Datasheet

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 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.

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 Webex 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 Webex has introduced integrations and controls to allow customers to manage the application of their security policies. 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 Control Hub is a premium offer for customers that require more advanced capabilities and integrations with their existing compliance, security, and analytics software.

Security differentiation

- Zero-Trust Security from Webex provides an open, standard based form of end-to-end encryption with strong identity verification for scheduled and personal room meetings. With end-to-end encrypted meetings, customers have exclusive control of the meeting encryption keys and Cisco and anyone cannot access their meeting content. No other collaboration vendor provides standard based end-to-end encryption for meetings with verified identity.

- 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.

- Customers’ ability to hold keys on-premises (using 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 platform.

- The 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).

End-to-end encryption with identity verification for Webex Meetings

Zero-Trust Security from Webex provides an open, standard based form of end-to-end encryption with strong identity verification for scheduled and personal room meetings, to keep your meetings safe from the full spectrum of attacks. For more details on end-to-end encryption for meetings see Zero-Trust Security for Webex White Paper.

Zero-Trust Security supports the following in end-to-end encrypted meetings:

- Standards-based, formally verified cryptography
- End-to-end-verified identity (E2EI)
- Webex Room devices (Room Series, Desk Series, and Board)
- End-to-end encryption (E2EE) in Personal Room meetings
- A security icon which lets all meeting participants know at a glance that their meeting is secure, as well as when end-to-end encryption is enabled for the meeting
- Verbal verification of meeting attendees using a new Security Verification Code

Data security using cloud key management services

The 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 App. This baseline for all customers, including online offer consumers, helps ensure that Webex always provides KMS and end-to-end encryption.

With cloud KMS, all Webex users get:

- A master key protected by the Hardware Security Module (HSM) in the cloud
- 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 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 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

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 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 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
- Encrypted connections between HDS nodes and database servers
- Proxy support: Transparent non-inspecting, Transparent tunneling, Explicit and support for Blocked External DNS Resolution Environments
- Automatic upgrades, alerts, and notifications
- Local logs and audits of access to keys using an on-premises "bring-your-own" syslog

Bring Your Own Key (BYOK)

Security conscious customers who want to protect their organizations' data can supply their own Main Key which will be used to encrypt content. This allows Organizations to have separation and more control of security (encryption) to meet their InfoSec requirements. Organization administrators and Infosec teams can manage the lifecycle of their main key from Control Hub. BYOK provides the follow functionality:

- Activate an Org specific Main Key: Admins can upload a Main Key (encrypted with the Webex Cloud KMS (Key Management Service) public key) and activate it to start protecting the data generated by users in their Org.
- Key rotation: Admins can periodically rotate out a main key (with a new main key) to improve their security posture and prevent attackers from accessing sensitive data.
- Key Revocation: As a war time response to security breaches, InfoSec teams can revoke their main key to prevent unauthorized users from gaining access to confidential data.
- Key Deletion: In extreme scenarios of compromise, Organizations can permanently delete the main key to prevent access to data going forward.
- Main keys will be permanently deleted from Webex's infrastructure after a grace period of 30 days. After the main key is permanently purged, Org admins can either delete the existing Organization and start over by provisioning users and services into a new Organization or go through a recovery flow to resurrect the main key (Note: This requires that the customer have the original main key saved. Should admins lose the original key, there is no way to recover the key and contents of the Org).
- Visibility: Admins can get the status of the Key used to protect their organization's content and history of key activity from Control Hub. In addition, an audit trail of key state changes is also recorded for compliance purposes
- Supported Content: Meetings content (recordings, transcripts), space content (space title, messages, files, whiteboard), calling content (voice mail), calendar events.

Security Health Insight

To help IT administrators get a clear picture of their organization's security posture, Control Hub now provides security health insights as part of Control Hub-As-A-Coach. This feature audits the organization's security configurations against the recommended baseline, provides insight into organization security level and provides coaching to improve security posture with recommended goals and tasks. Security health insight provides the follow functionality:

- Monitors key security settings across various workloads such as meetings and messaging.
- Audits organization's security configurations against a baseline and gives a security score (standard, enhanced or advanced).
- Provides a dashboard which monitors key security settings and provides a completion score based on the security posture.
- Suggests recommended tasks to improve security posture via an intuitive dashboard and alert capabilities.

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 for Meetings	Standard offer	Webex provides an open, standard based end-to-end encryption with strong identity verification for scheduled and personal room meetings. With end-to-end encrypted meetings, customers have exclusive control of the meeting encryption keys and Cisco and no others can access their meeting content.
End-to-end encryption of content Note: Includes user-generated content such as messages, file uploads, space names, meeting subjects, device nicknames, and Webex Board content	Standard offer	Webex uses industry-leading encryption to help ensure that messages, files, and whiteboards remain confidential, available, and secure at all times. Webex 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 App uses to encrypt and decrypt content.
Encryption in transit	Standard offer	We use secure HTTPS for all web transactions between Webex Messaging 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 Cloud (at developer.webex.com) use HTTPS. There is no support for HTTP. Consequently, all transport in and out of the Cloud is encrypted. HTTPS is also used to protect data in transit from or to 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 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, 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.

