Whitepaper

Webex Meetings security

webex by CISCO

Contents

Introduction

Webex Meetings helps enable global employees and virtual teams to collaborate in real time as though they were working in the same room. Businesses, institutions, and government agencies worldwide rely on Webex Meetings solutions. These solutions help simplify business processes and improve results for sales, marketing, training, project management, and support teams.

For all these companies and agencies, security is a fundamental concern. Online collaboration must provide multiple levels of security for tasks that range from scheduling meetings to authenticating participants to sharing documents.

Cisco makes security the top priority in the design, development, deployment, and maintenance of its networks, platforms, and applications. You can incorporate Webex Meetings solutions into your business processes with confidence, even with the most rigorous security requirements.

This paper provides details about the security measures of Webex Meetings and its underlying infrastructure to help you with an important part of your investment decision.

What you will learn

This paper describes the security features of Webex Meetings Suite. It discusses the tools, processes, and engineering that help customers confidently collaborate on Webex.

Webex Meetings include:

- Webex Meetings
- Webex Webinars[1]
- Webex Training
- Webex Support
- Webex Edge
- Webex Cloud Connected Audio
- Webex Assistant
- Slido (Polling)[2]

Webex security model

Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout our 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 we do.

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

The Webex security model (Figure 1) 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. We will discuss some of these elements in this document.

[1] Formerly Webex Events

[2] For Slido security information refer to the Slido in Webex (Polling) security white paper available at cisco.com/content/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/Slido-in-Webex-Security-Paper_1-0.pdf

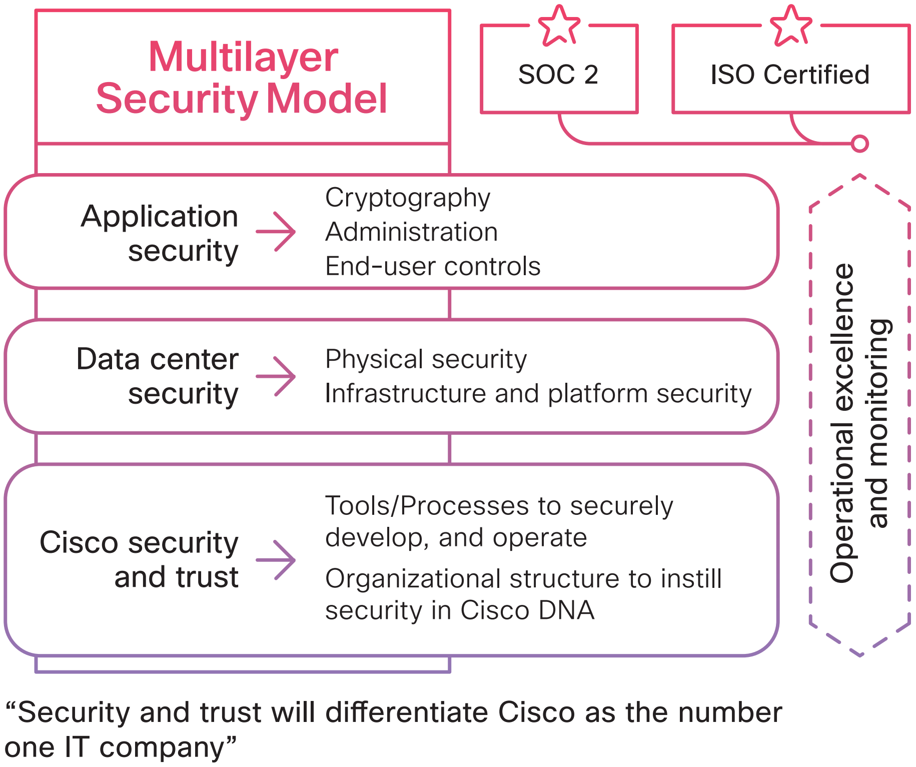

Multilayer Security Model
SOC 2
ISO Certified
Application security
Cryptography
Administration
End-user controls
Data center security
Physical security
Infrastructure and platform security
Cisco security and trust
Tools/Processes to securely develop, and operate
Organizational structure to instill security in Cisco DNA
Operational excellence and monitoring
"Security and trust will differentiate Cisco as the number one IT company"

Figure 1. Webex security model

Cisco security and trust

Cisco security tools and processes

Cisco secure development lifecycle

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. 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.

Read more about the Secure Development Lifecycle.

