Webex Messaging Security

Cloud Collaboration Security Technical Paper

December 2022

Contents

Webex is a cloud collaboration platform that provides messaging, calling, and meeting features. This paper describes the architecture and security features related to the Webex Messaging service and the suite of tools that the Webex Messaging service provides to keep customers' data safe from Cisco as well as external attackers.

1. Webex Messaging Overview

Webex Messaging Service

Webex Messaging is a cloud-based service that provides a secure and persistent messaging service. The service is globally distributed and allows for regionalized storage of user generated content (messages, files, whiteboards, etc.), identity services, and encryption keys. Users access the messaging service using the Webex App, where they can create spaces to participate in conversations with other users, by exchanging messages and files.

A key architectural differentiator of the Webex Messaging service is "Webex End-to-End Encryption", an additional layer of security that it provides for user generated content. Today, most cloud service providers offer security by encrypting data in transit and data at rest. Data in transit is encrypted using TLS, data at rest by using disk and/or database encryption.

With Webex Messaging, in addition to encrypting data in transit and at rest, all content (messages, files, whiteboards etc.) generated by users is also encrypted by the Webex App before being sent over TLS. User generated content is stored in this encrypted form on encrypted content servers in the Webex cloud. This additional layer of security protects user data in transit from TLS interception attacks, and stored user data from potential bad actors in the Webex cloud.

Beyond architectural security, the Webex Messaging service provides a rich set of security controls that can be configured via Webex Control Hub. Administrators can define multiple security policies for their users, such as:

- Data retention policies
- File sharing controls
- Anti-Malware file scanning
- Controlling communication with external organizations
- Controlling communication between groups of users within your organization

The Webex Messaging service also integrates with third party applications that can provide additional layers of security and control, such as:

- Data Loss Prevention (DLP) applications that can monitor and manage content posted by users
- Enterprise Content Management (ECM) applications for external file storage
- Mobile Device and Application Management applications (MDM/MAM)
- Message and file archival, e-discovery, and cloud access security broker (CASB) systems

For more details, refer to the Control Hub (Data Security and Privacy) Data Sheet.

The Webex App

The Webex App is a multifunctional collaboration application that provides messaging, meeting, and calling services. By combining these services, the Webex App provides continuity of collaboration, by allowing users to:

- Initiate a conversation and share documents in a messaging space.
- Upgrade the conversation to a Webex meeting or one-to-one call.
- Continue the conversation in the space once the meeting or call has ended.

As well as joining Webex Meetings, the application also has the capability to make calls to:

- Webex Apps and Webex devices
- The PSTN
- SIP-based devices

Webex App is supported on Windows, macOS, Linux, iOS, Android, ChromeOS, and web browsers.

For more information on Webex App security refer to the Webex App Security Technical Paper.

2. Webex Messaging Service Architecture

Messaging Services

Webex Messaging services can be roughly divided into two types:

1. Services that process user content and associated data, but do not store data.
2. Services that manage, store, or secure user generated content and user information.

Services that process user content and associated data, but do not store user generated content

These micro services provide the features and functions that make up the core of the Webex Messaging service, for example:

- Search service

- Search Indexing service
- e-Discovery service
- Directory Connector service
- Conversation service
- Document Transcoding service
- Client log service
- Client upgrade service
- Presence service
- And numerous other services…

These micro services are loosely coupled, allowing the Webex cloud to introduce new features using a continuous development model.

Services that manage, store, or secure user generated content and user information

- Content storage (messages, files, whiteboards, meeting information)
- Key Management Service (for user generated content encryption)
- Webex Identity Service (common to Webex Meetings, Messaging, and Calling services)

These services are regionalized, allowing customers to choose the region in which they store their data when they sign up to the Webex Messaging service. This stored data is encrypted at rest, with user generated content having an additional layer of encryption, using a unique encryption key per Webex Messaging space, file, meeting, or whiteboard instance.

Data Regionalization

As shown in Figure 1, Webex Messaging currently supports two geographic regions:

Region 1: North America / Rest of the World

Region 2: European Region

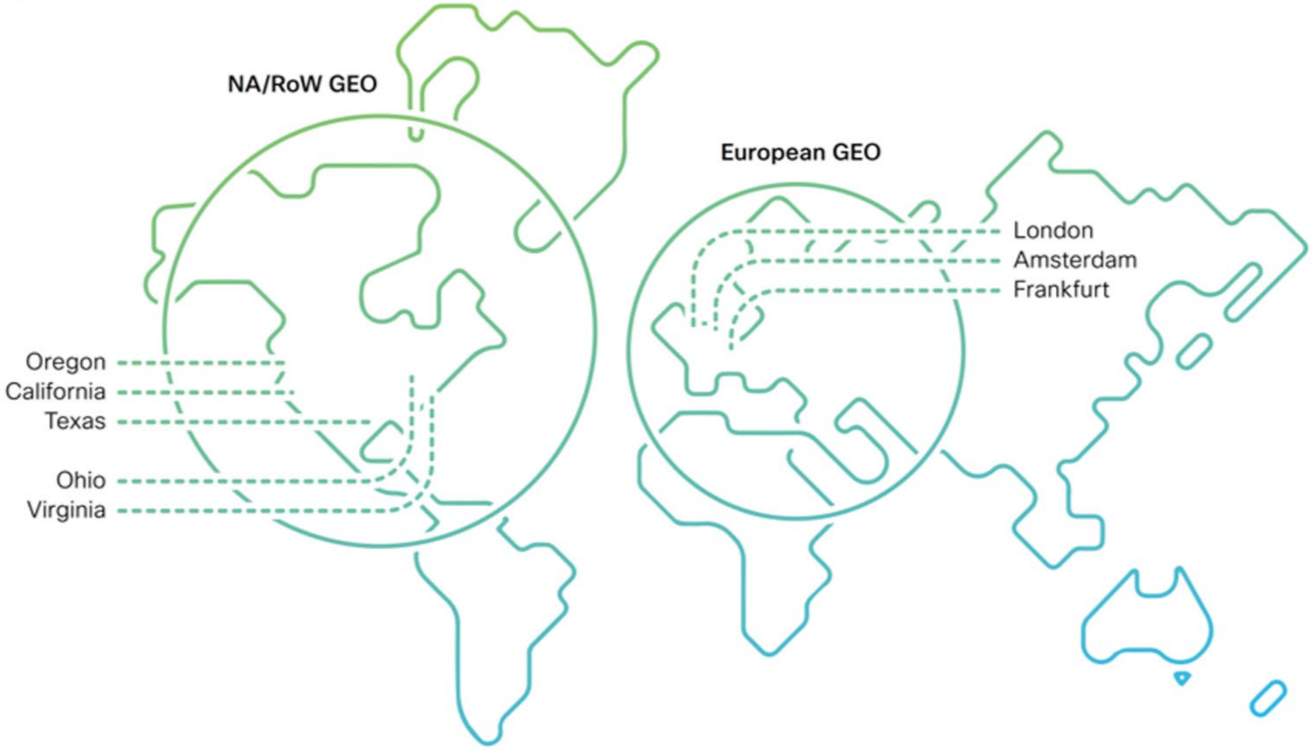


Figure 1. Webex Messaging Regions

For more information on data residency, refer to the Data Residency in Webex App article.

Media Services

In addition to messaging services, Webex App users can also join Webex Meetings and make calls. For example, two or more users having a conversation in a messaging space can escalate a message-based conversation to a one-to-one call or Webex meeting.

Cloud registered Webex Apps and Webex Room devices use HTTPS signaling to communicate with Webex cloud services. Webex Apps and Webex Room devices can make and receive calls to join Webex Meetings, and to establish one-to-one calls to other Webex Apps and Webex devices, SIP based endpoints including desk phones, and to the PSTN. The media for these calls is typically anchored on media servers in the Webex cloud. Media servers are clustered and globally distributed in the Webex cloud (they can also be deployed on-premises as Webex Video Mesh Nodes).

Webex Apps and Webex Room devices periodically perform reachability tests to determine the availability of media nodes within these clusters. These reachability results are reported to the Webex cloud prior to establishing a call so that the cloud can determine the best/nearest media node to use. Media node selection is predominantly based on the round-trip time from the endpoint to the media node, but available media transport protocols (UDP (preferred)/TCP/TLS), and media node resources also come into play when selecting a media node to use. All media (audio/ video/ content sharing) sent and received by Webex Apps and Webex Room devices is encrypted.

3. Cloud Security for Signaling and Media

All signaling and media sent by cloud registered Webex Apps and devices to and from the Webex cloud is encrypted.

Signaling Traffic

The Webex App and Webex devices use HTTPS and WebSocket Secure (WSS) connections for signaling. Signaling connections from the Webex App and Webex devices are outbound only and use fully qualified domain names to establish sessions to Webex services.

Signaling traffic is protected by TLS using strong encryption suites. Webex services use TLS version 1.2 or 1.3. The cipher selection is based on the Webex server TLS preference.

