



Webex Teams Tech Ops and Security – Frequently Asked Questions (FAQs)

First Published: October 31, 2017

Last Updated: October 16, 2019

Question: Can Cisco provide a detailed architectural diagram of the Cisco Webex Teams service?

Answer: No.

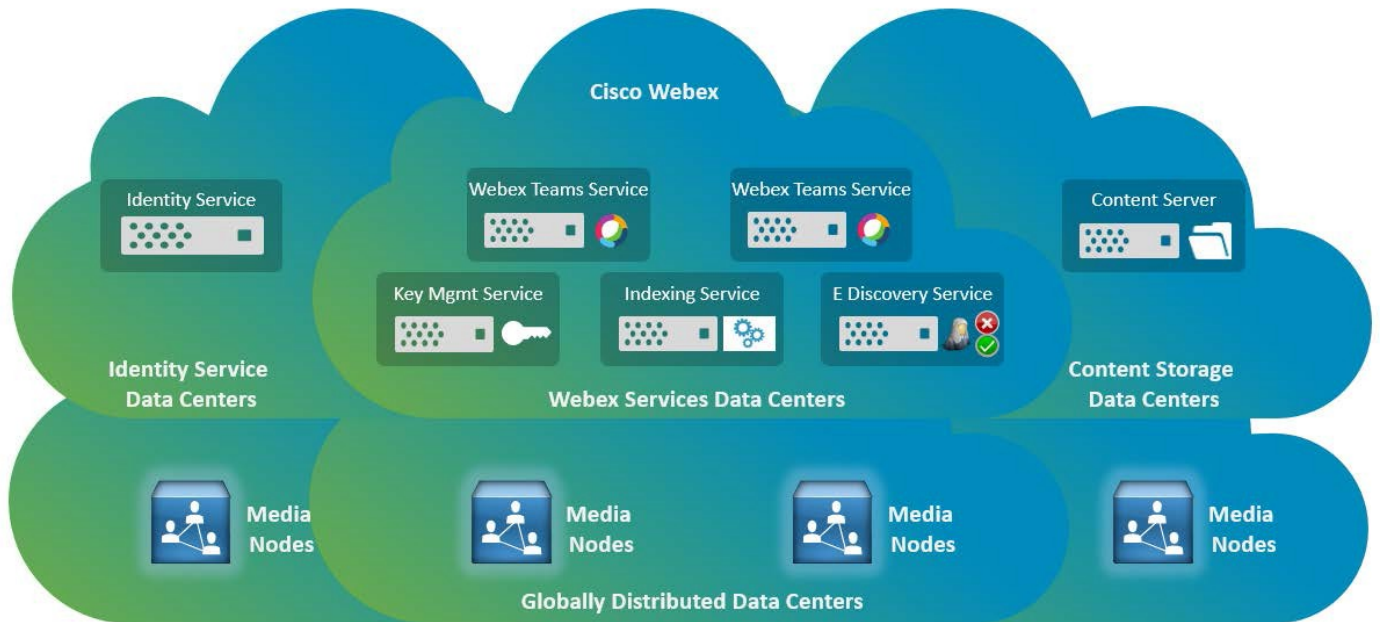
For security reasons, Cisco does not provide detailed architectural diagrams and data flows for Webex Teams services. An overview of the Webex Teams service architecture is described below.

Webex Teams uses services that are located in several data centers as shown in Figure 1. The services within these data centers can be broadly categorized as follows:

- **Identity Services**
Storage of user identities, user authentication, single sign on, and directory synchronization
- **Webex Teams Micro Services**
Encryption key management, message indexing services for search functions and eDiscovery services, signaling services for Webex Teams apps, Webex devices, and API functions
- **Content Services**
Storage and retrieval of user-generated content such as messages and files
- **Media Services**
Media nodes for switching and transcoding for voice, video, and screen sharing content
- **Anonymized Data Collection and Analytics Services**
Critical Webex Teams services are replicated across data centers for geographical redundancy. Within each data center, these Webex Teams services are hosted on virtual machines (VMs). These VMs can be moved for support and maintenance purposes, or new virtual machines can be installed as services expand.
Webex Teams data centers and services undergo regular penetration testing by external agencies. We can provide attestation documents that describe the results of these penetration tests to customers who sign nondisclosure agreements (NDAs).