Table 1. Data security features

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.
Bring Your Own Key (BYOK)	Pro Pack required	Organizations can bring their own main Key to encrypt confidential data generated by users in their Org. With the BYOK feature, admins can easily activate a new main key to encrypt data, rotate the key periodically and delete it under extreme circumstances. The feature allows Organizations to improve their overall security posture and gives them the ability to control and respond to security incidents more effectively
Security health insight	Standard Offer	Webex now provides an intuitive dashboard that audits key security settings and compares it against a baseline standard to give your organization a security posture score. It guides you to improve the security posture of your organization by enabling key security settings across various workloads there by making your collaboration more secure.

Application and mobile device security controls

Overview

The Webex application is enterprise-grade, and Webex is committed to meeting customer security needs. Enterprise IT requires basic controls on the security of the applications it deploys to users. With Webex App, the available controls include capabilities such as PIN lock enforcement, token revocation and remote wipe of Webex cached content on mobile devices, and Webex 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 Webex App for iPhone and Android 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 Webex service and to the user's organization-defined KMS (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 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.
- Disable message preview on mobile device's lock screen to ensure that nearby users cannot peek into the messages delivered via notification previews. Or if the device is locked and left behind inadvertently, other users do not continue to see previews of messages being sent by looking at the device's locked screen.
- Disable the use of unmanaged App to ensure that users can only use a corporate managed version of Webex App and comply with organization security and compliance policies
- Encryption at rest on Webex for mobile apps.
- Basic Mobile Device Management (MDM) support certified with many vendors including but not limited to Mobile Iron, Cisco Meraki® Systems Manager, AirWatch, MaaS360 etc.

Webex App unlock using Face Id: Provide users the ability to lock the Webex App (to prevent unauthorized access) and sign in via a modern and frictionless Authentication mechanism, Face Id. To use this feature users must have a device that supports Face Id and enroll in it. Users can optionally add a layer of security to prevent unauthorized access to Webex App and content.

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

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 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 App.

Table 2. Application and mobile device security control

FEATURE	STANDARD OFFER/ PRO PACK REQUIRED	BENEFIT
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 cached content from the mobile device (iPhone and Android), helping ensure content security for the enterprise.
Disable message preview on mobile device's lock screen	Pro Pack required	A customer can ensure that message previews for mobile notifications are always disabled so that nearby users cannot peek into the messages being exchanged. Or if the device is locked and left behind inadvertently, other users do not continue to see previews of messages being sent by looking at the device's locked screen.
Disable the use of unmanaged App	Pro Pack required	An admin can choose to restrict users to a corporate managed version of the Webex App. With this setting enabled in Control Hub, users won't be able to use an unmanaged version of the Webex app (downloaded from Apple App Store / Google Play Store or via other means).

Webex application and mobile device security features

Table 3 summarizes the application and mobile device security controls.

Table 3. Application and mobile device security control

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 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 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 cached content from the mobile device (iPhone and Android), helping ensure content security for the enterprise.

Table 3. Application and mobile device security control

FEATURE	STANDARD OFFER/ PRO PACK REQUIRED	BENEFIT
Disable message preview on mobile device's lock screen	Pro Pack required	A customer can ensure that message previews for mobile notifications are always disabled so that nearby users cannot peek into the messages being exchanged. Or if the device is locked and left behind inadvertently, other users do not continue to see previews of messages being sent by looking at the device's locked screen.
Disable the use of unmanaged App	Pro Pack required	An admin can choose to restrict users to a corporate managed version of the Webex App. With this setting enabled in Control Hub, users won't be able to use an unmanaged version of the Webex app (downloaded from Apple App Store / Google Play Store or via other means).
File share controls	Pro Pack required	A customer who has a locked-down environment can ensure their users can upload and download files only from the preferred client type (desktop instead of mobile, for example) or from specific IP ranges or based on Active Directory groups. Uploads and downloads can also be based on file types or internal vs external organization users.
Basic MDM support	Standard offer	Webex 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, VMware AirWatch, Mobile Iron and IBM MaaS360 but the basic controls are expected to work with most MDM providers who conform to the app config community standards.
MAM: Intune SDK integration	Standard offer	Webex mobile applications support Microsoft Intune integration with a Software Development Kit (SDK). With this SDK, IT administrators can control user access to application functions and configuration policies for Webex Meetings and Messaging, in order to control and secure corporate data.
MAM app wrapping	Standard offer	A customer who would like to support a BYOD environment usually requires containerization of enterprise applications. With the option to allow a customer to perform app wrapping of the Webex App through their choice of MAM provider, a customer can onboard their users seamlessly to the Webex app while maintaining their enterprise compliance for mobile devices without having to manage them.

