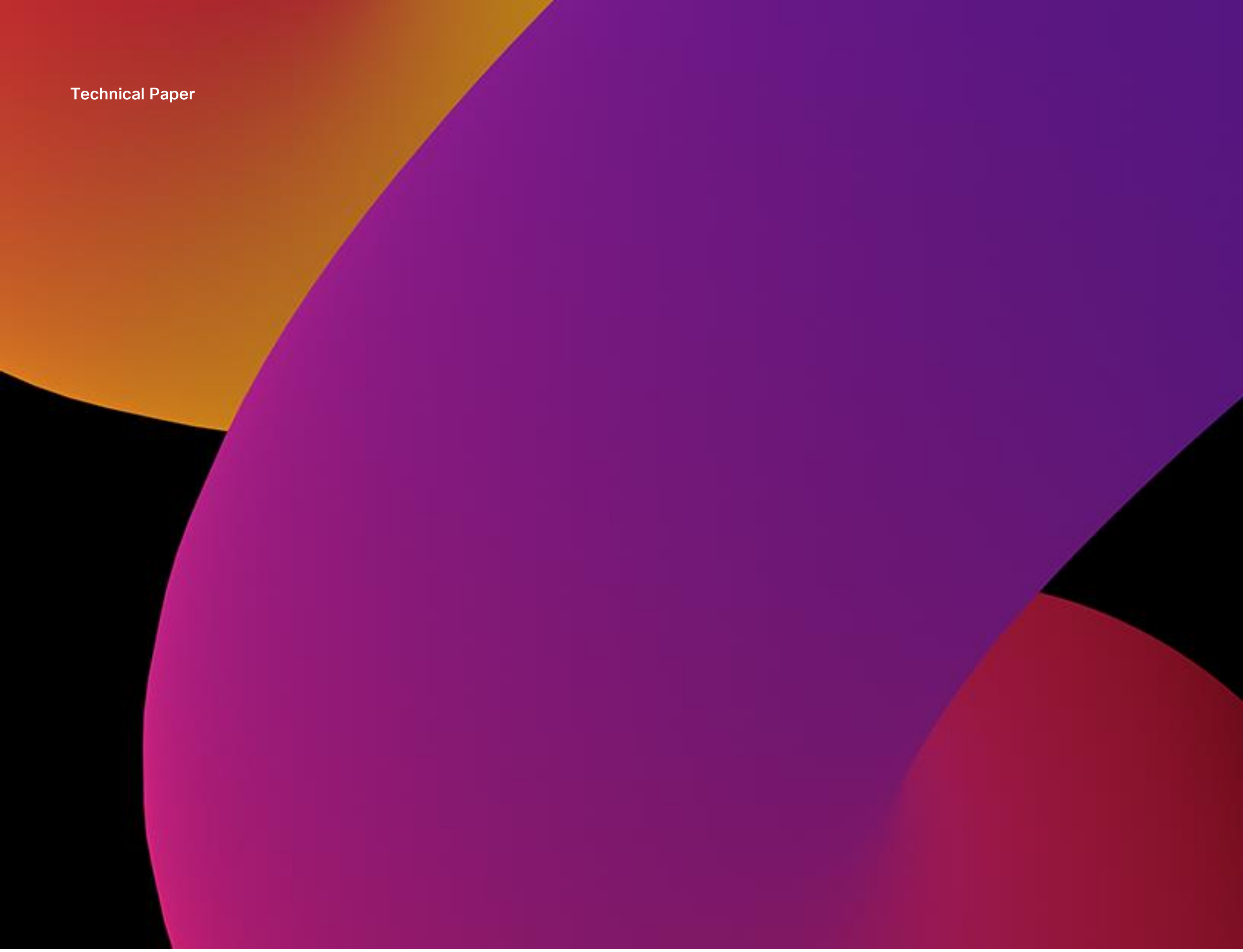
Technical Paper



Cloud Collaboration Security Paper

Webex Edge for Devices

December 2021

Contents

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 from Webex Control Hub. With Webex Edge for Devices, features that are typically served to cloud devices can be extended to on-premises devices. This Technical Paper provides details of how Webex Edge for Devices works and the benefits and features that it offers.

1. Introduction

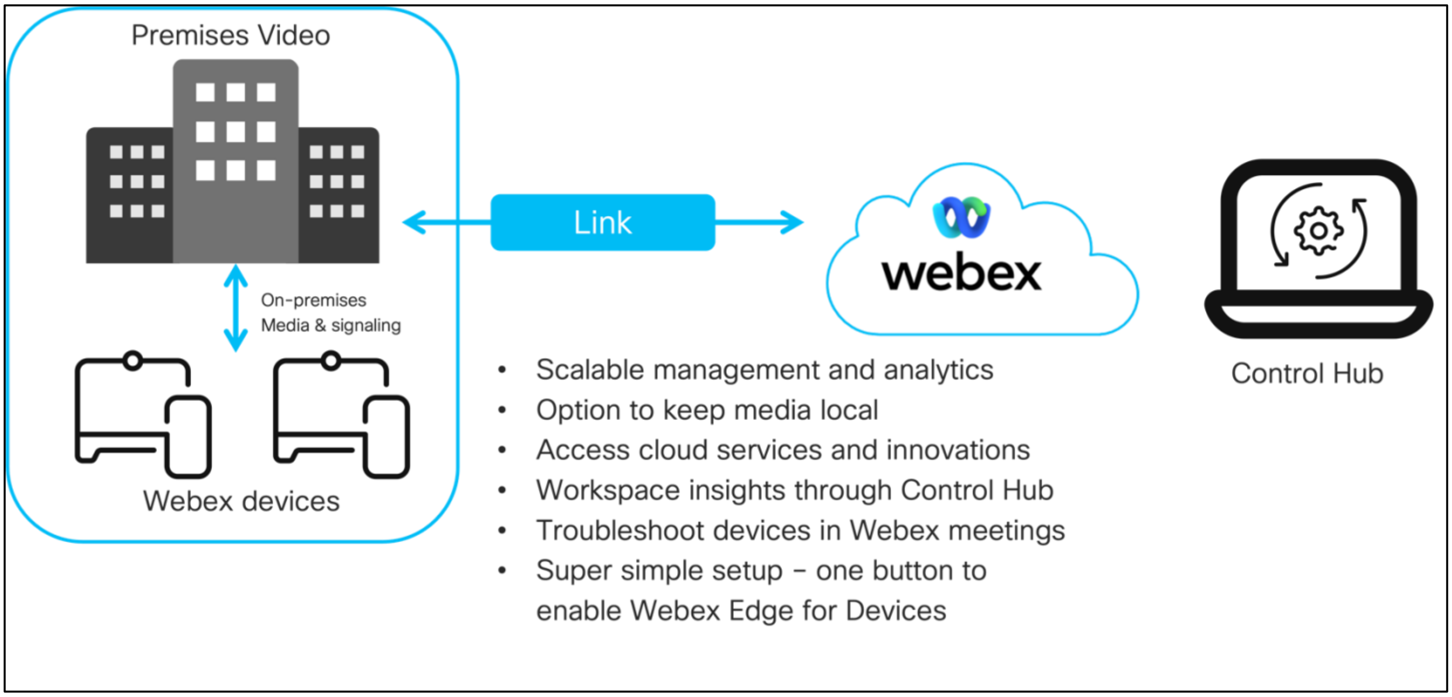
Hosting Webex in the cloud enables Cisco to rapidly develop and deploy services and features on our powerful cloud platform using new and innovative technologies. These new features and services can now be extended to customers with on-premises Cisco products. Video devices registered to Unified CM or 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, 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 Control Hub
- Device Diagnostics with the ability to set admin alerts
- Device Historical Analytics available directly in Control Hub
- Cloud xAPI Access
- Real-Time Troubleshooting of Webex Meetings
- Hybrid Calendar through Control Hub
- Webex Assistant
- Cloud Management – Configurations
- Workspace Metrics
    - Occupancy detection
    - Call Detection
    - Sound levels and ambient noise (dBA)
- Webex Optimized Meeting experience