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 our customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into our 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.

Learn more about PSIRT online here.

Security responsibility

Although every person in Webex group is responsible for security, 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. As needed, Cisco InfoSec can provide a letter of attestation from these vendors.

Webex data center security

Webex is a software-as-a-service (SaaS) solution delivered through the Webex Cloud, a highly secure service-delivery platform with industry-leading performance, integration, flexibility, scalability, and availability. The Webex Cloud is a communications infrastructure purpose-built for real-time web communications.

Webex meeting sessions use switching equipment located in multiple data centers around the world. Cisco data centers are used for the majority of Webex Cloud services. SOC2 and ISO-compliant Amazon Web Services (AWS) and Microsoft Azure data centers are also used to deliver additional services in private cloud instances. These data centers are strategically placed near major internet access points and use dedicated high-bandwidth fiber to route traffic around the world.

Additionally, Cisco operates network Point-of-Presence (PoP) locations that facilitate backbone connections, internet peering, global site backup, and caching technologies to enhance performance and availability for end users.

Physical security

Physical security at the data center includes video surveillance for facilities and buildings and enforced two-factor identification for entry. Within Cisco data centers, access is controlled through a combination of badge readers and biometric controls. In addition, environmental controls (e.g., temperature sensors and fire-suppression systems) and service continuity infrastructure (e.g., power backup) help ensure that systems run without interruption.

Data center servers are segmented into “trust zones”, based on infrastructure sensitivity. For example, databases are “caged”, the network infrastructure has dedicated rooms, and all equipment racks are locked. Only Cisco security personnel and authorized visitors accompanied by Cisco personnel can enter the data centers.

Cisco’s production network is a highly trusted network: only very few people with high trust levels have access to the network.

Infrastructure and platform security

Platform security encompasses the security of the network, systems, and the overall Webex data center. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening, security patching, and vulnerability scanning and assessment.

Servers are hardened using the Security Technical Implementation Guidelines (STIGs) published by the National Institute of Standards and Technology (NIST). Firewalls protect the network perimeter. Access Control Lists (ACLs) segregate the different security zones. Intrusion Detection Systems (IDSs) are in place, and activities are signed and monitored on a continuous basis. Daily internal and external security scans are conducted across Webex. All systems are hardened and patched as part of regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

Service continuity and disaster recovery are critical components of security planning. The design of Cisco data centers with global site backups and high-availability help enable the geographic failover of Webex services. There is no single point of failure.

Webex application security

Cryptography

Encryption of data in transit

All communications between cloud registered Webex apps, Webex devices and the Webex services occur over encrypted channels. Webex uses TLS protocol with version 1.2 or later with high strength cipher suites for signaling.

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted[3].

Encrypted media can be transported over UDP, TCP, or TLS. Cisco prefers and strongly recommends UDP as the transport protocol for Webex voice and video media streams. This is because TCP and TLS are connection-orientated and transport protocols designed to reliably deliver correctly ordered data to upper-layer protocols. Using TCP or TLS, the sender will retransmit lost packets until they are acknowledged, and the receiver will buffer the packet stream until the lost packets are recovered. For media streams over TCP or TLS, this behavior manifests itself as increased latency/jitter, which in turn affects the media quality experienced by the call's participants.

Media packets are encrypted using either AES 256 or AES 128 based ciphers. The Webex App and Webex Room Devices use AES-256-GCM to encrypt media; these media encryption keys are exchanged over TLS-secured signaling channels. SIP and H323 devices that support media encryption with SRTP can use AES-256-GCM, AES-128-GCM, or AES-CM-128-HMAC-SHA1 (AES-256-GCM is the Webex preferred media encryption cipher).

Zero Trust Security based end-to-end encryption for Webex Meetings

For standard meetings, where devices and services use SRTP to encrypt media on a hop by hop basis, Webex media servers need access to the media encryption keys to decrypt the media for each SRTP call leg. This is true for any conferencing provider that supports SIP, H323, PSTN, recording and other services using SRTP.

[3] For SIP and H323 based endpoints connecting to a Webex meeting, Cisco strongly recommends that all media and signaling streams are encrypted from the endpoint, Expressway/SBC at the enterprise network edge, such that no unencrypted traffic traverses the Internet.

