Cisco Collaboration Video Device Security

Cloud Collaboration Security Technical Paper

May 2023

webex by CISCO

Contents

Webex by Cisco is a cloud collaboration platform that provides messaging, calling, and meeting features. This technical paper provides an overview of the security features of Cisco Collaboration video devices when registered to the Webex cloud.

.

1. Introduction

Cisco Collaboration video devices are rich collaboration devices that allow real time video conferencing, content sharing, whiteboarding and much more; all with the opportunity to include remote team members.

Cisco Collaboration video devices are available in several forms:

- Cisco Desk Series
- Cisco Board Series
- Cisco Room Series

This document focuses on the implementation of security in Webex registered Cisco video devices.

Note: This paper covers Webex registered Cisco Desk, Cisco Board, and Cisco Room Series devices, running RoomOS. These devices will be collectively referred to as 'Cisco Collaboration video device(s)' or 'Cisco video device(s)' throughout this document.

2. RoomOS Software

RoomOS devices arrive with software from the factory and usually this software is current enough to allow onboarding to Webex. If older software is installed, it will automatically be updated when the device attempts to register to Webex. As an alternative, prior to onboarding, the latest software images can be downloaded from Cisco.com and uploaded through the device's web interface on a private network.

As shown in Figure 1, if new software is loaded onto the device, the device first performs an integrity check of the file to be installed and verifies the file's signature before installing it. It is not possible to install software on to the device if the software is not signed by Cisco. Devices also reverify the software's signature during boot.

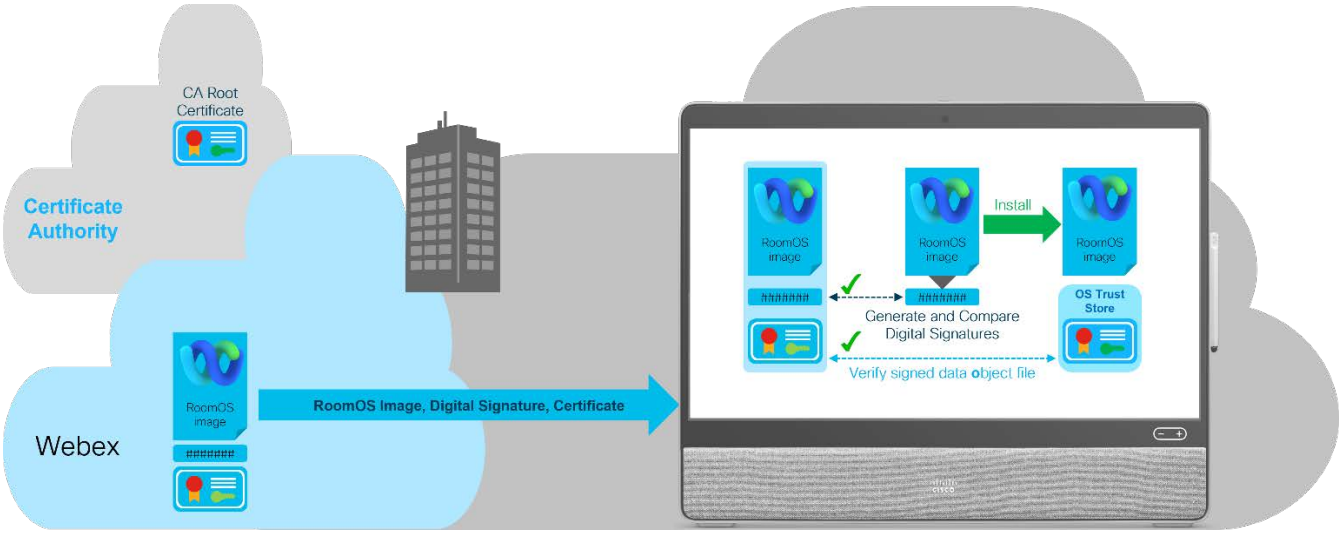

Figure 1. RoomOS Software Validation: Digital Signature Verification

By default, there are no user-accessible accounts on the device, only service accounts under which the device's software runs. In particular, there is no root user account on the device.

3. Secure Data Storage

Any Cisco Collaboration video device configuration data, such as settings and images, are encrypted and stored in non-volatile memory. The encryption key for this data is stored in the device's EEPROM and is deleted on factory reset of the device, making any stored data inaccessible. Real-time data such as audio and video information for an active video call is stored only in volatile memory. The encryption keys for this type of data are also stored only in volatile memory, and they are deleted at the end of a call. When the device is restarted, data in volatile memory is removed. Access to the information on a device is limited to the methods outlined in the Cisco Collaboration Devices Configuration section, otherwise access is not possible without special software and/or special hardware, which cannot be obtained commercially.

Where a video device can access files or whiteboards, these are stored in the Webex cloud. This storage period for user-generated content follows the retention period specified in Control Hub for your organization. Any whiteboards created on shared-mode devices are automatically deleted from the device every night. Note that if a whiteboard has been created and then added to a space, it is no longer affected by this nightly data deletion as it is no longer owned by the device.

4. Webex End-to-end Encryption of User-generated Content

Cisco video devices can request end-to-end encryption keys to access secure content created by users of Webex messaging and calendaring services. Cisco video devices participate in end-to-end encryption for the following services:

- Calendaring and One Button to Push (OBTP) meeting join functionality
- Whiteboarding
- To retrieve and present files shared in Webex messaging spaces

Like Webex Apps, Cisco video devices can request end-to end-encryption keys from the Webex Key Management Service (KMS) and use these keys to encrypt and decrypt content. End-to end-encryption keys, OAuth access tokens, and content for Webex messaging spaces and calendar events are not persistently stored in RoomOS. OAuth Refresh Tokens are securely stored by RoomOS and are renewed when access tokens are renewed.

For more information on how end-to end-encryption works for Webex messaging and calendaring services see: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf

Cisco video devices can also access message layer security (MLS) end-to-end encryption keys used for ephemeral content in zero trust-based end-to-end encrypted meetings. For more information refer to Zero-Trust Security: End to End Encryption for Webex Meetings.

5. Onboarding Cisco Collaboration Video Devices to Webex

Control Hub provides a simple interface to onboard and activate Cisco video devices. Devices can be onboarded using a 16-digit activation code generated in Control Hub. Alternatively, users can generate the 16-digit activation code for their personal Cisco video devices at https://settings.webex.com or within the Webex App.

Once devices are onboarded, administrators can view details about those devices and can update selected configuration settings via Control Hub.

Figure 2. Cisco Collaboration Video Device Onboarding: Activation Code, Discovery Service

As shown in Figure 2, at the beginning of the onboarding process, Cisco video devices establish a TLS connection with the Webex Global Discovery Service (GDS) (certificate trust anchors for the TLS connection are installed on the device during manufacturing) and sends the service its activation code. The 16-digit activation code allows GDS to identify the organization and machine account for the device. The organizational information in the code is used by the Webex GDS to redirect the device to the Webex identity service.

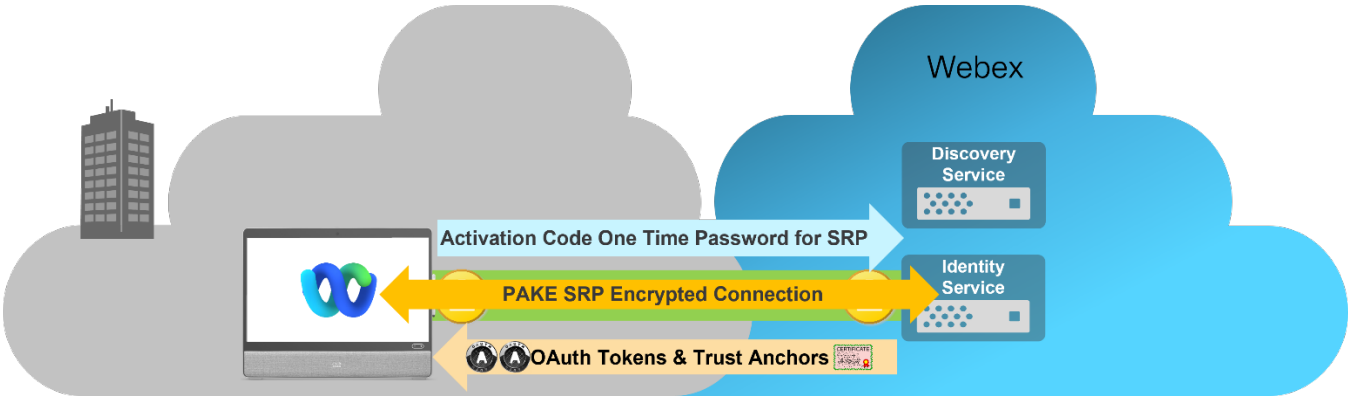

Figure 3. Cisco Collaboration Video Device Onboarding: Secure Remote Password Protocol (SRP) Connection to Identity Service

As shown in Figure 3, the Cisco video device establishes an encrypted TLS connection to the Webex identity service. To provide an extra layer of security against TLS interception attacks, the device uses Secure Remote Password (SRP) protocol to create an additional encrypted connection to the identity service and uses this tunnel to download the OAuth tokens and additional certificate trust anchors that the device needs to register to and use Webex services.

Secure Remote Password protocol is an augmented password-authenticated key agreement (PAKE) protocol (RFC 2945). The Cisco video device's activation code is used to authenticate the device with the identity service and to establish a password-entangled SRP session key between the device and the identity service. A key derivation function (KDF) uses the session key as input to create a symmetric AES encryption key that is used to encrypt data exchanged between the device and identity service.

During this onboarding stage, Enterprise CA Certificate trust anchors can also be downloaded from the identity service into the device to permit TLS inspection of Webex Room Series signaling traffic by an Enterprise Proxy server. (Customers need to open a service request with Cisco TAC to upload their Enterprise CA certificates)

Cisco video devices use the installed certificate trust anchors to validate TLS server certificates from Webex services, and the OAuth Tokens as a proof of authentication and authorized registration to Webex services.

6. Connecting to Webex Services

Cisco Collaboration video devices use TLS to establish encrypted signaling connections to services in the Webex cloud.

During onboarding, connections from Cisco Collaboration video devices are outbound only and use fully qualified domain names to establish sessions to Webex services. Signaling traffic is protected by TLS using strong encryption cipher suites. Webex cloud services support TLS version 1.2 and 1.3 and a limited set of cipher suites.

TLS Cipher Suites used by Webex

The cipher selection for each connection is based on the Webex server's TLS preference.

Figure 4 shows that during TLS session establishment, the device (TLS client) sends a list of its supported cipher suites in order of preference in a Client Hello message to the Webex Service (TLS server). The server selects one cipher suite, based on the subset of cipher suites that both the client and server support and the server's preference and returns this selected cipher suite to the device in a Server Hello message.

