowed by default, and the user can choose which one to use from the user interface. With this setting, the administrator can disable Wi-Fi configuration, so that it cannot be set up from the user interface.

The systems support the following standards: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, and IEEE 802.11n. The system supports the following security protocols: WPA-PSK (AES), WPA2-PSK (AES), EAP-TLS, EAP-TTLS, EAP-FAST, PEAP, EAP-MSCHAPv2, EAP-GTC, and open networks (not secured).

If the PID (Product ID), found on the rating label at the rear of the video system, contains the letters NR (No Radio) the system does not support Wi-Fi.

Requires user role: ADMIN, USER

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, USER

Default value: True

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.

Peripherals settings

Peripherals InputDevice Mode

Define whether or not to allow the use of a third-party input device, such as a USB keyboard or a wireless remote control with a USB dongle. The input device must advertise itself as a USB keyboard. You must define and implement the actions to be taken as response to key clicks yourself.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

Off: A third-party USB input device is not allowed.

On: A third-party USB input device can be used to control certain functions on the video system.

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, INTEGRATOR

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

126

Phonebook settings

Phonebook Server [n] ID

n: 1..1

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 [n] Pagination

n: 1..1

Configure if the phonebook server supports pagination (paging) or not. Pagination means that the server supports consecutive searches, and these searches can be relative to an offset. This allows the user interface to perform as many consecutive searches as required to get the complete search result.

If Pagination is Disabled the video system does a single search and returns a maximum of 100 entries in the search result. It is not possible to scroll to any further search results beyond that.

Requires user role: ADMIN

Default value: Enabled

Value space: Disabled/Enabled

    Disabled: The phonebook server does not support pagination. The video system does a single search, and the maximum number of entries in the search result is 100.

    Enabled: The phonebook server supports pagination.

Phonebook Server [n] Type

n: 1..1

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 in the Cisco Webex cloud service.

    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 [n] URL

n: 1..1

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 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 selected 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.

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/Webex/TMS/VCS

Off: The video system is not configured by a provisioning system.

Auto: The provisioning server is automatically selected as set up in the DHCP 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 Expressway infrastructure. In order to register over Expressway the encryption option key must be installed on the video system.

Webex: Push configurations to the video system from the Cisco Webex cloud service.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

129

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

130

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

131

RoomReset settings

RoomReset Control

This setting is for use with control systems or macros. Macros allow you to write snippets of JavaScript code that can automate parts of your video endpoint, thus creating custom behavior.

When a room has been idle for some time the system can send an event to indicate that the room is ready to be reset.

The events that are sent when this setting is enabled are:

*e RoomReset SecondsToReset: 30

** end

*e RoomReset Reset

** end

Requires user role: ADMIN

Default value: On

Value space: CameraPositionsOnly/Off/On

    CameraPositionsOnly: Not applicable.

    Off: No RoomReset events will be sent.

    On: The room reset control is enabled and RoomReset events will be sent.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

132

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

RTP settings

RTP Ports Range Start

Define the first port in the range of RTP ports.

As default, the system is using the ports in the range 2326 to 2486 for RTP and RTCP media data. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

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 ports in the range 2326 to 2487 for RTP and RTCP media data. If the RTP Video Ports Range is enabled the system is using the ports in the range 1024 to 65436. The minimum range is 100 when RTP Video Ports Range is disabled, and 20 when RTP Video Ports Range is enabled.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 2486

Value space: Integer (1120..65535)

Set the last port in the range of RTP ports.

RTP Video Ports Range Start

Define the first port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65454)

Set the first port in the range of RTP video ports.

RTP Video Ports Range Stop

Define the last port in the range of RTP video ports.

If both the start and stop values are set to 0, the RTP Video Ports Range is disabled. To enable it, set the first port to a value between 1024 and 65454 and the last port between 1024 and 65535. The minimum range is 80.

If the RTP Video Ports Range is enabled, audio will use the range defined by the RTP Ports Range settings, and other media data will use the range defined by the RTP Video Ports Range settings. The two ranges must not overlap.

A change in the setting will take effect on new calls.

Requires user role: ADMIN

Default value: 0

Value space: Integer (0, 1024..65535)

Set the last port in the range of RTP video ports.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

133

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Security settings

Security Audit Logging Mode

Define where to record or transmit the audit logs. The audit logs are sent to a syslog server. This setting has no effect if the Logging Mode setting is set to Off.

When using the External or ExternalSecure mode you must enter the address of the audit server in the Security Audit Server Address setting.

Requires user role: AUDIT

Default value: Internal

Value space: External/ExternalSecure/Internal/Off

　　External: The system sends the audit logs to an external syslog server. The syslog server must support UDP.

　　ExternalSecure: The video 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 video system using the web interface. The common_name parameter of a certificate in the CA list must match the IP address or DNS name of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages.

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

　　Off: No audit logging is performed.

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

Set the IP address or DNS name of the syslog server that the audit logs are sent to. 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, IPv6 address, or DNS name.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

134

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 Setup > 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 FailedLoginsLockoutTime

Define how long the system will lock out a user after failed login to a web or SSH session.

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

Requires user role: ADMIN

Default value: 60

Value space: Integer (0..10000)

Set the lockout time (minutes).

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 MaxFailedLogins

Define the maximum number of failed login attempts per user for a web or SSH session. If the user exceeded the maximum number of attempts the user will be locked out. 0 means that there is no limit for failed logins.

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

Requires user role: ADMIN

Default value: 0

Value space: Integer (0..10)

Set the maximum number of failed login attempts per user.

Security Session MaxSessionsPerUser

The maximum number of simultaneous sessions per user is 20 sessions.

Requires user role: ADMIN

Default value: 20

Value space: Integer (1..20)

Set the maximum number of simultaneous sessions per user.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

135

Security Session MaxTotalSessions

The maximum number of simultaneous sessions in total is 20 sessions.

Requires user role: ADMIN
Default value: 20

Value space: Integer (1..20)
    Set the maximum number of simultaneous sessions in total.

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
    On: Show information about the last session.
    Off: Do not show information about the last session.

SerialPort settings

SerialPort Mode

Enable/disable the serial port.

Requires user role: ADMIN, INTEGRATOR
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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

137

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: Auto/TCP/Tls/UDP

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

138

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 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 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.

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). As a security measure, SIP ListenPort should be Off when the endpoint is registered to a SIP Proxy.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

139

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

SIP MinimumTLSVersion

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

Requires user role: ADMIN

Default value: TLSv1.0

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.

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.

IPv6: The preferred IP version for signaling is IPv6.

SIP Proxy [n] Address

n: 1..4

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

140

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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).
    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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

141

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Standby settings

Standby Control

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

Requires user role: ADMIN, INTEGRATOR

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, INTEGRATOR

Default value: 10

Value space: Integer (1..480)

Set the standby delay (minutes).

Standby WakeupOnMotionDetection

Automatic wake up on motion detection is a feature that will sense when a person walks into
the room. The feature is based on ultrasound detection.

Requires user role: ADMIN, INTEGRATOR

Default value: Off

Value space: Off/On

Off: The wake up on motion detection is disabled.

On: When people walk into the room the system will automatically wake up from standby
(only applicable to DX80).

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

142

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.

SystemUnit CrashReporting Advanced

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

    Off: The ACR tool will perform standard log analyses.

    On: The ACR tool will perform advanced log analyses.

SystemUnit CrashReporting Mode

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: Off

Value space: Off/On

    Off: No logs will be sent to ACR tool.

    On: The logs will automatically be sent to ACR tool.

SystemUnit CrashReporting Url

If the video system (codec) crashes, the system can automatically send logs to the Cisco Automatic Crash Report tool (ACR) for analyses. The ACR tool is for Cisco internal usage only and not available to customers.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

    The URL to the Cisco Automatic Crash Report tool (ACR).