For more details on data center locations and how the Cisco Webex Service processes personal data, see https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

Figure 1: Webex Teams Cloud Service Architecture Overview



Question: Which URIs, IP addresses and port ranges must be whitelisted at a proxy/firewall to use the Webex Teams service?

Answer: You can find this information in the *Network Requirements for Webex Teams Services* article here: <https://help.webex.com/article/WBX000028782>

Question: Do all audio/video calls transit through the Webex Teams data centers?

Answer: Typically, audio and video from Webex Teams or Webex device transits from the user's location to media nodes in the Webex cloud. This is true for all call types (such as 1:1 calls and multiparty calls or meetings.) All audio and video media streams are sent over the Secure Real-Time Transport Protocol (SRTP) using AES_CM_128_HMAC_SHA1_80 encryption.

We recommend UDP as the transport protocol for Webex Teams media, although most Webex Teams and Webex devices support TCP and HTTP (apps only) as a fallback protocol. TCP and HTTP are not recommended as media transport protocols because they are connection orientated and designed for reliability, rather than timeliness. Using HTTP can also mean that media traffic must pass through a proxy server to reach media servers in the Webex cloud. Media quality can be impacted if the proxy server reaches a performance threshold when processing large numbers of high bandwidth video streams.

Internet Access for cloud-based services

As enterprise customers increase their adoption of cloud-based services, the amount of internet traffic generated by enterprise users also increases. Today, the ratio of the cost of enterprise WAN bandwidth (e.g. MPLS) to that of internet bandwidth, can be as much as 200:1. Moving your cloud/internet access to sites where your cloud users reside can provide significant savings in monthly bandwidth costs. Although

this direct internet access model is growing in popularity, many customers who deploy a centralized/regionalized internet access model today have concerns that provisioning internet access in each of their sites will perforate the security perimeter that surrounds their network. These security concerns can be addressed by limiting internet access in these sites, so that only traffic to and from approved cloud-based services is accessible via the site-based internet connection.

Our recommendations for Webex cloud access from the enterprise:

Provision internet access as close as possible to the site where your Webex Teams and Webex devices reside. By providing local cloud/internet access at each site for Webex devices, you can eliminate the need to transport Webex Teams traffic over the enterprise WAN to a regionalized/centralized internet access point.

Figures 2 & 3 below show the media flows for Webex Teams deployments with per-branch internet access and centralized internet access.

Figure 2: Media Paths for Webex Teams Deployments with per Branch Internet/Cloud Access (Recommended)

