Cisco Webex Control Hub (Data Security and Privacy)

Contents

Data security and privacy overview

One of the key benefits for enterprises of consuming cloud services is the ability to leverage value-added features and functionality as quickly as the cloud service provider can deploy them. But for many cloud providers, “adding value” often means having full access to user data and content. For collaboration applications, most cloud providers directly access message, call, and meeting content in order to offer features such as message search, content transcoding, and integration with third-party applications. On the other hand, modern consumer collaboration services tend to be geared toward protecting consumer privacy by offering end-to-end encryption at the expense of features that add value.

Cisco Webex® provides the best of both worlds: an end-to-end encrypted cloud collaboration platform that offers enterprises the ability to choose which, if any, of the value-added integrations Cisco and third parties provide. Webex uses an open architecture for the secure distribution of encryption keys, allowing enterprises to gain control over the management of their encryption keys and the confidentiality of their data. This means that content is encrypted on the user’s Cisco Webex Teams app and remains encrypted until it reaches the recipient, with no intermediaries having access to decryption keys for content unless the enterprise explicitly chooses to grant such access.

The impact of breaches can be severe, and so Cisco has introduced integrations and controls into its Webex portfolio to allow customers to manage the application of their security policies. Cisco® Webex Control Hub is a web-based, intuitive, single-pane-of-glass management portal that enables you to provision, administer, and manage Webex services.

The Pro Pack for Webex Control Hub is a premium offer for customers that require more advanced capabilities and integrations with their existing compliance, security, and analytics software.

Webex security differentiation

- Webex baseline security for user-generated data is among the strongest in the collaboration solutions market. Frequently, other collaboration vendors provide security through piecemeal encryption of data during transit, while at rest on devices, and during storage—all using different solutions. No enterprise messaging offer today supplies the true end-to-end encryption provided by Webex Teams.
- Customers’ ability to hold keys on-premises (using Webex Hybrid Data Security or HDS) also differentiates Webex from the competition, because customers can not only manage their key storage, but also host key compliance and search services on-premises. HDS handles unencrypted content for compliance and search services in the customer’s secure data centers instead of on the Webex platform.
- The Webex platform always stores encrypted content in a realm separate from the storage of keys and services that handle unencrypted content. Despite having achieved this level of data security, Webex has not compromised on enterprise-grade features such as content searches, e-discovery, archival capabilities, and Data Loss Prevention (DLP).

Webex data security using cloud key management services

Webex platform-based Key Management Services (cloud KMS) are available by default to all customers to encrypt their content before it leaves a user's Webex Teams™ app. This baseline for all customers, including online offer consumers, helps ensure that Cisco always provides KMS and end-to-end encryption.

With cloud KMS, every Webex Teams users get:

- Clear separation between the services that handle storage and transport of encrypted content and the services that handle encryption and security key management
- An end-to-end encrypted channel between the cloud KMS and the Webex Teams app or Webex registered device for exchanging keys
- Industry-standard encryption of user-generated content using symmetric keys managed by the cloud KMS (minimum of one key per Webex Teams space)
- Controlled authorization to access keys using users' access tokens
- Encrypted search capabilities
- Enterprise capabilities such as e-discovery, DLP APIs, and archival capabilities, with decryption done at the perimeter, authorized by the administrator

Webex data security with Hybrid Data Security

Security-conscious enterprise customers may choose to deploy the security realm services, including KMS, on their own premises. This works no differently than using the cloud KMS, except that keys are obtained and accessed through an on-premises deployment of the servers.

Hybrid Data Security (HDS) includes:

- On-premises deployment and management of the security realm through the Pro Pack for Webex Control Hub
- KMS and storage
- Deployment that supports both inspecting and non-inspecting for both transparent and explicit proxies, including the mode where external DNS resolution is blocked
- Search indexer: Ability to securely search encrypted Webex Teams content
- E-discovery on-premises engine: Although the e-discovery user interface will be hosted in the cloud, the engine remains on the premises for customers who opt to deploy HDS in their own data centers
- Automatic upgrades, alerts, and notifications
- Local logs and audits of access to keys using an on-premises "bring-your-own" syslog

Webex data security features

Table 1 summarizes Webex data security features.

