

Collaboration Endpoint Software 9.9
OCTOBER 2019



Application Programming Interface (API) Reference Guide

Cisco Collaboration Endpoint Software 9.9



What's in this guide?

The top menu bar and the entries in the table of contents are all hyperlinks, just click on them to go to the topic.

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

Go to: ▶ <https://www.cisco.com/go/telepresence/docs>

Table of Contents

Introduction.....	3
About this guide.....	4
About the API.....	5
API fundamentals.....	6
Connecting to the API	6
SSH	6
Telnet.....	6
HTTP/HTTPS	6
WebSocket.....	6
RS-232 / serial connection	7
Ethernet ports.....	7
User roles	7
Passphrase.....	8
API output	9
Using the command line	10
API commands	10
Other commands.....	10
Command line shortcuts	11
Searching	11
Value types and formats.....	11
Multiline commands	13
Synchronous API calls	14
Events	15
Feedback mechanism.....	16
Feedback expressions	16
Terminal connections	17
Using HTTP.....	18
HTTP XMLAPI Authentication.....	18
HTTP XMLAPI Session Authentication.....	18
Getting status and configurations	19
Sending commands and configurations.....	19
Feedback from the device over HTTP.....	20
Registering for feedback.....	20
Translating from terminal mode to XML	21
Dos and don'ts.....	22
xConfiguration commands.....	23
Description of the xConfiguration commands	24
xCommand commands	98
Description of the xCommand commands	99
xStatus commands	179
Description of the xStatus commands.....	180
Appendices.....	249
Startup scripts	250
The SystemTools commands.....	251
Disconnect cause types	253
User documentation on the Cisco web site.....	254



Chapter 1

Introduction



About this guide

This guide introduces you to the Application Programming Interface (API) for the Collaboration Endpoint software, and serves as a reference guide for the command line commands.

The guide describes the API for on-premise registered video conferencing devices (CUCM, VCS) as well as devices registered to Cisco's cloud service (Cisco Webex).

Which commands are available depends on the product, the back-end (on-premise, cloud), and the user role of the local user (admin, audit, integrator, roomcontrol, user).

This guide applies to the following products:

- Webex Boards:
 - Webex Board 55 and 55S
 - Webex Board 70 and 70S
 - Webex Board 85S

Which call services support a configuration, status, or command

Some of the configurations, commands, and statuses that are available in the API only apply to on-premises registered devices. They don't apply to Webex registered devices.

Among the non-applicable configurations, commands, and statuses, are everything that is related to H.323, H.320, SIP, NTP, CUCM, LDAP, Proximity, and Far End Camera Control.

Downloading the user documentation

You can download the user documentation from the Cisco web site, go to:

► <https://www.cisco.com/go/telepresence/docs>

For Cisco Webex registered devices, go to:

► <https://help.webex.com>

Guidelines for how to find the documentation on the Cisco web site are included in the ► [User documentation on the Cisco web site](#) appendix.



Chapter 2

About the API



API fundamentals

This chapter contains a top-level view of the mechanisms supported by the device API.

Here you can read about how to access the API, how to use the command line and what the different parts of the API can be used for. This chapter also describes how to use the feedback functions that are available for the device.

The API consists of four major groups:

- Commands
- Configurations
- Status
- Events

These four groups are hierarchically organized, which makes it easier to find related functionality. You can find the complete lists of all commands, configurations and statuses in the following chapters.

NOTE: The commands return values that may affect how the device interacts with third-party systems. These may change from release to release and are not documented.

¹ Telnet is only available for DX, MX, and SX series.

Connecting to the API

There are several ways to access the device API:

- SSH
- Telnet¹
- HTTP/HTTPS
- WebSocket
- Serial connection²

Regardless of which method you choose, the structure of the API is the same. Choose the connection method that suits your application best. Note that all methods are not available for all products.

Before you start, please read this section about the different methods, as some of them may require additional configuration changes before being enabled. The configurations, apart from password, can be set from the Configuration menu on the web interface or from the command line interface. The examples are for the command line interface.

SSH

SSH is a secure TCP/IP connection and it is enabled by default on the device. It can be disabled. You need an SSH client, such as PuTTY, to access the API over SSH.

```
xConfiguration NetworkServices SSH Mode:  
<Off,On>
```

Telnet

Telnet¹ can be viewed as the equivalent of the serial protocol in the TCP/IP world. Telnet is disabled by default. Before connecting to the device with Telnet you have to enable it.

To enable the Telnet service, configure the following setting on the device. Changing this setting does not require a reboot of the device, but it may take some time to take effect.

```
xConfiguration NetworkServices Telnet Mode:  
<Off,On>
```

HTTP/HTTPS

As HTTP/HTTPS are connectionless protocols, there is no persistent connection. There are several ways of communicating with the API over HTTP.

In order to enable or disable the HTTP and HTTPS services, configure the following setting on the device.

```
xConfiguration NetworkServices HTTP Mode:  
<Off, HTTP+HTTPS, HTTPS>
```

Connecting

You can inspect the API by entering the IP-address or host name of the device in your web browser. This opens the web interface, and you can find the API documents under the menu section *Integration > Developer API*. The HTTP POST and GET methods are used to execute commands and get feedback from the device. This is described in “[Using HTTP](#)” on page 18 in this document.

WebSocket

WebSocket is a protocol that provides a full-duplex communication channel between a client and the API of the device. The API commands are embedded in JSON-RPC objects before they are sent over WebSocket.

In order to enable or disable the use of WebSocket, configure the following settings. Because WebSocket is tied to HTTP, also HTTP or HTTPS must be enabled before you can use WebSocket.

```
xConfiguration NetworkServices WebSocket:  
<Off, FollowHTTPService>  
xConfiguration NetworkServices HTTP Mode:  
<Off, HTTP+HTTPS, HTTPS>
```

Read the [xAPI over WebSocket](#) guide for details how to convey API commands in JSON-RPC objects over WebSocket.

RS-232 / serial connection

Depending on the product the device has either an USB or a standard COM-port for serial communication.² It can be used without an IP-address, DNS, or a network. Serial connection is allowed by default.³

`xConfiguration SerialPort Mode: <Off/On>`

Baud-rate and other serial port parameters

The serial port uses 115200 bps, 8 data bits, no parity and 1 stop bit. The default baud rate is set to 115200 bps.

The exception to this is SX20, where the serial port uses 38400 bps, 8 data bits, no parity, and 1 stop bit. The default baud rate is set to 38400 bps.

The device can give very much feedback. We therefore recommend keeping the connection at this speed or higher to avoid sluggishness.

On MX700, MX800, SX20, SX80, and the Room series, you can change the baud rate if required.

`xConfiguration SerialPort BaudRate`

During the initial boot sequence, the device uses a baud rate of 38400 bps regardless of the baud rate you have set.

Login and password

You can choose whether login is required or not for serial connections. For security reasons the password prompting is turned on by default, but it can be turned off if preferred.

`xConfiguration SerialPort LoginRequired: <Off/On>`

² Serial connection is not available for DX70, DX80, Room 55 Dual, and Room 70.

³ Only the default serial connection settings are available for Webex Board 55 and 70.

⁴ Depending on the device, Network port 1 is marked with the number 1, the network symbol (Ethernet), or both.

Ethernet ports

The main network port - Network port 1 - is always reserved for the connection to LAN.⁴ This applies to all devices.

Some of our devices have more than one network port. The additional ports can be used for peripheral devices like cameras, Touch 10, and more.

A device that is connected to such a network port gets a local IP-address from the video conferencing device, and therefore is not part of the corporate network.

- A Cisco 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 device with SSH. In this case you can use the IP-address 169.254.1.1.

Power over Ethernet (PoE)

The following products have one or more Ethernet ports that provide PoE:

- Codec Plus, Room Kit Mini, Room 55, Room 55 Dual, Room 70 (marked with the Touch controller symbol (Touch))
- Codec Pro, Room 70 G2 (2 ports: one marked with the Touch controller symbol (Touch), the other with the letters "PoE")

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 associated 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 devices with third-party equipment. Such a user can also create in-room controls.



Passphrase

The device is delivered with a default user account with full credentials. The user name is *admin*, and initially, no passphrase is set for the default user.

It is mandatory to set a passphrase for the *admin* user in order to restrict access to device configuration. You should in addition set a passphrase for any other user with similar credentials.

You can set the passphrase on the device's web interface. Open a web browser and enter the IP-address of the device in the address bar and sign in. Click your user name in the upper right corner and choose *Change passphrase* in the drop down menu.



API output

The xPreferences is used to set preferences for the RS-232, Telnet and SSH sessions.

The output modes are:

Terminal: Line based output for use with line based control systems

XML: XML output for use with control systems that understand XML.

JSON: JSON format is convenient when integrating with web based systems.

The default output mode is [terminal](#). To change this you have to define your preferences for each session individually. Examples in this guide are in terminal mode.

To set output mode to XML, issue the command:

```
xPreferences outputmode xml
```

To revert to terminal mode, issue the command:

```
xPreferences outputmode terminal
```

Example: Command in terminal mode

```
xCommand Audio Volume Set Level: 50
```

Example: Command in XML mode

```
<Command>
  <Audio>
    <Volume>
      <Set command="True">
        <Level>50</Level>
      </Set>
    </Volume>
  </Audio>
</Command>
```

Using the command line

Help

To get a list of all supported top level commands you can type `? or help` after connecting to the device using RS-232, Telnet or SSH (Example 1).

Bye

Typing the bye command closes the command line interface.

API commands

xConfiguration

Configurations are device settings, such as device name and network settings. These are persistent across boots. Refer to ["Configurations" on page 12](#).

xCommand

Commands instruct the device to execute actions, such as to dial a number or to search the phone book.

Refer to ["Commands" on page 12](#).

xStatus

A status contains the current state of the device, such as connected calls, the status of the gatekeeper registration, connected inputs and output sources.

Refer to ["Status" on page 12](#).

xFeedback

The Feedback commands are used to specify what parts of the configuration and status hierarchies to monitor. Feedback is only issued on the RS-232, Telnet or SSH session for which it is specified. If you are connecting to the device with multiple sessions, you have to define feedback individually for each session. Refer to ["Feedback mechanism" on page 16](#).

Example 1:

```
?
      - User Commands -
help           xcommand        xconfiguration   xevent          xfeedback
xgetxml        xdocument       xpreferences     xtransaction   xstatus
bye            echo            log             systemtools
```

xPreferences

The xPreferences command is used to set preferences for the RS-232, Telnet and SSH sessions.

Refer to ["API output" on page 9](#).

Echo <on/off>

If echo is set to **On** the key inputs are displayed when entering text in a command line interface.

If echo is set to **Off** user input is not displayed when entering text in a command line interface.

xEvent

The xEvent command returns information on which events are available for feedback. Refer to ["Events" on page 15](#).

xGetxml

The xGetxml request returns an XML document based on the location parameter attached to the request. The elements (or a complete document) matching the expression will be returned. Refer to ["Feedback mechanism" on page 16](#).

Other commands

Systemtools

The systemtools commands are a set of command line tools for administrative control and diagnostics. The commands can be used for advanced troubleshooting together with Cisco technical support. Systemtools are not a part of the programming API. Refer to ["The SystemTools commands" on page 251](#).

Log

The log command is used to enable advanced logs. It is only used for debugging the device.



Command line shortcuts

If your client supports it, there are some timesaving shortcuts you can use:

- Tab-completion to complete the commands and arguments.
- Arrow up and arrow down keys to navigate your command history.
- <CTRL-a>: Jump to the beginning of the line.
- <CTRL-e>: Jump to the end of the line.
- <CTRL-r>: Incremental command history search.
- <CTRL-w>: Erase the current line.

Searching

You can use `//` to search for elements anywhere in the status or configuration hierarchy (Example 1).

You can also combine multiple `//`'s (Example 2).

NOTE: The search shortcuts work well for inspecting the API, but should not be used in applications. We recommend that you always use the complete paths to avoid command ambiguity when upgrading to newer firmware releases.

Example 1:

List all configurations that include words that starts with OUT and HDMI:

```
xconfiguration //out//hdmi
*c xConfiguration Audio Output HDMI 1 Level: 0
*c xConfiguration Audio Output HDMI 1 Mode: On
*c xConfiguration Audio Output HDMI 2 Level: 0
*c xConfiguration Audio Output HDMI 2 Mode: Off
** end
```

Example 2:

Get the resolution width of all connected sources for both inputs and outputs:

```
xStatus //vid//res//wid
*s Video Input Source 1 Resolution Width: 1920
*s Video Input Source 2 Resolution Width: 0
*s Video Input Source 3 Resolution Width: 0
*s Video Input Source 4 Resolution Width: 0
*s Video Output Connector 1 Resolution Width: 1920
*s Video Output Connector 2 Resolution Width: 1280
*s Video Output Connector 3 Resolution Width: 1280
** end
```

Value types and formats

The device supports the following value types:

- **Integer values: <x..y>**
Defines the valid range for an integer input. x = min value, y = max value.
- **Literal values: <X/Y/.I/Z>**
Defines the possible values for a given configuration.
- **String values: <S: x, y>**
Defines that the valid input for this configuration is a string with minimum length of x and maximum length of y characters. Strings can have rules that further specify their format and length.

Input values that contain spaces need to be quoted

Any values for configurations and commands containing spaces must be enclosed in quotes. Quotes are not necessary for values without spaces.

Example:

Correct: xCommand dial number: "my number contains spaces"
Correct: xCommand dial number: 12345
Incorrect: xCommand dial number: my number contains spaces

Case sensitivity

All commands are case-insensitive. All of the following commands will work.

```
XCOMMAND DIAL NUMBER: foo@bar.org
xcommand dial number: foo@bar.org
xCommand Dial Number: foo@bar.org
```



Commands

Commands instruct the device to execute actions, such as to dial a number or to search the phone book. All commands start with the prefix xCommand followed by a command path.

Writing [xCommand ?](#) on the command line will list all the top level commands.

To view the complete list of commands and their parameters, write [xCommand ??](#) on the command line.

Command arguments are key-value pairs.

When issuing a xCommand, the command consists of one argument and one required parameter. In this document the command usage is described for all xCommands, with both required and optional parameters. The optional parameters are in brackets.

Example:

```
xCommand Dial Number: 123
```

xCommand is the command prefix. The command to be executed is Dial.

The example contains one argument, Number: 123. Number is the key and 123 is its value. The key/value pair is separated with ":".

Configurations

Configurations are device settings that are persistent across boots. Like commands, also configurations are structured in a hierarchy.

Writing [xConfiguration ?](#) on the command line lists all the top level configurations.

Writing [xConfiguration ??](#) lists all configurations and their value spaces.

Writing [xConfiguration](#) lists all configurations and their current values. To list out only some of the configurations, write xConfiguration followed by one or more parts of the configuration paths.

Example: Set the H323 Alias ID

Type:

```
xConfiguration H323 Profile 1 H323Alias ID:  
"changed@company.com"
```

Example: Get the H323 Alias ID

Type:

```
xConfiguration H323 Profile 1 H323Alias ID
```

Result:

```
*c xConfiguration H323 Profile 1 H323Alias ID:  
"changed@company.com"
```

```
**end
```

Status

A status contains the current state of the device, such as connected calls, the status of the gatekeeper registration, connected inputs and output sources.

Writing [xStatus ?](#) on the command line lists all top level statuses.

Writing [xStatus](#) lists all statuses and their current values.

To list out only some of the statuses, write xstatus followed by the relevant part of the status path (address expression):

```
xStatus <address expression>
```



Multiline commands

Multiline commands are commands that support larger amounts of data as input than the single line commands. Typical use for these commands is to allow for provisioning of in-room control definitions, branding images (base64 encoded), macros, welcome banners, and security certificates.

To issue a multiline command, you start issuing it like any other xAPI command. However, once you enter the command, you have set the API into an input mode where anything you issue on the API after this is treated as input to that command, including line breaks. You now enter the payload for this command in accordance to the input format expected by this command

When done, finish with a line break("\n") and a separate line containing just a period ending with a line break ("\n"). The command will now be executed, and you get a command result with an OK or ERROR depending on the command being executed successfully or not.

The commands that require multiline input format are marked as such in the command descriptions in this guide.

The multiline commands are marked as multiline in xCommand overview section in this guide.

Example: Set up welcome banner text

```
xCommand SystemUnit WelcomeBanner Set
Hello!
This is the second line of text.
This is the third.
Thank you!
.

OK
*r WelcomeBannerSetResult (status=OK):
** end
```



Synchronous API calls

The API works asynchronously. This means that there is no guarantee that command responses arrive in the same order as the commands were issued. The device may also respond with feedback between your request and the response, in form of status changes or events, due to changes on the device.

For some applications it might be crucial to match requests with responses. The API therefore supports a response-tagging mechanism.

This mechanism works with all command types: xcommand, xconfiguration, and xstatus. A typical use of this would be to create a command queue in your application and assign unique IDs to every command sent to the device. A listener then listens to all feedback from the device and matches the ID on the response with the corresponding ID in the command queue. This enables matching the original request with the specific response.

Example:

```
xcommand Video Layout Add | resultId="mytag_1"
OK
*r VideoLayoutAddResult (status=OK):
LayoutId: 1
** resultId: "mytag_1"
** end
```

In XML mode the resultId is added as an attribute to the top-level XmlDocument tag:

```
xgetxml /Configuration/Video/Layout/Scaling | resultId="mytag_2"
<XmlDoc resultId="mytag_2">
<Configuration item="1">
  <Video item="1">
    <Layout item="1">
      <Scaling item="1" valueSpaceRef="...">Off</Scaling>
    </Layout>
  </Video>
</Configuration>
</XmlDoc>
```



Events

Event returns information about the events that are available for feedback. This overview presents examples of some the events that are available on the API.

To get an overview of the supported events:

- **xEvent** - Lists the top level events
- **xEvent <top level category>** - List all of the available events in that category
- **xEvent *** - Lists all available events on that device

The result for events depends on the state of the device.

Example 1: Outgoing Call Indication

Outgoing Call Indication is an event reported when an outgoing call is about to be dialled. Returns the CallId the call has been assigned.

```
*e OutgoingCallIndication CallId: x  
** end
```

Example 2: Call Disconnect

Call Disconnect is an event reported when a call is disconnected. Returns the CallId of the disconnected call and reason for the call's disconnection.

```
*e CallDisconnect CallId: x CauseValue: 0  
CauseString: "" CauseType: LocalDisconnect  
OrigCallDirection: "outgoing"  
** end
```

Example 3: Call Successful

Call Successful is an event reported when a call is connected successfully, that is when all channels are up and established.

```
*e CallSuccessful CallId: 132 Protocol: "h223"  
Direction: "outgoing" CallRate: 768 RemoteURI:  
"h223:integratorHQ@company.com" EncryptionIn:  
"Off" EncryptionOut: "Off"  
** end
```

Example 4: FECC Action request

FECC Action request is an event reported when far end is sending FECC commands.

```
*e FeccActionInd Id: 132 Req: 1 Pan: 1 PanRight:  
1 Tilt: 0 TiltUp: 0 Zoom: 0 ZoomIn: 0 Focus: 0  
FocusIn: 0 Timeout: 300 VideoSrc: 0 m: 0  
** end
```

Example 5: TString message received

TString message received is an event reported when far end has sent a TString message.

```
*e TString CallId: 132 Message: "ee"  
** end
```

Example 6: SString message received

SString message received is an event reported when far end has sent a SString message.

```
*e SString String: "ee" Id: 132  
** end
```



Feedback mechanism

To build solutions that can reliably keep the state between your application and the device synchronized, you can set up a notification system to report the changes in the state of the device.

The API supports notifications on the following:

- Configuration changes
- Status changes
- Event notifications

These notifications will not be sent unless you have explicitly told the device to do so. You can subscribe to the feedback by registering feedback expressions. How you register feedback expressions varies according to the connection method used.

When using HTTP, the method of handling feedback differs slightly from what is presented in this section. See “[Feedback from the device over HTTP](#)” on page 20 for more information.

WARNING: A device may give very much feedback, especially when calls are connected and disconnected. Do only subscribe to the feedback you need.

Never register for all status feedback by issuing `xFeedback register /Status`. This may give the control application too much data to handle, which may lead to sluggish or unpredictable behavior.

Feedback expressions

The expression used when registering for feedback is a variant of the XPath language. The XPath language describes a way to select nodes from an XML/JSON document. The CE software contains three main feedback documents.

Document	API command	Path
Status	<code>xStatus</code>	<code>/Status</code>
Configuration	<code>xConfiguration</code>	<code>/Configuration</code>
Event	<code>xEvent</code>	<code>/Event</code>

The syntax for feedback registering is:

`xFeedback register <path>`

Never register for all status feedback by issuing `xFeedback register /Status`.

It is safe to register for all configuration changes using `xFeedback register /Configuration`, as configuration changes will most likely not occur that often.

By going through some examples, we can see how this information can be used to build feedback expressions. A good way to verify the expressions is to point your browser to <http://<ip-address>/getxml?location=path> or to execute `xgetxml <path>` from the terminal, and check that the output matches the nodes you want feedback on.

Example 1: Microphones Mute status

Terminal query

```
xStatus Audio Microphones Mute  
*s Audio Microphones Mute: Off  
** end
```

Equivalent feedback expression

```
xFeedback register /Status/Audio/Microphones/Mute
```

Example 2: Name of all video input connectors

Terminal query

```
xConfiguration Video Input Connector Name  
*c xConfiguration Video Input Connector 1 Name:  
"NameA"  
*c xConfiguration Video Input Connector 2 Name:  
"NameB"  
*c xConfiguration Video Input Connector 3 Name:  
"NameC"  
*c xConfiguration Video Input Connector 4 Name:  
"NameD"  
*c xConfiguration Video Input Connector 5 Name:  
"NameE"  
** end
```

Equivalent feedback expression

```
xFeedback register /Configuration/Video/Input/  
Connector/Name
```

Example 3: Name of video input connector 3

Terminal query

```
xConfiguration Video Input Connector 3 Name  
*c xConfiguration Video Input Connector 3 Name:  
"NameC"  
** end
```

Equivalent feedback expression

```
xFeedback register /Configuration/Video/Input/  
Connector[item='3']/Name
```



Terminal connections

Managing feedback subscriptions

To register, list and deregister feedback expressions you use the command xFeedback and its corresponding sub commands.

The registered expressions are only valid for the currently active connection. If you open two Telnet sessions and register to get feedback in one session, you do not receive feedback in the other session. This also means that if you disconnect from a session, you have to re-register all expressions after reconnecting.

You can register up to 38 expressions.

Feedback output

The feedback output is exactly the same as you get when querying the device using the xConfiguration and xStatus commands. E.g., if you issue the command xStatus Standby Active on the command line the result is:

```
*s Standby Active: On  
** end
```

If you have registered for feedback on status changes the feedback you get when the device goes to standby-mode will be exactly the same:

```
*s Standby Active: On  
** end
```

This means that when you are programming against the device you only need to handle one format.

Example: Managing feedback subscriptions

A: Register feedback expressions.

Write in: xFeedback register /Status/Audio
Result: ** end
OK

Write in: xFeedback register /Event/CallDisconnect
Result: ** end
OK

Write in: xFeedback register /Configuration/Video/
MainVideoSource
Result: ** end
OK

B: List out currently registered expressions.

Write in: xFeedback list
Result: /Configuration/Video/MainVideoSource
/Event/CallDisconnect
/Status/Audio
** end
OK

C: Deregister feedback expressions.

Write in: xFeedback deregister /Event/CallDisconnect
Result: ** end
OK
Write in: xFeedback deregister /Status/Audio
Result: ** end
OK

D: List the new feedback expressions.

Write in: xFeedback list
Result: /Configuration/Video/MainVideoSource
** end
OK



Using HTTP

The device supports sending commands and configurations over HTTP and HTTPS. It is also possible to retrieve configurations and statuses this way. This interface exposes the same API as the command line, but in XML format.

HTTP XMLAPI Authentication

Access to the XMLAPI requires the user to authenticate using HTTP Basic Access Authentication as a user with 'ADMIN' role. Unauthenticated requests prompt a 401 HTTP response containing a Basic Access Authentication challenge. How to use HTTP Basic Access Authentication varies according to the HTTP library or tool that you are using.

If your application will be issuing multiple commands through the API, we highly recommend that you use Session Authentication (see below). The standard basic authentication does a full re-authentication per request, which may affect the performance of your application.

HTTP XMLAPI Session Authentication

Authenticating with your username and password combination for each API request might introduce too much latency for some use-cases. To mitigate this, the API supports a session-based authentication mechanism.

To open a session, issue a POST to <http://<ip-address>/xmlapi/session/begin> with Basic Access Authentication. The response sets a SessionId-cookie that can be used with subsequent requests.

Note that when using API Session Authentication, it is important to explicitly close the session when you are done. Failing to do so may cause the device to run out of sessions, as there are a limited number of concurrent sessions available, and they do not time out automatically.

URL cheat sheet

The following table contains the main URLs used when accessing the API over HTTP.

Method	URL	Description
GET	http://<ip-address>/status.xml	Complete status document
GET	http://<ip-address>/configuration.xml	Complete configuration document
GET	http://<ip-address>/command.xml	Complete command document
GET	http://<ip-address>/valuespace.xml	Complete valuespace document
GET	http://<ip-address>/getxml?location=<path>	Retrieve document based on a path
POST	http://<ip-address>/putxml	Configurations and commands in HTTP body

Example: Starting a HTTP XMLAPI session

Request:

```
POST /xmlapi/session/begin HTTP/1.1
Authorization: Basic <Base64 encoded authentication string>
```

Response:

```
HTTP/1.1 204 No Content
Server: nginx/1.8.0
Connection: keep-alive
Set-Cookie: SessionId=f08102c8ce5aaf8fba23a7238cc2ef46
cc2ef464b990e18bfb7fb048820c0e28955c54; Path=/;
HttpOnly
```

This session counts toward the device's concurrent sessions limit.

With an open session, provide the SessionId cookie to following requests. Your tool/library may do this automatically.

Example: Using a HTTP XMLAPI session

Request:

```
GET /configuration.xml HTTP/1.1
Cookie: SessionId=f08102c8ce5aaf8fba23a7238cc2ef46
4b990e18bfb7fb048820c0e28955c54
```

Response:

```
HTTP/1.1 200 OK
Server: nginx/1.8.0
Content-Type: text/xml; charset=UTF-8
Content-Length: 43549
Connection: keep-alive
<?xml version="1.0"?>
<Configuration product="Cisco Codec" version="ce8.2.0" apiVersion="4"> ...
</Configuration>
```

To close a session after use, issue a POST to <http://<ip-address>/xmlapi/session/end> with the provided cookie.

Example: Closing a HTTP XMLAPI session

Request:

```
POST /xmlapi/session/end HTTP/1.1
Cookie: SessionId=f08102c8ce5aaf8fba23a7238cc2ef46
4b990e18bfb7fb048820c0e28955c54
```

Response:

```
HTTP/1.1 204 No Content
Server: nginx/1.8.0
Connection: keep-alive
Set-Cookie: SessionId=; Max-Age=0; Path=/;
HttpOnly
```



Getting status and configurations

Example 1: Get all status entries on the device

```
http://<ip-address>/getxml?location=/Status
```

Example 2: Get just the audio statuses of the device

```
http://<ip-address>/getxml?location=/Status/Audio
```

Example 3: Get all configurations of the device

```
http://<ip-address>/getxml?location=/Configuration
```

Example 4: Get all video configurations of the device

```
http://<ip-address>/getxml?location=/Configuration/Video
```

Sending commands and configurations

Using HTTP POST

When sending configurations and commands to the device, it is important that the HTTP header Content-Type is set to text/xml, i.e. [Content-Type: text/xml](#). The body of the POST should contain the XML content.

Example 1: Changing the device name**Request**

```
POST /putxml HTTP/1.1  
Content-Type: text/xml
```

```
<Configuration>  
  <SystemUnit>  
    <Name>newName</Name>  
  </SystemUnit>  
</Configuration>
```

Example 2: Setting the camera position**Request**

```
POST /putxml HTTP/1.1  
Content-Type: text/xml  
  
<Command>  
  <Camera>  
    <PositionSet command="True">  
      <CameraId>1</CameraId>  
      <Pan>200</Pan>  
      <Tilt>200</Tilt>  
    </PositionSet>  
  </Camera>  
</Command>
```

Response

```
HTTP/1.1 200 OK  
Content-Type: text/xml  
Content-Length: 91  
  
<?xml version="1.0"?>  
<Command>  
  <CameraPositionSetResult item="1" status="OK"/>  
</Command>
```



Feedback from the device over HTTP

You can get the device to post http feedback messages (also known as webhooks) on changes to the API state, e.g. statuses, events and configuration updates. The HTTP Post feedback messages will be sent to the specified ServerURL. You can choose between events being posted in either XML or JSON format. You can subscribe to changes on multiple parts of the API by register up to 15 different feedback expressions.

Registering for feedback

The command for registering is `xCommand HttpFeedback Register`. The syntax for this command and its arguments are described in this section.

HttpFeedback Register syntax:

```
xCommand HttpFeedback Register
  FeedbackSlot: <1..4>
  ServerUrl(r): <S: 1, 2048>
  Format: <XML/JSON>
  Expression: <S: 1, 255>
  Expression: <S: 1, 255>
```

HttpFeedback Register arguments:

FeedbackSlot: The device can register up to 4 slots of servers requesting HTTP feedback. Set the registering to one of them.

NOTE: Avoid using FeedbackSlot 3 in an environment where Cisco TelePresence Management Suite (TMS) is used as TMS uses this feedback slot to register its expressions.

ServerUrl: The URL to the HTTP server where you want the device to post the HTTP feedback messages to.

Format: Set the format for the feedback from the HTTP server to XML or JSON.

Expression 1-15: The XPath expression specifies which parts of the Status, Configuration or Event documents are monitored. You can have from 1 to 15 XPath expressions

Register the expressions you want to receive feedback on. See ["Feedback mechanism" on page 16](#) for more information about the expression formats.

Example: Registering feedback on configuration changes, disconnect events and call status changes.

```
POST /putxml HTTP/1.1
Content-Type: text/xml

<Command>
  <HttpFeedback>
    <Register command="True">
      <FeedbackSlot>1</FeedbackSlot>
      <ServerUrl>http://127.0.0.1/
        myhttppostscripturl</ServerUrl>
      <Format>XML</Format>
      <Expression item="1">/Configuration</
        Expression>
      <Expression item="2">/Event/
        CallDisconnect</Expression>
      <Expression item="3">/Status/Call</
        Expression>
    </Register>
  </HttpFeedback>
</Command>
```

Feedback output

When the device notifies the registered HTTP server about changes, the body contains the same XML as when polling. There is however one small difference. The root-node contains an **Identification** node with children that specify the device from which the notification originated. This means that you can handle multiple devices with a single HTTP server URI.

Example: Audio volume changed.

```
<Configuration xmlns="http://www.company.com/XML/
CUIL/2.0">
  <Identification>
    <SystemName>My Device Name</SystemName>
    <MACAddress>00:00:de:ad:be:ef</MACAddress>
    <IPAddress>192.168.1.100</IPAddress>
    <ProductType>Cisco Codec</ProductType>
    <ProductID>Cisco Codec SX80</ProductID>
    <SWVersion>CE8.3.0.199465</SWVersion>
    <HWBoard>101401-5 [08]</HWBoard>
    <SerialNumber>PH0000000</SerialNumber>
  </Identification>
  <Audio item="1">
    <Volume item="1">60</Volume>
  </Audio>
</Configuration>
```



Translating from terminal mode to XML

Translating commands

The XML commands maintain the same structure as the terminal commands, but they use a parent-child relationship to describe the hierarchy. You can see this structure in the examples below.

Example 1: Setting up a call

Terminal

```
xCommand Dial Number: "12345" Protocol: H323
```

XML

```
<Command>
  <Dial command="True">
    <Number>12345</Number>
    <Protocol>H323</Protocol>
  </Dial>
</Command>
```

Example 2: Assigning volume level

Terminal

```
xCommand Audio Volume Set Level: 50
```

XML

```
<Command>
  <Audio>
    <Volume>
      <Set command="True">
        <Level>50</Level>
      </Set>
    </Volume>
  </Audio>
</Command>
```

Translating configurations

Translating from xConfiguration to XML is similar to commands, but with the addition of a special attribute item="NN" for specifying the index in arrays.

Example: Configuring the input source type for video input connector 2

Terminal

```
xConfiguration Video Input Connector 2
  InputSourceType: camera
```

XML

```
<Configuration>
  <Video>
    <Input>
      <Connector item="2">
        <InputSourceType>camera</
      InputSourceType>
    </Connector>
  </Input>
</Video>
</Configuration>
```



Dos and don'ts

Here are some best practices when programming the Cisco DX, MX, SX, and Room series and Webex Board API.

AVOID remote control emulation

The use of xCommand UserInterface OSD Key Click and xCommand UserInterface OSD Key Press commands is highly discouraged. The commands are still available in the API, but we recommend the use of direct commands, as this ensures backwards compatibility in your integrations. Program against the device, not the on-screen-display.

DO use complete commands

You should always use complete commands when programming, i.e. always use xConfiguration Video instead of xconf vid. The shortcuts can be used for searches in the API on the command line, but not for programming. The reason for this is that you might end up with ambiguous code when additional commands are added to the API.

DO NOT subscribe to unnecessary feedback

Subscribing to too much feedback may congest the control application. Although the amount of feedback may seem fine in the current version, the amount of feedback may grow in future releases.



Chapter 3

xConfiguration commands



Description of the xConfiguration commands

In this chapter, you can find a complete list of the xConfiguration commands.

We recommend you visit our web site regularly for updated versions of the manual.

Go to: ▶ <https://www.cisco.com/go/telepresence/docs>

Audio configuration	29	xConfiguration Conference Encryption Mode.....	34
xConfiguration Audio DefaultVolume	29	xConfiguration Conference FarEndControl Mode.....	34
xConfiguration Audio KeyClickDetector Attenuate.....	29	xConfiguration Conference FarEndControl SignalCapability	35
xConfiguration Audio KeyClickDetector Enabled	29	xConfiguration Conference FarEndMessage Mode.....	35
xConfiguration Audio SoundsAndAlerts RingTone.....	29	xConfiguration Conference MaxReceiveCallRate	35
xConfiguration Audio SoundsAndAlerts RingVolume	30	xConfiguration Conference MaxTransmitCallRate.....	35
xConfiguration Audio Ultrasound MaxVolume	30	xConfiguration Conference MaxTotalReceiveCallRate	36
CallHistory configuration	30	xConfiguration Conference MaxTotalTransmitCallRate	36
xConfiguration CallHistory Mode	30	xConfiguration Conference MicUnmuteOnDisconnect Mode.....	36
Cameras configuration	31	xConfiguration Conference Multipoint Mode	37
xConfiguration Cameras Camera [n] Backlight DefaultMode.....	31	FacilityService configuration	37
xConfiguration Cameras Camera [n] Brightness Mode.....	31	xConfiguration FacilityService Service [n] Type	37
xConfiguration Cameras Camera [n] Brightness DefaultLevel	31	xConfiguration FacilityService Service [n] Name	38
xConfiguration Cameras Camera [n] Focus Mode	31	xConfiguration FacilityService Service [n] Number	38
xConfiguration Cameras Camera [n] Gamma Mode	32	xConfiguration FacilityService Service [n] CallType	38
xConfiguration Cameras Camera [n] Gamma Level	32	H323 configuration	39
xConfiguration Cameras SpeakerTrack Mode.....	32	xConfiguration H323 Authentication Mode	39
Conference configuration.....	33	xConfiguration H323 Authentication LoginName.....	39
xConfiguration Conference AutoAnswer Mode	33	xConfiguration H323 Authentication Password	39
xConfiguration Conference AutoAnswer Mute	33	xConfiguration H323 CallSetup Mode.....	39
xConfiguration Conference AutoAnswer Delay	33	xConfiguration H323 Encryption KeySize	40
xConfiguration Conference DefaultCall Protocol	33	xConfiguration H323 Gatekeeper Address	40
xConfiguration Conference DefaultCall Rate	34	xConfiguration H323 H323Alias E164.....	40
xConfiguration Conference DoNotDisturb DefaultTimeout	34	xConfiguration H323 H323Alias ID.....	40
		xConfiguration H323 NAT Mode	41



xConfiguration H323 NAT Address	41	xConfiguration Network [n] IEEE8021X Eap Peap	48
HttpClient configuration	42	xConfiguration Network [n] IPStack	48
xConfiguration HttpClient Mode	42	xConfiguration Network [n] IPv4 Assignment	49
xConfiguration HttpClient AllowHTTP	42	xConfiguration Network [n] IPv4 Address	49
xConfiguration HttpClient AllowInsecureHTTPS	42	xConfiguration Network [n] IPv4 Gateway	49
HttpFeedback configuration	43	xConfiguration Network [n] IPv4 SubnetMask	49
xConfiguration HttpFeedback TlsVerify	43	xConfiguration Network [n] IPv6 Assignment	50
Logging configuration	43	xConfiguration Network [n] IPv6 Address	50
xConfiguration Logging External Mode	43	xConfiguration Network [n] IPv6 Gateway	50
xConfiguration Logging External Protocol	43	xConfiguration Network [n] IPv6 DHCPOptions	50
xConfiguration Logging External Server Address	44	xConfiguration Network [n] MTU	51
xConfiguration Logging External Server Port	44	xConfiguration Network [n] QoS Mode	51
xConfiguration Logging External TlsVerify	44	xConfiguration Network [n] QoS Diffserv Audio	51
xConfiguration Logging Internal Mode	44	xConfiguration Network [n] QoS Diffserv Video	51
Macros configuration	45	xConfiguration Network [n] QoS Diffserv Data	52
xConfiguration Macros Mode	45	xConfiguration Network [n] QoS Diffserv Signalling	52
xConfiguration Macros AutoStart	45	xConfiguration Network [n] QoS Diffserv ICMPv6	53
Network configuration	45	xConfiguration Network [n] QoS Diffserv NTP	53
xConfiguration Network [n] DNS DNSSEC Mode	45	xConfiguration Network [n] RemoteAccess Allow	53
xConfiguration Network [n] DNS Domain Name	45	xConfiguration Network [n] Speed	53
xConfiguration Network [n] DNS Server [m] Address	46	xConfiguration Network [n] VLAN Voice Mode	54
xConfiguration Network [n] IEEE8021X Mode	46	xConfiguration Network [n] VLAN Voice VlanId	54
xConfiguration Network [n] IEEE8021X TlsVerify	46	NetworkServices configuration	54
xConfiguration Network [n] IEEE8021X UseClientCertificate	46	xConfiguration NetworkServices CDP Mode	54
xConfiguration Network [n] IEEE8021X Identity	47	xConfiguration NetworkServices H323 Mode	54
xConfiguration Network [n] IEEE8021X Password	47	xConfiguration NetworkServices HTTP Mode	55
xConfiguration Network [n] IEEE8021X AnonymousIdentity	47	xConfiguration NetworkServices HTTP Proxy LoginName	55
xConfiguration Network [n] IEEE8021X Eap Md5	47	xConfiguration NetworkServices HTTP Proxy Password	55
xConfiguration Network [n] IEEE8021X Eap Ttls	48	xConfiguration NetworkServices HTTP Proxy Mode	55
xConfiguration Network [n] IEEE8021X Eap Tls	48	xConfiguration NetworkServices HTTP Proxy Url	56
		xConfiguration NetworkServices HTTP Proxy PACUrl	56
		xConfiguration NetworkServices HTTPS Server MinimumTLSVersion	56
		xConfiguration NetworkServices HTTPS StrictTransportSecurity	56
		xConfiguration NetworkServices HTTPS VerifyClientCertificate	57



xConfiguration NetworkServices NTP Mode	57	Provisioning configuration.....	66
xConfiguration NetworkServices NTP Server [n] Address	57	xConfiguration Provisioning Connectivity	66
xConfiguration NetworkServices NTP Server [n] Key	57	xConfiguration Provisioning ExternalManager Address	66
xConfiguration NetworkServices NTP Server [n] KeyId	58	xConfiguration Provisioning ExternalManager AlternateAddress	66
xConfiguration NetworkServices NTP Server [n] KeyAlgorithm.....	58	xConfiguration Provisioning ExternalManager Protocol	67
xConfiguration NetworkServices SIP Mode.....	58	xConfiguration Provisioning ExternalManager Path	67
xConfiguration NetworkServices SMTP Mode	58	xConfiguration Provisioning ExternalManager Domain	67
xConfiguration NetworkServices SMTP Server.....	59	xConfiguration Provisioning Mode	67
xConfiguration NetworkServices SMTP Port	59	xConfiguration Provisioning LoginName	68
xConfiguration NetworkServices SMTP Username	59	xConfiguration Provisioning Password.....	68
xConfiguration NetworkServices SMTP Password.....	59	xConfiguration Provisioning TlsVerify.....	68
xConfiguration NetworkServices SMTP From	60	Proximity configuration.....	69
xConfiguration NetworkServices SMTP Security	60	xConfiguration Proximity Mode.....	69
xConfiguration NetworkServices SNMP Mode.....	60	xConfiguration Proximity Services CallControl	69
xConfiguration NetworkServices SNMP Host [n] Address.....	60	xConfiguration Proximity Services ContentShare FromClients	69
xConfiguration NetworkServices SNMP CommunityName	61	xConfiguration Proximity Services ContentShare ToClients.....	69
xConfiguration NetworkServices SNMP SystemContact	61	RoomAnalytics configuration.....	70
xConfiguration NetworkServices SNMP SystemLocation	61	xConfiguration RoomAnalytics AmbientNoiseEstimation Mode	70
xConfiguration NetworkServices SSH Mode	61	xConfiguration RoomAnalytics PeopleCountOutOfCall	70
xConfiguration NetworkServices SSH HostKeyAlgorithm	62	xConfiguration RoomAnalytics PeoplePresenceDetector	70
xConfiguration NetworkServices UPnP Mode	62	Security configuration	71
xConfiguration NetworkServices Webcam	63	xConfiguration Security Audit Logging Mode	71
xConfiguration NetworkServices WelcomeText.....	63	xConfiguration Security Audit OnError Action.....	71
xConfiguration NetworkServices Wifi Allowed	63	xConfiguration Security Audit Server Address	71
Peripherals configuration	64	xConfiguration Security Audit Server Port	72
xConfiguration Peripherals Profile ControlSystems	64	xConfiguration Security Audit Server PortAssignment	72
Phonebook configuration	64	xConfiguration Security Session FailedLoginsLockoutTime	72
xConfiguration Phonebook Server [n] ID	64	xConfiguration Security Session InactivityTimeout.....	72
xConfiguration Phonebook Server [n] Pagination	64	xConfiguration Security Session MaxFailedLogins	73
xConfiguration Phonebook Server [n] TlsVerify	65	xConfiguration Security Session MaxSessionsPerUser	73
xConfiguration Phonebook Server [n] Type.....	65	xConfiguration Security Session MaxTotalSessions	73
xConfiguration Phonebook Server [n] URL	65		



xConfiguration Security Session ShowLastLogon.....	73	xConfiguration SystemUnit CrashReporting Mode	80
SerialPort configuration.....	74	xConfiguration SystemUnit CrashReporting Url.....	81
xConfiguration SerialPort Mode.....	74		
xConfiguration SerialPort BaudRate.....	74		
xConfiguration SerialPort LoginRequired.....	74		
SIP configuration	75	Time configuration.....	81
xConfiguration SIP ANAT	75	xConfiguration Time TimeFormat.....	81
xConfiguration SIP Authentication UserName	75	xConfiguration Time DateFormat	81
xConfiguration SIP Authentication Password	75	xConfiguration Time Zone.....	82
xConfiguration SIP DefaultTransport	75		
xConfiguration SIP DisplayName	76		
xConfiguration SIP Ice DefaultCandidate	76	UserInterface configuration.....	83
xConfiguration SIP Ice Mode.....	76	xConfiguration UserInterface Accessibility IncomingCallNotification	83
xConfiguration SIP ListenPort	76	xConfiguration UserInterface Branding AwakeBranding Colors	83
xConfiguration SIP MinimumTLSVersion	77	xConfiguration UserInterface ContactInfo Type	84
xConfiguration SIP Proxy [n] Address	77	xConfiguration UserInterface KeyTones Mode.....	84
xConfiguration SIP Turn Server	77	xConfiguration UserInterface Features Call End	84
xConfiguration SIP Turn UserName	77	xConfiguration UserInterface Features Call MidCallControls	85
xConfiguration SIP Turn Password.....	78	xConfiguration UserInterface Features Call Start	85
xConfiguration SIP URI	78	xConfiguration UserInterface Features Call VideoMute	85
Standby configuration	78	xConfiguration UserInterface Features HideAll.....	85
xConfiguration Standby Control.....	78	xConfiguration UserInterface Features Share Start	86
xConfiguration Standby Delay.....	78	xConfiguration UserInterface Features Whiteboard Start	86
xConfiguration Standby Signage Audio	79	xConfiguration UserInterface Language	86
xConfiguration Standby Signage InteractionMode	79	xConfiguration UserInterface OSD EncryptionIndicator	86
xConfiguration Standby Signage Mode	79	xConfiguration UserInterface OSD Output	87
xConfiguration Standby Signage RefreshInterval	79	xConfiguration UserInterface Phonebook Mode	87
xConfiguration Standby Signage Url	80	xConfiguration UserInterface Security Mode	87
xConfiguration Standby WakeupOnMotionDetection	80	xConfiguration UserInterface SettingsMenu Mode	88
SystemUnit configuration	80	xConfiguration UserInterface SettingsMenu Visibility	88
xConfiguration SystemUnit Name	80	xConfiguration UserInterface SoundEffects Mode	88
		UserManagement configuration	89
		xConfiguration UserManagement LDAP Admin Filter	89
		xConfiguration UserManagement LDAP Admin Group	89
		xConfiguration UserManagement LDAP Attribute	89
		xConfiguration UserManagement LDAP BaseDN	89
		xConfiguration UserManagement LDAP Encryption	90



xConfiguration UserManagement LDAP MinimumTLSVersion	90
xConfiguration UserManagement LDAP Mode	90
xConfiguration UserManagement LDAP Server Address	91
xConfiguration UserManagement LDAP Server Port	91
xConfiguration UserManagement LDAP VerifyServerCertificate	91
Video configuration	92
xConfiguration Video DefaultMainSource	92
xConfiguration Video Input Connector [n] CameraControl Camerald	92
xConfiguration Video Input Connector [n] CameraControl Mode	92
xConfiguration Video Input Connector [n] CEC Mode	92
xConfiguration Video Input Connector [n] InputSourceType	93
xConfiguration Video Input Connector [n] Name	93
xConfiguration Video Input Connector [n] PreferredResolution	93
xConfiguration Video Input Connector [n] PresentationSelection	94
xConfiguration Video Input Connector [n] Quality	94
xConfiguration Video Input Connector [n] Visibility	94
xConfiguration Video Output Connector [n] Resolution	95
xConfiguration Video Presentation DefaultSource	95
xConfiguration Video Presentation Priority	95
xConfiguration Video Selfview Default FullscreenMode	95
xConfiguration Video Selfview Default Mode	96
xConfiguration Video Selfview Default OnMonitorRole	96
xConfiguration Video Selfview Default PIPPosition	96
xConfiguration Video Selfview OnCall Mode	96
xConfiguration Video Selfview OnCall Duration	97
WebEngine configuration	97
xConfiguration WebEngine Mode	97
xConfiguration WebEngine RemoteDebugging	97



Audio configuration

xConfiguration Audio DefaultVolume

Requires user role: ADMIN, INTEGRATOR, USER

Define the default volume for the speakers. The volume is set to this value when you switch on or restart the video conferencing device. 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 device is running, and to reset to default value.

