API Reference Guide for Room Navigator (stand-alone)

Software version: RoomOS 11.9

All entries in the table of contents are hyperlinks that take you to the corresponding chapter. To go between the main sections, you can use the buttons in the top menu bar.

Table of contents

Introduction

A Room Navigator can either be paired to a video conferencing device, or used as a stand-alone device in rooms not equipped with a video conferencing device.

A stand-alone Room Navigator has a powerful public API, just like other devices running RoomOS software. A paired Room Navigator doesn't have a public API of its own; it is the API of the device that the Room Navigator is paired to that applies.

A stand-alone Room Navigator can be either registered to Webex or set up as a customer managed device.

This API reference guide applies only to stand-alone Room Navigators. If your Room Navigator is paired to a video conferencing device, the regular API reference guide for the video conferencing devices applies.

Further reading

Article about the Webex registered stand-alone Room Navigator on Help Center,

▶ Room Navigator as a standalone device

Section on customer managed stand-alone Room Navigator in this guide,

▶"Customer managed Room Navigator in stand-alone mode" on page 73

The regular API reference guide for the video conferencing devices (pdf) on cisco.com,

▶ API Reference Guide for Cisco collaboration devices

The RoomOS website for developers and integrators,

▶ https://roomos.cisco.com/

Cisco terms and conditions

Your use of Cisco software and cloud services are subject to these terms and conditions. Your use of Cisco APIs are subject to the Cisco Webex Developer Terms of Service.

Permitted commercial use for scheduled meeting join experience

In addition to the Cisco Terms and Conditions, the following use case requires separate permission for commercial use: providing a scheduled meeting join experience similar to one button to push. This includes use of any API that updates the device with calendar data from an external source to provide this functionality, including "`xCommand Bookings Put`", or previous private APIs, such as "`bookingsputxml`". In addition, using other APIs to accomplish the same functionality would also require permission for commercial use.

If you are providing a Scheduled Meeting Join Experience, you either must comply with the permitted commercial use terms or it must be for non-commercial use. Non-commercial use is defined as being solely for your internal business operations only and not for any activities that involve you using the API as part of or in furtherance of an income-generating service or product, whether directly or indirectly.

Any use to provide a Scheduled Meeting Join Experience that does not qualify under non-commercial use requires separate permission from Cisco.

Cisco reserves the right to revoke your license to use our API if, in our sole discretion, we deem that your use is for unauthorized commercial purposes or otherwise violates the Webex Developer Terms of Service. Please contact us at devsupport@webex.com if you have any questions about whether your intended use of the API is permitted, or to inquire about obtaining permission.

xConfiguration changes in RoomOS 11.9

New xConfigurations

xConfiguration Logging Mode

xConfiguration Provisioning Mode

xConfiguration UserInterface RoomScheduler AmbientTemperature Show

xConfiguration UserInterface RoomScheduler PeopleCount Current

xConfiguration UserInterface RoomScheduler StatusWhenInUse

xConfigurations that are modified

NetworkServices HTTPS Server MinimumTLSVersion

OLD: TLSv1.1/TLSv1.2

NEW: TLSv1.1/TLSv1.2/TLSv1.3

Security Session MaxTotalSessions

OLD: Integer (1..20), Default: 20

NEW: Integer (1..30), Default: 30

NEW: Auto/Current/Off/On, Default: Auto

WebEngine MinimumTLSVersion

OLD: TLSv1.0/TLSv1.1/TLSv1.2

NEW: TLSv1.0/TLSv1.1/TLSv1.2/TLSv1.3

xCommand changes in RoomOS 11.9

New xCommands

xCommand WebEngine Logging Set

xCommand WebEngine Tracing Start

xCommand WebEngine Tracing Stop

xCommands that are modified

Bookings Delete

NEW: Id: String (1, 128)
OLD: MeetingId (required parameter)
NEW: MeetingId (optional parameter)

HttpClient Delete

OLD: ResponseSizeLimit: Integer (1..100000), Default: 100000
NEW: ResponseSizeLimit: Integer (1..1048576), Default: 1048576

HttpClient Get

OLD: ResponseSizeLimit: Integer (1..100000), Default: 100000
NEW: ResponseSizeLimit: Integer (1..1048576), Default: 1048576

HttpClient Patch

OLD: ResponseSizeLimit: Integer (1..100000), Default: 100000
NEW: ResponseSizeLimit: Integer (1..1048576), Default: 1048576

HttpClient Post

OLD: ResponseSizeLimit: Integer (1..100000), Default: 100000
NEW: ResponseSizeLimit: Integer (1..1048576), Default: 1048576

HttpClient Put

OLD: ResponseSizeLimit: Integer (1..100000), Default: 100000
NEW: ResponseSizeLimit: Integer (1..1048576), Default: 1048576

Logging AddEvent

OLD: Text: String (0, 128)
NEW: Text: String (0, 256)

xStatus changes in RoomOS 11.9

New xStatuses

Network [n] ActiveInterface

RoomAnalytics AirQuality Index

RoomAnalytics AmbientTemperature

RoomAnalytics RelativeHumidity

SystemUnit LastShutdownReason

SystemUnit LastShutdownTime

WebEngine Tracing CustomCategories

WebEngine Tracing Duration

WebEngine Tracing Mode

WebEngine Tracing Systrace

xStatuses that are modified

Diagnostics Message [n] Type *(All products)*

Added to valuespace: InstantMeetingConfiguration/LockedDeviceCompanionMode/NavigatorDeviceLocationConfiguration/ThousandEyesStatus/TouchDeviceRunningMTRMemoryStatus/WebRTCWebViewTerminatedUnexpectedly/WebWidgetTerminatedUnexpectedly

Removed from valuespace: AirPlayConfiguration/CamerasDetected/ConceptCompositor

Configurations

Software version: RoomOS 11.9.2

Network configuration

xConfiguration Network [n] DNS Domain Name

Requires user role: ADMIN

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 "mydevice", this will result in the DNS lookup "mydevice.company.com".

USAGE:

```
xConfiguration Network [n] DNS Domain Name: "Name"
```

where

n: Index that identifies the network. Range: 1..1

Name: String (0, 64) - Default value: ""

The DNS domain name.

xConfiguration Network [n] DNS Server [m] Address

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

m: Index that identifies the DNS server. Maximum three DNS servers are allowed. Range: 1..3

Address: String (0, 64) - Default value: ""

A valid IPv4 address or IPv6 address.

xConfiguration Network [n] IEEE8021X Mode

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Mode: Off/On - Default value: Off

Off: The 802.1X authentication is disabled.

On: The 802.1X authentication is enabled.

xConfiguration Network [n] IEEE8021X TlsVerify

Requires user role: ADMIN

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

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

USAGE:

```
xConfiguration Network [n] IEEE8021X TlsVerify: TlsVerify
```

where

n: Index that identifies the network. Range: 1..1

TlsVerify: Off/On - Default value: Off

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.

xConfiguration Network [n] IEEE8021X UseClientCertificate

Requires user role: ADMIN

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

USAGE:

```
xConfiguration Network [n] IEEE8021X UseClientCertificate: UseClientCertificate
```

where

n: Index that identifies the network. Range: 1..1

UseClientCertificate: Off/On - Default value: Off

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

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

xConfiguration Network [n] IEEE8021X Identity

Requires user role: ADMIN

Define the username for 802.1X authentication.

USAGE:

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

where

n: Index that identifies the network. Range: 1..1

Identity: String (0, 64) - Default value: ""

The username for 802.1X authentication.

xConfiguration Network [n] IEEE8021X Password

Requires user role: ADMIN

Define the password for 802.1X authentication.

USAGE:

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

where

n: Index that identifies the network. Range: 1..1

Password: String (0, 50) - Default value: ""

The password for 802.1X authentication.

xConfiguration Network [n] IEEE8021X AnonymousIdentity

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

AnonymousIdentity: String (0, 64) - Default value: ""

The 802.1X Anonymous ID string.

xConfiguration Network [n] IEEE8021X Eap Md5

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Md5: Off/On - Default value: On

Off: The EAP-MD5 protocol is disabled.

On: The EAP-MD5 protocol is enabled.

xConfiguration Network [n] IEEE8021X Eap Ttls

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Ttls: Off/On - Default value: On

Off: The EAP-TTLS protocol is disabled.

On: The EAP-TTLS protocol is enabled.

xConfiguration Network [n] IEEE8021X Eap Tls

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Tls: Off/On - Default value: On

Off: The EAP-TLS protocol is disabled.

On: The EAP-TLS protocol is enabled.

xConfiguration Network [n] IEEE8021X Eap Peap

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Peap: Off/On - Default value: On

Off: The EAP-PEAP protocol is disabled.

On: The EAP-PEAP protocol is enabled.

xConfiguration Network [n] IPStack

Requires user role: ADMIN

Select if the device should use IPv4, IPv6, or dual IP stack, on the network interface. It may take up to 30 seconds before the change takes effect.

USAGE:

```
xConfiguration Network [n] IPStack: IPStack
```

where

n: Index that identifies the network. Range: 1..1

IPStack: Dual/IPv4/IPv6 - Default value: Dual

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.

xConfiguration Network [n] IPv4 Assignment

Requires user role: ADMIN

Define how the device will obtain its IPv4 address, subnet mask, and gateway address.

The client identifier, which is used in the DHCP requests, is the DHCP Unique Identifier (DUID) as specified in RFC 4361.

USAGE:

```
xConfiguration Network [n] IPv4 Assignment: Assignment
```

where

n: Index that identifies the network. Range: 1..1

Assignment: Static/DHCP - Default value: 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.

xConfiguration Network [n] IPv4 Address

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Address: String (0, 64) - Default value: ""

A valid IPv4 address.

xConfiguration Network [n] IPv4 Gateway

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Gateway: String (0, 64) - Default value: ""

A valid IPv4 address.

xConfiguration Network [n] IPv4 InterfaceIdentifier

Requires user role: ADMIN

Select which identifier to use for IPv4 DHCP.

USAGE:

`xConfiguration Network [n] IPv4 InterfaceIdentifier: InterfaceIdentifier`

where

n: Index that identifies the network. Range: 1..1

InterfaceIdentifier: Auto/MAC/Opaque - Default value: Auto

MAC: The device will send "01" followed by the MAC address of the device as identifier.

Opaque: The device will use an RFC4361-based DHCP Unique Identifier (DUID); DUID-LL, based on the link-layer address with no timestamp.

Auto: The device will use Opaque, that is, the DHCP Unique Identifier (DUID) as specified in RFC 4361.

xConfiguration Network [n] IPv4 SubnetMask

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

SubnetMask: String (0, 64) - Default value: ""

A valid IPv4 address.

xConfiguration Network [n] IPv6 Assignment

Requires user role: ADMIN

Define how the device will obtain its IPv6 address, subnet mask, and gateway address.

The client identifier, which is used in the DHCP requests, is the DHCP Unique Identifier (DUID) as specified in RFC 4361.

USAGE:

`xConfiguration Network [n] IPv6 Assignment: Assignment`

where

n: Index that identifies the network. Range: 1..1

Assignment: Static/DHCPv6/Autoconf - Default value: 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.

xConfiguration Network [n] IPv6 Address

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Address: String (0, 64) - Default value: ""

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

xConfiguration Network [n] IPv6 Gateway

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Gateway: String (0, 64) - Default value: ""

A valid IPv6 address.

xConfiguration Network [n] IPv6 DHCPOptions

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

DHCPOptions: Off/On - Default value: 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.

xConfiguration Network [n] IPv6 InterfaceIdentifier

Requires user role: ADMIN

Define the IPv6 interface identifier for the device. The interface identifier you choose, either MAC or Opaque, will determine the method that is used for generating part of the the IPv6 address. This is applicable to both link-local IPv6 addresses and Stateless Address Autoconfiguration (SLAAC) addresses.

The address contains a 64-bit prefix and a 64-bit interface identifier generated by the device. With MAC, an EUI-64 based interface identifier is generated, as described in RFC-2373.

With Opaque, a random 64-bit interface identifier is generated as described in RFC-7217 on the first boot of the device, and this is used forever, or until factory reset.

