The bridge to possible

White paper
Cisco public

Cisco Webex Meetings Security

Contents

How to Buy

Introduction

Cisco 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.

Note: The terms “Webex Meetings” and “Webex Meetings sessions” refer to the integrated audio conferencing, Internet voice conferencing, and video conferencing used in all Webex Meetings online products. Unless otherwise specified, the security features we describe pertain equally to all the Webex Meetings applications listed in this paper.

What you will learn

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

Webex Meetings applications include:

- Webex Meetings
- Webex Events
- Webex Training
- Webex Support (including Webex Remote Access)
- Webex Edge
- Webex Cloud Connected Audio

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.

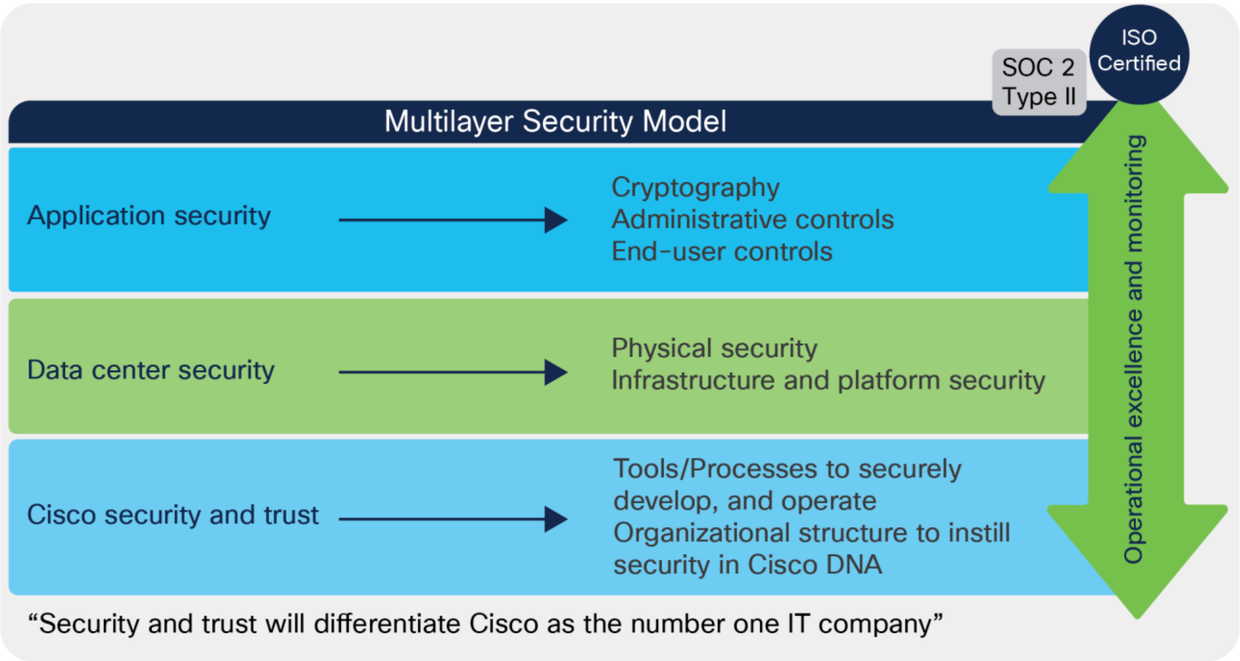
SOC 2 Type II
ISO Certified
Multilayer Security Model
Application security
Cryptography
Administrative controls
End-user controls
Data center security
Physical security
Infrastructure and platform security
Cisco security and trust
Tools/Processes to securely develop, and operate
Organizational structure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

Figure 1.
Cisco Security Model

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 at cisco.com/go/psirt.

Security responsibility

Although every person in Cisco's 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 data center within the Webex Cloud. 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 and firewalls. 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 of the Webex Cloud. 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 at run time

All communications between cloud registered Webex apps, Webex Room devices and the Webex Cloud occur over encrypted channels. Webex uses TLS 1.2 protocol 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.[1]

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 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 128 or AES 256 based ciphers. Webex video devices and 3rd party video devices that support media encryption with SRTP use AES-CM-128-HMAC-SHA1. The Webex app uses AES-256-GCM to encrypt media. Media encryption keys are exchanged over TLS-secured signaling channels.