USAGE:

xConfiguration Audio DefaultVolume: DefaultVolume

where

DefaultVolume: 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.

Default value: 70

xConfiguration Audio KeyClickDetector Attenuate

Requires user role: ADMIN, INTEGRATOR, USER

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb the other participants. If the participant types on the keyboard and speaks at the same time the microphone signal will not be attenuated. Requires that the Audio KeyClickDetector Enabled setting is set to On.

USAGE:

xConfiguration Audio KeyClickDetector Attenuate: Attenuate

where

Attenuate: False/True

False: The attenuation of the microphone signal is disabled.

True: The device attenuates the microphone signal if clicking noise from keyboards is detected. If voice or voice + keyboard clicks are detected the microphone signal is not attenuated.

Default value: True

xConfiguration Audio KeyClickDetector Enabled

Requires user role: ADMIN, INTEGRATOR, USER

The device can detect clicking noise from a keyboard and automatically attenuate the microphone signal. This is useful when a meeting participant starts typing on the keyboard, because the noise can disturb other participants. To enable attenuation on the microphone signal, set the Audio KeyClickDetector Attenuate to On.

USAGE:

xConfiguration Audio KeyClickDetector Enabled: Enabled

where

Enabled: False/True

False: The key click detection is disabled.

True: The device will detect clicking noise from keyboards.

Default value: True

xConfiguration Audio SoundsAndAlerts RingTone

Requires user role: ADMIN, INTEGRATOR, USER

Define which ringtone to use for incoming calls.

USAGE:

xConfiguration Audio SoundsAndAlerts RingTone: RingTone

where

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

Select a ringtone from the list.

Default value: Waves



xConfiguration Audio SoundsAndAlerts RingVolume

Requires user role: ADMIN, INTEGRATOR, USER

Define the ring volume for incoming calls.

USAGE:

xConfiguration Audio SoundsAndAlerts RingVolume: *RingVolume*

where

RingVolume: 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.

Default value: 50

xConfiguration Audio Ultrasound MaxVolume

Requires user role: ADMIN, INTEGRATOR

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

USAGE:

xConfiguration Audio Ultrasound MaxVolume: *MaxVolume*

where

MaxVolume: Integer (0..70)

Select a value in the specified range. If set to 0, the ultrasound is switched off.

Default value: 70

CallHistory configuration

xConfiguration CallHistory Mode

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration CallHistory Mode: *Mode*

where

Mode: Off/On

Off: New entries are not added to the call history.

On: New entries are stored in the call history list.

Default value: On



Cameras configuration

xConfiguration Cameras Camera [n] Backlight DefaultMode

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Cameras Camera n Backlight DefaultMode: DefaultMode

where

DefaultMode: Off/On

Off: Turn off the camera backlight compensation.

On: Turn on the camera backlight compensation.

Default value: Off

xConfiguration Cameras Camera [n] Brightness Mode

Requires user role: ADMIN, INTEGRATOR

Define the camera brightness mode.

USAGE:

xConfiguration Cameras Camera n Brightness Mode: Mode

where

Mode: Auto/Manual

Auto: The camera brightness is automatically set by the device.

Manual: Enable manual control of the camera brightness. The brightness level is set using the Cameras Camera [n] Brightness DefaultLevel setting.

Default value: Auto

xConfiguration Cameras Camera [n] Brightness DefaultLevel

Requires user role: ADMIN, INTEGRATOR

Define the brightness level. Requires the Cameras Camera [n] Brightness Mode to be set to Manual.

USAGE:

xConfiguration Cameras Camera n Brightness DefaultLevel: DefaultLevel

where

DefaultLevel: Integer (1..31)

The brightness level.

Default value: 20

xConfiguration Cameras Camera [n] Focus Mode

Requires user role: ADMIN, INTEGRATOR

Define the camera focus mode.

USAGE:

xConfiguration Cameras Camera n Focus Mode: Mode

where

Mode: Auto/Manual

Auto: The camera will do single shot auto focusing once a call is connected and when the view has changed.

Manual: Turn the autofocus off and adjust the camera focus manually.

Default value: Auto



xConfiguration Cameras Camera [n] Gamma Mode

Requires user role: ADMIN, INTEGRATOR

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

USAGE:

xConfiguration Cameras Camera n Gamma Mode: Mode

where

Mode: Auto/Manual

Auto: Auto is the default and the recommended setting.

Manual: In manual mode the gamma value is changed with the gamma level setting, ref. Cameras Camera [n] Gamma Level.

Default value: Auto

xConfiguration Cameras Camera [n] Gamma Level

Requires user role: ADMIN, INTEGRATOR

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

USAGE:

xConfiguration Cameras Camera n Gamma Level: Level

where

Level: Integer (0..7)

Define the gamma level.

Default value: 0

xConfiguration Cameras SpeakerTrack Mode

Requires user role: ADMIN, INTEGRATOR

The video conferencing device supports the Best overview feature. Best overview uses automatic camera framing to select the best camera view based on where people are in the room. Speaker tracking is not supported.

USAGE:

xConfiguration Cameras SpeakerTrack Mode: Mode

where

Mode: Auto/Off

Auto: Best overview is switched on. The device will detect people in the room and automatically select the best camera framing. Users can switch best overview on or off instantly in the camera control panel on the Touch controller, but the feature is switched back on after each call so that the device is ready for the next user.

Off: Best overview is switched off.

Default value: Auto



Conference configuration

xConfiguration Conference AutoAnswer Mode

Requires user role: ADMIN

Define the auto answer mode. Use the Conference AutoAnswer Delay setting if you want the device 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.

USAGE:

xConfiguration Conference AutoAnswer Mode: Mode

where

Mode: Off/On

Off: You can answer incoming calls manually by tapping Answer on the Touch controller.

On: The device 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.

Default value: Off

xConfiguration Conference AutoAnswer Mute

Requires user role: ADMIN

Define if the microphone shall be muted when an incoming call is automatically answered. Requires that AutoAnswer Mode is switched on.

USAGE:

xConfiguration Conference AutoAnswer Mute: Mute

where

Mute: Off/On

Off: The incoming call will not be muted.

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

Default value: Off

xConfiguration Conference AutoAnswer Delay

Requires user role: ADMIN

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

USAGE:

xConfiguration Conference AutoAnswer Delay: Delay

where

Delay: Integer (0..50)

The auto answer delay (seconds).

Default value: 0

xConfiguration Conference DefaultCall Protocol

Requires user role: ADMIN

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

USAGE:

xConfiguration Conference DefaultCall Protocol: Protocol

where

Protocol: 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 device 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 devices. Do not use.

Default value: Auto



xConfiguration Conference DefaultCall Rate

Requires user role: ADMIN, INTEGRATOR

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

USAGE:

xConfiguration Conference DefaultCall Rate: Rate

where

Rate: Integer (64..10000)

The default call rate (kbps).

Default value: 10000

xConfiguration Conference DoNotDisturb DefaultTimeout

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Conference DoNotDisturb DefaultTimeout: DefaultTimeout

where

DefaultTimeout: Integer (1..1440)

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

Default value: 60

xConfiguration Conference Encryption Mode

Requires user role: ADMIN

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 device, the encryption mode is always Off.

USAGE:

xConfiguration Conference Encryption Mode: Mode

where

Mode: Off/On/BestEffort

Off: The device will not use encryption.

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

BestEffort: The device will use encryption whenever possible.

> In Point to point calls: If the far end device 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.

Default value: BestEffort

xConfiguration Conference FarEndControl Mode

Requires user role: ADMIN

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).

USAGE:

xConfiguration Conference FarEndControl Mode: Mode

where

Mode: 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.

Default value: On



xConfiguration Conference FarEndControl SignalCapability

Requires user role: ADMIN

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

USAGE:

xConfiguration Conference FarEndControl SignalCapability: SignalCapability

where

SignalCapability: Off/On

Off: Disable the far end control signal capability.

On: Enable the far end control signal capability.

Default value: On

xConfiguration Conference FarEndMessage Mode

Requires user role: ADMIN

Toggle whether it is allowed to send data between two devices 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.

USAGE:

xConfiguration Conference FarEndMessage Mode: Mode

where

Mode: Off/On

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

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

Default value: Off

xConfiguration Conference MaxReceiveCallRate

Requires user role: ADMIN

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.

USAGE:

xConfiguration Conference MaxReceiveCallRate: MaxReceiveCallRate

where

MaxReceiveCallRate: Integer (64..10000)

The maximum receive call rate (kbps).

Default value: 10000

xConfiguration Conference MaxTransmitCallRate

Requires user role: ADMIN

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.

USAGE:

xConfiguration Conference MaxTransmitCallRate: MaxTransmitCallRate

where

MaxTransmitCallRate: Integer (64..6000)

The maximum transmitt call rate (kbps).

Default value: 6000



xConfiguration Conference MaxTotalReceiveCallRate

Requires user role: ADMIN

This configuration applies when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

Define the maximum overall receive bit rate allowed. The bit rate will be divided fairly among all active calls at any time. This means that the individual calls will be up-speeded or down-speeded as appropriate when someone leaves or enters a multipoint conference, or when a call is put on hold (suspended) or resumed.

The maximum receive bit rate for each individual call is defined in the Conference MaxReceiveCallRate setting.

USAGE:

xConfiguration Conference MaxTotalReceiveCallRate: [MaxTotalReceiveCallRate](#)

where

[MaxTotalReceiveCallRate](#): Integer (64..10000)

The maximum receive call rate (kbps).

Default value: 10000

xConfiguration Conference MaxTotalTransmitCallRate

Requires user role: ADMIN

This configuration applies when using a device's built-in MultiSite feature (optional) to host a multipoint video conference.

Define the maximum overall transmit bit rate allowed. The bit rate will be divided fairly among all active calls at any time. This means that the individual calls will be up-speeded or down-speeded as appropriate when someone leaves or enters a multipoint conference, or when a call is put on hold (suspended) or resumed.

The maximum transmit bit rate for each individual call is defined in the Conference MaxTransmitCallRate setting.

USAGE:

xConfiguration Conference MaxTotalTransmitCallRate: [MaxTotalTransmitCallRate](#)

where

[MaxTotalTransmitCallRate](#): Integer (64..6000)

The maximum transmit call rate (kbps).

Default value: 6000

xConfiguration Conference MicUnmuteOnDisconnect Mode

Requires user role: ADMIN

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 device for the next user.

USAGE:

xConfiguration Conference MicUnmuteOnDisconnect Mode: [Mode](#)

where

[Mode](#): 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.

Default value: On



xConfiguration Conference Multipoint Mode

Requires user role: ADMIN

Define how the device handles multiparty video conferences (ad hoc conferences).

If registered to a Cisco TelePresence Video Communication Server (VCS), the device can use its own built-in MultiSite feature. If registered to a Cisco Unified Communications Manager (CUCM) version 8.6.2 or newer, the device can use either the CUCM conference bridge, or the device's own built-in MultiSite feature. Which option to use, is set-up by CUCM.

The CUCM conference bridge allows you to set up conferences with many participants. The MultiSite feature allows up to four participants (yourself included).

The MultiSite feature is optional and may not be available on all devices.

USAGE:

xConfiguration Conference Multipoint Mode: Mode

where

Mode: Auto/CUCMMediaResourceGroupList/MultiSite/Off

Auto: The multipoint method is selected automatically; if no multipoint method is available, the Multipoint Mode will be set to Off.

CUCMMediaResourceGroupList: Multiparty conferences are hosted by the CUCM configured conference bridge. This setting is provisioned by CUCM in a CUCM environment, and should never be set manually by the user.

MultiSite: Multiparty conferences are set up using the built-in MultiSite feature. If MultiSite is selected when the MultiSite feature is not available, the Multipoint Mode will automatically be set to Off.

Off: Multiparty conferences are not allowed.

Default value: Auto

FacilityService configuration

xConfiguration FacilityService Service [n] Type

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration FacilityService Service n Type: Type

where

Type: 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.

Default value: Helpdesk



xConfiguration FacilityService Service [n] Name

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

```
xConfiguration FacilityService Service n Name: "Name"
```

where

Name: String (0, 1024)

The name of the facility service.

Default value: Service 1: "Live Support" Other services: "

xConfiguration FacilityService Service [n] Number

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

```
xConfiguration FacilityService Service n Number: "Number"
```

where

Number: String (0, 1024)

The number (URI or phone number) of the facility service.

Default value: "

xConfiguration FacilityService Service [n] CallType

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

```
xConfiguration FacilityService Service n CallType: CallType
```

where

CallType: Audio/Video

Audio: Select this option for audio calls.

Video: Select this option for video calls.

Default value: Video



H323 configuration

xConfiguration H323 Authentication Mode

Requires user role: ADMIN

Define the authenticatin mode for the H.323 profile.

USAGE:

xConfiguration H323 Authentication Mode: Mode

where

Mode: Off/On

Off: The device 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 device will try to authenticate itself to the gatekeeper. Requires the H323 Authentication LoginName and H323 Authentication Password settings to be defined on both the device and the Gatekeeper.

Default value: Off

xConfiguration H323 Authentication LoginName

Requires user role: ADMIN

The device 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 device to the H.323 Gatekeeper, i.e. the device is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the device will still try to register. Requires the H.323 Authentication Mode to be enabled.

USAGE:

xConfiguration H323 Authentication LoginName: "LoginName"

where

LoginName: String (0, 50)

The authentication login name.

Default value: ""

xConfiguration H323 Authentication Password

Requires user role: ADMIN

The device 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 device to the H.323 Gatekeeper, i.e. the device is authenticated to the gatekeeper. If the H.323 Gatekeeper indicates that no authentication is required, the device will still try to register. Requires the H.323 Authentication Mode to be enabled.

USAGE:

xConfiguration H323 Authentication Password: "Password"

where

Password: String (0, 50)

The authentication password.

Default value: ""

xConfiguration H323 CallSetup Mode

Requires user role: ADMIN

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.

USAGE:

xConfiguration H323 CallSetup Mode: Mode

where

Mode: Direct/Gatekeeper

Direct: You can only make an H.323 call by dialing an IP address directly.

Gatekeeper: The device uses a Gatekeeper to make an H.323 call. When choosing this option, the H323 Gatekeeper Address must also be configured.

Default value: Gatekeeper



xConfiguration H323 Encryption KeySize

Requires user role: ADMIN

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.

USAGE:

xConfiguration H323 Encryption KeySize: KeySize

where

KeySize: Max1024bit/Min1024bit/Min2048bit

Max1024bit: The maximum size is 1024 bit.

Min1024bit: The minimum size is 1024 bit.

Min2048bit: The minimum size is 2048 bit.

Default value: Min1024bit

xConfiguration H323 Gatekeeper Address

Requires user role: ADMIN

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

USAGE:

xConfiguration H323 Gatekeeper Address: "Address"

where

Address: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""

xConfiguration H323 H323Alias E164

Requires user role: ADMIN

The H.323 Alias E.164 defines the address of the device, 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.

USAGE:

xConfiguration H323 H323Alias E164: "E164"

where

E164: String (0, 30)

The H.323 Alias E.164 address. Valid characters are 0-9, * and #.

Default value: ""

xConfiguration H323 H323Alias ID

Requires user role: ADMIN

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

USAGE:

xConfiguration H323 H323Alias ID: "ID"

where

ID: String (0, 49)

The H.323 Alias ID. Example: "firstname.lastname@company.com", "My H.323 Alias ID"

Default value: ""



xConfiguration H323 NAT Mode

Requires user role: ADMIN

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 device (when the IP traffic goes through a NAT router). NOTE: NAT does not work in conjunction with gatekeepers.

USAGE:

xConfiguration H323 NAT Mode: Mode

where

Mode: Auto/Off/On

Auto: The device 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 devices on the LAN as well as devices on the WAN. If the H323 NAT Address is wrong or not set, the real IP address will be used.

Off: The device will signal the real IP address.

On: The device 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.

Default value: Off

xConfiguration H323 NAT Address

Requires user role: ADMIN

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

In the router, the following ports must be routed to the video conferencing device's IP address:

* Port 1720

* Port 5555-6555

* Port 2326-2487

USAGE:

xConfiguration H323 NAT Address: "Address"

where

Address: String (0, 64)

A valid IPv4 address or IPv6 address.

Default value: ""



HttpClient configuration

xConfiguration HttpClient Mode

Requires user role: ADMIN

Allow or prohibit communication with an external HTTP(S) server using HTTP(S) requests and responses.

USAGE:

```
xConfiguration HttpClient Mode: Mode
```

where

Mode: Off/On

Off: The video conferencing device cannot communicate with an external HTTP(S) server.

On: The video conferencing device is allowed to communicate with an external HTTP(S) server.

Default value: Off

xConfiguration HttpClient AllowHTTP

Requires user role: ADMIN

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.

USAGE:

```
xConfiguration HttpClient AllowHTTP: AllowHTTP
```

where

AllowHTTP: False/True

False: The video conferencing device can communicate only over HTTPS.

True: The video conferencing device can communicate over both HTTPS and HTTP.

Default value: True

xConfiguration HttpClient AllowInsecureHTTPS

Requires user role: ADMIN

You can choose whether or not to allow the video conferencing device to communicate with a server over HTTPS without checking the server's certificate first.

Even if the device 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.

USAGE:

```
xConfiguration HttpClient AllowInsecureHTTPS: AllowInsecureHTTPS
```

where

AllowInsecureHTTPS: False/True

False: The device always checks that the HTTPS server has a valid certificate. No communication with the server takes place if the certificate validation fails.

True: The device is allowed to skip the certificate validation process before communicating with the server.

Default value: False

HttpFeedback configuration

xConfiguration HttpFeedback TlsVerify

Requires user role: ADMIN

This setting applies when a video conferencing device connects to an HTTPS server for arbitrary HTTPS communication (refer to the HttpClient Post/Put/Patch/Get/Delete commands). For phone book, provisioning, and external logging servers, see the Phonebook Server 1 TlsVerify, Provisioning TlsVerify, and Logging External TlsVerify settings.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

USAGE:

xConfiguration HttpFeedback TlsVerify: TlsVerify

where

TlsVerify: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.

Default value: On

Logging configuration

xConfiguration Logging External Mode

Requires user role: ADMIN

Determine whether or not to store the device 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.

USAGE:

xConfiguration Logging External Mode: Mode

where

Mode: Off/On

Off: Device logs will not be stored on the remote syslog server.

On: Device logs will be stored on the remote syslog server.

Default value: Off

xConfiguration Logging External Protocol

Requires user role: ADMIN

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.

USAGE:

xConfiguration Logging External Protocol: Protocol

where

Protocol: Syslog/SyslogTLS

Syslog: Syslog protocol in plain text.

SyslogTLS: Syslog protocol over TLS.

Default value: SyslogTLS



xConfiguration Logging External Server Address

Requires user role: ADMIN

The address of the remote syslog server.

USAGE:

xConfiguration Logging External Server Address: "Address"

where

Address: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""

xConfiguration Logging External Server Port

Requires user role: ADMIN

The port that the remote syslog server listens for messages on. If set to 0, the device will use the standard syslog port. The standard syslog port is 514 for syslog, and 6514 for syslog over TLS.

USAGE:

xConfiguration Logging External Server Port: Port

where

Port: Integer (0..65535)

The number of the port that the remote syslog server is using. 0 means that the device uses the standard syslog port.

Default value: 514

xConfiguration Logging External TlsVerify

Requires user role: ADMIN

This setting applies when a video conferencing device connects to a remote syslog server. It applies to both regular logging (refer to the Logging External Mode setting) and audit logging (refer to the Security Audit Logging Mode setting).

Before establishing a connection between the device and the syslog server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

The minimum TLS (Transport Layer Security) version for the syslog connection is 1.1.

USAGE:

xConfiguration Logging External TlsVerify: TlsVerify

where

TlsVerify: Off/On

Off: The device doesn't check the certificate of the syslog server.

On: The device checks if the certificate of the syslog server can be trusted. If not, the connection between the device and the server is not established.

Default value: On

xConfiguration Logging Internal Mode

Requires user role: ADMIN

Determine whether or not to store the system logs on the device (local files). These are the files that you get when you download the log bundles from the device. This setting has no effect if the Logging Mode setting is set to Off.

USAGE:

xConfiguration Logging Internal Mode: Mode

where

Mode: Off/On

Off: System logs will not be stored on the device.

On: System logs will be stored on the device.

Default value: On



Macros configuration

xConfiguration Macros Mode

Requires user role: ADMIN

Macros allow you to write snippets of JavaScript code that can automate parts of your video conferencing device, 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 device. Use this setting when you want to manually enable, or to permanently disable the use of macros on the device. You can disable the use of macros within the Macro Editor. But this will not permanently disable macros from running, because every time the device is reset the macros will be re-enabled automatically.

USAGE:

xConfiguration Macros Mode: Mode

where

Mode: Off/On

Off: Permanently disable the use of macros on this device.

On: Enable the use of macros on this device.

Default value: Off

xConfiguration Macros AutoStart

Requires user role: ADMIN

All the macros run in a single process on the video conferencing device, called the macro runtime. It should be running by default, but you can choose to stop and start it manually. If you restart the device, the runtime will automatically start again if auto start is enabled.

USAGE:

xConfiguration Macros AutoStart: AutoStart

where

AutoStart: Off/On

Off: The macro runtime will not start automatically after a restart of the device.

On: The macro runtime will start automatically after a restart of the device.

Default value: On

Network configuration

xConfiguration Network [n] DNS DNSSEC Mode

Requires user role: ADMIN

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.

USAGE:

xConfiguration Network n DNS DNSSEC Mode: Mode

where

Mode: Off/On

Off: Disable Domain Name System Security Extensions.

On: Enable Domain Name System Security Extensions.

Default value: Off

xConfiguration Network [n] DNS Domain Name

Requires user role: ADMIN, USER

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".

USAGE:

xConfiguration Network n DNS Domain Name: "Name"

where

Name: String (0, 64)

The DNS domain name.

Default value: ""



xConfiguration Network [n] DNS Server [m] Address

Requires user role: ADMIN, USER

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.

USAGE:

`xConfiguration Network n DNS Server m Address: "Address"`

where

Address: String (0, 64)

A valid IPv4 address or IPv6 address.

Default value: ""

xConfiguration Network [n] IEEE8021X Mode

Requires user role: ADMIN, USER

The device 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.

USAGE:

`xConfiguration Network n IEEE8021X Mode: Mode`

where

Mode: Off/On

Off: The 802.1X authentication is disabled.

On: The 802.1X authentication is enabled.

Default value: Off

xConfiguration Network [n] IEEE8021X TlsVerify

Requires user role: ADMIN, USER

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 conferencing device. This can be done from the web interface.

This setting takes effect only when Network [1] IEEE8021X Eap Tls is enabled (On).

USAGE:

`xConfiguration Network n IEEE8021X TlsVerify: TlsVerify`

where

TlsVerify: 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 device.

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.

Default value: Off

xConfiguration Network [n] IEEE8021X UseClientCertificate

Requires user role: ADMIN, USER

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

USAGE:

`xConfiguration Network n IEEE8021X UseClientCertificate: UseClientCertificate`

where

UseClientCertificate: Off/On

Off: When set to Off client-side authentication is not used (only server-side).

On: When set to On the client (video conferencing device) will perform a mutual authentication TLS handshake with the server.

Default value: Off



xConfiguration Network [n] IEEE8021X Identity

Requires user role: ADMIN, USER

Define the username for 802.1X authentication.

USAGE:

```
xConfiguration Network n IEEE8021X Identity: "Identity"
```

where

Identity: String (0, 64)

The username for 802.1X authentication.

Default value: ""

xConfiguration Network [n] IEEE8021X Password

Requires user role: ADMIN, USER

Define the password for 802.1X authentication.

USAGE:

```
xConfiguration Network n IEEE8021X Password: "Password"
```

where

Password: String (0, 50)

The password for 802.1X authentication.

Default value: ""

xConfiguration Network [n] IEEE8021X AnonymousIdentity

Requires user role: ADMIN, USER

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.

USAGE:

```
xConfiguration Network n IEEE8021X AnonymousIdentity: "AnonymousIdentity"
```

where

AnonymousIdentity: String (0, 64)

The 802.1X Anonymous ID string.

Default value: ""

xConfiguration Network [n] IEEE8021X Eap Md5

Requires user role: ADMIN, USER

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.

USAGE:

```
xConfiguration Network n IEEE8021X Eap Md5: Md5
```

where

Md5: Off/On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled.

Default value: On



xConfiguration Network [n] IEEE8021X Eap Ttls

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n IEEE8021X Eap Ttls: Ttls

where

Ttls: Off/On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled.

Default value: On

xConfiguration Network [n] IEEE8021X Eap Tls

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n IEEE8021X Eap Tls: Tls

where

Tls: Off/On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled.

Default value: On

xConfiguration Network [n] IEEE8021X Eap Peap

Requires user role: ADMIN, USER

Define the Peap (Protected Extensible Authentication Protocol) mode. Authenticates LAN clients without the need for client certificates. Developed by Microsoft, Cisco and RSA Security.

USAGE:

xConfiguration Network n IEEE8021X Eap Peap: Peap

where

Peap: Off/On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled.

Default value: On

xConfiguration Network [n] IPStack

Requires user role: ADMIN, USER

Select if the device 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.

USAGE:

xConfiguration Network n IPStack: IPStack

where

IPStack: 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 device will use IPv4 on the network interface.

IPv6: When set to IPv6, the device will use IPv6 on the network interface.

Default value: Dual



xConfiguration Network [n] IPv4 Assignment

Requires user role: ADMIN, USER

Define how the device 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.

USAGE:

xConfiguration Network n IPv4 Assignment: Assignment

where

Assignment: 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 device addresses are automatically assigned by the DHCP server.

Default value: DHCP

xConfiguration Network [n] IPv4 Address

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv4 Address: "Address"

where

Address: String (0, 64)

A valid IPv4 address.

Default value: ""

xConfiguration Network [n] IPv4 Gateway

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv4 Gateway: "Gateway"

where

Gateway: String (0, 64)

A valid IPv4 address.

Default value: ""

xConfiguration Network [n] IPv4 SubnetMask

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv4 SubnetMask: "SubnetMask"

where

SubnetMask: String (0, 64)

A valid IPv4 address.

Default value: ""



xConfiguration Network [n] IPv6 Assignment

Requires user role: ADMIN, USER

Define how the device 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.

USAGE:

xConfiguration Network n IPv6 Assignment: Assignment

where

Assignment: Static/DHCPv6/Autoconf

Static: The device 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.

Default value: Autoconf

xConfiguration Network [n] IPv6 Address

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv6 Address: "Address"

where

Address: String (0, 64)

A valid IPv6 address including a network mask. Example: 2001:DB8::/48

Default value: ""

xConfiguration Network [n] IPv6 Gateway

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv6 Gateway: "Gateway"

where

Gateway: String (0, 64)

A valid IPv6 address.

Default value: ""

xConfiguration Network [n] IPv6 DHCPOptions

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n IPv6 DHCPOptions: DHCPOptions

where

DHCPOptions: 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.

Default value: On



xConfiguration Network [n] MTU

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n MTU: MTU

where

MTU: Integer (576..1500)

Set a value for the MTU (bytes).

Default value: 1500

xConfiguration Network [n] QoS Mode

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Mode: Mode

where

Mode: 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.

Default value: Diffserv

xConfiguration Network [n] QoS Diffserv Audio

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv Audio: Audio

where

Audio: 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".

Default value: 0

xConfiguration Network [n] QoS Diffserv Video

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv Video: Video

where

Video: 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".

Default value: 0



xConfiguration Network [n] QoS Diffserv Data

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv Data: Data

where

Data: 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".

Default value: 0

xConfiguration Network [n] QoS Diffserv Signalling

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv Signalling: Signalling

where

Signalling: 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".

Default value: 0



xConfiguration Network [n] QoS DiffServ ICMPv6

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv ICMPv6: ICMPv6

where

ICMPv6: 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".

Default value: 0

xConfiguration Network [n] QoS DiffServ NTP

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n QoS Diffserv NTP: NTP

where

NTP: 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".

Default value: 0

xConfiguration Network [n] RemoteAccess Allow

Requires user role: ADMIN, USER

Define which IP addresses (IPv4/IPv6) are allowed for remote access to the device from SSH/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.

USAGE:

xConfiguration Network n RemoteAccess Allow: Allow

where

Allow: String (0..255)

A valid IPv4 address or IPv6 address.

Default value: ""

xConfiguration Network [n] Speed

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Network n Speed: Speed

where

Speed: 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.

Default value: Auto



xConfiguration Network [n] VLAN Voice Mode

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Network n VLAN Voice Mode: Mode

where

Mode: 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.

Default value: Auto

xConfiguration Network [n] VLAN Voice VlanId

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Network n VLAN Voice VlanId: VlanId

where

VlanId: Integer (1..4094)

Set the VLAN voice ID.

Default value: 1

NetworkServices configuration

xConfiguration NetworkServices CDP Mode

Requires user role: ADMIN

Enable or disable the CDP (Cisco Discovery Protocol) daemon. Enabling CDP will make the device 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.

USAGE:

xConfiguration NetworkServices CDP Mode: Mode

where

Mode: Off/On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

Default value: On

xConfiguration NetworkServices H323 Mode

Requires user role: ADMIN

Define whether the device should be able to place and receive H.323 calls or not.

USAGE:

xConfiguration NetworkServices H323 Mode: Mode

where

Mode: Off/On

Off: Disable the possibility to place and receive H.323 calls.

On: Enable the possibility to place and receive H.323 calls.

Default value: Off



xConfiguration NetworkServices HTTP Mode

Requires user role: ADMIN

Define whether or not to allow access to the device using the HTTP or HTTPS (HTTP Secure) protocols. Note that the device'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 devices that have been upgraded to CE9.4 (or later) from an earlier software version, provided that the device has not been factory reset after the upgrade.

USAGE:

xConfiguration NetworkServices HTTP Mode: Mode

where

Mode: Off/HTTP+HTTPS/HTTPS

Off: Access to the device not allowed via HTTP or HTTPS.

HTTP+HTTPS: Access to the device allowed via both HTTP and HTTPS.

HTTPS: Access to the device allowed via HTTPS, but not via HTTP.

Default value: HTTPS (changed from HTTP+HTTPS to HTTPS in CE9.4)

xConfiguration NetworkServices HTTP Proxy LoginName

Requires user role: ADMIN, USER

This is the username part of the credentials for authentication towards the HTTP proxy.

Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

USAGE:

xConfiguration NetworkServices HTTP Proxy LoginName: "LoginName"

where

LoginName: String (0, 80)

The authentication login name.

Default value: ""

xConfiguration NetworkServices HTTP Proxy Password

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration NetworkServices HTTP Proxy Password: "Password"

where

Password: String (0, 64)

The authentication password.

Default value: ""

xConfiguration NetworkServices HTTP Proxy Mode

Requires user role: ADMIN, USER

You can configure a device that is registered to the Cisco Webex cloud service to use a proxy server for HTTPS and WebSocket traffic. 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.

If the device is registered to an on-premise service such as CUCM or VCS, keep this setting Off.

USAGE:

xConfiguration NetworkServices HTTP Proxy Mode: Mode

where

Mode: 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.

Default value: Off



xConfiguration NetworkServices HTTP Proxy Url

Requires user role: ADMIN, USER

Set the URL of the HTTP proxy server. Requires that the NetworkServices HTTP Proxy Mode is set to Manual.

USAGE:

```
xConfiguration NetworkServices HTTP Proxy Url: "Url"
```

where

Url: String (0..255)

The URL of the HTTP proxy server.

Default value: ""

xConfiguration NetworkServices HTTP Proxy PACUrl

Requires user role: ADMIN, USER

Set the URL of the PAC (Proxy Auto Configuration) script. Requires that the NetworkServices HTTP Proxy Mode is set to PACUrl.

USAGE:

```
xConfiguration NetworkServices HTTP Proxy PACUrl: "PACUrl"
```

where

PACUrl: String (0..255)

The URL of the PAC (Proxy Auto Configuration) script.

Default value: ""

xConfiguration NetworkServices HTTPS Server MinimumTLSVersion

Requires user role: ADMIN

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

USAGE:

```
xConfiguration NetworkServices HTTPS Server MinimumTLSVersion: MinimumTLSVersion
```

where

MinimumTLSVersion: TLSv1.1/TLSv1.2

TLSv1.1: Support of TLS version 1.1 or higher.

TLSv1.2: Support of TLS version 1.2 or higher.

Default value: TLSv1.1

xConfiguration NetworkServices HTTPS StrictTransportSecurity

Requires user role: ADMIN

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.

USAGE:

```
xConfiguration NetworkServices HTTPS StrictTransportSecurity:
```

StrictTransportSecurity

where

StrictTransportSecurity: Off/On

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

Default value: Off



xConfiguration NetworkServices HTTPS VerifyClientCertificate

Requires user role: ADMIN

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

USAGE:

xConfiguration NetworkServices HTTPS VerifyClientCertificate:

VerifyClientCertificate

where

VerifyClientCertificate: 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 device in advance.

Default value: Off

xConfiguration NetworkServices NTP Mode

Requires user role: ADMIN

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

USAGE:

xConfiguration NetworkServices NTP Mode: Mode

where

Mode: Auto/Manual/Off

Auto: The device 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 device will use the NTP server that is specified in the NetworkServices NTP Server [n] Address setting for time reference.

Off: The device will not use an NTP server. The NetworkServices NTP Server [n] Address setting will be ignored.

Default value: Auto

xConfiguration NetworkServices NTP Server [n] Address

Requires user role: ADMIN

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.

USAGE:

xConfiguration NetworkServices NTP Server n Address: "Address"

where

Address: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: "0.tandberg.pool.ntp.org"

xConfiguration NetworkServices NTP Server [n] Key

Requires user role: ADMIN

To make sure that the NTP information comes from a trusted source, the video conferencing device 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.

USAGE:

xConfiguration NetworkServices NTP Server n Key: "Key"

where

Key: String (0, 2045)

The key, which is part of the ID/key pair that the NTP source uses.

Default value: ""



xConfiguration NetworkServices NTP Server [n] KeyId

Requires user role: ADMIN

To make sure that the NTP information comes from a trusted source, the video conferencing device 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.

USAGE:

```
xConfiguration NetworkServices NTP Server n KeyId: "KeyId"
```

where

KeyId: String (0, 10)

The ID, which is part of the ID/key pair that the NTP source uses.

Default value: ""

xConfiguration NetworkServices NTP Server [n] KeyAlgorithm

Requires user role: ADMIN

Choose the authentication hash function that the NTP server uses, and that the video conferencing device must use to authenticate the time messages.

USAGE:

```
xConfiguration NetworkServices NTP Server n KeyAlgorithm: KeyAlgorithm
```

where

KeyAlgorithm: 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).

Default value: ""

xConfiguration NetworkServices SIP Mode

Requires user role: ADMIN

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

USAGE:

```
xConfiguration NetworkServices SIP Mode: Mode
```

where

Mode: Off/On

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

On: Enable the possibility to place and receive SIP calls.

Default value: On

xConfiguration NetworkServices SMTP Mode

Requires user role: ADMIN

You can set up the device to use SMTP (Simple Mail Transfer Protocol) for sending email from the device to a mail server for relaying. This is required if you want to allow users to send their whiteboards and presentations via email to people inside or outside their organization.

If the device is set up for encrypted communication (see the NetworkServices SMTP Security setting), the device only allows connections where the SMTP server's certificate is validated. There is no option for ignoring the certificate check.

USAGE:

```
xConfiguration NetworkServices SMTP Mode: Mode
```

where

Mode: Off/On

Off: Disable SMTP (and email) support.

On: Enable SMTP support for sending email.

Default value: Off



xConfiguration NetworkServices SMTP Server

Requires user role: ADMIN

This is the address of the SMTP server.

USAGE:

xConfiguration NetworkServices SMTP Server: "Server"

where

Server: String (0, 255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""

xConfiguration NetworkServices SMTP Port

Requires user role: ADMIN

This port is used for outgoing emails from the device to the SMTP server.

Set a port number based on the encryption setting (NetworkServices SMTP Security) and the requirements of the SMTP server. Do not use the default value.

USAGE:

xConfiguration NetworkServices SMTP Port: Port

where

Port: Integer (0..65535)

The port used for outgoing emails from the device.

Default value: 0

xConfiguration NetworkServices SMTP Username

Requires user role: ADMIN

This is the username part of the credentials that are used to authenticate the device with the SMTP server. This setting may be required by the SMTP server.

USAGE:

xConfiguration NetworkServices SMTP Username: "Username"

where

Username: String (0, 50)

A valid username.

Default value: ""

xConfiguration NetworkServices SMTP Password

Requires user role: ADMIN

This is the password part of the credentials that are used to authenticate the device with the SMTP server. This setting may be required by the SMTP server.

USAGE:

xConfiguration NetworkServices SMTP Password: "Password"

where

Password: String (0, 64)

A valid password.

Default value: ""



xConfiguration NetworkServices SMTP From

Requires user role: ADMIN

When sending an email message from this device, this is the name of the mailbox that the message is sent from.

USAGE:

xConfiguration NetworkServices SMTP From: From

where

From: String (0..255)

An email address that meets the requirements of the SMTP server.

Default value: ""

xConfiguration NetworkServices SMTP Security

Requires user role: ADMIN

Choose if and how to secure the communication between the device and the SMTP server.

USAGE:

xConfiguration NetworkServices SMTP Security: Security

where

Security: None/StartTls/Tls

None: Connect to the SMTP server without encryption.

StartTls: Initially connect to the SMTP server without encryption, and then send a STARTTLS command to upgrade to an encrypted connection (TLS).

Tls: Connect to the SMTP server over TLS (Transport Layer Security).

Default value: None

xConfiguration NetworkServices SNMP Mode

Requires user role: ADMIN, INTEGRATOR

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 devices, which describe the device configuration. These variables can then be queried (set to ReadOnly) and sometimes set (set to ReadWrite) by managing applications.

USAGE:

xConfiguration NetworkServices SNMP Mode: Mode

where

Mode: 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.

Default value: ReadOnly

xConfiguration NetworkServices SNMP Host [n] Address

Requires user role: ADMIN, INTEGRATOR

Define the address of up to three SNMP Managers.

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

USAGE:

xConfiguration NetworkServices SNMP Host n Address: "Address"

where

Address: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""



xConfiguration NetworkServices SNMP CommunityName

Requires user role: ADMIN, INTEGRATOR

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 device. 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.

USAGE:

xConfiguration NetworkServices SNMP CommunityName: "CommunityName"

where

CommunityName: String (0, 50)

The SNMP community name.

Default value: ""

xConfiguration NetworkServices SNMP SystemContact

Requires user role: ADMIN, INTEGRATOR

Define the name of the Network Services SNMP System Contact.

USAGE:

xConfiguration NetworkServices SNMP SystemContact: "SystemContact"

where

SystemContact: String (0, 50)

The name of the SNMP system contact.

Default value: ""

xConfiguration NetworkServices SNMP SystemLocation

Requires user role: ADMIN, INTEGRATOR

Define the name of the Network Services SNMP System Location.

USAGE:

xConfiguration NetworkServices SNMP SystemLocation: "SystemLocation"

where

SystemLocation: String (0, 50)

The name of the SNMP system location.

Default value: ""

xConfiguration NetworkServices SSH Mode

Requires user role: ADMIN

The SSH (or Secure Shell) protocol can provide secure encrypted communication between the video conferencing device and your local computer.

USAGE:

xConfiguration NetworkServices SSH Mode: Mode

where

Mode: Off/On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

Default value: On



xConfiguration NetworkServices SSH HostKeyAlgorithm

Requires user role: ADMIN

Choose the cryptographic algorithm that shall be used for the SSH host key. Choices are RSA (Rivest-Shamir-Adleman) with 2048 bits keysizes, ECDSA (Elliptic Curve Digital Signature Algorithm) with NIST curve P-384, and EdDSA (Edwards-curve Digital Signature Algorithm) with ed25519 signature schema.

USAGE:

xConfiguration NetworkServices SSH HostKeyAlgorithm: [HostKeyAlgorithm](#)

where

[HostKeyAlgorithm](#): ECDSA/RSA/ed25519

ECDSA: Use the ECDSA algorithm (nist-384p).

RSA: Use the RSA algorithm (2048 bits).

ed25519: Use the ed25519 algorithm.

Default value: RSA

xConfiguration NetworkServices UPnP Mode

Requires user role: ADMIN

Fully disable UPnP (Universal Plug and Play), or enable UPnP for a short time period after the video conferencing device has been switched on or restarted.

The default operation is that UPnP is enabled when you switch on or restart the video conferencing device. Then UPnP is automatically disabled after the timeout period that is defined in the NetworkServices UPnP Timeout setting.

When UPnP is enabled, the device advertises its presence on the network. The advertisement permits a Touch controller to discover video conferencing devices automatically, and you do not need to manually enter the device's IP address in order to pair the Touch controller.

USAGE:

xConfiguration NetworkServices UPnP Mode: [Mode](#)

where

[Mode](#): Off/On

Off: UPnP is disabled. The video conferencing device does not advertise its presence, and you have to enter the device's IP address manually in order to pair a Touch controller to the device.

On: UPnP is enabled. The video conferencing device advertises its presence until the timeout period expires.

Default value: On



xConfiguration NetworkServices Websocket

Requires user role: ADMIN

It is possible to interact with the API of the device 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).

USAGE:

xConfiguration NetworkServices Websocket: [Websocket](#)

where

Websocket: 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.

Default value: Off

xConfiguration NetworkServices WelcomeText

Requires user role: ADMIN

Choose which information the user should see when logging on to the device through SSH.

USAGE:

xConfiguration NetworkServices WelcomeText: [WelcomeText](#)

where

WelcomeText: 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.

Default value: On

xConfiguration NetworkServices Wifi Allowed

Requires user role: ADMIN, USER

Devices 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 devices support the following standards: IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, and IEEE 802.11ac. The device 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 device, contains the letters NR (No Radio) the device does not support Wi-Fi.

USAGE:

xConfiguration NetworkServices Wifi Allowed: [Allowed](#)

where

Allowed: False/True

False: Wi-Fi cannot be used. You must connect to the network via Ethernet.

True: Both Ethernet and Wi-Fi are allowed.

Default value: True



Peripherals configuration

xConfiguration Peripherals Profile ControlSystems

Requires user role: ADMIN, INTEGRATOR

Define if a third-party control system, for example Crestron or AMX, is expected to be connected to the video conferencing device. This information is used by the video conferencing device's diagnostics service. If the number of connected control systems does not match this setting, the diagnostics service will report it as an inconsistency.

Such information is currently not available on this product.

USAGE:

xConfiguration Peripherals Profile ControlSystems: [ControlSystems](#)

where

[ControlSystems](#): NotSet

NotSet: No check for a third-party control system is performed.

Default value: NotSet

Phonebook configuration

xConfiguration Phonebook Server [n] ID

Requires user role: ADMIN

Define a name for the external phone book.

USAGE:

xConfiguration Phonebook Server [n](#) ID: "[ID](#)"

where

[ID](#): String (0, 64)

The name for the external phone book.

Default value: ""

xConfiguration Phonebook Server [n] Pagination

Requires user role: ADMIN

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 device 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.

USAGE:

xConfiguration Phonebook Server [n](#) Pagination: [Pagination](#)

where

[Pagination](#): Disabled/Enabled

Disabled: The phonebook server does not support pagination. The device does a single search, and the maximum number of entries in the search result is 100.

Enabled: The phonebook server supports pagination.

Default value: Enabled



xConfiguration Phonebook Server [n] TlsVerify

Requires user role: ADMIN

This setting applies when a video conferencing device connects to an external phone book server via HTTPS.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

USAGE:

xConfiguration Phonebook Server n TlsVerify: TlsVerify

where

TlsVerify: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.

Default value: On

xConfiguration Phonebook Server [n] Type

Requires user role: ADMIN

Select the phonebook server type.

USAGE:

xConfiguration Phonebook Server n Type: Type

where

Type: 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.

Default value: Off

xConfiguration Phonebook Server [n] URL

Requires user role: ADMIN

Define the address (URL) to the external phone book server.

USAGE:

xConfiguration Phonebook Server n URL: "URL"

where

URL: String (0..255)

A valid address (URL) to the phone book server.

Default value: ""



Provisioning configuration

xConfiguration Provisioning Connectivity

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Provisioning Connectivity: [Connectivity](#)

where

[Connectivity](#): 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.

Default value: Auto

xConfiguration Provisioning ExternalManager Address

Requires user role: ADMIN, USER

Define the IP Address or DNS name of the external manager / provisioning system.

If an External Manager Address (and Path) is configured, the device 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.

USAGE:

xConfiguration Provisioning ExternalManager Address: "[Address](#)"

where

[Address](#): String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""

xConfiguration Provisioning ExternalManager AlternateAddress

Requires user role: ADMIN, USER

Only applicable when the device 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 device will be provisioned by the alternate CUCM. When the main CUCM is available again, the device will be provisioned by this CUCM.

USAGE:

xConfiguration Provisioning ExternalManager AlternateAddress: "[AlternateAddress](#)"

where

[AlternateAddress](#): String (0, 64)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""



xConfiguration Provisioning ExternalManager Protocol

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Provisioning ExternalManager Protocol: Protocol

where

Protocol: HTTPS/HTTP

HTTPS: Send requests via HTTPS.

HTTP: Send requests via HTTP.

Default value: HTTP

xConfiguration Provisioning ExternalManager Path

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Provisioning ExternalManager Path: "Path"

where

Path: String (0..255)

A valid path to the external manager or provisioning system.

Default value: ""

xConfiguration Provisioning ExternalManager Domain

Requires user role: ADMIN, USER

Define the SIP domain for the VCS provisioning server.

USAGE:

xConfiguration Provisioning ExternalManager Domain: "Domain"

where

Domain: String (0, 64)

A valid domain name.

Default value: ""

xConfiguration Provisioning Mode

Requires user role: ADMIN, USER

It is possible to configure a device using a provisioning system (external manager). This allows video conferencing network administrators to manage many devices 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.

USAGE:

xConfiguration Provisioning Mode: Mode

where

Mode: Off/Auto/CUCM/Edge/Webex/TMS/VCS

Off: The device 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 device from CUCM (Cisco Unified Communications Manager).

Edge: Push configurations to the device from CUCM (Cisco Unified Communications Manager). The device connects to CUCM via the Expressway infrastructure. In order to register over Expressway the encryption option key must be installed on the device.

Webex: Push configurations to the device from the Cisco Webex cloud service.

TMS: Push configurations to the device from TMS (Cisco TelePresence Management System).

VCS: Push configurations to the device from VCS (Cisco TelePresence Video Communication Server).

Default value: Auto



xConfiguration Provisioning LoginName

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Provisioning LoginName: "LoginName"

where

LoginName: String (0, 80)

A valid username.

