White Paper

Cloud Collaboration Security White Paper Series

Cloud Aware On-Premises Video Devices

Webex Edge for Devices

Version 2.0 (September 2020)

Webex Edge for Devices allows Cisco devices on Unified CM and VCS/Expressway to link with the Webex cloud. With Webex Edge for Devices your cloud registered, and on-premises linked devices can be monitored and managed via Webex Control Hub. With Webex Edge for Devices features that are typically served to cloud devices can be extended to on premises devices. This White Paper provides details of how Webex Edge for devices works and the benefits and features that it offers. *

* Some of the Cisco products, services, and features described in this document are still under development or planned for future. After being described, a planned feature will be marked with a "🔨" icon. Cisco will have no liability for delay in the delivery or failure to deliver the products, services or features marked with this icon.

Introduction

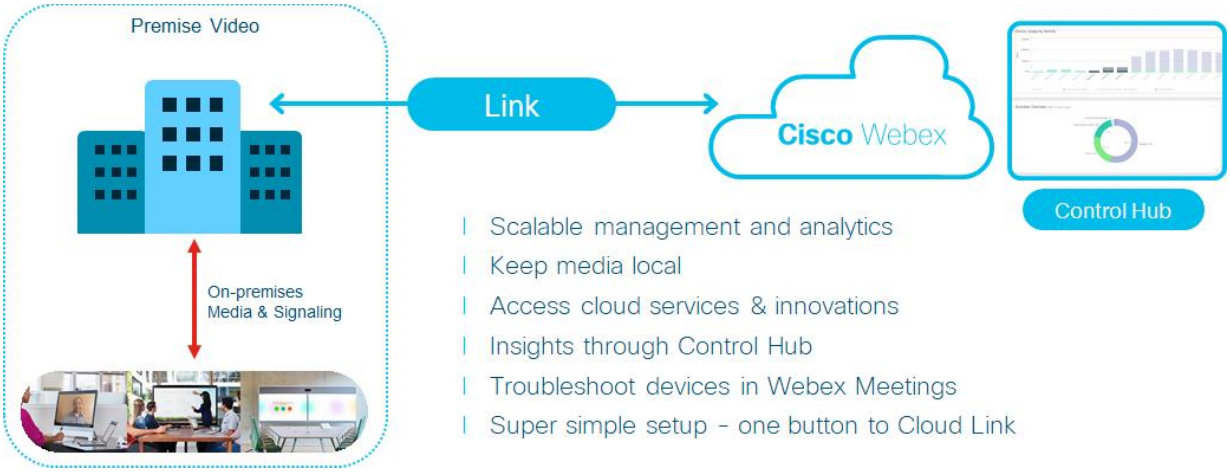
Hosting Webex in the cloud enables Cisco to rapidly develop and deploy services and features on our powerful cloud platform using new and innovative technologies. These new features and services can now be extended to customers with on-premises Cisco products. Video devices registered to Unified CM or VCS/Expressway can now also be linked to the Webex cloud and benefit from features that can only be cloud delivered.

With Webex Edge for Devices, customers with a mixture of on-premises and cloud video devices can monitor and manage these devices from a single administrative platform, Webex Control Hub. On-premises video devices maintain their registration to Unified CM or VCS/Expressway and the media path for calls between these devices remains the same, but they also have an additional link to the Webex cloud for management, analytics and more.

Webex Edge for Devices currently offers the following features and functionality:

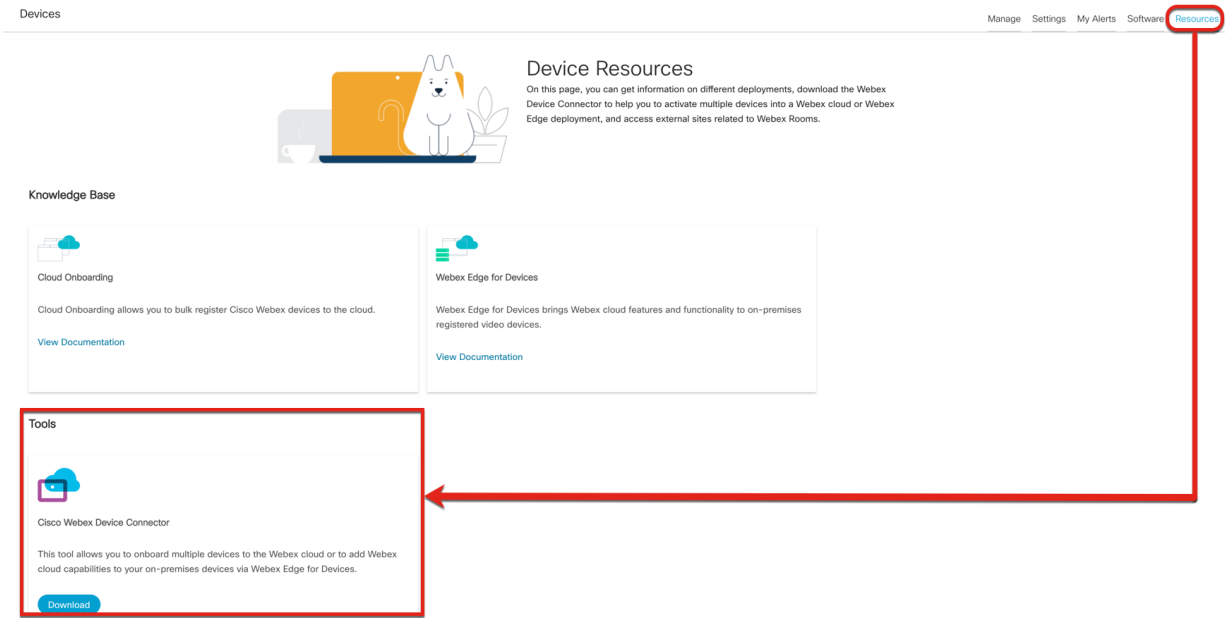
- Online/Offline Connection Status in Webex Control Hub
- Device Diagnostics with the ability to set admin alerts
- Device Historical Analytics available directly in Webex Control Hub
- Cloud xAPI Access
- Real Time Troubleshooting of Webex Meetings
- Hybrid Calendar through Webex Control Hub
- Webex Assistant
- Cloud Management – Configurations
- Workspace Metrics
    - Occupancy detection
    - Call Detection
    - Sound levels and ambient noise (dBA)

Figure 1- Webex Edge for Devices – overview



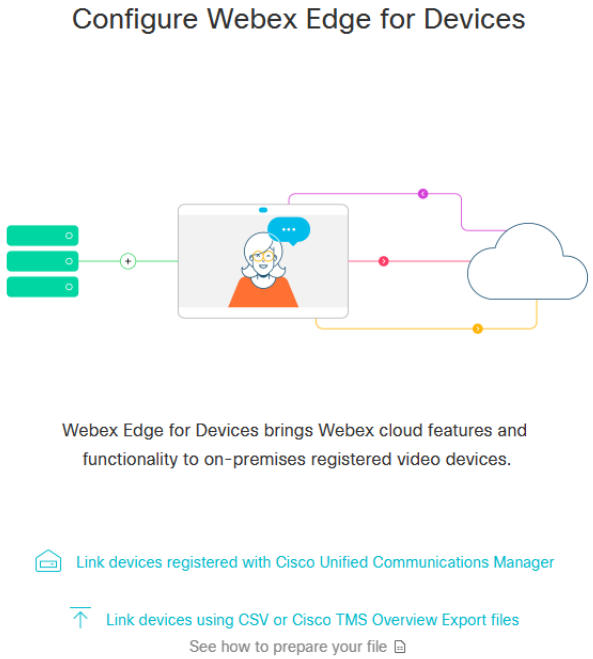
Webex Edge for Devices – Device Onboarding and Cloud Linking

To onboard and link on-premises devices to the Webex Cloud, start by downloading the Cisco Webex Device Connector desktop application from Webex Control Hub.