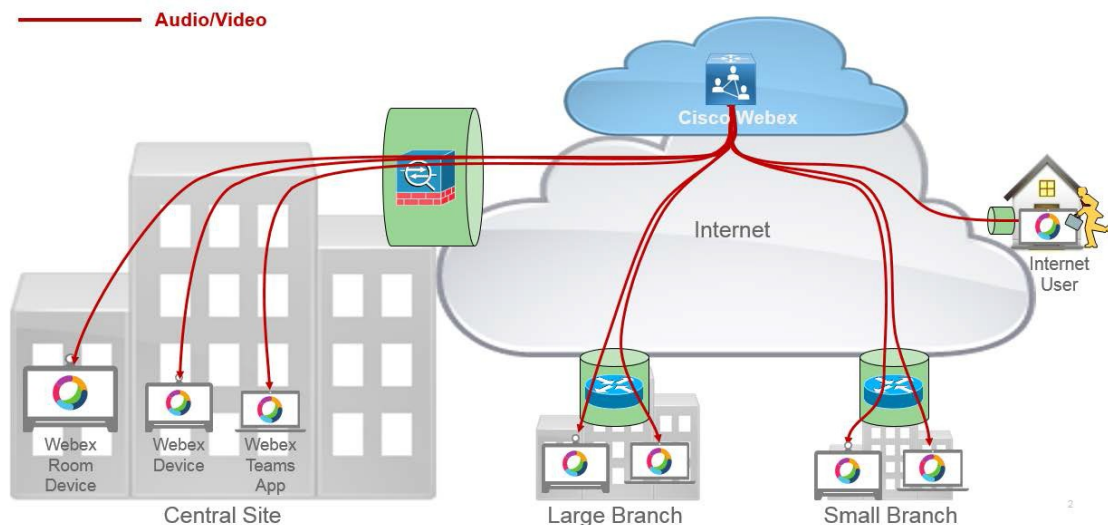
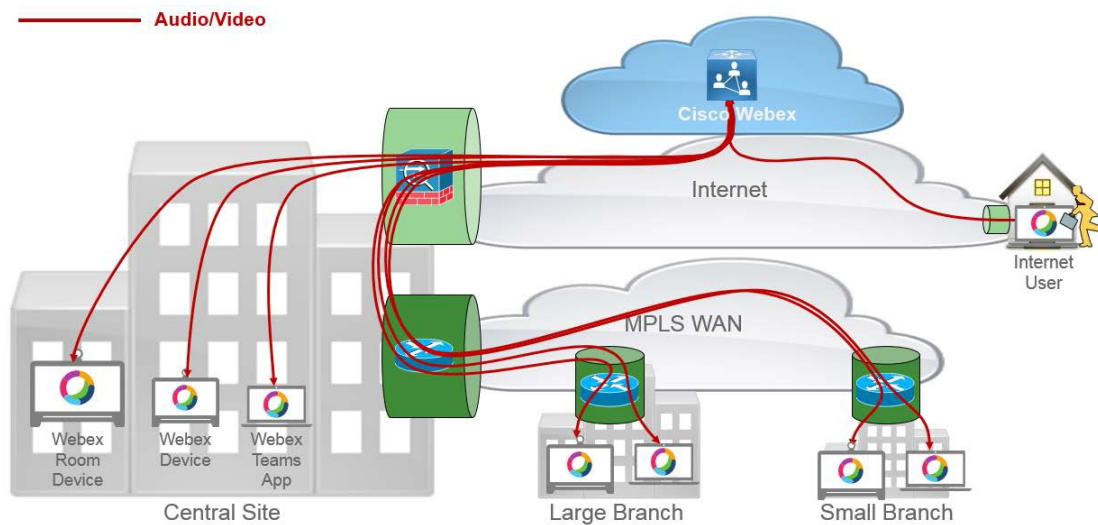


Figure 3: Media paths for Webex Teams Deployments with Centralized Internet/Cloud Access



Reducing traffic to the Webex Cloud by deploying Video Mesh Nodes

Deploy Video Mesh Nodes in the enterprise network to provide local media processing. By processing audio and video media locally, the Video Mesh Nodes deliver a better quality experience for audio, video, and content sharing in meetings. A Video Mesh Node can also reduce or eliminate bandwidth consumption from the enterprise network to the Webex cloud. Webex Teams also provides automatic overflow to Media Nodes in the Webex cloud when large meetings/large numbers of meetings exhaust the locally available Video Mesh Node resources.

Figures 4 & 5 below show the media flows for Webex Teams deployments with per-branch internet access and centralized internet access, where a Video Mesh Node has also been deployed at the central site to provide local media processing. The Video Mesh Node processes media for local devices in meetings and, if needed, creates a cascade link to a Media Node in the Webex cloud for remote meeting participants.