Default value: ""

xConfiguration Provisioning Password

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Provisioning Password: "Password"

where

Password: String (0, 64)

A valid password.

Default value: ""

xConfiguration Provisioning TlsVerify

Requires user role: ADMIN, USER

This setting applies when a video conferencing device connects to a provisioning server via HTTPS.

Before establishing a connection between the device and the HTTPS server, the device checks if the certificate of the server is signed by a trusted Certificate Authority (CA). The CA certificate must be included in the CA list on the device, either pre-installed or manually uploaded using the web interface or API.

In general, the minimum TLS (Transport Layer Security) version for the HTTPS connection is 1.1. There are two exceptions to this rule: 1) For compatibility reasons, the minimum TLS version is 1.0 for devices that are registered to CUCM. 2) Devices registered to the Webex cloud service always use version 1.2.

Note: The value is set to Off for a device that has been upgraded to CE9.9 (or later) from CE9.8 or earlier software versions, provided that the device has not been factory reset after the upgrade, and that the old NetworkServices HTTPS VerifyServerCertificate setting was not explicitly set to On.

The certificate check is always performed, regardless of this setting, if the device is provisioned from the Cisco Webex cloud service or from CUCM via Expressway (also known as MRA or Edge).

USAGE:

xConfiguration Provisioning TlsVerify: TlsVerify

where

TlsVerify: Off/On

Off: The device doesn't check the certificate of the HTTPS server.

On: The device checks if the certificate of the HTTPS server can be trusted. If not, the connection between the device and the server is not established.

Default value: On



Proximity configuration

xConfiguration Proximity Mode

Requires user role: ADMIN, USER

Determine whether the device will emit ultrasound pairing messages or not.

When the device emits ultrasound, Proximity clients can detect that they are close to the device. 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.

USAGE:

xConfiguration Proximity Mode: Mode

where

Mode: Off/On

Off: The device does not emit ultrasound, and Proximity services cannot be used.

On: The device emits ultrasound, and Proximity clients can detect that they are close to the device. Enabled Proximity services can be used.

Default value: On

xConfiguration Proximity Services CallControl

Requires user role: ADMIN, USER

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.

USAGE:

xConfiguration Proximity Services CallControl: CallControl

where

CallControl: Enabled/Disabled

Enabled: Call control from a Proximity client is enabled.

Disabled: Call control from a Proximity client is disabled.

Default value: Disabled

xConfiguration Proximity Services ContentShare FromClients

Requires user role: ADMIN, USER

Enable or disable content sharing from Proximity clients. When this setting is enabled, you can share content from a Proximity client wirelessly on the device, 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.

USAGE:

xConfiguration Proximity Services ContentShare FromClients: FromClients

where

FromClients: Enabled/Disabled

Enabled: Content sharing from a Proximity client is enabled.

Disabled: Content sharing from a Proximity client is disabled.

Default value: Enabled

xConfiguration Proximity Services ContentShare ToClients

Requires user role: ADMIN, USER

Enable or disable content sharing to Proximity clients. When enabled, Proximity clients will receive the presentation from the device. 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.

USAGE:

xConfiguration Proximity Services ContentShare ToClients: ToClients

where

ToClients: Enabled/Disabled

Enabled: Content sharing to a Proximity client is enabled.

Disabled: Content sharing to a Proximity client is disabled.

Default value: Disabled



RoomAnalytics configuration

xConfiguration RoomAnalytics AmbientNoiseEstimation Mode

Requires user role: ADMIN, INTEGRATOR, USER

The device can estimate the stationary ambient noise level (background noise level) in the room. The result is reported in the RoomAnalytics AmbientNoise Level dBA status. The status is updated when a new ambient noise level is detected.

USAGE:

xConfiguration RoomAnalytics AmbientNoiseEstimation Mode: Mode

where

Mode: Off/On

On: The device regularly estimates the stationary ambient noise level.

Off: The device doesn't estimate the stationary ambient noise level.

Default value: Off

xConfiguration RoomAnalytics PeopleCountOutOfCall

Requires user role: ADMIN, INTEGRATOR, USER

By using face detection, the device has the capability to find how many persons are in the room. By default, the device only counts people when in a call, or when displaying the self-view picture.

USAGE:

xConfiguration RoomAnalytics PeopleCountOutOfCall: PeopleCountOutOfCall

where

PeopleCountOutOfCall: Off/On

Off: The device counts people only when the device is in a call, or when self-view is on.

On: The device counts people as long as the device is not in standby mode. This includes outside of call, even if self-view is off.

Default value: Off

xConfiguration RoomAnalytics PeoplePresenceDetector

Requires user role: ADMIN, INTEGRATOR, USER

The device has the capability to find whether or not people are present in the room, and report the result in the RoomAnalytics PeoplePresence status. The feature is based on ultrasound. Read the status description for more details.

USAGE:

xConfiguration RoomAnalytics PeoplePresenceDetector: PeoplePresenceDetector
where

PeoplePresenceDetector: Off/On

Off: Information about the presence of people is not reported in the device's status.

On: Information about the presence of people is reported in the device's status.

Default value: Off



Security configuration

xConfiguration Security Audit Logging Mode

Requires user role: AUDIT

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.

USAGE:

xConfiguration Security Audit Logging Mode: Mode

where

Mode: External/ExternalSecure/Internal/Off

External: The device sends the audit logs to an external syslog server. The syslog server must support UDP.

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

Off: No audit logging is performed.

Default value: Internal

xConfiguration Security Audit OnError Action

Requires user role: AUDIT

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.

USAGE:

xConfiguration Security Audit OnError Action: Action

where

Action: Halt/Ignore

Halt: If a halt condition is detected the device 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-spoiled 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 device 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.

Default value: Ignore

xConfiguration Security Audit Server Address

Requires user role: AUDIT

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.

USAGE:

xConfiguration Security Audit Server Address: "Address"

where

Address: String (0..255)

A valid IPv4 address, IPv6 address, or DNS name.

Default value: ""



xConfiguration Security Audit Server Port

Requires user role: AUDIT

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

USAGE:

xConfiguration Security Audit Server Port: Port

where

Port: Integer (0..65535)

Set the audit server port.

Default value: 514

xConfiguration Security Audit Server PortAssignment

Requires user role: AUDIT

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.

USAGE:

xConfiguration Security Audit Server PortAssignment: PortAssignment

where

PortAssignment: 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.

Default value: Auto

xConfiguration Security Session FailedLoginsLockoutTime

Requires user role: ADMIN

Define how long the device will lock out a user after failed login to a web or SSH session. Restart the device for any change to this setting to take effect.

USAGE:

xConfiguration Security Session FailedLoginsLockoutTime: FailedLoginsLockoutTime

where

FailedLoginsLockoutTime: Integer (0..10000)

Set the lockout time (minutes).

Default value: 60

xConfiguration Security Session InactivityTimeout

Requires user role: ADMIN

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

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

USAGE:

xConfiguration Security Session InactivityTimeout: InactivityTimeout

where

InactivityTimeout: Integer (0..10000)

Set the inactivity timeout (minutes); or select 0 when inactivity should not enforce automatic logout.

Default value: 0



xConfiguration Security Session MaxFailedLogins

Requires user role: ADMIN

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 device for any change to this setting to take effect.

USAGE:

xConfiguration Security Session MaxFailedLogins: MaxFailedLogins

where

MaxFailedLogins: Integer (0..10)

Set the maximum number of failed login attempts per user.

Default value: 0

xConfiguration Security Session MaxSessionsPerUser

Requires user role: ADMIN

The maximum number of simultaneous sessions per user is 20 sessions.

USAGE:

xConfiguration Security Session MaxSessionsPerUser: MaxSessionsPerUser

where

MaxSessionsPerUser: Integer (1..20)

Set the maximum number of simultaneous sessions per user.

Default value: 20

xConfiguration Security Session MaxTotalSessions

Requires user role: ADMIN

The maximum number of simultaneous sessions in total is 20 sessions.

USAGE:

xConfiguration Security Session MaxTotalSessions: MaxTotalSessions

where

MaxTotalSessions: Integer (1..20)

Set the maximum number of simultaneous sessions in total.

Default value: 20

xConfiguration Security Session ShowLastLogon

Requires user role: ADMIN

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

USAGE:

xConfiguration Security Session ShowLastLogon: ShowLastLogon

where

ShowLastLogon: Off/On

On: Show information about the last session.

Off: Do not show information about the last session.

Default value: Off



SerialPort configuration

xConfiguration SerialPort Mode

Requires user role: ADMIN, INTEGRATOR

Enable/disable the serial port.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

USAGE:

xConfiguration SerialPort Mode: Mode

where

Mode: Off/On

Off: Disable the serial port.

On: Enable the serial port.

Default value: On

xConfiguration SerialPort BaudRate

Requires user role: ADMIN, INTEGRATOR

Set the baud rate (data transmission rate, bits per second) for the serial port.

Other connection parameters for the serial port are: Data bits: 8; Parity: None; Stop bits: 1; Flow control: None.

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

USAGE:

xConfiguration SerialPort BaudRate: BaudRate

where

BaudRate: 115200

Choose a baud rate from the baud rates listed (bps).

Default value: 115200

xConfiguration SerialPort LoginRequired

Requires user role: ADMIN

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

This setting is not available for the first generation of boards (Webex Board 55 and Webex Board 70).

USAGE:

xConfiguration SerialPort LoginRequired: LoginRequired

where

LoginRequired: Off/On

Off: The user can access the device via the serial port without any login.

On: Login is required when connecting to the device via the serial port.

Default value: On



SIP configuration

xConfiguration SIP ANAT

Requires user role: ADMIN

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

USAGE:

xConfiguration SIP ANAT: ANAT

where

ANAT: Off/On

Off: Disable ANAT.

On: Enable ANAT.

Default value: Off

xConfiguration SIP Authentication UserName

Requires user role: ADMIN

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

USAGE:

xConfiguration SIP Authentication UserName: "UserName"

where

UserName: String (0, 128)

A valid username.

Default value: ""

xConfiguration SIP Authentication Password

Requires user role: ADMIN

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

USAGE:

xConfiguration SIP Authentication Password: "Password"

where

Password: String (0, 128)

A valid password.

Default value: ""

xConfiguration SIP DefaultTransport

Requires user role: ADMIN

Select the transport protocol to be used over the LAN.

USAGE:

xConfiguration SIP DefaultTransport: DefaultTransport

where

DefaultTransport: Auto/TCP/Tls/UDP

TCP: The device will always use TCP as the default transport method.

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

Tls: The device will always use TLS as the default transport method. For TLS connections a SIP CA-list can be uploaded to the device. If no such CA-list is available on the device then anonymous Diffie Hellman will be used.

Auto: The device will try to connect using transport protocols in the following order: TLS, TCP, UDP.

Default value: Auto



xConfiguration SIP DisplayName

Requires user role: ADMIN

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

USAGE:

`xConfiguration SIP DisplayName: "DisplayName"`

where

DisplayName: String (0, 550)

The name to be displayed instead of the SIP URI.

Default value: ""

xConfiguration SIP Ice DefaultCandidate

Requires user role: ADMIN

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 device will be sent to the Default Candidate as defined in this setting.

USAGE:

`xConfiguration SIP Ice DefaultCandidate: DefaultCandidate`

where

DefaultCandidate: Host/Rflx/Relay

Host: Send media to the device's private IP address.

Rflx: Send media to the device's public IP address, as seen by the TURN server.

Relay: Send media to the IP address and port allocated on the TURN server.

Default value: Host

xConfiguration SIP Ice Mode

Requires user role: ADMIN

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

USAGE:

`xConfiguration SIP Ice Mode: Mode`

where

Mode: 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.

Default value: Auto

xConfiguration SIP ListenPort

Requires user role: ADMIN

Turn on or off the listening for incoming connections on the SIP TCP/UDP ports. If turned off, the device will only be reachable through a SIP Proxy (CUCM or VCS). As a security measure, SIP ListenPort should be Off when the device is registered to a SIP Proxy.

USAGE:

`xConfiguration SIP ListenPort: ListenPort`

where

ListenPort: Auto/Off/On

Auto: Listening for incoming connections on the SIP TCP/UDP ports is automatically turned off if the device is registered to a SIP Proxy; otherwise it is turned 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.

Default value: Auto



xConfiguration SIP MinimumTLSVersion

Requires user role: ADMIN

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

USAGE:

xConfiguration SIP MinimumTLSVersion: MinimumTLSVersion

where

MinimumTLSVersion: 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.

Default value: TLSv1.0

xConfiguration SIP Proxy [n] Address

Requires user role: ADMIN

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.

USAGE:

xConfiguration SIP Proxy n Address: "Address"

where

Address: String (0..255)

A valid IPv4 address, IPv6 address or DNS name.

Default value: ""

xConfiguration SIP Turn Server

Requires user role: ADMIN

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 device's own public IP address.

USAGE:

xConfiguration SIP Turn Server: "Server"

where

Server: 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.

Default value: ""

xConfiguration SIP Turn UserName

Requires user role: ADMIN

Define the username needed for accessing the TURN server.

USAGE:

xConfiguration SIP Turn UserName: "UserName"

where

UserName: String (0, 128)

A valid username.

Default value: ""



xConfiguration SIP Turn Password

Requires user role: ADMIN

Define the password needed for accessing the TURN server.

USAGE:

xConfiguration SIP Turn Password: "Password"

where

Password: String (0, 128)

A valid password.

Default value: ""

xConfiguration SIP URI

Requires user role: ADMIN

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

USAGE:

xConfiguration SIP URI: "URI"

where

URI: String (0..255)

An address (URI) that is compliant with the SIP URI syntax.

Default value: ""

Standby configuration

xConfiguration Standby Control

Requires user role: ADMIN, INTEGRATOR

Define whether the device should go into standby mode or not.

USAGE:

xConfiguration Standby Control: Control

where

Control: Off/On

Off: The device will not enter standby mode.

On: The device will enter standby mode when the Standby Delay has timed out. Requires the Standby Delay to be set to an appropriate value.

Default value: On

xConfiguration Standby Delay

Requires user role: ADMIN, INTEGRATOR

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

USAGE:

xConfiguration Standby Delay: Delay

where

Delay: Integer (1..480)

Set the standby delay (minutes).

Default value: 4



xConfiguration Standby Signage Audio

Requires user role: ADMIN, INTEGRATOR

By default, a device does not play out audio in digital signage mode even if the web page has audio. You can use this setting to override the default behavior.

USAGE:

xConfiguration Standby Signage Audio: [Audio](#)

where

Audio: Off/On

Off: The device does not play out audio with the web page.

On: If the web page has audio, the device plays it out. The volume follows the volume setting of the device.

Default value: Off

xConfiguration Standby Signage InteractionMode

Requires user role: ADMIN, INTEGRATOR

By default, a user cannot interact with a digital signage web page. You can use this setting to enable the ability to interact with the web page.

USAGE:

xConfiguration Standby Signage InteractionMode: [InteractionMode](#)

where

InteractionMode: Interactive/NonInteractive

Interactive: It's possible to interact with the web page.

NonInteractive: It's not possible to interact with the web page.

Default value: NonInteractive

xConfiguration Standby Signage Mode

Requires user role: ADMIN

Content from a URL (a web page) can replace the traditional half-wake background image and information. This feature is called digital signage. Users can interact with the web page, for example click on a link or enter text in a form.

The use of digital signage does not prevent the device from entering standby the normal way. Therefore, the Standby Delay setting determines for how long the digital signage is shown before the device goes into standby.

USAGE:

xConfiguration Standby Signage Mode: [Mode](#)

where

Mode: Off/On

Off: Digital signage is not enabled on the device.

On: Digital signage is enabled and replaces the device's half-wake mode, provided that also the WebEngine Mode setting is On.

Default value: Off

xConfiguration Standby Signage RefreshInterval

Requires user role: ADMIN, INTEGRATOR

You can use this setting to force a web page to refresh at regular intervals. This is useful for web pages that are not able to refresh themselves. It is not recommended to set a refresh interval with the interactive mode.

USAGE:

xConfiguration Standby Signage RefreshInterval: [RefreshInterval](#)

where

RefreshInterval: Integer (0..1440)

The number of seconds between each web page refresh. The value of 0 means that the web page is never forced to refresh.

Default value: 0



xConfiguration Standby Signage Url

Requires user role: ADMIN, INTEGRATOR

Set the URL of the web page you want to display on the screen (digital signage). If the length of the URL is 0, the device retains normal half-wake mode. If the URL fails, the device retains normal half-wake mode and a diagnostics message is issued.

USAGE:

xConfiguration Standby Signage Url: "Url"

where

Url: String (0, 2000)

The URL of the web page.

Default value: ""

xConfiguration Standby WakeupOnMotionDetection

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Standby WakeupOnMotionDetection: WakeupOnMotionDetection

where

WakeupOnMotionDetection: Off/On

Off: The wake up on motion detection is disabled.

On: When people walk into the room the device will automatically wake up from standby.

Default value: On

SystemUnit configuration

xConfiguration SystemUnit Name

Requires user role: ADMIN

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

USAGE:

xConfiguration SystemUnit Name: "Name"

where

Name: String (0, 50)

Define the device name.

Default value: ""

xConfiguration SystemUnit CrashReporting Mode

Requires user role: ADMIN

If the device crashes, the device 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.

USAGE:

xConfiguration SystemUnit CrashReporting Mode: Mode

where

Mode: Off/On

Off: No logs will be sent to ACR tool.

On: The logs will automatically be sent to ACR tool.

Default value: On



xConfiguration SystemUnit CrashReporting Url

Requires user role: ADMIN

If the device crashes, the device 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.

USAGE:

xConfiguration SystemUnit CrashReporting Url: "Url"

where

Url: String (0..255)

The URL to the Cisco Automatic Crash Report tool (ACR).

Default value: "acr.cisco.com"

Time configuration

xConfiguration Time TimeFormat

Requires user role: ADMIN, USER

Define the time format.

USAGE:

xConfiguration Time TimeFormat: TimeFormat

where

TimeFormat: 24H/12H

24H: Set the time format to 24 hours.

12H: Set the time format to 12 hours (AM/PM).

Default value: 24H

xConfiguration Time DateFormat

Requires user role: ADMIN, USER

Define the date format.

USAGE:

xConfiguration Time DateFormat: DateFormat

where

DateFormat: 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

Default value: DD_MM_YY



xConfiguration Time Zone

Requires user role: ADMIN, INTEGRATOR, USER

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

USAGE:

xConfiguration Time Zone: Zone

where

Zone: 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/Yukutat, 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/Aqttau, Asia/Aqtobe, Asia/Ashgabad, 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/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/GMTO, 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/Apiap, 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.

Default value: Etc/UTC

UserInterface configuration

xConfiguration UserInterface Accessibility IncomingCallNotification

Requires user role: ADMIN, INTEGRATOR, USER

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 device 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.

USAGE:

xConfiguration UserInterface Accessibility IncomingCallNotification:
[IncomingCallNotification](#)

where

[IncomingCallNotification](#): AmplifiedVisuals/Default

AmplifiedVisuals: Enable the amplified visuals on screen and touch panel when the device receives a call.

Default: Enable the default behavior with a notification on screen and touch panel.

Default value: Default

xConfiguration UserInterface Branding AwakeBranding Colors

Requires user role: ADMIN, INTEGRATOR

If the device is set up with branding customizations, this setting affects the colors of the logo that is shown when the device 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.

USAGE:

xConfiguration UserInterface Branding AwakeBranding Colors: [Colors](#)

where

[Colors](#): Auto/Native

Auto: The opacity of the logo is reduced.

Native: The logo has full colors.

Default value: Auto



xConfiguration UserInterface ContactInfo Type

Requires user role: ADMIN

Choose which type of contact information to show in the user interface.

USAGE:

xConfiguration UserInterface ContactInfo Type: Type

where

Type: Auto/DisplayName/E164Alias/H320Number/H323Id/IPv4/IPv6/None/SipUri/
SystemName

Auto: Show the address which another device should dial to reach this video conferencing device. The address depends on the default call protocol and device registration.

None: Do not show any contact information.

IPv4: Show the device's IPv4 address.

IPv6: Show the device's IPv6 address.

H323Id: Show the device's H.323 ID (refer to the H323 H323Alias ID setting).

H320Number: Show the device's H.320 number as contact information (only supported if used with Cisco TelePresence ISDN Link).

E164Alias: Show the device's H.323 E164 Alias as contact information (refer to the H323 H323Alias E164 setting).

SipUri: Show the device's SIP URI (refer to the SIP URI setting).

SystemName: Show the device's name (refer to the SystemUnit Name setting).

DisplayName: Show the device's display name (refer to the SIP DisplayName setting).

Default value: Auto

xConfiguration UserInterface KeyTones Mode

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration UserInterface KeyTones Mode: Mode

where

Mode: Off/On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

Default value: Off

xConfiguration UserInterface Features Call End

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration UserInterface Features Call End: End

where

End: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

Default value: Auto



xConfiguration UserInterface Features Call MidCallControls

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration UserInterface Features Call MidCallControls: [MidCallControls](#)

where

[MidCallControls](#): Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

Default value: Auto

xConfiguration UserInterface Features Call Start

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration UserInterface Features Call Start: [Start](#)

where

[Start](#): Auto/Hidden

Auto: Shows the default buttons in the user interface.

Hidden: Removes the default buttons from the user interface.

Default value: Auto

xConfiguration UserInterface Features Call VideoMute

Requires user role: ADMIN, INTEGRATOR

Choose whether or not to show the default "Turn video off" button in the user interface.

USAGE:

xConfiguration UserInterface Features Call VideoMute: [VideoMute](#)

where

[VideoMute](#): Auto/Hidden

Auto: Shows the "Turn video off" button in the user interface if this feature is supported in the ongoing call.

Hidden: The "Turn video off" button is never shown in the user interface.

Default value: Auto

xConfiguration UserInterface Features HideAll

Requires user role: ADMIN, INTEGRATOR

Choose whether or not to remove all default buttons from the user interface. The setting removes only the buttons, not their functionality as such.

USAGE:

xConfiguration UserInterface Features HideAll: [HideAll](#)

where

[HideAll](#): False/True

False: Shows all default buttons in the user interface.

True: Removes all default buttons from the user interface.

Default value: False



xConfiguration UserInterface Features Share Start

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration UserInterface Features Share Start: Start

where

Start: 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.

Default value: Auto

xConfiguration UserInterface Features Whiteboard Start

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration UserInterface Features Whiteboard Start: Start

where

Start: Auto/Hidden

Auto: Shows the default button in the user interface.

Hidden: Removes the default button from the user interface.

Default value: Auto

xConfiguration UserInterface Language

Requires user role: ADMIN, USER

Select the language to be used in the user interface. If the language is not supported, the default language (English) will be used.

USAGE:

xConfiguration UserInterface Language: Language

where

Language: 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.

Default value: English

xConfiguration UserInterface OSD EncryptionIndicator

Requires user role: ADMIN

Define for how long the encryption indicator is shown on screen. The icon for encrypted calls is a locked padlock.

USAGE:

xConfiguration UserInterface OSD EncryptionIndicator: EncryptionIndicator

where

EncryptionIndicator: 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.

Default value: Auto



xConfiguration UserInterface OSD Output

Requires user role: ADMIN, INTEGRATOR

Define on which monitor the on-screen information and indicators (OSD) should be displayed.

USAGE:

xConfiguration UserInterface OSD Output: [Output](#)

where

[Output](#): 1

1: The device sends the on-screen information and indicators to the device's integrated screen.

Default value: 1

xConfiguration UserInterface Phonebook Mode

Requires user role: ADMIN, INTEGRATOR

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 device.

USAGE:

xConfiguration UserInterface Phonebook Mode: [Mode](#)

where

[Mode](#): 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.

Default value: ReadWrite

xConfiguration UserInterface Security Mode

Requires user role: ADMIN

This setting allows you to prevent important device 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 conferencing device, 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.

USAGE:

xConfiguration UserInterface Security Mode: [Mode](#)

where

[Mode](#): Normal/Strong

Normal: IP addresses and other device 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).

Default value: Normal



xConfiguration UserInterface SettingsMenu Mode

Requires user role: ADMIN

The Settings panel in the user interface (Touch 10 or on-screen) can be protected by the device's admin password. If this password is blank, anyone can access the settings in the Settings panel, and for example factory reset the device. If authentication is enabled, all settings that require authentication have a padlock icon. You will be prompted to enter the administrator's username and passphrase when you select the setting. Some settings do not require authentication, they do not have a padlock icon.

USAGE:

xConfiguration UserInterface SettingsMenu Mode: Mode

where

Mode: Locked/Unlocked

Locked: Authentication with administrator's username and passphrase is required.

Unlocked: No authentication is required.

Default value: Unlocked

xConfiguration UserInterface SettingsMenu Visibility

Requires user role: ADMIN

Choose whether or not to show the device name (or contact information) and the associated drop down menu and Settings panel on the user interface.

USAGE:

xConfiguration UserInterface SettingsMenu Visibility: Visibility

where

Visibility: Auto/Hidden

Auto: Shows the device name with drop down menu and Settings panel on the user interface.

Hidden: Doesn't show the device name with drop down menu and Settings panel on the user interface.

Default value: Auto

xConfiguration UserInterface SoundEffects Mode

Requires user role: ADMIN, USER

You can configure the device to make a sound effect, e.g. when someone connects a laptop or mobile through Proximity.

The keyboard click sound effect when typing text is not affected by this setting (refer to the UserInterface Keytones Mode setting).

USAGE:

xConfiguration UserInterface SoundEffects Mode: Mode

where

Mode: Off/On

Off: There are no sound effects.

On: The sound effects are switched on.

Default value: On



UserManagement configuration

xConfiguration UserManagement LDAP Admin Filter

Requires user role: ADMIN

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.

USAGE:

xConfiguration UserManagement LDAP Admin Filter: "Filter"

where

Filter: 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))"

Default value: ""

xConfiguration UserManagement LDAP Admin Group

Requires user role: ADMIN

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.

USAGE:

xConfiguration UserManagement LDAP Admin Group: "Group"

where

Group: String (0..255)

The distinguished name of the AD group. Example: "CN=admin group, OU=company groups, DC=company, DC=com"

Default value: ""

xConfiguration UserManagement LDAP Attribute

Requires user role: ADMIN

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

USAGE:

xConfiguration UserManagement LDAP Attribute: "Attribute"

where

Attribute: String (0..255)

The attribute name.

Default value: ""

xConfiguration UserManagement LDAP BaseDN

Requires user role: ADMIN

The distinguishing name of the entry at which to start a search (base).

USAGE:

xConfiguration UserManagement LDAP BaseDN: "BaseDN"

where

BaseDN: String (0..255)

The distinguishing name of the base. Example: "DC=company, DC=com"

Default value: ""



xConfiguration UserManagement LDAP Encryption

Requires user role: ADMIN

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

USAGE:

xConfiguration UserManagement LDAP Encryption: Encryption

where

Encryption: LDAPS/None/STARTTLS

LDAPS: Connect to the LDAP server on port 636 over TLS (Transport Layer Security).

None: Connect to the LDAP server on port 389 with no encryption.

STARTTLS: Connect to the LDAP server on port 389, then send a STARTTLS command to upgrade to an encrypted connection (TLS).

Default value: LDAPS

xConfiguration UserManagement LDAP MinimumTLSVersion

Requires user role: ADMIN

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

USAGE:

xConfiguration UserManagement LDAP MinimumTLSVersion: MinimumTLSVersion

where

MinimumTLSVersion: 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.

Default value: TLSv1.2

xConfiguration UserManagement LDAP Mode

Requires user role: ADMIN

The device supports the use of an LDAP (Lightweight Directory Access Protocol) server as a central place to store and validate usernames 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))"

USAGE:

xConfiguration UserManagement LDAP Mode: Mode

where

Mode: Off/On

Off: LDAP authentication is not allowed.

On: LDAP authentication is allowed.

Default value: Off



xConfiguration UserManagement LDAP Server Address

Requires user role: ADMIN

Set the IP address or hostname of the LDAP server.

USAGE:

xConfiguration UserManagement LDAP Server Address: "Address"

where

Address: String (0..255)

A valid IPv4 address, IPv6 address or hostname.

Default value: ""

xConfiguration UserManagement LDAP Server Port

Requires user role: ADMIN

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).

USAGE:

xConfiguration UserManagement LDAP Server Port: Port

where

Port: Integer (0..65535)

The LDAP server port number.

Default value: 0

xConfiguration UserManagement LDAP VerifyServerCertificate

Requires user role: ADMIN

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

USAGE:

xConfiguration UserManagement LDAP VerifyServerCertificate:

VerifyServerCertificate

where

VerifyServerCertificate: Off/On

Off: The device will not verify the LDAP server's certificate.

On: The device 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 device in advance. Use the device's web interface to manage the list of trusted CAs (see more details in the administrator guide).

Default value: On



Video configuration

xConfiguration Video DefaultMainSource

Requires user role: ADMIN, USER

Define which video input source to be used as the default main video source when you start a call.

USAGE:

xConfiguration Video DefaultMainSource: DefaultMainSource

where

DefaultMainSource: 1

The source that is used as the default main video source.

Default value: 1

xConfiguration Video Input Connector [n] CameraControl Camerald

Requires user role: ADMIN, INTEGRATOR

The camera ID is a unique identifier of the camera that is connected to this video input.

USAGE:

xConfiguration Video Input Connector n CameraControl CameraId: CameraId

where

CameraId: Connector n: 1

The camera ID is fixed and cannot be changed.

Default value: Connector n: 1

xConfiguration Video Input Connector [n] CameraControl Mode

Requires user role: ADMIN, INTEGRATOR

Define whether the camera that is connected to this video input connector can be controlled or not.

Note that camera control is not available for Connector 2 (HDMI).

USAGE:

xConfiguration Video Input Connector n CameraControl Mode: Mode

where

Mode: Connector 1: Off/On Connector 2: Off

Off: Disable camera control.

On: Enable camera control.

Default value: Connector 1: On Connector 2: Off

xConfiguration Video Input Connector [n] CEC Mode

Requires user role: ADMIN, INTEGRATOR

The video input (HDMI) supports Consumer Electronics Control (CEC). When this setting is enabled, information about the connected device (for example device type and device name) is available in the video conferencing device status (Video Input Connector[n] ConnectedDevice CEC [n]), provided that the connected device also supports CEC.

USAGE:

xConfiguration Video Input Connector n CEC Mode: Mode

where

Mode: Connector n: Off/On

Off: CEC is disabled.

On: CEC is enabled.

Default value: On



xConfiguration Video Input Connector [n] InputSourceType

Requires user role: ADMIN, INTEGRATOR

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

Note that Connector 1 is the device's integrated camera.

USAGE:

xConfiguration Video Input Connector n InputSourceType: InputSourceType

where

InputSourceType: 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.

Default value: Connector 1: camera Connector 2: PC

xConfiguration Video Input Connector [n] Name

Requires user role: ADMIN, INTEGRATOR

Define a name for the video input connector.

USAGE:

xConfiguration Video Input Connector n Name: "Name"

where

Name: String (0, 50)

Name for the video input connector.

Default value: Connector 1: "Camera" Connector 2: "PC"

xConfiguration Video Input Connector [n] PreferredResolution

Requires user role: ADMIN, INTEGRATOR

Define the preferred screen resolution and refresh rate that the video conferencing device advertises to the input sources that are connected via HDMI (for example a laptop). The logic for selection of the resolution on the source side will choose this resolution and refresh rate automatically, unless it is overridden manually by the source device (for example the laptop's display configuration software).

Note that the formats 2560_1440_60 and 3840_2160_30 use about twice the amount of data compared to the 1920_1080_60 format, and requires a presentation cable (or adapter) that is qualified for at least HDMI 1.4b data rates.

USAGE:

xConfiguration Video Input Connector n PreferredResolution: PreferredResolution

where

PreferredResolution: Connector n: 1920_1080_60/2560_1440_60/3840_2160_30

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

2560_1440_60: The resolution is 2560 x 1440, and the refresh rate is 60 Hz.

3840_2160_30: The resolution is 3840 x 2160, and the refresh rate is 30 Hz.

Default value: Connector n: 1920_1080_60



xConfiguration Video Input Connector [n] PresentationSelection

Requires user role: ADMIN, INTEGRATOR

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

If the device 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.

USAGE:

xConfiguration Video Input Connector n PresentationSelection:

PresentationSelection

where

PresentationSelection: 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.

Default value: Connector n: AutoShare

xConfiguration Video Input Connector [n] Quality

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Video Input Connector n Quality: Quality

where

Quality: 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.

Default value: Connector n: Sharpness

xConfiguration Video Input Connector [n] Visibility

Requires user role: ADMIN, INTEGRATOR

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

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

USAGE:

xConfiguration Video Input Connector n Visibility: Visibility

where

Visibility: 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: The 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.

Default value: Connector 1: Never Connector 2: IfSignal



xConfiguration Video Output Connector [n] Resolution

Requires user role: ADMIN, INTEGRATOR, USER

The resolution and refresh rate for the integrated screen. This value is fixed and cannot be changed.

USAGE:

xConfiguration Video Output Connector n Resolution: Resolution

where

Resolution: 3840_2160_60

3840_2160_60: The resolution is 3840 x 2160, and the refresh rate is 60 Hz.

Default value: 3840_2160_60

xConfiguration Video Presentation DefaultSource

Requires user role: ADMIN, USER

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

USAGE:

xConfiguration Video Presentation DefaultSource: DefaultSource

where

DefaultSource: 1/2

The video input source to use as default presentation source.

Default value: 2

xConfiguration Video Presentation Priority

Requires user role: ADMIN

Determine how to distribute the bandwidth between the presentation channel and the main video channel.

USAGE:

xConfiguration Video Presentation Priority: Priority

where

Priority: 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.

Default value: Equal

xConfiguration Video Selfview Default FullscreenMode

Requires user role: ADMIN, INTEGRATOR

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).

USAGE:

xConfiguration Video Selfview Default FullscreenMode: FullscreenMode

where

FullscreenMode: 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.

Default value: Current

xConfiguration Video Selfview Default Mode

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Video Selfview Default Mode: [Mode](#)

where

Mode: 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.

Default value: Current

xConfiguration Video Selfview Default OnMonitorRole

Requires user role: ADMIN, INTEGRATOR

Define which screen/output to display the main video source (self-view) after a call. The value reflects the monitor roles set for the different outputs in the Video Output Connector [n] MonitorRole setting.

The setting applies both when self-view is displayed in full screen, and when it is displayed as picture-in-picture (PiP).

USAGE:

xConfiguration Video Selfview Default OnMonitorRole: [OnMonitorRole](#)

where

OnMonitorRole: Current/First/Second

Current: When leaving a call, the self-view picture will be retained on the same output as it was during the call.

First: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to First.

Second: The self-view picture will be shown on outputs with the Video Output Connector [n] MonitorRole set to Second.

Default value: Current

xConfiguration Video Selfview Default PIPPosition

Requires user role: ADMIN, INTEGRATOR

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).

USAGE:

xConfiguration Video Selfview Default PIPPosition: [PIPPosition](#)

where

PIPPosition: 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.

Default value: LowerRight

xConfiguration Video Selfview OnCall Mode

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Video Selfview OnCall Mode: [Mode](#)

where

Mode: Off/On

Off: Self-view is not shown automatically during call setup.

On: Self-view is shown automatically during call setup.

Default value: Off



xConfiguration Video Selfview OnCall Duration

Requires user role: ADMIN, INTEGRATOR

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.

USAGE:

xConfiguration Video Selfview OnCall Duration: Duration

where

Duration: Integer (1..60)

Range: Choose for how long self-view remains on. The valid range is between 1 and 60 seconds.

Default value: 10

WebEngine configuration

xConfiguration WebEngine Mode

Requires user role: ADMIN

The web engine is a prerequisite for features that use the device's web view, for example digital signage and web apps.

USAGE:

xConfiguration WebEngine Mode: Mode

where

Mode: Off/On

Off: The web engine is disabled.

On: The web engine is enabled.

Default value: Off

xConfiguration WebEngine RemoteDebugging

Requires user role: ADMIN

If you encounter a problem with a web page, it can be a good idea to turn on remote debugging. Remote debugging lets you access the Chrome developer console and identify potential issues with a web page. When enabled, a banner is displayed at the bottom of the screen, warning the users that they may be monitored. The banner also shows the URL that you can enter in your local Chrome browser to open the developer console.

Make sure to turn off remote debugging after use.

USAGE:

xConfiguration WebEngine RemoteDebugging: RemoteDebugging

where

RemoteDebugging: Off/On

Off: Remote debugging is switched off.

On: Remote debugging is switched on.

Default value: Off



Chapter 4

xCommand commands



Description of the xCommand commands

In this chapter, you can find a complete list of all xCommand type commands with parameters.

We recommend you visit our web site regularly for updated versions of the manual.

Go to: ▶ <https://www.cisco.com/go/telepresence/docs>

Audio commands.....	104
xCommand Audio Diagnostics Advanced Run.....	104
xCommand Audio Diagnostics MeasureDelay.....	104
xCommand Audio Microphones Mute.....	105
xCommand Audio Microphones ToggleMute.....	105
xCommand Audio Microphones Unmute.....	105
xCommand Audio Sound Play.....	105
xCommand Audio Sound Stop.....	105
xCommand Audio SoundsAndAlerts Ringtone List.....	105
xCommand Audio SoundsAndAlerts Ringtone Play.....	106
xCommand Audio SoundsAndAlerts Ringtone Stop.....	106
xCommand Audio Volume Decrease	106
xCommand Audio Volume Increase.....	106
xCommand Audio Volume Mute.....	106
xCommand Audio Volume Set	107
xCommand Audio Volume SetToDefault	107
xCommand Audio Volume ToggleMute.....	107
xCommand Audio Volume Unmute	107
xCommand Audio VuMeter Start	107
xCommand Audio VuMeter Stop.....	108
xCommand Audio VuMeter StopAll.....	108
Bookings commands	108
xCommand Bookings Clear.....	108
xCommand Bookings Get	108
xCommand Bookings List	109
xCommand Bookings NotificationSnooze.....	109
Call commands.....	110
xCommand Call Accept.....	110
xCommand Call Disconnect.....	110
xCommand Call DTMFSend	110
xCommand Call FarEndControl Camera Move	110
xCommand Call FarEndControl Camera Stop.....	111
xCommand Call FarEndControl RoomPreset Activate	111
xCommand Call FarEndControl Source Select	111
xCommand Call FarEndMessage Send.....	111
xCommand Call Forward.....	112
xCommand Call Hold.....	112
xCommand Call Ignore.....	112
xCommand Call Join	112
xCommand Call Reject.....	113
xCommand Call Resume	113
xCommand Call UnattendedTransfer	113
CallHistory commands.....	114
xCommand CallHistory AcknowledgeAllMissedCalls	114
xCommand CallHistory AcknowledgeMissedCall	114
xCommand CallHistory DeleteAll	114
xCommand CallHistory DeleteEntry	114
xCommand CallHistory Get	115
xCommand CallHistory Recents	115
Camera commands	116
xCommand Camera PositionSet	116
xCommand Camera Preset Activate	116



xCommand Camera Preset ActivateDefaultPosition.....	116	
xCommand Camera Preset Edit.....	117	
xCommand Camera Preset List.....	117	
xCommand Camera Preset Remove.....	117	
xCommand Camera Preset Show.....	118	
xCommand Camera Preset Store.....	118	
xCommand Camera Ramp.....	119	
Cameras commands.....	120	
xCommand Cameras SpeakerTrack Activate.....	120	
xCommand Cameras SpeakerTrack Deactivate.....	120	
xCommand Cameras SpeakerTrack Diagnostics Start.....	120	
xCommand Cameras SpeakerTrack Diagnostics Stop.....	121	
Conference commands	121	
xCommand Conference Call AuthenticationResponse.....	121	
xCommand Conference DoNotDisturb Activate	122	
xCommand Conference DoNotDisturb Deactivate	122	
xCommand Conference Participant Admit	122	
xCommand Conference Participant Disconnect.....	122	
xCommand Conference Participant Mute.....	123	
xCommand Conference Participant Search	123	
xCommand Conference Recording Pause.....	124	
xCommand Conference Recording Resume	124	
xCommand Conference Recording Start.....	124	
xCommand Conference Recording Stop	124	
xCommand Conference SpeakerLock Release	124	
xCommand Conference SpeakerLock Set	125	
Diagnostics commands	125	
xCommand Diagnostics Run	125	
Dial commands.....	126	
xCommand Dial	126	
HttpClient commands.....	127	
xCommand HttpClient Allow Hostname Add	127	
xCommand HttpClient Allow Hostname Clear	127	
xCommand HttpClient Allow Hostname List	127	
xCommand HttpClient Allow Hostname Remove	127	
xCommand HttpClient Delete	128	
xCommand HttpClient Get	129	
xCommand HttpClient Patch.....	130	
xCommand HttpClient Post.....	131	
xCommand HttpClient Put.....	132	
HttpFeedback commands	133	
xCommand HttpFeedback Deregister	133	
xCommand HttpFeedback Enable	133	
xCommand HttpFeedback Register	133	
Logging commands.....	134	
xCommand Logging SendLogs.....	134	
Macros commands	134	
xCommand Macros Log Clear	134	
xCommand Macros Log Get	134	
xCommand Macros Macro Activate	134	
xCommand Macros Macro Deactivate	135	
xCommand Macros Macro Get	135	
xCommand Macros Macro Remove	135	
xCommand Macros Macro RemoveAll	135	
xCommand Macros Macro Rename	136	
xCommand Macros Macro Roles Set	136	
xCommand Macros Macro Save	136	
xCommand Macros Runtime Restart	136	
xCommand Macros Runtime Start	136	
xCommand Macros Runtime Status	137	
xCommand Macros Runtime Stop	137	



Message commands	137
xCommand Message Send.....	137
 Peripherals commands.....	 138
xCommand Peripherals Connect.....	138
xCommand Peripherals HeartBeat.....	138
xCommand Peripherals List.....	139
xCommand Peripherals Pairing DeviceDiscovery Start.....	139
xCommand Peripherals Pairing Pair.....	139
xCommand Peripherals Pairing Unpair	140
xCommand Peripherals Purge	140
 Phonebook commands.....	 140
xCommand Phonebook Contact Add	140
xCommand Phonebook Contact Delete	141
xCommand Phonebook Contact Modify	141
xCommand Phonebook ContactMethod Add	142
xCommand Phonebook ContactMethod Delete	142
xCommand Phonebook ContactMethod Modify.....	143
xCommand Phonebook Folder Add.....	143
xCommand Phonebook Folder Delete	143
xCommand Phonebook Folder Modify.....	144
xCommand Phonebook Search	144
 Presentation commands.....	 145
xCommand Presentation Start.....	145
xCommand Presentation Stop	146
 Provisioning commands	 146
xCommand Provisioning CompleteUpgrade.....	146
xCommand Provisioning PostponeUpgrade.....	146
xCommand Provisioning CUCM ExtensionMobility Login.....	147
xCommand Provisioning CUCM ExtensionMobility Logout	147
 xCommand Provisioning Service Fetch	 147
 Proximity commands	 148
xCommand Proximity Services Activate.....	148
xCommand Proximity Services Deactivate.....	148
 RoomPreset commands	 149
xCommand RoomPreset Activate	149
xCommand RoomPreset Clear	149
xCommand RoomPreset Store	149
 Security commands.....	 150
xCommand Security Certificates CA Add	150
xCommand Security Certificates CA Delete.....	150
xCommand Security Certificates CA Show	150
xCommand Security Certificates Services Activate	150
xCommand Security Certificates Services Add	150
xCommand Security Certificates Services Deactivate	151
xCommand Security Certificates Services Delete	151
xCommand Security Certificates Services Show	151
xCommand Security Certificates ThirdParty Disable	151
xCommand Security Certificates ThirdParty Enable.....	152
xCommand Security Certificates ThirdParty List	152
xCommand Security Certificates ThirdParty Show	152
xCommand Security Certificates Webex Show	153
xCommand Security FIPSMode Activate	153
xCommand Security Persistency	154
xCommand Security Session Get	154
xCommand Security Session List	154
xCommand Security Session Terminate	154
 Standby commands.....	 155
xCommand Standby Activate	155



xCommand Standby Deactivate.....	155	xCommand UserInterface Extensions List.....	163
xCommand Standby Halfwake.....	155	xCommand UserInterface Extensions Panel Clicked.....	163
xCommand Standby ResetHalfwakeTimer.....	155	xCommand UserInterface Extensions Panel Close	163
xCommand Standby ResetTimer.....	155	xCommand UserInterface Extensions Panel Open.....	163
SystemUnit commands.....	156	xCommand UserInterface Extensions Panel Remove	163
xCommand SystemUnit Boot.....	156	xCommand UserInterface Extensions Panel Save.....	164
xCommand SystemUnit FactoryReset.....	156	xCommand UserInterface Extensions Panel Update.....	164
xCommand SystemUnit FirstTimeWizard Stop	157	xCommand UserInterface Extensions Set.....	164
xCommand SystemUnit Notifications RemoveAll	157	xCommand UserInterface Extensions Widget Action	164
xCommand SystemUnit OptionKey Add	157	xCommand UserInterface Extensions Widget SetValue	165
xCommand SystemUnit OptionKey List	157	xCommand UserInterface Extensions Widget UnsetValue	165
xCommand SystemUnit OptionKey Remove	157	xCommand UserInterface Message Alert Clear	165
xCommand SystemUnit OptionKey RemoveAll	158	xCommand UserInterface Message Alert Display	165
xCommand SystemUnit SignInBanner Clear	158	xCommand UserInterface Message Prompt Clear	166
xCommand SystemUnit SignInBanner Get	158	xCommand UserInterface Message Prompt Display	166
xCommand SystemUnit SignInBanner Set	158	xCommand UserInterface Message Prompt Response	167
xCommand SystemUnit SoftReset.....	158	xCommand UserInterface Message TextInput Clear	167
xCommand SystemUnit SoftwareUpgrade	159	xCommand UserInterface Message TextInput Display	168
xCommand SystemUnit WelcomeBanner Clear	159	xCommand UserInterface Message TextInput Response	169
xCommand SystemUnit WelcomeBanner Get	159	xCommand UserInterface Message TextLine Clear	169
xCommand SystemUnit WelcomeBanner Set	159	xCommand UserInterface Message TextLine Display	169
Time commands	160	xCommand UserInterface WebView Clear	169
xCommand Time DateTime Get	160	xCommand UserInterface WebView Display	170
xCommand Time DateTime Set	160		
UserInterface commands	160		
xCommand UserInterface Branding Clear	160	UserManagement commands.....	170
xCommand UserInterface Branding Delete	160	xCommand UserManagement RemoteSupportUser Create	170
xCommand UserInterface Branding Fetch	161	xCommand UserManagement RemoteSupportUser Delete	170
xCommand UserInterface Branding Get	161	xCommand UserManagement RemoteSupportUser DisablePermanently	170
xCommand UserInterface Branding Updated	162	xCommand UserManagement RemoteSupportUser GetState	171
xCommand UserInterface Branding Upload	162	xCommand UserManagement User Add	171
xCommand UserInterface Extensions Clear	162	xCommand UserManagement User Delete	172
		xCommand UserManagement User Get	172
		xCommand UserManagement User List	172
		xCommand UserManagement User Modify	173
		xCommand UserManagement User Passphrase Change	173



xCommand UserManagement User Passphrase Set	173
xCommand UserManagement User Unblock	174
Video commands.....	174
xCommand Video ActiveSpeakerPIP Set.....	174
xCommand Video CEC Input KeyClick.....	175
xCommand Video Input MainVideo Mute.....	175
xCommand Video Input MainVideo Unmute	175
xCommand Video Layout LayoutFamily Set	175
xCommand Video Output Monitor Backlight Set	176
xCommand Video Output Monitor Reset	176
xCommand Video PresentationPIP Set.....	176
xCommand Video PresentationView Set.....	176
xCommand Video Selfview Set.....	177
WebEngine commands.....	177
xCommand UserInterface WebEngine DeleteStorage.....	177
Webex commands.....	178
xCommand Webex Registration Cancel	178
xCommand Webex Registration Start.....	178



Audio commands

xCommand Audio Diagnostics Advanced Run

Requires user role: ADMIN, USER

This command sends out a noise signal sequentially on all audio output connectors and measures the room impulse response (RIR) between the output and the microphones. If a RIR is detected, the detected number of microphones (input), the detected number of output connectors, and the detected delay between the output and input is reported back.