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

143

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 DateFormat

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, INTEGRATOR, 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/Blantyre, Africa/Brazzaville, Africa/Bujumbura, Africa/Cairo, Africa/Casablanca, Africa/Ceuta, Africa/Conakry, Africa/Dakar, Africa/Dar_es_Salaam, Africa/Djibouti, Africa/Douala, Africa/El_Aaiun, Africa/Freetown, Africa/Gaborone, Africa/Harare, Africa/Johannesburg, Africa/Juba, Africa/Kampala, Africa/Khartoum, Africa/Kigali, Africa/Kinshasa, Africa/Lagos, Africa/Libreville, 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-Novo, 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/Belize, 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/Eirunepe, 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/Juneau, 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/Metlakatla, 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/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, 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/Yakutat, America/Yellowknife, Antarctica/Casey, 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/Choibalsan, 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/Kabul, 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/Omsk, Asia/Oral, Asia/Phnom_Penh, Asia/Pontianak, Asia/Pyongyang, Asia/Qatar, Asia/Qyzylorda, Asia/Rangoon, Asia/Riyadh, Asia/Saigon, Asia/Sakhalin, Asia/Samarkand, 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/Ulaanbaatar, 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/Faeroe, Atlantic/Faroe, Atlantic/Jan_Mayen, Atlantic/Madeira, Atlantic/Reykjavik, Atlantic/South_Georgia, Atlantic/St_Helena, Atlantic/Stanley, Australia/ACT, Australia/Adelaide, Australia/Brisbane, Australia/Broken_Hill, Australia/Canberra, Australia/Currie, Australia/Darwin, Australia/Eucla, Australia/Hobart, Australia/LHI, Australia/Lindeman, Australia/Lord_Howe, Australia/Melbourne, Australia/NSW, Australia/North, Australia/Perth, Australia/Queensland, Australia/South, Australia/Sydney, Australia/Tasmania, Australia/Victoria, Australia/West, Australia/Yancowinna, Brazil/Acre, Brazil/DeNoronha, Brazil/East, Brazil/West, CET, CST6CDT, Canada/Atlantic, Canada/Central, Canada/East-Saskatchewan, Canada/Eastern, Canada/Mountain, Canada/Newfoundland, Canada/Pacific, Canada/Saskatchewan, Canada/Yukon, Chile/Continental, Chile/EasterIsland, Cuba, EET, EST, EST5EDT, Egypt, Eire, Etc/GMT, Etc/GMT+0, Etc/GMT+1, Etc/GMT+10, Etc/GMT+11, Etc/GMT+12, Etc/GMT+2, Etc/GMT+3, Etc/

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

145

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

GMT+4, Etc/GMT+5, Etc/GMT+6, Etc/GMT+7, Etc/GMT+8, Etc/GMT+9, Etc/GMT-0, Etc/GMT-1, Etc/GMT-10, Etc/GMT-11, Etc/GMT-12, Etc/GMT-13, Etc/GMT-14, Etc/GMT-2, Etc/GMT-3, Etc/GMT-4, Etc/GMT-5, Etc/GMT-6, Etc/GMT-7, Etc/GMT-8, Etc/GMT-9, Etc/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Lisbon, Europe/Ljubljana, Europe/London, Europe/Luxembourg, Europe/Madrid, Europe/Malta, Europe/Mariehamn, Europe/Minsk, Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kiritimati, Pacific/Kosrae, Pacific/Kwajalein, Pacific/Majuro, Pacific/Marquesas, Pacific/Midway, Pacific/Nauru, Pacific/Niue, Pacific/Norfolk, Pacific/Noumea, Pacific/Pago_Pago, Pacific/Palau, Pacific/Pitcairn, Pacific/Pohnpei, Pacific/Ponape, Pacific/Port_Moresby, Pacific/Rarotonga, Pacific/Saipan, Pacific/Samoa, Pacific/Tahiti, Pacific/Tarawa, Pacific/Tongatapu, Pacific/Truk, Pacific/Wake, Pacific/Wallis, Pacific/Yap, Poland, Portugal, ROC, ROK, Singapore, Turkey, UCT, US/Alaska, US/Aleutian, US/Arizona, US/Central, US/East-Indiana, US/Eastern, US/Hawaii, US/Indiana-Starke, US/Michigan, US/Mountain, US/Pacific, US/Pacific-New, US/Samoa, UTC, Universal, W-SU, WET, Zulu

Select a time zone from the list.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

146

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

UserInterface settings

UserInterface Accessibility IncomingCallNotification

You can enable an incoming call notification with amplified visuals. The screen and Touch 10 will flash red/white approximately once every second (1.75 Hz) to make it easier for hearing impaired users to notice an incoming call. If the system is already in a call the screen will not flash as this will disturb the on-going call, instead you will get a normal notification on screen and touch panel.

Requires user role: ADMIN, INTEGRATOR, USER

Default value: Default

Value space: AmplifiedVisuals/Default

AmplifiedVisuals: Enable the amplified visuals on screen and touch panel when the video system receives a call.

Default: Enable the default behavior with a notification on screen and touch panel.

UserInterface Branding AwakeBranding Colors

If the video system is set up with branding customizations, this setting affects the colors of the logo that is shown when the video system is awake. You can choose whether you want to show the logo in full color, or reduce the opacity of the logo so that it blends in more naturally with the background and other elements on the screen.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Native

Auto: The opacity of the logo is reduced.

Native: The logo has full colors.

UserInterface ContactInfo Type

Choose which type of contact information to show in the user interface.

Requires user role: ADMIN

Default value: Auto

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

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

None: Do not show any contact information.

IPv4: Show the system's IPv4 address.

IPv6: Show the system's IPv6 address.

H323Id: Show the system's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the system's H.320 number as contact information (only supported if used with Cisco TelePresence ISDN Link).

E164Alias: Show the system's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

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 CustomMessage

A custom message can be displayed, in the lower left side of the screen, in awake mode.

Requires user role: ADMIN, INTEGRATOR

Default value: ""

Value space: String (0, 128)

Add a custom message. Add an empty string to remove a custom message.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

147

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 Features Call End

Choose whether or not to remove the default End Call button from the user interface. The setting removes only the button, not its functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

UserInterface Features Call MidCallControls

Choose whether or not to remove the default Hold, Transfer, and Resume in-call buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

UserInterface Features Call Start

Choose whether or not to remove the default Call button (including the directory, favorites, and recent calls lists) and the default in-call Add participant button from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

UserInterface Features HideAll

Choose whether or not to remove all default buttons from the user interface. The setting removes only the buttons, not their functionality as such.

Requires user role: ADMIN, INTEGRATOR

Default value: False

Value space: False/True

False: Shows all default buttons in the user interface.

True: Removes all default buttons from the user interface.

UserInterface Features Share Start

Choose whether or not to remove the default buttons and other UI elements for sharing and previewing content, both in call and out of call, from the user interface. The setting removes only the buttons and UI elements, not their functionality as such. You can share content using Proximity or the Cisco Webex Teams app still.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default buttons and UI elements in the user interface.

Hidden: Removes the default buttons and UI elements from the user interface.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

148

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

UserInterface Features Whiteboard Start

Choose whether or not to remove the default Whiteboard button from the user interface. The setting removes only the button, not its functionality as such. This setting only applies to Cisco Webex registered devices.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

UserInterface Language

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

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/Portuguese/PortugueseBrazilian/Russian/Spanish/ SpanishLatin/Swedish/Turkish

Select a language from the list.

UserInterface OSD EncryptionIndicator

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a 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. Then, an encryption indicator icon is shown for the rest of the call.

If the call is not encrypted, a "Call is not encrypted" notification is shown for 5 seconds. No encryption indicator icon is shown.

AlwaysOn: The "Call is encrypted" notification is shown for 5 seconds. Then, an encryption indicator icon is shown for the rest of the call.

AlwaysOff: The encryption indicator is never displayed on screen.

UserInterface OSD HalfwakeMessage

A custom message can be displayed in the middle of the main screen when the system is in the half wake state. The custom message will replace the default message, which gives instructions how to start using the video system. You can also delete the default message, without adding a custom message.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 128)

The custom message. An empty string: Restore the default message. A space only: There will be no message at all.

UserInterface OSD Output

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

Requires user role: ADMIN, INTEGRATOR

Default value: Auto

Value space: Auto

Auto: The system sends the on-screen information and indicators to the system's screen.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

149

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

UserInterface Phonebook Mode

This setting determines if a user is allowed to add or change a contact in the Directory and Favorites list from the user interface of the video system.