USAGE:

`xConfiguration Network [n] IPv6 InterfaceIdentifier: InterfaceIdentifier`

where

n: Index that identifies the network. Range: 1..1

InterfaceIdentifier: MAC/Opaque - Default value: MAC

MAC: Select MAC as the Interface Identifier method.

Opaque: Select Opaque as the Interface Identifier method.

xConfiguration Network [n] MTU

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

MTU: Integer (576..1500) - Default value: 1500

Set a value for the MTU (bytes).

xConfiguration Network [n] QoS Mode

Requires user role: ADMIN

The QoS (Quality of Service) is a method which handles the priority of audio, video and other data in the network. The QoS settings must be supported by the infrastructure. Diffserv (Differentiated Services) is a networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic. It provides QoS priorities on IP networks.

USAGE:

```
xConfiguration Network [n] QoS Mode: Mode
```

where

n: Index that identifies the network. Range: 1..1

Mode: Off/Diffserv - Default value: Diffserv

Off: No QoS method is used.

Diffserv: The 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.

xConfiguration Network [n] QoS Diffserv Video

Requires user role: ADMIN

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Video packets should have in the IP network. The packets of the presentation channel (shared content) are also in the Video packet category. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use AF41 for Video. AF41 equals the decimal value 34.

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

n: Index that identifies the network. Range: 1..1

Video: Integer (0..63) - Default value: 34

Set the priority of the video packets in the IP network. 0 means "best-effort".

xConfiguration Network [n] QoS Diffserv Data

Requires user role: ADMIN

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority Data packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use AF41 for Data. AF41 equals the decimal value 34.

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

n: Index that identifies the network. Range: 1..1

Data: Integer (0..63) - Default value: 34

Set the priority of the data packets in the IP network. 0 means "best-effort".

xConfiguration Network [n] QoS Diffserv Signalling

Requires user role: ADMIN

This setting takes effect only 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 traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use CS3 for Signalling. CS3 equals the decimal value 24.

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

n: Index that identifies the network. Range: 1..1

Signalling: Integer (0..63) - Default value: 24

Set the priority of the signalling packets in the IP network. 0 means "best-effort".

xConfiguration Network [n] QoS Diffserv ICMPv6

Requires user role: ADMIN

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority ICMPv6 packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use 0 for ICMPv6.

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

n: Index that identifies the network. Range: 1..1

ICMPv6: Integer (0..63) - Default value: 0

Set the priority of the ICMPv6 packets in the IP network. 0 means "best effort".

xConfiguration Network [n] QoS Diffserv NTP

Requires user role: ADMIN

This setting takes effect only if Network QoS Mode is set to Diffserv.

Define which priority NTP packets should have in the IP network. The traffic classes recommended in the DiffServ RFCs map to a decimal value between 0 and 63. We recommend you use 0 for NTP.

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

n: Index that identifies the network. Range: 1..1

NTP: Integer (0..63) - Default value: 0

Set the priority of the NTP packets in the IP network. 0 means "best-effort".

xConfiguration Network [n] RemoteAccess Allow

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Allow: String (0, 255) - Default value: ""

A valid IPv4 address or IPv6 address.

xConfiguration Network [n] VLAN Voice Mode

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

Mode: Auto/Manual/Off - Default value: Auto

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.

xConfiguration Network [n] VLAN Voice VlanId

Requires user role: ADMIN

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

n: Index that identifies the network. Range: 1..1

VlanId: Integer (1..4094) - Default value: 1

Set the VLAN voice ID.

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 - Default value: On

Off: The CDP daemon is disabled.

On: The CDP daemon is enabled.

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 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.

USAGE:

```
xConfiguration NetworkServices HTTP Mode: Mode
```

where

Mode: Off/HTTP+HTTPS/HTTPS - Default value: 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.

xConfiguration NetworkServices HTTP Proxy LoginName

Requires user role: ADMIN

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. We support the following HTTP authentication schemes: Digest using the MD5 algorithm, and the Basic HTTP authentication scheme.

USAGE:

```
xConfiguration NetworkServices HTTP Proxy LoginName: "LoginName"
```

where

LoginName: String (0, 80) - Default value: ""

The authentication login name.

xConfiguration NetworkServices HTTP Proxy Mode

Requires user role: ADMIN

You can configure a proxy server for HTTP, HTTPS, and WebSocket traffic. The HTTP proxy can be set up manually, it can be auto-configured (PACUrl), fully automated (WPAD), or it can be turned off.

If NetworkServices HTTP Proxy Mode is not turned Off, you can further specify if the web engine shall use the proxy in the WebEngine UseHttpProxy setting.

Communication with the Webex cloud will always go via the proxy if NetworkServices HTTP Proxy Mode is not turned Off.

USAGE:

```
xConfiguration NetworkServices HTTP Proxy Mode: Mode
```

where

Mode: Manual/Off/PACUrl/WPAD - Default value: Off

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.

xConfiguration NetworkServices HTTP Proxy PACUrl

Requires user role: ADMIN

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) - Default value: ""

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

xConfiguration NetworkServices HTTP Proxy Password

Requires user role: ADMIN

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. We support the following HTTP authentication schemes: Digest using the MD5 algorithm, and the Basic HTTP authentication scheme.

USAGE:

```
xConfiguration NetworkServices HTTP Proxy Password: "Password"
```

where

Password: String (0, 64) - Default value: ""

The authentication password.

xConfiguration NetworkServices HTTP Proxy Url

Requires user role: ADMIN

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) - Default value: ""

The URL of the HTTP proxy server.

xConfiguration NetworkServices HTTPS Server MinimumTLSVersion

Requires user role: ADMIN

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

USAGE:

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

where

MinimumTLSVersion: TLSv1.1/TLSv1.2/TLSv1.3 - Default value: TLSv1.1

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

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

TLSv1.3: Support of TLS version 1.3 or higher.

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 - Default value: Off

Off: The HTTP strict transport security feature is disabled.

On: The HTTP strict transport security feature is enabled.

xConfiguration NetworkServices HTTPS VerifyClientCertificate

Requires user role: ADMIN

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

USAGE:

```
xConfiguration NetworkServices HTTPS VerifyClientCertificate:
VerifyClientCertificate
```

where

VerifyClientCertificate: Off/On - Default value: Off

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.

xConfiguration NetworkServices SSH Mode

Requires user role: ADMIN

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

USAGE:

```
xConfiguration NetworkServices SSH Mode: Mode
```

where

Mode: Off/On - Default value: On

Off: The SSH protocol is disabled.

On: The SSH protocol is enabled.

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 keysize, 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 - Default value: RSA

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

RSA: Use the RSA algorithm (2048 bits).

ed25519: Use the ed25519 algorithm.

Provisioning configuration

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/Webex - Default value: Auto

Off: The device is not configured by a provisioning system.

Auto: The provisioning server is automatically selected as set up in the DHCP server.

Webex: Push configurations to the device from the Webex cloud service. In order to register to the Webex cloud service, the encryption option key must be installed on the device.

RoomScheduler configuration

xConfiguration RoomScheduler Enabled

Requires user role: ADMIN

Doesn't apply for a customer managed Room Navigator.

The room scheduling feature allows you to book a room directly from the touch controller for the meeting room. You can also extend an ongoing meeting if the room is still available. You can also use the Webex Assistant (voice-driven virtual assistant) to book or extend a meeting.

The room scheduling feature requires the room to be set up with a calendar service that allows booking.

USAGE:

```
xConfiguration RoomScheduler Enabled: Enabled
```

where

Enabled: False/True - Default value: False

False: The room scheduling feature is not available.

True: The room scheduling feature is available if the prerequisites listed above are met.

Security configuration

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) - Default value: 60

Set the lockout time (minutes).

xConfiguration Security Session InactivityTimeout

Requires user role: ADMIN

Define how long the device will accept inactivity from the user before automatically logging 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) - Default value: 0

Set the inactivity timeout (minutes). Specifying 0 will result in a time out of 1 hour. The maximum timeout length is 12 hours.

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) - Default value: 0

Set the maximum number of failed login attempts per user.

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) - Default value: 20

Set the maximum number of simultaneous sessions per user.

xConfiguration Security Session MaxTotalSessions

Requires user role: ADMIN

The maximum number of simultaneous sessions in total is 30 sessions.

USAGE:

```
xConfiguration Security Session MaxTotalSessions: MaxTotalSessions
```

where

MaxTotalSessions: Integer (1..30) - Default value: 30

Set the maximum number of simultaneous sessions in total.

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 - Default value: Off

On: Show information about the last session.

Off: Do not show information about the last session.

xConfiguration Security Xapi WebSocket ApiKey Allowed

Requires user role: ADMIN

Enable or disable access to the device's API over web sockets. A typical use case that requires API access is a persistent web app, for example a custom booking app that wants to control the color of the LEDs. If API access is disabled, apps that don't require any communication with the API can still run.

USAGE:

```
xConfiguration Security Xapi WebSocket ApiKey Allowed: Allowed
```

where

Allowed: False/True - Default value: False

True: A web app can interact with the device's API over web sockets, provided that the domain of the server hosting the app is listed in the WebEngine Features Xapi Peripherals AllowedHosts Hosts setting.

False: The web app is not allowed to interact with the device's API over web sockets.

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) - Default value: ""

Define the device name.

xConfiguration SystemUnit BroadcastName

Requires user role: ADMIN

Not applicable for stand-alone Room Navigator.

USAGE:

```
xConfiguration SystemUnit BroadcastName: BroadcastName
```

where

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 use only and not available to customers.

USAGE:

```
xConfiguration SystemUnit CrashReporting Mode: Mode
```

where

Mode: Off/On - Default value: On

Off: No logs will be sent to ACR tool.

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

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 use only and not available to customers.

USAGE:

```
xConfiguration SystemUnit CrashReporting URL: "URL"
```

where

URL: String (0, 255) - Default value: "acr.cisco.com"

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

xConfiguration SystemUnit CustomDeviceId

Requires user role: ADMIN, INTEGRATOR

The SystemUnit CustomDeviceId provides a place for you to store custom information about a unit. This can be useful, for example, in aiding to track devices in a provisioning setup).

USAGE:

```
xConfiguration SystemUnit CustomDeviceId: "CustomDeviceId"
```

where

CustomDeviceId: String (0, 255) - Default value: ""

xConfiguration SystemUnit TouchPanel Location

Requires user role: ADMIN

Specify the location of the device. The device may be in the room, but can also be placed outside the room, for example to facilitate room booking.

USAGE:

```
xConfiguration SystemUnit TouchPanel Location: Location
```

where

Location: InsideRoom/NotSet/OutsideRoom - Default value: NotSet

InsideRoom: The device is inside the room.

NotSet: Information about the location of the device is not specified.

OutsideRoom: The device is outside the room.

Time configuration

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 - Default value: DD_MM_YY

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

xConfiguration Time TimeFormat

Requires user role: ADMIN, USER

Define the time format.

USAGE:

xConfiguration Time TimeFormat: *TimeFormat*

where

TimeFormat: 24H/12H - Default value: 24H

24H: Set the time format to 24 hours.

