Cisco Webex Meetings Security

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 Cisco® 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 Cisco 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 Cisco Webex Meetings and its underlying infrastructure to help you with an important part of your investment decision.

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

What you will learn

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

Cisco Webex Meetings applications include:

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

Contents

Cisco Webex Security Model

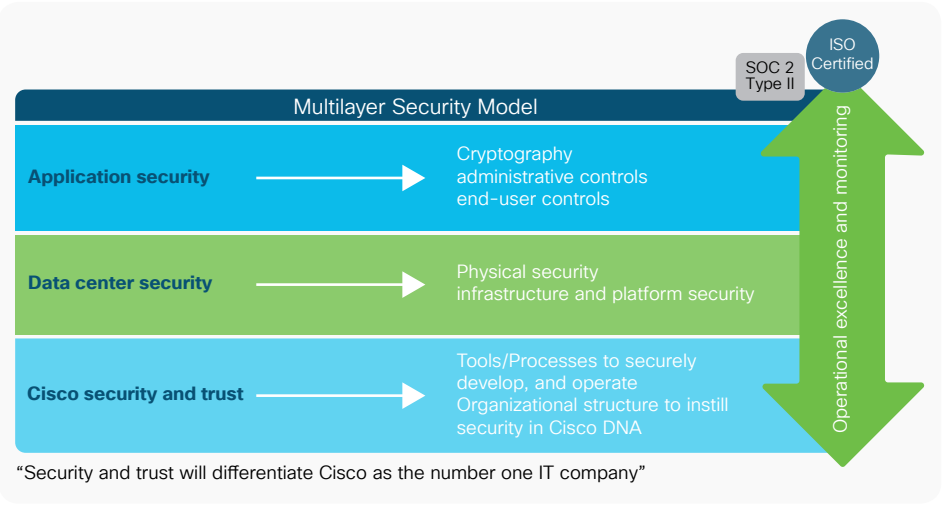
Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout our company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet 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 Cisco Webex security model (Figure 1) is built on the same security foundation deeply engraved in Cisco's processes.

The Cisco Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Cisco Webex services. We will be discussing some of these elements in this document.

Figure 1. Cisco Security Model



"Security and trust will differentiate Cisco as the number one IT company"

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 Cisco Webex Product Development team passionately follows this lifecycle in every aspect of product development.

Read more about the Secure Development Lifecyle.

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

Additionally, Cisco InfoSec Cloud works with other teams across Cisco to respond to any security threats to Cisco Webex.

Cisco InfoSec is also responsible for continuous improvement in Cisco 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 the Cisco 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 Cisco 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 Cisco Webex engineering staff to explain findings and validate the remediation. As needed, Cisco InfoSec can provide a letter of attestation from these vendors.

Cisco Webex Data Center Security

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

Cisco Webex meeting sessions use switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the world. Cisco operates the entire infrastructure within the Cisco Webex Cloud with industry-standard enterprise security.

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 (for example, temperature sensors and fire-suppression systems) and service continuity infrastructure (for example, power backup) help ensure that systems run without interruption.

Within the data centers are also “trust zones,” or segmented access to equipment based on infrastructure sensitivity. For example, databases are “caged”: the network infrastructure has dedicated rooms and 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 Cisco 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.

All systems undergo a thorough security review and acceptance validation prior to production deployment. 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 logged and monitored on a

continuous basis. Daily internal and external security scans are conducted of Cisco Webex Cloud. All systems are hardened and patched as part of the regular maintenance. Additionally, vulnerability scanning and assessments are performed continuously.

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

Cisco Webex Application Security

Cryptography

Encryption at run time

All communications between Cisco Webex applications and Cisco Webex Cloud occur over encrypted channels. Cisco Webex uses TLS 1.2 protocol and uses high-strength ciphers (for example, AES 256).[1]

After a session is established over TLS, all media streams (audio VoIP, video, screen share, and document share) are encrypted.[2]

User Datagram Protocol (UDP) is the preferred protocol for transmitting media. In UDP, media packets are encrypted using AES 128. The initial key exchange happens on a TLS-secured channel. Additionally, each datagram uses Hashed- Based Message Authentication Code (HMAC) for authentication and integrity.