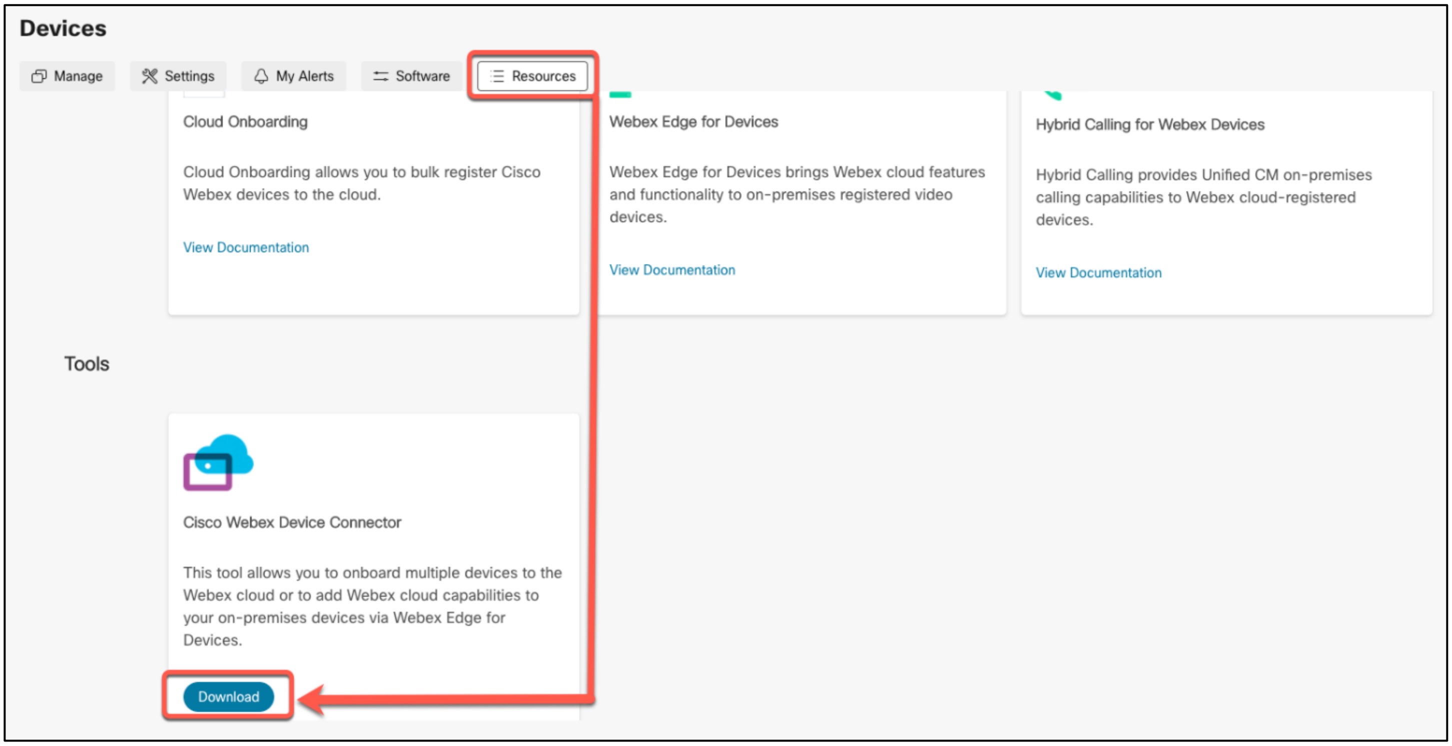
Figure 1 – Webex Edge for Devices overview



- Scalable management and analytics
- Option to keep media local
- Access cloud services and innovations
- Workspace insights through Control Hub
- Troubleshoot devices in Webex meetings
- Super simple setup – one button to enable Webex Edge for Devices

2. Webex Edge for Devices – Device onboarding and linking

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



Cloud Onboarding

Cloud Onboarding allows you to bulk register Cisco Webex devices to the cloud.

View Documentation

Webex Edge for Devices

Webex Edge for Devices brings Webex cloud features and functionality to on-premises registered video devices.

View Documentation

Hybrid Calling for Webex Devices

Hybrid Calling provides Unified CM on-premises calling capabilities to Webex cloud-registered devices.

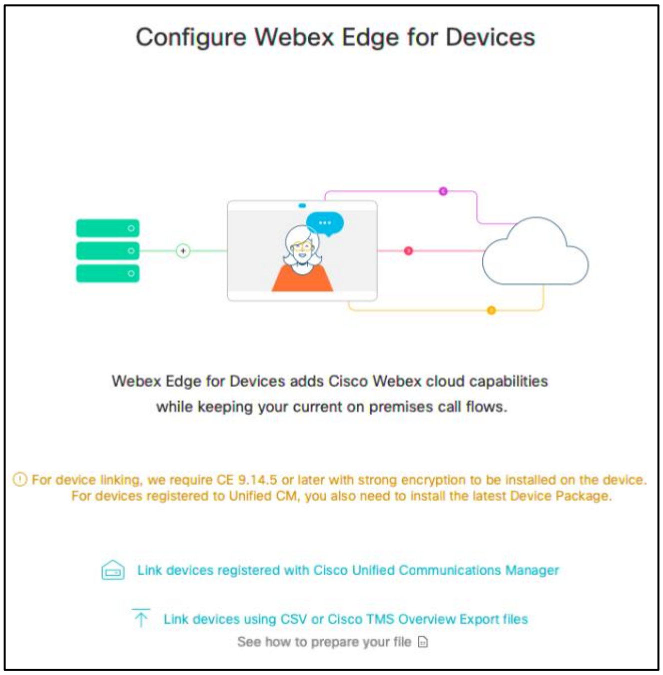
View Documentation

Cisco Webex Device Connector

This tool allows you to onboard multiple devices to the Webex cloud or to add Webex cloud capabilities to your on-premises devices via Webex Edge for Devices.