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

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/Ciudad_Juarez, 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/Nuuk, 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/Punta_Arenas, America/Rainy_River, America/Rankin_Inlet, America/Recife, America/Regina, America/Resolute, America/Rio_Branco, America/Rosario, America/Santa_Isabel, America/Santarem, America/Santiago, America/Santo_Domingo, America/Sao_Paulo, America/Scoresbysund, America/Shiprock, America/Sitka, America/St_Barthelemy, America/St_Johns, America/St_Kitts, America/St_Lucia, America/St_Thomas, America/St_Vincent, America/Swift_Current, America/Tegucigalpa, America/Thule, America/Thunder_Bay, America/Tijuana, America/Toronto, America/Tortola, America/Vancouver, America/Virgin, America/Whitehorse, America/Winnipeg, America/Yakutat, America/Yellowknife, Antarctica/Casey, Antarctica/Davis, Antarctica/DumontDUrville, Antarctica/Macquarie, Antarctica/Mawson, Antarctica/McMurdo, Antarctica/Palmer, Antarctica/Rothera, Antarctica/South_Pole, Antarctica/Syowa, Antarctica/Troll, Antarctica/Vostok, Arctic/Longyearbyen, Asia/Aden, Asia/Almaty, Asia/Amman, Asia/Anadyr, Asia/Aqtau, Asia/Aqtobe, Asia/Ashgabat, Asia/Ashkhabad, Asia/Atyrau, 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/Famagusta, 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/Qostanay, 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/Yangon, 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/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/GMT0, Etc/Greenwich, Etc/UCT, Etc/UTC, Etc/Universal, Etc/Zulu, Europe/Amsterdam, Europe/Andorra, Europe/Astrakhan, Europe/Athens, Europe/Belfast, Europe/Belgrade, Europe/Berlin, Europe/Bratislava, Europe/Brussels, Europe/Bucharest, Europe/Budapest, Europe/Busingen, Europe/Chisinau, Europe/Copenhagen, Europe/Dublin, Europe/Gibraltar, Europe/Guernsey, Europe/Helsinki, Europe/Isle_of_Man, Europe/Istanbul, Europe/Jersey, Europe/Kaliningrad, Europe/Kiev, Europe/Kirov, Europe/Kyiv, 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/Saratov, Europe/Simferopol, Europe/Skopje, Europe/Sofia, Europe/Stockholm, Europe/Tallinn, Europe/Tirane, Europe/Tiraspol, Europe/Ulyanovsk, Europe/Uzhgorod, Europe/Vaduz, Europe/Vatican, Europe/Vienna, Europe/Vilnius, Europe/Volgograd, Europe/Warsaw, Europe/Zagreb, Europe/Zaporozhye, Europe/Zurich, GB, GB-Eire, GMT, GMT+0, GMT-0, GMT0, Greenwich, HST, Hongkong, Iceland, Indian/Antananarivo, Indian/Chagos, Indian/Christmas, Indian/Cocos, Indian/Comoro, Indian/Kerguelen, Indian/Mahe, Indian/Maldives, Indian/Mauritius, Indian/Mayotte, Indian/Reunion, Iran, Israel, Jamaica, Japan, Kwajalein, Libya, MET, MST, MST7MDT, Mexico/BajaNorte, Mexico/BajaSur, Mexico/General, NZ, NZ-CHAT, Navajo, PRC, PST8PDT, Pacific/Apia, Pacific/Auckland, Pacific/Bougainville, Pacific/Chatham, Pacific/Chuuk, Pacific/Easter, Pacific/Efate, Pacific/Enderbury, Pacific/Fakaofo, Pacific/Fiji, Pacific/Funafuti, Pacific/Galapagos, Pacific/Gambier, Pacific/Guadalcanal, Pacific/Guam, Pacific/Honolulu, Pacific/Johnston, Pacific/Kanton, 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/Samoa, UTC, Universal, W-SU, WET, Zulu – Default value: Etc/UTC

Select a time zone from the list.

UserInterface configuration

xConfiguration UserInterface HomeScreen Peripherals WebApp URL

Requires user role: ADMIN

Set the URL of the persistent web app you want to run on the device. The application displays on the entire screen, and it can't be dismissed by the user.

If the app is going to interact with the device's API, remember to set Security Xapi WebSocket ApiKey Allowed to True, and add the domain name of the server hosting the app to the allow list in the WebEngine Features Xapi Peripherals AllowedHosts Hosts setting.

USAGE:

```
xConfiguration UserInterface HomeScreen Peripherals WebApp URL: "URL"
```

where

URL: String (0, 2048) - Default value: ""

The URL of the web application.

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 - Default value: On

Off: There is no key tone sound effect.

On: The key tone sound effect is turned on.

xConfiguration UserInterface Language

Requires user role: ADMIN, USER

Select the language to be used on 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/Ukrainian - Default value: English

Select a language from the list.

xConfiguration UserInterface LedControl Mode

Requires user role: ADMIN

The wall mount version of the Room Navigator has LED lights. You can configure how they should be controlled.

USAGE:

```
xConfiguration UserInterface LedControl Mode: Mode
```

where

Mode: Auto/Manual/Off - Default value: Auto

Auto: The device controls the LED lights automatically, typically based on the room booking status (for example, green: room available, red: room in use). The UserInterface LedControl Color Set Color command will have no effect.

Manual: You can control the LED lights and set the color using the UserInterface LedControl Color Set Color command.

Off: The LED lights are turned off permanently.

xConfiguration UserInterface RoomScheduler AmbientTemperature Show

Requires user role: ADMIN

This setting applies when a Room Navigator is set up as a room booking device (also referred to as scheduler mode). The Room Navigator may show the room temperature, if that is available from the device it's connected to. Use this setting to decide whether to display it.

USAGE:

```
xConfiguration UserInterface RoomScheduler AmbientTemperature Show: Show
```

where

Show: Auto/Hidden/ShowCelsius/ShowFahrenheit - Default value: Auto

Auto: Show the temperature in both degrees Celsius and Fahrenheit.
Hidden: Don't show the temperature.
ShowCelcius: Show the temperature in degrees Celsius
ShowFahrenheit: Show the temperature in degrees Fahrenheit.

xConfiguration UserInterface RoomScheduler PeopleCount Current

Requires user role: ADMIN

This setting applies when a Room Navigator is set up as a room booking device (also referred to as scheduler mode). The Room Navigator may show the number of people currently in the meeting room, if that information is available from the device it's connected to. Use this setting to decide whether to display this information.

USAGE:

```
xConfiguration UserInterface RoomScheduler PeopleCount Current: Current
```

where

Current: Auto/Hidden - Default value: Auto

Auto: Show the number of people.
Hidden: Don't show the number of people.

xConfiguration UserInterface Security Mode

Requires user role: ADMIN

Not applicable for stand-alone Room Navigator.

USAGE:

```
xConfiguration UserInterface Security Mode: Mode
```

where

xConfiguration UserInterface SettingsMenu Mode

Requires user role: ADMIN

Not applicable for stand-alone Room Navigator.

USAGE:

```
xConfiguration UserInterface SettingsMenu Mode: Mode
```

where

xConfiguration UserInterface SettingsMenu Visibility

Requires user role: ADMIN

Not applicable for stand-alone Room Navigator.

USAGE:

```
xConfiguration UserInterface SettingsMenu Visibility: Visibility
```

where

UserManagement configuration

xConfiguration UserManagement PasswordPolicy Complexity MinimumDigits

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of numerical characters (0..9) in the password.

USAGE:

```
xConfiguration UserManagement PasswordPolicy Complexity MinimumDigits:
MinimumDigits
```

where

MinimumDigits: Integer (0..4) - Default value: 0

The minimum number of numerical characters. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy Complexity MinimumLength

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of characters in the password.

USAGE:

```
xConfiguration UserManagement PasswordPolicy Complexity MinimumLength:
MinimumLength
```

where

MinimumLength: Integer (0..256) - Default value: 8

The minimum number of characters. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy Complexity MinimumLowercase

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of lower-case letters in the password.

USAGE:

```
xConfiguration UserManagement PasswordPolicy Complexity MinimumLowercase:
MinimumLowercase
```

where

MinimumLowercase: Integer (0..4) - Default value: 0

The minimum number of lower-case characters. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy Complexity MinimumSpecial

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of special characters in the password.

USAGE:

```
xConfiguration UserManagement PasswordPolicy Complexity MinimumSpecial:
MinimumSpecial
```

where

MinimumSpecial: Integer (0..4) - Default value: 0

The minimum number of special characters. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy Complexity MinimumUppercase

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the minimum number of upper-case letters in the password.

USAGE:

```
xConfiguration UserManagement PasswordPolicy Complexity MinimumUppercase: MinimumUppercase
```

where

MinimumUppercase: Integer (0..4) - Default value: 0

The minimum number of upper-case characters. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy MaxLifetime

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the maximum number of days before a password becomes invalid.

USAGE:

```
xConfiguration UserManagement PasswordPolicy MaxLifetime: MaxLifetime
```

where

MaxLifetime: Integer (0..7300) - Default value: 0

The minimum number of days. 0 means no restrictions.

xConfiguration UserManagement PasswordPolicy ReuseLimit

Requires user role: ADMIN

When signing in to the device as a local user, the password must follow the rules set by the UserManagement PasswordPolicy settings. A new password rule will not apply to existing passwords but will take effect on the next password change.

This setting specifies the reuse limit (n), which means that a user cannot change to either of their previous n passwords.

USAGE:

```
xConfiguration UserManagement PasswordPolicy ReuseLimit: ReuseLimit
```

where

ReuseLimit: Integer (0..24) - Default value: 12

The minimum number of passwords. 0 means no restrictions.

Video configuration

xConfiguration Video Output Connector BrightnessMode

Requires user role: ADMIN, USER

Decide whether the screen brightness should be adjusted automatically or set to a fixed value.

USAGE:

`xConfiguration Video Output Connector BrightnessMode: BrightnessMode`

where

BrightnessMode: Auto/Manual - Default value: Auto

Auto: The device automatically adjusts the screen brightness according to the ambient light.

Manual: The screen brightness level is set in the Video Output Connector BrightnessValue setting.

xConfiguration Video Output Connector BrightnessValue

Requires user role: ADMIN, USER

Set the screen brightness level to be used if Video Output Connector BrightnessMode is set to Manual.

USAGE:

`xConfiguration Video Output Connector BrightnessValue: BrightnessValue`

where

BrightnessValue: Integer (0..100) - Default value: 100

The brightness level, from bright (maximum brightness, 100) to dark (minimum brightness, 0).

WebEngine configuration

xConfiguration WebEngine Features Xapi Peripherals AllowedHosts Hosts

Requires user role: ADMIN

If the domain name of the server hosting a persistent web app is listed here, the app is allowed to run API commands on the device. Otherwise, only apps that don't require any communication with the device can run.

The URL, specified with UserInterface HomeScreen Peripherals WebApp URL setting, will be checked, and matched against this list of allowed hosts before it's allowed to run API commands on the device.

USAGE:

`xConfiguration WebEngine Features Xapi Peripherals AllowedHosts Hosts: "Hosts"`

where

Hosts: String (0, 1024) - Default value: ""

Specify one or more domain names. If more than one, separate them by comma. You can use the "*" as a wildcard. For example, "*.cisco.com" allows any host ending in cisco.com. To allow any domain, specify "*".

xConfiguration WebEngine MinimumTLSVersion

Requires user role: ADMIN

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

USAGE:

`xConfiguration WebEngine MinimumTLSVersion: MinimumTLSVersion`

where

MinimumTLSVersion: TLSv1.0/TLSv1.1/TLSv1.2/TLSv1.3 - Default value: TLSv1.1

TLSv1.0: Support of TLS version 1.0 or higher.

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

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

TLSv1.3: Support of TLS version 1.3 or higher.

xConfiguration WebEngine Mode

Requires user role: ADMIN

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

USAGE:

`xConfiguration WebEngine Mode: Mode`

where

Mode: Off/On - Default value: Off

Off: The web engine is disabled.

On: The web engine is enabled.

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 - Default value: Off

Off: Remote debugging is switched off.

On: Remote debugging is switched on.

xConfiguration WebEngine UseHttpProxy

Requires user role: ADMIN

The WebEngine UseHttpProxy setting specifies if web view based features such as web apps shall communicate via an HTTP proxy or not.

For this setting to have any effect, a proxy server for HTTP, HTTPS, and WebSocket traffic must be set up using the NetworkServices HTTP Proxy settings.

USAGE:

`xConfiguration WebEngine UseHttpProxy: UseHttpProxy`

where

UseHttpProxy: Off/On - Default value: On

Off: Set up communication directly with the server (not using a proxy).

On: Set up communication via proxy.

Commands

Software version: RoomOS 11.9.2

Bookings commands

xCommand Bookings Book

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Book the meeting room for the specified period. If you don't specify the start time and duration, the room will be booked from now on and for 30 minutes.