Requires user role: ADMIN, INTEGRATOR

Default value: ReadWrite

Value space: ReadOnly/ReadWrite

ReadOnly: You neither can add a contact to the Favorites list, edit a contact in the Favorites list, nor edit any contact from the Directory or Favorites list before calling.

ReadWrite: You are able to add a contact to the Favorites list, edit a contact in the Favorites list, and edit a contact from the Directory or Favorites list before calling.

UserInterface Security Mode

This setting allows you to prevent important system information from being exposed in the user interface (drop down menu and Settings panel), for example the contact information and IP addresses of the video system, touch controller, and UCM/VCS registrars. It is important to note that such information is not hidden when navigating further into the Settings panel.

If you want to fully prevent that people without administrator rights can see the contact information, IP addresses, MAC address, serial number, and software version, you must also set the UserInterface SettingsMenu Mode to Locked, and of course have a passphrase for all user accounts with administrator rights.

Requires user role: ADMIN

Default value: Normal

Value space: Normal/Strong

Normal: IP addresses and other system information are shown on the user interface.

Strong: Contact information and IP addresses are not displayed on the user interface (drop down menu and Settings panel).

UserInterface SettingsMenu Mode

The Settings panel in the user interface (Touch 10 or on-screen) can be protected by the video system's admin password. If this password is blank, anyone can access the settings in the Settings panel, and for example factory reset the system. If authentication is enabled, all settings that require authentication have a padlock icon. You will be prompted to enter the administrator's user name and passphrase when you select the setting. Some settings do not require authentication, they do not have a padlock icon.

Requires user role: ADMIN

Default value: Unlocked

Value space: Locked/Unlocked

Locked: Authentication with administrator's username and passphrase is required.

Unlocked: No authentication is required.

UserInterface SettingsMenu Visibility

Choose whether or not to show the system name (or contact information) in the upper left corner of the user interface, and the associated drop down menu and Settings panel.

Requires user role: ADMIN

Default value: Auto

Value space: Auto/Hidden

Auto: Shows the system name with drop down menu and Settings panel in the upper left corner of the user interface.

Hidden: Doesn't show the system name with drop down menu and Settings panel in the upper left corner of the user interface.

UserInterface Sounds Mode

Not applicable in this version.

Requires user role: ADMIN, USER

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

150

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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, INTEGRATOR, 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

151

UserManagement settings

UserManagement LDAP Admin Filter

The LDAP filter is used to determine which users should be granted administrator privileges.

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0, 1024)

    Refer to the LDAP specification for the syntax of this string. Example: "(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

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>).

You always have to set either an LDAP Admin Group or an LDAP Admin Filter. An LDAP Admin Filter takes precedence, so if the UserManagement LDAP Admin Filter is set, the UserManagement LDAP Admin Group setting is ignored.

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

    The distinguished name of the AD group. Example: "CN=admin group, OU=company groups, DC=company, DC=com"

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 BaseDN

The distinguishing name of the entry at which to start a search (base).

Requires user role: ADMIN

Default value: ""

Value space: String (0..255)

    The distinguishing name of the base. Example: "DC=company, DC=com"

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

152

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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 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.

If you switch on LDAP Mode, make sure to configure the other UserManagement LDAP settings to suit your setup. Here is a few examples.

Example 1:

– UserManagement LDAP Mode: On

– UserManagement LDAP Address: "192.0.2.20"

– UserManagement LDAP BaseDN: "DC=company, DC=com"

– UserManagement LDAP Admin Group: "CN=admin group, OU=company groups, DC=company, DC=com"

Example 2:

– UserManagement LDAP Mode: On

– UserManagement LDAP Address: "192.0.2.20"

– UserManagement LDAP BaseDN: "DC=company, DC=com"

– UserManagement LDAP Admin Filter: "(|(memberof=CN=admin group, OU=company groups, DC=company, DC=com)(sAMAccountName=username))"

Requires user role: ADMIN

Default value: Off

Value space: Off/On
    Off: LDAP authentication is not allowed.
    On: LDAP authentication is allowed.

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 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).

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

153

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Video settings

Video ActiveSpeaker DefaultPlPPosition

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, INTEGRATOR

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 in the stream that is sent to the remote participants (far end). This setting applies only when using a video system's built-in MultiSite feature (optional) to host a multipoint video conference.

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 DefaultMainSource

Define which video input source to be used as the default main video source when you start a call.

Requires user role: ADMIN, USER

Default value: 1

Value space: 1

The source that is used as the default main video source.

Video Input Connector [n] CameraControl CameraId

n: 1..2

The camera ID is a unique identifier of the camera that is connected to this video input.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: 1

Value space: Connector n: 1

The camera ID is fixed and cannot be changed.

Video Input Connector [n] CameraControl Mode

n: 1..2

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, INTEGRATOR

Default value: Connector n: Off

Value space: Connector n: Off

Off: Disable camera control.

Video Input Connector [n] InputSourceType

n: 1..2

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, INTEGRATOR

Default value: Connector 1: camera   Connector 2: PC

Value space: Connector 1: camera   Connector 2: PC/camera/document_camera/mediaplayer/whiteboard/other

    PC: Use this when a computer is connected to the video input.

    camera: Use this when a camera is connected to the video input.

    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.

    whiteboard: Use this when a whiteboard camera is connected to the video input.

    other: Use this when the other options do not match.

Video Input Connector [n] Name

n: 1..2

Define a name for the video input connector.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector n: ""

Value space: String (0, 50)

    Name for the video input connector.

Video Input Connector [n] OptimalDefinition Profile

n: 1..2

This setting will not take effect if the corresponding Video Input Connector [n] Quality setting is set to Sharpness.

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. 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, INTEGRATOR

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

156

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Video Input Connector [n] PresentationSelection

n: 2..2

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, INTEGRATOR

Default value: Connector n: Desktop

Value space: Connector n: 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 [n] Quality

n: 2..2

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, INTEGRATOR

Default value: Connector n: Sharpness

Value space: Connector n: 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 [n] RGBQuantizationRange

n: 2..2

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, INTEGRATOR

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 [n] Visibility

n: 1..2

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.

Requires user role: ADMIN, INTEGRATOR

Default value: Connector 1: Never   Connector 2: IfSignal

Value space: Connector 1: Never   Connector 2: Always/IfSignal/Never

Always: The menu selection for the video input connector will always be visible on the user interface.

IfSignal: Yhe menu selection for the video input connector will only be visible when something is connected to the video input.

Never: The input source is not expected to be used as a presentation source, and will not show up on the user interface.

Video Monitors

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

Requires user role: ADMIN, INTEGRATOR

Default value: Single

Value space: Single

Single: The layout is shown on the video system's screen.

Video Output Connector [n] Brightness

n: 1..1

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

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 [n] Resolution

n: 1..1

The resolution and refresh rate for the integrated screen. This value is fixed and cannot be changed.

Default value: 1920_1080_60

Value space: 1920_1080_60

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

Video Output Connector [n] Whitebalance Level

n: 1..1

The integrated screen'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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

158

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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, INTEGRATOR

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 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 Presentation Priority

Determine how to distribute the bandwidth between the presentation channel and the main video channel.

Requires user role: ADMIN

Default value: Equal

Value space: Equal/High/Low

Equal: The available bandwidth is shared equally between the presentation channel and the main video channel.

High: The presentation channel is assigned a larger portion of the available bandwidth at the expense of the main video channel.

Low: The main video channel is assigned a larger portion of the available bandwidth at the expense of the presentation channel.

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, INTEGRATOR

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 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, INTEGRATOR

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 OnMonitorRole

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

Requires user role: ADMIN, INTEGRATOR

Default value: First

Value space: First

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

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, INTEGRATOR

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 Mirrored

You can configure the video system to show the self-view image the way other people see you, or as you would see yourself in a mirror.
This setting has no effect on the video that is sent to the far end.

Requires user role: ADMIN, INTEGRATOR

Default value: On

Value space: Off/On

Off: Display the self-view image as other people see you.

On: Display the self-view image as you see yourself in a mirror.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

160

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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, INTEGRATOR

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, INTEGRATOR

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

161

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

162

Appendices

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

163

The user interface

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

On the right side of the unit:
· USB and mini-jack sockets for headset

Microphone: mute/unmute.

Loudspeaker volume control.