The 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 – Webex Device Connector – Webex Edge for Devices



Configure Webex Edge for Devices

Webex Edge for Devices adds Cisco Webex cloud capabilities while keeping your current on premises call flows.

ⓘ For device linking, we require CE 9.14.5 or later with strong encryption to be installed on the device. For devices registered to Unified CM, you also need to install the latest Device Package.

Link devices registered with Cisco Unified Communications Manager

Link devices using CSV or Cisco TMS Overview Export files

See how to prepare your file

The connection from Webex Device Connector to Unified CM uses HTTPS with TLS version 1.2. The 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. The error message is shown in Figure 3 below.

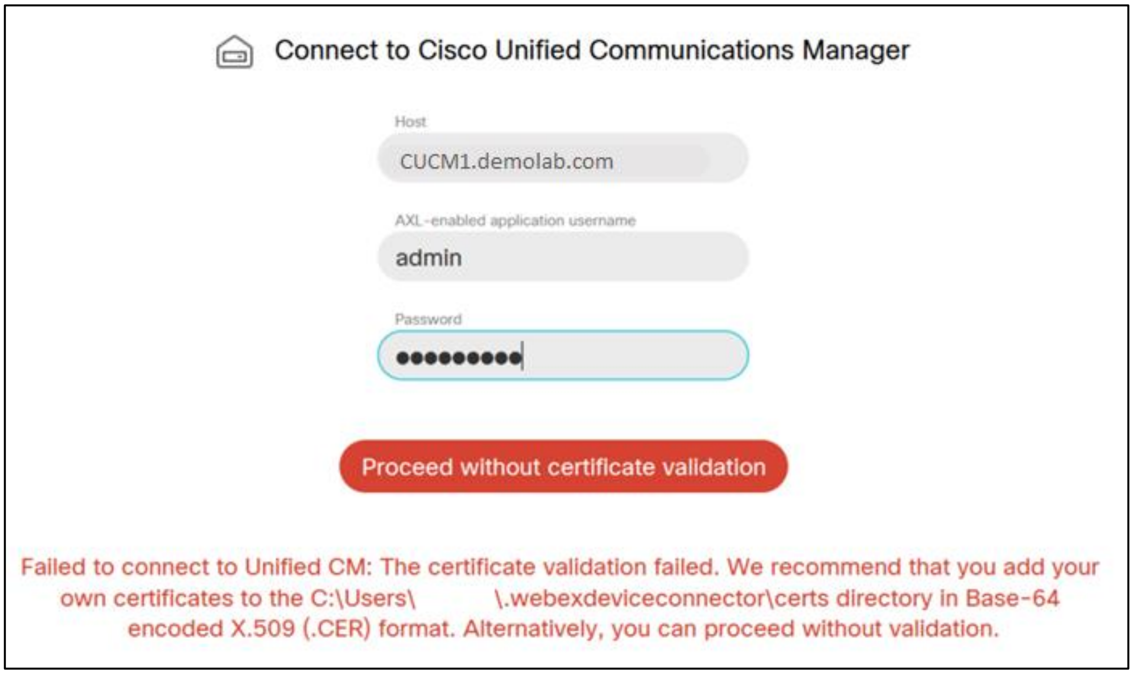
If you are using a Proxy server in your enterprise network, the initial Cisco Webex Device Connector login page allows you to enter the Proxy server address and port number, and if required user credentials for Proxy Authentication (Basic and Digest authentication are supported).

TLS intercepting proxies is supported between the Webex Device Connector tool and the Cloud. Webex Device Connector trusts certificates in the `.webexdeviceconnector/certs` folder for both calls made to the Webex Cloud and to a Unified CM environment.

To connect to a Unified CM cluster, you will need to activate the Cisco AXL Web Service (disabled by default) and create, if one does not already exist, a user account in your cluster with the Standard AXL API Access entitlement.

The user account details will be entered into the Webex Device Connector tool (as shown in figure 3 below) together with either the Fully Qualified Domain Name (FQDN) or IP Address of Unified CM.