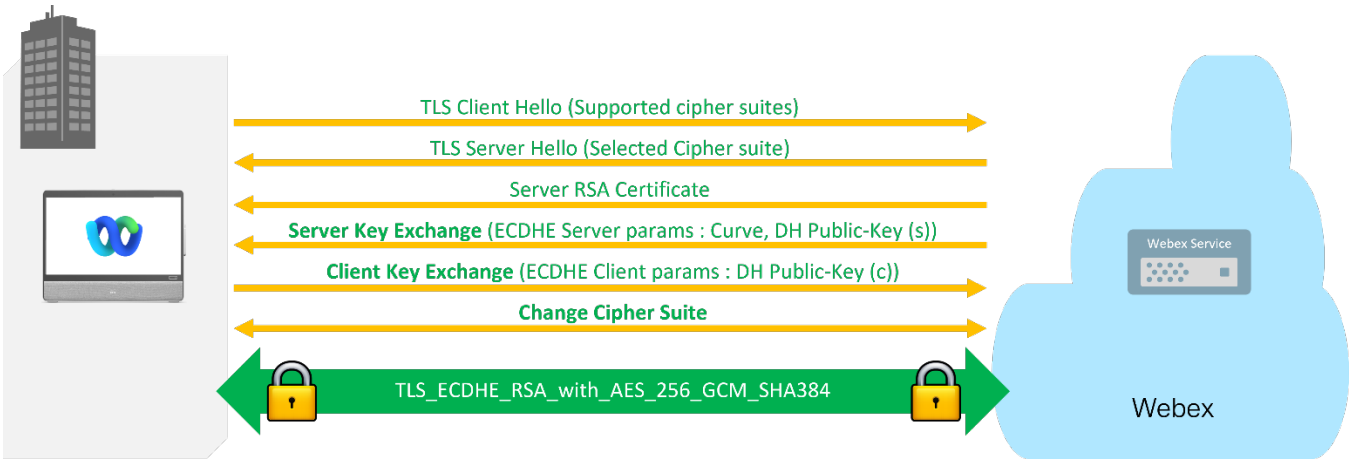

Figure 4. TLS Session Establishment from Cisco Collaboration Video Device to Webex

Webex services prefer the following:

- ECDHE for key negotiation
- RSA-based certificates (2048-bit or higher key size)
- SHA2 authentication (SHA384 or SHA256)
- Strong encryption ciphers using 128 or 256 bits (for example, AES_256_GCM, AES_128_GCM, and CHACHA20_POLY1305)

Example:
TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS 1.3: TLS_AES_256_GCM_SHA384

These cipher suites meet the guidelines defined in the US National Institute of Standards and Technology (NIST) Special Publication 800-52 Revision 2. For more information, see Guidelines for the Selection, Configuration, and Use of Transport 4 Layer Security (TLS) Implementations.

Figure 5 shows the Webex Service selecting TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 for the TLS 1.2 secure connection.

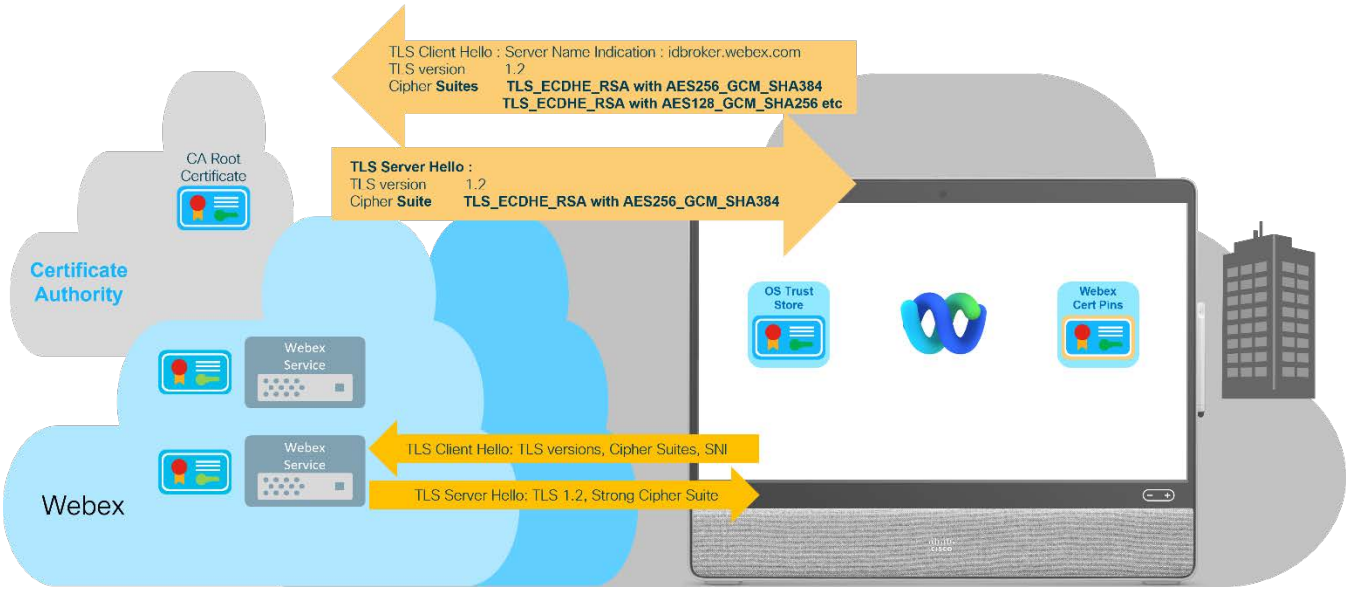

Figure 5. Cisco Collaboration Video Device: Client to Server TLS Cipher Suite Negotiation

Authenticating Webex Services

When a Cisco Collaboration video device establishes a TLS connection to Webex, the Webex server sends its CA signed server certificate, CA Root certificate, and any intermediate certificates to the Cisco video device, as shown in Figure 6. Before proceeding with the TLS handshake, the device validates the chain of certificates to verify the authenticity of the Webex service.

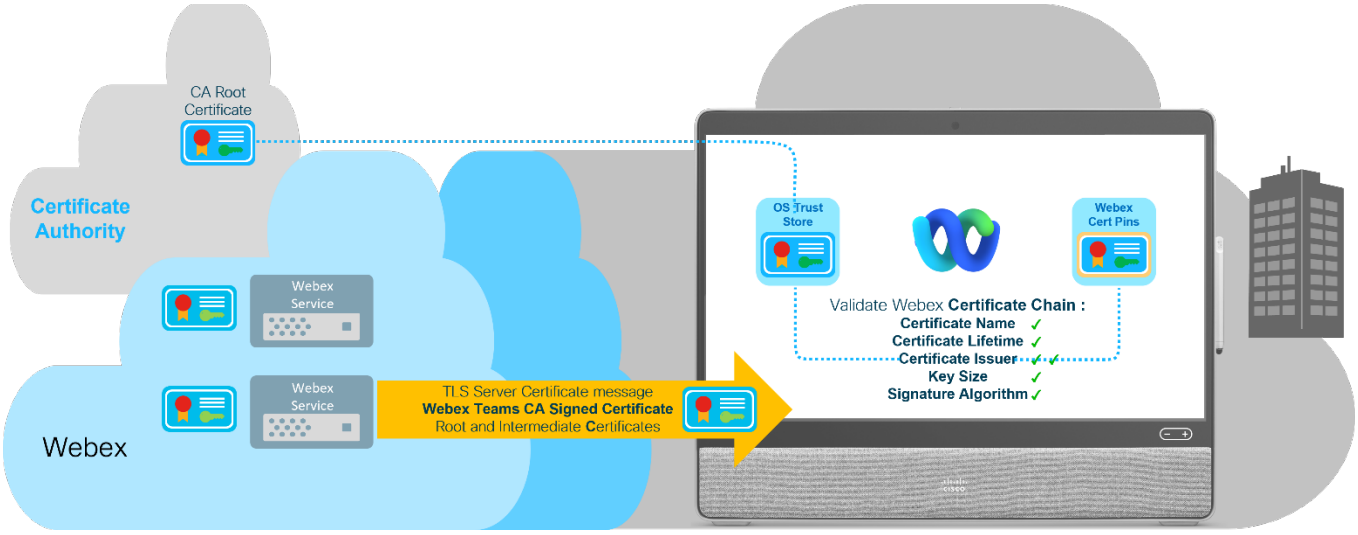

Figure 6. Verifying the Authenticity of a Webex Service

Cisco Collaboration Video Device - Certificate Validation

During the TLS handshake the server sends the device a Certificate message which includes the CA-signed server certificate, intermediate certificate, and root certificate. The Cisco video device performs a series of checks, as depicted in Figure 7, to validate the received certificates and authenticate the Webex service:

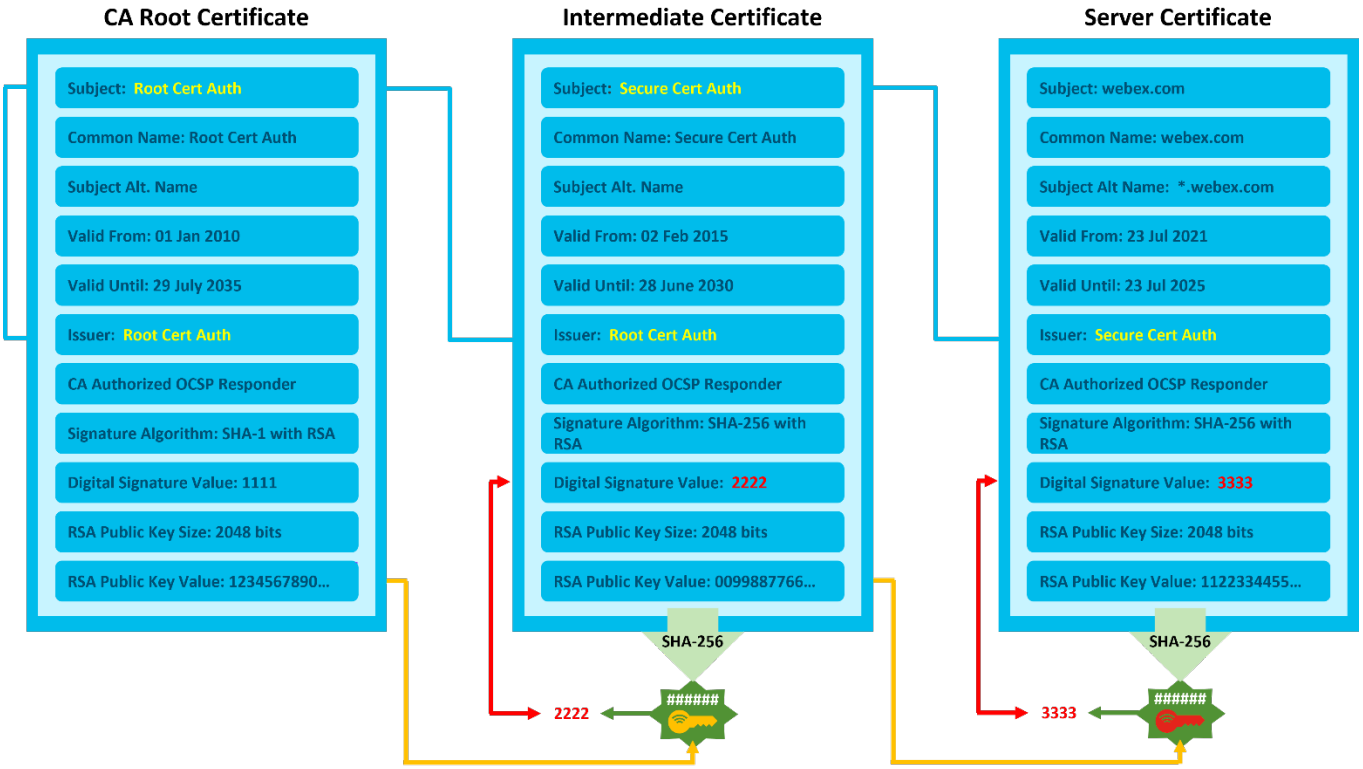

Figure 7. Certificate and Certificate Chain Validation

The primary processes used to validate the integrity of the chain of certificates sent to the device are as follows:

Certificate Chain – Digital Signature Verification

Starting with the CA Root certificate, the public key of the certificate is used to decrypt the digital signature of the first sub-root intermediate certificate and produce its hash value. A hash of the intermediate certificate is then calculated and compared with the decrypted hash value, if they match the integrity of intermediate certificate is validated. The same process is then repeated with any other intermediate certificates until the server certificate is reached. As a final step, the public key of the intermediate certificate that signed the server certificate is used to decrypt the digital signature of the server certificate and produce its hash value. A hash of the server certificate is then calculated and compared with the decrypted hash value. If they match, the integrity of server certificate is validated.

Certificate Issuer Verification

The name of the issuer in the server certificate is compared with the name in the subject field of its signing intermediate certificate for matching values. This process continues up the certificate chain, until the name of the issuer in the intermediate certificate signed by the Root CA certificate is compared with the name in the subject field of the CA Root certificate. Finally, the issuer name and subject name of the self-signed CA Root certificate should match.

Certificate Validity Period

The “Valid from” and “Valid until” values in each certificate are checked to make sure that each certificate has not expired.

Server Hostname Validation

The Cisco video device validates that the name of the service to which it is connecting matches a name in either the server certificate’s Subject field or Subject Alternative Name field.

7. Secure Media for Cisco Collaboration Video Devices

Cisco video devices use real-time media for audio, video, and content sharing streams. Typically, media from any Cisco video device transits from the user's location to media nodes in the Webex cloud, where the streams are switched and distributed. This is true for all call types, for example, calls to one other person, and multiparty calls. Optionally, instead of media nodes in the Webex cloud, on-premises Webex Video Mesh Nodes (VMNs) may also be deployed to switch and distribute media locally.

Secure Real-Time Transport Protocol (SRTP)

Cisco video devices secure media streams using the Secure Real-time Transport Protocol (SRTP), described in RFC 3711. Voice and video codecs, the media encryption cipher suite and encryption keys are securely negotiated over HTTPS, using SDES described in RFC 4568.

Cisco video devices support the following media encryption ciphers, in the following preference order:

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

1:1 calls between cloud registered Cisco video devices and 1:1 calls between Webex Apps and cloud registered Cisco video devices will use AES-256-GCM as their media encryption cipher (see Figure 8). Similarly, calls from cloud registered Cisco video devices into Webex Meetings also use AES-256-GCM as their media encryption cipher (for both standard and End to End Encrypted meetings).

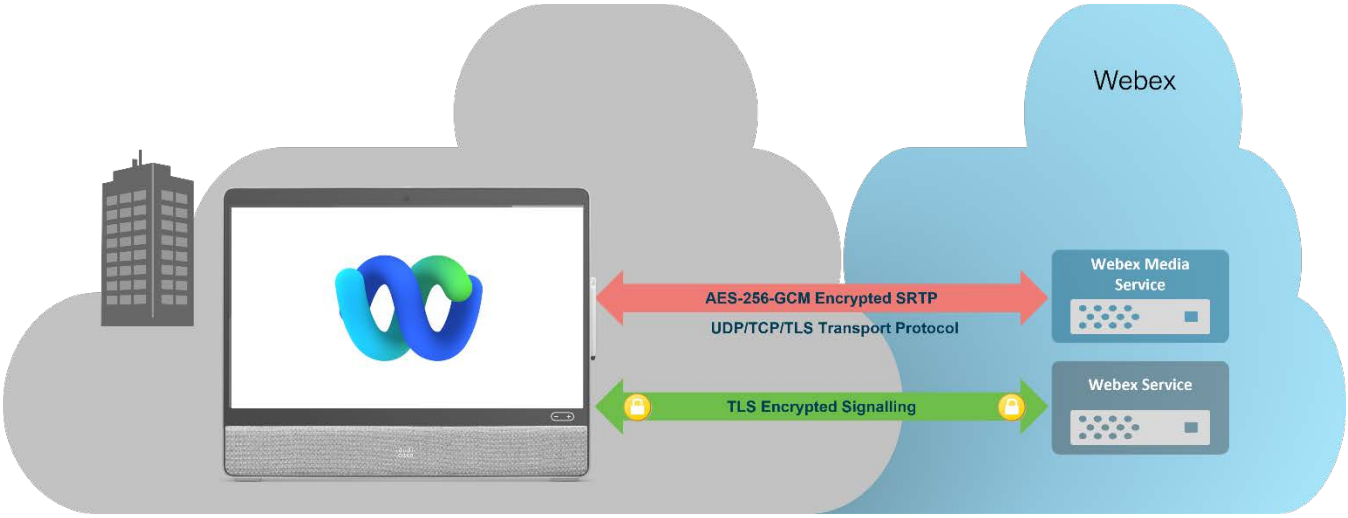

Figure 8. Cisco Collaboration Video Device Encrypted Media and Signaling Connections to Webex

The AES-CM-128-HMAC-SHA1 encryption cipher is supported for interoperability with SIP and 3rd Party devices that either prefer or support only this encryption cipher for media.

Transport Protocols for Encrypted Media

Cisco video devices support UDP, TCP and TLS as transport protocols for media.

In line with RFC 3550 (RTP – A Transport Protocol for Real -Time Applications), Cisco uses UDP as the preferred transport protocol for voice and video media streams. Being a connectionless transport protocol, UDP does not guarantee that all packets will be delivered, or delivered in the order that they were sent, to the upper layer

application (in this case the voice or video codec). However, when UDP is used as the media transport protocol, the codec ignores out-of-order packets that exceed the jitter buffer capacity and conceals those that are either lost enroute, or received too late, to render the real time media stream with as little delay as possible.

Cisco video devices also support TCP as a fallback media transport protocol. However, Cisco does not recommend TCP as a transport protocol for voice and video media streams, as TCP is connection-oriented and designed to reliably deliver correctly ordered data to upper layer applications. Using TCP, the sender retransmits lost packets until they are acknowledged, and the receiver buffers the packet stream until the lost packets are recovered. For media streams, this behavior manifests itself as increased latency or jitter which affects the media quality experienced by the call's participants.

Cisco video devices also support TLS (secured TCP) as a last resort option for media transport. Note that if media is sent over TLS from a Cisco video device it does not traverse a TLS Proxy server, if one is configured on the device.

Cisco video media flows in both directions using a symmetric inside-initiated, 5-tuple (source IP address, destination IP address, source port, destination port, protocol) stream outbound to the Webex cloud.

Cisco video also uses STUN (RFC 5389) for firewall traversal and media node reachability testing.

Media Transport Protocols: Source and Destination Port Numbers

Table 1 shows the source and destination transport protocol port numbers for real time media used by Cisco Collaboration video devices. The IP subnets used by Webex cloud media service can be found in the Network Requirements for Webex Services article.

Table 1. Cisco Collaboration Video Devices: Media Transport Protocols and Ports

TRANSPORT PROTOCOL	SOURCE PORT	DESTINATION PORT
UDP	Voice: 52050-52099 Video: 52200-52299	5004, 9000
TCP	Ephemeral	5004
TLS	Ephemeral	443

DSCP Values for Media Streams

Cisco video devices use the following Differentiated Services Code Point (DSCP) values for media traffic:

- Voice: Expedited Forwarding (EF), DSCP 46
- Video: Assured Forwarding (AF41), DSCP 34

The DSCP values used by Cisco video devices align with those in RFC 4594 (Configuration Guidelines for DiffServ Service Classes).

The DSCP values in the media traffic sent by Cisco video devices can be used to queue and preferentially treat voice and video streams as they traverse the enterprise network. Webex media streams traversing the internet will generally have their DSCP values set to zero by the internet service provider. For media using the UDP

transport protocol, the zeroed DSCP values in returning media streams sent over the internet can be reassigned by an enterprise edge router using the UDP source port ranges to identify the voice and video streams.

Cisco Collaboration Video Devices: Media Node Reachability Testing

Cisco video devices use a media node discovery process at start up, when network connections change, and then periodically, to determine the reachability of media node clusters available to their organization (cloud media nodes and on-premises Video Mesh Nodes). During call establishment, the Cisco video device sends its reachability report to the Webex cloud. Based on the available transport protocol (UDP/TCP/TLS), Round Trip Times (RTT) and resource availability, the Webex cloud determines the media node that will be used by each device. As shown in Figure 9, media cascade connections are established if multiple media servers are used in a call.

Note: For Webex video integration for Microsoft Teams (VIMT) The media path for video integration calls differs from other Webex Meetings call flows because specialized media clusters in Azure data centers handle this call type. The specialized media clusters for VIMT are not part of the reachability tests that Webex registered devices perform. Instead, the integration attempts to use the optimal media cluster for each call based on where the caller originates. For more details, see Deploy the Webex video integration for Microsoft Teams.