Tap the system name or contact information to access *System Information, Settings, Restart* and *Factory reset*. You can also adjust the brightness of the screen and activate *Call forwarding, Standby,* and *Do not disturb* modes.

Selfview: on/off

Time of day.

Tap *?* to contact Help desk or access other facility services, if available.

Entry point for user interface extensions (your system may have zero or more such buttons with different color, text and icons)

Indicates that at least one client is paired to the video system using *Proximity*.

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

Microphone mute indicator.

On the right side of the unit:
· Microphone mute button
· Loudspeaker volume controls
· USB socket for headset

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

164

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.
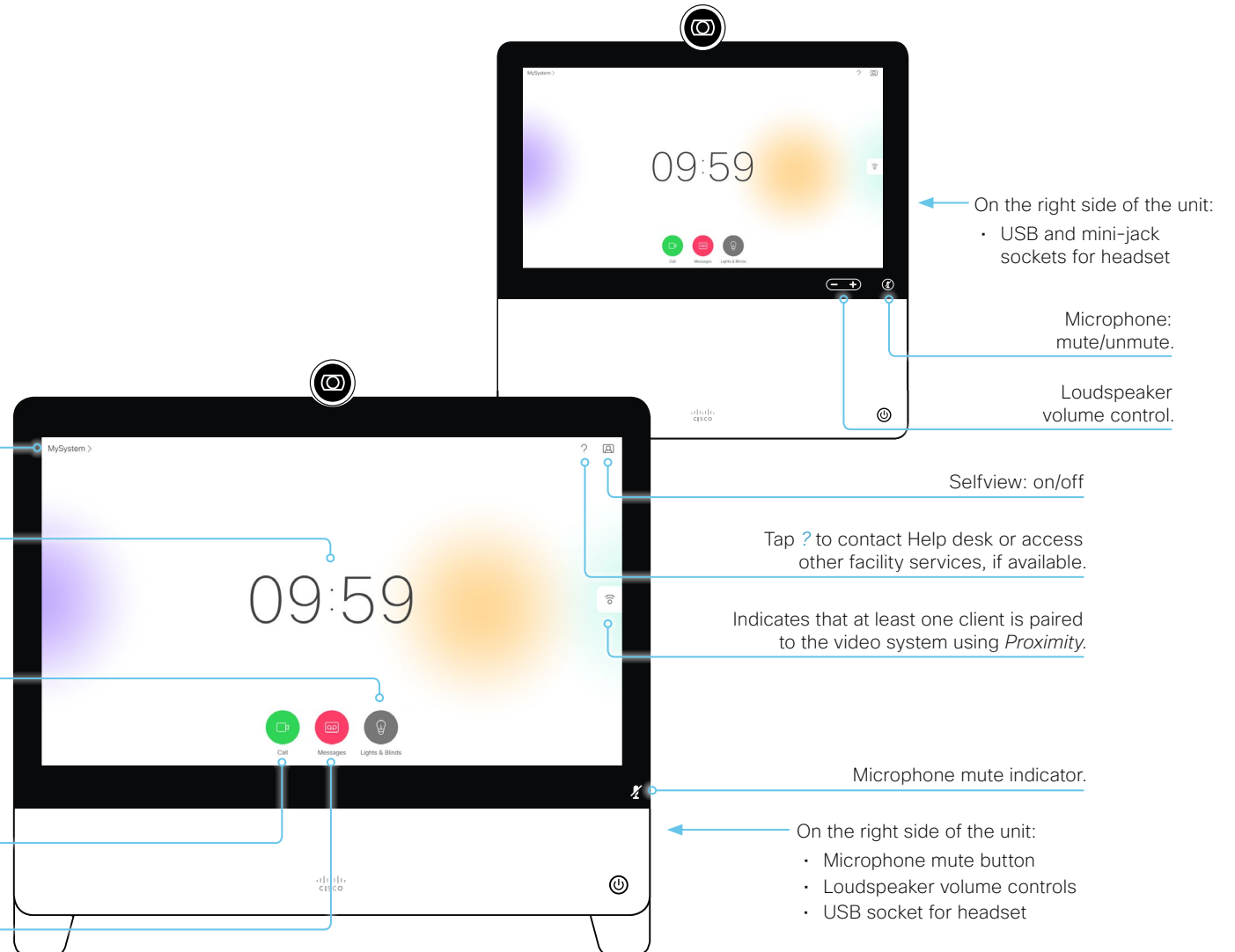
Set up remote monitoring

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.
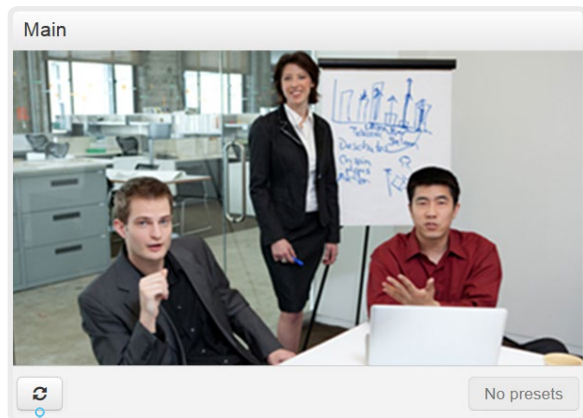
Automatically refresh snapshots

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

165

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Access call information and answer a call while using the web interface
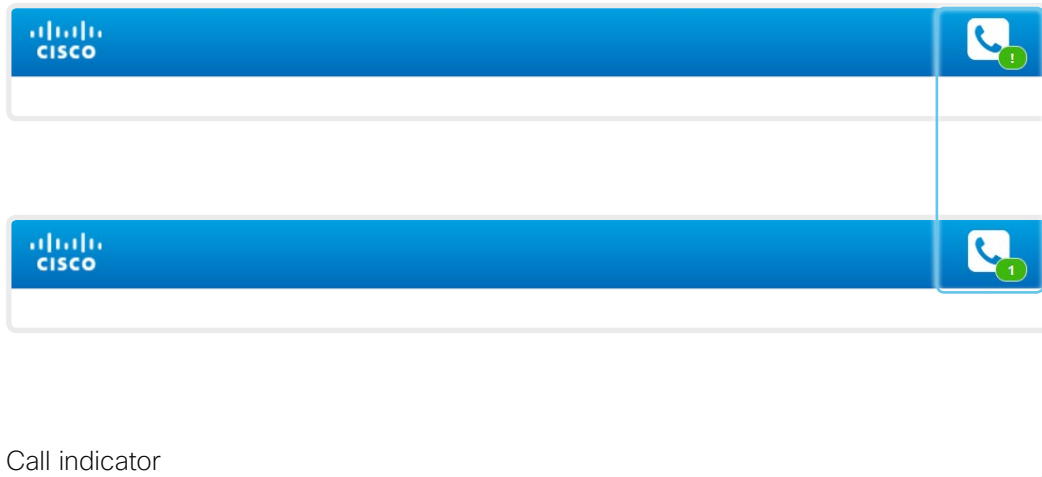
Notification of an incoming call

Click the *Call indicator* to open the *Call Control* page, where you can accept or decline the call.

The system is in a call

Call indicator

The call indicator is present to notify you about an incoming call, and to show when the system is in a call.

If the system is idle, there is no call indicator.

Control the call

Relevant control buttons are present on the *Call Control* page. 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 <small>(page 1 of 2)</small>

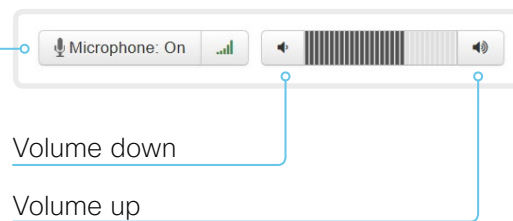Sign in to the web interface and navigate to *Call Control*.

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 *Favorites, 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 ⏸ button next to a participant's name to put that participant on hold.

To resume the call, use the ▶ 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 ☎ button.

---

* When searching, matching entries from the *Favorites, Directory* and *Recents* lists will be listed as you type.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

167

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.