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



Connect to Cisco Unified Communications Manager

Host: CUCM1.demolab.com

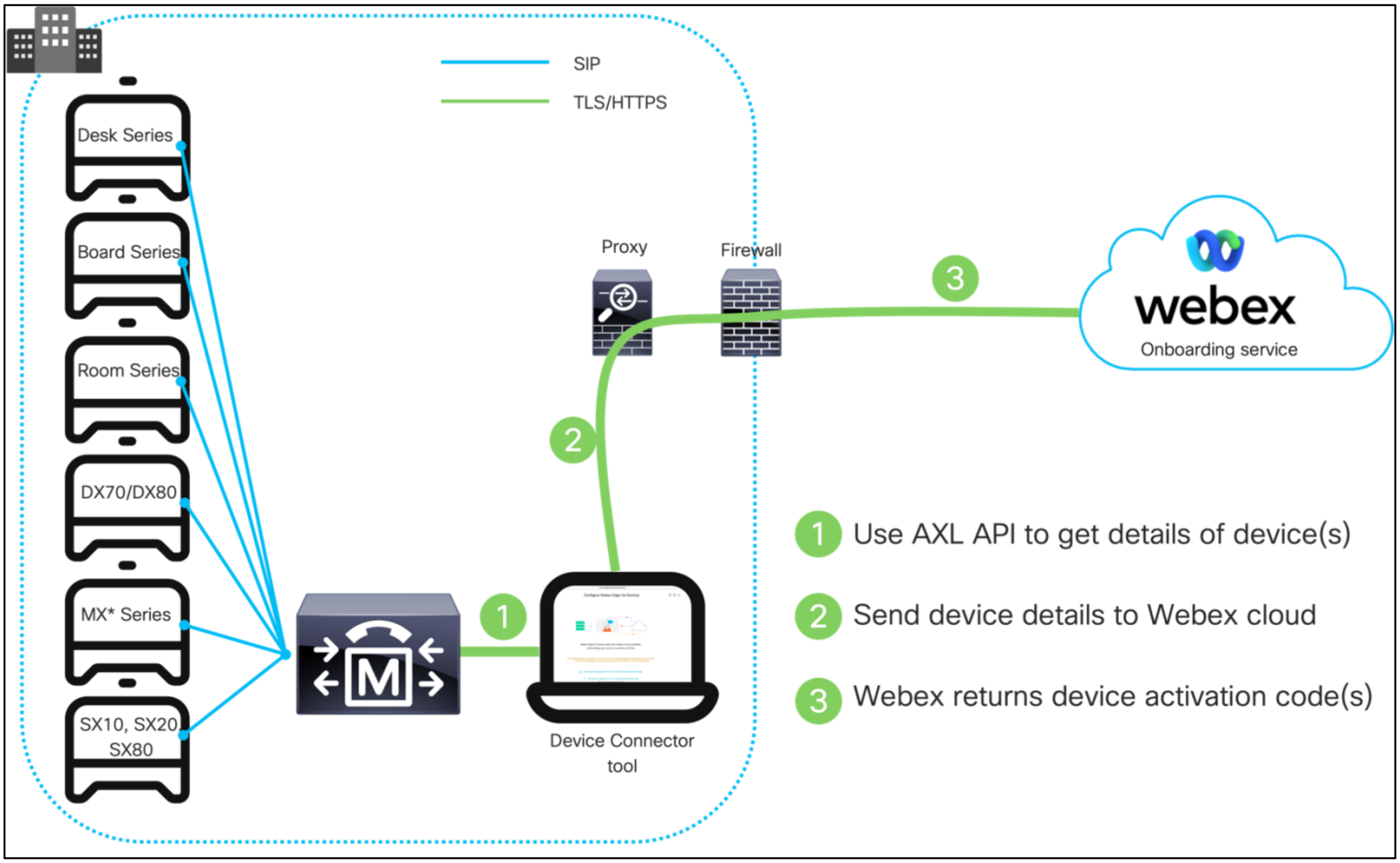
AXL-enabled application username: admin

Password: ●●●●●●●●●

Failed to connect to Unified CM: The certificate validation failed. We recommend that you add your own certificates to the C:\Users\ \.webexdeviceconnector\certs directory in Base-64 encoded X.509 (.CER) format. Alternatively, you can proceed without validation.

As shown in Figure 4, when the Webex Device Connector has retrieved the names and MAC addresses of video devices configured in Unified CM, it establishes a TLS connection to the 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 to the Webex Device Connector tool, which in turn forwards these on to the Unified CM environment.

Figure 4 – Webex Device Connector operation



1 Use AXL API to get details of device(s)

2 Send device details to Webex cloud

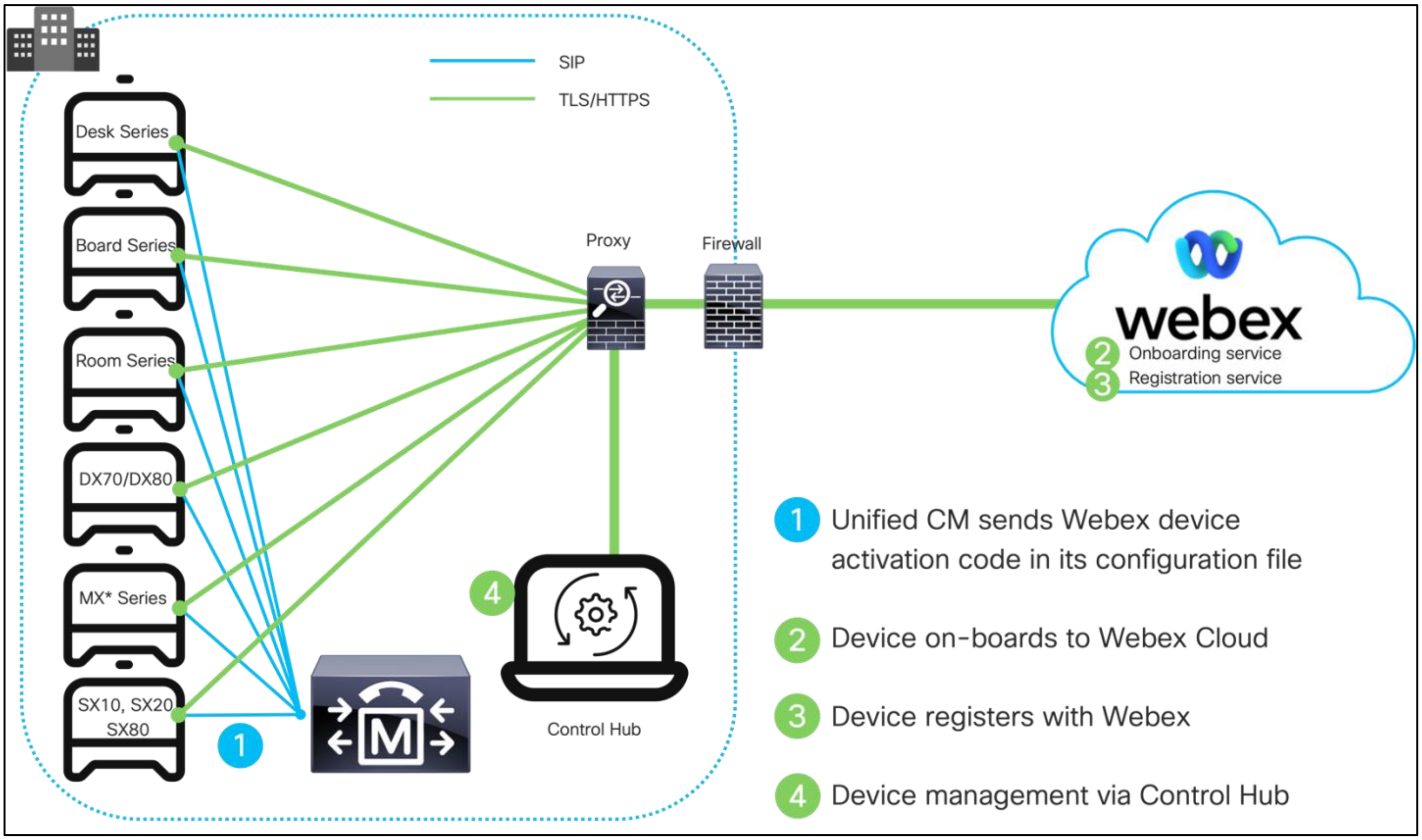
3 Webex returns device activation code(s)

*MX200G2, MX300G2, MX700, MX800

As shown in Figure 5, Unified CM sends the activation code in a configuration file to each video device. Webex video devices running software version CE9.14.5 or above, can establish a TLS connection to the Webex Cloud and use the activation code received from Unified CM to automatically onboard and link to your Webex organization.