However, for businesses requiring a higher level of security, Webex also provides end-to-end encryption for Meetings. With this option, the Webex Cloud does not have access to the encryption keys used by meeting participants and cannot decrypt their media streams. Webex Zero Trust Security based end-to-end encryption uses standards track protocols to generate a shared meeting encryption key (Messaging Layer Security (MLS)) used to encrypt meeting content (Secure Frame (S-Frame)). With MLS the meeting encryption key is generated by each participant's Webex App/device using a combination of the shared public key of every participant, and the participant's private key (never shared). The meeting encryption key never traverses the cloud and is rotated as participants join and leave the meeting. For more details on Zero Trust Security based end-to-end encryption see the Zero Trust Security for Webex white paper.

With end-to-end encryption, all meeting data (voice, video, chat, etc.) generated by Webex App and Webex Devices is encrypted using the locally derived meeting encryption key, and this data cannot be deciphered by the Webex service.

End-to-end encrypted meeting types are available for Webex Meetings. When end-to-end encryption is enabled, Webex services and endpoints that need access to meeting keys to decrypt content (e.g. devices using SRTP where encryption is performed hop by hop) are not supported. This restricts meeting participants to those using the Webex App or cloud registered Webex Devices only, and excludes services such as network based recording, speech recognition, etc.

For details of supported and unsupported features see End-to-End Encryption with Identity Verification for Webex Meetings.

Private Webex Meetings

If your organization has Video Mesh on your network, your administrator can enable private meetings by contacting your account representative. This feature enhances the security of your meeting by terminating the media on your premises. When you schedule a private meeting, the media always terminates on the Video Mesh nodes inside your corporate network with no cloud cascade.

For more details on Private Webex meetings and design guidance for Video Webex Edge Video Mesh, click here.

Encrypted Webex Signaling

Webex services support TLS version 1.2 and later. TLS version 1.2 cipher suites are listed below in preference order for secured communication. Webex services will select the strongest possible cipher for the customer's environment.

Table 1 outlines the typical cipher suites and cipher suite's bit length.

Table 1. Cipher suites and bit lengths

CIPHER SUITES	BIT LENGTH
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128

Protecting meeting contents stored in the Webex Cloud

The Webex service allows you to securely store Meeting recordings and transcripts in the Webex Cloud. These files are individually encrypted and stored in your region.

Meeting recordings and transcripts are encrypted using the AES-256-GCM encryption cipher. These files are protected in a similar way to files and messages shared in Webex Spaces.

- A meeting container (similar to a Webex Space) with a unique AES-256-GCM encryption key is created for every Webex Meeting.
- When a meeting recording is encrypted and stored in the Webex Cloud; a message is added to the meeting container with the key used to encrypt the file and a URL for the encrypted file's location. This message is encrypted using the meeting container's encryption key.
- Users with permission to access to the meeting container can retrieve recordings and transcripts by retrieving the encrypted message containing the file's location and file encryption key and then decrypting this message using the meeting container encryption key.

Meeting containers use the same key management system (KMS) as Webex Messaging, allowing organizations using the Webex Meetings service to deploy Hybrid Data Security (on-premises KMS) and Bring Your Own Key (BYOK) services to enhance the secure storage and protection of encryption keys.

Storage, access and deletion of meeting recordings and transcripts

Administrators can define a retention period for stored meeting content in Control Hub, once the retention period has been reached, stored content will be deleted from the Webex Cloud. Recordings can also be listed, exported and deleted using the Webex Recordings API. Learn more.

Recordings and transcripts stored in the Webex Cloud can be:

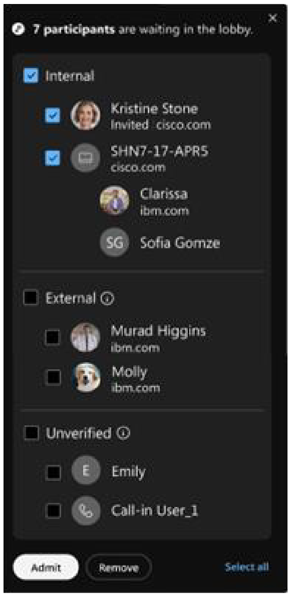
- Password protected (passwords are stored using SHA-2 (one-way hashing algorithm) and salts)
- Restricted to signed-in users only
- Prevented from being downloaded
- Managed by the content owner from their Webex page/Webex App

Administrators can also allow users to record meetings on their computers.