Presentation

∙∙|∙∙|∙∙
cisco

Cisco TelePresence Systems

☞ Start Presentation
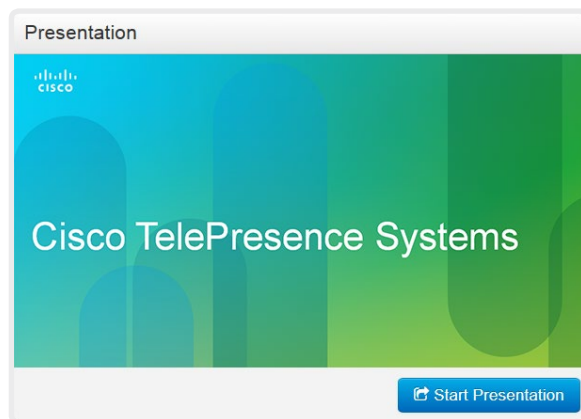
Snapshot area

Shows snapshots of the selected presentation source.

Only available on video systems that have the *Remote Monitoring* option.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

169

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Local layout control

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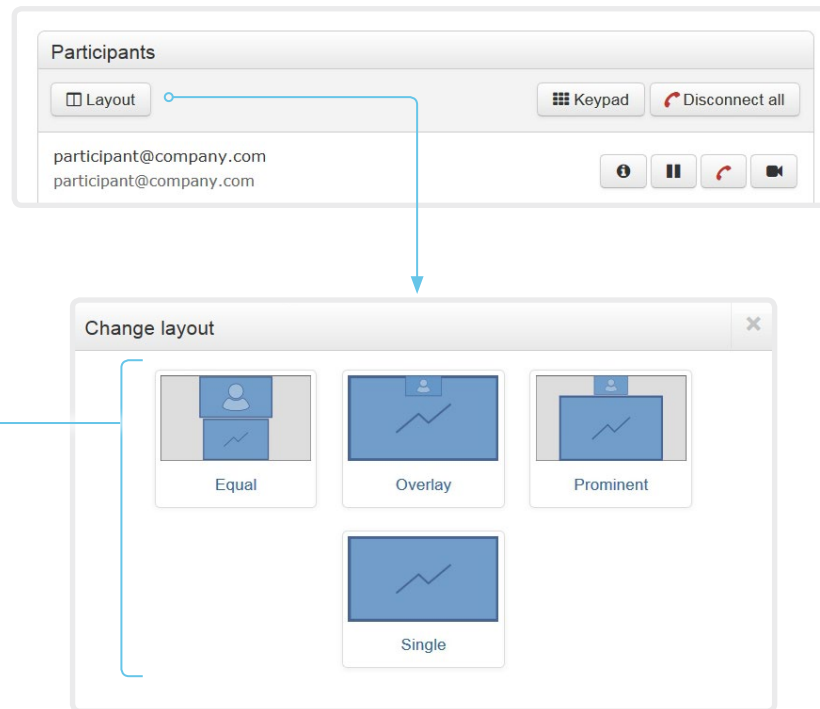
Change the layout

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

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

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

About layouts

The term layout is used to describe the various ways presentations and videos can appear on the screen. Different types of meetings may require different layouts.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

170

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.
- Speaker tracking is not switched On on the far end camera.
- The local video system has the *Remote Monitoring* option.
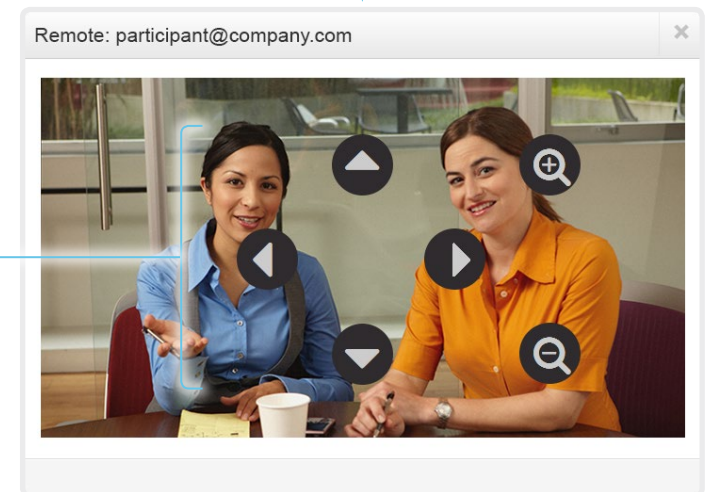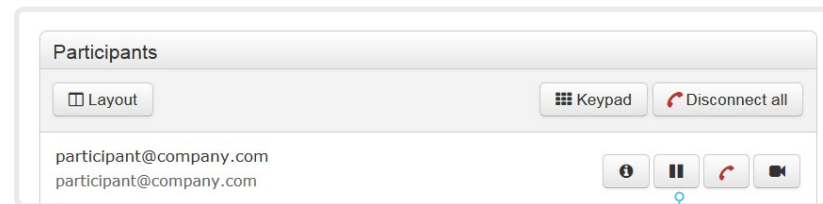
Control the remote participant's camera

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.

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).

172

Customization

Customize the video system's user interface (page 1 of 2)

You can customize the user interface to allow control of peripherals in a meeting room, for example lights and blinds, or to modify the video system's behavior by triggering macros.

This allows for the powerful combination of a control system's functionality and the video system's user-friendly user interface.
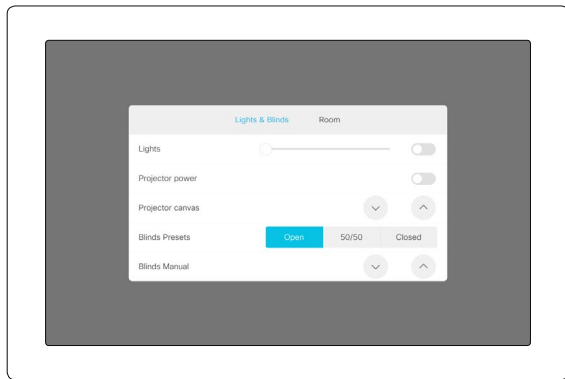
Example in-room control panel

Consult the *Customization guide* for full details about how to design custom user interface panels (in-room control panels) using the In-Room Control editor, and how to use the video system's API to program the in-room controls. Go to:

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

In-room control architecture

You need a Cisco video system with a touch interface, and a control system. The control system may be a third-party system, such as Crestron or AMX, with hardware drivers for 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.
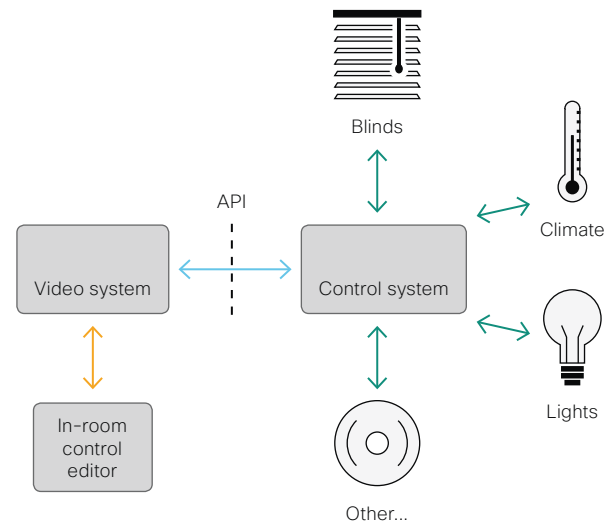
In-room control schematics

The video system's macro framework may also serve as a control system. In this case the control system can use the video system's API to trigger all sorts of local functionality: Speed dial, language selection, customized system reset, and much more.

Customization

Customize the video system's user interface (page 2 of 2)

The In-Room Control editor

Free of charge editor

An easy to use drag-and-drop editor, which you should use to compose the custom user interface panels (in-room control panels), comes free of charge with the video system's software.

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 run locally on your browser from your hard drive.

  Then you can compose your custom interfaces without being connected to a video system. You can export and import to file to move your work between your local version and the video system later.

Preview function

The editor also provides a preview function, which allows you to see how the custom interfaces will appear on the user interface.

The preview function is also a complete software version of your custom (in-room control) panels, so clicking the controls will result in the same actions as selecting them on the real user interface.

Therefore, you can use the preview function to test your integrations without having a real user interface available. You can also use the video system's in-room controls from a remote location

The room simulator

You can use the room simulator to visualise how the in-room controls on the user interface changes the state of the room.