Table 1. Data security features

Feature	Standard offer/ Pro Pack required	Description
End-to-end encryption of content **Note: Includes user-generated content such as messages, file uploads, space names, meeting subjects, device nicknames, and Cisco Webex Board content**	Standard offer	Webex Teams uses industry-leading encryption to help ensure that Webex messages, files, and whiteboards remain confidential, available, and secure at all times. The Webex Teams application encrypts your data before it leaves your device, using dynamic keys from the KMS. Data stays encrypted when it's in transit to our cloud servers, when we process your data (data in use), and when we store it (data at rest). The KMS is responsible for creating, maintaining, and authorizing access to the encryption keys that the Webex Teams app uses to encrypt and decrypt content.
Encryption in transit	Standard offer	We use secure HTTPS for all web transactions between Webex Teams for Mac, Windows, iPhone, Android, and web and our cloud. Similarly, HTTPS is used for all web transactions from Webex devices (for example, Webex room devices, IP phones, Webex Board). Web APIs on the Cisco® Collaboration Cloud (at developer.webex.com) use HTTPS. There is no support for HTTP. Consequently, all transport in and out of the Cisco Collaboration Cloud is encrypted. HTTPS is also used to protect data in transit from or to Webex Control Hub. All media in Webex, such as voice, video, desktop share, and whiteboarding, are transmitted using Secure Real-Time Transport Protocol (SRTP, defined in RFC 3711). Currently, the Webex platform decrypts real-time media for mixing, distribution, PSTN trunking, and demarcation purposes.
Search on encrypted content	Standard offer	Search indexes for all user-generated messages are created when encrypted content is received in the Cisco Collaboration Cloud. Search indexes are one-way hashed using dynamic keys before being stored. When the end user searches for a word in Webex Teams, the word is encrypted before leaving the app. Words are appropriately hashed and searched against previously stored encrypted search words. Matches are retrieved and sent to the app for decryption and display to the end user.

Feature	Standard offer/ Pro Pack required	Description
Hybrid Data Security (customer-controlled data security)	Pro Pack required	Enterprises can opt to deploy both the services that manage and store the keys used for encrypting content and the services that generate search index hashes. The deployment supports both inspecting and non-inspecting for both transparent and explicit proxies, including the mode where external DNS resolution is blocked. With these capabilities, enterprise customers have the additional assurance of choosing the location where their users' keys are physically stored. This capability, once it is deployed, should be run in a trial mode first for a select set of users, to help ensure a smooth rollout of the service. More details can be found in the deployment guide.

Frequently asked questions

Q. What encryption algorithm is used for encrypting content?

A. The symmetric cipher used to encrypt Webex Teams content is AES-256 GCM.

Q. Is there an Internet Engineering Task Force (IETF) protocol defined for KMS?

A. Webex builds on open standards and protocols for securing data, including key management specifications designed by Cisco and openly submitted for consideration as Internet standards.

Q. How can I obtain HDS?

A. HDS is one of the many features available for purchase as part of the Pro Pack for Webex Control Hub.

Q. Is a detailed deployment guide available for HDS?

A. Please see https://www.cisco.com/go/hybrid-data-security

Q. What additional security does HDS guarantee?

A. HDS gives you physical control of the keys that are generated and owned by your organization. Although certain cloud services can access those keys, separating the keys from the encrypted content in the cloud assures security-conscious organizations that their content cannot be compromised by outside attacks unless the attacker can access both the encrypted content and the keys.

Application and mobile device security controls

Overview

The Cisco Webex Teams application is enterprise-grade, and Cisco is committed to meeting customer security needs with the Webex platform. Enterprise IT requires basic controls on the security of the applications it deploys to users. With Webex Teams, the available controls include capabilities such as PIN lock enforcement, token revocation and remote wipe of Webex Teams cached content on mobile devices, and Webex Teams for Web idle session timeout.