Webex Meetings – lobby controls and verified identity

The Webex Meeting lobby allows meeting hosts (and co-hosts) to vet and manage users before they are admitted to a meeting as a participant. Users in the meeting lobby are grouped and managed in three categories (Figure 2):

1. Signed-in (authenticated) users in your organization
2. Signed-in (authenticated) users outside of your organization
3. Unverified users – Unauthenticated Guest users, whose identity is not verified



7 participants are waiting in the lobby.

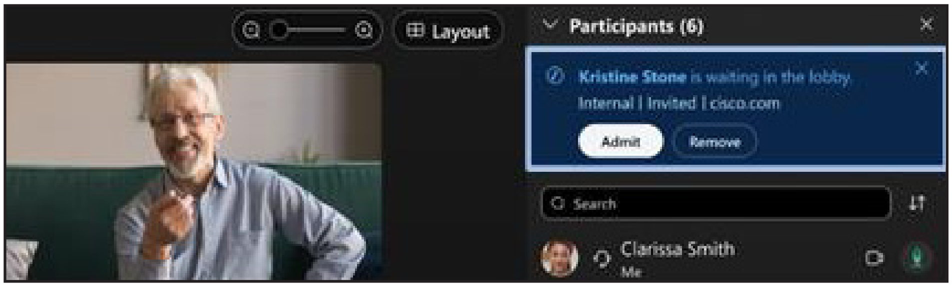
☑ Internal
- ☑ Kristine Stone, Invited cisco.com
- ☑ SHN7-17-APR5, cisco.com
- Clarissa, ibm.com
- SG Sofia Gomze

□ External
- □ Murad Higgins, ibm.com
- □ Molly, ibm.com

□ Unverified
- □ E Emily
- □ Call-in User_1

Figure 2. Webex Meeting lobby

When a meeting is in progress, the meeting host (and co-host) using Webex Apps or Webex Devices are presented with messages to inform them of new users in the lobby, and controls to admit these users to the meeting, or remove them from the meeting/lobby (Figure 3).



Participants (6)

Kristine Stone is waiting in the lobby.
Internal | Invited | cisco.com

Clarissa Smith
Me

Figure 3. Lobby notification

Webex Role-Based access

Webex application behavior is built from the ground up around five roles, each of which is granted different privileges. They are described below.

Host

The host schedules and starts a Webex meeting. The host controls the meeting experience for everyone and makes relevant decisions while scheduling the meeting and during it.

The site administrator (a role described later) can mandate many of these controls. If they are not mandated, then the host can make choices on how to secure meetings.

Cohost (in Webex Meetings and Webex Webinars only)

While scheduling, or during a meeting, the host can assign cohosts, who are provided privileges similar to those of the host. Cohosts can help to improve meeting productivity. If the host is running late or can't attend, a cohost can start and manage the meeting. Cohosts can also assist the host with meeting management, which is useful for larger meetings.

Presenter

A presenter can share presentations, specific applications, or an entire desktop. The presenter controls the annotation tools. From a security standpoint, the presenter can grant and revoke remote control over the shared applications and desktop to individual attendees.

Panelist (in Webex Training and Webex Webinars only)

A panelist is primarily responsible for helping the host and presenter keep the event running smoothly. Panelists can be assigned during scheduling or promoted by host from attendees list during the event. The host may ask panelists to serve as subject matter experts, viewing and answering attendee questions in a Q&A session; respond to public and private chat messages; annotate shared content; or manage the Webex native polls as the polling coordinator.

Attendee

Attendees have no security responsibilities or privileges unless they are assigned the presenter or host role.

Ultimately, the site administrator and the host can allow an attendee to grab the Webex ball (presenter role) anytime in the course of the meeting. This setting is off by default.

Interpreter (In Webex Meetings and Webex Webinars only)

An interpreter is responsible for translating the language that is spoken by the speaker into an interpreted language assigned by the host in a separate audio channel for the Simultaneous Interpretation feature. Host can assign interpreters during scheduling or inside the meetings.

Site administrator

This role is authorized for managing accounts as well as for managing and enforcing policies on a site basis or per-user basis. The administrator can choose the Webex capabilities that are available to all other roles and users.