Figure 4: Media Paths for Webex Teams Deployments with a central site Video Mesh Node and per-branch Internet Access (Recommended)

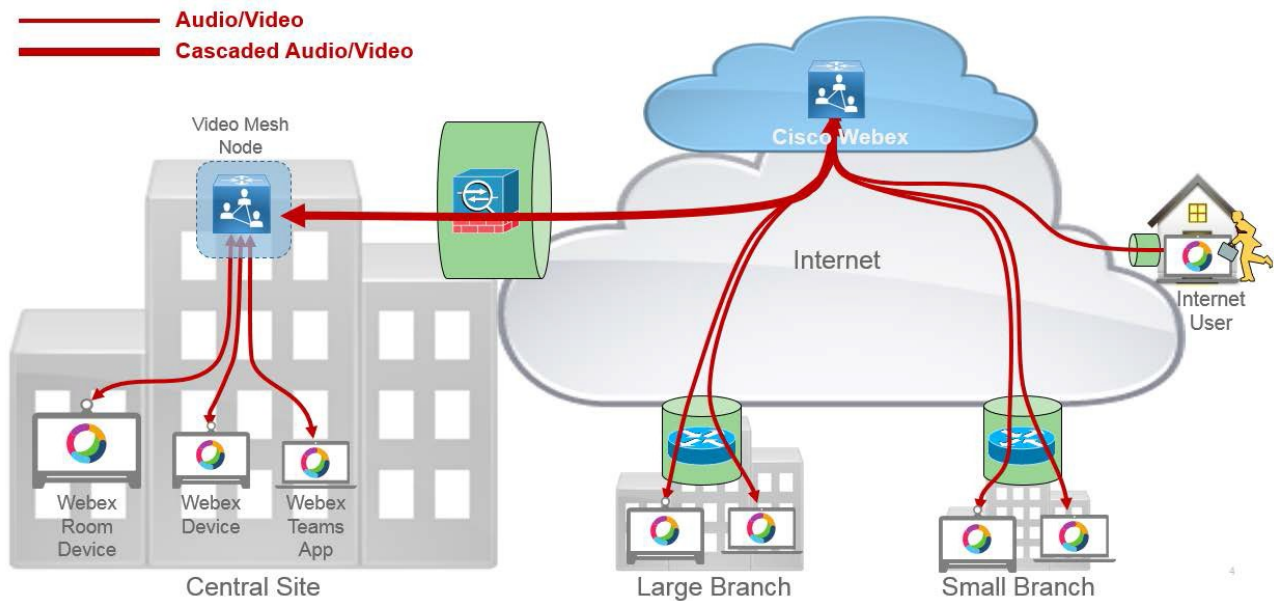
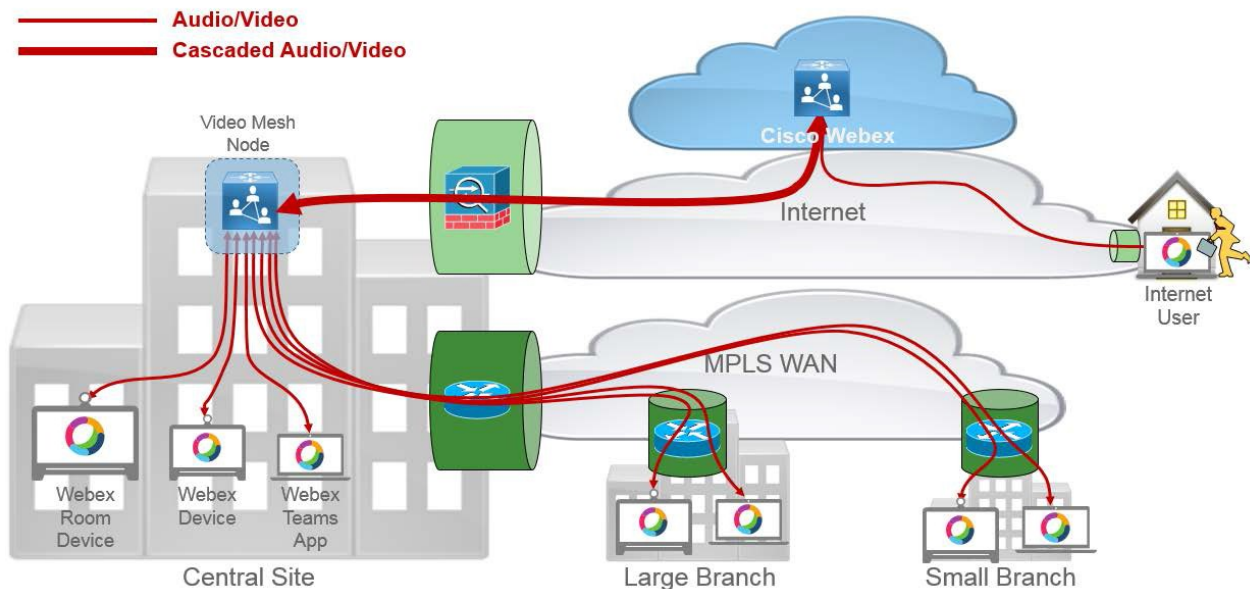