Using either TLS 1.2 or 1.3, Webex prefers ciphers suites using:

- ECDHE for key negotiation
- RSA-based certificates (3072-bit key size)
- SHA2 authentication (SHA384 or SHA256)
- Strong encryption ciphers using 128 or 256 bits (for example, AES_256_GCM, AES_128_GCM, and CHACHA20_POLY1305)

For example:

- TLS 1.2: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS 1.3: TLS_AES_256_GCM_SHA384

Media Traffic

All media sent and received by Webex Apps and Webex Room devices is encrypted. The Webex App and Webex Room devices encrypt real-time media for audio, video, and content sharing streams using the following encryption ciphers:

- AES-256-GCM cipher
- AES-CM-128-HMAC-SHA1-80 cipher

AES-256-GCM is a modern encryption cipher with a 256-bit encryption key. AES-256-GCM is the preferred media encryption cipher used by the Webex App and Webex Room devices. AES-CM-128-HMAC-SHA1 is a mature encryption cipher that has proven interoperability between vendors. AES-CM-128-HMAC-SHA1 may be used to encrypt media to Webex services (e.g., PSTN), or for SIP based calls to Cisco and 3rd party SIP devices.

Webex End-to-End (E2E) Encryption and Zero-Trust E2E Encryption

The Webex suite offers two types of end-to-end encryption:

1. Webex End-to-End Encryption
2. Zero-Trust End-to-End Encryption

While both forms of end-to-end encryption provide an additional layer of encryption that safeguards data from interception attacks, they differ in the levels of confidentiality that they offer.

Webex End-to-End Encryption

Webex End-to-End Encryption uses Webex's cloud-based Key Management System (KMS) to generate and distribute encryption keys for Webex Messaging, file sharing, calendaring, and whiteboarding services. Customers can even generate the master encryption key with the Bring Your Own Key (BYOK) option. Webex Hybrid Data Security (HDS) is also available as an on-premises version of KMS. With Webex End-to-End Encryption, in addition to encrypting data in transit and at rest, all content (messages, files, whiteboards, and so on) generated by users is also encrypted by the Webex App before being sent over TLS. User generated content is stored in this encrypted form on encrypted content servers in Webex. This additional layer of security protects user data in transit from TLS interception attacks, and stored user data from potential bad actors in the Webex cloud.

With Webex End-to-End Encryption, the Webex cloud can access encryption keys to decrypt data for core services such as Message Indexing for search functions, Data Loss Prevention, File Transcoding, eDiscovery, and data archival. Webex End-to-End Encryption is discussed in depth in this document.

Zero-Trust End-to-End Encryption

Zero-Trust End-to-End Encryption is used by Webex Meetings to provide meetings that offer additional levels of security and confidentiality. Zero-Trust End-to-End Encryption uses the Messaging Layer Security (MLS) protocol to exchange information that allows participants in a Webex Meeting to create a common meeting encryption key. This meeting encryption key is only accessible to the participants in the meeting and cannot be accessed by the Webex service, hence Zero-Trust.

For more information on Zero-Trust End-to-End Encryption refer to the Zero-Trust Security for Webex technical paper.

4. Webex App Security

The Webex App is a downloadable application for Windows, macOS, Linux, IOS, Android operating systems, and ChromeOS. The Webex App is a multifunctional collaboration application that provides messaging, meeting, and calling services providing voice, video, and messaging services to its users. The Webex App has been built with security in mind using Cisco best practices for secure software development. For details on how the Webex App is secured see the Webex App Security technical paper.

5. Webex Control Hub: Administrative Security

Webex Control Hub provides a plethora of security features that allow administrators of Webex Messaging to control how messaging is securely used within their organization and with external organizations. Examples of some of these security features are:

- Data Loss Prevention (DLP)
- Block External Communications
- Block Internal Communications (Ethical Walls)
- E-Discovery: Content Search and Extraction
- Management of Integrations and Bots
- Auditing of Administrator activities
- Legal Hold
- Mobile Device Controls and MDM/MAM controls
- Data Retention Policies
- Anti-Malware file scanning
- File Sharing Controls

Details of the administrative and security features available for Webex Messaging can be found in the following Webex Control Hub data sheets:

- Control Hub Compliance Data Sheet
- Control Hub Data Security and Privacy Data Sheet
- Control Hub Extended Security Pack Data Sheet
- Control Hub Management and Analytics Data Sheet

6. How Webex Messaging Addresses Security & Privacy Challenges

Webex Messaging encryption provides an additional layer of encryption for user generated content (messages, files, whiteboards etc.). Each Webex Messaging space uses a unique key to encrypt user content before it is sent from the Webex App, these encryption keys are generated, stored, and distributed by the Webex Messaging KMS.

The Webex Messaging service uses an open architecture for the management of encryption keys for user generated content. Customers can choose where the KMS for their organization is located and where encryption keys are stored:

- The organization can use the KMS located in the Webex cloud. In this case, Webex manages and stores the content encryption keys used by the customer's organization.

- The organization can choose to deploy Hybrid Data Security (HDS) nodes to host the KMS on their premises and use their own database to store their content encryption keys.

In controlled and limited circumstances, the Webex cloud can use a specific service account to access content encryption keys and decrypt user content. Usage of this service account is strictly controlled and used by machine accounts only. The Webex cloud decrypts user content to deliver value added services such as:

- Document transcoding
- Search Indexing
- eDiscovery
- Calendar Connector
- API/Application Integration (e.g., DLP applications)

In all these cases, no decrypted content is stored in the Webex cloud.

Our commitment to providing a trusted service offering is not limited to protection of user content. With Webex Messaging, all data about users and usage is protected using a combination of privacy tools and features that includes obfuscated identity, choice, and transparency. As with encryption of user content, these protections were built into the service from the ground up.

7. KMS-Based Security

As shown in Figure 2, KMS-based security is a central security feature for Webex Messaging, providing an extra layer of protection beyond standard cloud security. All customer data transmitted through the Webex cloud is encrypted before being sent, so that cloud components handle customer data in a safe, encrypted form. Before encrypting traffic at the TLS connection layer with the TLS encryption key, the Webex App first uses the KMS content encryption key to encrypt the message data. As a result, even if a cloud component is fully compromised – a situation where an “encryption at rest” and “encryption in transit” approach would fail – the attacker still cannot access customer data, because it’s encrypted using the KMS user generated content encryption keys. Webex only makes exceptions to this rule for a limited set of internal services (e.g., file transcoding, the creation of hashed indexes for search functions), and where customers choose to integrate applications that require access to unencrypted content (e.g., Data Loss Prevention (DLP) applications). More information on these exceptions can be found in the Feature Access to Keys section.