End-to-end encryption

Media streams flowing from a client to Cisco Webex servers are decrypted after they cross the Cisco Webex firewalls. Cisco can then provide network- based recordings, and all media streams can be recorded for future reference. Cisco Webex then re-encrypts the media stream before sending it to other clients. However, for businesses requiring a higher level of security, Cisco Webex also provides end-to-end encryption. With this option, Cisco Webex Cloud does not decrypt the media streams. As it does for normal communications, it establishes a TLS channel for client-server communication.

Additionally, all Cisco Webex clients generate key pairs and send the public key to the host's client. The host generates a random symmetric key using a Cryptographically Strong Secure Pseudo-Random Number Generator (CSPRNG), encrypts it using the public key that the client sends, and sends the encrypted symmetric key back to the client.

The traffic generated by clients is encrypted using the symmetric session key. In this model traffic cannot be deciphered by the Cisco Webex server.

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

- Web App
- Network-based recordings
- Join Before Host
- Video Endpoints

Different ciphers

Cisco Webex supports following cipher suites for secured communications. Cisco Webex will allow the strongest possible cipher for the customer's environment. Table 1 outlines cipher suites and each suite's bit length.

[1] Actual encryption protocol and strength depend on the OS and browser settings, based on which a host negotiates connections with Cisco Webex.

[2] Users connecting to a cloud meeting using a third-party video endpoint may be sending and receiving unencrypted media streams. Configuring your firewall to prevent unencrypted traffic to and from Cisco Webex helps keep your meetings safe. However, allowing attendees outside your firewall to join your meeting using third-party devices can still send your meeting data unencrypted on the Internet.

Table 1. Cipher suites and bit lengths

Cipher suites	Bit length
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	128
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	128

Protecting data at rest

When configured by the customer to do so, Cisco Webex Meetings stores meeting and user data that may be critical to your business. Cisco 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 key is a 256-bit block AES GCM key. This file key is then encrypted with a master key based on AES HmacSHA256 that is rotated based on policy and saved to a DB. During the playback and download flow, the encrypted recording file is then decrypted before or during the operation. Cisco maintains these keys for the customer.

Cisco Webex Role-Based access

Cisco 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 Cisco 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.

Alternate host

While scheduling, the host can assign alternate hosts, who can start the meeting in lieu of the host and essentially have the same set of privileges as the host.

A host can also pass on his or her privileges to another user during the meeting. With respect to security, there is no difference between the host and alternate host.

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 and 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 Cisco 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 Cisco Webex capabilities that are available to all other roles and users.

Administrative capabilities

Cisco Webex has granular site administration capabilities to effectively align your Cisco Webex site with your business needs. This section describes the main security-related features. For further information on all security features, please refer to the Cisco Webex site administration guide here.

Account management

You can integrate your identity management technology with Cisco Webex to allow single sign-on and give you full control over account management and access policies. When your accounts are kept in Cisco Webex, a number of site administration capabilities allow you to manage accounts according to your needs.

- SSO support for SHA-2 SSL certificates

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

Additionally, the administrator can manage password criteria using the 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 avatar

Meeting settings

The granular settings for 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 center level to allow Cisco Webex Meetings, Cisco Webex Events, and Cisco 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.

Meeting settings can:

- Allow users to store their names and email addresses to easily host and join future meetings
- Allow hosts to reassign recordings to other hosts
- Require authentication for all hosts and attendees to access the site
- Apply strong password rules to remote access service
- Hide all meetings that are currently publicly listed
- Mandate a password for all meetings
- Require administrator approval of a "Forgot Password?" request
- Allow hosts to let other hosts schedule on their behalf
- Allow a host to appoint an alternate host when scheduling
- Enable content sharing with external integrations such as Dropbox and Box (when presenting from an iPad)
- Automatically end meetings in a configurable time if there is only one participant left; applies for scheduled meetings, Personal Room meetings, and audio-only meetings
- Enforce a meeting password when joining by phone or video conferencing system
- Enforce a disclaimer to any attendee (including a host) joining a meeting
- Enforce a disclaimer to any attendee prior to viewing or downloading a recording
- Allow attendees to join before the host
- Allow attendees to join telephony before the host
- Restrict the viewing of recordings to signed-in users
- Prevent the download of recordings
- Enforce passwords for all network-based recordings

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

Personal Room security settings

Every Cisco Webex 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 Cisco 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 where a host is available.