[1] 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.

End-to-end encryption

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.

However, for businesses requiring a higher level of security, Webex also provides end-to-end encryption. With this option, the Webex Cloud does not have access to the encryption keys used by meeting participants and cannot decrypt their media streams.

With end-to-end encryption, the meeting encryption key is generated by the meeting host and securely distributed to all other participants in the meeting. To secure the meeting encryption key prior to transmitting it via the Webex cloud to each meeting participant, the key is encrypted by the meeting host.

To achieve this, each participant's Webex app generates 2048-bit RSA public and private key pair and sends the public key to the host's Webex app. The host's app encrypts the meeting key using the participant's public key and returns the encrypted meeting encryption key back to the participant's app. The Webex app can then decrypt the meeting key using its RSA private key.

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

This end-to-end encryption option is available for Webex Meetings and Webex Support services. Note that when end-to-end encryption is enabled, the following features are not supported:

- Personal Room meetings
- Join Before Host
- Move to Lobby
- Video-device enabled meetings
- Breakout sessions
- Webex Meetings Web App
- Linux clients
- Network-Based Recording (NBR)
- Webex Assistant
- Remote computer sharing
- Saving session data transcripts, Meeting Notes
- PSTN Call-in/Call-back[2]

[2] When end-to-end encryption is enabled, if the Pro-E2E-Unencrypted Audio session type is used, only Webex apps use end-to-end encryption; media from PSTN users is not end-to-end encrypted.

Different ciphers

Webex services support TLS cipher suites in the following preference order for secured communications. Table 1 outlines the typical cipher suites and cipher suite preference order used by Webex Services.

Table 1. Cipher suites and bit lengths

Cipher suites	Bit length
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	256
TLS_RSA_WITH_AES_128_GCM_SHA256	128
TLS_RSA_WITH_AES_256_GCM_SHA384	256
TLS_RSA_WITH_AES_128_CBC_SHA256	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	256
TLS_RSA_WITH_AES_128_CBC_SHA	128
TLS_RSA_WITH_AES_256_CBC_SHA	256

Protecting data at rest

When configured by the customer to do so, Webex Meetings stores meeting and user data that may be critical to your business. Webex Meetings uses the following safeguards to protect data at rest:

- Stores all user passwords using SHA-2 (one-way hashing algorithm) and salts
- Encrypts other passwords such as for meetings or recordings
- Encrypts stored Network Based Recordings. Webex recordings are encrypted both at the file level and at the logical volume level. The file encryption uses AES-256-GCM. This file encryption key is then encrypted with a 256-bit master key based that is rotated based on policy and saved to a Key Management Server (KMS). During the playback and download flow, the encrypted recording file is decrypted before or during the operation. Cisco maintains these keys for the customer.

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

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 Training and Events only)

A panelist is primarily responsible for helping the host and presenter keep the event running smoothly. Any number of attendees can be panelists. 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 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.

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.

Administrative capabilities

Webex has granular site administration capabilities to effectively align your Webex site with your business needs. This section describes the main administrative security-related features.

Account management

You can integrate your identity management technology with Webex to allow Single Sign-On (SSO) with your IdP, and giving you full control over account management and access policies. When your accounts are kept in Webex, a number of site administration capabilities allow you to manage accounts according to your needs.

The site administrator can carry out the following actions:

- Lock out an account after a configurable number of failed login attempts
- Automatically unlock a locked-out account after a specified time interval
- Deactivate accounts after a defined period of inactivity
- Require a user to change the password at the next login
- Lock or unlock a user account
- Activate or deactivate a user account
- Require security text on new account requests
- Require email confirmation of new accounts
- Allow self-registration (sign-up) for new accounts
- Configure rules for self-registration of new accounts
- Set a security option to automatically end a meeting if there is only one participant present
- Display caller ID for dial-in users when available
- Allow hosts to upload a personal avatar
- Allow hosts to add custom virtual backgrounds
- Allow participants to share in meetings (meetings only)
- Allow attendees to join before hosts (off by default)
- Allow attendees to join audio before hosts (off by default)
- Un-list meetings (off by default)
- Require confirmation for the user to update email address