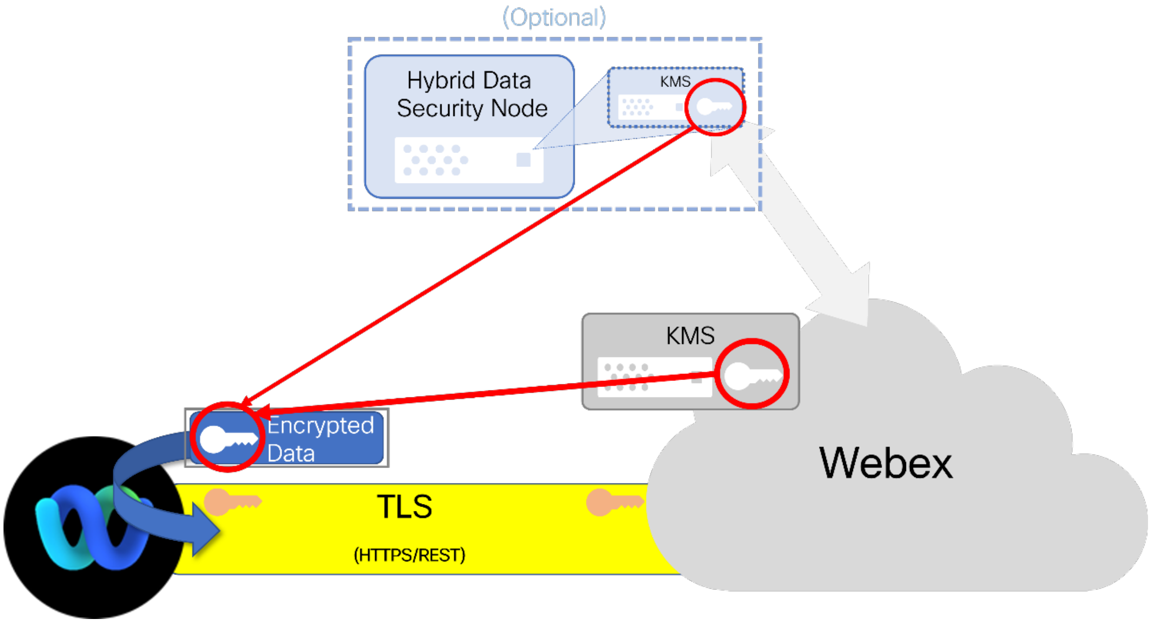


Figure 2. Webex Messaging KMS Encryption over Encrypted TLS

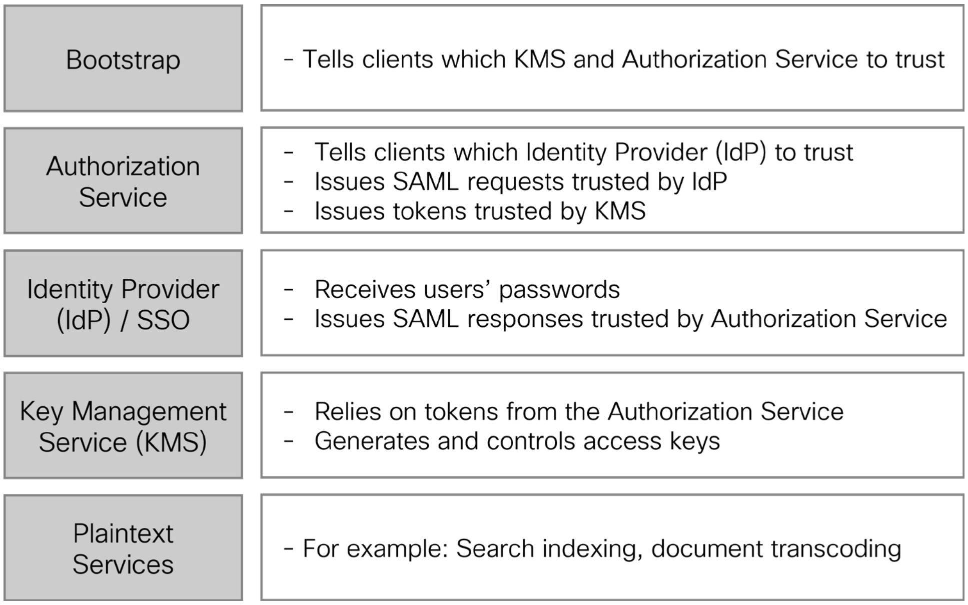
Note that in the case of an optional on-premises Hybrid Data Security (HDS) node, KMS resides in HDS rather than in Webex (see Figure 2).

The separation between customer data and Webex is fundamental to the way the Webex Messaging service is architected and operated – so much so that you can think of the overall functionality of the Webex Messaging service as being divided between two trust domains, a "Customer Domain" and a "Webex Messaging Core." The Customer Domain comprises things that run directly under the customer's control: the clients and hardware endpoints used within an enterprise as well as any client-operated Webex Messaging infrastructure that helps these clients communicate securely. The Webex Messaging Core contains Cisco-operated Webex services that enable these clients to collaborate with each other and with the infrastructure of the Customer Domain.

Using the additional layer of encryption provided by the KMS service produces a dramatic reduction in the information that an attacker can get by breaching the cloud provider. Even with encrypted storage and encrypted connections between cloud components, a breach in any cloud service could potentially compromise customer information. In contrast, the additional layer of encryption provided by the KMS service with Webex Messaging means that customer information is encrypted by default and only decrypted when needed. With typical cloud services that handle customer information in plaintext, the more services the cloud provides, the more risk to customer information should a breach occur. The additional layer of encryption provided by the KMS service allows the Webex Messaging service to provide rich cloud services while maintaining a small attack surface.

KMS-Encrypted Data

The separation between the Customer Domain and the Webex Messaging Core is ultimately enforced by cryptography – encryption of customer data protects it from access by untrusted elements in the Webex Messaging Core. The strength of the separation comes down to how well those encryption keys are protected. As shown in Figure 3, management of keys and access to keys involves a set of important components that work together as an "end-to-end critical path".



Bootstrap	- Tells clients which KMS and Authorization Service to trust
Authorization Service	- Tells clients which Identity Provider (IdP) to trust - Issues SAML requests trusted by IdP - Issues tokens trusted by KMS
Identity Provider (IdP) / SSO	- Receives users' passwords - Issues SAML responses trusted by Authorization Service
Key Management Service (KMS)	- Relies on tokens from the Authorization Service - Generates and controls access keys
Plaintext Services	- For example: Search indexing, document transcoding

Figure 3. Webex Messaging End-to-End Critical Path

The elements of the critical path work together to ensure that only authorized entities and built-in plaintext services can access the keys to decrypt that customer's content and that all unauthorized parties are locked out. To understand how the elements in the critical path work together to achieve this separation, refer to the Webex App Webex Messaging Service login flow shown in Figure 4.

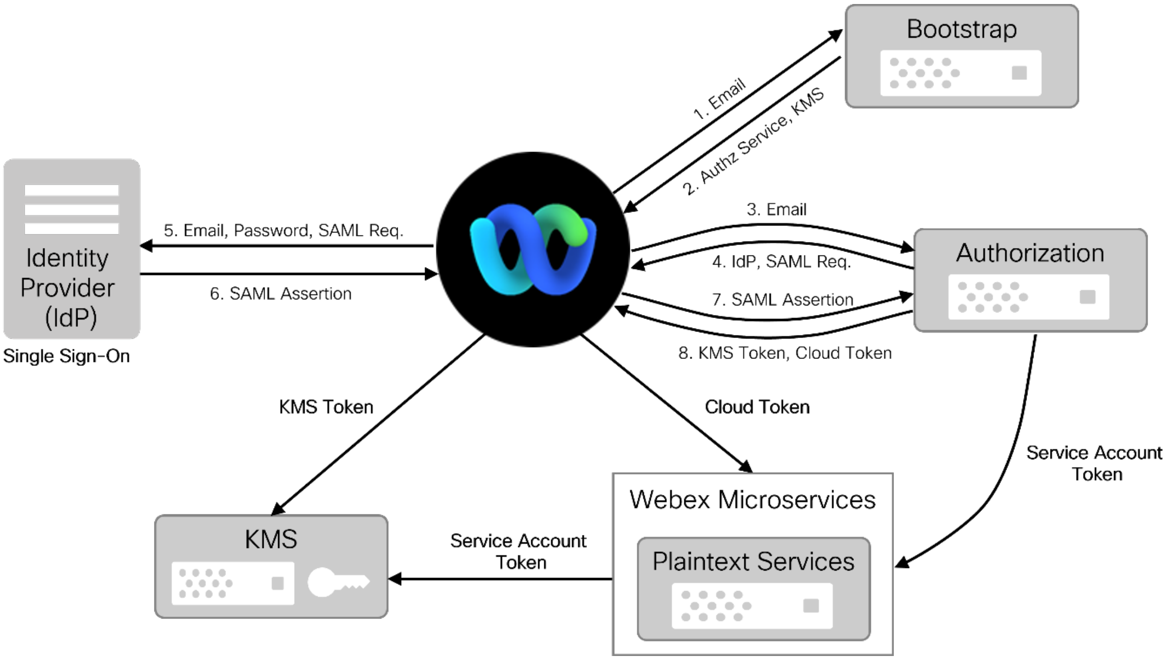


Figure 4. Webex Messaging Service Login Flow

The first thing a user does when logging into the Webex Messaging service is enter their email address. This email address is used to identify the user's organization, the Webex App then looks up which authorization service and KMS it should trust from a bootstrapping service provided by the Webex Messaging service (1, 2). The Webex App then engages in a standard Security Assertion Markup Language (SAML) login with the authorization service, where the client is redirected to the proper identity provider (IdP) based on its email address (3, 4), authenticates with the identity provider to get a SAML assertion (5, 6), and provides the SAML assertion back to the authorization service (7). The authorization service then provides the client with two Open Authorization (OAuth) 2.0 access tokens (8): A KMS token that it will use to authenticate only to its KMS, and a cloud token that it will use to authenticate to microservices in the Webex cloud.

The KMS safeguards the keys used to encrypt a customer's data. Requests by the Webex App are authenticated with the KMS tokens discussed above. The separation between KMS tokens and cloud tokens means that the Webex App will only ever send the KMS token to the KMS. When the Webex Messaging microservice needs to access some content (a "plaintext service" discussed in more detail below), that microservice gets a special token ("Services Account Token") from the Authorization Service that proves to the KMS that the service is of an authorized type.

Using the additional layer of encryption provided by the KMS service allows the Webex Messaging service to provide extra protection for user-generated content. Some Webex Messaging services such as the KMS and the search indexer (a plaintext service), can be operated directly, on the customer's premises with the Hybrid Data Security (HDS) architecture. However, when these components are hosted by Cisco, they are kept under separate access controls from the rest of the Webex Messaging services.

The Webex KMS manages a database of encryption keys that are used to encrypt that enterprise's user-generated content. As shown in Table 1, customers have three options for KMS deployments:

1. Webex KMS
   By default, customers will use the Cisco-operated Webex KMS. The records in the encryption key database are encrypted with a master key that is stored in a Cisco-managed cloud-based Hybrid Security Module (HSM). With Webex KMS, Cisco controls the master key and manages key lifecycle.
2. Hybrid Data Security (HDS)
   This option allows customers to operate their own on-premises KMS on HDS nodes. In this case, the database (Postgres or Microsoft SQL) is provided by the customer and the records are encrypted using a master key stored separately in a secure configuration file. With HDS, the customer controls and manages the master key.
3. Bring Your Own Key (BYOK)
   With this option, a Cisco-operated Webex KMS and cloud-based HSM for key storage is used, however, the customer can import their own key material to generate the master key. With this option, the customer controls and manages the master key, but relies on Cisco to manage the KMS and HSM.