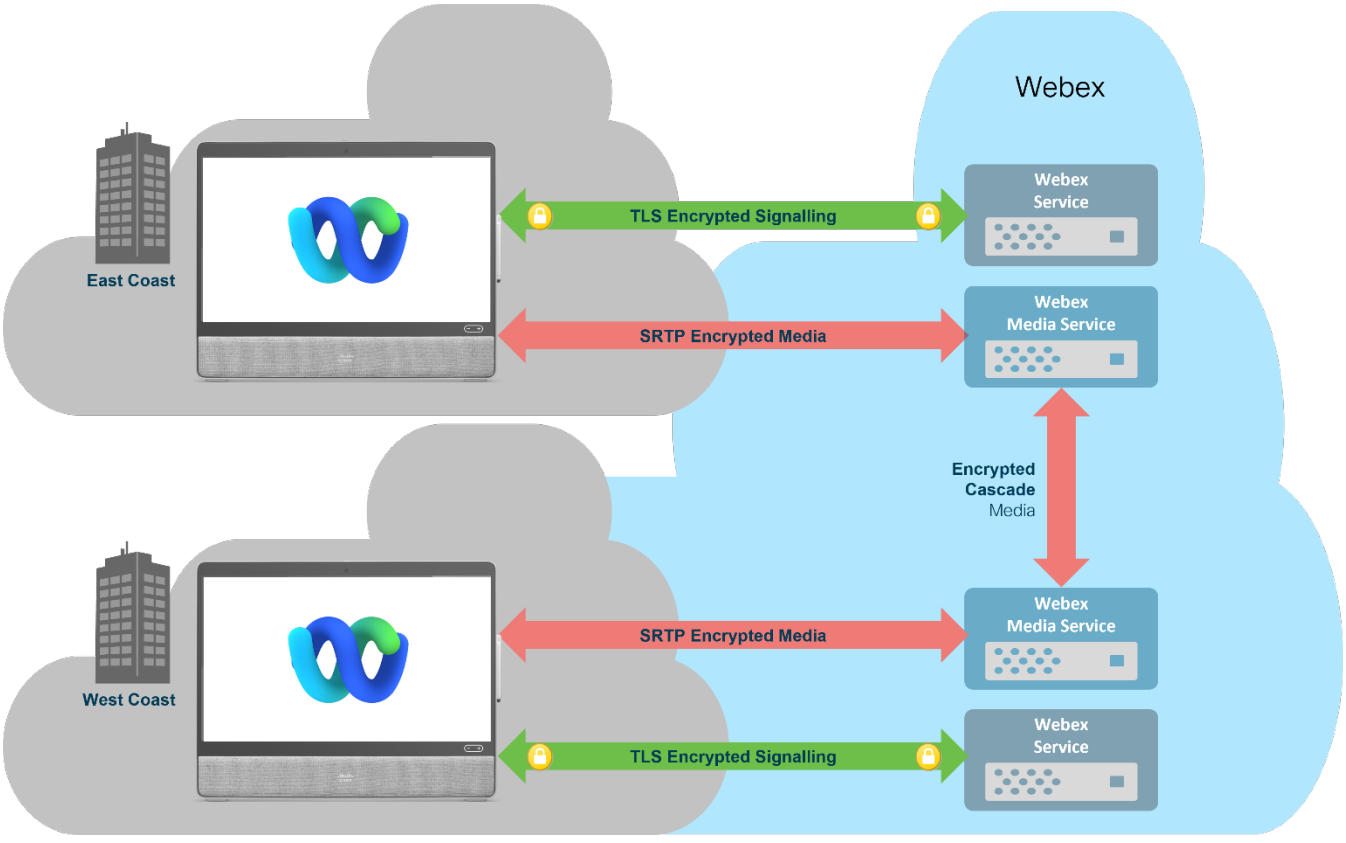

Figure 9. Media and Signaling: Call Between Two Cisco Collaboration Video Devices

Zero-Trust Security: End to End Encryption for Webex Meetings

Zero-Trust Security for Webex Meetings is a new framework for end-to-end encryption that is built on industry-standard cryptographic protocols. Zero-Trust Security allows Cisco video devices and Webex Apps to join Webex Meetings using a new standards-based form of end-to-end encryption (E2EE), where Cisco does not have access to the meeting encryption keys.

Zero-Trust security adds an additional end-to-end layer of protection on top of standard SRTP media encryption and Single Sign-On (SSO) for authentication.

- **Key Exchange:** Devices participating in an E2EE meeting need to set up keys for E2EE without the conferencing provider being able to access those keys. Zero-Trust Security for Webex Meetings uses the Messaging Layer Security (MLS) protocol for key exchange. MLS is a standard that builds on technologies developed in the open-source community and puts them in a rigorous, formally-verified setting. MLS allows Webex to provide forward secrecy and post-compromise security for participants in a meeting.
- **Content Protection:** To protect the media in a Webex Meeting using end-to-end encryption. Zero-Trust Security uses Secure Frames (SFrame), a fast and simple encryption framework for encrypting real-time media, which allows an extra layer of encryption to be added with minimal overhead.

Zero-Trust Security: End to End Identity for E2EE Webex Meetings

In addition to end-to-end encryption, Zero-Trust Security for Webex Meetings also provides end to end (E2E) identity, where user and device identities can be independently verified, by a non-Webex Certificate authority or Identity Provider.

E2E identity requires that Cisco Collaboration video devices and Webex Apps have credentials that prove their identity.

E2E identity for Cisco video devices in Webex Meetings uses the Automated Certificate Management Environment (ACME) protocol together with some extensions to leverage enterprise identity systems, to allow Webex to provide high-grade identity assurance with a seamless user experience.

In the future, E2E identity for Webex Apps in Webex Meetings will use new Open ID Connect standards for "UserInfo Verifiable Credentials" that integrate with MLS to provide strong and frictionless user authentication.

As shown in Figure 10, the identity verification status of each participant in a Webex E2EE meeting is shown in the meeting roster, allowing each participant to see at a glance how each users identity has been verified, and to drill down to check the specific details of a participant's identity.

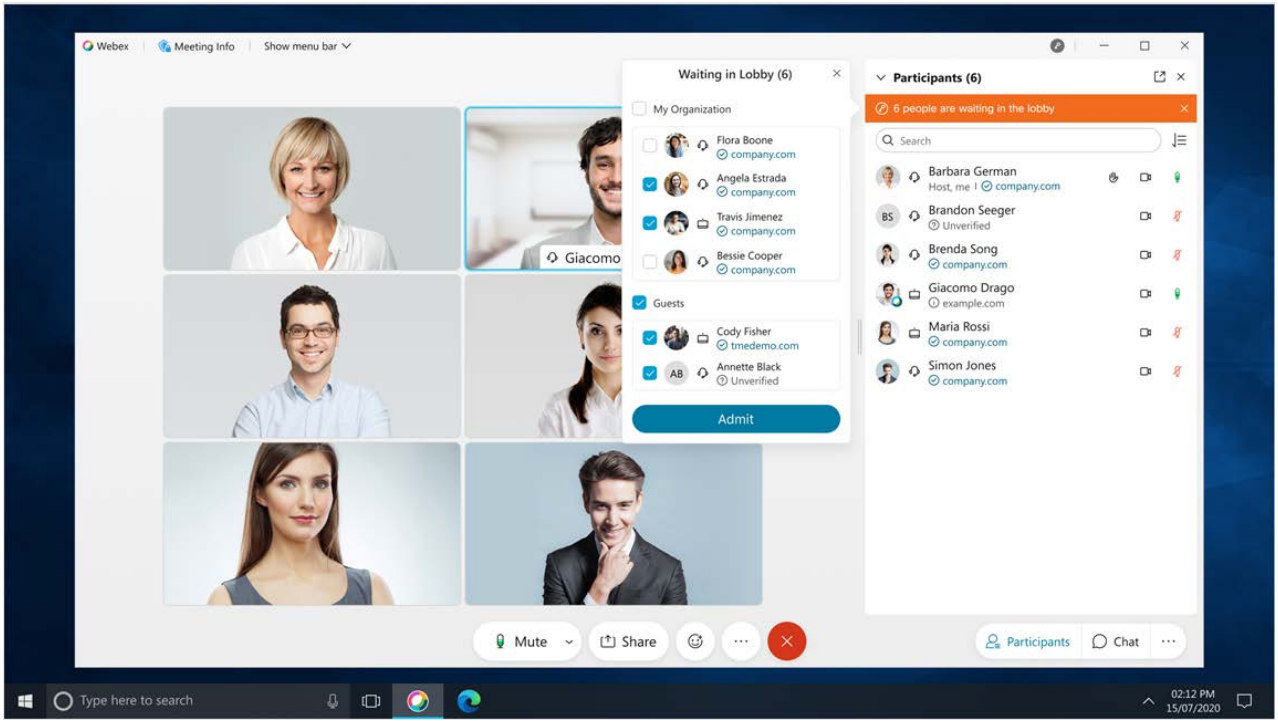

Figure 10. Webex Meetings Roster: Identity Visibility

For more details on Webex Zero-Trust Security see:
https://www.cisco.com/c/en/us/solutions/collateral/collaboration/white-paper-c11-744553.html

8. Cisco Collaboration Devices Configuration

After a device has been onboarded to Control Hub, an administrator often needs to make configuration changes. Configuration of the device is possible via several methods:

- Control Hub
- Video Device Web Interface
- Application Programming Interface (API)

The following sections discuss each source of configuration from a security perspective.

Control Hub

Control Hub provides several security-related configuration options, including:

- Face Recognition - Name Labels
- Webex Assistant
- Automatic Crash Reporting
- Device Configurations
- Remote Access Key

When you enable face recognition from Control Hub for your organization, you can send an email to invite your users to enroll. It includes a link that they can follow to take a photo of themselves and sign up. Once both the organization setting is enabled and a user has enrolled, that user can be recognized by Webex when they are seen by a Room, Board or Desk Series device. Further information on the security of face recognition can be found in the Cisco Collaboration Video Device Privacy section.

Once enabled from Control Hub, Webex Assistant provides a quick and convenient way for anyone to use their voice to interact with Room, Board and Desk Series devices. Further information on the security of Webex Assistant can be found in the Webex Assistant section below.

Automatic Crash Reporting will allow the device to upload logs to Cisco in the event of a video device crash. This helps Cisco diagnose problems independently of raised support cases. Crash reports can include user and organization identifiers, user agent strings, sanitized browser strings, client IP addresses and user device MAC addresses. All information is treated confidentially and used solely for product quality enhancement.

You can access a subset of advanced configurations for individual video devices directly from Control Hub. Some configurations will be shown as Read Only and cannot be changed from Control Hub whereas others can be viewed and edited; any changes will then be made on the video device using the same secure communication methods discussed above.

Control Hub also allows generation of a Remote Support Key for a video device. The use of this key may be requested by Cisco Technical Assistance Center (TAC) to troubleshoot a problem. Once the key is generated it must be sent to TAC who will then use an internal tool to convert this to an authentication method directly on the video device, removing any need for you to generate a user account or provide credentials to the video device. You can deactivate the key after the support process is complete, by resetting it.