Reset access

In the user profile, an administrator has the ability to revoke the user's access. This will remove all access and refresh the tokens of that user and will also remotely wipe all cached content on the mobile devices that the user is authenticated into. The typical use cases for this capability are when a user loses a mobile device or when a user is terminated but not yet deprovisioned from Webex.

Mobile device security controls

The Cisco Webex Teams for iPhone and Android apps benefit from the following enterprise-grade security features:

- All supported Webex authentication – password based or single sign-on based – establishes OAuth tokens for authorizations. Once established, the client refreshes the access tokens, never requiring a reauthentication unless specific events such as deprovisioning or token revocation occur.
- End-to-end encryption using dynamic keys.
- Secure Transport Layer Security (TLS) connection to the Cisco Webex service and to the user's organization-defined KMS (Cisco Webex platform or HDS).
- PIN lock requirement when enabled (Pro Pack required). This capability requires users to secure their devices with PIN lock or passcode, helping ensure that enterprise content in the Webex Teams app is not accessible if the device is misplaced, lost, or in the wrong hands.
- Remote wipe of content cached on mobile devices when either the user is deprovisioned from Webex or the user's access tokens are revoked by an administrator.
- Encryption at rest on Webex Teams for mobile apps.
- Basic Mobile Device Management (MDM) support certified with Cisco Meraki® Systems Manager and AirWatch, but not limited to these providers.

Webex application and mobile device security features

Table 2 summarizes the application and mobile device security controls.

Table 2. Application and mobile device security control features

Feature	Standard offer/ Pro Pack required	Benefit
PIN lock enforcement **Note: Only for iOS and Android smartphones; does not include Chromebook**	Pro Pack required	Once enabled by an enterprise administrator, PIN lock enforcement requires the user of Webex Teams for iPhone and Android to enable the device's PIN lock when using certain features in the mobile app, in order to continue using the app. This feature helps ensure the security of the content in the Webex Teams app.
Remote wipe and access reset by administrator	Pro Pack required	When a user loses their mobile device or has left the organization, an administrator can revoke all access and wipe Webex Teams cached content from the mobile device (iPhone and Android), helping ensure content security for the enterprise.
File share controls	Pro Pack required	An enterprise can choose not to use Webex file shares if there is concern for data leaks or they have other file management vendors for compliance or regulatory reasons.

Feature	Standard offer/ Pro Pack required	Benefit
Basic MDM support	Standard offer	Webex Teams mobile apps can be managed through MDM providers and security controls enabled for the device to protect data leaks or exfiltration. • Disable copy/paste, backups, document sharing. • Enforce device-level passcode and remote wipe. Note: This support is specifically verified with Meraki Systems Manager and VMware AirWatch, but the basic controls are expected to work with most MDM providers.
External communication control	Pro Pack required	An Enterprise can choose not to allow external communication due to information security and data loss concerns. As a result, users within the org cannot add users outside the org in spaces owned by the org and users within the org will not be able to join external spaces. Guest meetings and calls will still be allowed.

Frequently asked questions

Q. Is Cisco Webex certified for specific MDM providers?

A. Yes.

Q. How can an administrator access the PIN lock enablement feature?

A. This is a premium feature enabled through the Pro Pack for Webex Control Hub. It becomes available under Settings when you purchase the add-on offer.

Q. Will more security controls be added?

A. Yes. Webex is a cloud service and will constantly be adding new features to help ensure ongoing control and visibility.

Endpoint connectivity

Cisco Webex supports seamless connectivity to the cloud through already deployed proxies. Authentication types supported include NoAuth, Basic, and NTLM for mobile and desktop clients, digest-based authentication for mobile clients, and TLS intercept proxy on desktop clients. Proxy configuration methods supported are manual configuration, Proxy Auto-Config (PAC), and Web Proxy Auto Discovery (WPAD). Group Policy Objects (GPO) are supported only on Windows clients.

