Cloud Collaboration Security White Paper Series

Cloud Aware On-Premises Video Devices

Webex Edge for Devices

Version 1.0 (January 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 through Webex Control Hub. With Webex Edge for Devices, features that are typically served to cloud devices are 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 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.

Initially, Webex Edge for on-premises devices will offer 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
- Hybrid Calendar through Webex Control Hub (optional feature)
- Webex Assistant (optional feature)

In later development phases, the following additional features are planned:

- Realtime Troubleshooting of Webex Meetings
- Name Labels in Call
- People Insights
- Cloud Management—Configurations
- Licensing Enablement Enhancements
- Additional Realtime Monitoring Datapoints
- On-Premises Software Management
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.

Figure 2. Download Cisco Webex Device Connector: Control Hub >Devices >Resources

To use the Cisco Webex Device Connector application, you are required to authenticate with your Webex organization. Support for single sign on (SSO) with on-premises identity providers (IdPs) is limited today. If you encounter issues, please open a case with Cisco TAC.
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 that are configured in Unified CM. (VCS Expressway deployments use a CSV file to import device details).

Figure 3. 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 are 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, Digest, and NTLM based authentication are supported).
To connect to a Unified CM cluster, you must 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 4. Connecting from Cisco Webex Device Connector to Unified CM (showing the certificate validation failure message)

As shown in Figure 5, when the Cisco Webex Device Connector retrieves the names and MAC addresses of video devices configured in Unified CM, the connector establishes a TLS connection to the Webex cloud and sends these details to the Webex identity service along with the details of your Webex organization. The Webex identity service creates an activation code for each device and returns these to the Cisco Webex Device Connector, which in turn forwards these on to the Unified CM cluster.

Figure 5. Cisco Webex Device Connector operation
As shown in Figure 6, Unified CM sends the activation code in a configuration file to each video device. Cisco Webex video devices that are running software version CE9.10 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.

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

*Figure 6. On-Premises devices—Cloud On-boarding and Linking*
Webex Edge for Devices – Enterprise Network Security Considerations

On-premises devices using the Webex Edge feature 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.

Note: Webex Edge for Devices provides limited support for proxy services today, primarily because HTTP traffic is directed from the device to both the Webex cloud and the Unified CM cluster. If your proxy server can forward HTTP traffic to your Unified CM cluster and the Webex cloud, the following proxy features are supported.

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

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.

Note: Enabling Webex Edge for Devices does not change the media paths that your on-premise video devices use today and no additional IP subnets for voice, video and content sharing need to be whitelisted in your enterprise firewall.
<table>
<thead>
<tr>
<th>URL</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.wbx2.com</td>
<td>Webex Teams micro-services. For example:</td>
</tr>
<tr>
<td></td>
<td>File management service</td>
</tr>
<tr>
<td></td>
<td>Key management service</td>
</tr>
<tr>
<td></td>
<td>Software upgrade service</td>
</tr>
<tr>
<td></td>
<td>Whiteboarding service</td>
</tr>
<tr>
<td></td>
<td>Proximity service</td>
</tr>
<tr>
<td></td>
<td>Registration service</td>
</tr>
<tr>
<td>*.webex.com</td>
<td>Identity provisioning</td>
</tr>
<tr>
<td></td>
<td>Identity storage</td>
</tr>
<tr>
<td></td>
<td>Authentication</td>
</tr>
<tr>
<td></td>
<td>Device onboarding</td>
</tr>
<tr>
<td></td>
<td>OAuth services</td>
</tr>
<tr>
<td>*.ciscospark.com</td>
<td>Other Webex Teams services including:</td>
</tr>
<tr>
<td></td>
<td>Device onboarding service</td>
</tr>
<tr>
<td>*.webexcontent.com</td>
<td>General File storage including:</td>
</tr>
<tr>
<td></td>
<td>Device log files</td>
</tr>
<tr>
<td></td>
<td>Software updates</td>
</tr>
<tr>
<td>*.activation.webex.com</td>
<td>Used for onboarding devices to the Webex service</td>
</tr>
</tbody>
</table>

| speech.googleapis.com | Google Speech Services. Used by Webex Assistant to handle speech recognition and text-to-speech. Disabled by default, is opt-in through Control Hub. Assistant can also be disabled on a per-device basis. |
| texttospeech.googleapis.com | Details of Webex Teams devices that support Webex Assistant are documented here: [https://help.webex.com/article/hzd1aj](https://help.webex.com/article/hzd1aj) |
| speech-services-manager-a.wbx2.com | |
| *.crashlytics.com | Diagnostic & troubleshooting data |

**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 cloud:

- Device name
- Device MAC address

Once your on-premises device is linked with the Webex cloud, the device sends 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. In phase one of Webex Edge for Devices, the signalling sent from the on-premises device to the Webex cloud is primarily used for management and monitoring purposes, although Cisco may add additional functionality in later phases.

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.

For details of how your personal information is managed and stored in the Webex cloud, see the Webex Teams Privacy data sheet:

Other useful technical reference documents:

Cisco Webex Teams Security and Privacy whitepaper

Cisco Webex Edge for Devices Deployment Guide
https://help.webex.com/cy2l2z/