It is possible to find the state of the Remote Support User, using `xCommand UserManagement RemoteSupportUser GetState`. If required, it is also possible to permanently disable the ability for Remote Support Users to be generated (a factory reset is required to re-enable the functionality) `xCommand UserManagement RemoteSupportUser DisablePermanently.`

Please note that for TAC to be able to use RemoteSupport to access the Cisco Collaboration device, the TAC agent must be connected through a PC that has IP connectivity to the target device. This would mean that a user on-site with the device would need to be in an online meeting with the TAC agent to allow this to happen.

Cisco TAC are not able to use RemoteSupport if they do not have IP connectivity to the target device.

Video Device Web Interface

By default, the web interface of a video device is not directly accessible as all local user accounts on the video device are deactivated during onboarding. It is possible to onboard a device with local user accounts by using the CLI command `xCommand Webex Registration Start and specifying SecurityAction: NoAction` or by using the Cisco video device Connector software. It is also possible to create a local account on a factory reset device, and for that account to persist when registering the device to Control Hub by entering the device activation token into the devices WebUI and unchecking the ‘Disable local users and integrations’ check box. Please note that if the default admin account does not have a password set, even with unchecking the above tick box, the account would still be made inactive due to the lack of password being present.

If no user accounts are active, it is possible to access the web interface of the video device by using the *Launch Web Portal* option under the Device in Control Hub. This will cross launch a browser session to the video device directly and create a temporary local user, *Webex Admin*. This process involves creating a temporary token that is passed to the Cisco Collaboration device via Webex and the web browser. As a direct connection to the Cisco Collaboration device is established, the PC attempting to connect to the Cisco device must either be on the same subnet as the Cisco device or be on a routable network to the Cisco device. If the device is unreachable (for example, two different networks with no routing in between), then Control Hub will fail to connect and will inform the user that the device is not available. This process can be made more secure by uploading a valid certificate to the Cisco Collaboration device so that HTTPS can be used.

Once connected to the web interface, it is possible to activate the admin account or create a new user. Users can have multiple roles: *Admin, Audit, RoomControl, Integrator* and *User.* The details of the roles and their capabilities can be found in the administrator guide for the video device, it is recommended that users with the most limited roles possible be used.

By default, the web interface will use HTTPS. To support older web browsers, the minimum version of TLS that the web server can use is 1.1 (TLS 1.1 can be disabled), but modern browsers will negotiate TLS 1.2 or 1.3.

The video device has a self-signed certificate and a set of Certificate Authority certificates pre-installed. Service Certificates and Certificate Authorities can be added via the web interface or the API. A Service Certificate can be used for HTTPS, Audit and 802.1X purposes, or a separate certificate can be used for each function. Service Certificates use the PEM format and may contain an RSA or DSA encrypted private key, with or without a passphrase. Alternatively, a certificate and private key can be uploaded separately. Certificate Authority certificates can be added to the endpoint in PEM format with one or many certificates in a single file.

Application Programming Interface (API)

There are several ways to access the device API:

- SSH
- HTTP/HTTPS
- WebSocket
- RS-232 / Serial connection
- Bot / Webex user

SSH is enabled by default, but authentication will only be possible once a user is activated on the video device or if public key authentication is used. The default host key mechanism is RSA (Rivest–Shamir–Adleman) with a 2048 bit key-size. ECDSA (Elliptic Curve Digital Signature Algorithm) with NIST curve P-384 and EdDSA (Edwards-curve Digital Signature Algorithm) with Ed25519 signature schema can be enabled if required.

HTTP/HTTPS API access follows the same principles outlined in the web interface section above. Access to the API requires the user to authenticate using HTTP Basic Access Authentication as a user with the *admin* role.

API WebSocket connections are disabled by default, to use them they must be activated and then they will follow the HTTP/HTTPS settings for connectivity. If only HTTPS is enabled, only encrypted WebSocket connections are allowed. Authentication is supported using Basic authentication and the auth protocol header.

Serial connection may be provided via the USB or COM port depending on the device. Serial is enabled by default, but authentication is required by default before the API can be accessed. Therefore, a user must be activated before this is possible.

Any Control Hub full admin or device admin is authorized to access the Device API via the cloud. See https://developer.webex.com/docs/api/v1/device-configurations for more details.

The `xConfiguration Network [n] RemoteAccess Allow` setting can be used to restrict remote access to HTTP, HTTPS, WebSocket, SSH or Telnet on the device from certain remote IPv4/IPv6 addresses. Note that cloud API access is not affected by this setting.

9. RoomOS WebEngine

The RoomOS WebEngine is a single-tab Chromium browser running on Cisco video devices (see Figure 11). The WebEngine is used to deliver the following features:

- Third party web apps (Miro, Jira, Trello, Realtime Board, etc.)
- Digital signage
- WebRTC third party calling (Microsoft Teams, Zoom, Google, etc.)
- Webex embedded apps
- Web views opened from macros and third-party extensions (building maps, evacuation maps, instructional videos, etc.)
- Enterprise Content Management (cloud documents available as integration)

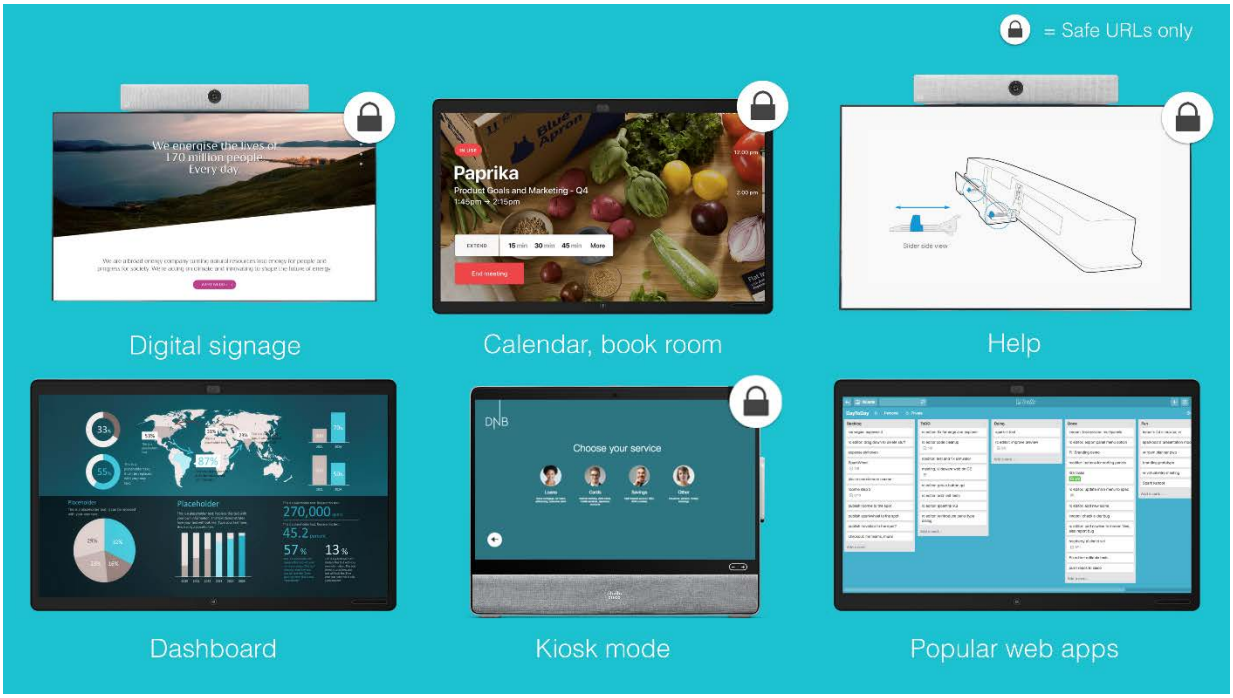

Figure 11. Cisco Collaboration Video Device: Web Engine

The WebEngine uses Linux sandboxing to run Chromium. Sandboxing isolates the Chromium instance from other processes on the device to ensure that code execution cannot make permanent changes to the host or access confidential information on the host. The WebEngine has no access to the file system and browser history is removed from the logs to protect the user's privacy. If a web proxy is configured on a Webex Room Series device, the WebEngine will send its traffic to this proxy.

Web features typically store user data in cookies, cache, local storage, etc. These data are managed s differently depending on the feature:

- Signage: Data persists and is never deleted automatically, but it can be deleted manually.
- Web apps: Data persists but is deleted once per day, by default. This can be disabled by setting `xConfiguration RoomCleanup AutoRun ContentType WebData` to `Off`. This is recommended for devices registered in personal mode. All web apps share the same profile, so you cannot delete data for web apps individually.
- WebRTC: Data is deleted after a call ends.
- Programmatic web views: Same as web apps.
- Embedded apps: Data is deleted after a call ends.

Any web data can be deleted manually with the xapi command `xCommand: WebEngine DeleteStorage`.

For more details on RoomOS WebEngine see: https://roomos.cisco.com/doc/TechDocs/WebEngine.

For RoomOS WebEngine xapi commands see: https://roomos.cisco.com/xapi/domain/?domain=WebEngine

10. Enterprise Network Security

Most enterprises implement multiple security products and features to protect their internal networks and data and to control external access. Cisco Collaboration devices support the following enterprise network security features, protocols, and products:

- VLANs: CDP, 802.1Q
- Network Access Control (802.1X): EAP-FAST, EAP-TLS
- Wi-Fi Security: EAP-FAST/TLS/TTLS/PEAP, WPA/WPA2/WPA3 Personal/Enterprise with CCMP128
- NAT/Firewall Traversal
- Proxy Server – Authentication and TLS Inspection

These security features are discussed at a high level in this document. For more details on enterprise network requirements for Webex services including Webex IP subnets for media and URLs for signaling to services, see (and subscribe to) the Network Requirements for Webex Services article.

Firewall and Proxy Traversal

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 as shown in Figure 12, a common deployment forces all HTTP/TLS based traffic through a proxy server allowing only HTTP/TLS traffic originating from the proxy server to traverse the firewall and reach the Internet. Other traffic types such as UDP, TCP and TLS-based media from Cisco video devices traverse the firewall directly and are not directed to the proxy server.