Single Sign-On

Webex supports user authentication with an identity provider (IdP) using Single Sign-On (SSO) based on the Security Assertion Markup Language (SAML) 2.0 protocol. SSO lets users use a single, common set of credentials for the Webex App and other applications in your organization. The Webex App uses the Webex service to communicate with the Webex Identity Service. The Webex Identity Service creates an agreement with the IdP, allowing the Webex App to authenticate with the IdP. Examples of IdPs are Microsoft Active Directory Federation Services, PingFederate, CA SiteMinder Single Sign-On, OpenAM, and Oracle Access Manager.

To enable SSO, a certificate has to be generated for your organization. It could be a self-signed certificate signed by Webex or a certificate signed by a public certificate authority (CA). Then metadata have to be exchanged between the IdP and Webex.

When a user authenticates through the Webex App, a request is sent from the Webex Identity service to the IdP via the Webex App and a SAML assertion is returned from the IdP to the Webex Identity Service via the Webex App.

Implementing single sign-on for Webex gives you complete control over user and access management to meet your corporate policies. Some benefits of using SSO with your IdP:

- The IdP is the authority for validating user credentials (which can be a certificate, fingerprint, or other)
- Webex does not store any user credentials
- Customers control who accesses the Webex service

For more information, refer to this Webex help article on Single Sign-on integration in Control Hub.

For users residing in the directory, Webex can synchronize users from a supported directory using Directory Connector with Active Directory or the System for Cross-domain Identity Management (SCIM) API with Azure AD or Okta to the Webex Identity. This ensures users are always in sync between the directory and the Webex organization. Whenever a user is created, updated, or removed in the directory, the changes will be synchronized and reflected in Control Hub.

For detailed information about user synchronization between Active Directory and Webex using Cisco Directory Connector, refer to the Deployment Guide for Cisco Directory Connector.

For detailed information about user synchronization between Azure AD and Webex using the SCIM API, refer to the help article Synchronize Azure Active Directory Users into Control Hub.

For detailed information about user synchronization between Okta and Webex using the SCIM API, refer to the help article Synchronize Okta Users into Cisco Webex Control Hub.

Meeting settings

The granular settings for Webex Meetings can be used to manage the behavior of users and system before, during, and after meetings. Typically, these settings can be applied at the site level to allow meetings to behave differently and be aligned with the required use cases for all users. The Webex administrator, he should ensure all meetings are secure and accessible only by the intended users and devices. Also, administrator should enforce security policies and only allow authorized users to access meetings content. For best practices for administrator to secure meetings, refer to the help articles, Webex Best Practices for Secure Meetings: Site Administration and Webex Best Practices for Secure Meetings: Control Hub.

Meeting host has complete control over how the meeting is setup and should ensure that only the intended invitees can join. Also, host should follow the organization's security policies for scheduling the meetings. To learn how to keep Webex Meetings secure as a host, refer to the help article Webex Best Practice for Secure Meetings: Hosts.

Depending on the security policies, some organizations might completely block their users from joining any external meetings or only allow their users to join meetings from a list of approved external sites. In addition, organization might restrict their users in using certain in-meeting features such as chat, file transfers, annotations, Q&A and polling when joining an external meeting. Collaboration restrictions from Webex can provide these functions. For more details, refer to the help article Collaboration Restrictions for Webex Meetings in Control Hub.

Additional Webex features and security

Users have the flexibility to use various clients and devices to join or start a Webex meeting. When using a video device to join or start a meeting, meeting participants can use Webex device (Cisco Unified CM registered (SIP), or Webex Cloud registered (HTTP) devices), or any third-party standards- based (SIP or H.323) video device or application by dialing the meeting video address. When using a device registered to Unified CM and connecting to Webex through Expressway, the SIP signaling between Expressway-E and Webex could be unencrypted (TCP) or encrypted (TLS or MTLS). Encrypted SIP signaling with MTLS is preferred as the certificates exchanged between the Webex Cloud and Expressway-E can be validated before proceeding with the connection. With SIP/TLS, the Webex Cloud media stream is encrypted using SRTP.

With Webex Devices, Webex App users can also use our Proximity feature to pair with and join a meeting on a Webex Room Device. For more details, click here.

Additionally, a site can be configured to require numeric passcode (audio PIN) for joining meetings using a video device.

Users can also join a Microsoft Teams meeting from a Webex device. Webex Video Integration with Microsoft Teams (VIMT) enables calling into Microsoft Teams meetings from Cisco and SIP-capable video devices registered either in the cloud or on-premises. This integration provides rich, seamless meeting experience, without requiring third party interop. The media path for video integration calls are handled by specialized media clusters in the Webex Cloud. For more information on Webex Video Integration with Microsoft Teams (VIMT), refer to this article.