Example:

```
xCommand Audio Diagnostics Advanced Run Volume: 50 MeasurementLength: 1
```

Result returned ->

OK

*r AdvancedRunResult (status=OK):

*r AdvancedRunResult HdmiSpeakersDelay: "100 ms"

*r AdvancedRunResult NumHdmiSpeakersDetected: 2

*r AdvancedRunResult NumMicsDetected: 1

** end

USAGE:

```
Audio Diagnostics Advanced Run [MeasurementLength: MeasurementLength] [Volume: Volume]
```

where

MeasurementLength:

Integer (1..100)

The length of the measurement in number of seconds. In a noisy environment a longer measurement duration will give a more reliable and robust result.

Default value: 3

Volume:

Integer (0..50)

The volume of the test signal. In a noisy environment a higher volume gives more reliable and robust results.

Default value: 20

xCommand Audio Diagnostics MeasureDelay

Requires user role: ADMIN, USER

This command measures the audio delay/latency in a device that is connected to the video conferencing device. A typical use case is to measure the delay in a TV connected to the video conferencing device via the HDMI connector. If the delay in a TV is too high, the real-time experience of a video call will be substantially degraded. If the delay is more than 50 ms we recommend the user to find a TV setting that has shorter delay. Typical TV settings that can reduce the delay are: Gaming Mode and PC Mode.

This command will measure the delay between output and input (microphone). This means that if you are using an external acoustic echo canceller or audio mixer, this command will also measure the delay of these devices.

USAGE:

```
Audio Diagnostics MeasureDelay [MeasurementLength: MeasurementLength] [Output: Output] [Volume: Volume]
```

where

MeasurementLength:

Integer (1..100)

The length of the measurement in number of seconds. In a noisy environment a longer measurement duration will give a more reliable and robust result.

Default value: 6

Output:

HDMI/Line/Internal/All

HDMI: Measure the delay of the device connected to the HDMI output.

Line: Measure the delay of the device connected to the Line output (only available on video conferencing devices that have a Line output).

Internal: Measure the delay of the internal loudspeaker (only available on video conferencing devices that have an internal loudspeaker).

All: Will measure the maximum delay of all outputs.

Default value: HDMI

Volume:

Integer (0..50)

The volume of the test signal. In a noisy environment a higher volume gives more reliable and robust results.

Default value: 20



xCommand Audio Microphones Mute

Requires user role: ADMIN, INTEGRATOR, USER

Mute all microphones.

USAGE:

```
Audio Microphones Mute
```

xCommand Audio Microphones ToggleMute

Requires user role: ADMIN, INTEGRATOR, USER

Toggle the microphone between muted and unmuted.

USAGE:

```
Audio Microphones ToggleMute
```

xCommand Audio Microphones Unmute

Requires user role: ADMIN, INTEGRATOR, USER

Unmute all microphones.

USAGE:

```
Audio Microphones Unmute
```

xCommand Audio Sound Play

Requires user role: ADMIN, INTEGRATOR, USER

Play a specified audio sound.

USAGE:

```
Audio Sound Play [Loop: Loop] Sound: Sound
```

where

Loop:

Off/On

Determines whether or not to loop the playout of the audio sound. The sound is looped by default. Irrespective of how this parameter is set, some of the sounds (Busy, CallWaiting, Dial, Ringing, and SpecialInfo) will play until the Audio Sound Stop command is issued.

Default value: Off

Sound:

Alert/Announcement/Binding/Bump/Busy/CallDisconnect/CallInitiate/CallWaiting/Dial/KeyInput/KeyInputDelete/KeyTone/Nav/NavBack/Notification/OK/Pairing/PresentationConnect/Ringing/SignIn/SpecialInfo/StartListening/TelephoneCall/VideoCall/VolumeAdjust/WakeUp

Choose which ringtone to play.

xCommand Audio Sound Stop

Requires user role: ADMIN, INTEGRATOR, USER

Stop playing audio sound.

USAGE:

```
Audio Sound Stop
```

xCommand Audio SoundsAndAlerts Ringtone List

Requires user role: ADMIN, INTEGRATOR, USER

List all available ringtones. Use the xConfiguration Audio SoundsAndAlerts RingTone setting to choose a ringtone.

USAGE:

```
Audio SoundsAndAlerts Ringtone List
```



xCommand Audio SoundsAndAlerts Ringtone Play

Requires user role: ADMIN, INTEGRATOR, USER

Play one of the available ringtones. Use the xCommand Audio SoundsAndAlerts Ringtone List command to get a list of the available ringtones.

USAGE:

Audio SoundsAndAlerts Ringtone Play [Loop: Loop] RingTone: "RingTone"

where

Loop:

On/Off

Repeats the chosen ringtone in a loop. To turn off the audio, use the Audio SoundsAndAlerts Ringtone Stop xCommand.

Default value: Off

RingTone:

String (1, 100)

The name of the ringtone.

xCommand Audio SoundsAndAlerts Ringtone Stop

Requires user role: ADMIN, INTEGRATOR, USER

Stops the chosen ringtone from playing. To start playing the ringtone again, use the Audio SoundsAndAlerts Ringtone Play xCommand.

USAGE:

Audio SoundsAndAlerts Ringtone Stop

xCommand Audio Volume Decrease

Requires user role: ADMIN, USER

Decrease the volume on the device. By default, the volume is decreased by 5 steps (each step is 0.5 dB). Use the Steps parameter if you want to override the default behavior.

USAGE:

Audio Volume Decrease [Steps: Steps]

where

Steps:

Integer (1..10)

Choose the number of steps to decrease the volume with. One step is 0.5 dB.

Default value: 5

xCommand Audio Volume Increase

Requires user role: ADMIN, USER

Increase the volume on the video conferencing device. By default, the volume is increased by 5 steps (each step is 0.5 dB). Use the Steps parameter if you want to override the default behavior.

USAGE:

Audio Volume Increase [Steps: Steps]

where

Steps:

Integer (1..10)

Choose the number of steps to increase the volume with. One step is 0.5 dB.

Default value: 5

xCommand Audio Volume Mute

Requires user role: ADMIN, USER

Mute the volume on the video conferencing device.

USAGE:

Audio Volume Mute



xCommand Audio Volume Set

Requires user role: ADMIN, USER

Set the volume on the video conferencing device to a specified level.

USAGE:

Audio Volume Set Level: Level

where

Level:

Integer (0..100)

Select the gain level. 70 equals 0 dB gain, and 100 equals 15 dB gain.

xCommand Audio Volume SetToDefault

Requires user role: ADMIN, USER

Set the volume to the default level that is defined in the xConfiguration Audio DefaultVolume setting.

USAGE:

Audio Volume SetToDefault

xCommand Audio Volume ToggleMute

Requires user role: ADMIN, USER

Toggle the loudspeaker between muted and unmuted.

USAGE:

Audio Volume ToggleMute

xCommand Audio Volume Unmute

Requires user role: ADMIN, USER

Set the volume on the device back on after muting.

USAGE:

Audio Volume Unmute

xCommand Audio VuMeter Start

Requires user role: ADMIN, USER

Start a VU meter to show the audio signal level on the specified connector. You have to specify both the connector's type and number (ConnectorType, ConnectorID) to uniquely identify the connector. The VU meter measures the input level for frequencies below 20 kHz.

USAGE:

Audio VuMeter Start ConnectorID: ConnectorID ConnectorType: ConnectorType [IncludePairingQuality: IncludePairingQuality] [IntervalMs: IntervalMs]

where

ConnectorID:

Integer (1..1) for Microphone; Integer (1..1) for HDMI

Select a connector number. Microphone [1] is the built-in microphone.

ConnectorType:

HDMI/Microphone/MicArray

Select the connector type.

IncludePairingQuality:

Off/On

The device can measure the pairing quality (value 0 to 100). With no other ultrasound sources in the same room this value will be high, but if there are other ultrasound sources in the same room the value will be low. To monitor the pairing quality, sign in to the device's web interface, navigate to Setup > Peripherals > Microphones and tick the Show Pairing Rate check box. Or, use the xFeedback and xEvents commands to monitor the value. Read more about the xFeedback and xEvents commands in the API introduction section in this guide.

Default value: Off

IntervalMs:

10..1000

Specifies the update interval in milliseconds of the VuMeter values. The values can be specified in 10 ms steps.

Default value: 100



xCommand Audio VuMeter Stop

Requires user role: ADMIN, USER

Stop the VU meter on the specified connector. You have to specify both the connector's type and number (ConnectorType, ConnectorID) to uniquely identify the connector.

USAGE:

Audio VuMeter Stop ConnectorID: ConnectorID ConnectorType: ConnectorType

where

ConnectorID:

Integer (1..1) for Microphone; Integer (1..1) for HDMI

Select a connector number. Microphone [1] is the built-in microphone.

ConnectorType:

HDMI/Microphone/MicArray

Select the connector type.

xCommand Audio VuMeter StopAll

Requires user role: ADMIN, USER

Stop all VU meters.

USAGE:

Audio VuMeter StopAll

Bookings commands

xCommand Bookings Clear

Requires user role: ADMIN, USER

Clear the current stored list of bookings.

USAGE:

Bookings Clear

xCommand Bookings Get

Requires user role: ADMIN, USER

Get the booking information for a specific ID.

USAGE:

Bookings Get Id: "Id"

where

Id:

String (0, 128)

The booking ID of a call or conference.



xCommand Bookings List

Requires user role: ADMIN, USER

List the stored bookings for the device. The list of booking details is received from the management system. All parameters are optional, and can be used to limit the search result.

If no parameters are set, past, present and future bookings are all listed. To avoid listing bookings from yesterday and before, use DayOffset = 0.

USAGE:

Bookings List [Days: Days] [DayOffset: DayOffset] [Limit: Limit] [Offset: Offset]

where

Days:

Integer (1..365)

Number of days to retrieve bookings from.

DayOffset:

Integer (0..365)

Which day to start the search from (today: 0, tomorrow: 1, ...).

Default value: 0

Limit:

Integer (1..65534)

Max number of bookings to list.

Offset:

Integer (0..65534)

Offset number of bookings for this search.

Default value: 0

xCommand Bookings NotificationSnooze

Requires user role: ADMIN, USER

Sets notifications for the stored bookings in this device to snooze.

USAGE:

Bookings NotificationSnooze [Id: "Id"] [SecondsToSnooze: SecondsToSnooze]

where

Id:

String (0..128)

The ID of the notification snooze setting.

SecondsToSnooze:

Integer (1..3600)

The duration of the snooze period, in seconds.

Default value: 300



Call commands

xCommand Call Accept

Requires user role: ADMIN, USER

Accept an incoming call. If no CallId is specified, all incoming calls are accepted.

USAGE:

```
Call Accept [CallId: CallId]
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During the call you can run the xStatus Call command to see the CallId.

Default value: 0

xCommand Call Disconnect

Requires user role: ADMIN,INTEGRATOR, USER

Disconnect a call.

USAGE:

```
Call Disconnect [CallId: CallId]
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During the call you can run the xStatus Call command to see the CallId.

Default value: 0

xCommand Call DTMFSend

Requires user role: ADMIN, USER

Send DTMF tones to the far end.

USAGE:

```
Call DTMFSend [CallId: CallId] DTMFString: "DTMFString"
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During the call you can run the xStatus Call command to see the CallId.

Default value: -1

DTMFString:

String (0..32)

Enter the DTMF string.

xCommand Call FarEndControl Camera Move

Requires user role: ADMIN, USER

Move the far end camera (the remote camera).

NOTE: The far end camera moves in the specified direction until the stop command (ref: xCommand FarEndControl Camera Stop) is issued.

USAGE:

```
Call FarEndControl Camera Move [CallId: CallId] Value: Value
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During the call you can run the xStatus Call command to see the CallId.

Default value: -1

Value:

Left/Right/Up/Down/ZoomIn/ZoomOut

Select the action for how to move the camera.



xCommand Call FarEndControl Camera Stop

Requires user role: ADMIN, USER

Stop the far end camera after the xCommand FarEndControl Camera Move has been issued.

USAGE:

```
Call FarEndControl Camera Stop [CallId: CallId]
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Default value: -1

xCommand Call FarEndControl RoomPreset Activate

Requires user role: ADMIN, USER

While in a call, this command is used to activate a preset on the far end codec. The preset covers the far end codec's camera positions and input video switcher settings.

The preset must be stored on the far end codec beforehand, either by using the xCommand Preset Store command locally on the far end codec, or by using the xCommand FarEndControl Preset Store command from a remote codec.

Note: The far end codec's xConfiguration Conference FarEndControl Mode setting must be switched On for the FarEndControl commands to work.

USAGE:

```
Call FarEndControl RoomPreset Activate [CallId: CallId] PresetId: PresetId
```

where

CallId:

Integer (0..65534)

The CallId is required to identify the far end codec only when in a Multipoint call. The CallId is returned when issuing the xCommand Dial command. During a call you can run the xStatus Call command to see the CallId.

Default value: -1

PresetId:

Integer (1..15)

The ID of the preset that is stored on the far end codec.

xCommand Call FarEndControl Source Select

Requires user role: ADMIN, USER

Select which video input source to use as the main source on the far end device.

USAGE:

```
Call FarEndControl Source Select [CallId: CallId] SourceId: SourceId
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Default value: -1

SourceId:

Integer (0..15)

Select a video input source on the far end.

xCommand Call FarEndMessage Send

Requires user role: ADMIN, USER

Send data between two codecs in a point-to-point call, for use with control systems or macros. Works with SIP calls only. Requires that the Conference FarEndMessage Mode is set to On.

USAGE:

```
Call FarEndMessage Send Text: "Text" Type: "Type" [CallId: CallId]
```

where

Text:

String (1, 1450)

Enter the message to be sent to the far end.

Type:

String (0, 255)

Enter the message type to be sent to the far end.

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.



xCommand Call Forward

Requires user role: ADMIN, USER

Specifies what number or URI you want to forward your incoming calls to. The display name is a local reference for the forwarded destination. A message, together with the local reference, is shown on screen when you have configured the device to forward all calls.

USAGE:

Call Forward DisplayName: "DisplayName" Number: "Number"

where

DisplayName:

String (0, 255)

The local reference for the forwarded destination.

Number:

String (0, 255)

The directory number or URI which you want to forward the incoming calls to.

xCommand Call Hold

Requires user role: ADMIN, USER

Put a call on hold.

USAGE:

Call Hold [CallId: CallId] [Reason: Reason]

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Default value: 0

Reason:

Conference/Transfer/Other

Internal usage only.

Default value: Other

xCommand Call Ignore

Requires user role: ADMIN, USER

Turns off the ringtone for the incoming call. The call can still be answered.

USAGE:

Call Ignore CallId: CallId

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

xCommand Call Join

Requires user role: ADMIN, USER

Internal usage only.

USAGE:

Call Join [CallId: CallId]

where

CallId:

Integer (0..65534)

You can have from 1 to 10 CallId parameters in the same command.



xCommand Call Reject

Requires user role: ADMIN, USER

Reject incoming call. If no call id is specified, all incoming calls are rejected.

USAGE:

```
Call Reject [CallId: CallId]
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Default value: 0

xCommand Call Resume

Requires user role: ADMIN, USER

Resume a call that have been put on hold.

USAGE:

```
Call Resume [CallId: CallId]
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Default value: 0

xCommand Call UnattendedTransfer

Requires user role: ADMIN, USER

Transfers an ongoing call to another participant. Fully supported for SIP calls only.

USAGE:

```
Call UnattendedTransfer CallId: CallId Number: "Number"
```

where

CallId:

Integer (0..65534)

The CallID is returned when the xCommand Dial command is run. During a call you can run the xStatus Call command to see the CallId.

Number:

String (0, 255)

The number the call is transferred to.



CallHistory commands

xCommand CallHistory AcknowledgeAllMissedCalls

Requires user role: ADMIN, USER

Turns off the missed calls indicator on the touch controller for all missed calls.

USAGE:

```
CallHistory AcknowledgeAllMissedCalls
```

xCommand CallHistory AcknowledgeMissedCall

Requires user role: ADMIN, USER

Turns off the missed calls indicator on the touch controller for the specified call.

USAGE:

```
CallHistory AcknowledgeMissedCall CallHistoryId: CallHistoryId
[AcknowledgeConsecutiveDuplicates: AcknowledgeConsecutiveDuplicates]
```

where

CallHistoryId:

Integer (1..2147483647)

CallHistoryId for the call in question. Run xCommand CallHistory Get to get the id number.

AcknowledgeConsecutiveDuplicates:

False/True

You can include or exclude all surrounding calls with duplicate information.

Default value: False

xCommand CallHistory DeleteAll

Requires user role: ADMIN, USER

Deletes all information on previous calls.

USAGE:

```
CallHistory DeleteAll [Filter: Filter]
```

where

Filter:

All/Missed/Placed/Received

You can filter which calls to delete.

Default value: All

xCommand CallHistory DeleteEntry

Requires user role: ADMIN, USER

Deletes all information on the specified call.

USAGE:

```
CallHistory DeleteEntry CallHistoryId: CallHistoryId
[DeleteConsecutiveDuplicates: DeleteConsecutiveDuplicates]
```

where

CallHistoryId:

Integer (1..2147483647)

CallHistoryId for the call in question. Run xCommand CallHistory Get to get the id number.

DeleteConsecutiveDuplicates:

False/True

You can delete the surrounding calls with duplicate information or not.

Default value: False



xCommand CallHistory Get

Requires user role: ADMIN, USER

Retrieve all information on previous calls made on the device.

USAGE:

CallHistory Get [Filter: Filter] [Offset: Offset] [Limit: Limit] [DetailLevel: DetailLevel] [SearchString: "SearchString"] [CallHistoryId: CallHistoryId]

where

Filter:

All/Missed/AnsweredElsewhere/Forwarded/Placed/NoAnswer/Received/Rejected/
UnacknowledgedMissed

You can filter which calls to retrieve.

Default value: All

Offset:

Integer (0..65534)

Sets the call from which to start.

Default value: 0

Limit:

Integer (0..65534)

Defines the amount of calls in the output.

Default value: 65534

DetailLevel:

Basic/Full

Sets the level of detail for the information on these calls.

Default value: Basic

SearchString:

String (0, 255)

Allows you to set the command to apply to a specified display name or call back number.

Default value: ""

CallHistoryId:

Integer (1..2147483647)

CallHistoryId for the call in question.

xCommand CallHistory Recents

Requires user role: ADMIN, USER

Retrieve aggregated information on previous calls made on the device.

USAGE:

CallHistory Recents [Filter: Filter] [Offset: Offset] [Limit: Limit] [DetailLevel: DetailLevel] [SearchString: "SearchString"] [Order: Order]

where

Filter:

All/Missed/AnsweredElsewhere/Forwarded/Placed/NoAnswer/Received/Rejected/
UnacknowledgedMissed

You can filter which calls to retrieve.

Default value: All

Offset:

Integer (0..65534)

Sets the call from which to start.

Default value: 0

Limit:

Integer (0..65534)

Defines the amount of calls in the output.

Default value: 65534

DetailLevel:

Basic/Full

Sets the level of detail for the information on these calls.

Default value: Basic

SearchString:

String (0, 255)

Allows you to set the command to apply to a specified display name or call back number.

Default value: ""

Order:

OccurrenceTime/OccurrenceFrequency

Define the order in which the previous calls are presented.

Default value: OccurrenceTime



Camera commands

xCommand Camera PositionSet

Requires user role: ADMIN, INTEGRATOR, USER

Set the camera position. If the combination of the pan, tilt, zoom, and roll values is not possible, the camera automatically adjusts the values to a valid combination.

USAGE:

```
Camera PositionSet CameraId: CameraId [Focus: Focus] [Lens: Lens] [Pan: Pan]  
[Tilt: Tilt] [Zoom: Zoom]
```

where

CameraId:

Integer (1..1)

The ID of the camera preset you want to reset.

Focus:

Integer (0..65535)

Focus the camera near or far.

Lens:

Wide/Center/Left/Right

Set the camera's lens position.

Pan:

Integer (-10000..10000)

Move the camera to the left or right.

Tilt:

Integer (-2500..2500)

Move the camera up or down.

Zoom:

Integer (0..11800)

Zoom in or out.

xCommand Camera Preset Activate

Requires user role: ADMIN, USER

Activate one of the stored camera presets.

Note that the xCommand Camera Preset commands applies to an individual camera. This is in contrast to the xCommand Preset commands where a single preset covers ALL connected cameras plus the Video Input switcher settings.

USAGE:

```
Camera Preset Activate PresetId: PresetId
```

where

PresetId:

Integer (1..35)

The ID of the camera preset you want to activate.

xCommand Camera Preset ActivateDefaultPosition

Requires user role: ADMIN, USER

Sets the cameras to their default position, if one is defined. The default position is defined by xCommand Camera Preset Store or by xCommand Camera Preset Edit. Only one default position can be defined per camera.

USAGE:

```
Camera Preset ActivateDefaultPosition [CameraId: CameraId]
```

where

CameraId:

Integer (1..1)

The ID of the camera preset you want to activate. If Camerald is not specified, all cameras will be set in their respective default position, if one is defined.



xCommand Camera Preset Edit

Requires user role: ADMIN, USER

Edit a stored camera preset. You can change the name of the camera preset and its position in the list that is returned by the xCommand Camera Preset List command. You can also change whether or not this preset is the default position for the associated camera.

Note that the xCommand Camera Preset commands applies to an individual camera. This is in contrast to the xCommand Preset commands where a single preset covers ALL connected cameras and the Video Input switcher settings.

USAGE:

```
Camera Preset Edit PresetId: PresetId [ListPosition: ListPosition] [Name: Name]  
[DefaultPosition: DefaultPosition]
```

where

PresetId:

Integer (1..35)

The ID of the camera preset you want to edit.

ListPosition:

Integer (1..35)

The position in the list returned by the xCommand Camera Preset List command.

Name:

String (0, 255)

The name of the camera preset. It will be used in the list returned by the xCommand Camera Preset List command.

DefaultPosition:

False/True

Defines whether or not this preset is the default position for the associated camera. Note that each camera can only have one default position, so if set, the old default preset will automatically be marked as not default.

xCommand Camera Preset List

Requires user role: ADMIN, USER

List information about available camera presets.

Note that the xCommand Camera Preset commands applies to an individual camera. This is in contrast to the xCommand Preset commands where a single preset covers ALL connected cameras plus the Video Input switcher settings.

USAGE:

```
Camera Preset List [CameraId: CameraId] [DefaultPosition: DefaultPosition]
```

where

CameraId:

Integer (1..1)

Only list presets for the specified camera.

DefaultPosition:

False/True

List default positions only, or only those that are not default positions.

xCommand Camera Preset Remove

Requires user role: ADMIN, USER

Remove a camera preset.

Note that the xCommand Camera Preset commands applies to an individual camera. This is in contrast to the xCommand Preset commands where a single preset covers ALL connected cameras plus the Video Input switcher settings.

USAGE:

```
Camera Preset Remove PresetId: PresetId
```

where

PresetId:

Integer (1..35)

The ID of the camera preset you want to remove.



xCommand Camera Preset Show

Requires user role: ADMIN, USER

Shows the preset details for the requested PresetId.

USAGE:

Camera Preset Show PresetId: PresetId

where

PresetId:

Integer (1..35)

The ID of the camera preset you wish to see.

xCommand Camera Preset Store

Requires user role: ADMIN, USER

Store the current position (pan and tilt), zoom and focus of the chosen camera. The camera is identified by the CameraId parameter.

Note that the xCommand Camera Preset commands applies to an individual camera. This is in contrast to the xCommand Preset commands where a single preset covers ALL connected cameras plus the Video Input switcher settings. The xCommand Camera Preset commands are useful when you want to handle multiple camera positions individually per camera, rather than working with complete sets of camera positions. The individual camera presets are not available for far end control.

USAGE:

Camera Preset Store [PresetId: PresetId] CameraId: CameraId [ListPosition: ListPosition] [Name: "Name"] [TakeSnapshot: TakeSnapshot] [DefaultPosition: DefaultPosition]

where

PresetId:

Integer (1..35)

The ID of this camera preset. If not set explicitly, the codec will assign a preset ID automatically.

CameraId:

Integer (1..1)

Select the camera for which to store the preset position.

ListPosition:

Integer (1..35)

The new camera preset's position in the list returned by the xCommand Camera Preset List command.

Name:

String (0, 255)

The name of the new camera preset. It will be used in the list returned by the xCommand Camera Preset List command.

TakeSnapshot:

False/True

Allow or disallow snapshot of the preview.

DefaultPosition:

False/True

Defines whether or not this preset shall be the default position of the associated camera.



Note that each camera can hold only one default position, so if set, the old default preset will automatically be marked as not default.

xCommand Camera Ramp

Requires user role: ADMIN, INTEGRATOR, USER

Move the camera in a specified direction. The camera moves at specified speed until a stop command is issued. In a daisy chain, you need to know the Camerald for the camera you want to address. Be aware that pan and tilt can be operated simultaneously, but no other combinations. In the latter case only the first operation specified is executed. For example, if you try to run both zoom and pan at the same time, only zoom is executed.

NOTE: You must run a stop command to stop the camera, see the example below.

USAGE:

Camera Ramp CameraId: CameraId [Pan: Pan] [PanSpeed: PanSpeed] [Tilt: Tilt] [TiltSpeed: TiltSpeed] [Zoom: Zoom] [ZoomSpeed: ZoomSpeed] [Focus: Focus]
where

CameraId:

Integer (1..1)

Select the camera.

Pan:

Left/Right/Stop

Move the camera to the Left or Right, followed by Stop.

PanSpeed:

Integer (1..15)

Set the pan speed.

Tilt:

Down/Up/Stop

Move the camera Up or Down, followed by Stop.

TiltSpeed:

Integer (1..15)

Set the tilt speed.

Zoom:

In/Out/Stop

Zoom the camera In or Out, followed by Stop.

ZoomSpeed:

Integer (1..15)

Set the zoom speed.

Focus:

*Far/Near/Stop*

Focus the camera Far or Near, followed by Stop.

Cameras commands

xCommand Cameras SpeakerTrack Activate

Requires user role: ADMIN, USER

Activate Best Overview mode. Requires that xConfiguration Cameras SpeakerTrack Mode is set to Auto (default).

USAGE:

```
Cameras SpeakerTrack Activate
```

xCommand Cameras SpeakerTrack Deactivate

Requires user role: ADMIN, USER

Deactivate Best Overview mode.

USAGE:

```
Cameras SpeakerTrack Deactivate
```

xCommand Cameras SpeakerTrack Diagnostics Start

Requires user role: ADMIN, INTEGRATOR, USER

Starts diagnostics on the camera's tracking for best overview.

USAGE:

```
Cameras SpeakerTrack Diagnostics Start [Tracking: Tracking]
```

where

Tracking:

On/Off

The Tracking parameter is not applicable for this product.

Default value: On



xCommand Cameras SpeakerTrack Diagnostics Stop

Requires user role: ADMIN, INTEGRATOR, USER

Stops diagnostics on the camera's tracking.

USAGE:

```
Cameras SpeakerTrack Diagnostics Stop
```

Conference commands

xCommand Conference Call AuthenticationResponse

Requires user role: ADMIN, USER

This command is only available for Cisco Webex registered devices. The command gives a response to an authentication request based on the Conference Call[n] AuthenticationRequest status.

USAGE:

```
Conference Call AuthenticationResponse [CallId: CallId] ParticipantRole: ParticipantRole [Pin: Pin]
```

where

CallId:

Integer (1..65534)

Unique identifier of the call. During a call you can run the xStatus Call command to see the CallId.

ParticipantRole:

Host/Panelist/Guest

Host: Join as host.

Panelist: Join as panelist.

Guest: Join as guest.

Pin:

String(0, 32)

PIN code. Must be provided if joining as host, panelist or as guest when the Conference Call[n] AuthenticationRequest status indicates that a PIN code must provided.



xCommand Conference DoNotDisturb Activate

Requires user role: ADMIN, INTEGRATOR, USER

This command switches on the Do Not Disturb mode, and the Timeout parameter allows you to control when it is switched off again. When Do Not Disturb is switched on, all incoming calls are rejected and registered as missed calls. The calling side receives a busy signal.

USAGE:

```
Conference DoNotDisturb Activate [Timeout: Timeout]
```

where

Timeout:

Integer (1..1440)

Set the number of minutes before Do Not Disturb is switched off. If not set, Do Not Disturb times out after 1440 minutes (24 hours).

xCommand Conference DoNotDisturb Deactivate

Requires user role: ADMIN, INTEGRATOR, USER

Switch off the Do Not Disturb mode. When Do Not Disturb is switched off incoming calls come through as normal.

USAGE:

```
Conference DoNotDisturb Deactivate
```

xCommand Conference Participant Admit

Requires user role: ADMIN, USER

Admits or lets in a participant that is waiting to be admitted into the call or meeting. This command is only available Cisco Webex registered devices.

A participant is waiting to be admitted if he has status "waiting" in the result from the Conference ParticipantList Search command (*r ParticipantListSearchResult Participant [n] Status = "waiting").

USAGE:

```
Conference Participant Admit CallId: CallId ParticipantId: "ParticipantId"
```

where

CallId:

Integer (0..65534)

Unique identifier of the call. During a call you can run the xStatus Call command to see the CallId.

ParticipantId:

String (0..255)

Unique identifier of a participant in the call.

xCommand Conference Participant Disconnect

Requires user role: ADMIN, USER

Disconnects the participant from a call or meeting. It is only possible to disconnect a participant if the Conference Call[n] Capabilities ParticipantDisconnect status for the meeting shows Available.

USAGE:

```
Conference Participant Disconnect CallId: CallId ParticipantId: "ParticipantId"
```

where

CallId:

Integer (0..65534)

Unique identifier of the call. During a call you can run the xStatus Call command to see the CallId.

ParticipantId:

String (0..255)

Unique identifier of a participant in the call.



xCommand Conference Participant Mute

Requires user role: ADMIN, USER

Mutes the participant in the call or meeting. It is only possible to mute a participant if the Conference Call[n] Capabilities ParticipantMute status shows Available.

USAGE:

Conference Participant Mute AudioMute: AudioMute CallId: CallId ParticipantId: "ParticipantId"

where

AudioMute:

On/Off

Indicate the desired mute state of the participant.

CallId:

Integer (0..65534)

Unique identifier of the call. During a call you can run the xStatus Call command to see the CallId.

ParticipantId:

String (0..255)

Unique identifier of a participant in the call.

xCommand Conference Participant Search

Requires user role: ADMIN, USER

Searches the list of participants in the call or meeting. There is a participant list that can be searched only if the Conference Call[n] Capabilities ParticipantList status shows Available.

USAGE:

Conference Participant Search [CallId: CallId] [Limit: Limit] [Offset: Offset] [SearchString: "SearchString"]

where

CallId:

Integer (0..65534)

Unique identifier of the call. During a call you can run the xStatus Call command to see the CallId.

Limit:

Integer (0..65534)

Limit the number of records (participants) in the result set to this number. For example, if the limit is set to 10, the result set will contain only 10 entries even if the total number of hits is larger.

Offset:

Integer (0..65534)

Get records starting with this offset in a search.

SearchString:

String (0..255)

URI or DisplayName. Leave this parameter empty if you want the search to return all participants in the call.



xCommand Conference Recording Pause

Requires user role: ADMIN, USER

Define if the recording of a meeting shall be paused. When you are recording a meeting, you can use this setting if you want to pause the recording. You can resume the recording by using the command Conference Recording Resume.

USAGE:

Conference Recording Pause [CallId: CallId]

where

CallId:

Integer (1..65534)

Identify CallID for the remote participant.

xCommand Conference Recording Resume

Requires user role: ADMIN, USER

Define if the recording of a meeting shall be resumed. When you are recording a meeting, you can use this setting if you want to resume a recording that has previously been paused.

USAGE:

Conference Recording Resume [CallId: CallId]

where

CallId:

Integer (1..65534)

Identify CallID for the remote participant.

xCommand Conference Recording Start

Requires user role: ADMIN, USER

Define if the meeting shall be recorded. Once you are in a meeting, you can use this setting if you want to start recording. Note that the recording commands are only available if your infrastructure (Cisco Meeting Server) supports recording.

USAGE:

Conference Recording Start [CallId: CallId]

where

CallId:

Integer (1..65534)

Identify CallID for the remote participant.

xCommand Conference Recording Stop

Requires user role: ADMIN, USER

Define if the recording of a meeting shall be stopped. When you are recording a meeting, you can use this setting to stop recording.

USAGE:

Conference Recording Stop [CallId: CallId]

where

CallId:

Integer (1..65534)

Identify CallID for the remote participant.

xCommand Conference SpeakerLock Release

Requires user role: ADMIN, USER

Releases locked speaker set by xCommand Conference SpeakerLock Set. Default voice switching is switched back on.

USAGE:

Conference SpeakerLock Release



xCommand Conference SpeakerLock Set

Requires user role: ADMIN, USER

For manually locking one of the speakers to the prominent speaker position. This overrides the default voice switching.

USAGE:

Conference SpeakerLock Set Target: Target [CallId: CallId]

where

Target:

Local/Remote

Identifies local or remote participant.

CallId:

Integer (0..65534)

Identify CallID for the remote participant. Only relevant if Target is set to "remote".

Default value: 0

Diagnostics commands

xCommand Diagnostics Run

Requires user role: ADMIN

This command runs self-diagnostics commands on the device.

USAGE:

Diagnostics Run [ResultSet: ResultSet]

where

ResultSet:

Alerts/All/None

You can filter the diagnostics results to alerts, all or none. If not set, the result will show all results.

Default value: Alerts



Dial commands

xCommand Dial

Requires user role: ADMIN, INTEGRATOR, USER

Dial out from the device. Returns information about the CallId and ConferenceId, which are required for some of the other commands.

USAGE:

```
Dial Number: "Number" [Protocol: Protocol] [CallRate: CallRate] [CallType: CallType] [BookingId: "BookingId"] [Appearance: Appearance] [DisplayName: "DisplayName"] [TrackingData: "TrackingData"]
```

where

Number:

String (0, 255)

Enter the number or address.

Protocol:

H320/H323/Sip/Spark

Select the call protocol.

CallRate:

Integer (64..10000)

Set the call rate.

CallType:

Audio/Video/Auto

Select a call type (audio or video). By selecting Auto, the device will detect the call type automatically.

BookingId:

String (0, 255)

Any identifier that an external booking system (e.g. TMS, CTS-MAN) can use for its own references to match placed calls with the booking systems internal identifier for a meeting. This can be any string, e.g. a GUID. The booking Id is supplied in call logs, call events etc for the call.

Default value: ""

Appearance:

Integer (1..999999999)

Not applicable. For internal usage only.

DisplayName:

String (0, 255)

The display name of the remote participant.

Default value: ""

TrackingData:

String (0, 255)

Adds a tag to a call, so that it can be identified in the call history.

Default value:



HttpClient commands

xCommand HttpClient Allow Hostname Add

Requires user role: ADMIN

Adds an HTTP(S) server to the list of allowed servers (hosts).

The HttpClient Allow Hostname commands let you set up and maintain a list of up to ten allowed hosts. As long as the list is not empty, you can send HTTP(S) requests only to the servers in the list. The check against the list is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

USAGE:

`HttpClient Allow Hostname Add Expression: "Expression"`

where

Expression:

`String (2, 200)`

Regular expression that matches a host name or IP address of an HTTP(S) server.

xCommand HttpClient Allow Hostname Clear

Requires user role: ADMIN

Removes all HTTP(S) servers from the list of allowed servers (hosts), leaving you with an empty list.

USAGE:

`HttpClient Allow Hostname Clear`

xCommand HttpClient Allow Hostname List

Requires user role: ADMIN

Returns the list of allowed HTTP(S) servers (hosts).

The HttpClient Allow Hostname commands let you set up and maintain a list of up to ten allowed hosts. As long as the list is not empty, you can send HTTP(S) requests only to the servers in the list. The check against the list is performed both when using insecure (HTTP) and secure (HTTPS) transfer of data.

USAGE:

`HttpClient Allow Hostname List`

xCommand HttpClient Allow Hostname Remove

Requires user role: ADMIN

Removes an HTTP(S) server from the list of allowed servers (hosts). Use the HttpClient Allow Hostname List command to find the identifier of each entry in the list.

USAGE:

`HttpClient Allow Hostname Remove Id: Id`

where

Id:

`Integer (0..9)`

The identifier of the HTTP(S) server you want to remove from the list.



xCommand HttpClient Delete

Requires user role: ADMIN

Sends an HTTP(S) Delete request to the server that is specified in the Url parameter. You can use the AllowInsecureHTTPS parameter to specify whether or not to validate the server's certificate before sending data over HTTPS. This parameter has no effect unless the xConfiguration HttpClient AllowInsecureHTTPS is set to On. The command returns the HTTP status code along with the data returned from the server (HTTP headers and body).

USAGE:

```
HttpClient Delete [AllowInsecureHTTPS: AllowInsecureHTTPS] [Header: "Header"]  
[ResponseSizeLimit: ResponseSizeLimit] [ResultBody: ResultBody] [Timeout:  
Timeout] Url: "Url"
```

where

AllowInsecureHTTPS:

False/True

If set to True the device skips the certificate validation process, and sends data to the server anyway. If set to False, the server certificate is checked, and data is not sent to the server if the certificate validation fails.

Header:

String (0, 1024)

An HTTP header field. You can add up 20 Header parameters in one command, each holding one HTTP header field.

ResponseSizeLimit:

Integer (1..100000)

The maximum payload size (bytes) of the response to this request. If the response payload is larger than this maximum size, the command returns a status error with a message saying that the maximum file size is exceeded. However, this has no effect on the server side; the request was received and processed properly by the server.

ResultBody:

None/PlainText/Base64

None: The body of the HTTP response (if any) is not included in the command result.

PlainText: The body of the HTTP response is included in the command result as plain text. If the response contain non-printable letters, the command returns a status error with a message saying that non-printable data was encountered.

Base64: The body of the HTTP response is Base64 encoded before it is included in the command result.

Timeout:

Integer (1..30)

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

Default value: 30

Url:

String (8, 2048)

The URL that the request will be sent to: <Protocol> + <Host name or IP address of an HTTP(S) server> + <Path>.



xCommand HttpClient Get

Requires user role: ADMIN

Sends an HTTP(S) Get request to the server that is specified in the Url parameter. You can use the AllowInsecureHTTPS parameter to specify whether or not to validate the server's certificate before sending data over HTTPS. This parameter has no effect unless the xConfiguration HttpClient AllowInsecureHTTPS is set to On. The command returns the HTTP status code along with the data returned from the server (HTTP headers and body).

USAGE:

```
HttpClient Get [AllowInsecureHTTPS: AllowInsecureHTTPS] [Header: "Header"]  
[ResponseSizeLimit: ResponseSizeLimit] [ResultBody: ResultBody] [Timeout:  
Timeout] Url: "Url"
```

where

AllowInsecureHTTPS:

False/True

If set to True the device skips the certificate validation process, and sends data to the server anyway. If set to False, the server certificate is checked, and data is not sent to the server if the certificate validation fails.

Header:

String (0, 1024)

An HTTP header field. You can add up 20 Header parameters in one command, each holding one HTTP header field.

ResponseSizeLimit:

Integer (1..100000)

The maximum payload size (bytes) of the response to this request. If the response payload is larger than this maximum size, the command returns a status error with a message saying that the maximum file size is exceeded. However, this has no effect on the server side; the request was received and processed properly by the server.

ResultBody:

None/PlainText/Base64

None: The body of the HTTP response (if any) is not included in the command result.

PlainText: The body of the HTTP response is included in the command result as plain text. If the response contain non-printable letters, the command returns a status error with a message saying that non-printable data was encountered.

Base64: The body of the HTTP response is Base64 encoded before it is included in the command result.

Timeout:

Integer (1..30)

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

Default value: 30

Url:

String (8, 2048)

The URL that the request will be sent to: <Protocol> + <Host name or IP address of an HTTP(S) server> + <Path>.



xCommand HttpClient Patch

Requires user role: ADMIN

Sends an HTTP(S) Patch request to the server that is specified in the Url parameter. This is a multiline command, so the payload (data) follows after the parameters. You can use the AllowInsecureHTTPS parameter to specify whether or not to validate the server's certificate before sending data over HTTPS. This parameter has no effect unless the xConfiguration HttpClient AllowInsecureHTTPS is set to On. The command returns the HTTP status code along with the data returned from the server (HTTP headers and body).

USAGE:

```
HttpClient Patch [AllowInsecureHTTPS: AllowInsecureHTTPS] [Header: "Header"]  
[ResponseSizeLimit: ResponseSizeLimit] [ResultBody: ResultBody] [Timeout:  
Timeout] Url: "Url"
```

where

AllowInsecureHTTPS:

False/True

If set to True the device skips the certificate validation process, and sends data to the server anyway. If set to False, the server certificate is checked, and data is not sent to the server if the certificate validation fails.

Header:

String (0, 1024)

An HTTP header field. You can add up 20 Header parameters in one command, each holding one HTTP header field.

ResponseSizeLimit:

Integer (1..100000)

The maximum payload size (bytes) of the response to this request. If the response payload is larger than this maximum size, the command returns a status error with a message saying that the maximum file size is exceeded. However, this has no effect on the server side; the request was received and processed properly by the server.

ResultBody:

None/PlainText/Base64

None: The body of the HTTP response (if any) is not included in the command result.

PlainText: The body of the HTTP response is included in the command result as plain text. If the response contain non-printable letters, the command returns a status error with a message saying that non-printable data was encountered.

Base64: The body of the HTTP response is Base64 encoded before it is included in the command result.

Timeout (1..30)

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

Default value: 30

Url:

String (8, 2048)

The URL that the request will be sent to: <Protocol> + <Host name or IP address of an HTTP(S) server> + <Path>.



xCommand HttpClient Post

Requires user role: ADMIN

Sends an HTTP(S) Post request to the server that is specified in the Url parameter.

You can use the AllowInsecureHTTPS parameter to specify whether or not to validate the server's certificate before sending data over HTTPS. This parameter has no effect unless the xConfiguration HttpClient AllowInsecureHTTPS is set to On.

This is a multiline command, so the payload (data) follows after the parameters.

USAGE:

```
HttpClient Post [AllowInsecureHTTPS: AllowInsecureHTTPS] [Header: "Header"]  
[ResponseSizeLimit: ResponseSizeLimit] [ResultBody: ResultBody] [Timeout:  
Timeout] Url: "Url"
```

where

AllowInsecureHTTPS:

False/True

If set to True the device skips the certificate validation process, and sends data to the server anyway. If set to False, the server certificate is checked, and data is not sent to the server if the certificate validation fails.

Header:

String (0, 1024)

An HTTP header field. You can add up 20 Header parameters in one command, each holding one HTTP header field.

ResponseSizeLimit:

Integer (1..100000)

The maximum payload size (bytes) of the response to this request. If the response payload is larger than this maximum size, the command returns a status error with a message saying that the maximum file size is exceeded. However, this has no effect on the server side; the request was received and processed properly by the server.

ResultBody:

None/PlainText/Base64

None: The body of the HTTP response (if any) is not included in the command result.

PlainText: The body of the HTTP response is included in the command result as plain text. If the response contain non-printable letters, the command returns a status error with a message saying that non-printable data was encountered.

Base64: The body of the HTTP response is Base64 encoded before it is included in the command result.

Timeout:

Integer (1..30)

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

Default value: 30

Url:

String (8, 2048)

The URL that the request will be sent to: <Protocol> + <Host name or IP address of an HTTP(S) server> + <Path>.



xCommand HttpClient Put

Requires user role: ADMIN

Sends an HTTP(S) Put request to the server that is specified in the Url parameter.

You can use the AllowInsecureHTTPS parameter to specify whether or not to validate the server's certificate before sending data over HTTPS. This parameter has no effect unless the xConfiguration HttpClient AllowInsecureHTTPS is set to On.

This is a multiline command, so the payload (data) follows after the parameters.

USAGE:

```
HttpClient Put [AllowInsecureHTTPS: AllowInsecureHTTPS] [Header: "Header"]  
[ResponseSizeLimit: ResponseSizeLimit] [ResultBody: ResultBody] [Timeout:  
Timeout] Url: "Url"
```

where

AllowInsecureHTTPS:

False/True

If set to True the device skips the certificate validation process, and sends data to the server anyway. If set to False, the server certificate is checked, and data is not sent to the server if the certificate validation fails.

Header:

String (0, 1024)

An HTTP header field. You can add up 20 Header parameters in one command, each holding one HTTP header field.

ResponseSizeLimit:

Integer (1..100000)

The maximum payload size (bytes) of the response to this request. If the response payload is larger than this maximum size, the command returns a status error with a message saying that the maximum file size is exceeded. However, this has no effect on the server side; the request was received and processed properly by the server.

ResultBody:

None/PlainText/Base64

None: The body of the HTTP response (if any) is not included in the command result.

PlainText: The body of the HTTP response is included in the command result as plain text. If the response contain non-printable letters, the command returns a status error with a message saying that non-printable data was encountered.

Base64: The body of the HTTP response is Base64 encoded before it is included in the command result.

Timeout:

Integer (1..30)

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

Default value: 30

Url:

String (8, 2048)

The URL that the request will be sent to: <Protocol> + <Host name or IP address of an HTTP(S) server> + <Path>.



HttpFeedback commands

xCommand HttpFeedback Deregister

Requires user role: ADMIN

Deregister the HTTP feedback over HTTP(S).

USAGE:

HttpFeedback Deregister FeedbackSlot: FeedbackSlot

where

FeedbackSlot:

Integer (1..4)

Deregister the feedback slot that was registered using the xCommand HttpFeedback Register command.

xCommand HttpFeedback Enable

Requires user role: ADMIN

Re-enables a previously registered feedback slot after it has failed and become deactivated.

USAGE:

HttpFeedback Enable FeedbackSlot: FeedbackSlot

where

FeedbackSlot:

Integer (1..4)

Specifies the feedback slot that is enabled.

xCommand HttpFeedback Register

Requires user role: ADMIN

Register the device to an HTTP(S) server to return XML feedback over HTTP(S) to specific URLs.