Figure 5: Media paths for Webex Teams Deployments with a central site Video Mesh Node and centralized Internet Access



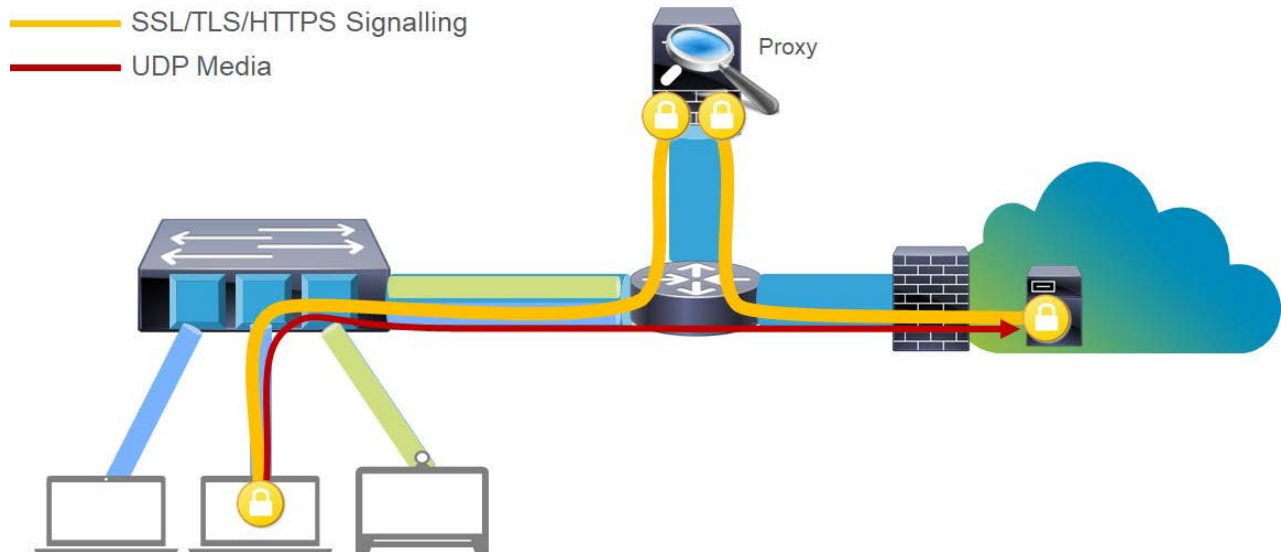
Question: Can the Webex Teams media be encrypted using customer provided encryption keys?

Answer: No, encryption keys for media are generated by each Webex Teams app or device and the Webex Teams media server that they communicate with. Encryption keys are securely exchanged over TLS. Cisco secures all Webex Teams media streams using the Secure Real-Time Transport Protocol (SRTP), described in RFC 3711. Cisco apps and devices encrypt media with the AES_CM_128_HMAC_SHA1_80 cipher suite.

Question: Does Webex Teams support SSL/TLS/HTTPS inspection?

Answer: Yes

Figure 6: SSL/TLS/HTTPS signaling inspection by a proxy server



SSL/TLS/HTTPS inspection allows Enterprise Proxies to:

- Decrypt internet bound traffic
- Inspect the traffic
- Re-encrypt the traffic before sending it on to its destination.

The signaling traffic from Webex devices use TLS for session encryption. Within a Webex Teams TLS session, messages and content, such as files and documents are also encrypted, so SSL/ TLS/ HTTPS inspection has limited value because these messages and files cannot be decrypted and inspected. Some information is visible in the decrypted TLS session, such as API calls, obfuscated user IDs (such as a Universally Unique User Identifier (UUID), a 128-bit random value that represents the Webex Teams user ID), and so on.