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

Figure 5 – On-Premises devices – Cloud onboarding and linking


SIP
TLS/HTTPS
Desk Series
Board Series
Room Series
DX70/DX80
MX* Series
SX10, SX20
SX80
Proxy
Firewall
webex
2 Onboarding service
3 Registration service
Control Hub
1
4
1 Unified CM sends Webex device activation code in its configuration file
2 Device on-boards to Webex Cloud
3 Device registers with Webex
4 Device management via Control Hub

*MX200G2, MX300G2, MX700, MX800

Please note: It is also possible to create a Workspace and a Device activation code for use with Webex Edge for Devices through Webex API's. The process is not as automated as the Webex Device Connector tool as it requires

1. A Workspace to be created
2. A Device Activation code to be created based upon the Workspace ID created in Step 1 above
3. The Device Activation code to be entered into the device using xAPI's.

For further details on

- Workspace creation, go here
- Device Activation code creation, go here
- xAPI commands, go here

3. 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 signaling, these connections are outbound only. Some of the connections are upgraded from HTTPS to bi-directional Secure WebSocket (WSS) connections.

The signaling connections from on-premises devices to Webex services are protected by TLS using strong encryption suites. Webex services prefer TLS cipher suites using ECDHE for key negotiation, 256-bit symmetric encryption cipher keys and SHA-2 hash functions, for example:

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

TLS version 1.2 and above is supported by Webex services.

All Webex features other than real-time media are invoked over a signaling channel that uses TLS.

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 Allow lists and Block lists, 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 and is now supported with Webex Edge for Devices.

When the on-premises device is linked with Webex Edge for Devices:

- 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.

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

Note: The passwords used in the Proxy configuration are hashed and stored locally on the on-premises registered device. The passwords used are not synchronized 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
*.wbx2.com	Webex services
*.ciscospark.com	Webex services
*.webex.com *.cisco.com	Authentication and identity services Webex meeting services Device onboarding
*.webexcontent.com	General file storage including: • Device log files • Software updates
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 from Control Hub. Assistant can also be disabled in a per-device basis
*.quovadisglobal.com *.digicert.com *.godaddy.com *.identrust.com *.lencr.org	Used to request Certificate Revocation Lists from these Certificate Authorities Note - Webex supports both CRL and OCSP stapling to determine the revocation status of certificates. With OCSP stapling, Webex apps and devices do not need to contact these Certificate Authorities
*.intel.com	Used to request Certificate Revocation Lists and check the certificate status with Intel's OCSP service, for certificates sent with background images used by Webex apps and devices

Please **always** check the Network Requirements for Webex Services help article for the latest information

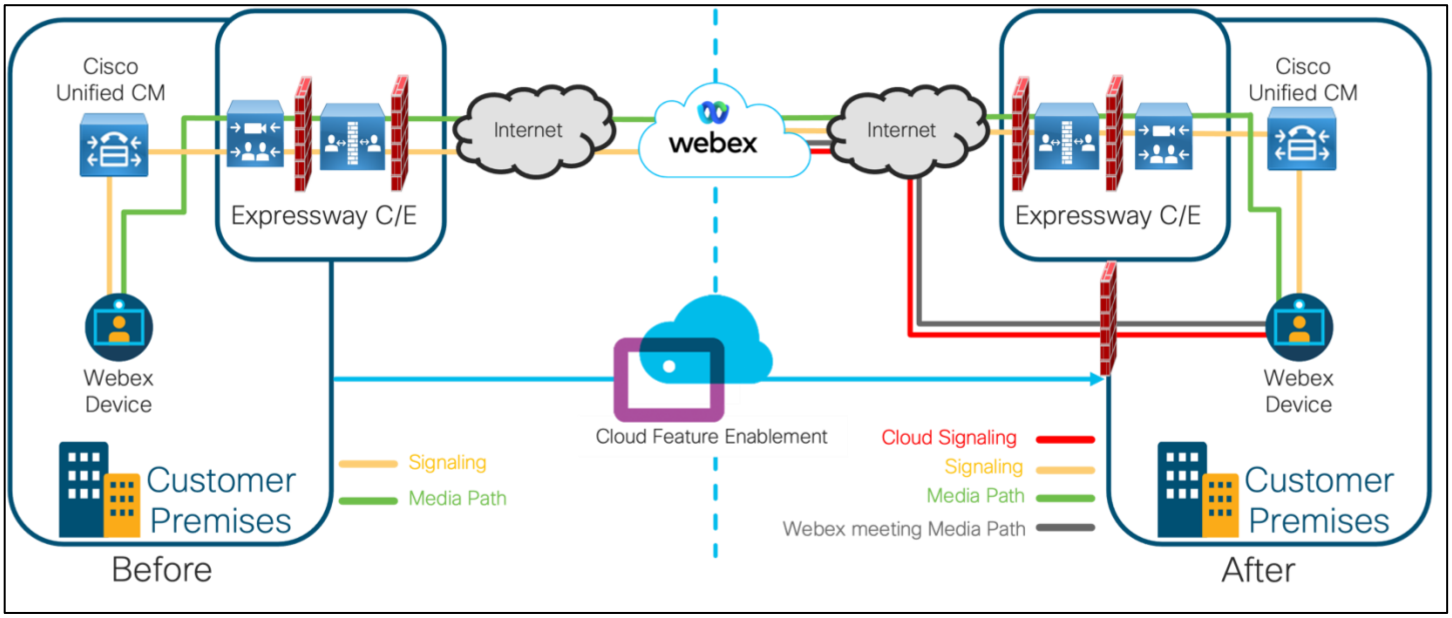
Enabling the standard Webex Edge for Devices service does not change the media paths that your on-premises video devices use today and no additional IP subnets for voice, video and content sharing need to be allowed in your enterprise firewall configuration.

However, enabling the Webex Optimized Meeting experience (this is an opt-in capability when Webex Edge for Devices is deployed) **will** change the media flow for voice, video, and content when the configured device is calling into a Webex meeting. The ability to support SRTP over UDP (port 5004) or the other backup protocols/ports that can be used, together with support for the IP subnets for Webex media services needs to be considered and accounted for within the firewall ruleset. Please see Network Requirements for Webex Services for the most up-to-date network requirements.

More details on how to enable the Webex Optimized Meeting experience can be found here.

Please note then when enabled, the media flow when a Webex Edge for Devices linked device with the Webex Optimized Meeting experience enabled is calling into a Webex Meeting will be direct between the Webex device and the Webex Cloud. The media will not traverse through Expressways/VCS. This can be seen in the diagram below.

Figure 6 – Webex Edge for Devices **with** Webex Optimized Meeting experience enabled



RoomOS 10 based devices that have the Webex Optimized Meeting experience enabled will always prefer the AES-256-GCM media encryption cipher when joining any Webex meeting.