USAGE:

HttpFeedback Register FeedbackSlot: FeedbackSlot [Format: Format] ServerUrl: ServerUrl [Expression: "Expression"]

where

FeedbackSlot:

Integer (1..4)

The codec can register up to 4 slots of servers requesting HTTP feedback. Set the registering to one of them.

Note: Avoid using FeedbackSlot 3 in an environment where Cisco TelePresence Management Suite (TMS) is used as TMS uses this feedbackslot to register its expressions.

Format:

XML/JSON

Set the format for the feedback from the HTTP server to XML or JSON.

Default value: XML

ServerUrl:

String (1, 2048)

The URL to the HTTP server where you want the codec to post the HTTP feedback messages to.

Expression:

String (1, 255)

The XPath expression specifies which parts of the Status, Configuration or Event XML documents are monitored. You can have from 0 to 15 XPath expressions in the same command.



Logging commands

xCommand Logging SendLogs

Requires user role: ADMIN, USER

This command applies only to devices that are registered to the Cisco Webex cloud service. Send logs to the Cisco Webex cloud. These logs can help diagnose and fix issues with the device. The command returns a log ID, which an administrator or TAC engineer can use to identify and download the logs.

USAGE:

Logging SendLogs

Macros commands

xCommand Macros Log Clear

Requires user role: ADMIN

Clears the Macros Logs.

USAGE:

Macros Log Clear

xCommand Macros Log Get

Requires user role: ADMIN

Shows the logs for all running macros and for the runtime itself.

USAGE:

Macros Log Get [Offset: Offset]

where

Offset:

Integer (0..65534)

Shows lines with the same or higher Offset than the one provided.

Default value: 0

xCommand Macros Macro Activate

Requires user role: ADMIN

Activates a macro created on this device.

USAGE:

Macros Macro Activate Name: "Name"

where

Name:

String (0..255)

Specifies the name of the macro to activate.



xCommand Macros Macro Deactivate

Requires user role: ADMIN

Deactivates a macro currently running on this device.

USAGE:

Macros Macro Deactivate Name: "Name"

where

Name:

String (0..255)

The name of the macro to deactivate.

xCommand Macros Macro Get

Requires user role: ADMIN

Shows the details of a macro created on this device.

USAGE:

Macros Macro Get [Content: Content] [Name: "Name"]

where

Content:

False/True

Shows the content for the specified Macro or not.

Default value: False

Name:

String (0..255)

The name of the macro.

xCommand Macros Macro Remove

Requires user role: ADMIN

Removes a macro created on this device.

USAGE:

Macros Macro Remove Name: "Name"

where

Name:

String (0..255)

The name of the macro that is removed.

xCommand Macros Macro RemoveAll

Requires user role: ADMIN

Removes all of the macros created on this device.

USAGE:

Macros Macro RemoveAll



xCommand Macros Macro Rename

Requires user role: ADMIN

Renames a macro created on this device.

USAGE:

```
Macros Macro Rename Name: "Name" NewName: "NewName" [Overwrite: Overwrite]
```

where

Name:

String (0..255)

The name of the macro that is renamed.

NewName:

String (0..255)

The new name of the macro.

Overwrite:

False/True

Overwrites the existing content or not.

Default value: False

xCommand Macros Macro Roles Set

Requires user role: ADMIN

Sets the role for a macro.

USAGE:

```
Macros Macro Roles Set Name: "Name" [Role: Role]
```

where

Name:

String (0..255)

The name of the macro that is set.

Role:

Admin/Audit/User/Integrator/RoomControl

The role that is set for this macro.

Default value: Admin

xCommand Macros Macro Save

Requires user role: ADMIN

Saves the details of a macro. This is a multiline command.

USAGE:

```
Macros Macro Save Name: "Name" [Overwrite: Overwrite] [Transpile: Transpile]
```

where

Name:

String (0..255)

The name of the macro that is saved.

Overwrite:

False/True

Overwrites the existing content or not.

Default value: True

Transpile:

False/True

Translates current JavaScript language features into EcmaScript 5.0/5.1.

Default value: True



xCommand Macros Runtime Status

Requires user role: ADMIN

Shows the current status of the macros runtime on this device.

USAGE:

Macros Runtime Status

xCommand Macros Runtime Stop

Requires user role: ADMIN

Stops all of the macros set up on this device.

USAGE:

Macros Runtime Stop

Message commands

xCommand Message Send

Requires user role: ADMIN, INTEGRATOR

Triggers a Message Send event which sends text to any listening clients.

USAGE:

Message Send Text: "Text"

where

Text:

String (0..255)

The text that the message contains.



Peripherals commands

xCommand Peripherals Connect

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Register peripherals that are connected to the codec, such as control systems and touch panels. The registered peripherals are displayed on the web interface under Configuration > Peripherals.

This command should be used when the peripheral connects to the codec for the first time or when the software version on the peripheral has changed. The list of connected devices is available with the command xStatus Peripherals ConnectedDevice [n] Status.

USAGE:

```
Peripherals Connect [HardwareInfo: "HardwareInfo"] ID: "ID" [Name: "Name"]  
[NetworkAddress: "NetworkAddress"] [SerialNumber: "SerialNumber"] [SoftwareInfo:  
"SoftwareInfo"] Type: Type
```

where

HardwareInfo:

String (0, 100)

The device's hardware number.

Default value: ""

ID:

String (1, 100)

A unique ID for the device you are connecting to, typically a MAC address.

Name:

String (0, 100)

Define a name for the device.

Default value: ""

NetworkAddress:

String (0, 100)

Network address for the device you are connecting to.

Default value: ""

SerialNumber:

String (0, 100)

The device's serial number.

Default value: ""

SoftwareInfo:

String (0, 100)

Software version the device is running.

Default value: ""

Type:

Byod/ControlSystem/Other/TouchPanel

Define the type of device you are connecting to.

xCommand Peripherals HeartBeat

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

When a peripheral is registered as a connected device, you can set it to send a heartbeat to the codec to let the codec know that it is still connected.

This will keep the device on the xStatus Peripherals ConnectedDevice list. If the peripheral is not set to send a heartbeat, the device will disappear from the list after a while.

Note: Does not apply to cameras.

USAGE:

```
Peripherals HeartBeat ID: "ID" [Timeout: Timeout]
```

where

ID:

String (1, 100)

A unique ID for the device you are connecting to, typically a MAC address.

Timeout:

Integer (1..65535)

Set how long the device will send heartbeat.

Default value: 60



xCommand Peripherals List

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Lists all currently and previously connected peripherals.

USAGE:

Peripherals List [Connected: Connected] [Type: Type]

where

Connected:

False/True

Limit the search to currently connected devices.

Type:

All/ControlSystem/ISDNLink/Other/TouchPanel

Limit the search by device type.

Default value: All

xCommand Peripherals Pairing DeviceDiscovery Start

Requires user role: ADMIN

Start device discovery to detect ISDN Links in the same network.

USAGE:

Peripherals Pairing DeviceDiscovery Start [AutoPairing: AutoPairing] [DeviceType: DeviceType] [Timeout: Timeout]

where

AutoPairing:

On/Off

You can select to automatically pair the detected device to the video conferencing device.

Default value: Off

DeviceType:

ISDNLink

Only look for ISDN Link.

Timeout:

Integer (3..60)

Set a maximum time for the search from 3 to 60 seconds.

Default value: 10

xCommand Peripherals Pairing Pair

Requires user role: ADMIN

Pair an ISDN Link to a video conferencing device.

USAGE:

Peripherals Pairing Pair MacAddress: "MacAddress"

where

MacAddress:

String (1, 1450)

Enter the MAC address for the ISDN Link you wish to pair to the video conferencing device.



xCommand Peripherals Pairing Unpair

Requires user role: ADMIN, USER

Unpair the video conferencing device from an ISDN Link, when the two have contact.

USAGE:

Peripherals Pairing Unpair MacAddress: "MacAddress"

where

MacAddress:

String (1, 100)

Enter the MAC address for the ISDN Link you wish to unpair from the video conferencing device.

xCommand Peripherals Purge

Requires user role: ADMIN, USER

Force unpair a video conferencing device from an ISDN Link when a connection has been lost.
Note: You must also unpair the ISDN Link to be able to pair it to another video conferencing device.

USAGE:

Peripherals Purge ID: "ID"

where

ID:

String (1, 100)

Mac address of the ISDN Link in the format "xx:xx:xx:xx:xx:xx".

Phonebook commands

xCommand Phonebook Contact Add

Requires user role: ADMIN, USER

Add a new contact to the local phonebook. The command returns the ContactId, which is a unique string that identifies the contact; typically, the format is "localContactId-n".

You can add several contact methods to a contact using the xCommand Phonebook ContactMethod Add command. Note that only the first contact method will appear in the Favorites list on the Cisco Touch controller. All contact methods are available on the other UIs.

USAGE:

Phonebook Contact Add Name: "Name" [Number: "Number" [CallRate: CallRate [CallType: CallType] [Device: Device] [FolderId: "FolderId" [ImageURL: "ImageURL"] [Protocol: Protocol] [Tag: Tag] [Title: "Title"]]

where

Name:

String (0, 255)

The name of the contact.

Number:

String (0, 255)

The phone number or address of the contact.

CallRate:

Integer (0..6000)

Set a call rate.

CallType:

Audio/Video/Auto

Select a call type (audio or video). By selecting Auto, the device will detect the call type automatically.

Device:

Mobile/Other/Telephone/Video

Select the device type.

FolderId:

String (0, 255)

The unique identifier for the folder that you want to store the contact in. The identifier will



be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued to make the folder.

ImageURL:

String (0, 255)

Currently not in use.

Protocol:

Auto/H320/H323/SIP/Spark

Select the Auto, Spark, SIP, H323 or H320 protocol.

Tag:

Untagged/Favorite

Tag the contact as a Favorite, or untag an already tagged contact.

Title:

String (0, 255)

The title of the contact.

xCommand Phonebook Contact Delete

Requires user role: ADMIN, USER

Delete an existing contact from the local phonebook.

USAGE:

Phonebook Contact Delete ContactId: "ContactId"

where

ContactId:

String (0, 255)

The unique identifier for the contact. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Contact Add command was issued to make the contact.

xCommand Phonebook Contact Modify

Requires user role: ADMIN, USER

Modify contact details of an existing contact in the local phonebook. The following parameters can be changed using this command: Name, FolderId, ImageURL and Title. You must use the xCommand Phonebook ContactMethod Modify command to change the other parameters: Number, Protocol, CallRate, CallType and Device.

USAGE:

Phonebook Contact Modify ContactId: "ContactId" [Name: "Name"] [FolderId: "FolderId"] [ImageURL: "ImageURL"] [Tag: Tag] [Title: "Title"]

where

ContactId:

String (0, 255)

The unique identifier for the contact you want to modify. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Contact Add command was issued to make the contact.

Name:

String (0, 255)

The name of the contact.

FolderId:

String (0, 255)

A unique identifier for the folder. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued.

ImageURL:

String (0, 255)

Currently not in use.

Tag:

Untagged/Favorite

Tag the contact as a Favorite, or untag an already tagged contact.

Title:

String (0, 255)

The title of the contact.



xCommand Phonebook ContactMethod Add

Requires user role: ADMIN, USER

Add contact details for an existing contact in the local phonebook. The command returns the ContactMethodId, which is a unique string that identifies the contact method; typically, the format is "n".

You can add several contact methods to a contact. Note that only the first contact method will appear in the Favorites list on the device's user interface. The first contact method may have been created when issuing the xCommand Phonebook Contact Add command to make the contact. All contact methods are available in the API and on the web interface.

USAGE:

```
Phonebook ContactMethod Add ContactId: "ContactId" [CallRate: CallRate]  
[CallType: CallType] [Device: Device] Number: "Number" [Protocol: Protocol]
```

where

ContactId:

String (0, 255)

The unique identifier for the contact that you want to add a contact method to. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Contact Add command was issued to make the contact.

CallRate:

Integer (0..6000)

Set a call rate.

CallType:

Audio/Video/Auto

Select a call type (audio or video). By selecting Auto, the device will detect the call type automatically.

Default value: Auto

Device:

Mobile/Other/Telephone/Video

Set which type of device to call to.

Number:

String (0, 255)

The phone number or address of the contact.

Protocol:

Auto/H320/H323/SIP/Spark

Select protocol.

xCommand Phonebook ContactMethod Delete

Requires user role: ADMIN, USER

Delete a contact method from an existing contact in the local phonebook.

USAGE:

```
Phonebook ContactMethod Delete ContactId: "ContactId" ContactMethodId:  
"ContactMethodId"
```

where

ContactId:

String (0, 255)

The unique identifier for the contact you want to change. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Contact Add command was issued to make the contact.

ContactMethodId:

String (0, 255)

The unique identifier for the contact method you want to delete. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook ContactMethod Add command was issued to make the contact method.



xCommand Phonebook ContactMethod Modify

Requires user role: ADMIN, USER

Modify details about the contact method for an existing contact in the local phonebook.

USAGE:

```
Phonebook ContactMethod Modify ContactId: "ContactId" ContactMethodId: "ContactMethodId" [Device: Device] [Number: "Number" ] [Protocol: Protocol]  
[CallRate: CallRate] [CallType: CallType]
```

where

ContactId:

String (0, 255)

The unique identifier for the contact. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Contact Add command was issued to make the contact.

ContactMethodId:

String (0, 255)

The unique identifier for the contact method you want to modify. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook ContactMethod Add or xCommand Phonebook Contact Add commands were issued to make the contact method.

Device:

Mobile/Other/Telephone/Video

Set which type of device to call to.

Number:

String (0, 255)

The phone number or address of the contact.

Protocol:

Auto/H320/H323/SIP/Spark

Select protocol.

CallRate:

Integer (0..6000)

Set a call rate.

CallType:

Audio/Video/Auto

Select a call type (audio or video). By selecting Auto, the device will detect the call type automatically.

Default value: Auto

xCommand Phonebook Folder Add

Requires user role: ADMIN, USER

Phonebook entries can be stored in folders. Use this command to add a folder to the local phonebook. The command returns the FolderId, which is a unique string that identifies the folder; typically, the format is "localGroupId-n".

USAGE:

```
Phonebook Folder Add Name: "Name" [ParentFolderId: "ParentFolderId"]
```

where

Name:

String (0, 255)

The name of the folder.

ParentFolderId:

String (0, 255)

The unique identifier for the parent folder. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued to make the parent folder.

xCommand Phonebook Folder Delete

Requires user role: ADMIN, USER

Delete an existing folder from the local phonebook.

USAGE:

```
Phonebook Folder Delete FolderId: "FolderId"
```

where

FolderId:

String (0, 255)

The unique identifier for the folder. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued to make the folder.



xCommand Phonebook Folder Modify

Requires user role: ADMIN, USER

Modify an existing phonebook folder.

USAGE:

Phonebook Folder Modify FolderId: "FolderId" [Name: "Name"] [ParentFolderId: "ParentFolderId"]

where

FolderId:

String (0, 255)

The unique identifier for the folder. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued to make the folder.

Name:

String (0, 255)

The name of the contact.

ParentFolderId:

String (0, 255)

The unique identifier for the parent folder. The identifier will be returned by an xCommand Phonebook Search command. It was also returned when the xCommand Phonebook Folder Add command was issued to make the parent folder.

xCommand Phonebook Search

Requires user role: ADMIN, USER

The search command lets you search in both the local and corporate phone books. A search gives a ResultSet.

The total number of folders and contacts (TotalRows) is always included in the result set when searching the local phone book. When searching a corporate phonebook the total number of folders and contacts may not be included. Whether it is included or not depends on the backend corporate phonebook service (e.g. CUCM, VCS, TMS) and its version.

USAGE:

Phonebook Search [PhonebookId: "PhonebookId"] [PhonebookType: PhonebookType] [SearchString: "SearchString"] [SearchField: SearchField] [SearchFilter: SearchFilter] [ContactType: ContactType] [Offset: Offset] [FolderId: "FolderId"] [Limit: Limit] [ContactMethodLimit: ContactMethodLimit] [Recursive: Recursive] [Tag: Tag]

where

PhonebookId:

String (0, 255)

The identifier of the phonebook server that will be searched. See the xConfiguration Phonebook Server ID setting.

PhonebookType:

Corporate/Local

Define whether to search the local phone book or the corporate phonebook.

Default value: Local

SearchString:

String (0, 255)

Search for entries containing this string (note that the entry does not have to begin with the string). If no FolderId is specified, all folders / phonebook directories will be searched.

SearchField:

Name/Number

Currently not in use.

SearchFilter:

All/Rooms/People

Only available for Cisco Webex registered devices. Filter search results by choosing the type of results you want to see. You can select rooms, people, or search in all directories.

ContactType:

**Any/Folder/Contact**

Search all contact types, or limit the search to folders or individual contacts.

Default value: Any

Offset:

Integer (0..65534)

Get records starting with this offset in a search. The default value is 0. Offset is used together with Limit to support paging.

Default value: 0

FolderId:

String (0, 255)

Search only in the specified folder. The FolderId (string) is listed in the ResultSet of a search result containing folders.

Limit:

Integer (0..65534)

Limit the number of records in the result set to this number. For example, if the limit is set to 10, the ResultSet will contain only 10 entries (Contacts and Folders) even if the total number of hits is larger. The maximum limit is 1000.

Default value: 50

ContactMethodLimit:

Integer (0..10)

Limit the number of records in the result set to this number. For example, if the limit is set to 2, the ResultSet will contain only 2 entries even if the total number of hits is larger.

Default value: 0

Recursive:

False/True

This parameter will only have effect when searching the local phone book. The setting determines whether a local phone book search should be limited to the given FolderId, or also recursively search in its subfolders. If not specified, the search will be recursive.

When issuing the command without specifying any parameters, all folders, contacts and contact methods in the local phone book will be returned.

Default value: True

Tag:

Untagged/Favorite

Limits the search to contacts that have been tagged as favorite or the untagged contacts.

Presentation commands

xCommand Presentation Start

Requires user role: ADMIN, USER

Open a media stream from the selected presentation source.

You can combine multiple presentation sources in a single presentation video stream (the maximum number of different input sources depend on the type of video conferencing device) by adding multiple ConnectorIds or PresentationSources in the same command. The order in which you write them in the command determines the order in which the sources show up on the screen. You can't use a mix of identifier types in the same command; use either ConnectorId or PresentationSource.

USAGE:

Presentation Start [ConnectorId: ConnectorId] [Instance: Instance] [Layout: Layout] [PresentationSource: PresentationSource] [SendingMode: SendingMode]
where

ConnectorId:

Integer (1..2)

Select the video input source to be used for presentation, identified by connectorId.

Instance:

New/1/2/3/4/5/6

Select which local presentation instance you wish to start.

Layout:

Equal/Prominent

Select the layout of the presentation if the stream is composed of multiple input sources.

Equal: The presentations are shown in same-sized images. There can be a maximum of four images on screen.

Prominent: The first presentation source is shown as a large image, and the next presentation sources are shown as smaller images placed below.

PresentationSource:

Integer (1..2)

Select the video input source to be used for presentation, identified by source number.

SendingMode:

LocalRemote/LocalOnly

Select whether the presentation is shown local and/or remote.



LocalRemote: The presentation is shown both local and remote.

LocalOnly: The presentation is shown locally.

Default value: LocalRemote

xCommand Presentation Stop

Requires user role: ADMIN, USER

Stop the media stream from the presentation source.

USAGE:

Presentation Stop [Instance: *Instance*] [PresentationSource: *PresentationSource*]

where

Instance:

1/2/3/4/5/6

Select which local presentation you wish to stop, identified by presentation instance.

PresentationSource:

Integer (1..2)

Select which local presentation you wish to stop, identified by source number.

Provisioning commands

xCommand Provisioning CompleteUpgrade

Requires user role: ADMIN, USER

Starts installing the software upgrade if you wish to install it before it is set to do so.

USAGE:

Provisioning CompleteUpgrade

xCommand Provisioning PostponeUpgrade

Requires user role: ADMIN, USER

Postpones the installing of the software upgrade.

USAGE:

Provisioning PostponeUpgrade SecondsToPostpone: *SecondsToPostpone*

where

SecondsToPostpone:

Integer (0..65534)

Set how long to postpone the upgrade. The value is in seconds.



xCommand Provisioning CUCM ExtensionMobility Login

Requires user role: ADMIN, USER

Login command for the Extension Mobility service. You log in to the Extension Mobility service with a username (UserId) and pin code (Pin). The username and pin code are set up in CUCM. CUCM also supports multiple profiles for a user.

If you, for a user that has multiple profiles, submit a login command with only username and pin code, CUCM will send a list of available profiles back to the device. Then the device will create corresponding ExtensionMobilityProfileSelection Profile events, so that a new login command, which contains the Profile parameter in addition to the username and pin code, can be submitted.

USAGE:

Provisioning CUCM ExtensionMobility Login UserId: "UserId" Pin: "Pin" [Profile: "Profile"]

where

UserId:

String (1, 255)

A valid username, as set up in CUCM.

Pin:

String (1, 255)

A valid pin code for the user, as set up in CUCM.

Profile:

String (1, 255)

A valid profile for the user, as set up in CUCM. This parameter applies only if the user has multiple profiles.

xCommand Provisioning CUCM ExtensionMobility Logout

Requires user role: ADMIN, USER

This command will log you out of your Extension Mobility profile.

USAGE:

Provisioning CUCM ExtensionMobility Logout

xCommand Provisioning Service Fetch

Requires user role: ADMIN

Add or update the customization template that details the custom elements of the device. Examples of custom elements are: branding images, macros, favorites, sign-in banner, and in-room control panels.

USAGE:

Provisioning Service Fetch [Checksum: "Checksum"] [ChecksumType: ChecksumType] [Mode: Mode] [Origin: Origin] URL: "URL"

where

Checksum:

String (0..128)

The checksum is used to ensure the integrity of the downloaded customization template. When using HTTP, it is mandatory to add a checksum. When using HTTPS, it is mandatory to add a checksum only if you are downloading the template from a server that presents an unsigned certificate, or a self-signed certificate that is not in the CA list of the device (not trusted).

ChecksumType:

SHA512

The algorithm that is used to calculate the checksum.

Default value: SHA512

Mode:

Add/Replace

If the mode is set to Add, all items listed in the uploaded file are added to the existing customization template. If the mode is set to Replace, the newer customization template that is uploaded, is compared against the previously uploaded template. Items that are not present in the newer file are removed. In both cases, items with the same name are overwritten.

Default value: Add

Origin:

Other/Provisioning

Specifies whether the customization template is used for provisioning or for another purpose. When the value is Provisioning, the configurations (xConfiguration) in the template are ignored, and the provisioning system (CUCM or TMS) can set configurations like they normally do. CUCM always acts as if this parameter is set to Provisioning. Note that some configurations may be specific to one device, and you may end up with devices that you cannot reach if you provision those configurations to more than one device.



Default value: Other

URL:

String (0..128)

The URL of the customization template.

Proximity commands

xCommand Proximity Services Activate

Requires user role: ADMIN, USER

Reactivate the Proximity services that were deactivated with xCommand Proximity Services Deactivate.

USAGE:

Proximity Services Activate

xCommand Proximity Services Deactivate

Requires user role: ADMIN, USER

This command deactivates all proximity services on the device. To reactivate proximity services use the command xCommand Proximity Services Activate.

USAGE:

Proximity Services Deactivate



RoomPreset commands

xCommand RoomPreset Activate

Requires user role: ADMIN, USER

Activate one of the locally stored presets.

Note that information about all video input sources, and pan, tilt, zoom and focus values for all cameras are included in the same preset. In contrast, the xCommand Camera Preset commands applies to individual cameras only.

USAGE:

RoomPreset Activate PresetId: PresetId

where

PresetId:

Integer (1..15)

The ID of the preset you want to activate.

xCommand RoomPreset Clear

Requires user role: ADMIN, USER

Delete a preset.

Note that information about all video input sources, and pan, tilt, zoom and focus values for all cameras are included in the same preset. In contrast, the xCommand Camera Preset commands applies to individual cameras only.

USAGE:

RoomPreset Clear PresetId: PresetId

where

PresetId:

Integer (1..15)

The ID of the preset you want to delete.

xCommand RoomPreset Store

Requires user role: ADMIN, USER

Store the connector selections for all video input sources and the current position (pan and tilt), zoom and focus values for all cameras.

Note that information about all video input sources, and pan, tilt, zoom and focus values for all cameras are included in the same preset. The device may hold 15 such predefined video input presets. These presets are available for far end control, i.e. they are referred in the PresetId parameter of the xCommand FarEndControl Preset Activate command. In contrast, the xCommand Camera Preset commands applies to individual cameras only. Those presets are not available for far end control.

USAGE:

RoomPreset Store [Description: "Description"] PresetId: PresetId Type: Type

where

Description:

String (0, 255)

Enter a description of the camera preset.

PresetId:

Integer (1..15)

The ID of this preset.

Type:

All/Camera

Not applicable. If you want to ensure that a preset only affects camera positions we recommend that you select Camera.



Security commands

xCommand Security Certificates CA Add

Requires user role: ADMIN

Uploads CA security certificates to this device. This is a multiline command.

USAGE:

```
Security Certificates CA Add
```

xCommand Security Certificates CA Delete

Requires user role: ADMIN

Deletes a CA security certificate from this device.

USAGE:

```
Security Certificates CA Delete Fingerprint: "Fingerprint"
```

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is deleted. You can get the fingerprint ID by running xCommand Security Certificates CA Show.

xCommand Security Certificates CA Show

Requires user role: ADMIN, USER

Shows the details for the CA security certificates on this device.

USAGE:

```
Security Certificates CA Show [Format: Format]
```

where

Format:

PEM/Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

Default value: Text

xCommand Security Certificates Services Activate

Requires user role: ADMIN

Activates a security certificate on this device.

USAGE:

```
Security Certificates Services Activate Fingerprint: "Fingerprint" Purpose: Purpose
```

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is activated. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

Purpose:

802.1X/HTTPS/Audit/SIP

The type of service which applies to this certificate.

xCommand Security Certificates Services Add

Requires user role: ADMIN

Uploads security certificates to this device. This is a multiline command.

USAGE:

```
Security Certificates Services Add [PrivateKeyPassword: "PrivateKeyPassword"]
```

where

PrivateKeyPassword:

String (0..128)

Stores the details of the private key for the password.

Default value: ""



xCommand Security Certificates Services Deactivate

Requires user role: ADMIN

Deactivates security certificates on this device.

USAGE:

Security Certificates Services Deactivate Fingerprint: "Fingerprint" Purpose:

Purpose

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is deactivated. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

Purpose:

802.1X/HTTPS/Audit/SIP

The type of service which applies to this certificate.

xCommand Security Certificates Services Delete

Requires user role: ADMIN

Deletes security certificates from this device.

USAGE:

Security Certificates Services Delete Fingerprint: "Fingerprint"

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is deleted. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

xCommand Security Certificates Services Show

Requires user role: ADMIN, USER

Shows details for security certificates on this device.

USAGE:

Security Certificates Services Show [Filter: Filter] [Format: Format]

where

Filter:

802.1X/HTTPS/Audit/SIP

Filters the results according to the chosen service.

Format:

PEM/Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

Default value: Text

xCommand Security Certificates ThirdParty Disable

Requires user role: ADMIN

Disables a bundled certificate used for SMTP and HttpClient.

Disabling a certificate results in a server providing a certificate signed with this root certificate will be declined.

USAGE:

Security Certificates ThirdParty Disable Fingerprint: "Fingerprint"

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is disabled. You can get the fingerprint ID by running xCommand Security Certificates Services Show.



xCommand Security Certificates ThirdParty Enable

Requires user role: ADMIN

Enables a bundled certificate used for SMTP and HttpClient.

USAGE:

Security Certificates ThirdParty Enable Fingerprint: "Fingerprint"

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate that is enabled. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

xCommand Security Certificates ThirdParty List

Requires user role: ADMIN

Lists all bundled certificates and their state.

USAGE:

Security Certificates ThirdParty List

xCommand Security Certificates ThirdParty Show

Requires user role: ADMIN

Shows a single third-party certificate.

USAGE:

Security Certificates ThirdParty Show Fingerprint: "Fingerprint" [Format: Format]

where

Fingerprint:

String (0..128)

The unique Identifier for the certificate you want to see. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

Format:

PEM/Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

Default value: Text



xCommand Security Certificates Webex Show

Requires user role: ADMIN, USER

This command applies only to devices that are registered to the Cisco Webex cloud service.

Shows the list of trusted CA certificates that verifies the certificates of servers and services used by the Cisco Webex cloud.

USAGE:

Security Certificates Webex Show [Filter: Filter] [Format: Format]

where

Filter:

Cisco/Non-Cisco/TLS-proxy

Cisco: Shows the list of CA certificates used when communicating with servers and services that are provided by Cisco.

Non-Cisco: Shows the list CA certificates used when communicating with servers and services that are provided by others than Cisco.

TLS-proxy: Shows the list of additional CA certificates required when using a TLS inspecting proxy for outbound traffic.

Format:

PEM/Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

Default value: Text

xCommand Security FIPSMode Activate

Requires user role: ADMIN

Activate FIPS (140-2) mode. Activating FIPS mode implies a reset to factory defaults.

While in FIPS mode, the following limitations apply: All calls are encrypted. Unencrypted communication protocols like Telnet and HTTP cannot be used. IEEE802.1x and SNMP are disabled. The remote support user is not available. Digest access authentication is not supported between the device and an HTTP Proxy, because Digest access authentication is using MD5 cryptographic hashing, which is not allowed in FIPS. This last limitation only affects Webex registered devices, since an HTTP Proxy is used only for the Webex solution.

To exit FIPS mode, perform a factory reset.

USAGE:

Security FIPSMode Activate Confirm: Confirm

where

Confirm:

Yes

Confirms setting the device in FIPS mode.



xCommand Security Persistency

Requires user role: ADMIN

Set the following features to persistent or non-persistent mode. In non-persistent mode the information gathered by the specified feature does not persist a reboot of the device. Persistent mode is the default. This command reboots the device.

USAGE:

Security Persistency Configurations: [Configurations](#) CallHistory: [CallHistory](#)
InternalLogging: [InternalLogging](#) LocalPhonebook: [LocalPhonebook](#) DHCP: [DHCP](#)
ConfirmAndReboot: [ConfirmAndReboot](#)

where

[Configurations](#):

NonPersistent/Persistent

In non-persistent mode, all configurations are set back to default when the device reboots.

[CallHistory](#):

NonPersistent/Persistent

In non-persistent mode call history is deleted when the device reboots.

[InternalLogging](#):

NonPersistent/Persistent

In non-persistent mode eventlog is deleted when the device reboots.

[LocalPhonebook](#):

NonPersistent/Persistent

In non-persistent mode local phone book is deleted when the device reboots.

[DHCP](#):

NonPersistent/Persistent

In non-persistent mode all IP related information is deleted when the device reboots.

[ConfirmAndReboot](#):

Yes

Reboots the device.

xCommand Security Session Get

Requires user role: ADMIN, AUDIT, INTEGRATOR, ROOMCONTROL, USER

Shows details of your current session.

USAGE:

Security Session Get

xCommand Security Session List

Requires user role: ADMIN

List active sessions.

USAGE:

Security Session List

xCommand Security Session Terminate

Requires user role: ADMIN

Terminate a session.

USAGE:

Security Session Terminate SessionId: "[SessionId](#)"

where

[SessionId](#):

String (0, 32)

The session ID number.



Standby commands

xCommand Standby Activate

Requires user role: ADMIN, INTEGRATOR, USER

Set the device in standby mode, which turns off the video outputs and put the camera into sleep mode.

USAGE:

Standby Activate

xCommand Standby Deactivate

Requires user role: ADMIN, INTEGRATOR, USER

Bring the device out of standby mode.

USAGE:

Standby Deactivate

xCommand Standby Halfwake

Requires user role: ADMIN, INTEGRATOR

Sets the device to "Halfwake" state. This state informs the user from the UI, to pick up a remote or to tap the touch device to get started.

USAGE:

Standby Halfwake

xCommand Standby ResetHalfwakeTimer

Requires user role: ADMIN, USER

Sets a temporary Halfwake timer delay. If the device is in Halfwake mode when the reset timer is set, the device is brought out of Halfwake mode. When left idle for the given delay the device goes into halfwake mode.

USAGE:

Standby ResetHalfwakeTimer Delay: Delay

where

Delay:

Integer (1..480)

Set the delay in minutes.

xCommand Standby ResetTimer

Requires user role: ADMIN, USER

Reset the standby delay timer or set a temporary standby delay. If the device is in standby mode when the timer is set, the device is brought out of standby mode before starting the countdown.

If you don't specify a Delay, the standby delay timer is reset, and the device goes into standby after the period that is given by the Standby Delay setting (xConfiguration Standby Delay). If you do specify a Delay, the device goes into standby when it has been idle for the specified period. Next time, the standby delay is as configured in the Standby Delay setting again.

USAGE:

Standby ResetTimer [Delay: Delay]

where

Delay:

Integer (1..480)

Set the delay in minutes.



SystemUnit commands

xCommand SystemUnit Boot

Requires user role: ADMIN, INTEGRATOR, USER

Reboot the device.

USAGE:

`SystemUnit Boot [Action: Action]`

where

Action:

Restart/Shutdown

As a default the device restarts after a reboot. By selecting Shutdown, the device will not restart.

Default value: Restart

xCommand SystemUnit FactoryReset

Requires user role: ADMIN, USER

Reset the codec to factory default settings. The call logs are deleted and all device parameters are reset to default values. All files that have been uploaded to the codec are deleted. Option key(s) are not affected. Use the parameter Keep in order to choose which configurations and files to keep when you factory reset the device.

As a default the device restarts after the factory reset, but other behaviors can be forced by selecting a different TrailingAction.

USAGE:

`SystemUnit FactoryReset Confirm: Confirm [Keep: Keep] [TrailingAction: TrailingAction]`

where

Confirm:

Yes

Include to confirm your choice.

Keep:

Certificates/HTTP/LocalSetup/Network/Provisioning/SerialPort/Webex

Select which configurations and files to keep when you factory reset the device. You can have up to 7 CallId parameters in the same command.

Certificates:

Client and CA certificates.

HTTP:

xConfiguration NetworkServices HTTP Mode

xConfiguration NetworkServices HTTPS Server MinimumTLSVersion

xConfiguration NetworkServices HTTPS StrictTransportSecurity

xConfiguration NetworkServices HTTPS VerifyClientCertificate

xConfiguration NetworkServices HTTPS VerifyServerCertificate

LocalSetup:

xConfiguration Audio DefaultVolume

xConfiguration Audio SoundsAndAlerts RingVolume

xConfiguration Time Zone

xConfiguration UserInterface Language

xConfiguration Video Output Connector OverscanLevel

xCommand Camera Preset Store

Network:

xConfiguration Network 1



xConfiguration NetworkServices Wifi Allowed
xConfiguration NetworkServices Wifi Enabled

Provisioning:

xConfiguration Provisioning Mode

SerialPort:

xConfiguration SerialPort Mode
xConfiguration SerialPort BaudRate
xConfiguration SerialPort LoginRequired

Spark:

xConfiguration Spark ServiceOverrides GdsBaseUrl
xConfiguration Spark ServiceOverrides U2CBaseUrl
xConfiguration Spark ServiceOverrides WdmBaseUrl

TrailingAction:

NoAction/Restart/Shutdown

Select Shutdown or NoAction to override the default behavior (Restart).

Default value: Restart

xCommand SystemUnit FirstTimeWizard Stop

Requires user role: ADMIN, INTEGRATOR, USER

Stops the wizard which appears the first time you start the device, so the device can be set up without it. The wizard only appears again if the device is reset to its factory default settings.

USAGE:

```
SystemUnit FirstTimeWizard Stop
```

xCommand SystemUnit Notifications RemoveAll

Requires user role: ADMIN

Clears the list of system notifications that are reported by xStatus SystemUnit Notifications Text/Type.

USAGE:

```
SystemUnit Notifications RemoveAll
```

xCommand SystemUnit OptionKey Add

Requires user role: ADMIN

Add an option key to support additional features.

USAGE:

```
SystemUnit OptionKey Add Key: "Key"
```

where

Key:

String (16, 24)

The key you have received for the option you wish to switch on.

xCommand SystemUnit OptionKey List

Requires user role: ADMIN

List all option keys.

USAGE:

```
SystemUnit OptionKey List
```

xCommand SystemUnit OptionKey Remove

Requires user role: ADMIN

Remove a specified option key.

USAGE:

```
SystemUnit OptionKey Remove Type: Type
```

where

Type:

Encryption/MultiSite/RemoteMonitoring

**xCommand SystemUnit OptionKey RemoveAll**

Requires user role: ADMIN

Remove all option keys.

USAGE:

```
SystemUnit OptionKey RemoveAll Confirm: Confirm
```

where

Confirm:

Yes

xCommand SystemUnit SignInBanner Clear

Requires user role: ADMIN

Clear the sign in banner set with xCommand SystemUnit SignInBanner Set.

USAGE:

```
SystemUnit SignInBanner Clear
```

xCommand SystemUnit SignInBanner Get

Requires user role: ADMIN, USER

Get the custom message set with xCommand SystemUnit SignInBanner Set.

USAGE:

```
SystemUnit SignInBanner Get
```

xCommand SystemUnit SignInBanner Set

Requires user role: ADMIN

Set a sign in banner with a custom message on the device's user interface. This is a multiline command.

Use:

```
xCommand SystemUnit SignInBanner Set <enter>
Banner text <enter>
. <enter>
```

USAGE:

```
SystemUnit SignInBanner Set
```

xCommand SystemUnit SoftReset

Requires user role: ADMIN, USER

Reset most parameters to their default values. This does not include parameters associated with room setup, such as camera position, language, and volume.

USAGE:

```
SystemUnit SoftReset Confirm: Confirm
```

where

Confirm:

Yes



xCommand SystemUnit SoftwareUpgrade

Requires user role: ADMIN

Initiate a software upgrade by fetching the software from a given URL.

USAGE:

```
SystemUnit SoftwareUpgrade URL: "URL" [Forced: Forced]
```

where

URL:

String (0, 255)

The URL to the software package location.

Forced:

False/True

You can force a device to accept a software upgrade immediately, without giving users a chance to acknowledge or postpone the update.

Default value: True

xCommand SystemUnit WelcomeBanner Clear

Requires user role: ADMIN

Clear the welcome banner set with xCommand SystemUnit WelcomeBanner Set.

USAGE:

```
SystemUnit WelcomeBanner Clear
```

xCommand SystemUnit WelcomeBanner Get

Requires user role: ADMIN, AUDIT, INTEGRATOR, ROOMCONTROL, USER

Get the custom message set with xCommand SystemUnit WelcomeBanner Set.

USAGE:

```
SystemUnit WelcomeBanner Get
```

xCommand SystemUnit WelcomeBanner Set

Requires user role: ADMIN

Set up a welcome banner that the user sees after they sign in to the device's web interface or the command line interface. The banner can for example contain information that the user needs to get started or things they need to be aware of when changing settings. This is a multi-line command.

Use:

```
xCommand SystemUnit WelcomeBanner Set <enter>
```

Banner text <enter>

. <enter>

USAGE:

```
SystemUnit WelcomeBanner Set
```



Time commands

xCommand Time DateTime Get

Requires user role: ADMIN, USER

Read the time and date from the device.

USAGE:

```
Time DateTime Get
```

xCommand Time DateTime Set

Requires user role: ADMIN, USER

Set the date and time for the device, if not available from NTP (Network Time Protocol).

USAGE:

```
Time DateTime Set [Year: Year] [Month: Month] [Day: Day] [Hour: Hour] [Minute: Minute] [Second: Second]
```

where

Year:

Integer (2015..2037)

Month:

Integer (1..12)

Day:

Integer (1..31)

Hour:

Integer (0..23)

Minute:

Integer (0..59)

Second:

Integer (0..59)

UserInterface commands

xCommand UserInterface Branding Clear

Requires user role: ADMIN, INTEGRATOR

Deletes the custom wallpaper, the brand background image, and the logo files from the device.

USAGE:

```
UserInterface Branding Clear
```

xCommand UserInterface Branding Delete

Requires user role: ADMIN, INTEGRATOR, USER

Deletes the image file, which is specified in the Type parameter, from the device.

USAGE:

```
UserInterface Branding Delete Type: Type
```

where

Type:

Branding/HalfwakeBackground/HalfwakeBranding

Background: Delete the custom wallpaper.

Branding: Delete the logo that is displayed when the device is active.

HalfwakeBackground: Delete the brand image that is displayed as a background when the device is in the halfwake state.

HalfwakeBranding: Delete the logo that is displayed when the device is in the halfwake state.



xCommand UserInterface Branding Fetch

Requires user role: ADMIN, INTEGRATOR, USER

Fetches an image file from a URL and stores the file on the device. The following image formats are supported: BMP, GIF, JPEG, and PNG. The maximum image size is 16 megapixels, and the maximum file size is 4 MByte.

The Type parameter determines what kind of image it is. If it is a background image, the associated feature (Custom wallpaper or Branding with background and logo) is automatically applied.

This command issues an HTTP request, so it is included in the HTTP requests count. The maximum number of concurrent requests is limited.

USAGE:

```
UserInterface Branding Fetch [Checksum: "Checksum"] [ChecksumType: ChecksumType]  
Type: Type URL: "URL"
```

where

Checksum:

String (0, 128)

The checksum is used to ensure the integrity of the downloaded image file. When using HTTP, it is mandatory to add a checksum. When using HTTPS, it is mandatory to add a checksum only if you are downloading the template from a server that presents an unsigned certificate, or a self-signed certificate that is not in the CA list of the device (not trusted).

ChecksumType:

SHA512

The algorithm that is used to calculate the checksum.

Default value: SHA512

Type:

Branding/HalfwakeBackground/HalfwakeBranding

Background: Fetches a background image that can be used as custom wallpaper.

Branding: Fetches a logo that can be displayed when the device is active.

HalfwakeBackground: Fetches a brand image that can be displayed as a background when the device is in the halfwake state.

HalfwakeBranding: Fetches a logo that can be displayed when the device is in the halfwake state.

URL:

String (5, 250)

The URL of the image file.

xCommand UserInterface Branding Get

Requires user role: ADMIN, INTEGRATOR, USER

The command returns the image file that is specified in the Type parameter, given that such a file is stored on the device. The file is Base64 encoded. The format is JPG for background images and PNG for logos, regardless of the format of the originally uploaded file.

Background images are stored in three sizes, one for the main screen, one for the Touch controller, and one for the web interface illustrations. Use the Size parameter to choose which one to get. Logos have only one size.

USAGE:

```
UserInterface Branding Get [Size: Size] Type: Type
```

where

Size:

Large/Small/Thumbnail

Large: The size of the image that is displayed on the main screen.

Small: The size of the image that is displayed on the Touch controller.

Thumbnail: The size of the image that is used in the web interface illustrations.

Default value: Large

Type:

Branding/HalfwakeBackground/HalfwakeBranding

Background: Return the custom wallpaper.

Branding: Return the logo that is displayed when the device is active.

HalfwakeBackground: Return the brand image that is displayed as a background when the device is in the halfwake state.

HalfwakeBranding: Return the logo that is displayed when the device is in the halfwake state.



xCommand UserInterface Branding Updated

Requires user role: ADMIN, INTEGRATOR, USER

This command creates an event that tells that a new image file is uploaded to the device and ready for use. The Type parameter identifies what kind of image it is.

USAGE:

UserInterface Branding Updated Type: Type

where

Type:

Branding/HalfwakeBackground/HalfwakeBranding

Background: A new background image that can be used as a custom wallpaper is ready for use.

Branding: A new logo that can be displayed when the device is active is ready for use.

HalfwakeBackground: A new brand image that can be displayed as a background when the device is in the halfwake state is ready for use.

HalfwakeBranding: A new logo that can be displayed when the device is in the halfwake state is ready for use.

xCommand UserInterface Branding Upload

Requires user role: ADMIN, INTEGRATOR, USER

Uploads an image file to the device. The following image formats are supported: BMP, GIF, JPEG, and PNG, and the maximum image size is 16 megapixels. The file must be Base64 encoded, and the maximum file size is 4 MByte.

The Type parameter determines what kind of image it is. If it is a background image, the associated feature (Custom wallpaper or Branding with background and logo) is automatically applied. This is a multiline command.

USAGE:

UserInterface Branding Upload Type: Type

where

Type:

Branding/HalfwakeBackground/HalfwakeBranding

Background: Uploads a background image that can be used as custom wallpaper.

Branding: Uploads a logo that can be displayed when the device is active.

HalfwakeBackground: Uploads a brand image that can be displayed as a background when the device is in the halfwake state.

HalfwakeBranding: Uploads a logo that can be displayed when the device is in the halfwake state.

xCommand UserInterface Extensions Clear

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Delete user interface extensions (web apps, custom buttons, panels, and widgets) from the device. If you don't specify an ActivityType, all extensions are deleted.

USAGE:

UserInterface Extensions Clear [ActivityType: ActivityType]

where

ActivityType:

Custom/WebApp

Custom: Custom buttons, panels, and widgets are removed. Web apps are not affected.

WebApp: Web apps are removed. Custom buttons, panels, and widgets are not affected.



xCommand UserInterface Extensions List

Requires user role: INTEGRATOR, ROOMCONTROL, USER

List user interface extensions (web apps, custom buttons, panels, and widgets) that exist on the device. If you don't specify an ActivityType, all extensions are listed.

USAGE:

```
UserInterface Extensions List [ActivityType: ActivityType]
```

where

ActivityType:

Custom/WebApp

Custom: Custom buttons, panels, and widgets are listed. Web apps are not included.

WebApp: Web apps are listed. Custom buttons, panels, and widgets are not included.

xCommand UserInterface Extensions Panel Clicked

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Creates an event when the user clicks an in-room control panel.

USAGE:

```
UserInterface Extensions Panel Clicked PanelId: "PanelId"
```

where

PanelId:

String (0..255)

The unique identifier of the in-room control panel.

xCommand UserInterface Extensions Panel Close

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Closes an opened in-room control panel.

USAGE:

```
UserInterface Extensions Panel Close
```

xCommand UserInterface Extensions Panel Open

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Opens the in-room control panel that has the given PanelId. If the panel has multiple pages you can specify which page to open by including the PageId parameter.

USAGE:

```
UserInterface Extensions Panel Open PanelId: "PanelId" [PageId: "PageId"]
```

where

PanelId:

String (0..255)

The unique identifier of the in-room control panel.

PageId:

String (0..255)

The unique identifier of a page on an in-room control panel.

xCommand UserInterface Extensions Panel Remove

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Removes the in-room control panel from the user interface of this device.

USAGE:

```
UserInterface Extensions Panel Remove PanelId: "PanelId"
```

where

PanelId:

String (0..255)

The unique identifier of the in-room control panel.



xCommand UserInterface Extensions Panel Save

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Adds an in-room control panel to the current configuration. The panel will be added to the configuration, but if a panel with the same panel ID already exists, it will be overwritten. This is a multiline command.

USAGE:

```
UserInterface Extensions Panel Save PanelId: "PanelId"
```

where

PanelId:

String (0..255)

The unique identifier of the in-room control panel.

xCommand UserInterface Extensions Panel Update

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Update the name of the in-room control panel that has the given PanelId. This is the name that you see just below the button on the user interface.