This command is only available for devices that support the room scheduling feature, refer to the RoomScheduler Enabled setting.

USAGE:

```
xCommand Bookings Book [BookingRequestUUID: "BookingRequestUUID"] [Duration: Duration] [StartTime: "StartTime"] [Title: "Title"]
```

where

BookingRequestUUID: String (1, 128)

A unique identifier for the booking request. If this parameter is omitted, a booking request identifier will be assigned automatically.

Duration: Integer (0..1440) - Default value: 30

The duration of the meeting, in minutes.

StartTime: String (1, 128)

The start time of the meeting in the following UTC format: YYYY-MM-DDThh:mm:ssZ. Example: 2021-01-24T01:29:00Z.

Title: String (1, 128)

The title or subject field in the calendar booking. It will also be displayed on screen in the today's bookings list.

xCommand Bookings Clear

Requires user role: ADMIN, USER

Clear the current stored list of bookings.

USAGE:

```
xCommand Bookings Clear
```

xCommand Bookings Delete

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Remove the meeting that is identified by the MeetingId parameter. Then the room becomes available for new bookings.

This command is only available for devices that support the room scheduling feature, refer to the RoomScheduler Enabled setting.

USAGE:

```
xCommand Bookings Delete [Id: "Id"] [MeetingId: "MeetingId"]
```

where

Id: String (1, 128)

A unique meeting identifier. It allows the deletion of meetings that are scheduled through either the Bookings Put command or hybrid calendar. The identifier is returned by the Bookings List command. For hybrid calendar, this id may not be persistent across reboots.

MeetingId: String (1, 128)

A unique meeting identifier. It is assigned to the meeting by the calendar service backend. The meeting identifier is returned by the Bookings List command. Note that this is different from the booking request identifier (BookingRequestUUID) that is provided when issuing the Bookings Book command.

xCommand Bookings Get

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Get the booking information for a specific ID.

USAGE:

```
xCommand Bookings Get Id: "Id"
```

where

Id: String (1, 128)

A unique meeting identifier. It is assigned to the meeting by the calendar service backend. The meeting identifier is returned by the Bookings List command. Note that this is different from the booking request identifier (BookingRequestUUID) that is provided when issuing the Bookings Book command.

xCommand Bookings List

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

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:

```
xCommand 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) - Default value: 0

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

Limit: Integer (1..65534)

Max number of bookings to list.

Offset: Integer (0..65534) - Default value: 0

Offset number of bookings for this search.

xCommand Bookings NotificationSnooze

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

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

USAGE:

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

where

Id: String (0, 128)

The ID of the notification snooze setting.

SecondsToSnooze: Integer (1..3600) - Default value: 300

The duration of the snooze period, in seconds.

xCommand Bookings Put

Requires user role: ADMIN

Doesn't apply for a customer managed Room Navigator.

NOTE: This API has special terms and conditions, please refer to the "Terms and conditions" section in the API guide for Room Navigator (stand-alone).

It replaces the list of stored bookings. This is a multiline command with details of the stored bookings as payload.

The meeting information is provided in JSON format.

For example:

```
{
 "Bookings": [
  {
   "Id": "1",
   "Number": "number@example.com",
   "Organizer": {
    "Name": "John Smith"
   },
   "Protocol": "SIP",
   "Time": {
   "Duration": 60,
   "EndTimeBuffer": 50,
   "StartTime": "2024-06-04T08:40:42.300000000Z"
   },
   "Title": "Booking Title"
  }
 ]
}
```

The required fields are: Id, Title, Number, Protocol, Organizer/Name, Time/StartTime, and Time/Duration.

StartTime: The meeting start time in UTC/Zulu time.

Duration: The meeting duration in minutes.

StartTimeBuffer: The number of seconds before the meeting start time that people can join the meeting.

EndTimeBuffer: The number of seconds longer than the scheduled hours (StartTime + Duration) that the meeting can last.

MeetingPlatform: The service that hosts the meeting.

The JSON structure supports the following fields (some of them are not relevant for the

stand-alone Room Navigator):

```
{
{ "Id", "id" },
{ "MeetingId", "MyMeeting" },
{ "Agenda", "MyAgenda" },
{ "Title", "MyBookingTitle" },
{ "Privacy", “Private/Public” },
{ "Protocol", "SIP/H323/ISDN/IP/Spark/WebRTC" },
{ "MeetingPlatform", "GoogleMeet/MicrosoftTeams/Zoom/Webex/Other" },
{ "MetaInfo", "...." },
{ "Time", {
  { "StartTime", "2020-06-10T09:31:42Z"},
  { "Duration", 60 },
  { "StartTimeBuffer", 300 },
  { "EndTimeBuffer", 0 },
}},
{ "Organizer", {
  { "Name", "John Smith" },
  { "Email", "johnsmith@example.com" },
  { "Id", "" },
}},
{ "Number", "number@example.com" },
{ "CallType", "Audio/Video" },
{ "Encryption", "On/Off" }
}
```

USAGE:

```
xCommand Bookings Put
```

xCommand Bookings Respond

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Accept or decline a meeting invitation.

USAGE:

```
xCommand Bookings Respond MeetingId: "MeetingId" Type: Type
```

where

MeetingId: String (1, 128)

The unique identifier for the meeting.

Type: Accept/Decline

Accept: Accept a meeting invitation given to the room.

Decline: Decline a meeting invitation given to the room.

Diagnostics commands

xCommand Diagnostics Run

Requires user role: ADMIN

This command runs self-diagnostics commands on the device.

USAGE:

```
xCommand Diagnostics Run [ResultSet: ResultSet]
```

where

ResultSet: Alerts/All/None - Default value: Alerts

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

HttpClient commands

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:

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

where

AllowInsecureHTTPS: False/True - Default value: False

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, 3072)

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

ResponseSizeLimit: Integer (1..1048576) - Default value: 1048576

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 - Default value: None

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) - Default value: 30

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

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:

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

where

AllowInsecureHTTPS: False/True - Default value: False

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, 3072)

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

ResponseSizeLimit: Integer (1..1048576) - Default value: 1048576

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 - Default value: None

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) - Default value: 30

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

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:

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

where

AllowInsecureHTTPS: False/True - Default value: False

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, 3072)

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

ResponseSizeLimit: Integer (1..1048576) - Default value: 1048576

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 - Default value: None

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) - Default value: 30

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

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:

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

where

AllowInsecureHTTPS: False/True - Default value: False

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, 3072)

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

ResponseSizeLimit: Integer (1..1048576) - Default value: 1048576

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 - Default value: None

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) - Default value: 30

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

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:

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

where

AllowInsecureHTTPS: False/True - Default value: False

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, 3072)

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

ResponseSizeLimit: Integer (1..1048576) - Default value: 1048576

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 - Default value: None

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) - Default value: 30

Timeout period in seconds. If the request is not completed during this period, the API will return an error.

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>.

Logging commands

xCommand Logging AddEvent

Requires user role: ADMIN, USER

Add a custom message to the device's log files.

USAGE:

```
xCommand Logging AddEvent Text: "Text" Type: Type
```

where

Text: String (0, 256)

The text that will be added to the log file.

Type: Error/Info/Warning

The type of message (error, information, or warning).

xCommand Logging SendLogs

Requires user role: ADMIN, USER

Send logs to the 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:

```
xCommand Logging SendLogs
```

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:

```
xCommand Provisioning CompleteUpgrade
```

xCommand Provisioning PostponeUpgrade

Requires user role: ADMIN, USER

Postpones the installing of the software upgrade.

USAGE:

```
xCommand Provisioning PostponeUpgrade [Reason: "Reason"] SecondsToPostpone: SecondsToPostpone
```

where

Reason: String (0, 255)

Provide information about why the upgrade was postponed.

SecondsToPostpone: Integer (0..65534)

Set how long to postpone the upgrade. The value is in seconds.

xCommand Provisioning SetType

Requires user role: ADMIN, INTEGRATOR

A Room Navigator can be paired to a video conferencing device or set up as a stand-alone device. This command determines which mode, paired or stand-alone, the device is to be onboarded in.

In most cases this information is entered in the startup wizard when setting up the device for the first time. Once the mode is set, you have to factory reset the device to change modes.

USAGE:

```
xCommand Provisioning SetType Type: Type
```

where

Type: PairedToCodec/Standalone

PairedToCodec: The Room Navigator is to be onboarded in paired mode.

Standalone: The Room Navigator is to be onboarded in stand-alone mode.

Security commands

xCommand Security Certificates CA Add

Requires user role: ADMIN

Uploads CA security certificates to this device. This is a multiline command.

USAGE:

```
xCommand Security Certificates CA Add
```

xCommand Security Certificates CA Delete

Requires user role: ADMIN

Deletes a CA security certificate from this device.

USAGE:

```
xCommand 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:

```
xCommand Security Certificates CA Show [Format: Format]
```

where

Format: PEM/Text - Default value: Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

xCommand Security Certificates Services Activate

Requires user role: ADMIN

Activates a security certificate on this device.

USAGE:

```
xCommand Security Certificates Services Activate Fingerprint: "Fingerprint"
Purpose: Purpose
```

where

Fingerprint: String (0, 1024)

The unique identifier (ID) for the certificate that is activated. You can get the fingerprint ID by running xCommand Security Certificates Services Show.

Purpose: 802.1X/Audit/HTTPS/HttpClient/HttpProxy/Pairing/SIP/WebexIdentity

The purpose of this certificate.

802.1X: For applying 802.1x security authentication.

Audit: Not applicable for a stand-alone Room Navigator.

HTTPS: For applying HTTPS security authentication.

HttpClient: For use with mutual TLS authentication when using the xCommand HttpClient commands.

HttpProxy: Not in use in this software version.

Pairing: Not applicable for a stand-alone Room Navigator.

SIP: Not applicable for a stand-alone Room Navigator.

WebexIdentity: For identifying the device in end-to-end encryption scenarios on the Webex cloud. Activates a specific certificate for WebexIdentity. For this Purpose, the command requires the identifying fingerprint to be encrypted and serialized in a JWE blob.

xCommand Security Certificates Services Add

Requires user role: ADMIN

Uploads security certificates to this device. This is a multiline command.

USAGE:

```
xCommand Security Certificates Services Add [PrivateKeyPassword:
"PrivateKeyPassword"]
```

where

PrivateKeyPassword: String (0, 128) - Default value: ""

Stores the details of the private key for the password.

xCommand Security Certificates Services Deactivate

Requires user role: ADMIN

Deactivates security certificates on this device.

USAGE:

```
xCommand Security Certificates Services Deactivate Fingerprint: "Fingerprint"
Purpose: Purpose
```

where

Fingerprint: String (0, 1024)

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/Audit/HTTPS/HttpClient/HttpProxy/Pairing/SIP/WebexIdentity)

The purpose of this certificate.

802.1X: For applying 802.1x security authentication.

Audit: Not applicable for a stand-alone Room Navigator.

HTTPS: For applying HTTPS security authentication.

HttpClient: For use with Mutual TLS authentication when using the xCommand HttpClient commands.

HttpProxy: Not in use in this software version.

Pairing: Not applicable for a stand-alone Room Navigator.

SIP: Not applicable for a stand-alone Room Navigator.

WebexIdentity: For identifying the device in end-to-end encryption scenarios on the Webex cloud. Activates a specific certificate for WebexIdentity. For this Purpose, the command requires the identifying fingerprint to be encrypted and serialized in a JWE blob.

xCommand Security Certificates Services Delete

Requires user role: ADMIN

Deletes security certificates from this device.