Cisco Webex Device Connector provides an onboarding service for Unified CM and VCS/Expressway registered devices. The connector uses the AXL API to retrieve the names and MAC addresses of video devices configured in Unified CM. (VCS/Expressway deployments use a CSV file to import device details).

Figure 2 - Cisco Webex Device Connector – Webex Edge for Devices service

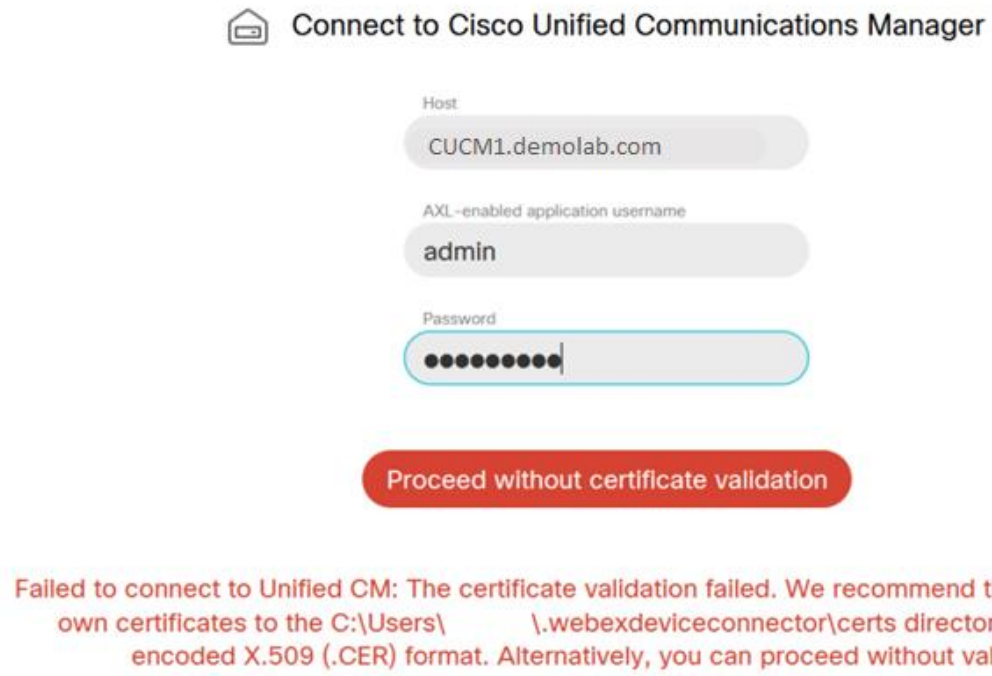


The connection from Cisco Webex Device Connector to Unified CM uses HTTPS with TLS version 1.2. Cisco Webex Device Connector validates the Unified CM (Tomcat) certificate, before proceeding with the connection. If the received server certificate is not trusted by the Java runtime default CA trust store, you will be prompted to either provide the certificate or proceed without certificate validation. If you are using a Proxy server in your enterprise network, the initial Cisco Webex Device Connector login page allows you to enter the Proxy server address and port number, and if required user credentials for Proxy Authentication (Basic and Digest authentication are supported).

TLS intercept is currently not supported between the Device Connector tool and the Webex Cloud.