USAGE:

```
UserInterface Extensions Panel Update PanelId: "PanelId" Name: "Name"
```

where

PanelId:

String (0..255)

The unique identifier of the in-room control panel.

Name:

String (0..255)

The new name of the in-room control panel.

xCommand UserInterface Extensions Set

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Set the configuration scheme you have chosen in the user interface extensions (widgets) for your device. Updates the UserInterface Extensions status tree. This is a multiline command.

USAGE:

```
UserInterface Extensions Set ConfigId: "ConfigId"
```

where

ConfigId:

String (0..40)

The unique identifier for the configuration.

xCommand UserInterface Extensions Widget Action

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Sets the action of the given widget. Updates the UserInterface Extensions status tree.

USAGE:

```
UserInterface Extensions Widget Action [Type: "Type"] [Value: "Value"] WidgetId: "WidgetId"
```

where

Type:

String (0..255)

The type of widget that is set.

Value:

String (0..255)

The value of the widget. The range of values depends on the widget type.

WidgetId:

String (0..255)

The unique identifier for the widget.



xCommand UserInterface Extensions Widget SetValue

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Set the value of the given widget. Updates the UserInterface Extensions status tree. Returns an error if the value is out of range.

USAGE:

```
UserInterface Extensions Widget SetValue Value: "Value" WidgetId: "WidgetId"
```

where

Value:

String (0, 255)

The value of the widget. The range of values depends on the widget type.

WidgetId:

String (0, 255)

The unique identifier for the widget.

xCommand UserInterface Extensions Widget UnsetValue

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Empties the value of the given widget. Updates the UserInterface Extensions status tree and notifies the user interface that this widget is no longer selected.

USAGE:

```
UserInterface Extensions Widget UnsetValue WidgetId: "WidgetId"
```

where

WidgetId:

String (0, 255)

The unique identifier for the widget.

xCommand UserInterface Message Alert Clear

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Remove the message which was displayed using the UserInterface Message Alert Display command. This is required when the Duration parameter is not set.

USAGE:

```
UserInterface Message Alert Clear
```

xCommand UserInterface Message Alert Display

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Display a message on screen. Optionally you can keep the message for a specified duration of time. If Duration is not set, the command must be followed by a UserInterface Message Alert Clear command.

USAGE:

```
UserInterface Message Alert Display [Title: "Title"] Text: "Text" [Duration: Duration]
```

where

Title:

String (0, 255)

The title of the message.

Default value: ""

Text:

String (0, 255)

The message to be displayed. The <p> and
 HTML tags will result in line breaks as normal; any other tags will appear as plain text.

Duration:

Integer (0..3600)

How long (in seconds) the message is to be displayed on the screen. If set to 0 (zero) the message is displayed until a UserInterface Message Alert Clear command is sent.

Default value: 0



xCommand UserInterface Message Prompt Clear

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Remove the window which was displayed using the UserInterface Message Prompt Display command. This is required when the Duration parameter is not set.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

```
UserInterface Message Prompt Clear [FeedbackId: "FeedbackId"]
```

where

FeedbackId:

String (0, 255)

The FeedbackId corresponds to the FeedbackId given by the UserInterface Message Prompt Display command.

Default value: ""

xCommand UserInterface Message Prompt Display

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Display a small window on screen with a title, text and up to five options for response from the user. The message is displayed on screen until the user gives a response, or until the device receives a UserInterface Message Prompt Clear command.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

```
UserInterface Message Prompt Display [Title: "Title" Text: "Text" [FeedbackId: "FeedbackId"] [Duration: Duration] [Option.1: "Option.1"] [Option.2: "Option.2"] [Option.3: "Option.3"] [Option.4: "Option.4"] [Option.5: "Option.5"]]
```

where

Title:

String (0, 255)

The title of the message.

Text:

String (0, 255)

Enter the text line to be displayed. The <p> and
 HTML tags will result in line breaks as normal; any other tags will appear as plain text.

FeedbackId:

String (0, 255)

To identify the feedback enter a FeedbackId.

Duration:

Integer (0, 3600)

How long (in seconds) the message window is to be displayed on the screen. If set to 0 (zero) the message window is displayed until a UserInterface Message Prompt Clear command is sent.

Default value: 0

Option.1:

String (0, 255)

The text to appear on feedback option 1.

Option.2:

String (0, 255)

The text to appear on feedback option 2.

Option.3:



String (0, 255)

The text to appear on feedback option 3.

option.4:

String (0, 255)

The text to appear on feedback option 4.

option.5:

String (0, 255)

The text to appear on feedback option 5.

xCommand UserInterface Message Prompt Response

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Give a response to the UserInterface Message Prompt Display command. This command is executed when the user selects an option in the user interface.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

UserInterface Message Prompt Response [FeedbackId: "FeedbackId"] OptionId:

OptionId

where

FeedbackId:

String (0, 255)

The FeedbackId corresponds to the FeedbackId given by the UserInterface Message Prompt Display command.

Default value: ""

OptionId:

Integer (1..5)

The OptionId corresponds to the OptionIds given as possible responses in the UserInterface Message Prompt Display command.

xCommand UserInterface Message TextInput Clear

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Remove the text input message which was displayed using the UserInterface Message TextInput Display command. This is required when the Duration parameter is not set.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

UserInterface Message TextInput Clear [FeedbackId: "FeedbackId"]

where

FeedbackId:

String (0, 255)

The FeedbackId corresponds to the FeedbackId given by the UserInterface Message TextInput Display command.

Default value: ""



xCommand UserInterface Message TextInput Display

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Displays an input dialog box to which a user can respond. This is only supported for devices with a touch-based user interface. The message is displayed on screen until the user gives a response, or until the device receives a UserInterface Message TextInput Clear command.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

```
UserInterface Message TextInput Display [Duration: Duration] [FeedbackId: "FeedbackId"] [InputText: "InputText"] [InputType: InputType] [KeyboardState: KeyboardState] [Placeholder: "Placeholder"] [SubmitText: "SubmitText"] Text: "Text" [Title: "Title"]
```

where

Duration:

Integer (0..3600)

How long (in seconds) the message is to be displayed on the screen. If set to 0 (zero) the message is displayed until a UserInterface Message TextInput Clear command is sent.

Default value: 0

FeedbackId:

String (0..255)

To identify the feedback enter a FeedbackId.

InputText:

String (0..255)

Text that is pre-populated in the text input field when the dialog box opens. Before submitting the response, you can edit this text, or delete it and enter your own text.

If this parameter is not included, the content of the Placeholder parameter is shown in the text input field when the dialog box opens.

Default value: ""

InputType:

SingleLine/Numeric/Password/PIN

The type of text input dialog box that is displayed. This also determines the keyboard layout that it displayed.

Default value: SingleLine

KeyboardState:

Open/Closed

Specifies if the device's keyboard should open when the text input message displays.

Default value: Open

Placeholder:

String (0..255)

Placeholder text that is displayed in the text input field until you start typing. If the InputText parameter is included, the Placeholder parameter has no effect.

Default value: ""

SubmitText:

String (0..32)

The text that is shown on the Submit button.

Default value: "OK"

Text:

String (0..128)

The message that is to be displayed to the user. The <p> and
 HTML tags will result in line breaks as normal; any other tags will appear as plain text.

Title:

String (0..40)

The title of the input dialog box.

Default value: ""



xCommand UserInterface Message TextInput Response

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Give a response to the UserInterface Message TextInput Display command. This command is executed when the user submits the reply that he has entered in the text input field in the user interface.

Use the xFeedback commands to monitor the feedback from the user. Read more about the xFeedback commands in the API introduction section in this guide.

USAGE:

```
UserInterface Message TextInput Response [FeedbackId: "FeedbackId"] Text: "Text"
```

where

FeedbackId:

String (0, 255)

To identify the feedback enter a FeedbackId.

Text:

String (0, 255)

The message that is to be displayed to the user.

xCommand UserInterface Message TextLine Clear

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Remove the text line which was displayed by the UserInterface Message TextLine Display command. This is required when the Duration parameter is not set.

USAGE:

```
UserInterface Message TextLine Clear
```

xCommand UserInterface Message TextLine Display

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL

Display a text line on screen. Optionally you can place the text line at a specified location and for a specified duration of time. If Duration is not set, the command must be followed by the UserInterface Message TextLine Clear command.

USAGE:

```
UserInterface Message TextLine Display Text: "Text" [X: X] [Y: Y] [Duration: Duration]
```

where

Text:

String (0, 140)

The text line to be displayed. The <p> and
 HTML tags will result in line breaks as normal; any other tags will appear as plain text.

X:

Integer (1..10000)

Enter the X-coordinate (horizontal) on screen. X=0 is in the upper left corner.

Default value: 0

Y:

Integer (1..10000)

Enter the Y-coordinate (vertical) on screen. Y=0 is in the upper left corner.

Default value: 0

Duration:

Integer (0..3600)

How long (in seconds) the text line is to be displayed on the screen. If set to 0 (zero) the text line is displayed until a UserInterface Message TextLine Clear command is sent.

Default value: 0

xCommand UserInterface WebView Clear

Requires user role: ADMIN, INTEGRATOR, USER

Closes the current web view.

USAGE:

```
UserInterface WebView Clear
```



xCommand UserInterface WebView Display

Requires user role: ADMIN, INTEGRATOR, USER

Opens the web view and displays the web page given by the URL.

USAGE:

```
UserInterface WebView Display [Options: "Options"] [Title: "Title"] Url: "Url"
```

where

Options:

String (0, 255)

This value is intended for internal use by the UI Extensions Editor.

Title:

String (0, 255)

The title of the web page.

Url:

String (0, 2000)

The URL of the web page.

UserManagement commands

xCommand UserManagement RemoteSupportUser Create

Requires user role: ADMIN

Create a remote support user passphrase that Technical Assistance Center (TAC) can use to access the device for troubleshooting.

USAGE:

```
UserManagement RemoteSupportUser Create [ExpiryDays: ExpiryDays]
```

where

ExpiryDays:

Integer (1..31)

Define the duration for the passphrase validity. Default is 7 days.

xCommand UserManagement RemoteSupportUser Delete

Requires user role: ADMIN

Delete the remote support user created with the command xCommand UserManagement RemoteSupportUser Create.

USAGE:

```
UserManagement RemoteSupportUser Delete
```

xCommand UserManagement RemoteSupportUser DisablePermanently

Requires user role: ADMIN

Disable the creation of new remote support users. To enable the remote support user again you must factory reset your device.

USAGE:

```
UserManagement RemoteSupportUser DisablePermanently Confirm: Confirm
```

where

Confirm:

Yes



xCommand UserManagement RemoteSupportUser GetState

Requires user role: ADMIN

Retrieves the state of the generated remote support user, if one exists.

USAGE:

```
UserManagement RemoteSupportUser GetState
```

xCommand UserManagement User Add

Requires user role: ADMIN

Adds a new user to this device.

USAGE:

```
UserManagement User Add [Active: Active] [ClientCertificateDN:  
"ClientCertificateDN"] Passphrase: "Passphrase" [PassphraseChangeRequired:  
PassphraseChangeRequired] [PinChangeRequired: PinChangeRequired] [Role: Role]  
[ShellLogin: ShellLogin] Username: "Username" [YourPassphrase: "YourPassphrase"]
```

where

Active:

False/True

Specifies whether this is an active user or not.

ClientCertificateDN:

String (0..255)

Identifies a user who logs in with a client certificate instead of a username and password.

Passphrase:

String (0..255)

Specifies a Passphrase for the user.

PassphraseChangeRequired:

False/True

Specifies whether the user's passphrase requires changing or not.

PinChangeRequired:

False/True

Specifies whether a user's PIN requires changing or not.

Role:

Admin/Audit/Integrator/RoomControl/User

Sets the user's role.

ShellLogin:

False/True

Specifies whether the user should have a shell login or not.

Username:

String (0..127)

Specifies the user's username.

YourPassphrase:



String (0..255)

The user's passphrase.

xCommand UserManagement User Delete

Requires user role: ADMIN

Deletes a user from this device.

USAGE:

```
UserManagement User Delete Username: "Username" [YourPassphrase:  
"YourPassphrase"]
```

where

Username:

String (0..127)

Specifies the username of the user that is deleted.

YourPassphrase:

String (0..255)

The passphrase of the user that is deleted.

xCommand UserManagement User Get

Requires user role: ADMIN

Shows the details of users on this device.

USAGE:

```
UserManagement User Get [ClientCertificateDN: "ClientCertificateDN"] [Username:  
"Username"]
```

where

ClientCertificateDN:

String (0..255)

Identifies a user who logs in with a client certificate instead of a username and password.

Username:

String (0..127)

Specify a username to show the details of a particular user.

xCommand UserManagement User List

Requires user role: ADMIN

Shows the list of users on this device.

USAGE:

```
UserManagement User List [Limit: Limit] [Offset: Offset]
```

where

Limit:

Integer (0..65536)

Limits the number of results that are shown.

Default value: 0

Offset:

Integer (0..65536)

Shows lines with the same or higher Offset than the one provided.

Default value: 0



xCommand UserManagement User Modify

Requires user role: ADMIN

Modifies the details of a particular user.

USAGE:

```
UserManagement User Modify [Active: Active] [AddRole: AddRole]  
[ClientCertificateDN: "ClientCertificateDN"] [PassphraseChangeRequired:  
PassphraseChangeRequired] [PinChangeRequired: PinChangeRequired] [RemoveRole:  
RemoveRole] [ShellLogin: ShellLogin] Username: "Username" [YourPassphrase:  
"YourPassphrase"]
```

where

Active:

False/True

Specifies whether this is an active user or not.

AddRole:

Admin/Audit/Integrator/RoomControl/User

Adds a new role for the specified user.

ClientCertificateDN:

String (0..255)

Identifies a user who logs in with a client certificate instead of a username and password.

PassphraseChangeRequired:

False/True

Specifies whether the user's passphrase requires changing or not.

PinChangeRequired:

False/True

Specifies whether a user's PIN requires changing or not.

RemoveRole:

Admin/Audit/Integrator/RoomControl/User

Removes a role from the specified user.

ShellLogin:

False/True

Specifies whether the user should have a shell login or not.

Username:

String (0..127)

Specifies the user's username.

YourPassphrase:

String (0..255)

The user's passphrase.

xCommand UserManagement User Passphrase Change

Requires user role: ADMIN, AUDIT, INTEGRATOR, ROOMCONTROL, USER

Change the passphrase for the user you logged in as. If you are logged in as the administrator, this will change the administrator passphrase.

USAGE:

```
UserManagement User Passphrase Change NewPassphrase: "NewPassphrase"  
OldPassphrase: "OldPassphrase"
```

where

NewPassphrase:

String (0, 255)

OldPassphrase:

String (0, 255)

xCommand UserManagement User Passphrase Set

Requires user role: ADMIN

Set a user passphrase for the specified user. You must be logged in as an administrator to set a user passphrase.

USAGE:

```
UserManagement User Passphrase Set NewPassphrase: "NewPassphrase" Username:  
"Username" [YourPassphrase: "YourPassphrase"]
```

where

NewPassphrase:

String (0, 255)

Username:

String (0, 127)

YourPassphrase:

String (0, 255)



xCommand UserManagement User Unblock

Requires user role: ADMIN

Unblocks a user who is blocked out because of too many failed login attempts.

USAGE:

```
UserManagement User Unblock Username: "Username" [YourPassphrase:  
"YourPassphrase"]
```

where

Username:

String (0, 127)

YourPassphrase:

String (0, 255)

Video commands

xCommand Video ActiveSpeakerPIP Set

Requires user role: ADMIN, USER

Sets position for the active speakers PiP (picture in picture).

USAGE:

```
Video ActiveSpeakerPIP Set Position: Position
```

where

Position:

CenterLeft/CenterRight/LowerLeft/LowerRight/UpperCenter/UpperLeft/UpperRight

Select one of the predefined positions.



xCommand Video CEC Input KeyClick

Requires user role: ADMIN, INTEGRATOR

Mimics a remote control key click event from the input device.

USAGE:

Video CEC Input KeyClick ConnectorId: ConnectorId [Key: Key] [LogicalAddress: LogicalAddress] [NamedKey: NamedKey]

where

ConnectorId:

Integer (2..2)

The unique identifier of the connector.

Key:

Integer (0..255)

The CEC specified key code for the key that is sent to the logical address of the device as if it was pushed on a remote control.

LogicalAddress:

Integer (0..15)

The logical address of the connected device.

NamedKey:

Up/Down/Right/Left/Ok/Back/Stop/Play

The name of the key that is sent to the logical address of the device as if it was pushed on a remote control.

xCommand Video Input MainVideo Mute

Requires user role: ADMIN, INTEGRATOR, USER

Stop sending video from the device. Selfview is also turned off. This command does not affect the presentation channel.

USAGE:

Video Input MainVideo Mute

xCommand Video Input MainVideo Unmute

Requires user role: ADMIN, INTEGRATOR, USER

Start sending video from the device if previously turned off using the Video Input MainVideo Mute command (or, if available, the "Turn off video" button on the user interface). Selfview is also available.

USAGE:

Video Input MainVideo Unmute

xCommand Video Layout LayoutFamily Set

Requires user role: ADMIN, USER

Select the screen layout mode.

USAGE:

Video Layout LayoutFamily Set [Target: Target] LayoutFamily: LayoutFamily [CustomLayoutName: "CustomLayoutName"]

where

Target:

Local/Remote

Select if the target is the local layout or the remote layout.

LayoutFamily:

auto/custom/equal/overlay/prominent/single

Select a layout family.

CustomLayoutName:

String (1, 128)

Enter a name for the layout.



xCommand Video Output Monitor Backlight Set

Requires user role: ADMIN

Adjust the monitor backlight.

USAGE:

Video Output Monitor Backlight Set Value: Value

where

Value:

Integer (0..100)

Select the level.

xCommand Video Output Monitor Reset

Requires user role: ADMIN

Reset monitor settings.

USAGE:

Video Output Monitor Reset

xCommand Video PresentationPIP Set

Requires user role: ADMIN, USER

Sets position for the presentation PiP (picture in picture).

USAGE:

Video PresentationPIP Set Position: Position

where

Position:

CenterLeft/CenterRight/LowerLeft/LowerRight/UpperCenter/UpperLeft/UpperRight

Select one of the predefined positions.

xCommand Video PresentationView Set

Requires user role: ADMIN, USER

Set the presentation view mode

USAGE:

Video PresentationView Set View: View

where

View:

Default/Maximized/Minimized

Select Default when you want the presentation to be viewed with the default settings for the codec. Select Maximized when you want the presentation to be displayed in full screen. Select

Minimized when you want the presentation to be displayed in a small picture on screen.



xCommand Video Selfview Set

Requires user role: ADMIN, USER

Sets self-view on/off and specifies its size and position. If the parameter is not specified, current value is used.

USAGE:

```
Video Selfview Set [Mode: Mode] [FullscreenMode: FullscreenMode] [PIPPosition: PIPPosition] [OnMonitorRole: OnMonitorRole]
```

where

Mode:

On/Off

Selfview is set to on or off.

FullscreenMode:

On/Off

Choose between displaying the self-view in full screen or as picture-in-picture.

PIPPosition:

CenterLeft/CenterRight/LowerLeft/LowerRight/UpperCenter/UpperLeft/UpperRight

Select the position for the self-view image.

OnMonitorRole:

First/Second/Third

Displays self-view on monitors with this role.

WebEngine commands

xCommand UserInterface WebEngine DeleteStorage

Requires user role: ADMIN

Deletes session data for web view types, such as digital signage and web apps.

USAGE:

```
UserInterface WebEngine DeleteStorage [Type: Type]
```

where

Type:

All/Signage/WebApps

All: Deletes the session data for all web view types.

Signage: Deletes the session data related to digital signage.

WebApps: Deletes the session data related to all web views except digital signage.

Default value: All



Webex commands

xCommand Webex Registration Cancel

Requires user role: ADMIN, USER

Cancel device registration to Cisco Webex. This command only works in the short period after the registration is started with xCommand Webex Registration Start.

USAGE:

Webex Registration Cancel

xCommand Webex Registration Start

Requires user role: ADMIN, USER

Start registering a device to Cisco Webex by entering the activation code that has been created in Control Hub and choosing whether to keep local users and integrations. You get a confirmation that the registration has been successful or failed.

USAGE:

Webex Registration Start ActivationCode: ActivationCode SecurityAction:
SecurityAction

where

ActivationCode:

String: 16, 19

The activation code that has been created in Control Hub for this device.

SecurityAction:

Harden/NoAction

Harden: Deactivates all local users that have been created for this device and deactivates Macros.

NoAction: Doesn't remove any configurations. Use NoAction if you wish to keep existing integrations.



Chapter 5

xStatus commands



Description of the xStatus commands

In this chapter, you can find all of the xStatus commands and the responses. Status type commands return information about the system and system processes. You can query all information or just some of it.

We recommend you visit our web site regularly for updated versions of the manual.

Go to: ▶ <https://www.cisco.com/go/telepresence/docs>

Audio status.....	186	xStatus Call [n] CallbackNumber	191
xStatus Audio Input Connectors ARC [n] EcReferenceDelay.....	186	xStatus Call [n] CallType	191
xStatus Audio Input Connectors HDMI [n] EcReferenceDelay	186	xStatus Call [n] DeviceType	191
xStatus Audio Input Connectors HDMI [n] Mute.....	186	xStatus Call [n] Direction	191
xStatus Audio Input Connectors Line [n] Mute	186	xStatus Call [n] DisplayName.....	191
xStatus Audio Input Connectors Microphone [n] ConnectionStatus.....	186	xStatus Call [n] Duration	192
xStatus Audio Input Connectors Microphone [n] EcReferenceDelay.....	187	xStatus Call [n] Encryption Type	192
xStatus Audio Input Connectors Microphone [n] Mute	187	xStatus Call [n] FacilityServiceId	192
xStatus Audio Input Connectors KeyClick Attenuate.....	187	xStatus Call [n] HoldReason	192
xStatus Audio Input Connectors KeyClick Detected.....	187	xStatus Call [n] Ice	192
xStatus Audio Input Connectors KeyClick Enabled.....	187	xStatus Call [n] PlacedOnHold.....	193
xStatus Audio Input RemoteInput [n] CallId	188	xStatus Call [n] Protocol	193
xStatus Audio Microphones Mute	188	xStatus Call [n] ReceiveCallRate.....	193
xStatus Audio Output Connectors Line [n] ConnectionStatus	188	xStatus Call [n] RemoteNumber	193
xStatus Audio Output Connectors Line [n] DelayMs	188	xStatus Call [n] Status.....	194
xStatus Audio Output MeasuredHdmiArcDelay	188	xStatus Call [n] TransmitCallRate.....	194
xStatus Audio Output MeasuredHdmiDelay.....	189		
xStatus Audio Output MeasuredHdmiCecDelay	189		
xStatus Audio Volume	189		
xStatus Audio VolumeMute	189		
Bookings status.....	190	Cameras status.....	194
xStatus Bookings Current Id.....	190	xStatus Cameras Camera [n] Capabilities Options	194
Call status.....	190	xStatus Cameras Camera [n] Connected.....	194
xStatus Call [n] AnswerState	190	xStatus Cameras Camera [n] LightingConditions.....	195
xStatus Call [n] AttendedTransferFrom.....	190	xStatus Cameras Camera [n] MacAddress	195
		xStatus Cameras Camera [n] Manufacturer	195
		xStatus Cameras Camera [n] Model.....	195
		xStatus Cameras Camera [n] SerialNumber.....	195
		xStatus Cameras Camera [n] SoftwareID.....	195
		xStatus Cameras SpeakerTrack ActiveConnector	196



xStatus Cameras SpeakerTrack Availability	196	xStatus Conference Presentation CallId	202
xStatus Cameras SpeakerTrack Status	196	xStatus Conference Presentation LocalInstanceId [n] SendingMode	202
Capabilities status	196	xStatus Conference Presentation LocalInstanceId [n] Source	202
xStatus Capabilities Conference MaxActiveCalls	196	xStatus Conference Presentation Mode	202
xStatus Capabilities Conference MaxAudioCalls	196	xStatus Conference SpeakerLock CallId	202
xStatus Capabilities Conference MaxCalls	197	xStatus Conference SpeakerLock Mode	203
xStatus Capabilities Conference MaxVideoCalls	197		
Conference status	197	Diagnostics status	203
xStatus Conference ActiveSpeaker CallId	197	xStatus Diagnostics Message [n] Description	203
xStatus Conference Call [n] AuthenticationRequest	197	xStatus Diagnostics Message [n] Level	203
xStatus Conference Call [n] BookingId	198	xStatus Diagnostics Message [n] References	204
xStatus Conference Call [n] Capabilities FarendMessage Mode	198	xStatus Diagnostics Message [n] Type	204
xStatus Conference Call [n] Capabilities FECC Mode	198		
xStatus Conference Call [n] Capabilities FECC NumberOfPresets	198	H320 status	205
xStatus Conference Call [n] Capabilities FECC NumberOfSources	198	xStatus H320 Gateway Address	205
xStatus Conference Call [n] Capabilities FECC Source [n] Name	198	xStatus H320 Gateway Id	205
xStatus Conference Call [n] Capabilities FECC Source [n] Options	199	xStatus H320 Gateway Mode	206
xStatus Conference Call [n] Capabilities FECC Source [n] SourceId	199	xStatus H320 Gateway Number	206
xStatus Conference Call [n] Capabilities Hold	199	xStatus H320 Gateway Reason	206
xStatus Conference Call [n] Capabilities IxChannel Status	199	xStatus H320 Gateway Status	206
xStatus Conference Call [n] Capabilities ParticipantDisconnect	199		
xStatus Conference Call [n] Capabilities ParticipantList	199	H323 status	207
xStatus Conference Call [n] Capabilities ParticipantMute	200	xStatus H323 Gatekeeper Address	207
xStatus Conference Call [n] Capabilities Presentation	200	xStatus H323 Gatekeeper Port	207
xStatus Conference Call [n] EventCenter Mode	200	xStatus H323 Gatekeeper Reason	207
xStatus Conference Call [n] Manufacturer	200	xStatus H323 Gatekeeper Status	207
xStatus Conference Call [n] MicrophonesMuted	200	xStatus H323 Mode Reason	207
xStatus Conference Call [n] SoftwareID	201	xStatus H323 Mode Status	208
xStatus Conference Call [n] Streamed	201		
xStatus Conference Call [n] VideoMutePoster	201	HttpFeedback status	208
xStatus Conference DoNotDisturb	201	xStatus HttpFeedback [n] Expression [n]	208
xStatus Conference Line [n] Mode	201	xStatus HttpFeedback [n] Format	208
xStatus Conference Multipoint Mode	202	xStatus HttpFeedback [n] Status	208
		xStatus HttpFeedback [n] URL	209



MediaChannels status	209
xStatus MediaChannels Call [n] Channel [n] Audio Channels.....	209
xStatus MediaChannels Call [n] Channel [n] Audio ChannelRole	209
xStatus MediaChannels Call [n] Channel [n] Audio Mute.....	210
xStatus MediaChannels Call [n] Channel [n] Audio Protocol	210
xStatus MediaChannels Call [n] Channel [n] Direction.....	210
xStatus MediaChannels Call [n] Channel [n] Encryption.....	210
xStatus MediaChannels Call [n] Channel [n] NetStat Bytes.....	210
xStatus MediaChannels Call [n] Channel [n] NetStat ChannelRate	210
xStatus MediaChannels Call [n] Channel [n] NetStat Jitter.....	211
xStatus MediaChannels Call [n] Channel [n] NetStat LastIntervalLost	211
xStatus MediaChannels Call [n] Channel [n] NetStat LastIntervalReceived	211
xStatus MediaChannels Call [n] Channel [n] NetStat Loss	211
xStatus MediaChannels Call [n] Channel [n] NetStat MaxJitter.....	212
xStatus MediaChannels Call [n] Channel [n] NetStat Packets.....	212
xStatus MediaChannels Call [n] Channel [n] ParticipantId.....	212
xStatus MediaChannels Call [n] Channel [n] Type	212
xStatus MediaChannels Call [n] Channel [n] Video ChannelRole	212
xStatus MediaChannels Call [n] Channel [n] Video FrameRate	212
xStatus MediaChannels Call [n] Channel [n] Video Protocol	213
xStatus MediaChannels Call [n] Channel [n] Video ResolutionX	213
xStatus MediaChannels Call [n] Channel [n] Video ResolutionY	213
 Network status	 213
xStatus Network [n] CDP Address.....	213
xStatus Network [n] CDP Capabilities	213
xStatus Network [n] CDP DeviceId	214
xStatus Network [n] CDP Duplex	214
xStatus Network [n] CDP Platform	214
xStatus Network [n] CDP PortID	214
xStatus Network [n] CDP PrimaryMgmtAddress.....	214
xStatus Network [n] CDP SysName	214
xStatus Network [n] CDP SysObjectId	215
xStatus Network [n] CDP Version	215
xStatus Network [n] CDP VoIPApplianceVlanId.....	215
 xStatus Network [n] CDP VTPMgmtDomain.....	 215
xStatus Network [n] DNS Domain Name	215
xStatus Network [n] DNS Server [n] Address	216
xStatus Network [n] Ethernet MacAddress	216
xStatus Network [n] Ethernet Speed	216
xStatus Network [n] IPv4 Address	216
xStatus Network [n] IPv4 Gateway	216
xStatus Network [n] IPv4 SubnetMask	216
xStatus Network [n] IPv6 Address	217
xStatus Network [n] IPv6 Gateway	217
xStatus Network [n] IPv6 LinkLocalAddress	217
xStatus Network [n] VLAN Voice VlanId	217
 NetworkServices status	 218
xStatus NetworkServices NTP CurrentAddress	218
xStatus NetworkServices NTP Server [n] Address	218
xStatus NetworkServices NTP Status.....	218
xStatus NetworkServices UPnP Status.....	218
 Peripherals status.....	 219
xStatus Peripherals ConnectedDevice [n] HardwareInfo	219
xStatus Peripherals ConnectedDevice [n] ID	219
xStatus Peripherals ConnectedDevice [n] Name	219
xStatus Peripherals ConnectedDevice [n] SerialNumber	219
xStatus Peripherals ConnectedDevice [n] SoftwareInfo	219
xStatus Peripherals ConnectedDevice [n] Status.....	220
xStatus Peripherals ConnectedDevice [n] Type	220
xStatus Peripherals ConnectedDevice [n] UpgradeFailureReason	220
xStatus Peripherals ConnectedDevice [n] UpgradeStatus	220
xStatus Peripherals ConnectedDevice [n] UpgradeURL	220
 Provisioning status	 221
xStatus Provisioning CUCM Customization Checksum	221
xStatus Provisioning CUCM ExtensionMobility Enabled	221
xStatus Provisioning CUCM ExtensionMobility LastLoggedInUserId	221



xStatus Provisioning CUCM ExtensionMobility LoggedIn.....	221	SIP status	228
xStatus Provisioning Software Current CompletedAt.....	221	xStatus SIP AlternateURI Alias [n] URI.....	228
xStatus Provisioning Software Current URL	222	xStatus SIP AlternateURI Primary [n] URI.....	228
xStatus Provisioning Software Current VersionId	222	xStatus SIP Authentication.....	228
xStatus Provisioning Software UpgradeStatus LastChange.....	222	xStatus SIP CallForward DisplayName.....	228
xStatus Provisioning Software UpgradeStatus Message	222	xStatus SIP CallForward Mode	228
xStatus Provisioning Software UpgradeStatus Phase.....	222	xStatus SIP CallForward URI.....	228
xStatus Provisioning Software UpgradeStatus SessionId	222	xStatus SIP Mailbox MessagesWaiting	229
xStatus Provisioning Software UpgradeStatus Status.....	223	xStatus SIP Mailbox URI	229
xStatus Provisioning Software UpgradeStatus Urgency	223	xStatus SIP Proxy [n] Address.....	229
xStatus Provisioning Software UpgradeStatus URL	223	xStatus SIP Proxy [n] Status	229
xStatus Provisioning Software UpgradeStatus VersionId	223	xStatus SIP Registration [n] Authentication.....	229
xStatus Provisioning Status.....	223	xStatus SIP Registration [n] Reason	229
Proximity status	224	xStatus SIP Registration [n] Status	230
xStatus Proximity Services Availability.....	224	xStatus SIP Registration [n] URI.....	230
RoomAnalytics status	224	xStatus SIP Secure.....	230
xStatus RoomAnalytics AmbientNoise Level A.....	224	xStatus SIP Verified.....	230
xStatus RoomAnalytics PeopleCount Current	224	Standby status	231
xStatus RoomAnalytics PeoplePresence.....	225	xStatus Standby State.....	231
xStatus RoomAnalytics Sound Level A.....	225	SystemUnit status	231
RoomPreset status	225	xStatus SystemUnit Hardware Module CompatibilityLevel	231
xStatus RoomPreset [n] Defined	225	xStatus SystemUnit Hardware Module SerialNumber	231
xStatus RoomPreset [n] Description	225	xStatus SystemUnit Hardware Monitoring Fan [n] Status	232
xStatus RoomPreset [n] Type	226	xStatus SystemUnit Hardware Monitoring Temperature Status	232
Security status	226	xStatus SystemUnit Notifications Notification [n] Text	232
xStatus Security FIPS Mode.....	226	xStatus SystemUnit Notifications Notification [n] Type	232
xStatus Security Persistency CallHistory	226	xStatus SystemUnit ProductId	233
xStatus Security Persistency Configurations	227	xStatus SystemUnit ProductPlatform	233
xStatus Security Persistency DHCP	227	xStatus SystemUnit ProductType	233
xStatus Security Persistency InternalLogging.....	227	xStatus SystemUnit Software DisplayName	233
xStatus Security Persistency LocalPhonebook	227	xStatus SystemUnit Software Name	233
		xStatus SystemUnit Software OptionKeys Encryption	233
		xStatus SystemUnit Software OptionKeys MultiSite	234



xStatus SystemUnit Software OptionKeys RemoteMonitoring	234	xStatus Video Input MainVideoMute	240
xStatus SystemUnit Software ReleaseDate	234	xStatus Video Input MainVideoSource	240
xStatus SystemUnit Software Version	234	xStatus Video Input Source [n] ConnectorId	240
xStatus SystemUnit State NumberOfActiveCalls	234	xStatus Video Input Source [n] FormatStatus	241
xStatus SystemUnit State NumberOfInProgressCalls	234	xStatus Video Input Source [n] FormatType	241
xStatus SystemUnit State NumberOfSuspendedCalls	235	xStatus Video Input Source [n] MediaChannelId	241
xStatus SystemUnit Uptime	235	xStatus Video Input Source [n] Resolution Height	241
Time status	235	xStatus Video Input Source [n] Resolution RefreshRate	241
xStatus Time SystemTime	235	xStatus Video Input Source [n] Resolution Width	241
UserInterface status	236	xStatus Video Layout LayoutFamily Local	242
xStatus UserInterface ContactInfo ContactMethod [n] Number	236	xStatus Video Layout LayoutFamily Remote	242
xStatus UserInterface ContactInfo Name	236	xStatus Video Monitors	242
xStatus UserInterface Extensions Widget [n] Value	236	xStatus Video Output Connector [n] Connected	242
xStatus UserInterface Extensions Widget [n] WidgetId	236	xStatus Video Output Connector [n] ConnectedDevice CEC [n] DeviceType	242
xStatus UserInterface Features Call End	236	xStatus Video Output Connector [n] ConnectedDevice CEC [n] LogicalAddress	243
xStatus UserInterface Features MidCallControls	237	xStatus Video Output Connector [n] ConnectedDevice CEC [n] Name	243
xStatus UserInterface Features Call Start	237	xStatus Video Output Connector [n] ConnectedDevice CEC [n] PowerStatus	243
xStatus UserInterface Features Share Start	237	xStatus Video Output Connector [n] ConnectedDevice CEC [n] VendorId	243
xStatus UserInterface Features Whiteboard Start	237	xStatus Video Output Connector [n] ConnectedDevice Name	244
xStatus UserInterface SettingsMenu Visibility	238	xStatus Video Output Connector [n] ConnectedDevice PreferredFormat	244
Video status	238	xStatus Video Output Connector [n] ConnectedDevice ScreenSize	244
xStatus Video ActiveSpeaker PIPPosition	238	xStatus Video Output Connector [n] MonitorRole	244
xStatus Video Input Connector [n] Connected	238	xStatus Video Output Connector [n] Resolution Height	244
xStatus Video Input Connector [n] ConnectedDevice CEC [n] DeviceType	239	xStatus Video Output Connector [n] Resolution RefreshRate	244
xStatus Video Input Connector [n] ConnectedDevice CEC [n] LogicalAddress	239	xStatus Video Output Connector [n] Resolution Width	245
xStatus Video Input Connector [n] ConnectedDevice CEC [n] Name	239	xStatus Video Output Connector [n] Type	245
xStatus Video Input Connector [n] ConnectedDevice CEC [n] PowerStatus	239	xStatus Video Output Monitor [n] Backlight	245
xStatus Video Input Connector [n] ConnectedDevice CEC [n] VendorId	239	xStatus Video Output Monitor [n] FirmwareVersion	245
xStatus Video Input Connector [n] SignalState	239	xStatus Video Output Monitor [n] ModelName	245
xStatus Video Input Connector [n] SourceId	240	xStatus Video Output Monitor [n] Position	246
xStatus Video Input Connector [n] Type	240	xStatus Video Output Monitor [n] SerialNumber	246
		xStatus Video Output Monitor [n] Temperature	246
		xStatus Video Presentation PIPPosition	246



xStatus Video Selfview FullscreenMode.....	246
xStatus Video Selfview Mode	247
xStatus Video Selfview OnMonitorRole	247
xStatus Video Selfview PIPPosition	247
WebEngine status.....	247
xStatus WebEngine Features Signage.....	247
xStatus WebEngine Features WebEngine.....	247
Webex status.....	248
xStatus Webex Status.....	248



Audio status

xStatus Audio Input Connectors ARC [n] EcReferenceDelay

Requires user role: ADMIN, USER

Returns the detected latency for each loudspeaker to microphone path for devices supporting ARC input used as microphone input. The result is in milliseconds.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Input Connectors ARC 1 EcReferenceDelay
*s Audio Input Connectors ARC 1 EcReferenceDelay: 0
** end
```

xStatus Audio Input Connectors HDMI [n] EcReferenceDelay

Requires user role: ADMIN, USER

Returns the detected latency for each loudspeaker to microphone path for devices supporting HDMI input used as microphone input. The result is in milliseconds.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Input Connectors HDMI 1 EcReferenceDelay
*s Audio Input Connectors HDMI 1 EcReferenceDelay: 0
** end
```

xStatus Audio Input Connectors HDMI [n] Mute

Requires user role: ADMIN, USER

Shows whether the audio channel on a HDMI input connector is muted or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Audio Input Connectors HDMI 1 Mute
*s Audio Input Connectors HDMI 1 Mute: Off
** end
```

xStatus Audio Input Connectors Line [n] Mute

Requires user role: ADMIN, USER

Shows whether the audio on a Line input connector is muted or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Audio Input Connectors Line 1 Mute
*s Audio Input Connectors Line 1 Mute: Off
** end
```

xStatus Audio Input Connectors Microphone [n] ConnectionStatus

Requires user role: ADMIN, INTEGRATOR, USER

Indicates whether a microphone is detected on the microphone input connector.

Value space of the result returned:

Connected/NotConnected/Unknown

Example:

```
xStatus Audio Input Connectors Microphone ConnectionStatus
*s Audio Input Connectors Microphone 1 ConnectionStatus: NotConnected
*s Audio Input Connectors Microphone 2 ConnectionStatus: Connected
** end
```



xStatus Audio Input Connectors Microphone [n] EcReferenceDelay

Requires user role: ADMIN, USER

Returns the detected latency for each loudspeaker to microphone path. The result is in milliseconds.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Input Connectors Microphone 1 EcReferenceDelay  
*s Audio Input Connectors Microphone 1 EcReferenceDelay: 120  
** end
```

xStatus Audio Input Connectors Microphone [n] Mute

Requires user role: ADMIN, USER

Shows whether the audio on a Microphone input connector is muted or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Audio Input Connectors Microphone 1 Mute  
*s Audio Input Connectors Microphone 1 Mute: Off  
** end
```

xStatus Audio Input KeyClick Attenuate

Requires user role: ADMIN, USER

Shows whether the device is automatically attenuating clicking noises, such as those detected microphone signals caused by the typing of a keyboard.

Value space of the result returned:

False/True

Example:

```
xStatus Audio Input KeyClick Attenuate  
*s Audio Input KeyClick Attenuate: True  
** end
```

xStatus Audio Input KeyClick Detected

Requires user role: ADMIN, USER

Shows what type of audio signals the device is detecting for attenuation. The device will attenuate the microphone signal if clicking noises from a keyboard are detected. If voice or silence is detected, the microphone signal will not be attenuated.

Value space of the result returned:

KeyClick/Voice/Silence

Example:

```
xStatus Audio Input KeyClick Detected  
*s Audio Input KeyClick Detected: KeyClick  
** end
```

xStatus Audio Input KeyClick Enabled

Requires user role: ADMIN, USER

Shows whether detection for attenuation on the microphone signal is enabled.

Value space of the result returned:

True/False

Example:

```
xStatus Audio Input KeyClick Enabled  
*s Audio Input KeyClick Enabled: On  
** end
```



xStatus Audio Input RemoteInput [n] CallId

Requires user role: ADMIN, USER

Shows the CallId for the remote audio input.

You can run the command xStatus Audio Input RemoteInput to find the identity [n] of the input.

Value space of the result returned:

0..65534

Example:

```
xStatus Audio Input RemoteInput 8 CallId
*s Audio Input RemoteInput 8 CallId: 28
** end
```

xStatus Audio Microphones Mute

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether the microphones are muted.

Value space of the result returned:

On/Off

Example:

```
xStatus Audio Microphones Mute
*s Audio Microphones Mute: Off
** end
```

xStatus Audio Output Connectors Line [n] ConnectionStatus

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether the audio output line is connected.

Value space of the result returned:

Connected/NotConnected/Unknown

Example:

```
xStatus Audio Output Connectors Line 1 ConnectionStatus
*s Audio Output Connectors Line 1 ConnectionStatus: Connected
** end
```

xStatus Audio Output Connectors Line [n] DelayMs

Requires user role: ADMIN, INTEGRATOR, USER

Shows the delay in milliseconds.

Value space of the result returned:

Integer (0..290)

Example:

```
xStatus Audio Output Connectors Line 1 DelayMs
*s Audio Output Connectors Line 1 DelayMs: 60
** end
```

xStatus Audio Output MeasuredHdmiArcDelay

Requires user role: ADMIN, INTEGRATOR, USER

Shows the measured audio delay of the device connected to the HDMI connector. This delay is measured through the HDMI audio return channel, and will secure good lip-synchronization between audio and video.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Output MeasuredHdmiArcDelay
*s Audio Output MeasuredHdmiArcDelay: 85
** end
```



xStatus Audio Output MeasuredHdmiDelay

Requires user role: ADMIN, INTEGRATOR, USER

Shows the measured audio delay of the device connected to the HDMI connector. This delay is measured from the HDMI output to one of the microphones.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Output MeasuredHdmiDelay
*s Audio Output MeasuredHdmiDelay: 134
** end
```

xStatus Audio Output MeasuredHdmiCecDelay

Requires user role: ADMIN, INTEGRATOR, USER

Shows the reported video delay of the device connected to the HDMI connector. This delay is reported through the consumer electronics control (CEC) protocol, and will secure good lip-synchronization between audio and video.

Value space of the result returned:

Integer

Example:

```
xStatus Audio Output ReportedHdmiCecDelay
*s Audio Output ReportedHdmiCecDelay: 39
** end
```

xStatus Audio Volume

Requires user role: ADMIN, INTEGRATOR, USER

Shows the volume level (dB) of the loudspeaker output.

Value space of the result returned:

0..100

Example:

```
xStatus Audio Volume
*s Audio Volume: 70
** end
```

xStatus Audio VolumeMute

Requires user role: ADMIN, USER

Shows whether the device volume is set to mute.

Value space of the result returned:

Off/On

Example:

```
xStatus Audio VolumeMute
*s Audio VolumeMute: Off
** end
```



Bookings status

xStatus Bookings Current Id

Requires user role: ADMIN, USER

The ID of the on going booking event, if any.

Value space of the result returned:

String

Example:

```
xStatus Bookings Current Id  
*s Bookings Current Id: "123"  
** end
```

Call status

xStatus Call [n] AnswerState

Requires user role: ADMIN, USER

Indicates if a call is answered, ignored or has been automatically answered by a device.

Value space of the result returned:

Unanswered/Ignored/Autoanswered/Answered

Example:

```
xStatus Call AnswerState  
*s Call 5 AnswerState: Answered  
** end
```

xStatus Call [n] AttendedTransferFrom

Requires user role: ADMIN, USER

Shows the CallId for the call the current call was transferred from.

Value space of the result returned:

Integer

Example:

```
xStatus Call 1 AttendedTransferFrom  
*s Call 1 AttendedTransferFrom: 1234  
** end
```



xStatus Call [n] CallbackNumber

Requires user role: ADMIN, USER

Shows the remote (far end) number or URI of an incoming or outgoing call, including the call protocol, for call back. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

String

Example:

```
xStatus Call 27 CallbackNumber  
*s Call 27 CallbackNumber: "h323:firstname.lastname@company.com"  
** end
```

xStatus Call [n] CallType

Requires user role: ADMIN, USER

Shows the call type of the incoming or outgoing call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

Video/Audio/VideoCanEscalate/ForwardAllCall/Unknown

Example:

```
xStatus Call 27 CallType  
*s Call 27 CallType: Video  
** end
```

xStatus Call [n] DeviceType

Requires user role: ADMIN, USER

Shows where the call is connected to.

Value space of the result returned:

Endpoint/MCU

Example:

```
xStatus Call DeviceType  
*s Call 4 DeviceType: Endpoint  
** end
```

xStatus Call [n] Direction

Requires user role: ADMIN, USER

Shows the direction of the call initiation. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

Incoming/Outgoing

Example:

```
xStatus Call 27 Direction  
*s Call 27 Direction: Outgoing  
** end
```

xStatus Call [n] DisplayName

Requires user role: ADMIN, USER

Shows the name of the remote (far end) participant in an incoming or outgoing call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

String

Example:

```
xStatus Call 27 DisplayName  
*s Call 27 DisplayName: "firstname.lastname@company.com"  
** end
```



xStatus Call [n] Duration

Requires user role: ADMIN, USER

Shows the duration of a call (in seconds). You can run the command xStatus Call to find the call identity.

Value space of the result returned:

Integer

Example:

```
xStatus Call 27 Duration
*s Call 27 Duration: 2354
** end
```

xStatus Call [n] Encryption Type

Requires user role: ADMIN, USER

Shows the encryption type of the call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

None/Aes-128

Example:

```
xStatus Call 27 Encryption Type
*s Call 27 Encryption Type: "None"
** end
```

xStatus Call [n] FacilityServiceId

Requires user role: ADMIN, INTEGRATOR, USER

When calling a facility service, the facility service id is shown. Otherwise the value 0 is returned.