With the proxy support now available with Webex, proxy whitelisting is no longer necessary. For network requirements to enable proxy support, please see the following two articles:

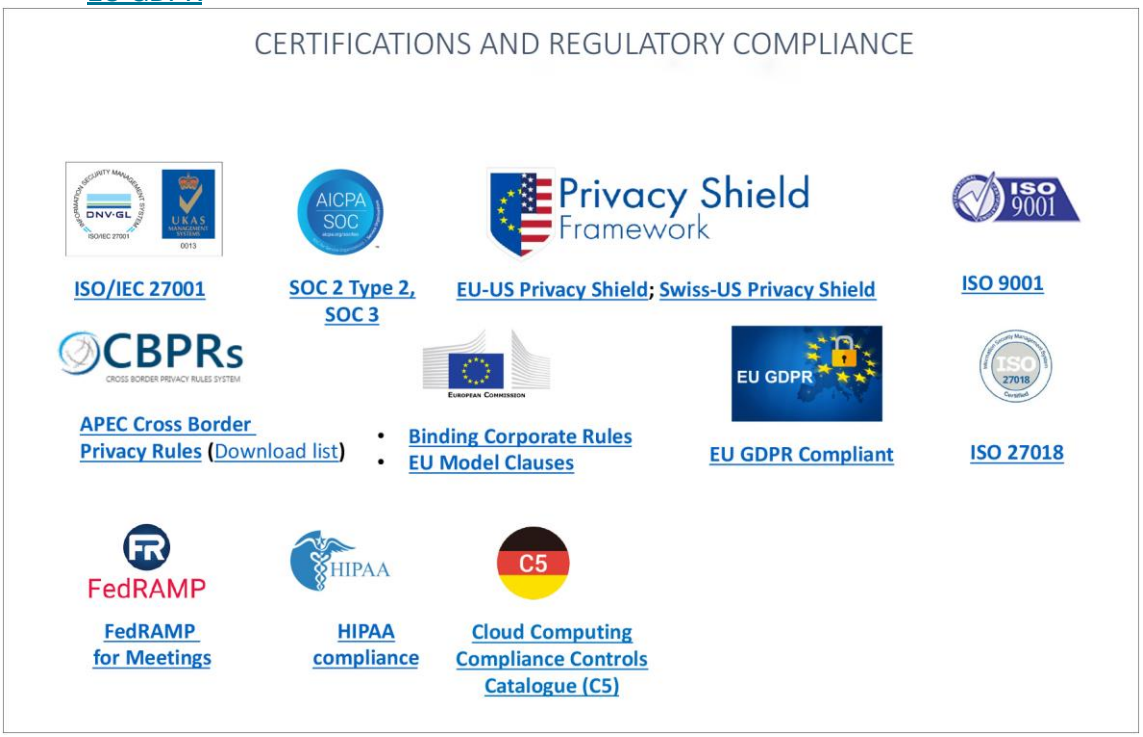
Network Requirements for Cisco Webex: https://collaborationhelp.cisco.com/article/en-us/WBX264

Network Requirements for Cisco Webex Teams Services: https://collaborationhelp.cisco.com/article/en-us/WBX000028782

Certifications and regulatory compliance

Cisco Webex has an impressive set of standard certifications and is in compliance with many of the international regulations, allowing Webex to be sold across the globe (Figure 1). These certifications and regulations are as follows:

- ISO/IEC 27001, 27017
- ISO 27018
- SOC 2 Type 1 and Type 2
- Cloud Computing Compliance Controls Catalogue (C5)
- HIPAA compliant for use by healthcare customers through a HIPAA Self-Assessment
- FedRamp for Meetings
- EU-US Privacy Shield
- Swiss-US Privacy Shield
- APEC Cross Border Privacy Rules
- Binding corporate rules
- EU Model Clauses
- EU GDPR



Data locality

Cisco Webex provides the option for European customers to choose to provision their user identities and encryption keys in European data centers. View the data locality overview for more details. Cisco Webex certifications and regulatory compliance

Cisco Capital

Flexible payment solutions to help you achieve your objectives

Cisco Capital makes it easier to get the right technology to achieve your objectives, enable business transformation and help you stay competitive. We can help you reduce the total cost of ownership, conserve capital, and accelerate growth. In more than 100 countries, our flexible payment solutions can help you acquire hardware, software, services and complementary third-party equipment in easy, predictable payments. Learn more.

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

C78-740771-01 09/19