USAGE:

```
xCommand 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:

```
xCommand Security Certificates Services Show [Filter: Filter]
[FingerprintAlgorithm: FingerprintAlgorithm] [Format: Format]
```

where

Filter: 802.1X/Audit/HTTPS/HttpClient/HttpProxy/Pairing/SIP/WebexIdentity

The purpose of this certificate.

802.1X: For applying 802.1x security authentication.

Audit: Not applicable for a stand-alone Room Navigator.

HTTPS: For applying HTTPS security authentication.

HttpClient: For use with Mutual TLS authentication when using the xCommand HttpClient commands.

HttpProxy: Not in use in this software version.

Pairing: Not applicable for a stand-alone Room Navigator.

SIP: Not applicable for a stand-alone Room Navigator.

WebexIdentity: For identifying the device in end-to-end encryption scenarios on the Webex cloud. Activates a specific certificate for WebexIdentity. For this Purpose, the command requires the identifying fingerprint to be encrypted and serialized in a JWE blob.

FingerprintAlgorithm: SHA-1/SHA-256 - Default value: SHA-1

Specifies which hash function is used when generating the fingerprint of the certificate.

SHA-1: The SHA-1 hash function is used.

SHA-256: The SHA-256 hash function (from the SHA-2 family of hash functions) is used.

Format: PEM/Text - Default value: Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain 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:

```
xCommand 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:

```
xCommand 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:

```
xCommand Security Certificates ThirdParty List
```

xCommand Security Certificates ThirdParty Show

Requires user role: ADMIN

Shows a single third-party certificate.

USAGE:

```
xCommand 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 - Default value: Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

xCommand Security Certificates Webex Show

Requires user role: ADMIN, USER

This command applies only to devices that are registered to the Webex cloud service.

Shows the list of trusted CA certificates that verifies the certificates of servers and services used by the Webex cloud.

USAGE:

```
xCommand 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 - Default value: Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

xCommand Security Certificates WebexIdentity Show

Requires user role: ADMIN, USER

This command applies only to devices that are registered to Webex cloud service.

Shows the root Certificate Authority (CA) list for Webex Identity.

USAGE:

```
xCommand Security Certificates WebexIdentity Show [Filter: Filter] [Format: Format]
```

where

Filter: External/Internal

Internal: Shows the list of internal certificate authorities.

External: Shows a list of external certificate authorities.

Format: PEM/Text – Default value: Text

Specifies the format of the listed certificates, PEM (Privacy Enhanced Mail) or plain text.

xCommand Security Ciphers List

Requires user role: ADMIN

List the ciphers supported by various services (domains). Result:

Name: Name of this domain.

* Syslog-TLS: Used for logging over TLS.
* HTTPS server: Used by the device's own web server.
* HTTPS client: Used for all https client traffic from the device.
* Pairing: Not applicable for stand-alone Room Navigator.
* SIP TLS: Not applicable for stand-alone Room Navigator.

Cipherlist: The actual cipher list string sent to the TLS library.

Ciphers: A space-separated list of ciphers by their TLS standard name.

USAGE:

```
xCommand Security Ciphers List
```

xCommand Security ClientSecret Populate

Requires user role: ADMIN

This command applies only to devices that are registered to the Webex cloud service.

Accepts a base64url encoded plain text value for seeding the client secret on the device for the first time.

To update the secret after that first time, you must supply a JWE blob containing the new secret encrypted by the old secret.

This is a multiline command.

USAGE:

```
xCommand Security ClientSecret Populate Secret: "Secret"
```

where

Secret: String (0, 1024)

First time: Supply a base64url encoded plain text value.

Thereafter: Supply a JWE blob containing the new secret encrypted by the old secret.

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:

```
xCommand Security Persistency Configurations: Configurations InternalLogging: InternalLogging DHCP: DHCP ConfirmAndReboot: ConfirmAndReboot
```

where

Configurations: NonPersistent/Persistent

In non-persistent mode, all configurations are set back to default when the device reboots.

InternalLogging: NonPersistent/Persistent

In non-persistent mode eventlog 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:

```
xCommand Security Session Get
```

xCommand Security Session List

Requires user role: ADMIN

List active sessions.

USAGE:

```
xCommand Security Session List
```

xCommand Security Session Terminate

Requires user role: ADMIN

Terminate a session.

USAGE:

```
xCommand Security Session Terminate SessionId: "SessionId"
```

where

SessionId: String (0, 32)

The session ID number.

SystemUnit commands

xCommand SystemUnit Boot

Requires user role: ADMIN, INTEGRATOR, USER

Reboot the device.

USAGE:

```
xCommand SystemUnit Boot [Action: Action] [Force: Force]
```

where

Action: Restart/Shutdown - Default value: Restart

As a default the device restarts after a reboot. By selecting Shutdown, the device will not restart.

Force: False/True - Default value: True

As a default the device reboots right away, regardless of whether the device is in use or not. By selecting False, the device reboots only if not in use (that is, in idle, standby, or halfwake mode).

xCommand SystemUnit DeveloperPreview Activate

Requires user role: ADMIN

Activate developer preview mode. When developer preview mode is activated and you have a DeveloperPreview option key installed, you will get access to public-api-preview xAPI nodes.

USAGE:

```
xCommand SystemUnit DeveloperPreview Activate
```

xCommand SystemUnit DeveloperPreview Deactivate

Requires user role: ADMIN

Deactivate developer preview mode.

USAGE:

```
xCommand SystemUnit DeveloperPreview Deactivate
```

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:

```
xCommand SystemUnit FactoryReset Confirm: Confirm [Keep: Keep]
[TrailingAction: TrailingAction]
```

where

Confirm: Yes

Include to confirm your choice.

Keep: Certificates/HTTP/LocalSetup/Network/Provisioning/RemoteSupportUser/Webex

Select which configurations and files to keep when you factory reset the device.

Certificates:

Client and CA certificates.

HTTP:

xConfiguration NetworkServices HTTP Mode
xConfiguration NetworkServices HTTPS Server MinimumTLSVersion
xConfiguration NetworkServices HTTPS StrictTransportSecurity
xConfiguration NetworkServices HTTPS VerifyClientCertificate

LocalSetup:

xConfiguration Time Zone
xConfiguration UserInterface Language

Network:

xConfiguration Network 1 *

Provisioning:

xConfiguration Provisioning Mode

RemoteSupportUser:

The remote support user (if any).

Webex:

xConfiguration Spark ServiceOverrides GdsBaseUrl
xConfiguration Spark ServiceOverrides U2CBaseUrl

TrailingAction: NoAction/Restart/Shutdown - Default value: Restart

Select Shutdown or NoAction to override the default behavior (Restart).

xCommand SystemUnit SetTouchPanelMode

Requires user role: ADMIN, INTEGRATOR

A Room Navigator can be the user interface for a video conferencing device, be a room booking device, or display a persistent web app. The information, buttons, and controls displayed on the screen depend on the mode. This command determines which of these modes the Room Navigator is to be onboarded in. Controller mode is only available when paired to a video conferencing device; the other modes can be used both when paired and stand-alone.

In most cases this information is entered in the startup wizard when setting up the device for the first time. Once the mode is set, you have to factory reset the device to change modes.

USAGE:

```
xCommand SystemUnit SetTouchPanelMode Mode: Mode
```

where

Mode: Controller/Scheduler/PersistentWebApp

Controller: The Room Navigator is the user interface of a video conferencing device.

Scheduler: The Room Navigator is used for room booking.

PersistentWebApp: A third-party web application (persistent web app) is running on the Room Navigator.

xCommand SystemUnit SignInBanner Clear

Requires user role: ADMIN

Clear the sign in banner set with xCommand SystemUnit SignInBanner Set.

USAGE:

```
xCommand SystemUnit SignInBanner Clear
```

xCommand SystemUnit SignInBanner Get

Requires user role: ADMIN, USER

Get the custom message set with xCommand SystemUnit SignInBanner Set.

USAGE:

```
xCommand SystemUnit SignInBanner Get
```

xCommand SystemUnit SignInBanner Set

Requires user role: ADMIN

Set up a sign in banner, which is a message that the users see before they sign in to the device's web interface or the command line interface. This is a multiline command.

Use:

xCommand SystemUnit SignInBanner Set <enter>

Banner text <enter>

. <enter>

USAGE:

```
xCommand SystemUnit SignInBanner Set
```

xCommand SystemUnit WelcomeBanner Clear

Requires user role: ADMIN

Clear the welcome banner set with xCommand SystemUnit WelcomeBanner Set.

USAGE:

```
xCommand 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:

```
xCommand SystemUnit WelcomeBanner Get
```

xCommand SystemUnit WelcomeBanner Set

Requires user role: ADMIN

Set up a welcome banner that the users see 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 must be aware of when changing settings. This is a multiline command.

Use:

xCommand SystemUnit WelcomeBanner Set <enter>

Banner text <enter>

. <enter>

USAGE:

```
xCommand SystemUnit WelcomeBanner Set
```

Time commands

xCommand Time DateTime Get

Requires user role: ADMIN, USER

Read the time and date from the device.

USAGE:

```
xCommand 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:

```
xCommand 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 LedControl Color Set

Requires user role: ADMIN, INTEGRATOR

The wall mount version of the Room Navigator has LED lights. Use this command to specify the color and turn the LED lights on or off.

The UserInterface LedControl Mode setting must be Manual for this command to have any effect.

USAGE:

```
xCommand UserInterface LedControl Color Set Color: Color
```

where

Color: Green/Off/Red/Yellow

Off: Turn the LED lights off.

Green/Red/Yellow: Turn on the LED lights with the specified color.

xCommand UserInterface WebView Display

Requires user role: ADMIN, INTEGRATOR, USER

Opens the web view and displays the web page given by the URL.

USAGE:

```
xCommand UserInterface WebView Display [Header: "Header"] [Options: "Options"]
[Title: "Title"] Url: "Url"
```

where

Header: String (0, 8192)

An HTTP header field. You can add up 15 Header parameters in one command, each holding one HTTP header field.

Options: String (0, 255)

This parameter is intended for internal use by the UI Extensions Editor, which is not available for a stand-alone Room Navigator.

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:

```
xCommand 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:

```
xCommand 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:

```
xCommand 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:

```
xCommand UserManagement RemoteSupportUser GetState
```

xCommand UserManagement User Add

Requires user role: ADMIN

Adds a new user to this device.

USAGE:

```
xCommand UserManagement User Add [Active: Active] [ClientCertificateDN:
"ClientCertificateDN"] Passphrase: "Passphrase" [PassphraseChangeRequired:
PassphraseChangeRequired] 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 signs in with a client certificate instead of a username and password.

Passphrase: String (0, 255)

The passphrase for the user.

PassphraseChangeRequired: False/True

Specifies whether the user must change his passphrase on the next sign-in.

Role: Admin/Audit/Integrator/RoomControl/User

Sets the user's role(s). You can assign more than one role to a user by adding multiple Role parameters.

ShellLogin: False/True

Specifies whether the user should have a shell login or not.

Username: String (0, 127)

The user's username.

YourPassphrase: String (0, 255)

The passphrase for the user you are signed in as when running this command.

xCommand UserManagement User Delete

Requires user role: ADMIN

Deletes a user from this device.

USAGE:

```
xCommand UserManagement User Delete Username: "Username" [YourPassphrase:
"YourPassphrase"]
```

where

Username: String (0, 127)

The username of the user that will be deleted.

YourPassphrase: String (0, 255)

The passphrase for the user you are signed in as when running this command.

xCommand UserManagement User Get

Requires user role: ADMIN

Shows the details of a user on this device. You must supply either a Username or ClientCertificateDN to identify the user.

USAGE:

```
xCommand 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:

```
xCommand UserManagement User List [Limit: Limit] [Offset: Offset]
```

where

Limit: Integer (0..65536) - Default value: 0

Limits the number of users that are shown to this number. 0 means no limit, i.e, all users are listed.

Offset: Integer (0..65536) - Default value: 0

Shows a list with users starting from index X, where X is the Offset. That is, the first X-1 users are not shown.

xCommand UserManagement User Modify

Requires user role: ADMIN

Modifies the details of a particular user.

USAGE:

```
xCommand UserManagement User Modify [Active: Active] [AddRole: AddRole]
[ClientCertificateDN: "ClientCertificateDN"] [PassphraseChangeRequired:
PassphraseChangeRequired] [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 signs in with a client certificate instead of a username and password.

PassphraseChangeRequired: False/True

Specifies whether the user must change his passphrase on the next sign-in.

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)

The user's username.