⚠ Back up any existing in-room configuration you may have before you export the simulator configuration to the video system. The simulator configuration will replace the existing configuration on the video system.

Sign in to the web interface, and navigate to *Integration > In-Room Control*.

- Click *Launch Simulator* to open a room simulator in your browser.

  The room simulator contains a predefined in-room control configuration that you can export to the video system. Then you can control the simulator's virtual meeting room from your real user interface.

- Click *Load simulator config* to export the simulator configuration to the video system.

---

* You need a user that holds the ROOMCONTROL, INTEGRATOR, 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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

174

Customization

Customize the video system's behavior using macros

With macros, you can create your own snippets of code that run on the video system. The language is JavaScript / ECMAScript 6 with support for features such as arrow functions, promises and classes.

The macro framework allows an integrator to write scripts that tailor a video system's behavior to suit an individual customer's requirements. The integrators can, for example, implement their own features or variations of features, automate specific configurations or re-configurations, and create custom tests and monitoring functions.

By combining the use of macros and creation of a custom user interface panel (formerly referred to as in-room control panel), you can amend the user interface to trigger customized local functionality. For examples:

- Add speed dialling buttons
- Add a button for room reset, which set all configurations back to your preferred default setup

Consult the *Customization guide* for details about macros and how to use the video system's built in Macro editor. Go to:

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

Allow using macros on the video system

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

- Set *Macros > Mode* to **On**.

  If you try to launch the Macro editor while this setting is **Off**, a pop-up message appears. If you respond by tapping *Enable Macros,* the *Macros > Mode* setting will automatically change to **On**, and the editor will launch.

Launch the macro editor

Sign in[*] to the web interface, and navigate to *Integration > Macro Editor*.

We don't offer a stand-alone version of the editor that you can use to work offline.

The Macro editor

The Macro editor is a powerful tool where you can:

- Load our code examples, which you can modify, use as is, or use as inspiration when writing your own macros.
- Read our detailed macro scripting tutorial, which also explains the code examples in more detailed.
- Write your own macros, and upload them to the video system.
- Enable/Disable individual macros.
- Check in an embedded Log Console what happens when you run a macro.

---

[*] You need a user that holds the ADMIN user role in order to access the Macro editor.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

175

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Customization
Remove default buttons from the user interface

In some use cases, you may never use a default button, like *Call* or *Share.* Such unused buttons may cause confusion. In these cases, you can remove the unused buttons from the user interface. Custom In-Room Control panels can be exposed still. Removing default buttons while adding custom buttons makes it possible fully to customize the user interface.

For example, you can remove the *Call* and *Share* buttons if nobody is going to share content or call from this video system. Instead, add custom buttons (In-Room Controls) for the tasks that are going to be performed.

Configurations

Use the following configurations to remove default buttons from the user interface. The configurations are available both from the web interface of the video system, and in the API.

· *UserInterface > Features > Call > Start*: Removes the default *Call* button (including the directory, favorites, and recent calls lists). Also removes the *Add* participant button while in a call.

· *UserInterface > Features > Call > VideoMute*: Removes the default *Turn video off* button.

· *UserInterface > Features > Share > Start*: Removes the default user interface for sharing and previewing content, both in call and out of call.

· *UserInterface > Features > HideAll*: Removes all the default buttons. In-Room Control panels are not removed.

· *UserInterface > Features > Call > End*: Removes the *End Call* button.

· *UserInterface > Features > Call > MidCallControls*: Removes the *Hold*, *Resume,* and *Transfer* in-call buttons.

ⓘ   The configurations remove only the buttons, not the functionality as such. You can share content using Proximity, even if you have removed the *Share* button from the user interface.

Further Information

Find more details about how to remove buttons and customize the user interface in the *Customization guide.* Go to:

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

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

176

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Customization

Use of a third-party USB input device

You can use a third-party USB input device to control certain functions on video system. A Bluetooth remote control (with a USB dongle) and a USB keyboard are examples of such input devices.

This feature is meant to complement the functionality of the Touch 10 or the DX user interfaces, wherever convenient. It is not meant to replace the Touch 10 and DX user interfaces.

Examples of applications:

· In classrooms and during lectures, a small remote control can be used to wake up a video system from standby mode. Also, it may be convenient to use a remote control to select which input source to present.

· Controlling the camera view (pan, tilt, and zoom) in situations where you are not allowed to use the Touch 10. For example, in operating rooms in a hospital.

Functional Overview

Pressing a button on the USB input device, generates an event in the API. Macros or third-party control devices can listen for such events, and respond to them. This behavior is similar to the behavior of In-Room Control buttons. It is also possible to listen for the events using webhooks, directly in an SSH session.

There isn't a library of actions readily available to select actions from. You must define and implement the actions to be taken as response to the events yourself. For example:

· Increase the volume of the video system when the Volume Up key is pressed.
· Put the video system in standby mode when the Sleep key is pressed.

Configurations, Events, and Status

The support for third-party USB input devices is disabled by default. Enable it explicitly by setting the *Peripherals > InputDevice > Mode* to **On**.

Pressing and releasing a button generates a Pressed and a Released event:

```
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Pressed
** end
*e UserInterface InputDevice Key Action Key: <name of the key>
*e UserInterface InputDevice Key Action Code: <id of the key>
*e UserInterface InputDevice Key Action Type: Released
** end
```

To listen for events, you must register feedback from the InputDevice events:

```
xFeedback Register /event/UserInterface/InputDevice
** end
```

When the room device detects the third-party input device, the input device is listed in the room device *UserInterface > Peripherals > ConnectedDevice* status. The input device may be reported as multiple devices.

Required Equipment

· A system from the Cisco Webex Room Series or DX Series.

· A third-party input device that advertises itself as a USB keyboard, for example a Bluetooth remote control with a USB dongle.
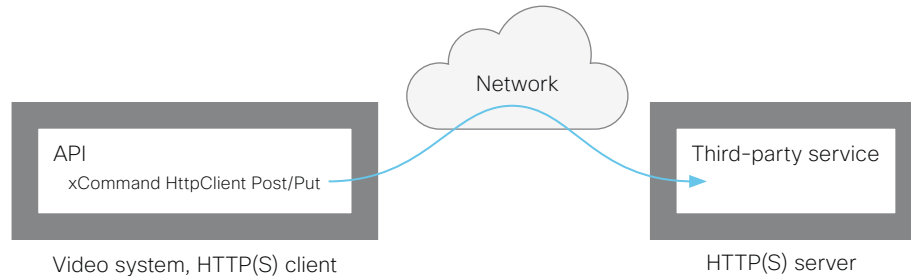
Further Information

Find more information about the use of a third-party input device in the *Customization guide*. Go to:

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

Cisco support (TAC) doesn't support debugging of third-party code, including macros. Please check the ► Cisco Collaboration Developer community if you need help with macros and third-party code.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

177

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Customization

Sending HTTP(S) Post and Put requests

Video system, HTTP(S) client   HTTP(S) server

This feature makes it possible to send arbitrary HTTP(S) Post and Put requests from a video system to an HTTP(S) server.

By using macros, you can send data to an HTTP(S) server whenever you want. You can choose what data to send, and structure them as you like. This way you can adapt the data to an already established service.

Security measures:

- The HTTP(S) Post/Put feature is disabled by default. A system administrator must explicitly enable the feature by setting *HttpClient > Mode* to **On**.
- The system administrator can prevent the use of HTTP by setting *HttpClient > AllowHTTP* to **False**.
- The system administrator can specify a list of HTTP(S) servers that the device is allowed to send data to.
- The number of concurrent Post and Put requests is limited.

List of Allowed HTTP(S) Servers

The system administrator can use these commands to set up and maintain a list of up to ten allowed HTTP(S) servers (hosts):

- xCommand HttpClient Allow Hostname Add Expression: <Regular expression that matches the host name or IP address of the HTTP(S) server>
- xCommand HttpClient Allow Hostname Clear
- xCommand HttpClient Allow Hostname List
- xCommand HttpClient Allow Hostname Remove Id: <id of an entry in the list>

If the list is not empty, you can send HTTP(S) requests only to the servers in the list. If the list is empty, you can send the requests to any HTTP(S) server.