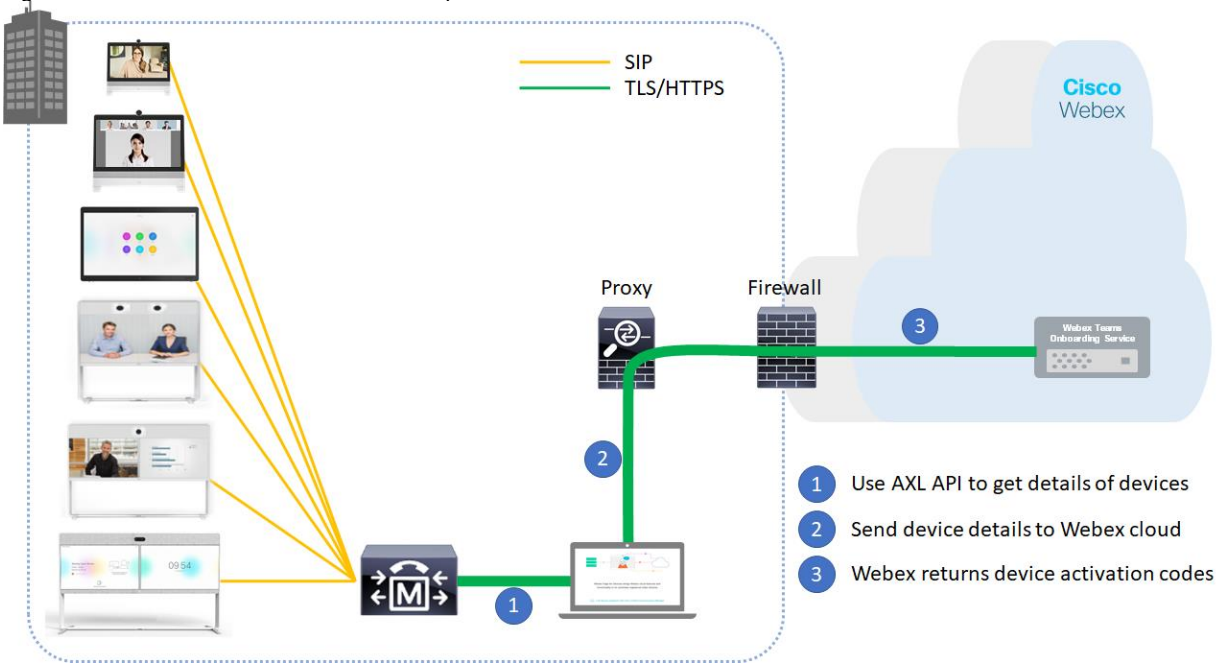
To connect to a Unified CM cluster, you will need to activate the Cisco AXL Web Service (disabled by default) and create a user account in your cluster with the Standard AXL API Access entitlement.

Figure 3 – Connecting from Cisco Webex Device Connector to Unified CM (showing the certificate validation failure message)



As shown in Figure 4, when the Cisco Webex Device Connector has retrieved the names and MAC addresses of video devices configured in Unified CM, it establishes a TLS connection to the Webex cloud and sends these details to the Webex identity service along with details of your Webex organization. The Webex identity service creates an activation code for each device and returns these the Cisco Webex Device Connector, which in turn forwards these on to the Unified CM cluster.

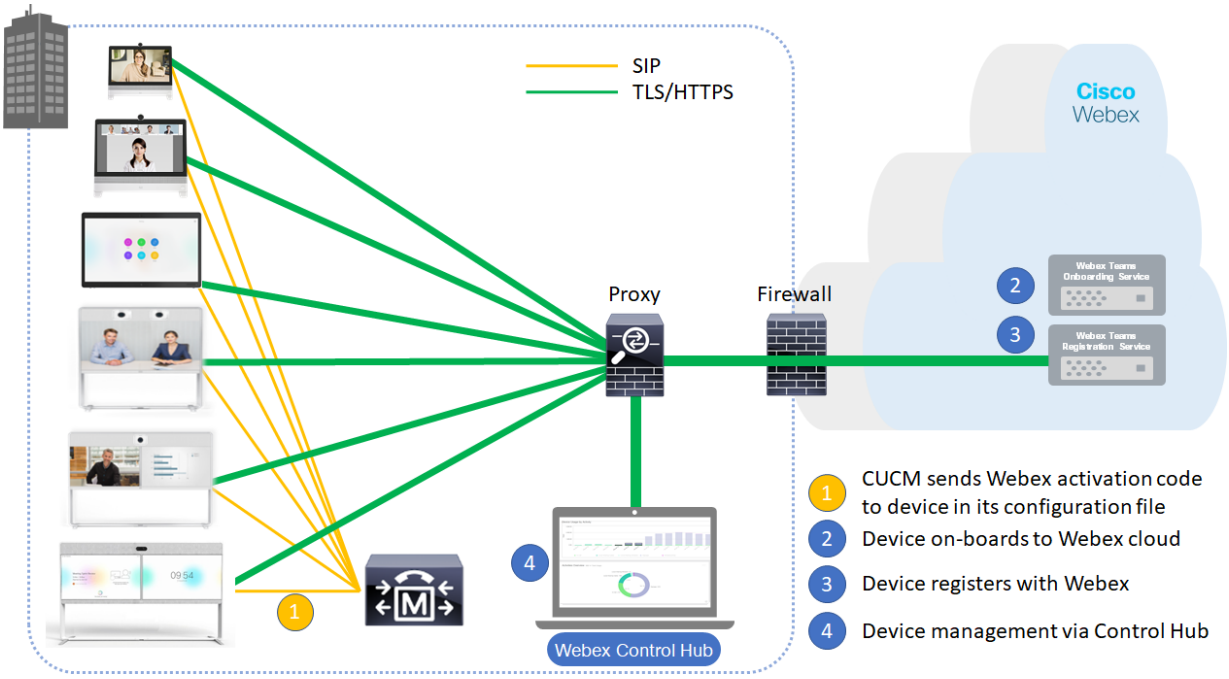
Figure 4 - Cisco Webex Device Connector operation