Table 1. Webex KMS Deployment Options

	KMS DEPLOYMENT OPTIONS		
	WEBEX KMS [DEFAULT]	HYBRID DATA SECURITY (HDS)	BRING YOUR OWN KEY (BYOK)
KMS Deployment Location	Cloud	On-Premises	Cloud
Master Key Storage Location	Cloud HSM	On-Premises	Cloud HSM
Master Key Control & Lifecycle	Cisco	Customer	Customer

KMS-based Content Encryption

In Webex Messaging, Webex Apps use an additional layer of encryption so that they can exchange content without that content being accessible to the cloud. As mentioned previously, the keys for this user-generated content encryption are managed by a KMS. The KMS for a customer is effectively the customer's agent for controlling who can access content encryption keys (and thus who can access that customer's content). The components running under the customer's control, for example, the customers KMS and Webex Apps comprise the Customer Domain. Even when some of these components are operated by Cisco, they are kept separate from other Webex Messaging service components. The actual encryption of content, though, is performed by Webex Apps, which get keys from the KMS – effectively "checking the encryption keys out" from the customer's KMS. To do this safely, each Webex App establishes an encrypted tunnel through the Webex cloud to the KMS for its organization. This tunnel works much the same way as the TLS and IPsec protocols used for things like HTTPS and VPNs, using an authenticated ephemeral Elliptic Curve Diffie-Hellman (ECDH) exchange.

As shown in Figure 5, the Webex App first receives a certificate that associates an RSA public key to the KMS's domain name (1). The Webex App generates an EC key pair, encrypts the public component of that pair using the KMS's RSA public key, and sends the result to the KMS over the Webex cloud (2). The KMS decrypts this message, generates its own ephemeral EC key pair, signs the public component with the RSA private key corresponding to the certificate, and sends the result in a message back to the Webex App (3). At this point, the Webex App and KMS server have a shared secret that they can use to derive an encryption key for further messages, and the KMS has proven its identity to the Webex App. To prove its identity the Webex App will send the KMS its KMS token with future requests (4).

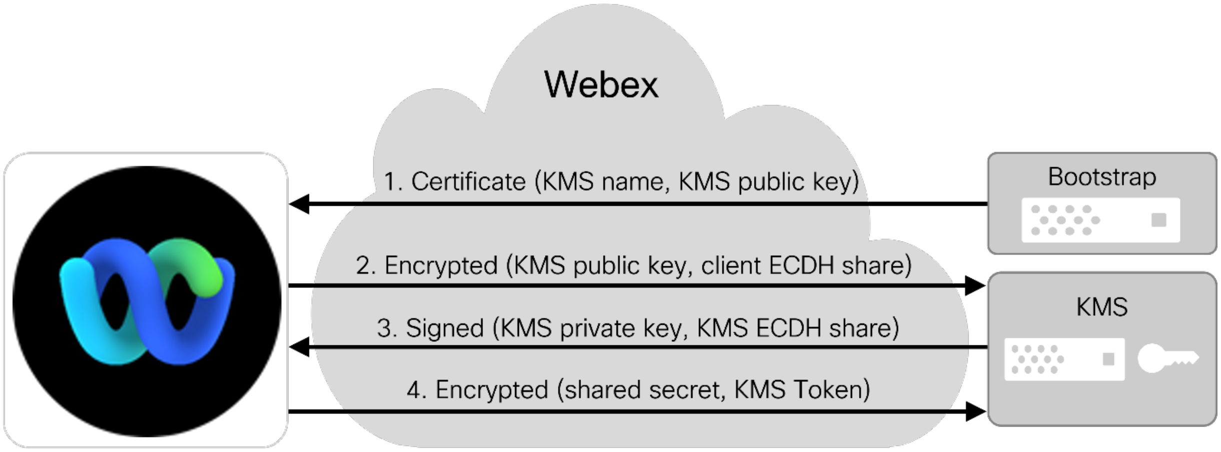

Webex
1. Certificate (KMS name, KMS public key)
Bootstrap
2. Encrypted (KMS public key, client ECDH share)
KMS
3. Signed (KMS private key, KMS ECDH share)
4. Encrypted (shared secret, KMS Token)

Figure 5. Secure Communication with KMS

Each encrypted item in Webex Messaging, such as, a message, or file, is tagged with a key URL that indicates what key can be used to decrypt it. When the Webex App needs a key, it requests it from its KMS. If the key's URL indicates that it is stored on another KMS, the requesting Webex App's KMS fetches it from that KMS on behalf of the Webex App. Each key has an associated access control list (ACL) that identifies the users that are allowed to access the key. Before granting access to a key, the KMS storing the key verifies that the requesting user is on the ACL. If it receives a request from another KMS, it also verifies that the requesting KMS is authorized to access the key.

To see how this all fits together, let's look at how two users, Alice and Bob, in different organizations can send messages to each other (see Figure 6). When Alice creates a conversation with Bob, Alice's Webex App gets a key for the conversation from KMS A (via an ECDH tunnel through the cloud). This also notifies KMS A that Bob is authorized (1). When Alice's Webex App creates the conversation with the Webex Messaging service, it also provides the key URL for the conversation, which the conversation service relays to Bob's Webex App (2). When Bob's Webex App joins the conversation, it requests the key from the KMS for Bob's enterprise (KMS B) (3). Bob's KMS sees that the key is stored on KMS A and forwards the request (4). KMS A checks that Bob's Webex App is authorized to receive the requested key and that KMS B is authorized to represent Bob. If these checks pass, KMS A provides the key to KMS B, which in turn provides it to Bob's Webex App. Bob's Webex App then uses the key to encrypt a message for Alice and safely send it to the conversation service in Webex (5), which will then store it and forward it to Alice's Webex App when it comes online (and likewise for any other participants in the space). Since Alice's Webex App has the same key, it can decrypt the message and display it.

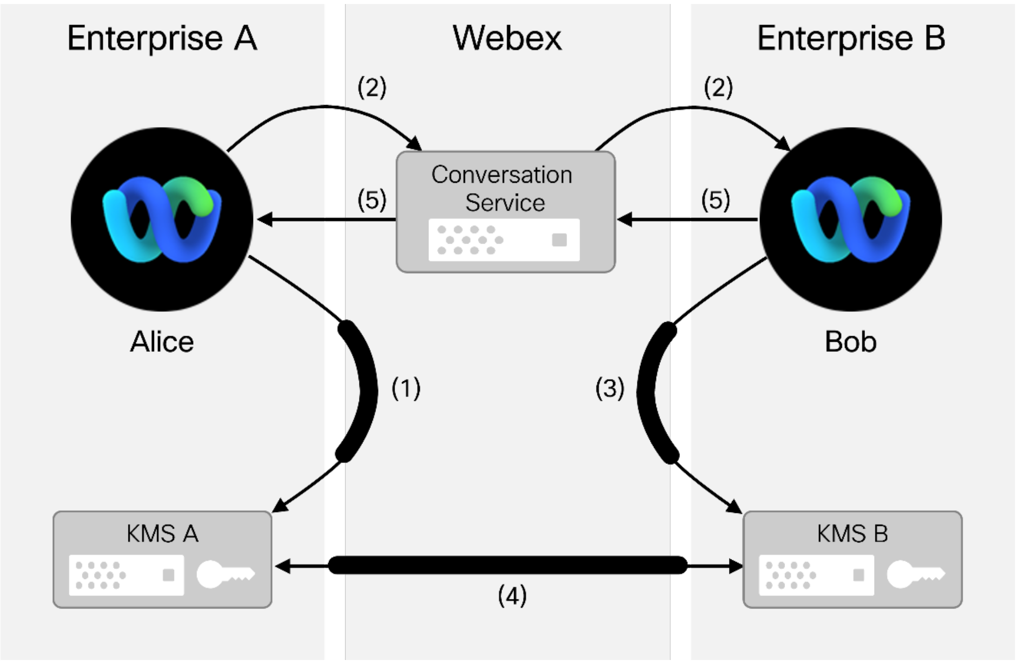


Figure 6. Secure Messaging with Webex Messaging Service

Files shared using the Webex Messaging service are protected in a similar way. As shown in Figure 7, when Bob wants to upload a file to a space, the Webex App generates a new key and uses it to encrypt the file. It then sends the encrypted file to a file storage service within the Webex cloud (1). To enable other Webex Apps in the space to download the file, Bob's Webex App constructs a message containing the key used to encrypt the file and a URL for the encrypted file. This message is then encrypted with the same key as other messages in the space and sent to the conversation service for propagation to other users in the space (2). When Alice's Webex App receives this special message, it can retrieve the encrypted file using the URL, decrypt it using the key, and display it (3).