The check against the list of allowed servers is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

Allowing HTTPS without certificate validation

When sending requests over HTTPS, the video system checks the certificate of the HTTPS server by default. If the HTTPS server certificate is not found to be valid, you get an error message. The video system doesn't send any data to that server.

We recommend using HTTPS with certificate validation. If this is not possible, the system administrator can set *HttpClient > AllowInsecureHTTPS* to **On**, which allows the use of HTTPS without validating the server's certificate.

Sending HTTP(S) Requests

Once the HTTP(S) Client Post feature is enabled, you can use the following commands to send Post and Put requests to an HTTP(S) server:

- xCommand HttpClient Post [AllowInsecureHTTPS: <True/False>] [Header: <Header text>] Url: <URL to send the request to>
- xCommand HttpClient Put [AllowInsecureHTTPS: <True/False>] [Header: <Header text>] Url: <URL to send the request to>

These are multiline commands. Read the API guide to find out how to use multiline commands, and also to find a detailed description of the command parameters.
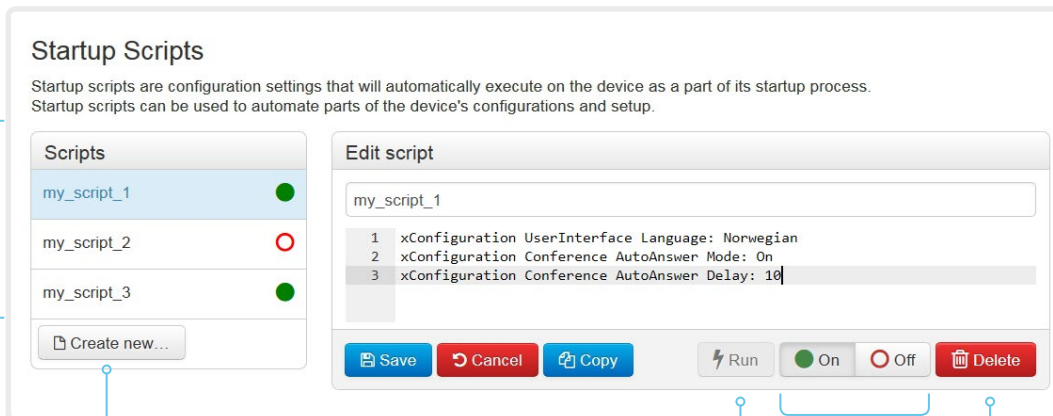
Further Information

Find more information about HTTP(S) Post requests in the *Customization guide*. Go to:

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

Manage startup scripts

Sign in to the web interface, and navigate to *Integration > Startup Scripts*.

Startup Scripts

Startup scripts are configuration settings that will automatically execute on the device as a part of its startup process. Startup scripts can be used to automate parts of the device's configurations and setup.

Scripts	Edit script

Scripts
my_script_1 ●
my_script_2 ○
my_script_3 ●
▢ Create new…

Edit script

my_script_1

```
1  xConfiguration UserInterface Language: Norwegian
2  xConfiguration Conference AutoAnswer Mode: On
3  xConfiguration Conference AutoAnswer Delay: 10
```

[💾 Save] [↺ Cancel] [⧉ Copy]   [⚡ Run] [● On] [○ Off] [🗑 Delete]

The script names and configurations shown in the illustration serve as examples. You may make your own scripts.

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.

Creat 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*.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

179

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

180

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).

Execute API commands and configurations

In the field below you can enter API commands (xCommand and xConfiguration) directly.

For example: xCommand Dial Number: "person@example.com" Protocol: Sip

Enter commands…

Execute

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.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

181

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

About Ethernet ports

The main network port

The main network port - Network port 1 - is always reserved for the connection to LAN. This applies to all video systems.

Depending on the video system, Network port 1 is marked with the number 1, the network symbol (⊞), or both.

Auxiliary network ports

Some video systems have more than one network port. The additional ports can be used for peripheral devices like cameras, Touch 10, third-party control systems, and more.

A device that is connected to such a network port gets a local IP address from the codec, and therefore is not part of the corporate network. It is not possible for packets to traverse the codec between the main network port (LAN) and the auxiliary network ports (link-local).

- A Cisco peripheral device is assigned a dynamic IP address in the range (DHCP): 169.254.1.41 to 169.254.1.240
- A non-Cisco device is assigned the dynamic IP address (DHCP): 169.254.1.30

  NOTE: Only one non-Cisco device can get a dynamic IP address at a time.

- A non-Cisco device can be assigned a static IP address in the range: 169.254.1.241 to 169.254.1.254

This method can also be used to connect to the codec with SSH. In this case you can use the IP address 169.254.1.1.

Product	Number of auxiliary network ports	Number of auxiliary network ports with PoE
Room Kit	1	0
Room Kit Mini	1	1 (⊡)
Room 55	1	1 (⊡)
Room 70 / Room 55 Dual	2	1 (⊡)
Room 70 G2	4	2 (⊡, PoE)
Codec Plus	2	1 (⊡)
Codec Pro	4	2 (⊡, PoE)
SX10	0	0
SX20	0	0
SX80	2	0
MX200 G2 / MX300 G2	2	0
MX700 / MX800	2	0*
DX70 / DX80	1	0

Power over Ethernet (PoE)

Some of the auxiliary network ports provide Power over Ethernet (PoE). These ports can power peripherals like the Touch 10 controller.

* These products have a separate PoE injector that is connected to one of the auxiliary network ports. The PoE injector is used for the Touch 10 controller.

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

182

Serial interface

Use the micro USB connector for direct communication with the video system[1]. 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.[2]

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
- Hardware flow control: Off

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

Computer — USB ——— USB to micro USB cable ——— Micro USB — Video system

Flip the connector cover up to uncover the connector panel.

DX70

Micro USB connector

Flip the connector cover up to uncover the connector panel.

DX80

Micro USB connector

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

183

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.
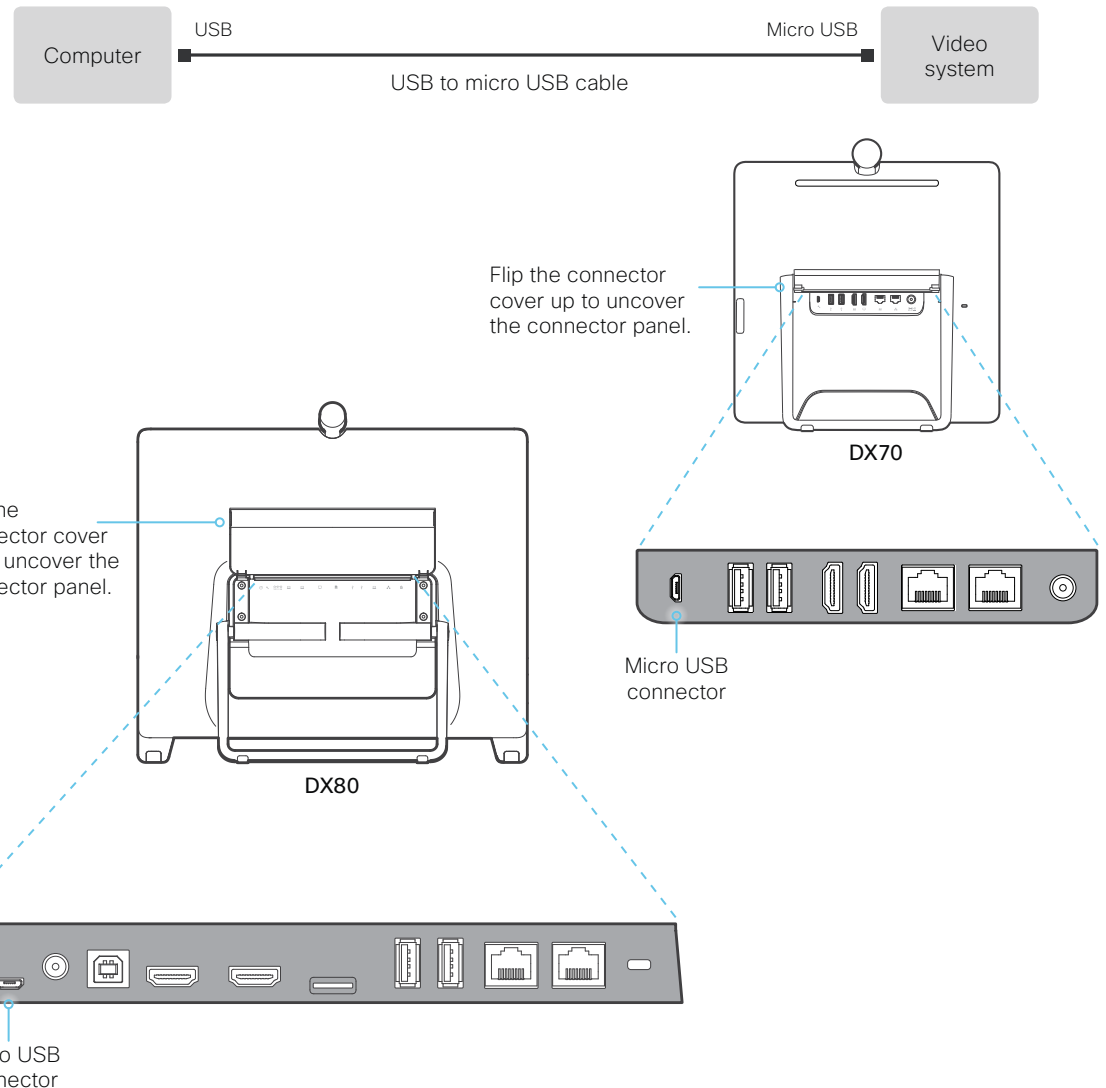
Open TCP Ports