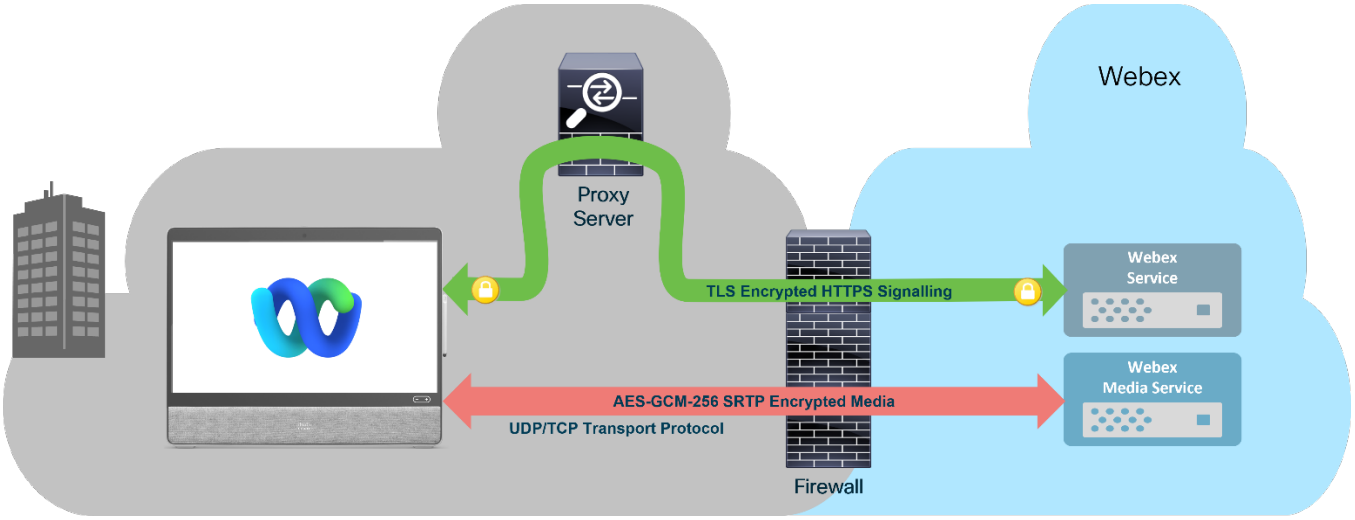

Figure 12. Typical Webex Traffic Flows Through Proxy and Firewall Devices

Note: All Cisco Collaboration video devices initiate outbound connections only from the enterprise network to Webex services.

HTTP Proxy Traffic Inspection and Certificate Pinning

Traffic inspection by a proxy server, where the proxy decrypts, inspects and re-encrypts the TLS/HTTPS traffic traversing the server, is commonly used by security conscious customers. Traffic inspection by a proxy server has limited value for Cisco video device traffic, as decrypting and inspecting traffic only reveals signaling information.

As shown in Figure 13, with traffic inspection, the proxy server presents its Enterprise CA signed certificate, instead of the Webex service certificate, to the Cisco video device. This allows the proxy server to directly establish a TLS connection to the Cisco video device and to decrypt and inspect its TLS traffic. Similarly, traffic between the proxy server and the Webex service can also be encrypted/decrypted and inspected.

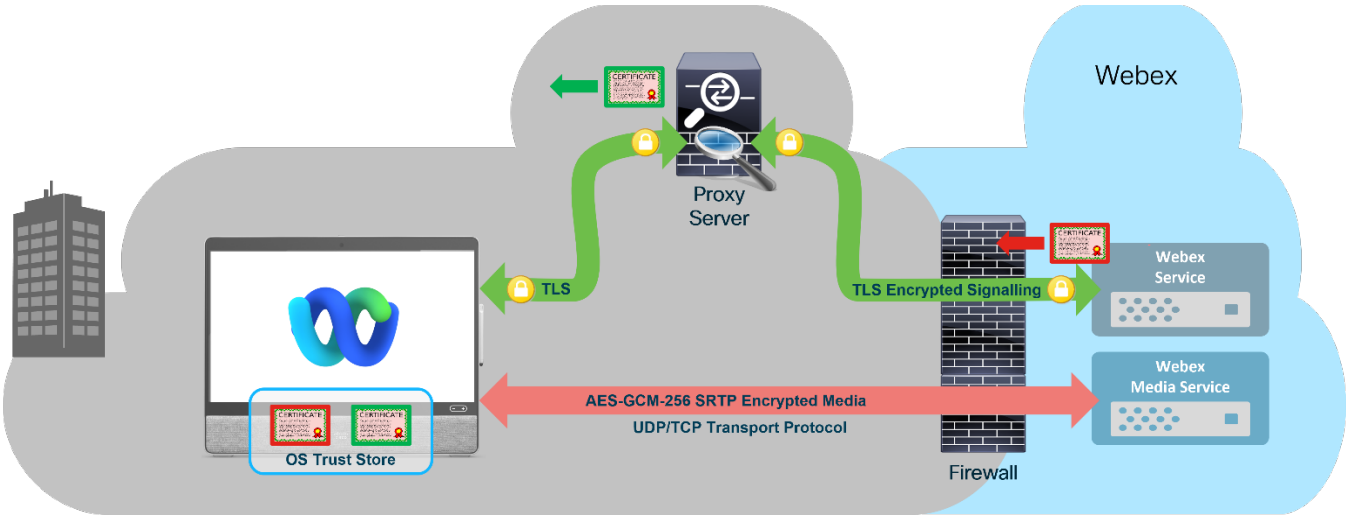

Figure 13. Proxy Server TLS Traffic Inspection

Cisco Collaboration devices validate certificates during TLS session establishment to verify that they originate from Webex services. With traffic inspection by the proxy server, the enterprise CA signed certificate sent by the proxy will not match the expected public CA signed Webex server certificates. In this case, the Cisco video device searches its trust store for a certificate that matches the one received from the proxy server. If a matching certificate is found, the TLS connection from the video device to the proxy server is allowed to be established.

As described earlier in Onboarding Cisco Video Devices to Webex, during the Cisco video device onboarding stage, Enterprise CA Certificate trust anchors can also be downloaded from the Webex identity service into the device, to permit TLS inspection of Cisco video device signaling traffic by an Enterprise Proxy server. Customers need to open a service request with Cisco TAC to upload their Enterprise CA certificates to the Webex Cloud identity service.

11. Cisco Collaboration Devices: Pairing with Webex Apps

Webex desktop and mobile applications can pair with Cisco Collaboration devices for device control and content sharing.

Cisco Desk, Board and Room series devices use ultrasonic signaling and tokens to pair with Webex Apps. In Figure 14, unique tokens are generated by the Webex cloud every 30 seconds and securely sent over TLS to the Cisco Collaboration device, which emits these tokens using ultrasonic signaling from the device speakers. A Webex App within range of the ultrasonic signal can use the received token to pair with the Cisco Desk, Board or Room series device, by sending the token to the Webex cloud service. Once the Cisco Collaboration device and

Webex App are paired, newly emitted tokens must be received by the Webex App and sent to the Webex cloud service to maintain the paired connection.

One reason for using ultrasonic signaling for device detection is its limited range; ultrasound signals typically do not pass through walls, limiting the pairing token's range to the enclosed room that the endpoint is placed within.

Automatic pairing with Cisco Desk, Board and Room series devices can be disabled by setting the ultrasound volume to zero.

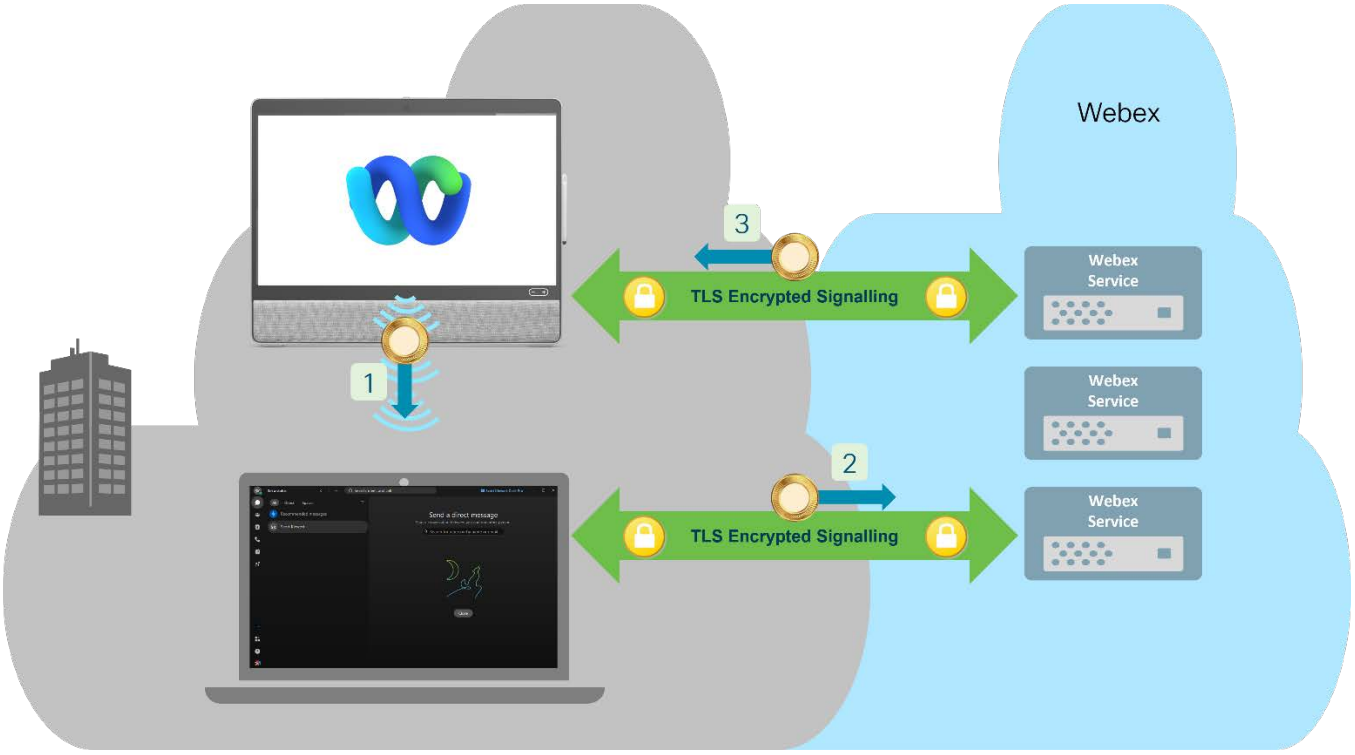

Figure 14. Ultrasound Pairing between Webex Apps and Cisco Collaboration Devices

Figure 15 shows that once the paired connection between the Cisco Desk, Board or Room series device and Webex App has been established using the Webex cloud, the Webex App can control the Cisco Collaboration device to make calls, join meetings, share content, mute the device microphone and so on. Both the Webex App and the Cisco Collaboration use their existing TLS connections to the Webex cloud, to exchange call control signaling and media for content sharing.