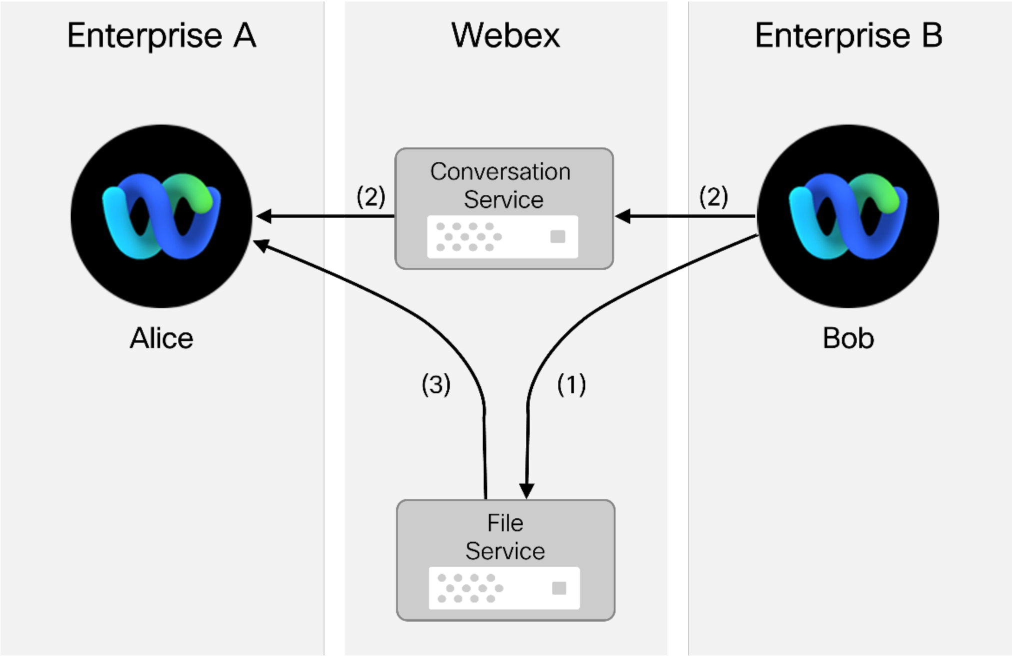


Figure 7. Secure File Sharing with Webex Messaging

When the access token's lifetime reaches 75% of its validity period (9 hours by default), the Webex App sends its refresh token to Webex authorization service to request a new access token and refresh token. The OAuth access and refresh tokens are securely stored in the application platform's OS and can be revoked by a Webex App administrator through the Reset Access option in Webex Control Hub or through the Authorizations API. These tokens can also be revoked by the end-users using their Webex App.

Controlling Access to Keys

In order to make sure that unauthorized parties cannot access the keys used for user generated content encryption, an organization's KMS keeps track of who is allowed to have each key. When a space is created, the KMS provisions a KMS Resource Object (KRO) that it uses to track the keys for the space and the people authorized to receive them (see Figure 8).

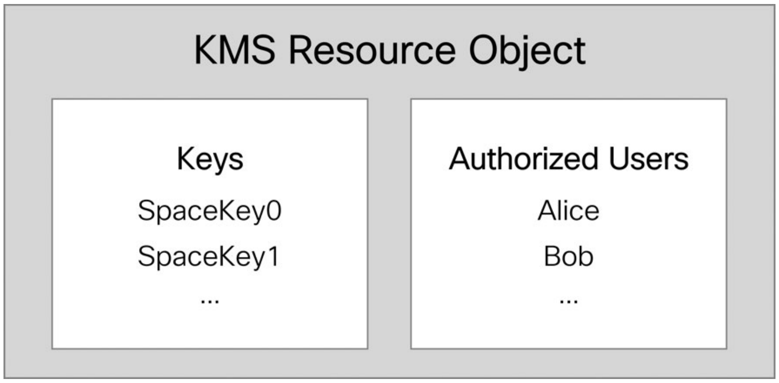


Figure 8. Structure of a KMS Resource Object

Each space has one key at any given time, which all participants in the space use to encrypt messages. When a user adds a new participant to a space, they also add the new participant to the corresponding KRO, so that the new participant can fetch the key. When someone leaves a space (or is removed), they are removed from the KRO.

Files are handled in a similar way. As discussed above, each file is encrypted with a separate key, which is sent alongside the URL to the file itself in an encrypted message. Since files are shared using messages encrypted for a space, a Webex App can only decrypt a file if it can access the keys for the space.

As a result of these mechanisms, the current participants in a space can download and decrypt any of the messages or files that were sent in the space, including ones sent before a given participant joined. Participants removed from the space are also removed from the KRO and will not be able to download any keys that were in use while they were in the space.

Feature Access to Keys

Certain Webex Messaging service features require a cloud service to have access to plaintext for content that would otherwise be encrypted. The current list of plaintext features is as follows:

- Document transcoding: Creates preview images from documents uploaded to a space so they can be viewed without the need to open the desktop application.
- API access: Allows bots and integrations to access space content without integrating with the KMS system. For example, Data Loss Prevention apps, which can monitor and manage all messages and files sent by users.
- IM & Presence Interoperability: Enables interoperation between Webex Messaging and some other messaging systems (for example, Cisco Jabber and Cisco Unified CM IM & Presence). Since these systems do not support KMS based encryption, the component providing interoperability needs to decrypt any encrypted content.

The following capabilities also require access to plaintext features, and it is possible for a customer to run these components on-premises.

- Search indexing: Creates an encrypted index of each posted message and file name that can safely be stored and searched in the cloud. Searching for these hashed terms, rather than plain text values, enables the global search of encrypted content without the need to decrypt it.
- eDiscovery: Enables searches on encrypted messages by compliance officers for compliance purposes
- Calendar connector: Enables meetings scheduled through Webex Messaging to automatically be reflected in a customers' calendaring system. (Meeting details are E2E encrypted using a KMS provided encryption key per meeting, connections to cloud and on premises calendar services are encrypted with TLS).

Suppose Enterprise A uses the Webex file transcoding service to provide document previews in spaces owned by the enterprise. As shown in Figure 9, when Bob posts a file into the space using the Webex App (1, 2), the transcoding service will get a notification of the upload, containing the encrypted message with the file URL and key (3). It can then fetch the key from KMS to decrypt this message (4), so that it can fetch the file (5) and decrypt it. After performing transcoding, the transcoding service will encrypt the resulting preview images and post them to the file service (6) and send a notification to the space (7). Other Webex Apps in the space can then fetch the preview image, decrypt it, and display it as they would any other file (8).

Note that decrypted customer content is only ever visible to the transcoding service and is never stored in the Webex cloud. Once transcoding is complete, the decrypted content is discarded.

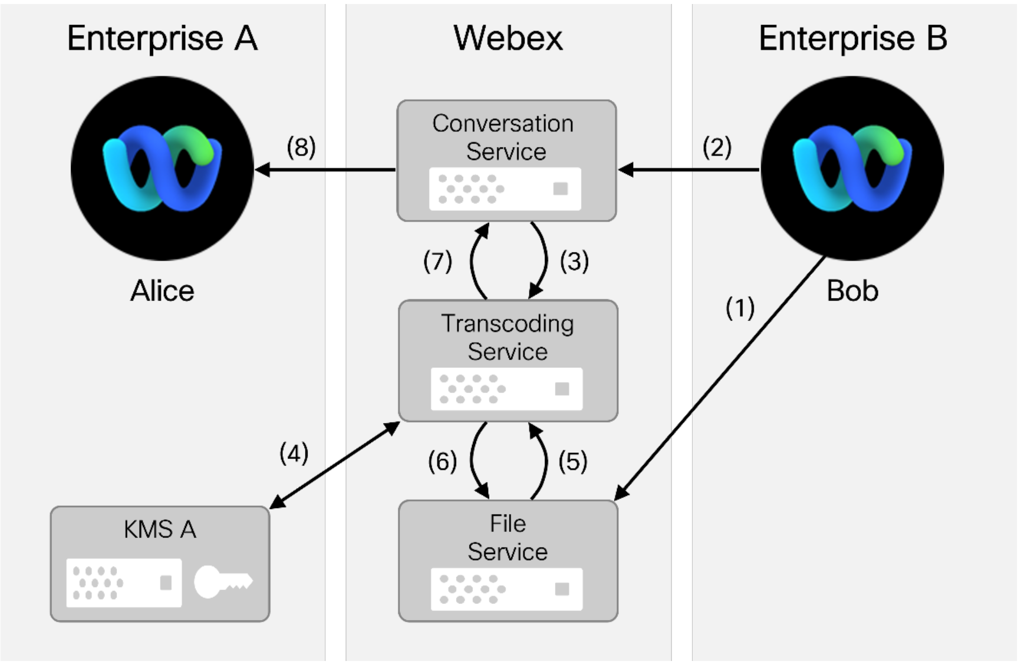


Figure 9. Key Access for Plaintext Services

If desired, a customer can open a service request to disable document transcoding in the Webex cloud.

8. Encrypted Search

One of the most frequently used features in any messaging system is search. A user can search through the history of the conversations in the Webex App as well as search to find people in the directory and local contacts, spaces, messages, files, meetings, and devices. A search can be broad, including but not limited to usernames, space names, message text, or can be refined with filters to narrow the results.

The scope of a search is limited to the organization a user belongs to and does not extend to people and spaces external to the user's organization, unless the user already had a conversation with those people, or the user is already part of those spaces. For example, a user can search for people within their organization. A user can search for spaces that they are already a member of, or spaces that are part of a team they are already a member of, or public spaces within their organization. But a user cannot search and find people that are outside of the organization unless they already had a conversation with the person. Also, a user cannot search for spaces in other organizations, even if they are public, unless they are a member of those spaces or a member of the teams to which those spaces belong.