YourPassphrase: String (0, 255)

The passphrase for the user you are signed in as when running this command.

xCommand UserManagement User Passphrase Change

Requires user role: ADMIN, AUDIT, INTEGRATOR, ROOMCONTROL, USER

Change the passphrase for the user you are signed in as. If you are signed in as the administrator, this will change the administrator passphrase.

USAGE:

```
xCommand UserManagement User Passphrase Change NewPassphrase: "NewPassphrase"
OldPassphrase: "OldPassphrase"
```

where

NewPassphrase: String (0, 255)

The passphrase you are changing to (new).

OldPassphrase: String (0, 255)

The passphrase you are changing from (old).

xCommand UserManagement User Passphrase Set

Requires user role: ADMIN

Set a passphrase for the specified user. You must be signed in as an administrator to set a user's passphrase.

USAGE:

```
xCommand UserManagement User Passphrase Set NewPassphrase: "NewPassphrase"
Username: "Username" [YourPassphrase: "YourPassphrase"]
```

where

NewPassphrase: String (0, 255)

The passphrase you are changing to (new).

Username: String (0, 127)

The username of the user you are setting a new passphrase for.

YourPassphrase: String (0, 255)

The passphrase for the user you are signed in as when running this command.

xCommand UserManagement User Unblock

Requires user role: ADMIN

Unblocks a user who is blocked out because of too many failed sign-in attempts.

USAGE:

```
xCommand UserManagement User Unblock Username: "Username" [YourPassphrase:
"YourPassphrase"]
```

where

Username: String (0, 127)

The username of the user that will be unblocked.

YourPassphrase: String (0, 255)

The passphrase for the user you are signed in as when running this command.

WebEngine commands

xCommand WebEngine DeleteStorage

Requires user role: ADMIN

Deletes session data for web view types, such as web apps.

USAGE:

```
xCommand WebEngine DeleteStorage [Type: Type]
```

where

Type: All/PersistentWebApp/Signage/WebApps - Default value: All

All: Deletes the session data for all web view types.

PersistentWebApp: Deletes the session data related to persistent web apps.

Signage: Not applicable for stand-alone Room Navigator.

WebApps: Not applicable for stand-alone Room Navigator.

xCommand WebEngine Logging Set

Requires user role: ADMIN, USER

Set what type of messages to add in the web engine log files. The level you set determines how serious an issue must be to be included in the logs. Messages for the set level and up (more serious) are included in the web engine logs. So, if you choose the lowest level (Verbose) the most information is added to the logs; if you choose the highest level (Fatal), only the most serious errors such as software crashes are added. The Verbose log level can be further refined by using the Verbosity parameter. All these log levels are as defined by Chromium.

USAGE:

```
xCommand WebEngine Logging Set Level: Level [Verbosity: Verbosity]
```

where

Level: Verbose/Info/Warning/Error/Fatal

The log level. The lowest level (most logging) is Verbose, then Info, Warning, Error, and finally the highest level is Fatal (least logging).

Verbosity: Integer (-20..-1) - Default value: -1

Refined log level for Verbose. -1 gives the least logging and -20 the most.

xCommand WebEngine Tracing Start

Requires user role: ADMIN, USER

Starts a chromium trace for use with advanced debugging. Please see the chromium documentation. Note that this generates a lot of data, so be mindful of the duration of the trace. Ideally, use the Duration parameter or the WebEngine Tracing Stop command to limit the trace to just a few seconds, to capture exactly the issue and nothing more. The resulting trace data is stored in /run/webengine_traces (requires remote access to the device).

USAGE:

```
xCommand WebEngine Tracing Start [CustomCategories: "CustomCategories"]
[Duration: Duration] Mode: Mode [Systrace: Systrace]
```

where

CustomCategories: String (0, 2048)

Only used when the Mode parameter is set to Custom. Allows you to manually specify which chromium categories to include in the trace. Accepts a comma-separated list of chromium tracing categories.

Duration: Integer (1..1800) - Default value: 15

The duration of the trace recording in seconds.

Mode: Custom/FrameViewer/InputLatency/JavascriptAndRendering/Rendering/WebDeveloper

Set a predefined set of categories to use in the trace. Each category captures different data. If Custom is chosen, see the CustomCategories parameter.

Systrace: Off/On - Default value: On

On: Use the Android Systrace format for the trace file (recommended).

Off: Use the legacy format for the trace file.

xCommand WebEngine Tracing Stop

Requires user role: ADMIN, USER

Stop an ongoing trace prematurely. If there is no active trace, nothing is done.

USAGE:

```
xCommand WebEngine Tracing Stop
```

Webex commands

xCommand Webex Registration Cancel

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Cancel device registration to Webex.

This command only works in the short period after the registration is started with xCommand Webex Registration Start.

USAGE:

```
xCommand Webex Registration Cancel
```

xCommand Webex Registration Start

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Register a device to the Webex cloud service, by entering the device activation code. Also choose whether to keep or deactivate existing local users.

Unless you add the AccountLinkMode parameter, you will get a confirmation that the registration has been successful or failed.

USAGE:

```
xCommand Webex Registration Start [AccountLinkMode: AccountLinkMode]
ActivationCode: "ActivationCode" SecurityAction: SecurityAction
```

where

AccountLinkMode: Asynchronous

When adding this parameter, the command returns immediately and doesn't wait for account linking to complete. This is convenient in cases where the command may time out and return "failed" before the account linking is complete.

ActivationCode: String (0, 128)

The activation code for the device.

SecurityAction: Harden/NoAction

Harden: Deactivate all existing local users when registering the device.

NoAction: Register the device as it is. No changes to local users and macros.

Statuses

Software version: RoomOS 11.9.2

Bookings status

xStatus Bookings Availability Status

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Indicates when and if a room is booked and for how long.
Valuespace of the result returned: BookedUntil/Free/FreeUntil

Free: The room is not booked for the foreseeable future, and the Bookings Availability TimeStamp status is empty (" ").

FreeUntil: The room is free right now, but there is a later booking. The start of the booking is in the Bookings Availability TimeStamp status.

BookedUntil: The room is booked right now, and the current booking's ending is in the Bookings Availability TimeStamp status.

Example:

```
xStatus Bookings Availability Status
*s Bookings Availability Status: Free
** end
```

xStatus Bookings Availability TimeStamp

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

A timestamp or an empty string set according to the room's current Bookings Availability Status.
Valuespace of the result returned: String

Example:

```
xStatus Bookings Availability TimeStamp
*s Bookings Availability TimeStamp: ""
** end
```

xStatus Bookings Current Id

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

The ID of the on going booking event, if any.
Valuespace of the result returned: String

Example:

```
xStatus Bookings Current Id
*s Bookings Current Id: "123"
** end
```

Diagnostics status

xStatus Diagnostics Message [n] Description

Requires user role: ADMIN, USER

Shows a description of the current diagnostics alerts.

Valuespace 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.

Valuespace of the result returned: Error/Warning/Critical

Error: There is an error in the device. The device can still be used, but there can be some restrictions.

Warning: A problem is detected and a more specific report follows indicating the exact problem.

Critical: The warning level is critical. The device cannot be used.

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.

Valuespace 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.

Valuespace of the result returned: ANATOnVCS/AbnormalCallTermination/ AirPlayBeacon/AirPlayProvisioning/AirPlayProvisioningCertificates/AmplifierDetection/ AmplifierFanStatus/AudioInternalSpeakerDisabled/AudioPairingInterference/ AudioPairingNoise/AudioPairingRate/AudioPairingSNR/AudioPairingTokenDecode/ BluetoothAudioInterference/BluetoothHardware/CAPFOperationState/CTLinstallation/ CUCMAndCloudConfigurability/CUCMVendorConfigurationFile/CallHistoryConfiguration/ CallProtocolDualStackConfig/CallProtocolIPStackPlatformCompatibility/ CallProtocolInvalidCloudProv/CallProtocolVcsProvisioningCompatibility/ CameraDetected/CameraId/CameraPairing/CameraSerial/CameraSoftwareVersion/ CameraStatus/CapsetFilterConfiguration/CaptivePortalDetected/ CertificateExpiry/CloudAwareConfigInvalid/CloudConfigurationWriteback/ CompanionModeIncompatibilityLocal/CompanionModeIncompatibilityRemote/ ConfigurationFile/ContactInfoMismatch/ControlSystemConnection/ CurrentNetworkQuality/DefaultCallProtocolRegistered/DeveloperPreview/ DigitalMicrophoneStatus/ECReferenceDelay/EmbeddedWebViewFailedToLoad/ EmbeddedWebViewTerminatedUnexpectedly/EthernetDuplexMatches/FanStatus/ FirstTimeWizardNotCompleted/H323EncrAes256AndDHSize/H323GatekeeperStatus/ HTTPFeedbackFailed/HTTPSModeSecurity/HasActiveCallProtocol/HasValidReleaseKey/ HdmiCecModeNoSound/HologramCameras/HotdeskConfiguration/ HotdeskKioskExclusivity/HttpProxyStatus/InstantMeetingConfiguration/IPv4Assignment/ IPv6Assignment/IPv6Mtu/ITLinstallation/InternalXapiAccessDenied/InternalXapiUsage/ InvalidSIPTransportConfig/IpCameraStatus/KioskSettingsMenuLockConfiguration/ KioskURLConfiguration/KioskWebEngineModeConfiguration/ KioskWebViewPageLoadStatus/KioskWebViewStatus/LockedDeviceCompanionMode/ LockDown/LowBattery/MacrosErrorLogged/MacrosProvisioningStatus/ MacrosRuntimeActive/MacrosRuntimeHasHadCrash/MacrosRuntimeResponsiveness/ MacrosRuntimeStopped/MediaBlockingDetected/MediaPortRangeNegative/ MediaPortRangeOdd/MediaPortRangeOverlap/MediaPortRangeTooSmall/ MediaPortRangeValueSpace/MicrophoneMuteOverride/MicrophoneOverloaded/ MicrophonePower/MicrophonesConnected/MiracastConfiguration/ MiracastWiredOnlyStatus/MiracastWpsPinLocked/MissingDisplay/MissingThirdDisplay/ MonitorDelay/MonitorFirmwareVersion/NavigatorDeviceLocationConfiguration/ NTPStatus/NetLinkStatus/NetSpeedAutoNegotiated/NetworkConnectivity/ NetworkQuality/NetworkSwitch/OSDVideoOutput/OutputConnectorLocations/ PIILoggingMode/PanoramaCameraHdmi/PanoramaView/PeripheralSoftwareUpgrade/ PeripheralSoftwareVersion/PersistentWebAppFailedToLoad/ PersistentWebAppTerminatedUnexpectedly/PersistentWebAppURLConfiguration/ PlatformSanity/PoEStatus/PresentationSourceSelection/PresenterTrack/ ProvModeWebexAndWebexEdgeEnabled/ProvisioningDeveloperOptions/ ProvisioningModeAndStatus/ProvisioningStatus/RoomControl/ RoomSchedulingConfiguration/SIPEncryption/SIPListenPortAndRegistration/ SIPProfileRegistration/SIPProfileType/SelectedVideoInputSourceConnected/ SignageFailedToLoad/SignageTerminatedUnexpectedly/SipIceAndAnatConflict/ SipOrH323ButNotBothEnabled/SoftwareUpgrade/SoftwareUpgradeAvailability/ SoftwareUpgradeKeepsFailing/SpeakerTrackEthernetConnection/

SpeakerTrackFrontPanelMountedCorrectly/SpeakerTrackMicrophoneConnection/ SpeakerTrackVideoInputs/StandbyCtrlOfficeHoursConfiguration/StylusBattery/ TCPMediaFallback/ThousandEyesStatus/TLSVerifyRequiredCerts/ TemperatureCheck/TouchDeviceRunningMTRMemoryStatus/ TouchPanelConnection/USBAudioSeparation/USBCameraMode/USBInterfaceType/ USBMicType/UltrasoundConfigSettings/UltrasoundSpeakerAvailability/ ValidPasswords/VideoFromInternalCamera/VideoInputSignalQuality/ VideoInputStability/VideoPortRangeNegative/VideoPortRangeOdd/ VideoPortRangeTooSmall/VideoPortRangeValueSpace/WebRTCCalling/ WebRTCWebViewTerminatedUnexpectedly/WebexAccountPlusWebexEdgeEnabled/ WebexActivationRequired/WebexAudioProximityConnectivity/ WebexConnectivity/WebexEdgeAccountPendingCloudRegistration/ WebexEdgeAccountPlusProvModeWebex/WebexLyraConnectivity/ WebexMustUpgradeCeSoftware/WebexNfcProximityConnectivity/ WebexNotificationConnectivity/WebexOffline/WebexQRCodeProximityConnectivity/ WebexShouldUpgradeCeSoftware/WebexUsbcProximityConnectivity/ WebWidgetTerminatedUnexpectedly/WifiCARequired/WirelessCharging/ WirelessConnectionStatus/XapiApiKeyWebsocketHttpsDisabled

Example:

```
xStatus Diagnostics Message Type
*s Diagnostics Message 1 Type: PersistentWebAppURLConfiguration
** end
```

Network status

xStatus Network [n] ActiveInterface

Requires user role: ADMIN, USER

Returns the type of network interface the device is currently connected to.