For SIP based calls, RoomOS devices support the following media encryption ciphers:

- AES-256-GCM
- AES-128-GCM
- AES-CM-128-HMAC-SHA1

DX, MX or SX based devices that are configured with the Webex Optimized Meeting experience will join into a Webex meeting with AES-128-GCM.

4. Webex Edge for Devices – Data Privacy

The Webex Device Connector and on-premises devices that are Webex Edge for Devices linked encrypt all data in transit using TLS connections to the Webex cloud.

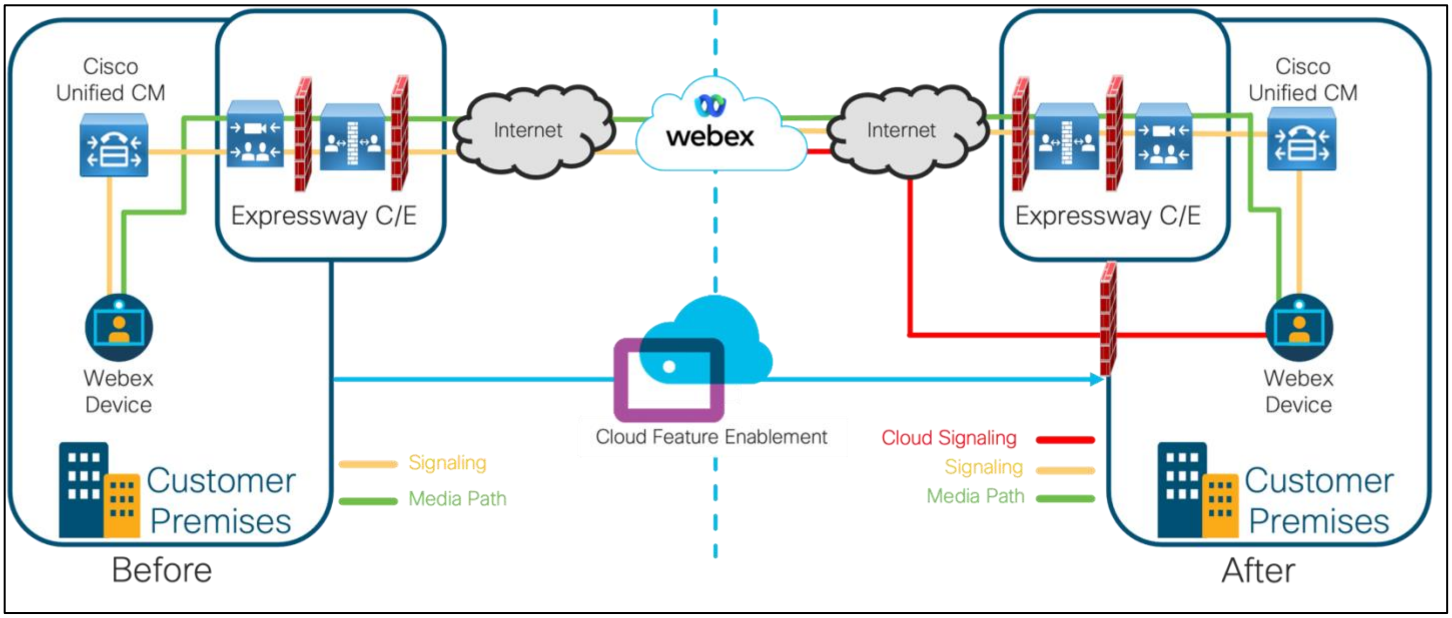
Webex Device Connector signaling to and from the Webex Cloud is primarily used to send the cloud details of on-premises devices and to receive their activation codes for on-boarding. The Device Connector sends the following information about your on-premises devices to the Webex Cloud:

- Device name
- Device MAC address

Webex Edge for Devices linked devices without Webex Optimized Meeting experience enabled

Once your on-premises device has linked with the Webex Cloud, the device will send a subset of the signaling 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 signaling traffic to the Webex Cloud does not and will not traverse the Expressways.

Figure 7 – Webex Edge for Devices **without** Webex Optimized Meeting experience



The following information is sent in the signaling 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 Control Hub for monitoring and management features although Cisco may add additional functionality in later phases.

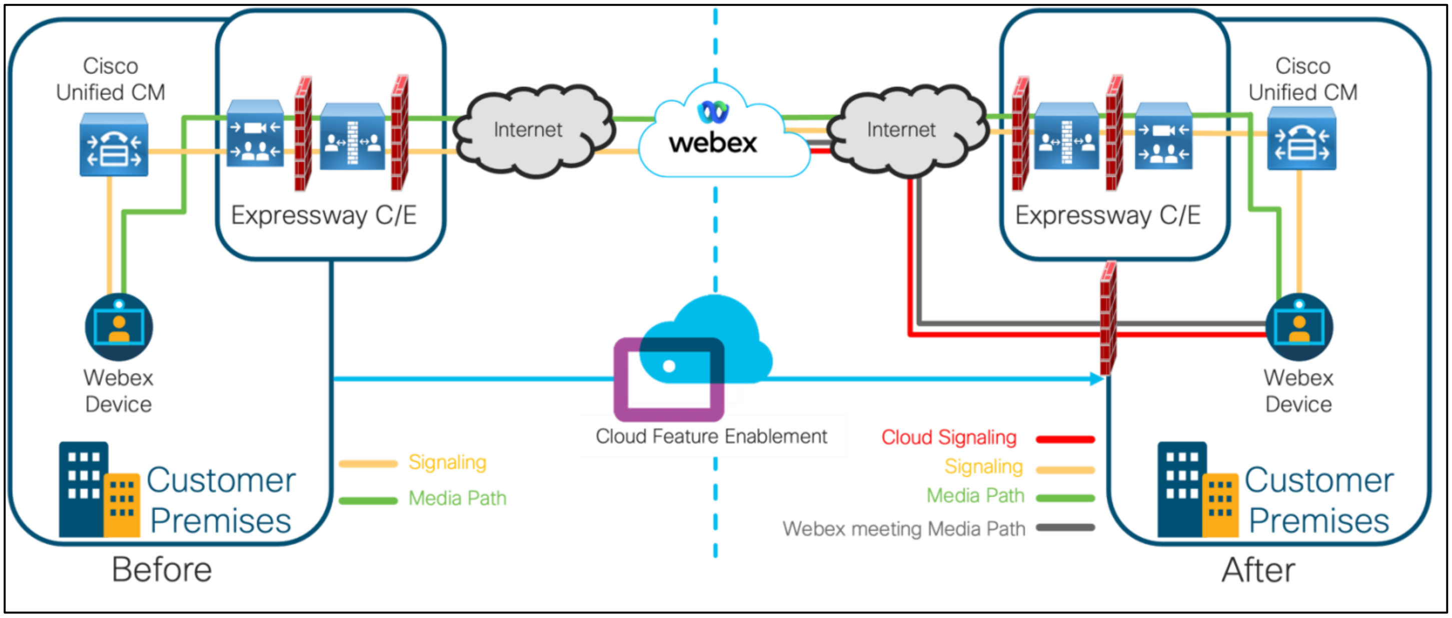
Webex Edge for Devices linked devices with Webex Optimized Meeting experience enabled