Depending on the type of search and the data available locally, a search uses the local data on the user's device first, and then could reach out to the Webex Cloud to return more results.

Search in the Webex Messaging service is built so that when a user performs a search, existing message content in the Webex Cloud is not decrypted. Instead, the Search service builds a search index as the users send messages in the Webex App, by briefly decrypting the content of the encrypted messages and creating a corresponding one-way hash of each individual term in the message. This one-way hash is used to perform future search requests. This decrypted content is never stored. After that, Webex Apps can do searches directly against the search index and the messages do not need to be decrypted after this initial indexing process.

Webex eDiscovery also uses the same process to allow a compliance officer to search and retrieve user generated content.

There are two major steps in the search process: First, creating a search index as messages are sent, and second, performing queries using that index. Both steps are assisted by a Search Indexer service. Because this service requires access to plaintext, it is kept separate from the rest of the Webex Messaging service. With Hybrid Data Security (HDS), the keys will stay in the customer network so that when Webex performs indexing, no decrypted content will leave the customer network. The plaintext version of the messages is only briefly available in-memory and is not stored either in the customer network or in the cloud.

To build the search index, the Search Indexer service takes in a feed of every message sent within an organization. When a user sends a message in a space, the message is encrypted by the Webex App and then sent to the Webex Cloud. A copy is sent to the Search Indexer, which fetches the appropriate encryption key from its organization's KMS and decrypts the message. The Search Indexer then transforms the text of the message into a set of possible search terms, first breaking the message into individual words (tokenizing), filtering out non-relevant words (e.g., words with one or two characters), and then reducing each word to a root form (stemming). Using a search indexing key (search key) from the KMS, the Search Indexer then uses a hash-based message authentication code (HMAC) algorithm to transform each search term into an opaque value that represents the term. The HMAC transformation is one-way encryption – given a particular HMAC output value, there is no way to reverse it back to the word that appeared in the original message. After all these steps, the Search Indexer has an index entry that is safe to upload to the cloud, associating a given message with a set of values.

As shown in Figure 10, to perform a search, a Webex App sends its query to the Search Indexer in an encrypted string using the same encryption mechanism as when a user sends a message in a space. The Search Indexer then repeats the same process performed on the original message (decryption, tokenizing, filtering, stemming, etc.) to reduce the message to its constituent parts. However, before applying HMAC to the parts, the Search Indexer retrieves a list of spaces the user is part of and the corresponding search keys from the Webex Messaging service. The search keys are different for each space, adding a layer of security where the user can only perform a message search on the spaces of which the user is member. The search indexer then generates the HMAC value for each part in the query with each space's search key. If a user is a member of 10 spaces and types in a two-word search query, the Search Indexer will produce around 20 HMAC output values. The Search Indexer passes these values off to the Search Service in the Webex cloud, which can compare them to its encrypted index and inform the client about matching messages.

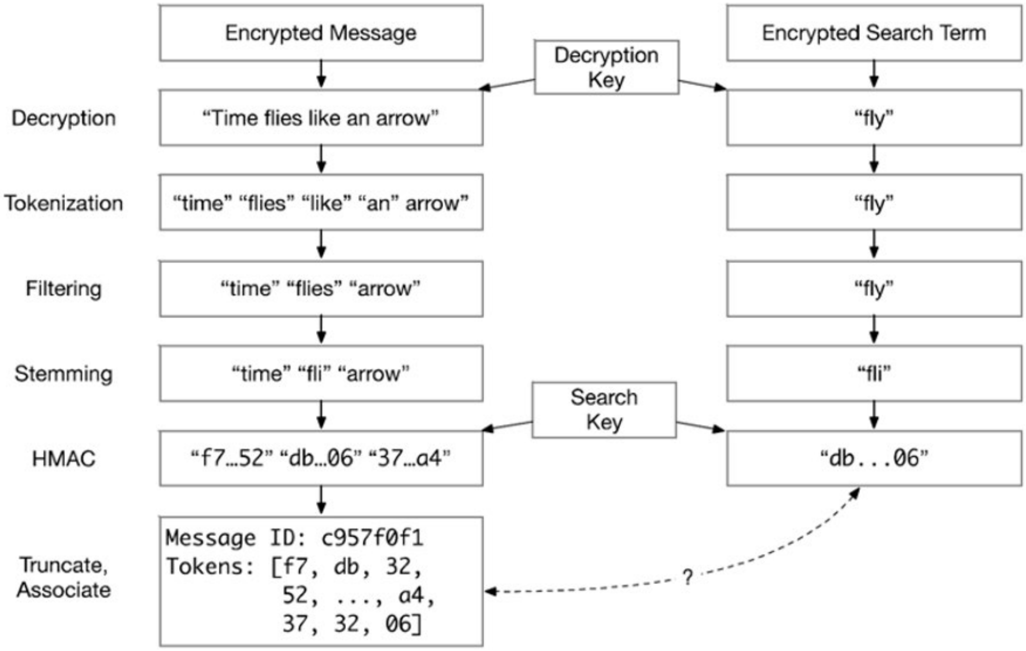


Figure 10. Encrypted Search in Webex Messaging

The search capability in the Webex Messaging service was built without sacrificing either security or user experience. While other cloud services need to decrypt user content in the cloud to provide search, Webex offers the same rapid search experience without the cloud ever needing to access user content.

9. Enterprise and User Privacy

The Webex Messaging service is designed to give both users and enterprises privacy choices without presenting complicated configuration interfaces. For enterprise administrators, these choices include:

- Single Sign-On (SSO): Administrators can configure Webex Messaging to work with their existing SSO solutions. We support identity providers using SAML 2.0 and OAuth 2.0.
- Directory synchronization: Administrators can have employee lifecycle changes reflected in the Webex cloud. Enterprise users can be synchronized to the Webex Identity Service using the Webex Directory Connector for customers using Microsoft Active Directory. The System for Cross-domain Identity Management (SCIM) protocol can also be used to synchronize user information from cloud identity repositories such as those in the Microsoft Azure Active Directory and Google cloud, or Okta.
- Enterprise privacy controls to comply with EU GDPR (EU General Data Protection Regulation) are detailed in the Webex App and Webex Messaging Privacy Data Sheet. These controls ensure that right to export, right to be forgotten, time-bound purges of user content, and other rights related to processing personal data are covered.

End-users have control of some features that relate to security. Below are some examples of those features.

- Space moderator control: Webex Messaging spaces can be moderated, allowing those participants chosen as moderators to have exclusive control of the space's title and participant list.
- External participant indicators: The Webex App makes it clear to users, through visual indicators, when a space contains participants that are not part of their enterprise organization.
- Further privacy controls are defined in the Webex App and Webex Messaging Privacy Data Sheet.

- Further compliance information on Webex Messaging can be found in the Control Hub Data Sheet.

Details about data collection and privacy for the Webex Messaging service can be found at the Cisco Trust Center.

Webex Calendar Service - Security

The Webex Calendar Service allows users to schedule Webex Meetings using on-premises (MSFT Exchange via Webex Calendar Connector) and cloud based (MSFT and Google) calendaring services. Connections to and from these on-premises and cloud calendaring services are secured with TLS. Within Webex, all personal data for each calendar scheduled Webex Meeting is E2E encrypted. Webex interacts with each external calendaring service as follows:

1. Webex reads the calendar invite and creates a Webex Meeting based on the scheduled meeting date, time, meeting title and listed invitees. This Webex Meeting instance is E2E encrypted using a unique KMS generated encryption key.
2. The E2E encrypted Webex Meeting information is stored in Webex.
3. The meeting instance in the external calendaring service is updated with the Webex Meeting information (Web join link, PSTN and SIP call in information (if enabled)).
4. For those invitees who have a Webex App or device, the Webex calendar service forwards the E2E encrypted meeting information to the application/device along with a link to the KMS encryption key for the meeting instance. The Webex App/device requests the meeting instance encryption key and decrypts and renders the meeting information so that it can be viewed in the Webex App, or on the Webex device.
5. The KMS generated meeting instance encryption key is rotated whenever significant changes are made to the meeting invite (e.g., attendees added or removed, date, time, or subject changed, etc.).

For more detailed information on calendar integrations see:

- Webex Hybrid Calendar Service with Microsoft Exchange Integration Reference
- Webex Hybrid Calendar Service with Office 365 Integration Reference
- Webex Hybrid Calendar Service with Google Calendar Integration Reference
- Deployment Guide for Webex Hybrid Calendar Service

10. Securing Webex Messaging Usage

Collaboration tools need to fit into an organization’s overall approach to operational security. The Webex Messaging service provides tools for administrators to manage usage of service to limit risk. Webex Messaging also works well with other tools that enterprises use to keep themselves safe, from firewalls and proxies to content management systems and data loss prevention applications.