Valuespace of the result returned: LAN/WLAN

LAN: The device is connected to a wired Ethernet network.

WLAN: The device is connected to a Wi-Fi network.

Example:

```
xStatus Network 1 ActiveInterface
  *s Network 1 ActiveInterface: LAN
  ** end
```

xStatus Network [n] CDP Address

Requires user role: ADMIN, USER

Returns the first network address of both receiving and sending devices.

Valuespace 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.

Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace of the result returned: String

Example:
```
xStatus Network 1 IPv6 LinkLocalAddress
*s Network 1 IPv6 LinkLocalAddress: "2001:DB8:0000:0000:0000:0000:0000:0001"
** end
```

xStatus Network [n] VLAN Voice VlanId

Requires user role: ADMIN, USER

The feedback shows the VLAN Voice ID.
Valuespace of the result returned: Off/1..4094

Off: The VLAN Voice Mode is not enabled.
1..4094: VLAN Voice ID

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.
Valuespace 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.
Valuespace 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.
Valuespace of the result returned: Discarded/Synced/NotSynced/Unknown/Off

Discarded: The NTP result has been discarded.
Synced: The device is in sync with the NTP server.
NotSynced: The device is not in sync with the NTP server.
Unknown: The state of the synchronization is unknown.
Off: No synchronization with the NTP server.

Example:
```
xStatus NetworkServices NTP Status
*s NetworkServices NTP Status: Synced
** end
```

Provisioning status

xStatus Provisioning ProvisioningType

Requires user role: ADMIN, USER

Reports whether the Room Navigator is set up as a stand-alone device or if it's paired to a video conferencing device (either directly or via the network). Refer to the Provisioning SetType command.
Valuespace of the result returned: NotSet/PairedToCodec/Standalone

NotSet: Information about the provisioning type is not known.
PairedToCodec: The Room Navigator is paired to a video conferencing device.
Standalone: The Room Navigator is set up as a stand-alone device.

Example:
```
xStatus Provisioning ProvisioningType
*s Provisioning ProvisioningType: Standalone
** end
```

xStatus Provisioning Software Current CompletedAt

Requires user role: ADMIN, USER

Shows date and time for when the current software upgrade was completed.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace 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.
Valuespace of the result returned: None/AboutToInstallUpgrade/DownloadDone/DownloadPaused/DownloadPending/Downloading/Installing/InstallingPeripherals/Postponed/UpgradingPeripherals

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.
Valuespace 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.
Valuespace 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.
Valuespace of the result returned: Low/Medium/Critical

Specifies the urgency of the software upgrade.

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.
Valuespace 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.
Valuespace 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.
Valuespace of the result returned: Failed/AuthenticationFailed/Provisioned/Idle/NeedConfig/ConfigError

Failed: The provisioning failed.
AuthenticationFailed: The authentication failed.
Provisioned: The device is provisioned.
Idle: The provisioning is not active.
NeedConfig: The device needs to be configured.
ConfigError: An error occurred during configuration.

Example:
```
xStatus Provisioning Status
*s Provisioning Status: Provisioned
** end
```

RoomAnalytics status

xStatus RoomAnalytics AmbientTemperature

Requires user role: ADMIN, USER

Shows the ambient temperature for the device.
Valuespace of the result returned: String

Example:
```
xStatus RoomAnalytics AmbientTemperature
  *s RoomAnalytics AmbientTemperature: "20.7"
  ** end
```

xStatus RoomAnalytics RelativeHumidity

Requires user role: ADMIN, USER

Shows the relative humidity for the device.
Valuespace of the result returned: Integer

Example:
```
xStatus RoomAnalytics RelativeHumidity
  *s RoomAnalytics RelativeHumidity: 26
  ** end
```

Standby status

xStatus Standby State

Requires user role: ADMIN, INTEGRATOR, ROOMCONTROL, USER

Shows whether the device is in standby mode or not.

Valuespace of the result returned: Standby/EnteringStandby/Halfwake/Off

Standby: The device is in standby state.

EnteringStandby: The device is entering the standby state.

Halfwake: The device is in standby, but greets the user when presence is detected by motion or the Proximity pairing app.

Off: The device is not in standby.

Example:

```
 xStatus Standby State
*s Standby State: Off
** end
```

SystemUnit status

xStatus SystemUnit DeveloperPreview Mode

Requires user role: ADMIN, USER

Shows whether developer preview mode is On or Off. This is controlled by the SystemUnit DeveloperPreview Activate and SystemUnit DeveloperPreview Activate commands.

Valuespace of the result returned: On/Off

Example:

```
 xStatusSystemUnit DeveloperPreview Mode
*s SystemUnit DeveloperPreview Mode: Off
** end
```

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.

Valuespace of the result returned: String

Shows the compatibility level for the device.

Example:

```
 xStatus SystemUnit Hardware Module CompatibilityLevel
*s SystemUnit Hardware Module CompatibilityLevel: 1
** end
```

xStatus SystemUnit Hardware Module DeviceId

Requires user role: ADMIN, USER

Shows a unique and persistent identifier for the device's hardware module.

Valuespace of the result returned: String

Example:

```
 xStatus SystemUnit Hardware Module DeviceId
*s SystemUnit Hardware Module DeviceId: "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
** end
```

xStatus SystemUnit Hardware Module Pcb

Requires user role: ADMIN, USER

Shows the identifier of the device's PCB.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Hardware Module Pcb
*s SystemUnit Hardware Module Pcb: "xx-xxxxxx"
** end
```

xStatus SystemUnit Hardware Module SerialNumber

Requires user role: ADMIN, USER

Shows the serial number of the hardware module in the device.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Hardware MainBoard SerialNumber
*s SystemUnit Hardware MainBoard SerialNumber: "FOC99999999"
** end
```

xStatus SystemUnit LastShutdownReason

Requires user role: ADMIN, USER

Returns the reason for the last shutdown of the device.
Valuespace of the result returned: ConvertToCloud/DisableHdmiOutput/EnableHdmiOutput/FactoryReset/FirstBoot/ModifySecurityPersistency/Restart/Shutdown/Standby/Unknown/Upgrade

Example:
```
xStatus SystemUnit LastShutdownReason
  *s SystemUnit LastShutdownReason: Upgrade
  ** end
```

xStatus SystemUnit LastShutdownTime

Requires user role: ADMIN, USER

Returns the date and time for the last shutdown of the device. The format of the returned string is: YYYY-MM-DDThh:mm:ssZ
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit LastShutdownTime
  *s SystemUnit LastShutdownTime: "2023-11-09T23:36:01Z"
  ** end
```

xStatus SystemUnit Notifications Notification [n] Text

Requires user role: ADMIN, USER

Lists text related to important system notifications. Notifications are issued, for example 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 SystemUnit Notifications RemoveAll command.
Valuespace 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, for example 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 SystemUnit Notifications RemoveAll command.
Valuespace of the result returned: SoftwareUpgradeOK/SoftwareUpgradeFailed/RebootRequired/Other

SoftwareUpgradeOK: This value is returned after a successful software upgrade.
SoftwareUpgradeFailed: This value is returned after a failed software upgrade attempt.
RebootRequired: This value is returned when a reboot is required.
Other: This value is returned for any other notifications.

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.
Valuespace of the result returned: String ("Cisco Room Navigator")

Example:
```
xStatus SystemUnit ProductId
*s SystemUnit ProductId: "Cisco Room Navigator"
** end
```

xStatus SystemUnit ProductPlatform

Requires user role: ADMIN, USER

Shows the product platform.
Valuespace of the result returned: String ("Room Navigator")

Example:
```
xStatus SystemUnit ProductPlatform
*s SystemUnit ProductPlatform: "Room Navigator"
** end
```

xStatus SystemUnit ProductType

Requires user role: ADMIN, USER

Shows the product type.
Valuespace of the result returned: String ("Cisco Codec")

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.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Software DisplayName
*s SystemUnit Software DisplayName: "RoomOS 11.3.1.10 1e761f985a1 2023-03-18"
** end
```

xStatus SystemUnit Software Name

Requires user role: ADMIN, USER

Shows the name of the software that is installed on the device.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Software Name
*s SystemUnit Software Name: "s53350"
** end
```

xStatus SystemUnit Software OptionKeys RemoteMonitoring

Requires user role: ADMIN, USER

Shows if the RemoteMonitoring option key is installed on the device.
Valuespace 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.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Software ReleaseDate
*s SystemUnit Software ReleaseDate: "2023-03-22"
** end
```

xStatus SystemUnit Software Version

Requires user role: ADMIN, USER

Shows the software version installed on the device.
Valuespace of the result returned: String

Example:
```
xStatus SystemUnit Software Version
*s SystemUnit Software Version: "ce11.3.1.10.1e761f985a1"
** end
```

xStatus SystemUnit State System

Requires user role: ADMIN, USER

This status provides information about the state of the system within a system unit. The status returns a value indicating the state of the system within the system unit.

Valuespace of the result returned: InCall/Initialized/Initializing/Multisite/Sleeping

InCall: This value indicates that the system unit is currently in an active call.

Initialized: The system unit has completed the initialization process and is in a ready state.

Initializing: The system unit is currently going through the initialization process. The system unit is in the process of starting up before it can become fully operational.

Multisite: The system unit is operating in a MultiSite mode.

Sleeping: The system unit is in a sleep mode.

Example:

```
xStatus SystemUnit State System
  *s SystemUnit State System: InCall
  ** end
```

xStatus SystemUnit TouchPanel Location

Requires user role: ADMIN, USER

Reports the location of the Room Navigator. Refer to the SystemUnit TouchPanel Location setting.

Valuespace of the result returned: NotSet/InsideRoom/OutsideRoom

InsideRoom: The device is inside the room.

NotSet: Information about the location of the device is not known.

OutsideRoom: The device is outside the room.

Example:

```
xStatus SystemUnit TouchPanel Location
*s SystemUnit TouchPanel Location: OutsideRoom
** end
```

xStatus SystemUnit TouchPanel Mode

Requires user role: ADMIN, USER

Reports whether a Room Navigator is the user interface for a video conferencing device (controller), is a room booking device (scheduler), or displays a persistent web app. Refer to the SystemUnit SetTouchPanelMode command.

Valuespace of the result returned: NotSet/Controller/Scheduler/PersistentWebApp

NotSet: The mode is not known.

Controller: The Room Navigator is the user interface of a video conferencing device.

Scheduler: The Room Navigator is used for room booking.

PersistentWebApp: A third-party web application (persistent web app) is running on the Room Navigator.

Example:

```
xStatus SystemUnit TouchPanel Mode
*s SystemUnit TouchPanel Mode: PersistentWebApp
** end
```

xStatus SystemUnit Uptime

Requires user role: ADMIN, USER

Shows the number of seconds since the last restart of the device.