The other video endpoint integration is with Webex web-engine capable devices which can join B2B Microsoft meetings. This can be used for example in the event an external organization does not have VIMT. With this integration, the signaling and media are sent over WebRTC streams.

Similarly, users can also join a Google Meet meeting from a Webex device. Webex integration with Google Meet enables calling into Google Meet from Webex devices with media and signaling going directly from Google's cloud to the Webex device and leveraging WebRTC technology. Vice-versa, Google Meet devices can join Webex Meetings with the familiar Google Meet UI and call controls and Webex Meeting experience.

Audio plans for Webex Meetings

Webex has integrated calling plans from premises based systems leveraging customers' existing calling solutions, to approved Cloud Connected Calling Providers (CCPP), as well as Cloud Connected Audio Service Provider (CCA-SP), BYoPSTN and Cisco PSTN.

Cisco PSTN provides the broadest global Public Switched Telephone Network (PSTN) dial-in and call-me services to attendees in Webex Meetings, Webinars, and Trainings. Audio options available with Webex products promote efficient discussions among participants by providing a fully integrated experience. As a cloud-based PSTN audio option, Webex Meetings Audio provides a broad coverage footprint with toll dial-in, toll-free dial-in, and call-me capabilities for local and global connections. It operates on a wide variety of devices, including cell phones, IP phones, and softphones, and supports the ability to enable telephony attendees as well as attendees and devices that use Voice over IP (VoIP) to all collaborate in the same session. Cisco PSTN is available wherever Webex is sold.

Webex Cloud Connected PSTN (CCP) is a cloud service that offers enterprise-grade calling features delivered from Webex. This platform is part of the complete Webex Suite that serves the calling, messaging, meeting, and contact center workloads needed by the 100+ user market segment. Webex supports a “Bring Your Own Carrier” model, allowing customers to use any carrier of their choice for PSTN service by deploying a local gateway. With CCP, customers may use an authorized CCP Provider for their PSTN access. Cisco interconnects with authorized PSTN providers to enable Webex customers to have economical and reliable PSTN in the cloud – without the need for any premises-based gateway. Cloud Connected PSTN providers have designed a set of all-inclusive service packages to connect your Webex users to the world with quality and security. Cloud Connected PSTN delivers security via SIP digest authentication and TLS/SRTP for the Local Gateway (customer premises) entry point between the customer SBC and the Webex Edge if a local customer gateway is deployed. For customers using only Cloud Calling components of Webex Cloud Connected PSTN, security is between the Webex App and devices directly to the Webex Cloud as described in the ‘Webex Security’ section.

Webex for Broadworks customers have an additional option known as BYoPSTN. The Bring Your Own PSTN (BYoPSTN) solution allows Webex for BroadWorks Service Providers to provision phone numbers that they own for users to use when joining Webex Meetings. The solution lets Partners leverage their own PSTN networks and make use of existing relationships with PSTN providers, rather than using Cisco-provided numbers.

The reference architecture provides an end-to-end design for the BYoPSTN option. This architecture is validated by Cisco and uses Cisco Unified Border Element (CUBE) as the Session Border Controller (SBC) for call traffic between BroadWorks and Webex Meetings. View the BYoPSTN Solution Guide for more information.

Calls routed from BroadWorks to CUBE within the partner infrastructure will use SIP TCP for call signaling and RTP for media. From CUBE to Webex, calls use SIP MTLS for signaling and SRTP for media. Call routing from CUBE to Webex is via the Internet and does not use a SIP Trunk. BYoPSTN leverages Webex Edge Audio architecture which incorporates authentication for SBC and encryption of all audio media which is carried over SRTP.

Cloud Connected Audio (CCA) connectivity is established through point-to-point private connections to Webex. CCA circuits are terminated on dedicated customer ports. Access control lists on edge routers and firewalls in both the customer's and Cisco's data centers secure the circuits. CCA Service has segmented IP subnets, and only the Cisco Unified Border Element (CUBE) IP segment is advertised to customers. No customer has any visibility into another customer's IP or CUBE.

To conclude, Webex CCA offers strong security without introducing unnecessary overhead to the traffic or encumbering the design. For more information, visit Webex CCA.

Webex privacy

Webex takes customer data protection seriously. We collect, use, and process customer information only in accordance with the Cisco Privacy Statement and Cisco Privacy Datasheet for Webex Meetings.