Management of Content Shared through Webex Messaging

As enabling as information-sharing can be for an organization, it also presents risks. For example, the risk that confidential information will be shared inappropriately, or the risk that necessary content will not be accessible when needed for compliance purposes. Webex Messaging provides a suite of tools that allow enterprises to manage these risks, such as:

- Archiving and Retention: All Webex Messaging user content can be stored for a defined retention interval, after which it is deleted. This retention interval can be customized by an administrator. If one is not specified, a default retention interval is applied. The Webex Messaging service can also connect with external archival services.

- Compliance APIs for Data Loss Prevention (DLP): The Webex Messaging service supports publicly available APIs that can be used by (machine) accounts with the compliance officer entitlement to integrate with a DLP provider to identify policy violations and take remediation action.
- eDiscovery: The Webex eDiscovery console allows administrators with the compliance entitlement to search user generated content and extract relevant messages and files, as well as contextual data such as timestamps, space IDs and participants IDs.
- Enterprise Content Management (ECM): Webex also allows IT administrators the flexibility to enable Microsoft OneDrive, Google Drive, and Box as an ECM solution to their users, in addition to Webex existing built-in file sharing and storage. Users can share, edit, and grab the latest Microsoft OneDrive, Google Drive, and Box files right within Webex spaces, while files are kept safe, secure, and protected in ECM via the customer's existing DLP/CASB and anti-malware solution.

Extending Webex Messaging

The Webex Messaging service provides open APIs that enterprises can use to automate Webex Messaging and connect it with other services. There are three different ways to extend the Webex Messaging service:

1. Bots provide extended functionality for an entire enterprise. A bot must either create a space or be invited to it before it has access. Even within a space, a bot only has access to messages that reference the bot explicitly (with an @ "mention").

2. Integrations provide extended functionality for a single user, such as a personal assistant or document translation. Integrations have the same Webex Messaging capabilities that the associated user does – access to the same spaces, messages, files, calls, etc. An integration can be thought of as a cloud or server hosted application with no user interface and with some additional intelligence.

3. Webhooks are a way that bots or integrations can have the Webex Messaging service "call out" to external services when certain events happen. Webhooks are only provided with metadata that is already visible to the Webex Messaging service; they do not have access to KMS encrypted user generated content. For example, a user can set a webhook to be notified when there is a message in a space, and the webhook will only be informed that the message has been posted; information such as who sent the message and which space it was sent in, not the content of the message.

More information about Webex APIs can be found at https://developer.webex.com/.

In order to provide developers with APIs that are easy to learn and use, we do not require bots and integrations to explicitly integrate with the Webex Messaging KMS encryption system. Instead, developers can use a Webex Messaging SDK or the Webex Messaging API server.

Using the SDK is the more secure option. When developers use the Webex Messaging SDK, the SDK will handle all the work of integrating with the KMS encryption system – the SDK authenticates directly to the appropriate KMS and does all the encryption/decryption locally. Customers that use SDK-based bots and integrations only need to make sure that the code for the bots/integrations runs in a secure context.

In contexts where it's not possible to use the SDK, the Webex Messaging service also provides an API server that can handle KMS interactions and decrypt content on behalf of the bot or integration. When a bot or integration requests access to encrypted content (such as a message or file), the API server requests the necessary encryption key from the appropriate KMS, decrypts the content, and provides it to the bot or integration. It is up to the organization to decide whether to provide the integrations and bots access to the enterprise's content.

While we believe that Webex security is the best in the industry, every Cisco customer has different security requirements. The key to making this hybrid model work is customer choice. Customers can choose to use only the core Webex Messaging system or to extend it with bots and integrations. Webex was designed around well-documented, standards-based APIs which means that bots, integrations, and webhooks can all be developed by customers or third parties without permission from the Webex Messaging service.

Cisco also provides a collection of bots and integrations at https://apphub.webex.com.

With an open platform comes concerns around how to secure the enterprise's content from 3rd party integrations. Integrations management through Webex Control Hub allows an administrator to:

- Have visibility into available integrations.
- Monitor the usage of these integrations by their users.
- Have the capability to set an allow/deny policy for these integrations for specific users or all users.

A Webex Control Hub administrator can also enable specific or all bots.

Device and Browser Protection

In order to keep sensitive information shared through the Webex Messaging service private from local attackers, it's important for the devices that the Webex App runs on to be secure. Webex Messaging offers administrators several ways to assure the safety of their organization's Webex Apps, for example:

- Require that mobile devices are secured with a PIN
- Remotely wipe Webex Messaging content if a device is lost, or a user leaves the organization
- Automatically log out users of the web clients for Webex Messaging after a period of inactivity
- Automatically log out users of Webex Control Hub after a period of inactivity
- Prohibit file uploads or downloads, for example, from certain types of clients, external users in internal group spaces, internal users in externally owned spaces, or external IP networks.

Those functions are part of Webex and can be configured via Webex Control Hub. The Webex App can also be managed through Mobile Device Management (MDM) or Mobile Application Management (MAM) systems and has been verified to work with several MDM/MAM controls, and can provide features such as:

- Preventing screen capture
- Preventing copy/paste
- Local back-ups
- Remote wipe
- Requiring PIN lock

For more details on Webex App security and mobile device management, refer to the Webex App Security technical paper.

Predictable Network Footprint

Enterprises have an increasingly challenging balance to strike: They want the flexibility of cloud-deployed applications, but they also want the assurance of knowing what's going on in their networks. Webex Messaging is designed to meet both needs by having a network traffic profile that stays within defined boundaries. Those boundaries are broad enough to enable the flexibility that a cloud-deployed product needs but narrow enough to limit the risk that malicious traffic could fit within them.

Webex Messaging only sends two types of traffic: encrypted signaling and encrypted media. Signaling traffic uses HTTPS and WSS to communicate with Webex and run over TCP port 443 (TLS). Encrypted media traffic uses UDP and can fall back to TCP or TLS as a transport protocol (although, UDP is strongly recommended). Media packets are exchanged with Webex media servers located within specified IP ranges and a small set of destination port numbers. A full description of the network requirements for Webex Messaging can be found in the Network Requirements for Webex Services article.

11. Secure Webex Messaging

Webex Messaging incorporates a full suite of security mechanisms to ensure that it is safe from interference by outside actors. It has ubiquitous, high-grade encryption, so that data is protected in transit and at rest, in addition to the KMS based encryption discussed above. Webex engineering follows Cisco's industry-leading practices to reduce the likelihood of vulnerabilities in the Webex Messaging service, and to ensure that when vulnerabilities exist, they are found and fixed quickly.

Communications Security

All network communications in Webex Messaging are protected by the Transport Layer Security (TLS) protocol, using certificates from publicly trusted certificate authorities (CAs). This includes communication between Webex Apps and devices and the Webex cloud, communication among messaging services in the Webex cloud, and communication between the cloud and customer-hosted services in the security realm. This level of protection ensures that attackers in customer networks, transit networks, or cloud data centers cannot read, intercept, or modify Webex Messaging communications.

Communications between Webex Apps and the services in Webex cloud use an additional technique known as public key pinning. Public key pinning dramatically decreases the risk of server impersonation. Without pinning, any of the roughly 2000 publicly trusted CAs could issue a certificate that a bad actor could use to intercept Webex Messaging communications. Pinning isolates this risk to a handful of CAs that have been well vetted. In addition to verifying that the CAs Webex allows have strong security practices themselves, Cisco requires that these CAs commit that they will not delegate their signing authority to anyone else, since this would introduce a risk that the delegate's practices would not be up to Cisco standards. This commitment must be expressed in the issuer's Certification Practice Statement (CPS) and in the CA's certificate (by including "pathLenConstraint" set to zero).

Some customer network environments include security devices that impersonate TLS servers. These devices are sometimes known as "SSL inspection" devices or HTTP/TLS proxies. By default, these devices are incompatible with pinning, because the certificate the client sees is not from one of the approved CAs. The Webex App thus applies a more flexible pinning policy: They allow a TLS connection if the server's certificate is issued by a pinned CA, or if the certificate is issued by a CA that an administrator has installed on the host computer. Webex devices (including Desk series and Room series) can also be configured to trust a customer CA.

Encrypted Storage

In addition to encrypting data as it transits the network, the Webex Messaging service also applies encryption "at rest" to guard against the compromise of storage devices it relies on. For most Webex Messaging services, customer data is already encrypted using the KMS encryption techniques discussed above.

The Webex App also stores content such as, the user's credentials, messages, and file previews a user has received, Webex space details and their KMS based content encryption keys. The Webex App maintains this information in an encrypted database, then protects the database encryption keys using platform-provided APIs such as the Windows Data Protection API. If the device the Webex App is installed on is lost or stolen, the Webex Messaging service enables an administrator to remotely delete the device's cached data and log out the user. The browser-based Webex web app does not persist user data.

12. Cisco's Security Model

Cisco remains firmly committed to maintaining leadership in cloud security. Cisco's Security and Trust organization works with teams throughout the 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 Cisco does.

This organization is also dedicated to providing customers with the information they need to mitigate and manage cybersecurity risks.

The Webex security model (Figure 11) is built on the same security foundation deeply engraved in Cisco's processes.

The Webex organization consistently follows the foundational elements to securely develop, operate, and monitor Webex services.