Value space of the result returned:

0..5

Example:

```
xStatus Call FacilityServiceId
*s Call 3 FacilityServiceId: 1
** end
```

xStatus Call [n] HoldReason

Requires user role: ADMIN, USER

Shows the reason the current outgoing call was put on hold.

Value space of the result returned:

Conference/Transfer/None

Example:

```
xStatus Call 2 HoldReason
*s Call 2 HoldReason: None
** end
```

xStatus Call [n] Ice

Requires user role: ADMIN, USER

ICE is a feature that enables two sides of a call to send media (video and audio) directly between each other, if a direct network path has been found through ICE negotiation. This status reflects the result of that negotiation.

Value space of the result returned:

Disabled/Passed/Failed

Example:

```
xStatus Call 2 Ice
*s Call 2 Ice: Passed
** end
```



xStatus Call [n] PlacedOnHold

Requires user role: ADMIN, USER

Shows the placed on hold status of the call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

True/False

Example:

```
xStatus Call 27 PlacedOnHold  
*s Call 27 PlacedOnHold: False  
** end
```

xStatus Call [n] Protocol

Requires user role: ADMIN, USER

Shows the call protocol of the incoming or outgoing call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

H320/H323/SIP/Spark/Unknown

Example:

```
xStatus Call 27 Protocol  
*s Call 27 Protocol: "h323"  
** end
```

xStatus Call [n] ReceiveCallRate

Requires user role: ADMIN, INTEGRATOR, USER

Shows the receive bandwidth in the call in kilobits per second (kbps). You can run the command xStatus Call to find the call identity.

Value space of the result returned:

Integer

Example:

```
xStatus Call 27 ReceiveCallRate  
*s Call 27 ReceiveCallRate: 4000  
** end
```

xStatus Call [n] RemoteNumber

Requires user role: ADMIN, USER

Shows the remote (far end) number or URI of an incoming or outgoing call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

String

Example:

```
xStatus Call 27 RemoteNumber  
*s Call 27 RemoteNumber: "5585232"  
** end
```



xStatus Call [n] Status

Requires user role: ADMIN, USER

Shows the status of a call. You can run the command xStatus Call to find the call identity.

Value space of the result returned:

*Idle/Dialling/Ringing/Connecting/Connected/Disconnecting/OnHold/EarlyMedia/Preserved/
RemotePreserved*

Example:

```
xStatus Call 27 Status  
*s Call 27 Status: Connected  
** end
```

xStatus Call [n] TransmitCallRate

Requires user role: ADMIN, INTEGRATOR, USER

Shows the transmit bandwidth in the call in kilobits per second (kbps). You can run the command xStatus Call to find the call identity.

Value space of the result returned:

Integer

Example:

```
xStatus Call 27 TransmitCallRate  
*s Call 27 TransmitCallRate: 768  
** end
```

Cameras status

xStatus Cameras Camera [n] Capabilities Options

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the camera capabilities (ptzf = pan, tilt, zoom, focus).

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 Capabilities Options  
*s Camera 1 Capabilities Options: "ptzf"  
** end
```

xStatus Cameras Camera [n] Connected

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows if the camera is connected or not.

Value space of the result returned:

True/False

Example:

```
xStatus Cameras Camera 1 Connected  
*s Camera 1 Connected: True  
** end
```



xStatus Cameras Camera [n] LightingConditions

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Shows how the camera perceives the lighting conditions in the room.

Value space of the result returned:

Unknown/Good/Dark/Backlight

Example:

```
xStatus Cameras Camera 1 LightingConditions  
*s Camera 1 LightingConditions: Good  
** end
```

xStatus Cameras Camera [n] MacAddress

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the MAC (Media Access Control) address for the camera.

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 MacAddress  
*s Camera 1 MacAddress: ""  
** end
```

xStatus Cameras Camera [n] Manufacturer

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the manufacturer of the camera.

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 Manufacturer  
*s Camera 1 Manufacturer: "Cisco"  
** end
```

xStatus Cameras Camera [n] Model

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the camera model.

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 Model  
*s Camera 1 Model: "Precision 40"  
** end
```

xStatus Cameras Camera [n] SerialNumber

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the camera serial number.

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 SerialNumber  
*s Camera 1 SerialNumber: "B1AB26B00010"  
** end
```

xStatus Cameras Camera [n] SoftwareID

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the software identity of the camera.

Value space of the result returned:

String

Example:

```
xStatus Cameras Camera 1 SoftwareID  
*s Camera 1 SoftwareID: "S01718-4.0FINAL [ID:40063] 2014-10-20"  
** end
```



xStatus Cameras SpeakerTrack ActiveConnector

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Not applicable.

Value space of the result returned:

Integer

Example:

```
xStatus Cameras SpeakerTrack ActiveConnector  
*s Cameras SpeakerTrack ActiveConnector: 1  
** end
```

xStatus Cameras SpeakerTrack Availability

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows whether or not the best overview feature is available.

Value space of the result returned:

Off/Unavailable/Available

Example:

```
xStatus Cameras SpeakerTrack Availability  
*s Cameras SpeakerTrack Availability: Available  
** end
```

xStatus Cameras SpeakerTrack Status

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows whether or not best overview is active.

Value space of the result returned:

Active/Inactive

Example:

```
xStatus Cameras SpeakerTrack Status  
*s Cameras SpeakerTrack Status: Active  
** end
```

Capabilities status

xStatus Capabilities Conference MaxActiveCalls

Requires user role: ADMIN, USER

Shows the maximum number of simultaneous active calls. Calls that are set on hold/transfer are not counted as active.

Value space of the result returned:

0..5

Example:

```
xStatus Capabilities Conference MaxNumberOfActiveCalls  
*s Capabilities Conference MaxNumberOfActiveCalls: 3  
** end
```

xStatus Capabilities Conference MaxAudioCalls

Requires user role: ADMIN, USER

Shows the maximum number of simultaneous audio calls that is supported.

Value space of the result returned:

Integer

Example:

```
xStatus Capabilities Conference MaxAudioCalls  
*s Capabilities Conference MaxAudioCalls: 3  
** end
```



xStatus Capabilities Conference MaxCalls

Requires user role: ADMIN, USER

Shows the maximum number of simultaneous calls.

Value space of the result returned:

0..5

Example:

```
xStatus Capabilities Conference MaxCalls
*s Capabilities Conference MaxCalls: 3
** end
```

xStatus Capabilities Conference MaxVideoCalls

Requires user role: ADMIN, USER

Shows the maximum number of simultaneous video calls that is supported.

Value space of the result returned:

Integer

Example:

```
xStatus Capabilities Conference MaxVideoCalls
*s Capabilities Conference MaxVideoCalls: 3
** end
```

Conference status

xStatus Conference ActiveSpeaker CallId

Requires user role: ADMIN, USER

Shows the CallId of the current active speaker.

Value space of the result returned:

Integer

Example:

```
xStatus Conference ActiveSpeaker CallId
*s Conference ActiveSpeaker CallId: 3
** end
```

xStatus Conference Call [n] AuthenticationRequest

Requires user role: ADMIN, INTEGRATOR, USER

This status is only relevant for Cisco Webex registered devices. When this status has another value than "None" the device is waiting for an authentication response. Use the Conference Call AuthenticationResponse command to give the response.

Value space of the result returned:

None/HostPinOrGuest/HostPinOrGuestPin/PanelistPin

Example:

```
xStatus Conference Call 2 AuthenticationRequest
*s Conference Call 2 AuthenticationRequest: None
** end
```



xStatus Conference Call [n] BookingId

Requires user role: ADMIN, USER

Shows the booking ID of a conference (if assigned). The booking ID can be used for easy identification of a call or conference.

Value space of the result returned:

String

Example:

```
xStatus Conference Call 2 BookingId
*s Conference Call 2 BookingId: "MyConference"
** end
```

xStatus Conference Call [n] Capabilities FarendMessage Mode

Requires user role: ADMIN, USER

Not applicable in this release.

Value space of the result returned:

On/Off

Example:

```
xStatus Conference Call Capabilities FarendMessage Mode
*s Conference Call 4 Capabilities FarendMessage Mode: Off
** end
```

xStatus Conference Call [n] Capabilities FECC Mode

Requires user role: ADMIN, USER

Shows whether or not you have permission to control the input sources at a far end site.

Value space of the result returned:

On/Off

Example:

```
xStatus Conference Call 2 Capabilities FECC Mode
*s Conference Call 2 Capabilities FECC Mode: On
** end
```

xStatus Conference Call [n] Capabilities FECC NumberOfPresets

Requires user role: ADMIN, USER

Shows the number of presets available for the input sources at a far end site.

Value space of the result returned:

1..15

Example:

```
xStatus Conference Call 2 Capabilities FECC NumberOfPresets
*s Conference Call 2 Capabilities FECC NumberOfPresets: 15
** end
```

xStatus Conference Call [n] Capabilities FECC NumberOfSources

Requires user role: ADMIN, USER

Shows the number of input sources that can be connected at a far end site.

Value space of the result returned:

1..5

Example:

```
xStatus Conference Call 2 Capabilities FECC NumberOfSources
*s Conference Call 2 Capabilities FECC NumberOfSources: 5
** end
```

xStatus Conference Call [n] Capabilities FECC Source [n] Name

Requires user role: ADMIN, USER

Shows the name of an input source that can be connected at a far end site.

Value space of the result returned:

String

Example:

```
xStatus Conference Call 2 Capabilities FECC Source 1 Name
*s Conference Call 2 Capabilities FECC Source 1 Name: "Main camera"
** end
```



xStatus Conference Call [n] Capabilities FECC Source [n] Options

Requires user role: ADMIN, USER

Shows available options for an input source that can be connected at a far end site (for a camera: p=pan; t=tilt; z=zoom; f=focus).

Value space of the result returned:

String

Example:

```
xStatus Conference Call 2 Capabilities FECC Source 1 Options  
*s Conference Call 2 Capabilities FECC Source 1 Options: "ptzf"  
** end
```

xStatus Conference Call [n] Capabilities FECC Source [n] Sourceld

Requires user role: ADMIN, USER

Shows the ID of an input source that can be connected at a far end site.

Value space of the result returned:

Integer

Example:

```
xStatus Conference Call 2 Capabilities FECC Source 1 SourceId  
*s Conference Call 2 Capabilities FECC Source 1 SourceId: 6  
** end
```

xStatus Conference Call [n] Capabilities Hold

Requires user role: ADMIN, USER

Indicates whether the far-end site can be placed on hold or not.

Value space of the result returned:

True/False

Example:

```
xStatus Conference Call Capabilities Hold  
*s Conference Call 2 Capabilities Hold: True  
** end
```

xStatus Conference Call [n] Capabilities IxChannel Status

Requires user role: ADMIN, USER

Not applicable in this release.

Value space of the result returned:

Active/Failed/Off

Example:

```
xStatus Conference Call 4 Capabilities IxChannel Status  
*s Conference Call 4 Capabilities IxChannel Status: Active  
** end
```

xStatus Conference Call [n] Capabilities ParticipantDisconnect

Requires user role: ADMIN, USER

Value space of the result returned:

Available/Unavailable

Example:

```
xStatus Conference Call 2 Capabilities ParticipantDisconnect  
*s Conference Call 2 Capabilities ParticipantDisconnect: Available  
** end
```

xStatus Conference Call [n] Capabilities ParticipantList

Requires user role: ADMIN, USER

Value space of the result returned:

Available/Unavailable

Example:

```
xStatus Conference Call 2 Capabilities ParticipantList  
*s Conference Call 2 Capabilities ParticipantList: Available  
** end
```



xStatus Conference Call [n] Capabilities ParticipantMute

Requires user role: ADMIN, USER

Value space of the result returned:

Available/Unavailable

Example:

```
xStatus Conference Call 2 Capabilities ParticipantMute
*s Conference Call 2 Capabilities ParticipantMute: Available
** end
```

xStatus Conference Call [n] Capabilities Presentation

Requires user role: ADMIN, USER

Lists the presentation capabilities for other participants in the conference.

Value space of the result returned:

True/False

Example:

```
xStatus Conference Call 2 Capabilities Presentation
*s Conference Call 2 Capabilities Presentation: True
** end
```

xStatus Conference Call [n] EventCenter Mode

Requires user role: ADMIN, USER

Shows if the Practice Session mode is currently in use on this call. This status is only available for cloud registered devices.

Value space of the result returned:

Normal/PracticeSession

Example:

```
xStatus Conference Call 2 EventCenter Mode
*s Conference Call 2 EventCenter Mode: Normal
** end
```

xStatus Conference Call [n] Manufacturer

Requires user role: ADMIN, USER

Shows the manufacturer of the device at a far end site.

Value space of the result returned:

String

Example:

```
xStatus Conference Call 2 Manufacturer
*s Conference Call 2 Manufacturer: "Cisco"
** end
```

xStatus Conference Call [n] MicrophonesMuted

Requires user role: ADMIN, USER

Lists the audio mute status for other participants in the conference.

Value space of the result returned:

True/False

Example:

```
xStatus Conference Call 2 MicrophonesMuted
*s Conference Call 2 MicrophonesMuted: True
** end
```

xStatus Conference Call [n] SoftwareID

Requires user role: ADMIN, USER

Shows the ID of the software running on the device at a far end site.

Value space of the result returned:

String

Example:

```
xStatus Conference Call 2 SoftwareID
*s Conference Call 2 SoftwareID: "CE8"
** end
```



xStatus Conference Call [n] Streamed

Requires user role: ADMIN, USER

Shows if the conference is being live streamed.

Value space of the result returned:

False/True

Example:

```
xStatus Conference Call 2 Streamed
*s Conference Call 2 Streamed: False
** end
```

xStatus Conference Call [n] VideoMutePoster

Requires user role: ADMIN, USER

Value space of the result returned:

False/True

xStatus Conference DoNotDisturb

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether DoNotDisturb mode is switched on or not.

Value space of the result returned:

Active/Inactive

Example:

```
xStatus Conference DoNotDisturb
*s Conference DoNotDisturb: Inactive
** end
```

xStatus Conference Line [n] Mode

Requires user role: ADMIN, USER

Indicates whether the device is configured as private or shared line on CUCM.

Value space of the result returned:

Shared/Private

Example:

```
xStatus Conference Line Mode
*s Conference Line 1 Mode: Private
** end
```

xStatus Conference Multipoint Mode

Requires user role: ADMIN, USER

Shows how the Multipoint video conferences are handled.

Value space of the result returned:

Auto/CUCMMediaResourceGroupList/MultiSite/Off

Example:

```
xStatus Conference Multipoint Mode
*s Conference Multipoint Mode: "Auto"
** end
```

xStatus Conference Presentation CallId

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the identity of the device that sends the presentation.

Value space of the result returned:

Integer

Example:

```
xStatus Conference Presentation CallId
*s Conference Presentation CallId: 0
** end
```



xStatus Conference Presentation LocalInstance [n] SendingMode

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows whether a presentation source is shared locally or with a remote participant. There can be multiple local presentations which all have their own instance.

Value space of the result returned:

LocalOnly/LocalRemote/Off

Example:

```
xStatus Conference Presentation LocalInstance 1 SendingMode  
*s Conference Presentation LocalInstance 1 SendingMode: LocalOnly  
** end
```

xStatus Conference Presentation LocalInstance [n] Source

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the SourcedId for a current presentation. There can be multiple local presentations which all have their own instance.

Value space of the result returned:

Integer

Example:

```
xStatus Conference Presentation LocalInstance 1 Source  
*s Conference Presentation LocalInstance 1 Source: 1  
** end
```

xStatus Conference Presentation Mode

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the status of the secondary video stream.

Value space of the result returned:

Off/Sending/Receiving

Example:

```
xStatus Conference Presentation Mode  
*s Conference Presentation Mode: Off  
** end
```

xStatus Conference SpeakerLock CallId

Requires user role: ADMIN, USER

Shows the CallId for the participant locked as the prominent speaker in the conference.

Value space of the result returned:

Integer

Example:

```
xStatus Conference SpeakerLock CallId  
*s Conference SpeakerLock CallId: 0  
** end
```

xStatus Conference SpeakerLock Mode

Requires user role: ADMIN, USER

Shows whether the speaker lock is enabled or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Conference SpeakerLock Mode  
*s Conference SpeakerLock Mode: Off  
** end
```



Diagnostics status

xStatus Diagnostics Message [n] Description

Requires user role: ADMIN, USER

Shows a description of the current diagnostics alerts.

Value space of the result returned:

String

Example:

```
xStatus Diagnostics Message Description
*s DiagnosticsResult Message 1 Description: "IP configuration incomplete"
** end
```

xStatus Diagnostics Message [n] Level

Requires user role: ADMIN, USER

Shows the level of importance of the diagnostics message.

Value space of the result returned:

Error/Warning/Critical

Example:

```
xStatus Diagnostics Message 4 Level
*s Diagnostics Message 4 Level: Warning
** end
```

xStatus Diagnostics Message [n] References

Requires user role: ADMIN, USER

Additional information on the diagnostics alert, if available.

Value space of the result returned:

String

Example:

```
xStatus Diagnostics Message 10 References
*s Diagnostics Message 10 References: "delay=190"
** end
```



xStatus Diagnostics Message [n] Type

Requires user role: ADMIN, USER

Shows information on the results of the latest diagnostics on the device.

Value space of the result returned:

```
ANATOnVCS/AbnormalCallTermination/AudioInternalSpeakerDisabled/
AudioPairingInterference/AudioPairingNoise/AudioPairingRate/
AudioPairingSNR/AudioPairingTokenDecode/CAPFOperationState/
CTLInstallation/CUCMVendorConfigurationFile/CallProtocolDualStackConfig/
CallProtocolIPStackPlatformCompatibility/CallProtocolVcsProvisioningCompatibility/
CameraDetected/Camerald/CameraPairing/CameraSerial/CameraSoftwareVersion/
CameraStatus/CamerasDetected/CaptivePortalDetected/CertificateExpiry/
CompanionModelIncompatibilityLocal/CompanionModelIncompatibilityRemote/
ConfigurationFile/ContactInfoMismatch/ControlSystemConnection/
DefaultCallProtocolRegistered/ECReferenceDelay/EmbeddedWebViewFailedToLoad/
EmbeddedWebViewTerminatedUnexpectedly/EthernetDuplexMatches/FanStatus/
FirstTimeWizardNotCompleted/H320GatewayStatus/H323GatekeeperStatus/
HasActiveCallProtocol/HasValidReleaseKey/HdmiCecModeNoSound/HTTPFeedbackFailed/
HTTPSSModeSecurity/IPv4Assignment/IPv6Assignment/IPv6Mtu/ISDNLinkCompatibility/
ISDNLinkIpStack/ITLInstallation/InvalidSIPTransportConfig/IpCameraStatus/
LockDown/MacrosRuntimeStatus/MediaBlockingDetected/MediaPortRangeNegative/
MediaPortRangeOdd/MediaPortRangeOverlap/MediaPortRangeTooSmall/
MediaPortRangeValueSpace/MicrophoneReinforcement/MicrophonesConnected/
MonitorDelay/NTPStatus/NetLinkStatus/NetSpeedAutoNegotiated/NetworkQuality/
OSDVideoOutput/OutputConnectorLocations/PeripheralSoftwareVersion/PlatformSanity/
PresentationSourceSelection/PresenterTrack/ProvisioningDeveloperOptions/
ProvisioningModeAndStatus/ProvisioningStatus/RoomControl/SIPEncryption/
SIPListenPortAndOutboundMode/SIPListenPortAndRegistration/SIPPProfileRegistration/
SIPPProfileTypeSelectedVideoInputSourceConnected/SignageFailedToLoad/
SignageTerminatedUnexpectedly/SipIceAndAnatConflict/SipOrH323ButNotBothEnabled/
SoftwareUpgrade/SoftwareUpgradeKeepsFailing/SpeakerTrackEthernetConnection/
SpeakerTrackFrontPanelMountedCorrectly/SpeakerTrackMicrophoneConnection/
SpeakerTrackVideoInputs/TCPMediaFallback/TLSVerifyRequiredCerts/
TemperatureCheck/TouchPanelConnection/TurnBandwidth/UltrasoundConfigSettings/
UltrasoundSpeakerAvailability/ValidPasswords/VideoFromInternalCamera/
VideoInputSignalQuality/VideoInputStability/VideoPortRangeNegative/VideoPortRangeOdd/
VideoPortRangeTooSmall/VideoPortRangeValueSpace/MicrophoneOverloaded/
WebexActivationRequired/WebexConnectivity/WebexOffline/WifiCARquired/
PIILoggingMode/WebexAudioProximityConnectivity/WebexLyraConnectivity/
WebexNotificationConnectivity
```

Example:

xStatus Diagnostics Message Type

*s Diagnostics Message 1 Type: CamerasDetected

** end



H320 status

xStatus H320 Gateway Address

Requires user role: ADMIN, USER

Returns the IPv4 address of the ISDN Gateway, if the video conferencing device is paired to one.

Value space of the result returned:

String

Example:

```
xStatus H320 Gateway Address
*s H320 Gateway Address: ""
** end
```

xStatus H320 Gateway Id

Requires user role: ADMIN, USER

Returns the unique identification of the H320 Gateway, if the video conferencing device is paired with an ISDN Link.

Value space of the result returned:

String

Example:

```
xStatus H320 Gateway Id
*s H320 Gateway Id: "00:50:60:0B:EF:11"
** end
```

xStatus H320 Gateway Mode

Requires user role: ADMIN, USER

Returns information on the type of calls the ISDN Gateway is configured for, if the video conferencing device is paired with an ISDN Link.

Value space of the result returned:

BRI/External/G703/PRI/Unknown

Example:

```
xStatus H320 Gateway Mode
*s H320 Gateway Mode: Unknown
** end
```

xStatus H320 Gateway Number

Requires user role: ADMIN, USER

Returns the IPv6 address of the ISDN Gateway if the video conferencing device is paired to one.

Value space of the result returned:

String

Example:

```
xStatus H320 Gateway Number
*s H320 Gateway Number: ""
** end
```



xStatus H320 Gateway Reason

Requires user role: ADMIN, USER

Shows the reason for rejected Gateway registration. Only available if the video conferencing device is connected to an ISDN Link.

Value space of the result returned:

String

Example:

```
xStatus H320 Gateway Reason
*s H320 Gateway Reason: ""
** end
```

xStatus H320 Gateway Status

Requires user role: ADMIN, USER

Returns the state of the H320 Gateway, if the video conferencing device is paired with an ISDN Link.

Value space of the result returned:

Error/Inactive/OK/OKWithWarning/Warning/NoConnection

Example:

```
xStatus H320 Gateway status
*s H320 Gateway Status: Error
** end
```

H323 status

xStatus H323 Gatekeeper Address

Requires user role: ADMIN, USER

Displays the IP address of the gatekeeper where the device is registered.

Value space of the result returned:

String

Example:

```
xStatus H323 Gatekeeper Address
*s H323 Gatekeeper Address: "192.0.1.20"
** end
```

xStatus H323 Gatekeeper Port

Requires user role: ADMIN, USER

Shows the port which is used when connecting to on the gatekeeper.

Value space of the result returned:

Integer

Example:

```
xStatus H323 Gatekeeper Port
*s H323 Gatekeeper Port: 1719
** end
```



xStatus H323 Gatekeeper Reason

Requires user role: ADMIN, USER

Shows the reason for rejected registration.

Value space of the result returned:

String

Example:

```
xStatus H323 Gatekeeper Reason
*s H323 Gatekeeper Reason: ""
** end
```

xStatus H323 Gatekeeper Status

Requires user role: ADMIN, USER

Shows the gatekeeper registration status.

Value space of the result returned:

*Required/Discovering/Discovered/Authenticating/Authenticated/Registering/Registered/
Inactive/Rejected*

Example:

```
xStatus H323 Gatekeeper Status
*s H323 Gatekeeper Status: Registered
** end
```

xStatus H323 Mode Reason

Requires user role: ADMIN, USER

Shows whether there is a conflict between H.323 settings and xStatus H323 Mode Status.

Value space of the result returned:

String

Example:

```
xStatus H323 Mode Reason
*s H323 Mode Reason: ""
** end
```

xStatus H323 Mode Status

Requires user role: ADMIN, USER

Shows the status for H.323 registration.

Value space of the result returned:

Enabled/Disabled

Example:

```
xStatus H323 Mode Status
*s H323 Mode Status: "Disabled"
** end
```



HttpFeedback status

xStatus HttpFeedback [n] Expression [n]

Requires user role: ADMIN, USER

Shows the feedback from the HTTP server. There can be up to 4 slots of servers requesting HTTP feedback and up to 15 expressions for each URL. See the xCommand HttpFeedback commands for more information.

Value space of the result returned:

String

xStatus HttpFeedback [n] Format

Requires user role: ADMIN, USER

Shows the format of the HTTP Feedback feedback from the HTTP server.

Value space of the result returned:

XML/JSON

Example:

```
xStatus HttpFeedback 1 Format
*s HttpFeedback 1 Format: XML
** end
```

xStatus HttpFeedback [n] Status

Requires user role: ADMIN, USER

Shows the status of the feedback sent to the HTTP server.

Value space of the result returned:

OK/Failed

Example:

```
xStatus HttpFeedback 1 Status
*s HttpFeedback 1 Status: OK
** end
```

xStatus HttpFeedback [n] URL

Requires user role: ADMIN, USER

Shows the URL (Uniform Resource Locator) of the HTTP server. There can be up to three HTTP servers, specified by the URL.

Value space of the result returned:

String

Example:

```
xStatus HttpFeedback 1 URL
*s HttpFeedback 1 URL: "http://tms.company.com/tms/public/feedback/code.aspx"
** end
```



MediaChannels status

xStatus MediaChannels Call [n] Channel [n] Audio Channels

Requires user role: ADMIN, USER

Shows the number of incoming or outgoing audio channels.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 Audio Channels
*s MediaChannels Call 27 Channel 327 Audio Channels: 1
** end
```

xStatus MediaChannels Call [n] Channel [n] Audio ChannelRole

Requires user role: ADMIN, USER

Shows the role of the incoming or outgoing audio channel.

Value space of the result returned:

Main/Presentation

Example:

```
xStatus MediaChannels Call 27 Channel 327 Audio ChannelRole
*s MediaChannels Call 27 Channel 327 Audio ChannelRole: Main
** end
```

xStatus MediaChannels Call [n] Channel [n] Audio Mute

Requires user role: ADMIN, USER

Audio mute status of the incoming audio.

Value space of the result returned:

True/False

Example:

```
xStatus MediaChannels Call 27 Channel 327 Audio Mute
*s MediaChannels Call 27 Channel 327 Audio Mute: False
** end
```

xStatus MediaChannels Call [n] Channel [n] Audio Protocol

Requires user role: ADMIN, USER

Shows the audio algorithm of the incoming or outgoing audio.

Value space of the result returned:

AACLD/G711A/G711Mu/G722/G7221/G7221C/G723_1/G728/G729/G729A/G729AB/Off/Opus

Example:

```
xStatus MediaChannels Call 27 Channel 327 Audio Protocol
*s MediaChannels Call 27 Channel 327 Audio Protocol: AACLD
** end
```

xStatus MediaChannels Call [n] Channel [n] Direction

Requires user role: ADMIN, USER

Shows the direction of the call.

Value space of the result returned:

Incoming/Outgoing

Example:

```
xStatus MediaChannels Call 27 Channel 327 Direction
*s MediaChannels Call 27 Channel 327 Direction: Incoming
** end
```



xStatus MediaChannels Call [n] Channel [n] Encryption

Requires user role: ADMIN, USER

Shows the encryption status for audio or video on the incoming or outgoing call.

Value space of the result returned:

On/Off

Example:

```
xStatus MediaChannels Call 27 Channel 327 Encryption
*s MediaChannels Call 27 Channel 327 Encryption: On
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat Bytes

Requires user role: ADMIN, USER

Shows the number of bytes for audio, video or data on the incoming or outgoing channel.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat Bytes
*s MediaChannels Call 27 Channel 327 NetStat Bytes: 496640
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat ChannelRate

Requires user role: ADMIN, USER

Shows the bandwidth for audio, video or data on the incoming or outgoing channel.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat ChannelRate
*s MediaChannels Call 27 Channel 327 NetStat ChannelRate: 128000
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat Jitter

Requires user role: ADMIN, USER

Shows the jitter for audio, video or data at the present moment on the incoming or outgoing channel, as specified by RFC 3550.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat Jitter
*s MediaChannels Call 27 Channel 327 NetStat Jitter: 2
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat LastIntervalLost

Requires user role: ADMIN, USER

Shows the number of packets lost for audio, video or data during the last interval on the incoming or outgoing channels.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat LastIntervalLost
*s MediaChannels Call 27 Channel 327 NetStat LastIntervalLost: 0
** end
```



xStatus MediaChannels Call [n] Channel [n] NetStat LastIntervalReceived

Requires user role: ADMIN, USER

Shows the number of packets received for audio, video or data during the last interval on the incoming or outgoing channels.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat LastIntervalReceived  
*s MediaChannels Call 27 Channel 327 NetStat LastIntervalReceived: 289  
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat Loss

Requires user role: ADMIN, USER

Shows the number of packets lost for audio, video or data on the incoming or outgoing channels.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat Loss  
*s MediaChannels Call 27 Channel 327 NetStat Loss: 0  
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat MaxJitter

Requires user role: ADMIN, USER

Shows the maximum jitter for audio, video or data that has been measured during last interval (about 5 seconds).

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat MaxJitter  
*s MediaChannels Call 27 Channel 327 NetStat MaxJitter: 2  
** end
```

xStatus MediaChannels Call [n] Channel [n] NetStat Packets

Requires user role: ADMIN, USER

Shows the number of packets that was received or sent for audio, video or data on the incoming or outgoing channels.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 NetStat Packets  
*s MediaChannels Call 27 Channel 327 NetStat Packets: 1551  
** end
```

xStatus MediaChannels Call [n] Channel [n] ParticipantId

Requires user role: ADMIN, USER

Shows the ID of the Active Control participant on the incoming audio or video channel.

Value space of the result returned:

String

Example:

```
xStatus MediaChannels Call 27 Channel 327 ParticipantId  
*s MediaChannels Call 27 Channel 327 ParticipantId: ""  
** end
```

**xStatus MediaChannels Call [n] Channel [n] Type**

Requires user role: ADMIN, USER

Shows the media type on the incoming or outgoing channel.

Value space of the result returned:

Audio/Video/Data

Example:

```
xStatus MediaChannels Call 27 Channel 327 Type
*s MediaChannels Call 27 Channel 327 Type: Audio
** end
```

xStatus MediaChannels Call [n] Channel [n] Video ChannelRole

Requires user role: ADMIN, USER

Shows the role of the incoming or outgoing video channel.

Value space of the result returned:

Main/Presentation

Example:

```
xStatus MediaChannels Call 27 Channel 327 Video ChannelRole
*s MediaChannels Call 27 Channel 327 Video ChannelRole: Main
** end
```

xStatus MediaChannels Call [n] Channel [n] Video FrameRate

Requires user role: ADMIN, USER

Shows the frame rate of the incoming or outgoing video channel.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 Video FrameRate
*s MediaChannels Call 27 Channel 327 Video FrameRate: 30
** end
```

xStatus MediaChannels Call [n] Channel [n] Video Protocol

Requires user role: ADMIN, USER

Shows the video algorithm of the incoming or outgoing video channel.

Value space of the result returned:

H261/H263/H263p/H263pp/H264/HEVC/JPEG/MP4V/Off

Example:

```
xStatus MediaChannels Call 27 Channel 327 Video Protocol
*s MediaChannels Call 27 Channel 327 Video Protocol: H264
** end
```

xStatus MediaChannels Call [n] Channel [n] Video ResolutionX

Requires user role: ADMIN, USER

Shows the width (resolution in direction X) of the incoming or outgoing video.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 Video ResolutionX
*s MediaChannels Call 27 Channel 327 Video ResolutionX: 1920
** end
```

xStatus MediaChannels Call [n] Channel [n] Video ResolutionY

Requires user role: ADMIN, USER

Shows the height (resolution in direction Y) of the incoming or outgoing video.

Value space of the result returned:

Integer

Example:

```
xStatus MediaChannels Call 27 Channel 327 Video ResolutionY
*s MediaChannels Call 27 Channel 327 Video ResolutionY: 1080
** end
```



Network status

xStatus Network [n] CDP Address

Requires user role: ADMIN, USER

Returns the first network address of both receiving and sending devices.

Value space of the result returned:

String

Example:

```
xStatus Network CDP Address
*s Network 1 CDP Address: "192.0.1.20"
** end
```

xStatus Network [n] CDP Capabilities

Requires user role: ADMIN, USER

Describes the functional capability for the switch in form of a device type. See documentation for CDP protocol for more information.

Value space of the result returned:

String

Example:

```
xStatus Network CDP Capabilities
*s Network 1 CDP Capabilities: "0x0029"
** end
```

xStatus Network [n] CDP DeviceId

Requires user role: ADMIN, USER

Identifies the name of the switch in form of a character string.

Value space of the result returned:

String

Example:

```
xStatus Network CDP DeviceId
*s Network 1 CDP DeviceId: "123456.company.com"
** end
```

xStatus Network [n] CDP Duplex

Requires user role: ADMIN, USER

Indicates the status (duplex configuration) of the CDP broadcast interface. Used by network operators to diagnose connectivity problems between adjacent network elements.

Value space of the result returned:

String

Example:

```
xStatus Network CDP Duplex
*s Network 1 CDP Duplex: "Full"
** end
```

xStatus Network [n] CDP Platform

Requires user role: ADMIN, USER

Returns the hardware platform name of the switch connected to the device.

Value space of the result returned:

String

Example:

```
xStatus Network CDP Platform
*s Network 1 CDP Platform: "cisco WS-C3750X-48P"
** end
```



xStatus Network [n] CDP PortID

Requires user role: ADMIN, USER

Returns the identification the switch uses of the port the device is connected to.

Value space of the result returned:

String

Example:

```
xStatus Network CDP PortID
*s Network 1 CDP PortID: "GigabitEthernet1/0/23"
** end
```

xStatus Network [n] CDP PrimaryMgmtAddress

Requires user role: ADMIN, USER

Returns the management address used to configure and monitor the switch the device is connected to.

Value space of the result returned:

String

Example:

```
xStatus Network CDP PrimaryMgmtAddress
*s Network 1 CDP PrimaryMgmtAddress: "10.1.1.2"
** end
```

xStatus Network [n] CDP SysName

Requires user role: ADMIN, USER

Returns the SysName as configured in the switch the device is connected to.

Value space of the result returned:

String

Example:

```
xStatus Network CDP SysName
*s Network 1 CDP SysName: ""
** end
```

xStatus Network [n] CDP SysObjectID

Requires user role: ADMIN, USER

Returns the SysObjectID as configured in the switch the device is connected to.

Value space of the result returned:

String

Example:

```
xStatus Network CDP SysObjectID
*s Network 1 CDP SysObjectID: ""
** end
```

xStatus Network [n] CDP Version

Requires user role: ADMIN, USER

Returns information about the software release version the switch is running.

Value space of the result returned:

String

Example:

```
xStatus Network 1 CDP Version
*s Network 1 CDP Version: "Cisco IOS Software, C3560CX Software (C3560CX-
UNIVERSALK9-M), Version 15.2(3)E, RELEASE SOFTWARE (fc4)*Technical Support:
http://www.cisco.com/techsupport*Copyright (c) 1986-2014 by Cisco Systems,
Inc.*Compiled Sun 07-Dec-14 13:15 by prod_rel_team"
** end
```



xStatus Network [n] CDP VoIPApplianceVlanID

Requires user role: ADMIN, USER

Identifies the VLAN used for VoIP traffic from the device to the switch. For more information see documentation of the IEEE 802.1Q protocol.

Value space of the result returned:

String

Example:

```
xStatus Network CDP VoIPApplianceVlanID
*s Network 1 CDP VoIPApplianceVlanID: "300"
** end
```

xStatus Network [n] CDP VTPMgmtDomain

Requires user role: ADMIN, USER

Returns the switch's configured VTP management domain name-string.

Value space of the result returned:

String

Example:

```
xStatus Network CDP VTPMgmtDomain
*s Network 1 CDP VTPMgmtDomain: "anyplace"
** end
```

xStatus Network [n] DNS Domain Name

Requires user role: ADMIN, USER

Shows the domain name.

Value space of the result returned:

String

Example:

```
xStatus Network 1 DNS Domain Name
*s Network 1 DNS Domain Name: "www.example.com www.example.int"
** end
```

xStatus Network [n] DNS Server [n] Address

Requires user role: ADMIN, USER

Shows the IP address of the DNS server.

Value space of the result returned:

String

Example:

```
xStatus Network 1 DNS Server 1. Address
*s Network 1 DNS Server 1 Address: "192.0.2.60"
** end
```

xStatus Network [n] Ethernet MacAddress

Requires user role: ADMIN, USER

Shows the MAC (Media Access Control) address for the Ethernet interface.

Value space of the result returned:

String

Example:

```
xStatus Network 1 Ethernet MacAddress
*s Network 1 Ethernet MacAddress: "00:50:60:02:FD:C7"
** end
```

xStatus Network [n] Ethernet Speed

Requires user role: ADMIN, USER

Shows the Ethernet speed in Mbps. The speed can be in full-duplex or half-duplex.

Value space of the result returned:

10half/10full/100half/100full/1000full

Example:

```
xStatus Network 1 Ethernet Speed
*s Network 1 Ethernet Speed: "100full"
** end
```



xStatus Network [n] IPv4 Address

Requires user role: ADMIN, USER

Shows the IPv4 address that uniquely identifies this device.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv4 Address  
*s Network 1 IPv4 Address: "192.0.2.149"  
** end
```

xStatus Network [n] IPv4 Gateway

Requires user role: ADMIN, USER

Shows the address of the IPv4 gateway.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv4 Gateway  
*s Network 1 IPv4 Gateway: "192.0.2.10"  
** end
```

xStatus Network [n] IPv4 SubnetMask

Requires user role: ADMIN, USER

Shows the subnet mask which determines which subnet an IPv4 address belongs to.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv4 SubnetMask  
*s Network 1 IPv4 SubnetMask: "255.255.255.0"  
** end
```

xStatus Network [n] IPv6 Address

Requires user role: ADMIN, USER

Shows the IPv6 address that uniquely identifies this device.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv6 Address  
*s Network 1 IPv6 Address: ""  
** end
```

xStatus Network [n] IPv6 Gateway

Requires user role: ADMIN, USER

Shows the address of the IPv6 gateway.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv6 Gateway  
*s Network 1 IPv6 Gateway: ""  
** end
```

xStatus Network [n] IPv6 LinkLocalAddress

Requires user role: ADMIN, USER

Shows the IPv6 link local address that is displayed on the primary user interface.

Value space of the result returned:

String

Example:

```
xStatus Network 1 IPv6 LinkLocalAddress  
*s Network 1 IPv6 LinkLocalAddress: "2001:DB8:0000:0000:0000:0000:0001"  
** end
```



xStatus Network [n] VLAN Voice VlanId

Requires user role: ADMIN, USER

The feedback shows the VLAN Voice ID.

Value space of the result returned:

Off/1..4094

Example:

```
xStatus Network 1 VLAN Voice VlanId  
*s Network 1 VLAN Voice VlanId: "Off"  
** end
```

NetworkServices status

xStatus NetworkServices NTP CurrentAddress

Requires user role: ADMIN, USER

Returns the address of the NTP server that is currently in use.

Value space of the result returned:

String

Example:

```
xStatus NetworkServices NTP CurrentAddress  
*s NetworkServices NTP CurrentAddress: "123.254.15.121"  
** end
```

xStatus NetworkServices NTP Server [n] Address

Requires user role: ADMIN, USER

Returns the address of the NTP server(s) the device is using.

Value space of the result returned:

String

Example:

```
xStatus NetworkServices NTP Address  
*s NetworkServices NTP Address: "12.104.193.12 64.104.222.16 144.254.15.121"  
** end
```



xStatus NetworkServices NTP Status

Requires user role: ADMIN, USER

Returns the status of the devices synchronizing with the NTP server.

Value space of the result returned:

Discarded/Synced/NotSynced/Unknown/Off

Example:

```
xStatus NetworkServices NTP Status
*s NetworkServices NTP Status: Synced
** end
```

xStatus NetworkServices UPnP Status

Requires user role: ADMIN, USER

Reports whether or not the UPnP service advertises the device's presence on the network. The advertisement permits a Touch controller to discover the device automatically, and you do not need to manually enter the device's IP address in order to pair the Touch controller.

Value space of the result returned:

Running/Stopped

Example:

```
xStatus NetworkServices UPnP Status
*s NetworkServices UPnP Status: Running
** end
```

Peripherals status

xStatus Peripherals ConnectedDevice [n] HardwareInfo

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows hardware information about connected device.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1007 HardwareInfo
*s Peripherals ConnectedDevice 1007 HardwareInfo: "1122330-0"
** end
```

xStatus Peripherals ConnectedDevice [n] ID

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the MAC-address of the connected device.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1007 ID
*s Peripherals ConnectedDevice 1007 ID: "00:10:20:20:be:21"
** end
```



xStatus Peripherals ConnectedDevice [n] Name

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the product name of connected device.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1007 Name
*s Peripherals ConnectedDevice 1007 Name: "Cisco TelePresence Touch"
** end
```

xStatus Peripherals ConnectedDevice [n] SerialNumber

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the serial number of a connected peripheral device, for example the Touch 10.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1001 SerialNumber
*s Peripherals ConnectedDevice 1001 SerialNumber: "ABC123..."
** end
```

xStatus Peripherals ConnectedDevice [n] SoftwareInfo

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows information of the software version running on the connected device.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1007 SoftwareInfo
*s Peripherals ConnectedDevice 1007 SoftwareInfo: "TI7.2.0"
** end
```

xStatus Peripherals ConnectedDevice [n] Status

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows peripheral devices that are currently connected to the video conferencing device.

Value space of the result returned:

Connected/ResponseTimedOut

Example:

```
xStatus Peripherals ConnectedDevice 1001 Status
*s Peripherals ConnectedDevice 1001 Status: Connected
** end
```

xStatus Peripherals ConnectedDevice [n] Type

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the peripheral types that are connected to the video conferencing device.

Note: The value space Camera only shows Precision 60 cameras.

Value space of the result returned:

Byod/Camera/ControlSystem/InputDevice/ISDNLink/Other/SpeakerTrack/TouchPanel

Example:

```
xStatus Peripherals ConnectedDevice 1001 Type
*s Peripherals ConnectedDevice 1001 Type: TouchPanel
** end
```

xStatus Peripherals ConnectedDevice [n] UpgradeFailureReason

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows that a connected device has failed during an upgrade and provides a reason.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1001 UpgradeFailureReason
*s Peripherals ConnectedDevice 1001 UpgradeFailureReason: ""
** end
```



xStatus Peripherals ConnectedDevice [n] UpgradeStatus

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the status of the previous software upgrade on the currently connected peripherals.

Value space of the result returned:

*Downloading/Failed/Installing/InstallationReady/None/Succeeded/Rebooting/Retrying/
Aborted/Paused*

Example:

```
xStatus Peripherals ConnectedDevice 1001 UpgradeStatus  
*s Peripherals ConnectedDevice 1001 UpgradeStatus: None  
** end
```

xStatus Peripherals ConnectedDevice [n] UpgradeURL

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the upgrade URL for the connected device.

Value space of the result returned:

String

Example:

```
xStatus Peripherals ConnectedDevice 1001 UpgradeURL  
*s Peripherals ConnectedDevice 1001 UpgradeURL: ""  
** end
```

Provisioning status

xStatus Provisioning CUCM Customization Checksum

Requires user role: ADMIN, USER

You can provision custom elements to multiple devices by using a customization template (a backup file). This status reports the checksum of the last customization template that has been uploaded to the device. Also see the xCommand Provisioning Service Fetch command.

Value space of the result returned:

String

Example:

```
xStatus Provisioning CUCM Customization Checksum  
*s Provisioning CUCM Customization Checksum: "633e163e2694b89ce37103b2448c36a..."  
** end
```

xStatus Provisioning CUCM ExtensionMobility Enabled

Requires user role: ADMIN, USER

Shows if Extension Mobility is enabled for a CUCM registered device.

Value space of the result returned:

True/False

Example:

```
xStatus Provisioning CUCM ExtensionMobility Enabled  
*s Provisioning CUCM ExtensionMobility Enabled: False  
** end
```



xStatus Provisioning CUCM ExtensionMobility LastLoggedInUserId

Requires user role: ADMIN, USER

Returns the user id that was last logged in to the device. Only in use if CUCM Extension Mobility is enabled, and CUCM is configured to remember the last logged in user on a device.

Value space of the result returned:

String

Example:

```
xStatus Provisioning CUCM ExtensionMobility LastLoggedInUserId  
*s Provisioning CUCM ExtensionMobility LastLoggedInUserId: "User 1"  
** end
```

xStatus Provisioning CUCM ExtensionMobility LoggedIn

Requires user role: ADMIN, USER

Shows if someone is logged in to Extension Mobility or not.

Value space of the result returned:

True/False

Example:

```
xStatus Provisioning CUCM ExtensionMobility LoggedIn  
*s Provisioning CUCM ExtensionMobility LoggedIn: False  
** end
```

xStatus Provisioning Software Current CompletedAt

Requires user role: ADMIN, USER

Shows date and time for when the current software upgrade was completed.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software Current CompletedAt  
*s Provisioning Software Current CompletedAt: "2011-06-07T07:20:03Z"  
** end
```

xStatus Provisioning Software Current URL

Requires user role: ADMIN, USER

Shows the URL that the current software was uploaded from.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software Current URL  
*s Provisioning Software Current URL: "http://.../s52020ce8_0_0.pkg"  
** end
```

xStatus Provisioning Software Current VersionId

Requires user role: ADMIN, USER

Shows the version ID of the current software.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software Current VersionId  
*s Provisioning Software Current VersionId: "s52020ce8_0_0.pkg"  
** end
```

xStatus Provisioning Software UpgradeStatus LastChange

Requires user role: ADMIN, USER

Shows the date and time for the latest software upgrade.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software UpgradeStatus LastChange  
*s Provisioning Software UpgradeStatus LastChange: "2011-06-07T07:20:03Z"  
** end
```



xStatus Provisioning Software UpgradeStatus Message

Requires user role: ADMIN, USER

Shows the system message for the software upgrade.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software UpgradeStatus Message
*s Provisioning Software UpgradeStatus Message: ""
** end
```

xStatus Provisioning Software UpgradeStatus Phase

Requires user role: ADMIN, USER

Shows the phase of the software upgrade.

Value space of the result returned:

*None/DownloadPending/FormingHierarchy/Downloading/DownloadPaused/DownloadDone/
Seeding/AboutToInstallUpgrade/Postponed/PeripheralsReady/UpgradingPeripherals/
Installing/InstallingPeripherals*

Example:

```
xStatus Provisioning Software UpgradeStatus Phase
*s Provisioning Software UpgradeStatus Phase: None
** end
```

xStatus Provisioning Software UpgradeStatus SessionId

Requires user role: ADMIN, USER

Shows the ID of the session for the software upgrade.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software UpgradeStatus SessionId
*s Provisioning Software UpgradeStatus SessionId: ""
** end
```

xStatus Provisioning Software UpgradeStatus Status

Requires user role: ADMIN, USER

Shows the status of the software upgrade.