Webex Teams apps and Webex devices use certificate pinning to verify that they are connecting to Cisco's Webex service and to ensure that the session data is not intercepted, read, or modified while in transit. SSL/TLS/HTTPS inspection is a form of man-in-the-middle (MITM) attack. For a description of certificate pinning, see https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning

Cisco pins server certificates to a few root Certificate Authorities (CAs) that have committed to not issue intermediate certificates through both the issuer's Certification Practice Statement and the root certificate containing a "pathLenConstraint" field in the Basic Constraints extension which is set to zero (0) to indicate that no CA certificates can follow the issuing certificate in a certification path. This means that, ordinarily, Webex apps will not accept an impersonation certificate sent by a proxy for SSL inspection.

- **SSL/TLS/HTTPS Inspection for Webex Teams Desktop Apps**
The Webex Teams apps rely on the certificates installed in the underlying OS Trust store to bypass the Webex Teams certificate pinning process. If the enterprise CA certificate exists in the OS Trust store, the Webex Teams app will trust certificates signed by the enterprise CA, when presented to it by the proxy server. This bypasses the certificate pinning process used by the Webex Teams app and allows a TLS connection to be established to the proxy server.
- **SSL/TLS/HTTPS Inspection for Webex Teams Devices**
The Webex Teams devices download a list of trusted certificates during the onboarding process. To include your Enterprise CA certificate into the device trust list for your organization, open a Service Request with Cisco TAC.

For details on Webex Teams app and device support for SSL/TLS/HTTPS inspection, see the *Network Requirements for Webex Teams Services* article here: <https://help.webex.com/article/WBX000028782>

Question: What proxy types does Webex Teams support?

Answer: Webex Teams apps and Webex devices support standard HTTP/TLS Proxies – for more information on the features supported by Proxy devices, see the *Network Requirements for Webex Teams Services* article here: <https://help.webex.com/article/WBX000028782>

Question: How does Webex Teams use Certificates?

Answer: We use certificates to allow Webex Teams apps and Webex devices to identify and authenticate the Webex Teams services that they connect to. Webex Teams apps and Webex devices use certificate pinning to verify their connections to the Webex cloud, thus ensuring that communications are not intercepted, read, or modified while in transit.

Webex Teams servers use certificates from root CAs that have committed to not issue intermediate certificates through both the issuer's Certification Practice Statement and the root certificate containing a "pathLenConstraint" field in the BasicConstraints extension set to zero (0) to indicate that no CA certificates may follow the issuing Certificate in a certification path.

Certificates are also used by the Hybrid Data Security nodes for KMS federation. KMS federation is explained in detail in the Webex Teams security and privacy white paper see: <https://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/cloud-collaboration/cisco-spark-security-white-paper.pdf>

Question: What is the hashing algorithm and key size used for Webex Teams certificates?

Answer: For Webex Teams certificates:

- The signature algorithm uses SHA-256 hashing with RSA
- The Public Key Pin uses the SHA-256 hashing algorithm
- RSA keys use a key size of 2048 bits

Question: Is SRTP traffic stored/cached when decrypted?

Answer: No, Webex Teams does not store or cache media. All media in Webex Teams, such as voice, video, and screen share, is encrypted using the Secure Real-Time Transport Protocol (SRTP). Webex Teams decrypts real-time media for mixing, distribution, and public switched telephone network (PSTN) trunk access.

Question: Can we restrict the access to certain regions based on IP ranges or domains?

Answer: Filtering Webex Teams signaling traffic by IP address is not supported as the IP addresses used by Webex Teams are dynamic and may change at any time. For details of the IP subnets used for Webex Teams media traffic, see the *Network Requirements for Webex Teams Services* article here: <https://help.webex.com/article/WBX000028782>

Question: What are the STUN servers associated to the service?