As shown in Figure 5, Unified CM sends the activation code in a configuration file to each video device. Cisco Webex video devices running software version CE9.12.3 or above, can establish a TLS connection to the Webex cloud and use the activation code received from CUCM to automatically onboard and link to your Webex organization.

These cloud linked on-premises devices can then be viewed and managed in Webex Control Hub.

Figure 5 – On Premises devices – Cloud On-boarding and Linking



Webex Edge for Devices – Enterprise Network Security Considerations

Webex Edge for Devices allows on-premises devices to be linked over the internet to Webex cloud services. These on-premises devices make multiple TLS/HTTPS connections to the Webex Cloud for signalling, these connections are outbound only and some connections are upgraded from HTTPS to bi-directional Secure WebSocket (WSS) connections.

The signalling connections from on-premises devices to Webex services use TLS version 1.2 only and negotiate the following strong cipher suites with Webex services, in order of preference:

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Most security conscious customers deploy both a firewall and proxy server to control access from applications and devices in their enterprise networks to the Internet and associated cloud services, such as Webex. Specific implementations may vary, but a common deployment forces all HTTP-based traffic through a proxy server allowing only

HTTP traffic originating from the proxy server to traverse the firewall and reach the Internet.

Proxies can be used to perform several security functions such as URL whitelisting and blacklisting, user authentication, IP address/domain/hostname/URI reputation look up, and traffic decryption and inspection.

HTTP Proxy support has until now only been supported for full Webex deployment. The feature has been re-worked for CE9.12.3 and above in order to support Webex Edge for Devices.

When the on-premises device is linked via Webex Edge for Devices (supported from CE9.12.3 and above):

- All HTTP requests to the Webex Cloud will use the configured HTTP Proxy.
- Any HTTP requests targeted for provisioning (Unified CM/TMS/Expressway) or phonebook will bypass the proxy settings.

Cisco Webex video devices connecting to the Webex Cloud support the following proxy server features:

Proxy Server configuration: WPAD, PAC, or Manual
Proxy Authentication: No Auth, Basic, Digest
Proxy TLS inspection support: Yes

Please Note: The passwords used in the Proxy configuration are hashed and stored locally on the on-premises registered device. The passwords used are not synchronised to the Webex Cloud

To support proxy TLS inspection, the trust list downloaded into the video device during onboarding must be customized to include the enterprise CA certificate that the proxy presents to the device during TLS establishment. You can open a service request with Cisco TAC to create a custom trust list for devices in your organization.

The following table describes the URLs that are used by on premises devices linking to Webex. If your organization uses a proxy, ensure that these URLs can be accessed.