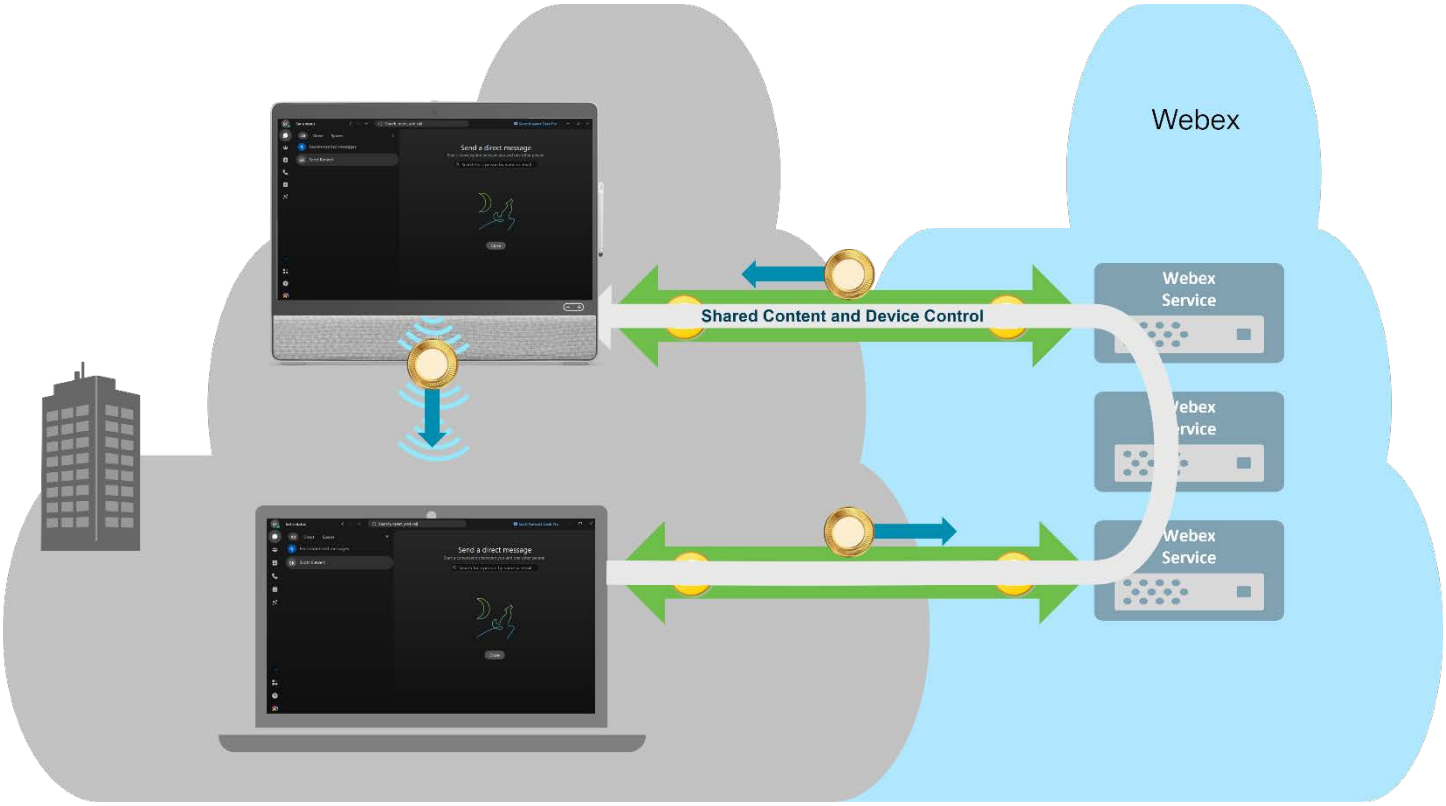

Figure 15. Content Sharing Between Webex Apps and Cisco Collaboration Device

Other Cisco Collaboration Video Device Discovery Mechanisms

The Webex App can also use Wi-Fi to discover Cisco Desk, Board and Room series devices and manually connect using a PIN. For more information, see the following articles:

- Manage discovery of nearby Webex devices
- Connect to a Webex App device

Apple AirPlay can also be enabled to allow Apple devices, such as iPhone, iPad and Mac's to be able to discover and share to an enabled Cisco Collaboration device without the need for the Webex App.

Please see the Configure wireless sharing with AirPlay article for further information. By default, the option to utilize Apple AirPlay is disabled and will require IT intervention using Control Hub to make it available to the end users.

Miracast® can also be enabled to allow Windows based PC and some Android based mobile devices to be able to discover and share to an enabled Cisco Collaboration device without the need for the Webex App. The Cisco Collaboration device does need to be connected to a wired network for Miracast to be supported. When enabled by IT, an end user will be able to share both in and out of call using a Wi-Fi Direct connection between the Windows PC/Android mobile device and the Cisco Collaboration device. Please see the Configure wireless sharing with Miracast® article for further information. By default, the ability to share via Miracast is disabled and requires a Control Hub admin to enable it.

Apple AirPlay and Miracast® both require RoomOS 11 to be deployed to the Cisco Collaboration device.

12. Cisco Collaboration Video Device Privacy

Webex offers a range of AI features that can enhance the user's experience when in a Webex call or Webex meeting:

- Background noise removal
- Optimize for my voice
- Music mode
- Gesture recognition
- Face recognition
- Language intelligence:
    - Webex Assistant
    - Closed captioning
    - Real time translation
    - Meeting transcription
- Room interpretation
- People presence detection
- Proximity Pairing

Cisco video devices process audio and video locally for most AI features. Webex only streams media to the cloud when the user is in a call or meeting. The next few sections provide additional information about some of the Webex AI features and Table 2 provides clarification on when media is processed locally or streamed to the cloud to facilitate these features.

Webex Audio Intelligence: Background Noise Removal & Audio Optimization

Audio intelligence is only used during a call or meeting and audio is processed locally on the device. Background noise reduction removes unwanted noise such as keyboard chatter, dog barking, etc. Audio optimization features are used to suppress the voices of those speaking in the background or to optimize audio for music. If a user has muted their microphone during a call, devices maintain access to the microphone and sample the audio to determine if they are speaking, so it can notify the user that their microphone is muted. Audio samples are never sent to the Webex cloud when the device is muted.

Gesture Recognition

Gesture recognition is only used during Webex Meetings and Webinars. Cisco video devices use the camera and onboard software to detect when meeting participants raise their hands, give a thumbs up or thumbs down, or clap. These gestures are momentarily presented as on-screen icons to participants in the meeting. The processing for this feature is done locally, and no media is sent to the cloud. For more information on using gesture recognition with a Cisco Desk Series, see Gesture Recognition on Desk Series.

Facial Recognition

Facial recognition is used to create and display name labels of meeting participants. When facial recognition is enabled in an organization, Cisco video device use the image from the camera to create a vector data set that represents the user's face. This data set is sent to the face recognition service in the Webex cloud. Cisco video devices only attempt to detect a user's face when they are an active participant in a meeting and will only detect the user's face and provide a name label if they have opted-in to the feature. Facial recognition technology never streams a user's image to the facial recognition service.

Language Intelligence

Language intelligence is used by Webex Assistant and in Webex Meetings for closed captioning, real-time translation, and meeting transcription.

Webex Assistant for devices is activated by the wake word “OK Webex” or “Hey Webex.” Once activated, users can give Webex Assistant verbal commands such as “start meeting,” “increase volume,” or “call a number.” When using Webex Assistant, Cisco video devices only listen for the wake word, which is processed locally. Devices do not continuously stream media to the Webex cloud. Meeting and webinar hosts can also activate Webex Assistant in a meeting. Once Webex Assistant has been activated, devices will send the user’s verbal instructions in an audio stream to the Webex cloud for interpretation and execution.

Additionally, to make meetings and webinars more accessible, Webex provides live automated closed captions which users can enable without needing to enable Webex Assistant. As participants speak, captions will appear above the meeting or webinar controls. If Webex Assistant is also enabled, then users can also make highlights or use voice commands, as described above.

For a comparison of Webex Assistant and automated closed captioning, see Compare Webex Assistant and Automated Close Captions.

Webex Meetings also uses Language intelligence for:

- Real-time translation for multiple languages
- Meeting transcription

Room Interpretation – People Count

People count uses the Cisco video device camera and software for head detection and sends the results to the Webex cloud. Cisco does not keep a record of who was in the room, only the average number of people detected. If needed, the people count feature can be enabled outside of a call or meeting.

People Presence Detection

Cisco video devices use the speaker to emit an ultrasonic audio signature and use the microphone to monitor for changes in the returned audio.

Ultrasonic Pairing

Cisco video devices use ultrasonic signaling to transmit beacons to nearby Webex Apps. This allows users to pair the device with their Webex App to make calls and share their screen on the device. The Webex App uses the microphone on a personal computer, or mobile device, to detect these ultrasonic beacons. With ultrasonic pairing enabled, the microphone used by the Webex App will be enabled to listen for beacons, but no audio is sent to the Webex cloud.

Wi-Fi Based Device Discovery and Pairing

Wi-Fi based device discovery and pairing allows the Webex App to discover, pair with, and control nearby Cisco video devices, so that users can join meetings, make calls and share their screen on the device.

Table 2 describes each of the Webex advanced collaboration features listed above and provides basic configuration and operational information.

Table 2. Webex Advanced Collaboration Feature Controls

WEBEX ADVANCED COLLABORATION FEATURE	SUPPORTED BY	AUDIO OR VIDEO SENT TO WEBEX CLOUD FOR THIS FEATURE?	WHERE THIS FEATURE CAN BE CONFIGURED	DEFAULT SETTING
Background noise removal	Cisco video devices Webex App	No	End User settings	On

Optimize for my voice/all voices	Cisco video devices (my voice) Webex App	No	End User settings	Off
Music Mode	Cisco video devices Webex App	No	End User settings	Off
Gesture Recognition	Cisco video devices Webex App	No	End User In-meeting controls	Off
Face Recognition	Cisco video devices	No	Webex administrator (global setting for organization) and End User settings	Org: Off User: Off
Language intelligence Webex Assistant (WXA)	Cisco video devices Webex App	Yes – But only when activated using the wake word, or when activated in a meeting.	Webex administrator (Organization and Site settings) and End User In-meeting controls	Site: Off User: Off
Language intelligence Real Time Translation	Cisco video devices Webex App	Yes - Used during a Webex Meeting	Webex administrator (Site setting) and End user In-meeting controls	Org: Off User: Off
Language intelligence Meeting transcript	Cisco video devices Webex App	Uses AI to convert meeting recordings into transcripts	Webex administrator (global setting for organization) and End User settings	Org: On User: On
Language intelligence Closed captioning	Cisco video devices Webex App	Yes - Used during a Webex Meeting	Webex administrator (global setting for organization) and End User In-meeting controls	Org: On User: Off
Room interpretation - People count	Cisco video devices	No	Webex administrator (global setting for organization)	Org: Off In call: Off Out of call: Off
People presence detection	Cisco video devices	No	Webex administrator (global setting for organization)	Org: Off
Ultrasound based pairing	Cisco video devices Webex App	No	Webex administrator (global setting for organization) Cisco video device settings Webex App: End User settings	Org: On Device: On Desktop app: On Mobile app: Off
Wi-Fi based pairing	Cisco video devices Webex App (Desktop only)	No	Cisco video device settings Webex App (Desktop): End User settings	Org: On Device: On App: On

Cisco Collaboration Video Devices – Remote Monitoring Option Key

The remote monitoring feature allows an administrator to monitor a room from the Cisco Collaboration device's web interface. As with the remote support access feature covered earlier, remote monitoring of the Cisco Collaboration device is only possible if the device is network reachable (e.g., on your corporate network). To enable the feature, an option key must be purchased for the device and installed. As part of this purchasing procedure, it will be made clear that use of this feature requires the purchaser to comply with local laws and regulations. Remote monitoring is useful when you want to control the video device from another location. Snapshots from the camera appear in the web interface, so you can check the camera view and control the camera without being in the room. If enabled, snapshots are automatically refreshed approximately every 5 seconds. While Remote Monitoring provides a useful function, local laws and regulations and user notification must be considered before enabling this feature.