The web server within the codec prohibit or restrict the use of nonsecure or unnecessary ports, protocols, modules, and/or services. Some ports are open or closed by default.

TCP 22: SSH

You can close the port by setting SSH mode to **Off**.

`NetworkServices SSH Mode: Off/On`

TCP 80: HTTP

You can close the port by setting HTTP mode to **Off** or **HTTPS**.

`NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off`

TCP 443: HTTPS

You can close the port by setting HTTP mode to **Off**.

`NetworkServices HTTP Mode: HTTP+HTTPS/HTTPS/Off`

TCP 5060/5061: SIP listen ports

The SIP listen pors are open by default. The SIP listen ports are disabled by the Cisco UCM (Unified Communication Manager). You can close the ports by setting the SIP listen ports to **Off**.

`SIP ListenPort: Off/On`

The system settings 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.

HTTPFeedback address from TMS

When a video system is added to Cisco TelePresence Management Suite (TMS), it is automatically configured to send information (events) back to TMS. The video system receives the address, that these events should be sent to, from TMS (HTTPFeedback address). If this address is absent or misconfigured, the video system cannot send events to TMS.

Missing response to events

If the video system does not receive a response to an event, it will retry sending it to the HTTPFeedback address up to 6 times at increasing intervals.

If the video system does not receive a response to any of the retries, the endpoint tries to send a message to the HTTPFeedback address every ten minutes. The HTTPFeedback status will indicate that it has failed, and there is a diagnostic message indicating the type of failure.

While retrying to send messages, there will be a loss of Call Detail Records (CDR) on TMS.

Get a new HTTPFeedback address from TMS

In order to get a new address to send events to, you must restart the video system and wait for the next management address push from TMS (scheduled or triggered by the TMS administrator).

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

185

Technical specification (page 1 of 2)

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
(depends on 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, 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 Managment Suite)
- Server directory supporting LDAP and H.350 (requires Cisco TelePresence Managment 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)

BANDWIDTH
- Up to 3 Mbps

MINIMUM BANDWIDTH FOR RESOLUTION AND FRAME RATE
- 720p30 from 768 kbps
- 1080p30 from 1472 kbps

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 × 480
- 720 × 480
- 800 × 600
- 1024 × 768
- 1280 × 720
- 1366 x 768
- 1920 x 1080

Extended Display Identification Data (EDID)

VIDEO OUTPUT
One HDMI output*. (reserved for future use) Supports format:
- 1920 × 1080 @ 60 fps (1080p60)

VESA Monitor Power Management

Extended Display Identification Data (EDID)

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)
- 1280 × 1024 @ 30 fps (SXGA)
- 1440 × 900 @ 30 fps (WXGA+)
- 1680 × 1050 @ 30 fps (WSXGA+)
- 1920 × 1080 @ 30 fps (HD1080p)

AUDIO STANDARDS
- 64 kbps AAC-LD
- OPUS
- G.722
- G.722.1
- G.711mu
- G.711a
- G.729AB

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 INPUTS
- Integrated microphone arrray
- One HDMI audio-in

---
* HDMI version 1.3

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

186

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Technical specification (page 2 of 2)

AUDIO OUTPUTS
· One line out, mini-jack (DX70)
· One HDMI (digital main audio)

DUAL STREAM
· H.239 dual stream (H.323)
· BFCP dual stream (SIP)
· Support for resolutions up to 1920 × 1080 at 15 fps

MULTIPOINT SUPPORT
· Cisco Ad-Hoc Conferencing (requires Cisco Unified Communications Manager (CUCM), and Cisco Meeting Server (CMS) or Cisco TelePresence Server with 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 QoS 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)
· Wi-Fi: IEEE 802.11a/b/g/n, 2.4 GHz, 5 GHz
· Bluetooth 4.0 LE

OTHER INTERFACES
· Three USB ports
· One MicroSD card slot for future use
· One Micro USB port for maintenance

APPROVALS AND COMPLIANCE
· Directive 2014/35/EU (Low-Voltage Directive)
· Directive 2014/30/EU (EMC Directive) – Class A
· Directive 2014/53/EU (Radio Equipment Directive)
· 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)

Please check the Product Approval Status Database at http://www.ciscofax.com for approval documents per country.

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.

April 2018

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

187

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

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).

CE software supports a range of RFCs, including the following:

- RFC 2782 DNS RR for specifying the location of services (DNS SRV)
- RFC 3261 SIP: Session Initiation Protocol
- RFC 3263 Locating SIP Servers
- RFC 3361 DHCP Option for SIP Servers
- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3711 The Secure Real-time Transport Protocol (SRTP)
- 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 4582 The Binary Floor Control Protocol

  draft-ietf-bfcpbis-rfc4582bis-00 Revision of the Binary Floor Control Protocol (BFCP) for use over an unreliable transport
- RFC 4733 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
- RFC 5245 Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols
- RFC 5589: SIP Call Control Transfer
- RFC 5766 Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)
- RFC 5905 Network Time Protocol Version 4: Protocol and Algorithms Specification

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

188

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

User documentation on the Cisco web site

Use the following short-links to find the documentation for the product series running CE software.

Room Series:

▶ https://www.cisco.com/go/room-docs

MX Series:

▶ https://www.cisco.com/go/mx-docs

SX Series:

▶ https://www.cisco.com/go/sx-docs

DX Series:

▶ https://www.cisco.com/go/dx-docs

In general, you can find user documentation for all Cisco Collaboration endpoints at ▶ https://www.cisco.com/go/telepresence/docs

The documents are organized in the following categories - some documents are not available for all products:

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

- *Getting started guide:* Initial configurations required to get the system up and running
- *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)
- *Spare parts overview, Spare parts replacement guides, Cable schemas*: Useful information when replacing spare parts

Maintain and Operate > End-User Guides

- *User guides:* How to use the product
- *Quick reference guides:* How to use the product
- *Physical interface guide:* Details about the codec's physical interface, including the connector panel and LEDs

Reference Guides > Command references

- *API reference guides:* Reference guide for the Application Programmer Interface (API)

Reference Guides > Technical References

- *CAD drawings:* 2D CAD drawings with measurements

Configure > Configuration Guides

- *Customization guide:* How to customize the user interface, how to use the video system's API to program in-room controls, making macros, use a video switch, and configure advanced audio set-ups using the Audio Console.

Design > Design Guides

- *Video conferencing room guidelines:* General guidelines for room design and best practice
- *Video conferencing room guidelines:* Things to do to improve the perceived audio quality

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*

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

189

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.

Cisco contacts

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

Go to: ► https://www.cisco.com/go/offices

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

Intellectual property rights

Cisco product security overview

D15362.11 DX70 and DX80 Administrator Guide CE9.7, APRIL 2019.

190

www.cisco.com — Copyright © 2019 Cisco Systems, Inc. All rights reserved.