URL	Description
*.ciscospark.com	Webex services
*.wbx2.com	Webex services
*.webex.com	Authentication and Identity services
*.webexcontent.com	General File storage including: • Device Log Files • Software Updates
*.activation.webex.com *.activate.cisco.com *.webapps.cisco.com	Used for onboarding devices to the Webex service
speech.googleapis.com texttospeech.googleapis.com speech-services-manager-a.wbx2.com	Google Speech Services. Used by Webex Assistant to handle speech recognition and text-to-speech. Disabled by default, opt-in via Control Hub

Enabling Webex Edge for Devices does not change the media paths that your on-premises video devices use today and no additional IP subnets for voice, video and content sharing need to be whitelisted in your enterprise firewall.

Webex Edge for Devices – Data Privacy

Cisco Webex Device Connector and on-premises devices using Webex Edge encrypt all data in transit using TLS connections to the Webex Cloud.

Cisco Webex Device Connector signalling to and from the Webex Cloud is primarily used to send the cloud details of on-premises devices and to receive their activation codes for on-boarding. Cisco Webex Device Connector sends the following information about your on-premises devices to the Webex Cloud:

- Device name
- Device MAC address

Once your on-premises device has linked with the Webex Cloud, the device will send a subset of the signalling that is typically sent by a device that is registered only to the Webex Cloud. For example, your Webex Edge Device does not use Webex services to set up calls and to join meetings.

The following information is sent in the signalling channels from on-premises devices linked to the Webex cloud:

- MAC Address
- Serial Number
- IP Address
- Display Name
- Product Type
- Active Interface
- SIP Address
- Diagnostics Messages reported by the device
- Connected Cisco Peripherals
- Anonymous State Usage (In Call, Local Sharing, Standby, Signage etc)
- Media Quality Stats In-Call (Packet Loss, Bandwidth, Jitter, Latency)
- Hardware Performance Metrics (TAC Troubleshooting purposes)

This information is used by Webex Control Hub for monitoring and management features although Cisco may add additional functionality in later phases.

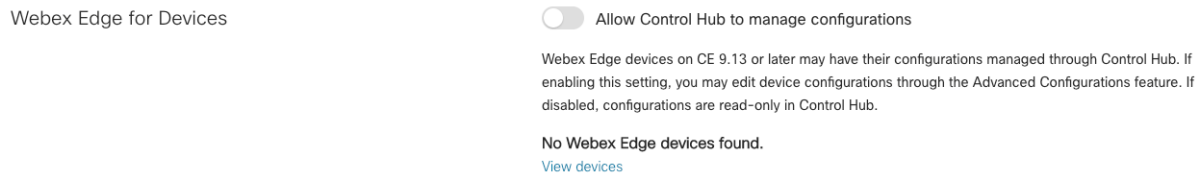
For details of how your personal information is managed and stored in the Webex cloud, see the Webex Teams Privacy data sheet:
https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

Webex Edge for Devices – Support for Cisco Webex Control Hub configuration management

This information is used by Webex Control Hub for monitoring and management features. CE9.13 is ready to let Cisco Webex Control Hub take care of the configuration management for devices linked via Webex Edge for Devices.
Configuration Management (write) is disabled in Control Hub by default and must be enabled to take effect.
If disabled, you will only be able to read the configuration from the devices.

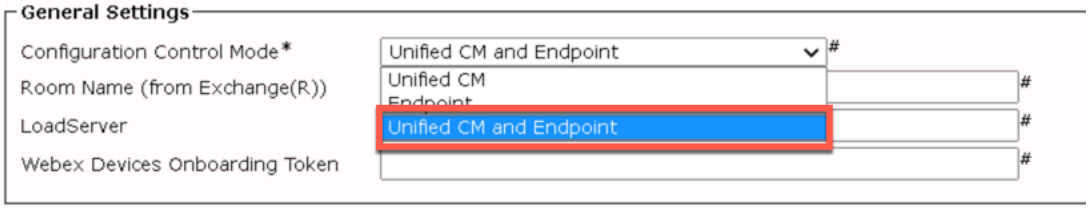
In order to change configurations on the device from Control Hub you must enable it in Control Hub (as shown in Figure 6 below).