PLEASE BE AWARE THAT IF YOU ENABLE THE REMOTE MONITORING OPTION YOU MUST MAKE SURE THAT YOU COMPLY WITH LOCAL LAWS AND REGULATIONS AND PROVIDE ADEQUATE NOTICE TO USERS OF THE SYSTEM THAT THE SYSTEM ADMINISTRATOR MAY MONITOR AND CONTROL THE CAMERA AND SCREEN. IT IS THE RESPONSIBILITY OF AN ORGANIZATION'S ADMINISTRATOR(S) TO COMPLY WITH APPLICABLE LAWS AND REGULATIONS WHEN USING THIS FEATURE. CISCO DISCLAIMS ALL LIABILITY FOR ANY UNLAWFUL USE OF THIS FEATURE.

13. Cisco Collaboration Video Devices – Physical Security

Cisco Collaboration Video Devices – Physical Port and Interface Security

Cisco video devices support several physical port types that can be used to connect to external devices, such as microphones, speakers, cameras, navigators, and PCs to augment your experience in meetings and calls. Common interface types for audio, video, and data connections supported by Cisco video devices include:

- Mini Jack (3.5mm)
- Ethernet
- Euroblock (Phoenix)
- USB
- HDMI
- SDI

Where applicable, video device interfaces can be enabled or disabled via API or the device's WebUI. For a complete list of physical interfaces on Cisco video devices and configuration options, refer to the product specific data sheets (Desk / Room / Board) and the latest command reference.

Current Cisco video devices do not possess the capability to share their network connections with connected peripherals, such as laptops. For more information refer to the Assessing the risks of network boundary compromise via Cisco RoomOS devices.

Ethernet Ports

Some video devices have more than one ethernet port. The Cisco Desk Pro offers an additional network port is available that acts as a switch. This allows a single ethernet connection to the device that can then be shared with another device such as a PC. Cisco Room series and Cisco Board series may have one or more ethernet ports that only provide a local network to the device. It is possible to connect a PC to one of these tertiary network ports and access the Cisco Collaboration device with, for instance, SSH, but the authentication requirements remain the same.

Wireless Interfaces

The latest Cisco Desk, Room, and Board series video devices also provide the following wireless interfaces:

- Wi-Fi - 802.11a/b/g/n/ac (2.4 GHz and 5 GHz bands)
- Wi-Fi – 802.11ax (6 GHz band) - refer to product data sheets for model support.
- Bluetooth® Note: Using a wireless network connection is a flexible option, however an Ethernet connection is always preferred for high performance.

Non-radio versions of Cisco Collaboration video devices are available for secure deployments where Wi-Fi and Bluetooth® radios are restricted.

Refer to product data sheets for model specific support information (Desk / Room / Board).

14. Cisco's Security Model

Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout the company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet the highest levels of security in everything Cisco does.

This organization is also dedicated to providing customers with the information they need to mitigate and manage cybersecurity risks.

The Webex security model (Figure 16) is built on the same security foundation deeply engraved in Cisco's processes.

The Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Webex services.

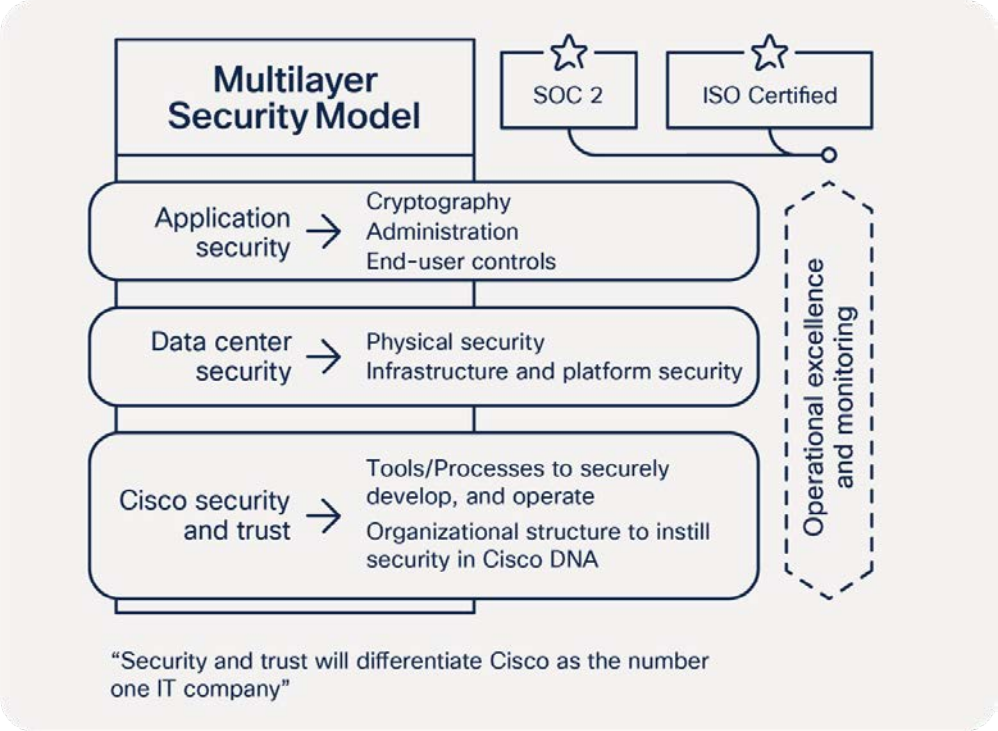

Figure 16. Webex Security Model

15. Webex Security and Trust

Cisco Security Tools and Processes

Cisco Secure Development Lifecycle (CSDL)

At Cisco, security is not an afterthought. It is a disciplined approach to building and delivering world-class products and services from the ground up. All Cisco product development teams are required to follow the Cisco Secure Development Lifecycle (CSDL). It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Webex Product Development team passionately follows this lifecycle in every aspect of product development.

For more information, refer to the Cisco Secure Development Lifecycle Overview.

Cisco Foundational Security Tools

The Cisco Security and Trust Organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development.

Some examples of tools include:

- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling
- Coding guidelines
- Validated or certified libraries that developers can use instead of writing their own security code
- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects
- Software tracking that monitors Cisco and third-party libraries and notifies the product teams when a vulnerability is identified

Organizational Structure that Instills Security in Cisco Processes

Cisco has dedicated departments in place to instill and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Webex environment to customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into customers' hands.
Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to the Webex service.
Cisco InfoSec is also responsible for continuous improvement in Webex's security posture.

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities.
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches.
- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, PSIRT may alert customers, even without full availability of patches.

In all cases, PSIRT discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.
Refer to the PSIRT infographic to learn more about PSIRT.

Security responsibility

Although every person in Webex group is responsible for security, the following are the main roles:

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications
- Vice president, engineering, Cisco Cloud Collaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

Internal and external penetration tests

The Webex group conducts rigorous penetration testing regularly, using internal assessors. Beyond its own stringent internal procedures, Cisco InfoSec also engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identifying critical application and service vulnerabilities and proposing solutions
- Recommending general areas for architectural improvement
- Identifying coding errors and providing guidance on coding practice improvements

Third-party assessors work directly with the Webex engineering staff to explain findings and validate the remediation. Penetration test letters of attestation for Webex services are available under NDA on the Cisco Trust Portal.

16. Data Privacy

Webex takes customer data protection seriously. Cisco collects, uses, and processes customer information only in accordance with the Cisco Privacy Statement and the privacy data sheets available on Cisco Trustportal.

Webex is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements, including the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Health Information Protection Act (PHIPA), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA).

17. Transparency

Webex users and customers should understand what their choices are and how Cisco manages and protects the data they entrust to Cisco. Cisco uses a layered model of transparency to make this happen. Short disclosures that help users make real-time decisions are provided within the Webex App itself. Further information is available on the support pages, which are updated on a regular basis. And for all the details of what information Cisco collects, how it is used, and how it is protected, refer to the privacy data sheets available on Cisco Trustportal.

Cisco is also committed to publishing data regarding requests or demands for customer data that are received from law enforcement and national security agencies around the world. Cisco publishes this data twice yearly (covering a reporting period of either January-to-June or July-to-December). Like other technology companies, Cisco will publish this data six months after the end of a given reporting period in compliance with restrictions on the timing of such reports.

More information can be found at in the transparency section of the Cisco Trust Center available at https://trust.cisco.com.

Cisco has also invested in several transfer mechanisms to enable the lawful use of data across jurisdictions, including:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

18. Industry Standards and Certifications

In addition to complying with our stringent internal standards, Webex also continually maintains third-party validations to demonstrate our commitment to information security. Webex has received the following certifications:

- ISO 27001, 27017, 27018 and 27701
- Service Organization Controls (SOC) 2 Type II
- SOC 3
- EU Cloud Code of Conduct Adherence by SCOPE Europe
- CAS CSTAR 2
- Cloud Computing Compliance Controls Catalogue (C5) attestation
- FedRAMP (visit https://cisco.com/go/fedramp for more details)

  Note: FedRAMP certified Webex service is only available to U.S. government and education customers.

19. Conclusion

Be collaborative and get more done, faster, using Cisco Collaboration video devices. Webex is a trusted industry leader in web and video conferencing, messaging, and calling. Webex offers a scalable architecture, consistent availability, and multilayer security that is validated and continuously monitored to comply with stringent internal and third-party industry standards. Cisco connects everything more securely to make anything possible.

20. How to Buy

To view buying options and speak with a Cisco sales representative, visit How to Buy Cisco Products.

21. For More Information

Cisco Collaboration Video Devices