Once your on-premises device has linked with the Webex cloud, the Webex Optimized Meeting experience can be enabled. This involves the following being set

- Control Hub manages the linked device
- Cloud Upgrade Mode is enabled (default is Off)
- Webex Join Protocol is set to Webex (default is SIP)
- Cloud Proximity is enabled

Once enabled, if calling into a Webex based meeting, the device will join as if it is a fully cloud registered device. This means that signaling **and** media will be sent direct from the device to the Webex Cloud as seen below. The signaling and media traffic does not and will not traverse the Expressways when the device is calling into a Webex meeting.

Figure 8 – Webex Edge for Devices **with** Webex Optimized Meeting experience enabled



The information sent over the signaling channel will be same as already mentioned in the section covering Webex Edge for Devices linked devices without Webex Optimized Meeting experience enabled. Additional API calls will be made during the setup of a call into the Webex cloud.

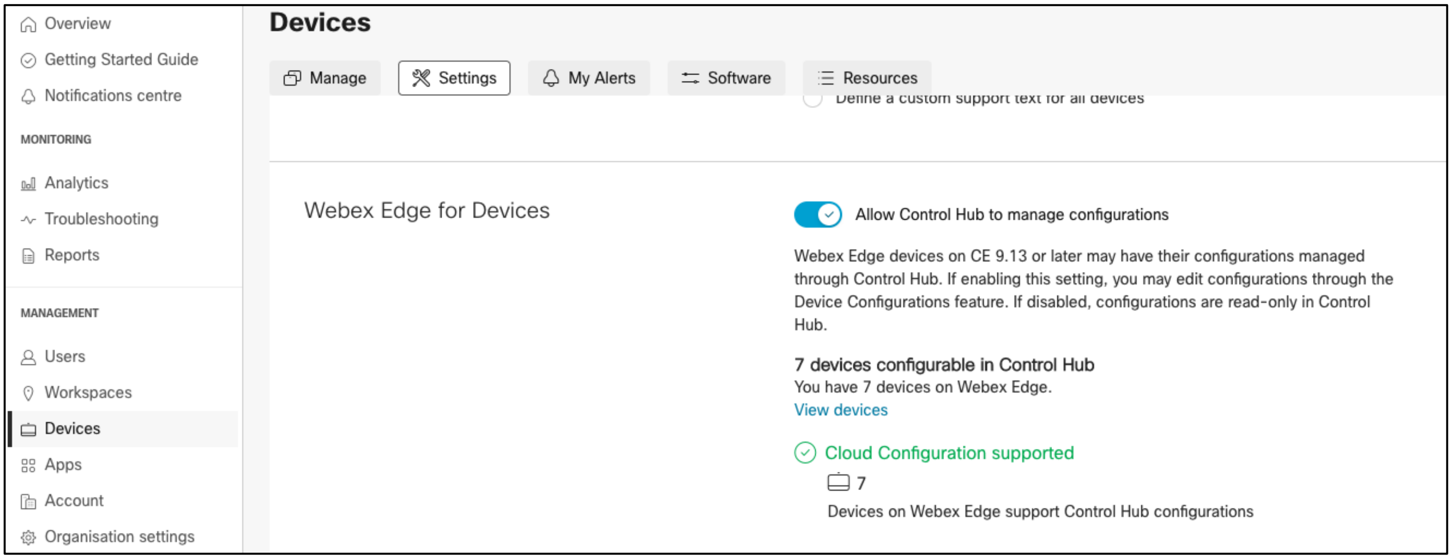
The signaling is outbound over HTTPS into the Webex Cloud.

For details on how personal information is managed and stored in the Webex Cloud, see Webex App & Webex Messaging privacy datasheet and Webex Meetings Privacy Data Sheet.

5. Webex Edge for Devices – Support for Control Hub configuration management

Control Hub has the option to manage the device that has been linked though Webex Edge for Devices. This can be found in Control Hub under **Devices > Settings** (as shown in Figure 9 below).

Figure 9 – Control Hub opt-in for device configuration



Webex Edge for Devices

Allow Control Hub to manage configurations

Webex Edge devices on CE 9.13 or later may have their configurations managed through Control Hub. If enabling this setting, you may edit configurations through the Device Configurations feature. If disabled, configurations are read-only in Control Hub.

7 devices configurable in Control Hub
You have 7 devices on Webex Edge.
View devices

Cloud Configuration supported
7
Devices on Webex Edge support Control Hub configurations

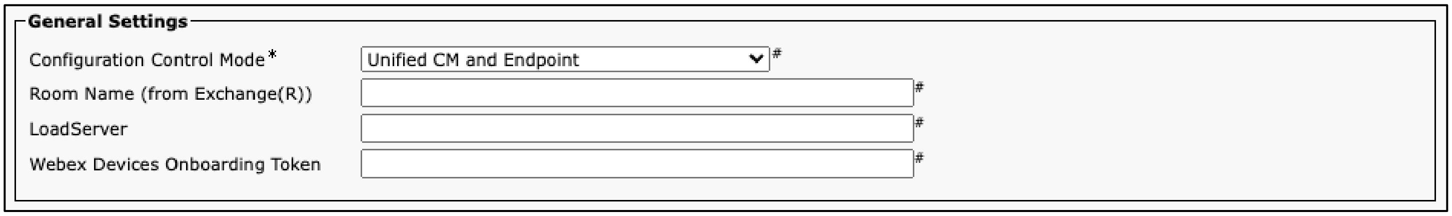
By default, the option for Control Hub to manage the device configuration is turned off.

In this default state, Control Hub will be able to read the configuration of the device, however it will not be able to make any changes.

Important: this setting is only relevant to Webex Edge for Devices. Devices that are registered directly to Control Hub will always be managed through Control Hub.

Please note that if the on-premises registered device is registered through Unified CM, the Configuration Control Mode in Unified CM must be set to `Unified CM and Endpoint` for Control Hub to be able to manage the on-premises device configuration as shown in Figure 10 below.