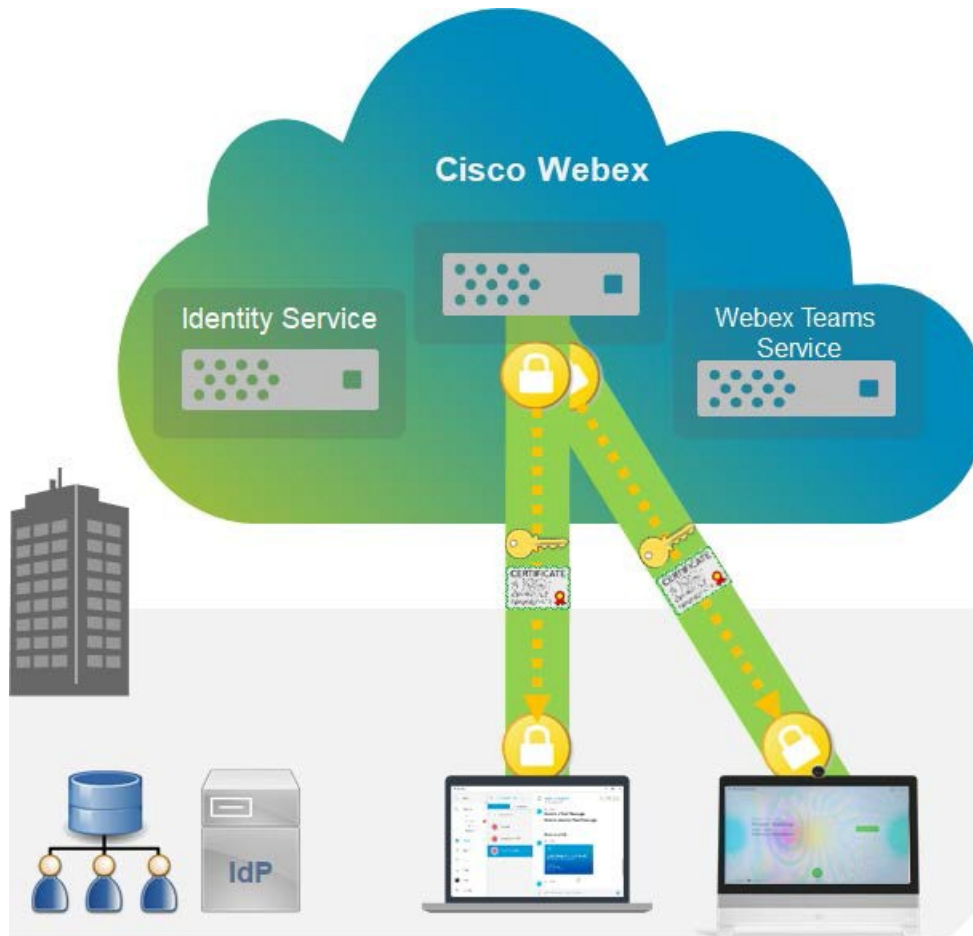
Answer: There are no separate STUN servers associated with the Webex Teams service; Webex Teams and devices use ICE, but do not gather server reflexive or relay candidates. There are STUN connectivity checks from Webex Teams to the Webex cloud; these are directed to the IP addresses of the media nodes which are publicly reachable. Thus, there are no DNS SRV records for STUN servers in the Webex cloud. For more details on how STUN is used by the Webex Teams service, see: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/whitepapers/cisco-spark-firewall-traversal-white-paper.pdf

Question: How does Webex Teams protect data in transit?

Answer: Webex Teams uses the following mechanisms to protect data in transit:

- All signaling connections from Webex Teams and Webex devices are protected using an encrypted TLS session. TLS cipher suites use 256-bit, or 128-bit symmetric cipher key sizes, and SHA-2 family hash functions. TLS cipher suites using 256-bit symmetric cipher keys are preferred, for example: TLS_EDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- Only TLS version 1.2 is supported.
- Webex Teams TLS servers also support TLS_FALLBACK_SCSV (<https://datatracker.ietf.org/doc/rfc7507/>) to prevent TLS version downgrade attacks.
- All messages and content (files) sent by Webex Teams are encrypted before they are sent over the TLS connection. Encrypted messages and content sent by the Webex Teams use AES_256_GCM Encryption Keys
- Media streams (voice, video and screen share) from Webex Teams and devices are encrypted using SRTP with AES_CM_128_HMAC_SHA1_80 ciphers. SRTP ciphers are negotiated using SDP. For more information, see <https://tools.ietf.org/html/rfc4568>

Figure 7: TLS Connections from Webex Teams and Webex Devices to the Webex Cloud



Question: Can a Webex Teams organization only accept connections from devices using TLS 1.2?