Valuespace 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.
Valuespace of the result returned: String

Example:
```
xStatus Time SystemTime
*s Time SystemTime: "2023-03-23T10:52:04+0100"
** end
```

UserInterface status

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.
Valuespace of the result returned: String

Example:
```
xStatus UserInterface ContactInfo Name
*s UserInterface ContactInfo Name: "MySystem"
** end
```

xStatus UserInterface LedControl Color

Requires user role: ADMIN, INTEGRATOR, USER

The wall mount version of the Room Navigator has LED lights. This status returns the state of the LED lights.
Valuespace of the result returned: Green/Off/Red/Yellow
Off: The LED lights are off.
Green/Red/Yellow: The LED lights are on, and they have the specified color.

Example:
```
xStatus UserInterface LedControl Color
*s UserInterface LedControl Color: Green
** end
```

xStatus UserInterface SettingsMenu Visibility

Requires user role: ADMIN, INTEGRATOR

This status reports whether or not the control panel, including the device settings panel, is part of the user interface.
Valuespace of the result returned: Visible/Hidden
Visible: The control panel is included in the user interface (swipe from right or tap the icon in the upper right corner of the user interface).
Hidden: The control panel is not shown.

Example:
```
xStatus UserInterface SettingsMenu Visibility
*s UserInterface SettingsMenu Visibility: Visible
** end
```

xStatus UserInterface WebView [n] Status

Requires user role: ADMIN, INTEGRATOR, USER

Shows whether a web view is being displayed currently or not.
Valuespace of the result returned: Visible/Error/NotVisible

Visible: A web view is being displayed.
NonVisible: No web view is being displayed.
Error: There is an error displaying a web view.

Example:

```
xStatus UserInterface WebView
*s UserInterface WebView 8 Status: Visible
** end
```

xStatus UserInterface WebView [n] Type

Requires user role: ADMIN, INTEGRATOR, USER

Shows the type of web view currently being displayed.
Valuespace of the result returned: ECM/ECMSignIn/EmbeddedApp/Integration/Kiosk/None/PersistentWebApp/Signage/WebApp/WebRTCMeeting

ECM: The web view is launched from the file browser to view a file hosted on an Enterprise Content Management (ECM) service.
ECMSignIn: The web view is launched by the system to authenticate the user (OAuth2) with an ECM service.
Integration: The web view is launched by the UserInterface WebView Display API command.
Kiosk: The web view is used for the kiosk application.
None: No web view is showing.
PersistentWebApp: The web view is used for a persistent web app.
Signage: The web view is used for the digital signage application.
WebApp: The web view is used for a web app.
WebRTCMeeting: The web view is used for a WebRTC Meeting (for example, Google Meet and Microsoft Teams).

Example:

```
xStatus UserInterface WebView
*s UserInterface WebView 8 Type: Integration
** end
```

xStatus UserInterface WebView [n] URL

Requires user role: ADMIN, INTEGRATOR, USER

Shows the URL of the web view that is currently being displayed.
Valuespace of the result returned: String

Example:

```
xStatus UserInterface WebView
*s UserInterface WebView 8 URL: "http://www.yr.no/"
** end
```

WebEngine status

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.

Valuespace of the result returned: On/Off

Example:

```
xStatus WebEngine Features WebEngine
*s WebEngine Features WebEngine: On
** end
```

xStatus WebEngine Tracing CustomCategories

Requires user role: ADMIN, USER

Valuespace of the result returned: String

Returns the list of custom categories (see the CustomCategories and Mode parameters of the WebEngine Tracing Start command). If no custom categories are used, this status returns an empty string.

Example:

```
xStatus WebEngine Tracing CustomCategories
  *s WebEngine Tracing CustomCategories: ""
  ** end
```

xStatus WebEngine Tracing Duration

Requires user role: ADMIN, USER

Returns the initial duration of the trace, in seconds (see the Duration parameter of the WebEngine Tracing Start command). Will be set to -1 when the trace ends.

Valuespace of the result returned: Integer

Example:

```
xStatus WebEngine Tracing Duration
  *s WebEngine Tracing Duration: 600
  ** end
```

xStatus WebEngine Tracing Mode

Requires user role: ADMIN, USER

Returns the mode used for the current trace (see the Mode parameter of the WebEngine Tracing Start command). Will be set to the empty string when the trace ends.

Valuespace of the result returned: Custom/FrameViewer/InputLatency/JavascriptAndRendering/Off/Rendering/WebDeveloper

Example:

```
xStatus WebEngine Tracing Mode
  *s WebEngine Tracing Mode: Rendering
  ** end
```

xStatus WebEngine Tracing Systrace

Requires user role: ADMIN, USER

Returns whether or not the Android Systrace format is used (see the Systrace parameter of the WebEngine Tracing Start command).

Valuespace of the result returned: Off/On

Example:

```
xStatus WebEngine Tracing Systrace
  *s WebEngine Tracing Systrace: On
  ** end
```

Webex status

xStatus Webex DeveloperId

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

This an id can be used to send cloud xAPI calls to devices through developer.webex.com.

The cloud xAPI allows you to send commands and status requests to devices that are registered to the Webex cloud service. Most xAPI requests require a deviceId which can be obtained using this status.

Valuespace of the result returned: String

Example:

```
 xStatus Webex DeveloperId
*s Webex DeveloperId: "********************"
** end
```

xStatus Webex Status

Requires user role: ADMIN, USER

Doesn't apply for a customer managed Room Navigator.

Reports the status of the connection between the device and the Webex cloud service. If the cloud service is up and running, the status reports Registered.

Valuespace of the result returned: Disabled/Error/Registered/Registering/Stopped

Example:

```
 xStatus Webex Status
*s Webex Status: Registered
** end
```

Other configurations (not for programming)

The following configurations are only available from the device web interface. They are not part of the public API, and you cannot use them for programming. They can be removed or changed without further notice.

Other configurations

Software version: RoomOS 11.9.2

Logging Internal Mode

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

Specify 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.

Default value: **On**

Valuespace: *Off/On*

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

On: System logs will be stored on the device.

NetworkServices CommonProxy

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

This setting is only for Cisco internal use. Do not change it.

NetworkServices HTTP Proxy Authentication Method

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

This setting is only for Cisco internal use. Do not change it.

NetworkServices XMLAPI Mode

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

Enable or disable the device's XML API. For security reasons this may be disabled. Disabling the XML API may limit the remote manageability of the device.

Default value: **On**

Valuespace: *Off/On*

Off: The XML API is disabled.

On: The XML API is enabled.

RoomScheduler BookingTimeout

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

Doesn't apply for a customer managed Room Navigator.

The scheduler will provide immediate feedback to a user when they book a room or a device; however, the calendar service can take some time to confirm the booking. If it takes too long to get the confirmation and this time exceeds the value set here, the booking will be cleared, and the device or room will be shown as available.

Default value: **60**

Valuespace: *Integer (60..300)*

The number of seconds to wait for a confirmation.

SystemUnit CrashReporting Advanced

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

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 use only and not available to customers.

Default value: **On**

Valuespace: *Off/On*

Off: The ACR tool will perform standard log analyses.

On: The ACR tool will perform advanced log analyses.

UserInterface Bookings Visibility TentativeMeetings

Requires user role: ADMIN, INTEGRATOR, USER

Availability: Only on device web interface (not for programming)

In general, the list of upcoming meetings is shown on the screen and touch controller. Set whether to include tentative meetings in the list.

Default value: **Auto**

Valuespace: *Auto/Hidden*

Auto: Tentative meetings are included in the list.

Hidden: Tentative meetings are not in the list.

UserInterface Bookings Visibility Title

Requires user role: ADMIN, INTEGRATOR, USER

Availability: Only on device web interface (not for programming)

Sets the meeting details to private. "Scheduled meeting" will be displayed as the title of the meeting.

Default value: **Auto**

Valuespace: *Auto/Hidden*

Auto: The title of the meeting is public and will be displayed on the user interface.

Hidden: The title of the meeting will be hidden and "Scheduled meeting" will be displayed on the user interface.

UserInterface PortraitOrientationSupport

Requires user role: ADMIN

Availability: Only on device web interface (not for programming)

Not applicable in this version.

Customer managed Room Navigator in stand-alone mode

Room Navigator can be setup as a customer managed device which is controlled through the xAPI or the device web interface. Software upgrades and configurations are managed by the customer.

A customer managed Room Navigator can be used for persistent web apps. The app that you select displays on the Room Navigator's entire screen, replacing the RoomOS user interface, and it can't be dismissed by end-users.

Software

To onboard a Room Navigator as customer managed device, it needs to be running software version RoomOS September 2023 11.8 or later.

You can download the software for a customer managed Room Navigator from: WHERE?

You can SSH to the Room Navigator to upgrade the software.

Access the API with SSH. Connect using the IP address or hostname of the device. When the device is new, or has been factory reset, the username is *admin*, and the password is blank.

Run the following command:

```
swupgrade https://binaries.webex.com/collaboration-endpoint-ce-production-stable/20230903194148/bifrost.pkg
```

Factory reset

Unless the Room Navigator is new, you need to factory reset it before setup.

- From tshell: Run

  ```
  xCommand SystemUnit FactoryReset Confirm: Yes
  ```

- Physical reset: You can find the reset button on the back of the Room Navigator. Use a paper clip (or similar) to press and hold the recessed reset button until the screen turns black (approximately 10 seconds). Then release the button.

Password

The device comes with a default administrator user account with full access rights. The username is *admin*, and initially, no passphrase is set.

It is mandatory to set a passphrase for the default admin user in order to restrict access to device configuration.

Setup Room Navigator through xAPI

You can find detailed command descriptions in this guide.

Set Room Navigator to Persistent Web App mode

```
xCommand SystemUnit SetTouchPanelMode Mode: PersistentWebApp
```

Set Room Navigator in Standalone mode

```
xCommand Provisioning SetType Type: Standalone
```

Set Room Navigator to Customer Managed Mode

```
xConfiguration Provisioning Mode: Off
```

Set Room Navigator Location (Note: Selecting NotSet may cause issues on the Room Navigator)

```
xConfiguration SystemUnit TouchPanel Location: <InsideRoom/NotSet/OutsideRoom>
```

Set Time Zone

```
xConfiguration Time Zone: <Your time zone>
```

Set Language

```
xConfiguration UserInterface Language: <UI language>
```

Set Admin Passphrase

```
xCommand UserManagement User Passphrase Set Username: admin YourPassphrase:
<old passphrase> NewPassphrase: <new eight-character-phrase>
```

Exit First Time Wizard

```
xCommand SystemUnit FirstTimeWizard Stop
```

Setup Room Navigator from first-time wizard

On a factory reset or new device, go through setup wizard on the Room Navigator's UI.

1. Select the UI language and tap *Start*.
2. Tap *Set up as standalone*.
3. Select *Persistent web app*.
4. Select the location of the Room Navigator.
5. Setup the network settings as preferred and tap *Continue*.
6. Select time zone and tap *Continue*.
7. Select *Customer managed setup* and tap *Continue* to confirm the choice.
8. Set an eight-character admin password for the Room Navigator and tap *Enter*.
9. The setup is complete. Tap *Continue*.

If you haven't setup a persistent web app, the device goes into an out of service screen. See the Setup persistent web app section in this chapter.

Setup persistent web app

You can find detailed command descriptions in this guide.

Launch Web App on Navigator

```
xConfiguration UserInterface HomeScreen Peripherals WebApp URL: <URL>
```

Set web engine that should be allowed. This should match the domain above

```
xConfiguration WebEngine Features Xapi Peripherals AllowedHosts Hosts:
<hostname>
```

Enable JSXAPI over websocket for use within persistent web app

```
xConfiguration Security XAPI WebSocket APIKey Allowed: True
```

Set the ability to control the LED strip on device

```
xConfiguration UserInterface LedControl Mode: Manual
```

Open the Settings menu

To access the *Settings* menu on a Room Navigator in customer managed mode, tap the screen three times with three fingers.

In the *Settings* menu you can find:

- Information about the device, such as the IP address, and software version.
- Issues and diagnostics. You can also send logs from the device from this menu.
- Restart and factory reset.

Cisco contacts

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

Go to: ▶ https://www.cisco.com/go/offices

Corporate Headquarters

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134 USA

Intellectual property rights

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)