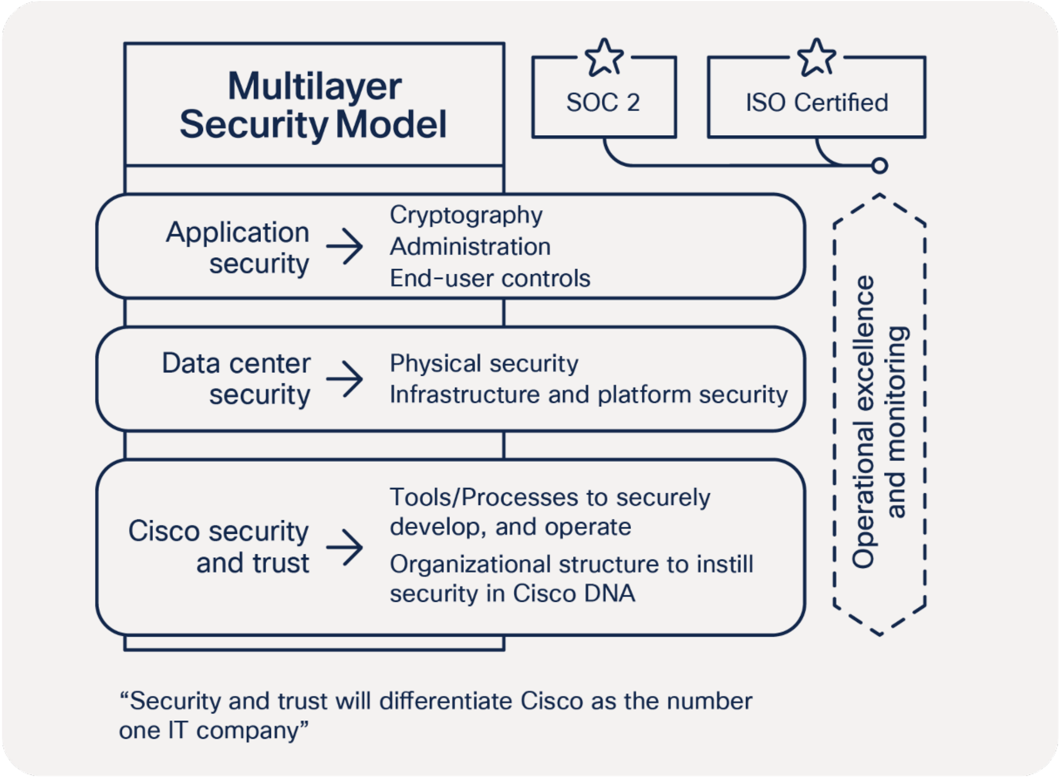

Multilayer Security Model
SOC 2
ISO Certified
Application security
Cryptography
Administration
End-user controls
Data center security
Physical security
Infrastructure and platform security
Cisco security and trust
Tools/Processes to securely develop, and operate
Organizational structure to instill security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

Figure 11. Webex Security Model

12. Webex Security and Trust

Cisco Security Tools and Processes

Cisco Secure Development Lifecycle (CSDL)

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 (CSDL). It is a repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products. The combination of tools, processes, and awareness training introduced in all phases of the development lifecycle helps ensure defense in depth. It also provides a holistic approach to product resiliency. The Webex Product Development team passionately follows this lifecycle in every aspect of product development.

For more information, refer to the Cisco Secure Development Lifecycle Overview.

Cisco Foundational Security Tools

The Cisco Security and Trust Organization provides the process and the necessary tools that give every developer the ability to take a consistent position when facing a security decision.

Having dedicated teams to build and provide such tools takes away uncertainty from the process of product development.

Some examples of tools include:

- Product Security Baseline (PSB) requirements that products must comply with
- Threat-builder tools used during threat modeling
- Coding guidelines
- Validated or certified libraries that developers can use instead of writing their own security code
- Security vulnerability testing tools (for static and dynamic analysis) used after development to test against security defects
- Software tracking that monitors Cisco and third-party libraries and notifies the product teams when a vulnerability is identified

Organizational Structure that Instills Security in Cisco Processes

Cisco has dedicated departments in place to instill and manage security processes throughout the entire company. To constantly stay abreast of security threats and challenges, Cisco relies on:

- Cisco Information Security (InfoSec) Cloud team
- Cisco Product Security Incident Response Team (PSIRT)
- Shared security responsibility

Cisco InfoSec Cloud

Led by the chief security officer for cloud, this team is responsible for delivering a safe Webex environment to customers. InfoSec achieves this by defining and enforcing security processes and tools for all functions involved in the delivery of Webex into customers' hands.

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

Cisco InfoSec is also responsible for continuous improvement in Webex's security posture.

Cisco Product Security Incident Response Team (PSIRT)

Cisco PSIRT is a dedicated global team that manages the inflow, investigation, and reporting of security issues related to Cisco products and services. PSIRT uses different mediums to publish information, depending on the severity of the security issue. The type of reporting varies according to the following conditions:

- Software patches or workarounds exist to address the vulnerability, or a subsequent public disclosure of code fixes is planned to address high-severity vulnerabilities.
- PSIRT has observed active exploitation of a vulnerability that could lead to a greater risk for Cisco customers. PSIRT may accelerate the publication of a security announcement describing the vulnerability in this case without full availability of patches.

- Public awareness of a vulnerability affecting Cisco products may lead to a greater risk for Cisco customers. Again, PSIRT may alert customers, even without full availability of patches.

In all cases, PSIRT discloses the minimum amount of information that end users will need to assess the impact of a vulnerability and to take steps needed to protect their environment. PSIRT uses the Common Vulnerability Scoring System (CVSS) scale to rank the severity of a disclosed issue. PSIRT does not provide vulnerability details that could enable someone to craft an exploit.
Refer to the PSIRT infographic to learn more about PSIRT.

Security responsibility

Although every person in Webex group is responsible for security, the following are the main roles:

- Chief security officer, Cloud
- Vice president and general manager, Cisco Cloud Collaboration Applications
- Vice president, engineering, Cisco Cloud Collaboration Applications
- Vice president, product management, Cisco Cloud Collaboration Applications

Internal and external penetration tests

The Webex group conducts rigorous penetration testing regularly, using internal assessors. Beyond its own stringent internal procedures, Cisco InfoSec also engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Cisco also uses third-party vendors to perform ongoing, in-depth, code-assisted penetration tests and service assessments. As part of the engagement, a third party performs the following security evaluations:

- Identifying critical application and service vulnerabilities and proposing solutions
- Recommending general areas for architectural improvement
- Identifying coding errors and providing guidance on coding practice improvements

Third-party assessors work directly with the Webex engineering staff to explain findings and validate the remediation. Penetration test letters of attestation for Webex services are available under NDA on the Cisco Trust Portal.

13. Data Privacy

Webex takes customer data protection seriously. Cisco collects, uses, and processes customer information only in accordance with the Cisco Privacy Statement and the Webex App and Webex Messaging Privacy Datasheet.

The Webex messaging service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements, including the EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA), Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA), Personal Health Information Protection Act (PHIPA), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA).

14. Transparency

Webex users and customers should understand what their choices are and how Cisco manages and protects the data they entrust to Cisco. Cisco uses a layered model of transparency to make this happen. Short disclosures that help users make real-time decisions are provided within the Webex App itself. Further information is available in support pages, which get updated on a regular basis. And for all the details of what information Cisco collects, how it is used, and how it is protected, refer to the Webex App and Webex Messaging Privacy Data Sheet.

Cisco is also committed to publishing data regarding requests or demands for customer data that are received from law enforcement and national security agencies around the world. Cisco publishes this data twice yearly (covering a reporting period of either January-to-June or July-to-December). Like other technology companies, Cisco will publish this data six months after the end of a given reporting period in compliance with restrictions on the timing of such reports.

More information can be found at in the transparency section of the Cisco Trust Center available at https://trust.cisco.com.

Cisco has also invested in several transfer mechanisms to enable the lawful use of data across jurisdictions, including:

- Binding Corporate Rules (Controller)
- APEC Cross-Border Privacy Rules
- APEC Privacy Recognition for Processors
- EU Standard Contractual Clauses

15. Industry Standards and Certifications

In addition to complying with our stringent internal standards, Webex also continually maintains third-party validations to demonstrate our commitment to information security. Webex has received the following certifications:

- ISO 27001, 27017, 27018 and 27701
- Service Organization Controls (SOC) 2 Type II
- SOC 3
- EU Cloud Code of Conduct Adherence by SCOPE Europe
- CAS CSTAR 2
- Cloud Computing Compliance Controls Catalogue (C5) attestation
- FedRAMP (visit https://cisco.com/go/fedramp for more details)

  Note: FedRAMP certified Webex service is only available to U.S. government and education customers.

16. Conclusion

Be collaborative and get more done, faster, using the Webex App. Webex is a trusted industry leader in web and video conferencing, messaging, and calling. 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. Cisco connects everything more securely to make anything possible.

17. How to Buy

To view buying options and speak with a Cisco sales representative, visit How to Buy Cisco Products.

18. For More Information

Webex Messaging

December 2022