Administrators of Webex sites that are not using SSO and are not on Webex Control Hub can manage password criteria settings using the settings' following options:

- Mixed case
- Minimum length
- Minimum number of numeric, alphabetic, or special characters
- No character to be repeated three times or more
- No reuse of a specified number of previous passwords
- No dynamic text (site name, host's name, username)

- No passwords from a configurable list (for example, “password”)
- Minimum time interval before password change
- Change of account password by the host at a configurable time interval
- Change of account password by all users at the next login
- Download a site configuration audit log that shows configuration changes made to “Options under Common Site Settings”
- Require authentication to retrieve a host key from a site for scheduled meetings
- Disable the ability for hosts to upload a personal
- Do not allow a character to be repeated 3 times or more
- Allow user’s account password to be saved in cookies

Meeting settings

The granular settings for Webex Meetings can be used to manage the behavior of users and system before, during, and after meetings. In most cases these settings can be applied at the site level to allow Webex Meetings, Webex Events, and Webex Training to behave differently and be aligned with required use cases for all users. In addition, many in-meeting features such as file transfer, desktop sharing, and recording can be enabled or disabled for a group of users using customized session types.

Webex Meetings settings can:

- Allow users to store their names and email addresses to easily host and join future meetings
- Allow hosts to appoint a cohost
- Allow hosts to let other hosts schedule on their behalf
- Allow hosts to reassign recordings to other hosts
- Require authentication for all hosts and attendees to access the site
- Hide all meetings that are currently publicly listed
- Mandate a password for all meetings
- Enforce a meeting password when joining by phone
- Enforce numeric passwords for video attendees
- Enforce a disclaimer to any attendee (including a host) joining a meeting
- Allow attendees to join before the host
- Control how guest users join an unlocked meeting (e.g., guests can join, must wait in the lobby, or cannot join the meeting)
- Enable lobby for audio-only users
- Automatically end meetings after a configurable time period if there is only one participant left
- Restrict viewing of recordings to signed-in users
- Prevent the download of recordings
- Enforce passwords for all network-based recordings

- Enforce a disclaimer to any attendee prior to viewing or downloading a recording
- Require administrator approval of a “Forgot Password” renewal request
- Enable content sharing with external integrations such as Dropbox and Box
- Enforce strong passwords for remote access service
- Prevent AI robots from joining Webex meetings

For most of these settings, the site administrator can choose to leave a setting at a lower security level for the entire site. Hosts can then make security decisions for specific meetings based on their needs.

For example, the site administrator may not require users to sign in to join meetings, but individual hosts can choose to secure specific meetings by allowing only signed-in attendees.

Personal Room security settings

Every Webex Meetings host can be given a dedicated URL for a Personal Room that can be used for meetings. The Personal Room URL is structured as follows: https://sitename.webex.com/meet/username. The host or the Webex administrator can change the username. Collaboration becomes much easier with Personal Rooms because attendees don’t have to look for emails or calendars to join a meeting. The Personal Room can be thought of as a personalized virtual room that is active when the host is present.

When it comes to securing the Personal Room, the Webex administrator can:

- Automatically lock the Personal Room
- Require attendees to authenticate prior to entering the host’s Personal Room (Webex apps and video endpoints)
- Apply policies for placing authenticated attendees and guests into the lobby, based on whether the meeting is locked or unlocked
- Allow or disallow attendees to notify the host when they are in the lobby
- Set lobby timeout values (maximum wait time)
- Enforce the host PIN length (to be used to enter the Personal Room from a video endpoint)

As a Personal Room host, you can:

- Manually lock your personal meeting room, or configure your room to automatically lock after a specified duration
- Apply policies for placing authenticated attendees and guests into the lobby, based on whether the meeting is locked or unlocked. For example, similar to real-world meeting rooms, where authorized employees can just walk into any room, but unauthorized visitors have to be escorted
- Allow host to start Personal Rooms from phone
- Allow (i) users with a host account on the Webex site, or (ii) participants joining from an authenticated Cisco video device - to host their Personal Room meetings
- Allow cohosts for your Personal Room
- Allow attendees to unmute themselves
- Mute attendees when they join the meeting
- Send an email notification when someone enters your Personal Room lobby while you are away

Single Sign-On

Webex supports user authentication with Single Sign-On (SSO) using the Security Assertion Markup Language (SAML) 2.0 protocol.