Figure 10 – Configuration Control Mode – Unified CM (image from Unified CM 14.0)



General Settings

Configuration Control Mode*	Unified CM and Endpoint #
Room Name (from Exchange(R))	#
LoadServer	#
Webex Devices Onboarding Token	#

If the Configuration Control Mode is set to `Unified CM only`, Control Hub will display an error message stating that it is unable to manage the device. If the Configuration Control Mode is set to `Endpoint only`, Control Hub will show the configurations however these will be in a 'Read Only' status

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(s) will continue to accept these settings from Unified CM. Please see the 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 on how personal information is managed and stored in the Webex Cloud, see Webex App & Webex Messaging privacy datasheet and Webex Meetings Privacy Data Sheet.
The following information is sent in the signaling channels from on-premises devices linked to the Webex cloud:
- Device configuration

Please note that this is a bi-directional sync. If Control Hub is not opted in or Configuration Control Mode is set to Unified CM only, device configuration will be read-only.

As from CE9.14.5, it is also possible to configure a device that is Webex Edge for Devices linked to Control Hub to allow for it to upload logs. This is particularly useful when it comes to troubleshooting and Cisco TAC support.

By default, the option to send logs is disabled. It needs to be enabled by an administrator through Control Hub and is enabled on a 'per device' basis. To enable, from the Devices section in Control Hub, locate the required device, open 'All configurations' in the Configurations section and go to **Logging>CloudUpload>Mode** and change setting in the dropdown from **'Following default (Off)'** to **'On'**. If multiple devices require configuration, it is possible to select multiple devices from the Devices tab and bulk edit the devices to enable the capability

Once enabled, there will be a 'Send logs' button available on the device from under **Settings > Issues and Diagnostics.** The logs when submitted from the device will be filtered for Personally Identifiable Information to protect the privacy of the users. If Extended Logging is enabled on the device, the user will be warned that Extended logging has been enabled and that Personally Identifiable Information can be logged to disk.

6. Secure Audit Logging

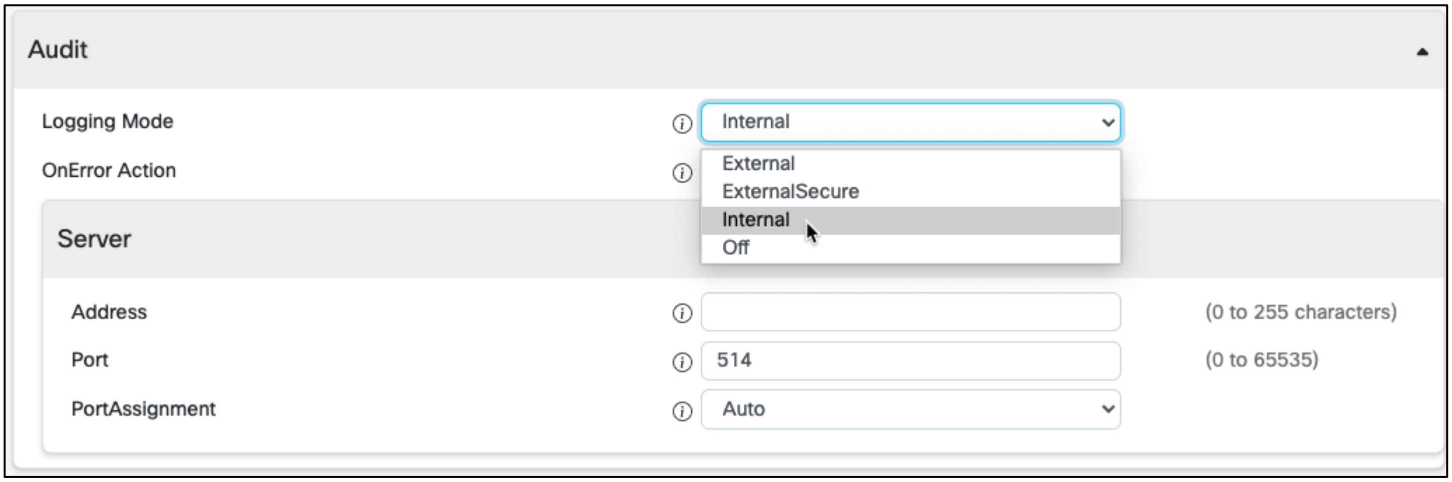
When audit logging mode is enabled, all sign-in activity and configuration changes made on the device are recorded.

As standard, the audit log is local to the device. It is important to understand that logs do rotate and may not persist after a reboot.

Please note that audit logs do not persist after a factory reset.

For a full 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).

Figure 11 – Device Security Audit configuration



Audit

Logging Mode: Internal

OnError Action

Server

Address: (0 to 255 characters)

Port: 514 (0 to 65535)

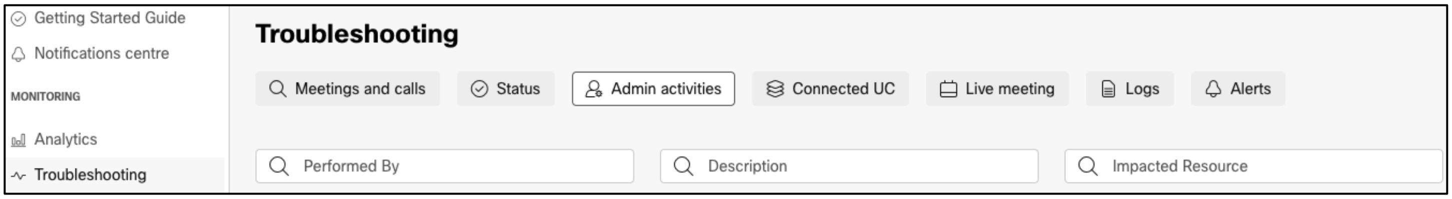
PortAssignment: Auto

With `ExternalSecure` audit logging mode enabled, the device sends encrypted audit logs to an external syslog server that is verified by a certificate in the Audit CA list. The Audit CA list file must be uploaded to the device using the web interface. The `common_name` parameter of a certificate in the CA list must match the IP address or DNS name of the syslog server, and the secure TCP server must be set up to listen for secure (TLS) TCP Syslog messages. If the audit server authentication fails, no audit logs are sent to the external server.

With audit logging enabled, changes made by local admin(s) through the web interface or SSH access together with changes made from Unified CM or TMS will be logged to the syslog server.

With an on-premises registered device that has also been linked to Control Hub, either through the Webex Device Connector Tool or through the Workspaces Webex API, assuming that the device is running the minimum supported version of CE software (currently CE9.14.5 at the time of the writing of this Technical Paper – please check the help article for up to date minimum release) and that Control Hub has been opted in to allow for Device Configuration, changes made from Control Hub will be logged in the Admin activities section under Troubleshooting.

Figure 12 – Admin Activities in Webex Control Hub



These changes will also be logged within the audit trail being sent to the syslog server.