Table 3. Application and mobile device security control

FEATURE	STANDARD OFFER/ PRO PACK REQUIRED	BENEFIT
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.
Webex App unlock using Face Id	Standard Tier	Users have the ability to add a layer of security and prevent unauthorized access to Webex Apps by enabling the Face Id unlock feature. After a period of inactivity (configurable) the access to the Webex App will be locked out until users Authenticate via Face Id

Endpoint connectivity

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 allowed listing is no longer necessary. For network requirements to enable proxy support, please see the following two articles:

- Network Requirements for Webex Meetings
- Network Requirements for Webex Services

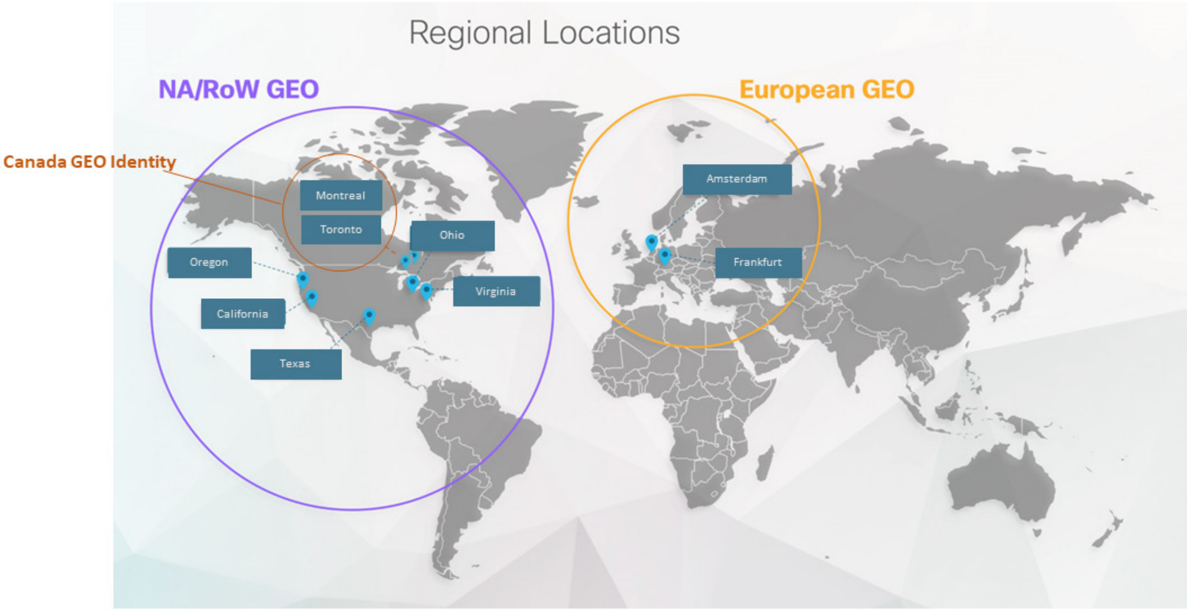
Certifications, standards, and regulatory compliance

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

Table 4. Certifications, standards, and regulatory compliance

INFORMATION SECURITY + PRIVACY	REGULATORY	CROSS-BORDER TRANSFERS
· ISO 2700X i.e ISO 27001 / 27017 / 27018 / 27701 · SOC 2 Type II and SOC 3 · Cloud Computing Compliance Controls Catalog (C5) · HITRUST · FedRAMP · Cisco's Quality Management System · ISO 9001 · CSA STAR L2 · DoD IL-5 (Webex for Defense Hosted) · Japan ISMAP · Spain ENS · Australia IRAP	· HIPAA · GDPR · FERPA · COPPA · PIPEDA · CCPA · PCI · Continually assessing regs	· Binding Corporate Rules · APEC cross-border privacy rules · EU Standard Contractual Clauses

Figure 1. Hybrid Work Powered by Global Webex Data Centers



Data locality

EU data residency is part of our commitment and strategy to lead with choice, trust and innovation. An important factor for our customers as they consider data residency is ensuring that the handling of their data meets EU data protection standards and that they have control over public authorities access to their data.

The additional new data centers in Canada and Germany are part of this effort and complement existing data centers in the region for backup, resiliency, and availability, providing additional opportunities to host data in the EU (European Union) and Canada.

New Webex customers in the EU can achieve full data residency within the EU — including billing data, Meetings, Messaging, Calling, user identities, analytics, and user generated content such as meeting recordings, transcripts, shared files, or chats, and encryption keys—all part of our customers' daily Webex experience.

New Webex customers from Canada can provision, store, and process their Webex Meetings, user identities, analytics, and user generated content including meeting recordings and transcripts in the data centers in Canada.

Migration plans are in place for existing customers from the EU and Canada with flexibility to manage the data migration to their region.

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.