Web Conferencing: Unleash the Power of Secure Real-Time Collaboration

Introduction

Cisco WebEx online solutions help 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 solutions. These solutions help simplify business processes and improve results for sales, marketing, training, project management, and support teams.

For all of 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 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 and its underlying infrastructure to help you with an important part of your investment decision.

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

What You Will Learn

This paper describes the security features of Cisco WebEx® centers and related services. It discusses the tools, processes, and engineering that help customers confidently collaborate on the Cisco WebEx platform. The paper covers:

- Cisco WebEx Meeting Center
- Cisco WebEx Event Center
- Cisco WebEx Training Center
- Cisco WebEx Support Center (including Cisco WebEx Remote Access)
- Cisco Collaboration Meeting Rooms Cloud
- Cisco WebEx Cloud Connected Audio

Cisco WebEx Security Model

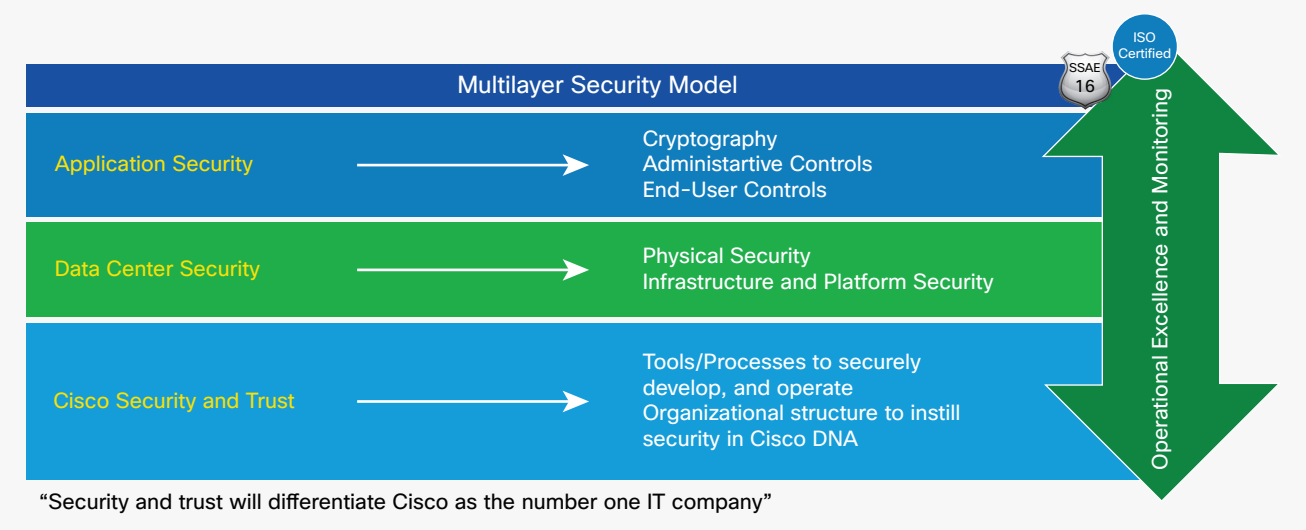
Cisco remains firmly committed to maintaining leadership in cloud security. Cisco’s Security and Trust Organization works with teams throughout our company to build security, trust, and transparency into a framework that supports the design, development, and operation of core infrastructures to meet 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 DNA.

The Cisco WebEx team 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 Secured Development Lifecycle

At Cisco, security is not an afterthought but 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.

Please read more about the Secure Development Lifecycle here.

Cisco Foundational Security Tools

The Cisco Security and Trust Organization provides not only the process but also the necessary tools that give every single 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 such tools are:

- 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 DNA

Cisco has dedicated departments in place to instill and manage security DNA 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 in 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 disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.

To learn more about PSIRT, please visit cisco.com/go/psirt.

Security Responsibility

Although every person in the Cisco WebEx team is responsible for security, the following are the main roles accountable for it:

- 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 team 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 globe. 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 Collaboration 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. There are intrusion detection systems (IDSs) in place, and activities are logged and monitored on continuous basis. There are daily internal and external security scans 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. Cisco data center's 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 supports the TLS 1.0, TLS 1.1, and TLS 1.2 protocols 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.

[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 CMR 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.

End-to-End Encryption (E2E)

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 Meeting Center and Cisco WebEx Support Center. Note that when end-to-end encryption is enabled, the following features are not supported:

- Network-based recordings
- Join Before Host
- Collaboration Meeting Rooms (CMR) Cloud

Different Ciphers

Cisco WebEx supports following cipher suites for secured communications. Cisco WebEx will allow the strongest possible cipher for the customer's environment.

Cipher Suites	Bit Length
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012) ECDH secp256r1 (eq. 3072 bits RSA) FS	112
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS	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) ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS	128

Cipher Suites	Bit Length
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	112

Protecting Data at Rest

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

- Splits the recording and stores the audio, video, and data share streams separately[3]
- Stores all user passwords using SHA-2 (one-way hashing algorithm) and salts
- Encrypts passwords

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 Event Centers 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 Cisco WebEx ball (presenter role) anytime in the course of the meeting. This setting is off by default.