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

- Require attendees authenticate prior to entering the host's Personal Room (Webex Meeting clients and video endpoints)
- Allow or not allow attendees to notify the host when they are in the lobby (a waiting area)
- Lobby available for Webex Meeting clients and video endpoints
- Enforce the host PIN length (to be used to enter the Personal Room from a video endpoint)
- Enforce unauthenticated attendees to be blocked in lobby even in a room, until admitted by hosts

As a Personal Room host, you can:

- Manually lock your room
- Configure your room to automatically lock after a specified duration (applies to Personal Rooms that are started on the Webex Meetings client and video endpoints)
- Require that meeting participants who join a Personal Room that is locked be placed in the lobby and the host will have the ability to manually admit them into the meeting
- Place configured authenticated attendees in the lobby, even when your room is open and require you to manually admit them. This is similar to real-world meeting rooms, where authorized employees can just walk into any room but unauthorized visitors have to be escorted

- Enable an email notification to be sent to you in the event someone enters your Personal Room lobby while you are away

Single Sign-On

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

The site administrator will have to upload a public key X.509 certificate to the customized Cisco Webex site.

You can then generate SAML assertions containing user attributes and digitally sign the assertions with the matching private key. Cisco Webex validates the SAML signature against the preloaded public key certificate before authenticating the user.

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

Implementing single sign-on on Cisco Webex gives you complete control over user and access management to meet your corporate policies. Some benefits:

- 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
- Cisco Webex does not store any user credentials
- Customers control who accesses Cisco Webex
- Onboarding and off-boarding users as they join or leave the corporate IdP is transparent

Additional Cisco Webex features and security

Join meetings with video devices

Users can join or start a Cisco Webex Meeting with a video device. This capability can be optionally made available on a Cisco Webex Meetings site. Once turned on, a user can use a Cisco TelePresence® endpoint, a soft client, a Skype for Business client, or any third-party standards-based video device to join meetings by dialing the meeting video address. Experience is amazing with Cisco end points as a user can join a meeting on a device by automatic wireless pairing.

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 Cisco Webex Cloud as the Cisco Webex Meeting Center 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 media stream is encrypted through 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

Cisco 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 Cisco Webex meetings. Cisco Webex CCA implements a Session Initiation Protocol (SIP) trunk from your premises into the Cisco Webex data center instead of using a traditional telephony connection. This solution provides the same integrated and intuitive user experience as all other Cisco Webex audio options. However, by directly using your IP telephony network, Cisco 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 Cisco Webex infrastructure ports. The Cisco Webex infrastructure is configured to receive traffic from preconfigured dial peers only.

CCA connectivity is established through point-to- point private connections to the Cisco 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 Webex 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, Cisco Webex CCA offers strong security without introducing unnecessary overhead to the traffic or encumbering the design.

Cisco Webex privacy

Customer data protection, retention, and compliance
Cisco Webex takes customer data protection seriously. We collect, use, and process customer information only in accordance with the Cisco Privacy Statement. The Cisco Webex Terms of Service provides additional information.

Cisco Webex Meetings is Privacy Shield Framework-certified.

Cisco 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 Cisco 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 Cisco Webex.

Customer data: 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 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 Cisco Webex Cloud is protected by several layers of robust security technologies and processes. Below are examples of controls placed in different layers of Cisco 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 Cisco Webex network perimeter is protected by firewalls. Any network traffic entering or leaving the Cisco Webex data center is continuously monitored using an Intrusion Detection System (IDS). The Cisco 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 Cisco Webex data center to Cisco Webex clients is encrypted, except for unencrypted video devices in a cloud-enabled meeting. Additionally, critical data stored in Cisco 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 Cisco Webex. A HIPAA-covered entity would need to consult with its own legal counsel to determine whether Cisco Webex's functionality is compliant for its business processes and GDPR ready.

- GDPR readiness
- Cisco Webex Meetings privacy sheet

Industry standards and certifications

In addition to complying with our stringent internal standards, Cisco Webex also continually maintains third-party validations to demonstrate our commitment to information security. Cisco Webex is:

- ISO 27001 certified
- Service Organization Controls (SOC) 2 Type II audited
- 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
- Cloud Computing Compliance Controls Catalogue (C5) attestation
- Privacy Shield Framework certified

Conclusion

Be collaborative and get more done, faster, using Cisco Webex solutions, a proven industry leader in web and video conferencing. Cisco 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.

For more information

To learn more about Cisco Webex solutions, visit our site:

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

C11-737588-02 02/19