Value space of the result returned:

None/InProgress/Failed/InstallationFailed/Succeeded

Example:

```
xStatus Provisioning Software UpgradeStatus Status
*s Provisioning Software UpgradeStatus Status: None
** end
```

xStatus Provisioning Software UpgradeStatus Urgency

Requires user role: ADMIN, USER

Shows how urgently the software needs to be upgraded.

Value space of the result returned:

Low/Medium/Critical

Example:

```
xStatus Provisioning Software UpgradeStatus Urgency
*s Provisioning Software UpgradeStatus Urgency: Low
** end
```

xStatus Provisioning Software UpgradeStatus URL

Requires user role: ADMIN, USER

Shows the URL that the new software currently is being uploaded and installed from.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software UpgradeStatus URL
*s Provisioning Software UpgradeStatus URL: "http://.../s52020ce8_0_0.pkg"
** end
```



xStatus Provisioning Software UpgradeStatus VersionId

Requires user role: ADMIN, USER

Shows the version ID of the software currently being uploaded and installed.

Value space of the result returned:

String

Example:

```
xStatus Provisioning Software UpgradeStatus VersionId  
*s Provisioning Software UpgradeStatus VersionId: "s52010ce8_0_0.pkg"  
** end
```

xStatus Provisioning Status

Requires user role: ADMIN, USER

Shows the status of the provisioning.

Value space of the result returned:

Failed/AuthenticationFailed/Provisioned/Idle/NeedConfig/ConfigError

Example:

```
xStatus Provisioning Status  
*s Provisioning Status: Provisioned  
** end
```

Proximity status

xStatus Proximity Services Availability

Requires user role: ADMIN, USER

Shows whether proximity services are available on the device.

Value space of the result returned:

Available, Deactivated, Disabled

Example:

```
xStatus Proximity Services Availability  
*s Proximity Services Availability: Disabled  
** end
```



RoomAnalytics status

xStatus RoomAnalytics AmbientNoise Level A

Requires user role: ADMIN, INTEGRATOR, USER

The device can be set up to estimate the stationary ambient noise level in the room (refer to the RoomAnalytics AmbientNoiseEstimation Mode setting). The result is reported in this status.

The value is an A-weighted decibel value (dBA). The value is only a relative value and should not be treated as an absolute SPL (Sound Pressure Level) value. Especially not for third-party microphones that the device doesn't know the sensitivity of.

Value space of the result returned:

Integer

Example:

```
xStatus RoomAnalytics AmbientNoise Level A
*s RoomAnalytics AmbientNoise Level A: 30
** end
```

xStatus RoomAnalytics PeopleCount Current

Requires user role: ADMIN, INTEGRATOR, USER

Shows the amount of people who are in the room by use of face detection. The call must have a duration of minimum two minutes in order to get a reliable average. Persons that have not faced the camera will not be counted. If there are objects or pictures in the room that can be detected as faces, these might be counted. The device will not keep record of who was in the room, only the average number of faces that were detected. When the device is in standby, or if the feature is turned off, the number returned is -1.

Value space of the result returned:

Integer

Example:

```
xStatus RoomAnalytics PeopleCount Current
*s RoomAnalytics PeopleCount Current: 2
** end
```

xStatus RoomAnalytics PeoplePresence

Requires user role: ADMIN, INTEGRATOR, USER

Shows if there are people present in the room or not. The feature is based on ultrasound. The device will not keep record of who was in the room, only whether or not there are people present in the room.

When someone enters the room, the status is updated immediately. After the room gets vacant, it may take up to two minutes for the status to change.

Value space of the result returned:

Yes/No/Unknown

Example:

```
xStatus RoomAnalytics PeoplePresence
*s RoomAnalytics PeoplePresence: No
** end
```

xStatus RoomAnalytics Sound Level A

Requires user role: ADMIN, INTEGRATOR, USER

If the RoomAnalytics AmbientNoiseEstimation Mode setting is On, the device will in addition to the ambient noise also measure the sound level in the room. The result is reported in this status every 10th second.

The value is an A-weighted averaged sound level in decibel (dBA). The value is only a relative value and should not be treated as an absolute SPL (Sound Pressure Level) value. Especially not for third-party microphones that the device doesn't know the sensitivity of.

Value space of the result returned:

Integer

Example:

```
xStatus RoomAnalytics Sound Level A
*s RoomAnalytics Sound Level A: 33
** end
```



RoomPreset status

xStatus RoomPreset [n] Defined

Requires user role: ADMIN, USER

Shows if a camera preset is stored at this position.

Value space of the result returned:

True/False

Example:

```
xStatus RoomPreset 1 Defined
*s RoomPreset 1 Defined: True
** end
```

xStatus RoomPreset [n] Description

Requires user role: ADMIN, USER

Lists the configured name for the specific preset.

Value space of the result returned:

String

Example:

```
xStatus RoomPreset 1 Description
*s RoomPreset 1 Description: "Zoom in"
** end
```

xStatus RoomPreset [n] Type

Requires user role: ADMIN, USER

Shows the camera preset type.

Value space of the result returned:

All/Camera

Example:

```
xStatus RoomPreset 1 Type
*s RoomPreset 1 Type: All
** end
```



Security status

xStatus Security FIPS Mode

Requires user role: ADMIN, USER

Shows the FIPS mode status.

Value space of the result returned:

On/Off

Example:

```
xStatus Security FIPS Mode
*s Security FIPS Mode: Off
** end
```

xStatus Security Persistency CallHistory

Requires user role: ADMIN, USER

Shows whether call history logging is set to persistent or non-persistent mode. Persistent is the default mode.

Value space of the result returned:

NonPersistent/Persistent

Example:

```
xStatus Security Persistency CallHistory
*s Security Persistency CallHistory: Persistent
** end
```

xStatus Security Persistency Configurations

Requires user role: ADMIN, USER

Shows whether all the device's configurations are set to persistent or non-persistent mode. Persistent is the default mode.

Value space of the result returned:

NonPersistent/Persistent

Example:

```
xStatus Security Persistency Configurations
*s Security Persistency Configurations: Persistent
** end
```

xStatus Security Persistency DHCP

Requires user role: ADMIN, USER

Shows whether DHCP logging is set to persistent or non-persistent mode. Persistent is the default mode.

Value space of the result returned:

NonPersistent/Persistent

Example:

```
xStatus Security Persistency DHCP
*s Security Persistency DHCP: Persistent
** end
```



xStatus Security Persistency InternalLogging

Requires user role: ADMIN, USER

Shows whether internal logging is set to persistent or non-persistent mode. Persistent is the default mode.

Value space of the result returned:

NonPersistent/Persistent

Example:

```
xStatus Security Persistency InternalLogging
*s Security Persistency InternalLogging: Persistent
** end
```

xStatus Security Persistency LocalPhonebook

Requires user role: ADMIN, USER

Shows whether local phone book is set to persistent or non-persistent mode. Persistent is the default mode.

Value space of the result returned:

NonPersistent/Persistent

Example:

```
xStatus Security Persistency LocalPhonebook
*s Security Persistency LocalPhonebook: Persistent
** end
```

SIP status

xStatus SIP AlternateURI Alias [n] URI

Requires user role: ADMIN, USER

Value space of the result returned:

String

Example:

```
xStatus SIP AlternateURI Alias
*s SIP AlternateURI Alias URI: ""
** end
```

xStatus SIP AlternateURI Primary [n] URI

Requires user role: ADMIN, USER

Value space of the result returned:

String

Example:

```
xStatus SIP AlternateURI Primary
*s SIP AlternateURI Primary URI: ""
** end
```

xStatus SIP Authentication

Requires user role: ADMIN, USER

Shows which authentication mechanism is used when registering to the SIP Proxy Server.

Value space of the result returned:

Digest/Off

Example:

```
xStatus SIP Authentication
*s SIP Authentication: Off
** end
```



xStatus SIP CallForward DisplayName

Requires user role: ADMIN, USER

Returns the URI that is displayed on the user interface for the forwarded call.

Value space of the result returned:

String

Example:

```
xStatus SIP CallForward DisplayName
*s SIP CallForward DisplayName: ""
** end
```

xStatus SIP CallForward Mode

Requires user role: ADMIN, USER

Indicates whether the call forward mode for SIP is set to on or off.

Value space of the result returned:

On/Off

Example:

```
xStatus SIP CallForward Mode
*s SIP CallForward Mode: Off
** end
```

xStatus SIP CallForward URI

Requires user role: ADMIN, USER

Indicates the address the incoming calls are directed to when call forward mode is set on.

Value space of the result returned:

String

Example:

```
xStatus SIP CallForward URI
*s SIP CallForward URI: ""
** end
```

xStatus SIP Mailbox MessagesWaiting

Requires user role: ADMIN, USER

Indicates how many new messages are in the mailbox.

Value space of the result returned:

Integer

Example:

```
xStatus SIP Mailbox MessagesWaiting
*s SIP Mailbox MessagesWaiting: 0
** end
```

xStatus SIP Mailbox URI

Requires user role: ADMIN, USER

Returns the URI for your SIP mailbox.

Value space of the result returned:

String

Example:

```
xStatus SIP Mailbox URI
*s SIP Mailbox URI: "12345678"
** end
```

xStatus SIP Proxy [n] Address

Requires user role: ADMIN, USER

Shows the address of the SIP Proxy that the device communicates with.

Value space of the result returned:

String

Example:

```
xStatus SIP Proxy 1 Address
*s SIP Proxy 1 Address: "192.0.2.50"
** end
```



xStatus SIP Proxy [n] Status

Requires user role: ADMIN, USER

Shows the status of the communication between the device and the SIP Proxy server.

Value space of the result returned:

Active/AuthenticationFailed/DNSFailed/Off/Timeout/UnableTCP/UnableTLS/Unknown

Example:

```
xStatus SIP Proxy 1 Status
*s SIP Proxy 1 Status: Active
** end
```

xStatus SIP Registration [n] Authentication

Requires user role: ADMIN, USER

Shows which authentication mechanism is used when registering to the SIP Proxy Server.

Value space of the result returned:

Digest/Off

Example:

```
xStatus SIP Registration 1 Authentication
*s SIP Registration 1 Authentication: Off
** end
```

xStatus SIP Registration [n] Reason

Requires user role: ADMIN, USER

Shows a message to explain the reason why the SIP registration failed.

Value space of the result returned:

String

Example:

```
xStatus SIP Registration 1 Reason
*s SIP Registration 1 Reason: "404 Not Found"
** end
```

xStatus SIP Registration [n] Status

Requires user role: ADMIN, USER

Shows the status of the registration to the SIP Proxy Server.

Value space of the result returned:

Deregister/Failed/Inactive/Registered/Registering

Example:

```
xStatus SIP Registration 1 Status
*s SIP Registration 1 Status: Registered
** end
```

xStatus SIP Registration [n] URI

Requires user role: ADMIN, USER

Shows the URI used for registration to the SIP Proxy server.

Value space of the result returned:

String

Example:

```
xStatus SIP Registration 1 URI
*s SIP Registration 1 URI: "firstname.lastname@company.com"
** end
```

xStatus SIP Secure

Requires user role: ADMIN, USER

Shows the encryption status of the signaling with the SIP Proxy server.

Value space of the result returned:

True/False

Example:

```
xStatus SIP Secure
*s SIP Secure: True
** end
```



xStatus SIP Verified

Requires user role: ADMIN, USER

Shows whether or not the SSL certificate of the server that the device tries to register to is included in the device's trusted CA-list. The server is typically a Cisco VCS or CUCM.

Value space of the result returned:

True/False

Example:

```
xStatus SIP Verified  
*s SIP Verified: False  
** end
```

Standby status

xStatus Standby State

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows whether the device is in standby mode or not.

Value space of the result returned:

Standby/EnteringStandby/Halfwake/Off

Example:

```
xStatus Standby State  
*s Standby State: Off  
** end
```



SystemUnit status

xStatus SystemUnit Hardware Module CompatibilityLevel

Requires user role: ADMIN, USER

The devices have different sets of compatibility levels. Please check the release note to find the compatibility levels and minimum software version required for your product.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Hardware Module CompatibilityLevel  
*s SystemUnit Hardware Module CompatibilityLevel: 1  
** end
```

xStatus SystemUnit Hardware Module SerialNumber

Requires user role: ADMIN, USER

Shows the serial number of the hardware module in the device.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Hardware MainBoard SerialNumber  
*s SystemUnit Hardware MainBoard SerialNumber: "FOC99999999"  
** end
```

xStatus SystemUnit Hardware Monitoring Fan [n] Status

Requires user role: ADMIN, USER

The feedback shows the speed (rpm) for the specified fan.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Hardware Monitoring Fan 1 Status  
*s SystemUnit Hardware Monitoring Fan 1 Status: "locked on 1096 rpm"  
** end
```

xStatus SystemUnit Hardware Monitoring Temperature Status

Requires user role: ADMIN, INTEGRATOR, USER

Shows the current temperature alarm level. "High" is meant to raise attention to the temperature trend since the operating temperature is higher than normal. At "Critical" level the device will shut down processes and processors to prevent any damage to the device. To avoid high operating temperatures, make sure the device is operating in a ventilated environment.

Value space of the result returned:

Unknown, Normal, High, Critical

Example:

```
xStatus SystemUnit Hardware Monitoring Temperature Status  
*s SystemUnit Hardware Monitoring Temperature Status: Normal  
** end
```



xStatus SystemUnit Notifications Notification [n] Text

Requires user role: ADMIN, USER

Lists text related to important system notifications. Notifications are issued e.g. when a device was rebooted because of a software upgrade, or when a factory reset has been performed.

All the notifications can be removed from the list by issuing the xCommand SystemUnit Notifications RemoveAll command.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Notifications Notification 1 Text
*s SystemUnit Notifications Notification 1 Text: "OK"
** end
```

xStatus SystemUnit Notifications Notification [n] Type

Requires user role: ADMIN, USER

Lists the system notification types. Notifications are issued e.g. when a device is rebooted because of a software upgrade, or when a factory reset is performed.

All the notifications can be removed from the list by issuing the xCommand SystemUnit Notifications RemoveAll command.

Value space of the result returned:

SoftwareUpgradeOK/SoftwareUpgradeFailed/RebootRequired/Other

Example:

```
xStatus SystemUnit Notifications Notification 1 Type
*s SystemUnit Notifications Notification 1 Type: SoftwareUpgradeOK
** end
```

xStatus SystemUnit ProductId

Requires user role: ADMIN, USER

Shows the product identity.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit ProductId
*s SystemUnit ProductId: "Cisco TelePresence SX80"
** end
```

xStatus SystemUnit ProductPlatform

Requires user role: ADMIN, USER

Shows the product platform.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit ProductPlatform
*s SystemUnit ProductPlatform: "SX80"
** end
```

xStatus SystemUnit ProductType

Requires user role: ADMIN, USER

Shows the product type.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit ProductType
*s SystemUnit ProductType: "Cisco Codec"
** end
```



xStatus SystemUnit Software DisplayName

Requires user role: ADMIN, USER

Shows the name of the software that is installed on the device, as it is displayed in the UI.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Software DisplayName  
*s SystemUnit Software DisplayName: "Display Name"  
** end
```

xStatus SystemUnit Software Name

Requires user role: ADMIN, USER

Shows the name of the software that is installed on the device.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Software Name  
*s SystemUnit Software Name: "s53200"  
** end
```

xStatus SystemUnit Software OptionKeys Encryption

Requires user role: ADMIN, USER

Shows if the device has the option key or the software installed that supports the encryption functionality. The option key is available for SX10, SX80, and the MX series.

Value space of the result returned:

False/True

Example:

```
xStatus SystemUnit Software OptionKeys Encryption  
*s SystemUnit Software OptionKeys Encryption: "true"  
** end
```

xStatus SystemUnit Software OptionKeys MultiSite

Requires user role: ADMIN, USER

Shows if the device has the option key installed that supports the MultiSite functionality.

Value space of the result returned:

False/True/NotApplicable

Example:

```
xStatus SystemUnit Software OptionKeys MultiSite  
*s SystemUnit Software OptionKeys MultiSite: "true"  
** end
```

xStatus SystemUnit Software OptionKeys RemoteMonitoring

Requires user role: ADMIN, USER

Shows whether the device has the remote monitoring option key installed. Remote monitoring option key enables snapshots from the web interface, and from a remote paired Touch 10.

Value space of the result returned:

False/True

Example:

```
xStatus SystemUnit Software OptionKeys RemoteMonitoring  
*s SystemUnit Software OptionKeys RemoteMonitoring: "true"  
** end
```

xStatus SystemUnit Software ReleaseDate

Requires user role: ADMIN, USER

Shows the release date of the software installed on the device.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Software ReleaseDate  
*s SystemUnit Software ReleaseDate: "2015-05-05"  
** end
```



xStatus SystemUnit Software Version

Requires user role: ADMIN, USER

Shows the software version installed on the device.

Value space of the result returned:

String

Example:

```
xStatus SystemUnit Software Version
*s SystemUnit Software Version: "CE8.0.0"
** end
```

xStatus SystemUnit State NumberOfActiveCalls

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the number of active calls.

Value space of the result returned:

0..5

Example:

```
xStatus SystemUnit State NumberOfActiveCalls
*s SystemUnit State NumberOfActiveCalls: 0
** end
```

xStatus SystemUnit State NumberOfInProgressCalls

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Shows the number of calls in progress.

Value space of the result returned:

0..5

Example:

```
xStatus SystemUnit State NumberOfInProgressCalls
*s SystemUnit State NumberOfInProgressCalls: 0
** end
```

xStatus SystemUnit State NumberOfSuspendedCalls

Requires user role: ADMIN, USER

Shows the number of suspended calls.

Value space of the result returned:

0..5

Example:

```
xStatus SystemUnit State NumberOfSuspendedCalls
*s SystemUnit State NumberOfSuspendedCalls: 0
** end
```

xStatus SystemUnit Uptime

Requires user role: ADMIN, USER

Shows the number of seconds since the last restart of the device.

Value space of the result returned:

Integer

Example:

```
xStatus SystemUnit Uptime
*s SystemUnit Uptime: 597095
** end
```



Time status

xStatus Time SystemTime

Requires user role: ADMIN, INTEGRATOR, USER

Returns the date and time set on the device.

Value space of the result returned:

String

Example:

```
xStatus Time SystemTime  
*s Time SystemTime: "2014-04-25T10:04:03Z"  
** end
```

UserInterface status

xStatus UserInterface ContactInfo ContactMethod [n] Number

Requires user role: ADMIN, USER

Returns the device's active contact information. This address is used to reach this device.

Value space of the result returned:

String

Example:

```
xStatus UserInterface ContactInfo ContactMethod Number  
*s UserInterface ContactInfo ContactMethod 1 Number: "12345678"  
** end
```

xStatus UserInterface ContactInfo Name

Requires user role: ADMIN, USER

Returns the device's active contact name. The result depends on which protocol, if any, the device is registered on. The automatically set contact name may have been overridden with the command xConfiguration UserInterface ContactInfo Type. This results in a diagnostics warning about contact mismatch.

Value space of the result returned:

String

Example:

```
xStatus UserInterface ContactInfo Name  
*s UserInterface ContactInfo Name: "MySystem"  
** end
```



xStatus UserInterface Extensions Widget [n] Value

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Returns the value for a widget. Widgets are used in custom panels, for example in-room controls, that are added to the user interface. The value space depends on the widget type. The value is an empty string until a value is set with the UserInterface Extensions Widget SetValue command.

Value space of the result returned:

String

xStatus UserInterface Extensions Widget [n] WidgetId

Requires user role: ADMIN, INTEGRATOR, USER, ROOMCONTROL

Returns the unique identifier for a widget. Widgets are used in custom panels, for example in-room controls, that are added to the user interface.

Value space of the result returned:

String

xStatus UserInterface Features Call End

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the default End call button is removed from the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface Features Call End
*s UserInterface Features Call End: Visible
** end
```

xStatus UserInterface Features MidCallControls

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the default Hold, Transfer, and Resume in-call buttons are removed from the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface Features MidCallControls
*s UserInterface Features MidCallControls: Visible
** end
```

xStatus UserInterface Features Call Start

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the default Call button and the Add participant button are removed from the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface Features Call Start
*s UserInterface Features Call Start: Visible
** end
```



xStatus UserInterface Features Share Start

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the default buttons and other UI elements for sharing and previewing content, both in call and out of call, are removed from the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface Features Share Start
*s UserInterface Features Share Start: Visible
** end
```

xStatus UserInterface Features Whiteboard Start

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the default Whiteboard button is removed from the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface Features Whiteboard Start
*s UserInterface Features Whiteboard Start: Visible
** end
```

xStatus UserInterface SettingsMenu Visibility

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the device name (or contact information) in the upper left corner of the user interface, and the associated drop down menu and Settings panel, are shown in the user interface.

Value space of the result returned:

Visible/Hidden

Example:

```
xStatus UserInterface SettingsMenu Visibility
*s UserInterface SettingsMenu Visibility: Visible
** end
```



Video status

xStatus Video ActiveSpeaker PIPPosition

Requires user role: ADMIN, INTEGRATOR, USER

Shows the position of the active speaker's image on the screen.

Value space of the result returned:

UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Example:

```
xStatus Video ActiveSpeaker PIPPosition
*s Video PIP ActiveSpeaker Position: UpperCenter
** end
```

xStatus Video Input Connector [n] Connected

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether something is connected to the specified connector. Not all connections can be detected.

Value space of the result returned:

False/True/Unknown

Example:

```
xStatus Video Input Connector 1 Connected
*s Video Input Connector 1 Connected: True
** end
```

xStatus Video Input Connector [n] ConnectedDevice CEC [n] DeviceType

Requires user role: ADMIN, INTEGRATOR, USER

Shows what type of input device is connected.

Value space of the result returned:

String

Example:

```
xStatus Video Input Connector 2 ConnectedDevice CEC 5 DeviceType
*s Video Input Connector 2 ConnectedDevice CEC 5 DeviceType: "Playback"
** end
```

xStatus Video Input Connector [n] ConnectedDevice CEC [n] LogicalAddress

Requires user role: ADMIN, INTEGRATOR, USER

Shows the CEC logical address of the connected input device. The address is fixed at 0.

Value space of the result returned:

Integer

Example:

```
xStatus Video Input Connector 1 ConnectedDevice CEC 1 LogicalAddress
*s Video Input Connector 1 ConnectedDevice CEC 1 LogicalAddress: 0
** end
```

xStatus Video Input Connector [n] ConnectedDevice CEC [n] Name

Requires user role: ADMIN, INTEGRATOR, USER

Shows the name of the connected input device.

Value space of the result returned:

String

Example:

```
xStatus Video Input Connector 2 ConnectedDevice CEC 5 Name
*s Video Input Connector 2 ConnectedDevice CEC 5 Name: "Device-2"
** end
```



xStatus Video Input Connector [n] ConnectedDevice CEC [n] PowerStatus

Requires user role: ADMIN, INTEGRATOR, USER

Shows the state of the CEC enabled device connected to the HDMI input.

Value space of the result returned:

String

Example:

```
xStatus Video Input Connector 2 ConnectedDevice CEC 5 PowerStatus  
*s Video Input Connector 2 ConnectedDevice CEC 5 PowerStatus: "Standby"  
** end
```

xStatus Video Input Connector [n] ConnectedDevice CEC [n] VendorId

Requires user role: ADMIN, INTEGRATOR, USER

Shows the vendor ID for the connected input device.

Value space of the result returned:

String

Example:

```
xStatus Video Input Connector 2 ConnectedDevice CEC 5 VendorId  
*s Video Input Connector 2 ConnectedDevice CEC 5 VendorId: "20576"  
** end
```

xStatus Video Input Connector [n] SignalState

Requires user role: ADMIN, INTEGRATOR, USER

Shows the signal state for the specified input.

Value space of the result returned:

OK/Unknown/Unsupported

Example:

```
xStatus Video Input Connector 1 SignalState  
*s Video Input Connector 1 SignalState: OK  
** end
```

xStatus Video Input Connector [n] SourceId

Requires user role: ADMIN, INTEGRATOR, USER

Shows the identifier of the input source that the connector is associated with.

Value space of the result returned:

Integer

Example:

```
xStatus Video Input Connector 1 SourceId  
*s Video Input Connector 1 SourceId: 1  
** end
```

xStatus Video Input Connector [n] Type

Requires user role: ADMIN, INTEGRATOR, USER

Shows which connector type it is.

Value space of the result returned:

Camera/Composite/DVI/3G-SDI/HD-SDI/HDMI/USB/Unknown/VGA/YC/YPbPr/USBC-DP

Example:

```
xStatus Video Input Connector 1 Type  
*s Video Input Connector 1 Type: HDMI  
** end
```

xStatus Video Input MainVideoMute

Requires user role: ADMIN, INTEGRATOR, USER

Indicates whether sending of main video has been stopped by using the Video Input MainVideo Mute command (or, if available, the "Turn video off" button on the user interface).

Value space of the result returned:

On/Off

Example:

```
xStatus Video Input MainVideoMute  
*s Video Input MainVideoMute: Off  
** end
```



xStatus Video Input MainVideoSource

Requires user role: ADMIN, USER

Returns the local video input currently used as the main source. The value Composed is returned if the main source is composed of more than one local input. The default main video source is set with the xConfiguration Video DefaultMainSource command. It can be changed using xCommand Video Input SetMainVideoSource (this command is not applicable to SX10, DX70, and DX80).

Value space of the result returned:

1/2/3/4/5/6/Composed

Example:

```
xStatus Video Input MainVideoSource
*s Video Input MainVideoSource: 1
** end
```

xStatus Video Input Source [n] ConnectorId

Requires user role: ADMIN, INTEGRATOR, USER

Shows the identifier of the connector that is associated with the input source.

Value space of the result returned:

Integer

Example:

```
xStatus Video Input Source 1 ConnectorId
*s Video Input Source 1 ConnectorId: 1
** end
```

xStatus Video Input Source [n] FormatStatus

Requires user role: ADMIN, INTEGRATOR, USER

Shows the resolution format status for the video input source.

Value space of the result returned:

Ok/OutOfRange/NotFound/Interlaced/Error/Unknown

Example:

```
xStatus Video Input Source 1 FormatStatus
*s Video Input Source 1 Resolution FormatStatus: Ok
** end
```

xStatus Video Input Source [n] FormatType

Requires user role: ADMIN, INTEGRATOR, USER

Shows the resolution format type for the video input source.

Value space of the result returned:

*Unknown/AnalogCVTBlanking/AnalogCVTReducedBlanking/AnalogGTFDefault/
AnalogGTFSecondary/AnalogDiscreteTiming/AnalogDMTBlanking/AnalogCEABlanking/Digital*

Example:

```
xStatus Video Input Source 1 FormatType
*s Video Input Source 1 Resolution FormatType: Digital
** end
```

xStatus Video Input Source [n] MediaChannelId

Requires user role: ADMIN, USER

For internal use only.

Value space of the result returned:

Integer

Example:

```
xStatus Video Input Source MediaChannelId
*s Video Input Source 1 MediaChannelId: 2
*s Video Input Source 2 MediaChannelId: 3
** end
```



xStatus Video Input Source [n] Resolution Height

Requires user role: ADMIN, INTEGRATOR, USER

Shows the resolution height (in pixels) for the video input source.

Value space of the result returned:

0..3000

Example:

```
xStatus Video Input Source 1 Resolution Height
*s Video Input Source 1 Resolution Height: 1080
** end
```

xStatus Video Input Source [n] Resolution RefreshRate

Requires user role: ADMIN, INTEGRATOR, USER

Shows the resolution refresh rate (Hz) for the video input source.

Value space of the result returned:

0..300

Example:

```
xStatus Video Input Source 1 Resolution RefreshRate
*s Video Input Source 1 Resolution RefreshRate: 50
** end
```

xStatus Video Input Source [n] Resolution Width

Requires user role: ADMIN, INTEGRATOR, USER

Shows the resolution width (in pixels) for the video input source.

Value space of the result returned:

0..4000

Example:

```
xStatus Video Input Source 1 Resolution Width
*s Video Input Source 1 Resolution Width: 1920
** end
```

xStatus Video Layout LayoutFamily Local

Requires user role: ADMIN, USER

Shows the local screen layout family.

Value space of the result returned:

String

Example:

```
xStatus Video Layout LayoutFamily Local
*s Video Layout LayoutFamily Local: "equal"
** end
```

xStatus Video Layout LayoutFamily Remote

Requires user role: ADMIN, USER

Shows the remote screen layout family.

Value space of the result returned:

String

Example:

```
xStatus Video Layout LayoutFamily Remote
*s Video Layout LayoutFamily Remote: "equal"
** end
```

xStatus Video Monitors

Requires user role: ADMIN, USER

Returns the monitor layout mode.

Value space of the result returned:

Single/Dual/DualPresentationOnly/Triple/TriplePresentationOnly

Example:

```
xStatus Video Monitors
*s Video Monitors: Single
** end
```



xStatus Video Output Connector [n] Connected

Requires user role: ADMIN, INTEGRATOR, USER

Describes whether a device (for example a display) is connected to the output connector or not. When a display enters standby mode, the video conferencing device may not be able to detect it. The connector status will then return False/Unknown even if the display is physically connected.

Value space of the result returned:

True/False

Example:

```
xStatus Video Output Connector 1 Connected
*s Video Output Connector 1 Connected: True
** end
```

xStatus Video Output Connector [n] ConnectedDevice CEC [n] DeviceType

Requires user role: ADMIN, INTEGRATOR, USER

Shows the type of CEC enabled device connected to the HDMI output that the video conferencing device has detected.

This information is only available when the device connected to the HDMI output has the CEC feature configured on and the video conferencing device has the configuration xConfiguration Video Output Connector [n] CEC Mode set to on.

Value space of the result returned:

Unknown/TV/Reserved/Recorder/Tuner/Playback/Audio

Example:

```
xStatus Video Output Connector 1 ConnectedDevice CEC DeviceType
*s Video Output Connector 1 ConnectedDevice CEC DeviceType: TV
** end
```

xStatus Video Output Connector [n] ConnectedDevice CEC [n] LogicalAddress

Requires user role: ADMIN, INTEGRATOR, USER

Shows the CEC logical address of the device.

Value space of the result returned:

Integer

Example:

```
xStatus Video Output Connector 1 ConnectedDevice CEC 1 LogicalAddress
*s Video Output Connector 1 ConnectedDevice CEC 1 LogicalAddress: 4
** end
```

xStatus Video Output Connector [n] ConnectedDevice CEC [n] Name

Requires user role: ADMIN, INTEGRATOR, USER

Returns the name of the connected device.

Value space of the result returned:

String

Example:

```
xStatus Video Output Connector 1 ConnectedDevice CEC Name
*s Video Output Connector 1 ConnectedDevice CEC 1 Name: "LG SIGNAGE TV"
** end
```



xStatus Video Output Connector [n] ConnectedDevice CEC [n] PowerStatus

Requires user role: ADMIN, INTEGRATOR, USER

Shows the state of the CEC enabled device connected to the HDMI output.

This information is only available when the device connected to the HDMI output has the CEC feature configured on and the video conferencing device has the configuration xConfiguration Video Output Connector CEC Mode set to on.

Value space of the result returned:

Unknown/Ok/In progress/Failed to power on/Failed to standby

Example:

```
xStatus Video Output Connector 1 ConnectedDevice CEC PowerStatus
*s Video Output Connector 1 ConnectedDevice CEC PowerStatus: Ok
** end
```

xStatus Video Output Connector [n] ConnectedDevice CEC [n] VendorId

Requires user role: ADMIN, INTEGRATOR, USER

Returns the vendor ID for the connected device.

Value space of the result returned:

String

Example:

```
xStatus Video Output Connector 1 ConnectedDevice CEC VendorId
*s Video Output Connector 1 ConnectedDevice CEC 1 VendorId: "57489"
** end
```

xStatus Video Output Connector [n] ConnectedDevice Name

Requires user role: ADMIN, INTEGRATOR, USER

Shows the name of the monitor connected to the HDMI port as defined in the monitors EDID.

Value space of the result returned:

String

Example:

```
xStatus Video Output Connector 1 ConnectedDevice Name
*s Video Output Connector 1 ConnectedDevice Name: "G2420HDBL"
** end
```

xStatus Video Output Connector [n] ConnectedDevice PreferredFormat

Requires user role: ADMIN, INTEGRATOR, USER

Shows the preferred input format of the monitor connected to the HDMI port as defined in the monitors EDID. This is not necessarily the format the video conferencing device is sending out.

Value space of the result returned:

String

Example:

```
xStatus Video Output Connector 1 ConnectedDevice PreferredFormat
*s Video Output Connector 1 ConnectedDevice PreferredFormat: "1920x1080@60Hz"
** end
```

xStatus Video Output Connector [n] ConnectedDevice ScreenSize

Requires user role: ADMIN, USER

Shows the screen size of the connected device in inches. If this information is not available, the default value is set to 0.

Value space of the result returned:

Integer

Example:

```
xStatus Video Output Connector 1 ConnectedDevice ScreenSize
*s Video Output Connector 1 ConnectedDevice ScreenSize: 55
** end
```



xStatus Video Output Connector [n] MonitorRole

Requires user role: ADMIN, USER

Describes which video stream is shown on the device that is connected to the video output connector.

Value space of the result returned:

First/Second/Third/PresentationOnly/Recorder

Example:

```
xStatus Video Output Connector 1 MonitorRole  
*s Video Output Connector 1 MonitorRole: First  
** end
```

xStatus Video Output Connector [n] Resolution Height

Requires user role: ADMIN, USER

Shows the resolution height (in pixels) for the video output connector.

Value space of the result returned:

120..3000

Example:

```
xStatus Video Output Connector 1 Resolution Height  
*s Video Output Connector 1 Resolution Height: 1080  
** en
```

xStatus Video Output Connector [n] Resolution RefreshRate

Requires user role: ADMIN, USER

Shows the resolution refresh rate (Hz) for the video output connector.

Value space of the result returned:

1..300

Example:

```
xStatus Video Output Connector 1 Resolution RefreshRate  
*s Video Output Connector 1 Resolution RefreshRate: 60  
** end
```

xStatus Video Output Connector [n] Resolution Width

Requires user role: ADMIN, USER

Shows the resolution width (in pixels) for the video output connector.

Value space of the result returned:

176..4000

Example:

```
xStatus Video Output Connector 1 Resolution Width  
*s Video Output Connector 1 Resolution Width: 1920  
** end
```

xStatus Video Output Connector [n] Type

Requires user role: ADMIN, USER

Shows the type of connector.

Value space of the result returned:

HDMI/DVI

Example:

```
xStatus Video Output Connector 1 Type  
*s Video Output Connector 1 Type: HDMI  
** end
```

xStatus Video Output Monitor [n] Backlight

Requires user role: ADMIN, USER

Returns the monitors backlight level, that has been set with xCommand Video Output Monitor Backlight Set.

Value space of the result returned:

Integer

Example:

```
xStatus Video Output Monitor 1 Backlight  
*s Video Output Monitor 1 Backlight: 80  
** end
```



xStatus Video Output Monitor [n] FirmwareVersion

Requires user role: ADMIN, USER

Shows the firmware version of the monitor. This status field is only populated when connecting with a supported LG monitor.

Value space of the result returned:

String

Example:

```
xStatus Video Output Monitor 1 FirmwareVersion
*s Video Output Monitor 1 FirmwareVersion: ""
** end
```

xStatus Video Output Monitor [n] ModelName

Requires user role: ADMIN, USER

Shows the model name of the monitor. This status field is only populated when connecting with a supported LG monitor.

Value space of the result returned:

String

Example:

```
xStatus Video Output Monitor 1 ModelName
*s Video Output Monitor 1 ModelName: ""
** end
```

xStatus Video Output Monitor [n] Position

Requires user role: ADMIN, USER

Shows whether the monitor is positioned on the left or the right. Applicable for dual screen devices only.

Value space of the result returned:

Left/Right

Example:

```
xStatus Video Output Monitor 1 Position
*s Video Output Monitor 1 Position: Left
** end
```

xStatus Video Output Monitor [n] SerialNumber

Requires user role: ADMIN, USER

Shows the serial number of the monitor. This status field is only populated when connecting with a supported LG monitor.

Value space of the result returned:

String

Example:

```
xStatus Video Output Monitor 1 SerialNumber
*s Video Output Monitor 1 SerialNumber: ""
** end
```



xStatus Video Output Monitor [n] Temperature

Requires user role: ADMIN, USER

Shows the temperature of the monitor. This status field is only populated when connecting with a supported LG monitor.

Value space of the result returned:

Normal/High

Example:

```
xStatus Video Output Monitor 1 Temperature
*s Video Output Monitor 1 Temperature: Normal
** end
```

xStatus Video Presentation PIPPosition

Requires user role: ADMIN, USER

Shows the position of the presentation image on the screen.

Value space of the result returned:

UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Example:

```
xStatus Video Presentation PIPPosition
*s Video PIP Presentation Position: CenterLeft
** end
```

xStatus Video Selfview FullscreenMode

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether selfview is set on full screen mode or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Video Selfview FullscreenMode
*s Video Selfview FullscreenMode: Off
** end
```

xStatus Video Selfview Mode

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether selfview mode is set on or not.

Value space of the result returned:

On/Off

Example:

```
xStatus Video Selfview Mode
*s Video Selfview Mode: Off
** end
```

xStatus Video Selfview OnMonitorRole

Requires user role: ADMIN, INTEGRATOR, USER

Identifies which monitor(s) contains the selfview, if present.

Value space of the result returned:

First/Second/Third

Example:

```
xStatus Video Selfview OnMonitorRole
*s Video Selfview OnMonitorRole: First
** end
```

xStatus Video Selfview PIPPosition

Requires user role: ADMIN, INTEGRATOR, USER

Shows the position of the selfview image on the screen.

Value space of the result returned:

UpperLeft/UpperCenter/UpperRight/CenterLeft/CenterRight/LowerLeft/LowerRight

Example:

```
xStatus Video Selfview PIPPosition
*s Video Selfview PIPPosition: LowerRight
** end
```



WebEngine status

xStatus WebEngine Features Signage

Requires user role: ADMIN, USER

Reports whether or not the digital signage feature is enabled. It is enabled (On) only when both the WebEngine Mode and Standby Signage Mode settings are On.

Value space of the result returned:

On/Off

Example:

```
xStatus WebEngine Features Signage
*s WebEngine Features Signage: On
** end
```

xStatus WebEngine Features WebEngine

Requires user role: ADMIN, USER

Reports whether or not the web engine is enabled. It is enabled (On) when the WebEngine Mode setting is On.

Value space of the result returned:

On/Off

Example:

```
xStatus WebEngine Features WebEngine
*s WebEngine Features WebEngine: On
** end
```

Webex status

xStatus Webex Status

Requires user role: ADMIN, USER

Reports the status of the connection between the device and the Cisco Webex cloud service. If the could service is up and running, the status reports Registered. If the device is registered to an on-premise service such as CUCM or VCS, the status reports Disabled.

Value space of the result returned:

Disabled/Error/Registered/Registering/Stopped

Example:

```
xStatus Webex Status
*s Webex Status: Disabled
** end
```





Chapter 6

Appendices



Startup scripts

You can add one or more startup scripts to the device. A startup script contains commands (xCommand) and configurations (xConfiguration) that will be executed as part of the start up procedure every time the device boots. A few commands and configurations cannot be placed in a startup script, e.g. xCommand SystemUnit Boot.

Use the device's web interface to create and manage startup scripts.

Read more about the web interface and startup scripts in the *Administrator guide* for your product.

The SystemTools commands

NOTE: The systemtools commands are used for administrative control of the device and are only available from a command line interface. Systemtools should not be used to program the device.

Required parameters in angle brackets: <text>

Optional parameters in square brackets: [text]

To get an overview of the supported commands type "systemtools ?".

Example:

```
systemtools ?
rootsettings
selectsw
whoami
license
network
ntp
passwd
pki
ps
securitysettings
securitystatus
sudo
idefixversion
pairing
```

To see the usage of the commands add a question mark after the command.

Example:

```
systemtools network ?
usage: network ping <hostname> | traceroute
<hostname> | netstat | addrs | ifconfig
```

systemtools idefixversion (Not for DX70 and DX80)

Returns the software version the connected Touch controller should have. Used when downgrading to TC7.3 or earlier.

systemtools license list

Lists all the licenses for the device.

systemtools license show <name>

Shows the content of a license file, defined by the name.

<name>: The name of the license file.

systemtools network ping <hostname>

Network debug command.

<hostname>: The IP-address or URL of the host.

systemtools network traceroute <hostname>

Network debug command.

<hostname>: The IP-address or URL of the host.

systemtools network netstat

Network debug command.

systemtools network addrs

Shows the device's IP-addresses.

systemtools network ifconfig

Network debug command.

systemtools ntp

Shows the NTP status.

systemtools pairing unpair

Remove association with Cisco Touch 10 controller.

systemtools passwd

Change the password for the logged in user.

systemtools pki list

Lists the device certificate and CA list if they exist.

systemtools pki delete <cert-name>

Delete the device certificate and CA list if they exist.

<cert-name>: The name of the certificate.

systemtools securitysettings jitc

Set up security requirements so they meet JTIC.

Set password and PIN policies enforced on the device.

systemtools securitysettings isjtic

Check if the current settings are JTIC compliant.

systemtools securitysettings default

Revert to default security settings.

systemtools securitysettings ask

Query for the separate configurations. When issuing this command you can see each policy separately.

- Press enter to keep the current value.
- Enter a number and press enter to change the given policy.
- The default value "0" indicates no restrictions.

Max failed login attempts [0]?

- Number of failed logins until a user is set inactive.



Suspend-time after max failed login attempts (minutes) [0]?

- Number of minutes the user is set inactive after maximum failed login attempts have been exceeded.

Max simultaneous sessions total [0]?

- Maximum number of users that can be logged in simultaneous to web and maximum number of users that can be logged in simultaneous to ssh/Telnet.

Max simultaneous sessions per user [0]?

- Maximum number of simultaneous sessions per user.

Number of passwords to remember [0]?

- Number of previous passwords that the new password must differ from.

Number of PINs to remember [0]?

- Number of previous PINs that the new PIN must differ from.

Maximum time between password renewals (days) [0]?

- If the user has not changed the password within the renewal time the user will be set inactive.

Minimum time between password renewals (hours) [0]?

- The user can only change password once within this limit.

Maximum time between PIN renewals (days) [0]?

- If the user has not changed the PIN within the renewal time the user will be set inactive.

Minimum time between PIN renewals (hours) [0]?

- The user can only change PIN once within this limit.

Maximum time between logins (days) [0]?

- If the user has not logged in within this limit the user will be set inactive.

Max consecutive equal digits in PINs [0]?

- Maximum consecutive equal digits in PINs.

Minimum number of digits in PINs [0]?

- Minimum number of digits in PINs.

Maximum number of digits in PINs [0]?

- Maximum number of digits in PINs.

Max consecutive identical characters in passwords [0]?

- Maximum consecutive identical characters in passwords.

Minimum number of characters in passwords [0]?

- Minimum number of characters in passwords.

Maximum number of characters in passwords [0]?

- Maximum number of characters in passwords.

Minimum number of lower-case letters in passwords [0]?

- Minimum number of lower-case letters in passwords.

Minimum number of upper-case letters in passwords [0]?

- Minimum number of upper-case letters in passwords.

Minimum number of numerical characters in passwords [0]?

- Minimum number of numerical characters in passwords.

Minimum number of special characters in passwords [0]?

- Minimum number of special characters in passwords.

Minimum number of character groups in passwords [0]?

- Minimum number of character groups in passwords.

Minimum number of character changed from previous password [0]?

- Minimum number of character changed from previous password.

systemtools securitystatus

Shows the security status for the device.

systemtools selectsw

Select which of the available software images to use. Changing the software image will restart the device.

No argument given: Lists the version of the available software images, and shows which one is active.

image name: Swap to the software with this name.

systemtools sudo on

Changes the user role of the current session to the role of the specified user

<username>: The name of the sudo user.

<password>: The password for the sudo user.

systemtools sudo off

Reverts back to the user role of the signed in user.

systemtools whoami

Lists the name and id of the signed in user, and the user roles held by this user.



Disconnect cause types

The following parameters are logged when a call is disconnected. The disconnect cause types are used in disconnect events (xEvent).

CauseValue	Proprietary. We recommend the use of CauseType and CauseCode.
CauseType	Describes why the call was disconnected. The value space is { OtherLocal, LocalDisconnect, UnknownRemoteSite, LocalBusy, LocalReject, InsufficientSecurity, OtherRemote, RemoteDisconnect, RemoteBusy, RemoteRejected, RemoteNoAnswer, CallForwarded, NetworkRejected }
CauseString	Describes the Cause Code.
CauseCode	The disconnect Cause Codes are defined in SIP and Q.850.
CauseOrigin	SIP, Q.850, internal.

Example:

```
xEvent DisconnectEvent

*e CallDisconnect CauseValue: 1
  CauseType: "LocalDisconnect"
  CauseString: ""
  OrigCallDirection: "outgoing"
  RemoteURI: "firstname.lastname@company.com"
  CallId: 89
  CauseCode: 0
  CauseOrigin: SIP
** end
```



User documentation on the Cisco web site

User documentation for the Cisco TelePresence products is available at

► <https://www.cisco.com/go/telepresence/docs>

Select the *Collaboration Endpoints* product category from the list. Then select the product series:

- Webex Boards
- Webex DX Series
- Webex Room Series
- TelePresence MX Series
- TelePresence SX Series

Alternatively, use the following short-links:

- <https://www.cisco.com/go/board-docs>
- <https://www.cisco.com/go/dx-docs>
- <https://www.cisco.com/go/mx-docs>
- <https://www.cisco.com/go/room-docs>
- <https://www.cisco.com/go/sx-docs>

Install and Upgrade

Installation and Upgrade Guides

- *Installation guides*: How to install the product
- *Getting started guide*: Initial configurations required to get the device up and running
- *Physical interface guide*: Details about the product's physical interface, including the connector panel and LEDs (SX80 only)
- *RCSL guide*: Regulatory compliance and safety information

Maintain and Operate

Maintain and Operate Guides

- *Administrator guide*: Information required to administer your product
- *Deployment guide for TelePresence endpoints on CUCM*: Tasks to perform to start using the product with the Cisco Unified Communications Manager (CUCM)

End-User Guides

- *User guides*: How to use the product
- *Quick reference guides*: How to use the product

Reference Guides

Command references

- *API reference guides*: Reference guide for the Application Programming Interface (API)

Technical References

- *CAD drawings*: 2D CAD drawings with dimensions

Configure

Configuration Guides

- *Customization Guide*: How to customize the user interface, how to use the device's API to program in-room controls, making macros, configure advanced audio set-ups using the Audio Console, and other customizations.
- *In-Room Control Editor*: Download the in-room control editor

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

Release notes

- *Release notes and deferral notices*

Licensing Information

- *Open source licences*: Licenses and notices for open source software used in this product

**Intellectual property rights**

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

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

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

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

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

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

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

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