Figure 6 – Webex Control Hub opt-in for Device Configuration



Please note that if the on-premises registered device is registered through Unified CM, the Configuration Control Mode must be set to 'Unified CM and Endpoint' for Webex Control Hub to be able to manage the on-premises device configuration as shown in Figure 7 below

Figure 7 – Unified CM Configuration Control Mode



When Control Hub is set to manage configurations the devices under such control will no longer accept most configurations from Unified CM except configurations not exposed in Control Hub. These settings are mostly related to network services and is to avoid making the device unreachable from Control Hub. The device will continue to accept these settings from Unified CM. Please see a list below for the most significant ones:

```
xconfig networkServices http proxy
xconfig networkServices h323
xconfig networkServices https
```

```
xconfig networkServices snmp
xconfig networkServices ssh hostkeyalgorithm
xconfig networkServices upnp
xconfig networkServices wifi
xconfig conference defaultcall protocol
xconfig conference encryption mode
xconfig phonebook
```

For details of how your personal information is managed and stored in the Webex cloud, see the Webex Teams Privacy data sheet : https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

The following information is sent in the signalling channels from on-premises devices linked to the Webex cloud:

- Device configuration

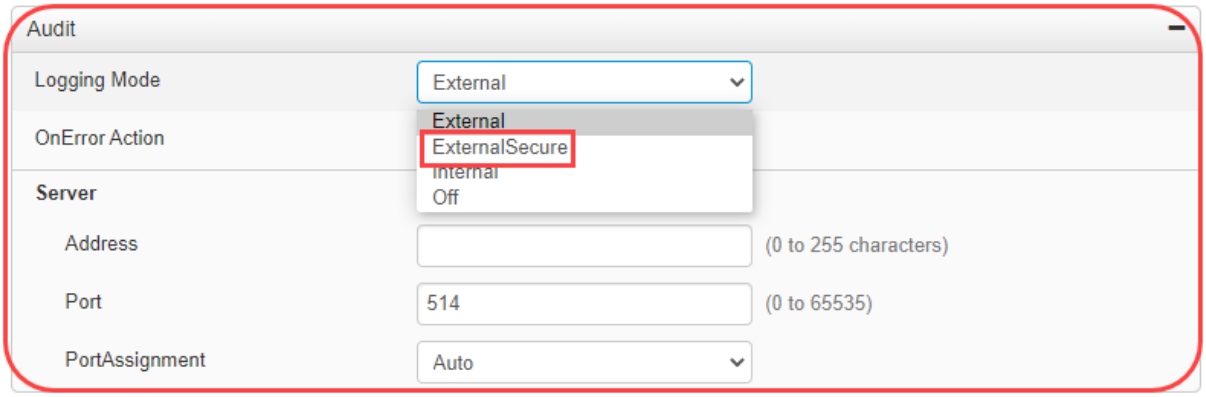
Please note that this is a bi-directional sync.

If not opted-in or Configuration Control Mode is set to Unified CM only, device configuration will be read-only.

Secure Audit Logging

When audit logging is enabled, all sign in activity and configuration changes on the device are recorded.
As standard, the audit log is local to the device. Of course, logs rotate and may not persist post reboot.

For a fully on-premises registered endpoint (not linked to the Webex Cloud through Webex Edge for Devices), it is possible to configure the endpoint to send the logs to an external audit server (syslog server).



With ExternalSecure audit logging mode enabled, the device sends encrypted audit logs to the external audit server. The identity of the external audit server must be verified by a signed certificate.
The signature of the audit server is verified using the the list of pre-installed CA Certificates or the custom CA list.

If the audit server authentication fails, no audit logs are sent to the external server.

With audit logging enabled, changes made by local admin via the web interface, SSH access and changes made via Unified CM or TMS will be logged to the syslog server.

With an on-premises registered endpoint that has also been linked to Webex Control Hub via the Device Connector tool, assuming the endpoint is running CE9.13 and above and Webex Control Hub has been opted in to allow Device Configuration, changes made via Webex Control Hub will be logged in Admin section with Troubleshooting section in Control Hub as well as being logged within the audit trail being sent to the syslog server.