To enable SSO, the site administrator needs to upload a X.509 certificate to the Webex site.

And then generate SAML assertions containing user attributes and digitally sign these assertions with the private key of the X.509 certificate. Webex validates the SAML signature against the public key in the preloaded certificate before authenticating the user.

SAML assertions are exchanged between the Webex site and the customer's Identity Provider (IdP) for example, Microsoft Active Directory Federation Services, PingFederate, CA Siteminder Single Sign-On, OpenAM, or Oracle Access Manager). The Webex site acts as the service provider. Webex supports both service-provider-initiated and IdP-initiated SSO flows.

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)
- Customers can implement two-factor authentication for users centrally rather than have each SaaS-based service use a different solution
- Webex does not store any user credentials
- Customers control who accesses the Webex service
- Onboarding and off-boarding of users as they join or leave the corporate IdP is transparent

Additional Webex features and security

Join meetings with video devices

Users can join or start a Webex meeting with a video device. Meeting participants can use Webex Room devices (Cisco UCM registered (SIP), or Webex cloud registered (HTTP) devices), or any third-party standards-based video device or application to join meetings by dialing the meeting video address. With Webex Room devices, Webex app users can also use our Proximity feature to pair with and join a meeting on a Webex Room device.

There is no additional video bridging equipment is required on the customer premises for video devices to work. The video-bridging capabilities are deployed in the same highly secure Webex Cloud as Webex Meetings and use the same industry-grade security controls (physical, network, infrastructure, and administrative). Video endpoints can join meetings over Session Initiation Protocol (SIP) and H.323 for signaling and Real-Time Transport Protocol/Secure Real-Time Protocol (RTP/SRTP) media. Webex Meetings supports TLS transport for SIP and SRTP for media. When video endpoints join a meeting over SIP/TLS, the Webex cloud media stream is encrypted using SRTP.

H.235 is used to secure H.323 connections.

Additionally, a site can be configured to require passcodes for joining meetings using a video device.

Cloud Connected Audio

Webex Cloud Connected Audio (CCA) is an end-to-end audio solution that uses your on-premises IP telephony network to provide an integrated audio experience for your Webex meetings. Webex CCA implements a Session Initiation Protocol (SIP) trunk from your premises into the Webex data center instead of using a traditional PSTN connection. This solution provides the same integrated and intuitive user experience as all other Webex audio options. However, by directly using your IP telephony network, Webex CCA can provide more attractive audio pricing.

CCA is a fully encapsulated environment. Reaching it from the Internet or perpetrating any kind of an attack is extremely difficult. Although the infrastructure is shared, there is no inter-tenant routing, so malicious traffic from other tenants is blocked. Furthermore, traffic over the trunk is limited to routing protocols and User Datagram Protocol (UDP) packets to desired Webex infrastructure ports. The Webex infrastructure is configured to receive traffic from preconfigured dial peers only.

CCA connectivity is established through point-to-point private connections to the Webex platform. 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.

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 Webex Terms of Service provides additional information.

Webex will, pursuant to appropriate lawful transfer mechanisms, transfer the administrative data, support data, and telemetry data from the EU to United States (and where appropriate, to other permissible locations). The definitions of these categories of data are provided below.

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 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 Room 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 Ethics (COBE) 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 readiness
- 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 and 27018 certified
- Service Organization Controls (SOC) 2 Type II audited
- SOC 3 certified
- 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 https://www.cisco.com/c/en/us/buy.

For more information

To learn more about Webex solutions, visit our site:

- Cisco Webex Meetings
- Cisco Webex Events
- Cisco Webex Training
- Cisco Webex Support
- Cisco Webex Cloud Connected Audio

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-737588-04 02/21