The Service 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), 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).

Administrative data

Information about employees or representatives of a customer or other third party that is collected and used by Cisco in order to administer or manage Cisco's delivery of products or services, or to administer or manage the customer's or third party's account for Cisco's own business purposes.

Administrative data may include the name, address, phone number, email address, and information about the contractual commitments between Cisco and a third party, whether collected at the time of the initial registration or later in connection with the management or administration of Cisco's products or services.

Administrative data may also include the meeting title, time, and other attributes of the meetings conducted on Webex by employees or representatives of a customer. Other examples of administrative data may include meeting title, meeting time, and other attributes of the meetings hosted on Webex.

Customer data

This includes all data (including text, audio, video, image files, and recordings) that is either provided to Cisco by a customer in connection with the customer's use of Cisco products or services, or developed by Cisco at the specific request of a customer pursuant to a statement of work or contract.

Customer data also includes log, configuration, or firmware files, and core dumps.

It is data taken from a product or service and provided to Cisco to help us troubleshoot an issue in connection with a support request. Customer data does not include administrative data, support data, or telemetry data.

Support data

Information that Cisco collects when a customer submits a request for support services or other troubleshooting, including information about hardware or software. It includes details related to the support incident, such as authentication information, information about the condition of the product, system, and registry data about software installations and hardware configurations, and error-tracking files. Support data does not include log, configuration, or firmware files, or core dumps taken from a product and provided to us to help us troubleshoot an issue in connection with a support request, all of which are examples of customer data.

Telemetry data

Information generated by instrumentation and logging systems created through the use and operation of the product or service.

All data collected in the Webex Cloud is protected by several layers of robust security technologies and processes. Below are examples of controls placed in different layers of Webex operations to protect customer data:

- **Physical access control:** Physical access is controlled through biometrics, badges, and video surveillance. Access to the data center requires approvals and is managed through an electronic ticketing system.
- **Network access control:** The Webex network perimeter is protected by firewalls. Any network traffic entering or leaving the Webex data center is continuously monitored using an Intrusion Detection System (IDS). The Webex network is also segmented into separate security zones. Traffic between the zones is controlled by firewalls and Access Control Lists (ACLs).
- **Infrastructure monitoring and management controls:** Every component of infrastructure, including network devices, application servers, and databases, is hardened to stringent guidelines. They are also subject to regular scans to identify and address any security concerns.
- **Cryptographic controls:** As noted earlier, all data to and from the Webex data center to cloud registered Webex Apps and Webex Devices is encrypted, except for PSTN traffic and unencrypted SIP/H323 video devices in a cloud-enabled meeting. Additionally, critical data stored in Webex, such as passwords, is encrypted.

Cisco employees do not access customer data unless access is requested by the customer for support reasons. Access to systems in this case is allowed by the manager only in accordance with the “segregation of duties” principle. It is granted only on a need-to-know basis and with only the level of access required to do the job. Employee access to these systems is also regularly reviewed for compliance. Employees with such access are required to take annual International Organization for Standardization (ISO) 27001 Information Security Awareness training.

In addition to these specialized controls, every Cisco employee undergoes a background check, signs a Nondisclosure Agreement (NDA), and completes Code of Business Conduct (COBC) training.

Health Insurance Portability and Accountability Act (HIPAA)

Cisco can provide information regarding the functionality, technology, and security of Webex. A HIPAA-covered entity would need to consult with its own legal counsel to determine whether Webex's functionality is compliant for its business processes and GDPR ready.

- GDPR Compliance
- Webex Meetings privacy sheet

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 is:

- ISO 27001, 27017, 27018 and 27701 certified
- Service Organization Controls (SOC) 2 Type II audited
- SOC 3 certified
- Cloud Code of Conduct
- CSTAR
- Cloud Computing Compliance Controls Catalogue (C5) attestation
- FedRAMP certified (visit cisco.com/go/fedramp for more details, scope, and availability)

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

Conclusion

Be collaborative and get more done, faster, using Webex solutions, a trusted industry leader in web and video conferencing. 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. We connect everything more securely to make anything possible.

How to buy

To view buying options and speak with a Cisco sales representative, visit cisco.com/c/en/us/buy.

For more information
Webex Meetings | Webex Events | Webex Training
Webex Support | Cloud Connected Audio

February 2022