[3] Split storage of recording is applicable only to native recording formats. If your site is configured to use CMR Cloud, then meetings whose attendees join using video endpoints are recorded as MP4. All MP4 recordings are stored as a single stream.

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.

The 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

Additionally, the administrator can manage password criteria using 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
- Ability of hosts to save password in cookies

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 Meeting Center, Cisco WebEx Event Center, and Cisco WebEx Training Center 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
- Unlist all meetings that are currently 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
- 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 (WBS31 and later)

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 follow: https://sitename.webex.com/meet/username, where 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 to have an account to enter the host's Personal Room
- Allow or not allow attendees to notify the host when they are in the lobby (a waiting area)
- Enforce the host PIN length (to be used to enter the Personal Room from a video endpoint)

Additionally, hosts can choose to lock their Personal Rooms as needed.

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 are:

- 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

Collaboration Meeting Rooms

Cisco Collaboration Meeting Rooms (CMR) Cloud is an add-on option to a Cisco WebEx Meeting Center subscription. It provides video conferencing capabilities without the need to buy new equipment. Customers can use a Cisco Telepresence® endpoint, a soft client, a Skype for Business client, or any third-party standards-based video device. CMR Cloud provides simple, highly secure collaboration from the scalable Cisco WebEx Cloud. Customers can use their video-capable endpoints to join CMR Cloud-enabled meetings by dialing the meeting video address. CMR Cloud combines Cisco WebEx conferencing with the video bridging. No additional video bridging equipment is required on customer premises.

The video-bridging capabilities are deployed in the same highly secure Cisco WebEx Cloud as the Cisco WebEx Meeting Center and uses the same industry-grade security controls (physical, network, infrastructure, and administrative). Video endpoints can join CMR Cloud–enabled meetings over Session Initiation Protocol (SIP) and H.323 for signaling and Real-Time Transport Protocol/Secure Real-Time Protocol (RTP/SRTP) media. CMR Cloud supports TLS transport for SIP and SRTP for media. When video endpoints join a CMR-enabled 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 CMR 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 intertenant routing, so malicious traffic from other tenants is blocked. Furthermore, traffic over the trunk is limited to routing protocols and 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 Collaboration Cloud. 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 to 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.

Please note that Cisco WebEx was previously operating under the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework to enable the transfer of EU personal data to the United States for processing. Cisco WebEx continues to adhere to the principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. Following the ruling from European Court of Justice on October 6, 2015, regarding the validity of Safe Harbor as transfer mechanism, Cisco has employed alternative means (that is, standard contractual clauses) to remain compliant with our legal obligations. We may participate in other approved frameworks as they are developed.

Where a customer has provisioned a Cisco WebEx site on a cluster that resides in a European data center, Cisco WebEx will not transfer customer data outside the EU.[4]

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.

[4] This statement applies only to Cisco WebEx Cloud conferencing products for enterprise: that is, Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Event Center, and Cisco WebEx Support Center (including Cisco WebEx remote access). This statement does not apply to Cisco WebEx Meetings, which is an offering for individuals and small businesses sold through www.webex.com. The Cisco WebEx Meetings product does transfer customer data (recordings and files) into the United States (and beyond, where appropriate).

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 CMR 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 an NDA (nondisclosure agreement), and completes COBC (Code of Business Ethics) training.

HIPAA (Health Insurance Portability and Accountability Act)

Passed in 1996, HIPAA is a federal law designed to protect medical records and other personal information.

The U.S. Department of Health and Human Services does not recognize the HIPAA Compliance Certification for products or services. The Cisco WebEx security functionality can support a customer's HIPAA compliance requirements. Compliance with the HIPAA privacy and security rules is a cradle-to-grave process imposed on the covered entity (for example, the customer). It requires the entity to implement the appropriate administrative, physical, and technical safeguards when handling protected health information. HIPAA is not directly applicable to Cisco and other manufacturers of products, software, and services that are used by a covered entity.

To be HIPAA compliant, the covered entity will need to self-certify that it has the appropriate internal policies and practices in place (including people, processes, and technology) to comply with the HIPAA Privacy Rule and Security Rule standards. These practices must cover all areas of data handling and network traffic.

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.

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 U.S government and education customers.

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 Meeting Center: http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/index.html
- Cisco WebEx Event Center: http://www.cisco.com/c/en/us/products/conferencing/webex-event-center/index.html
- Cisco WebEx Training Center: http://www.cisco.com/c/en/us/products/conferencing/webex-training-center/index.html
- Cisco WebEx Support Center: http://www.cisco.com/c/en/us/products/conferencing/webex-support-center/index.html
- Cisco® Collaboration Meeting Rooms Cloud: http://www.cisco.com/c/en/us/products/conferencing/collaboration-meeting-rooms-cmr-cloud/index.html
- Cisco WebEx Cloud Connected Audio: http://www.cisco.com/c/en/us/products/conferencing/webex-cloud-connected-audio/index.html

C11-737588-01 11/16