Answer: Webex Teams and Webex devices make outbound connections only to the Cisco Webex cloud. Webex Teams services only support TLS versions 1.2.

Webex Teams supports the TLS Fallback Signaling Cipher Suite Value (SCSV) feature, which is used to prevent TLS version downgrade attacks, by indicating to the TLS server that the connection should only be established if the highest TLS version supported by the server is equal to, or lower than, that received by the app.

Question: Is the Unique User Identity (UUID) encrypted in transit?

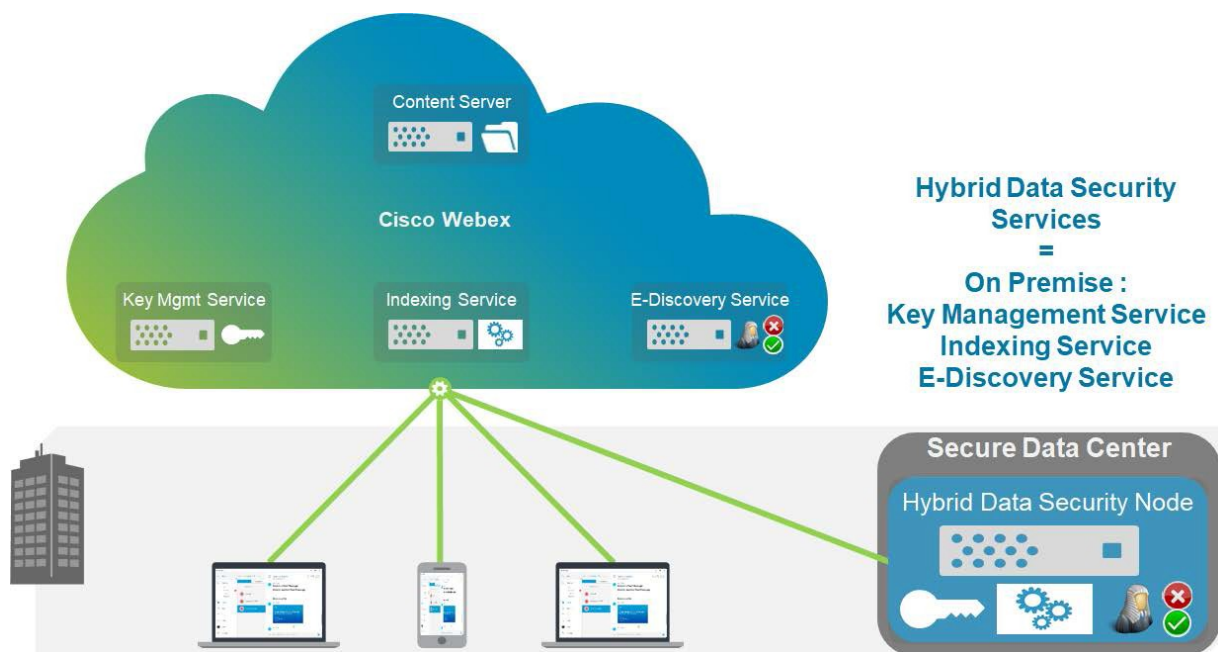
Answer: Yes, all Webex Teams data in transit (including the UUID) is encrypted using Transport Layer Security (TLS).

Question: Because content is currently stored in the United States only, what is our security story for non-U.S. customers?

Answer: By default, all encrypted files and encrypted messages sent by Webex Teams to the Webex Teams Service are stored in U.S. data centers. The encrypted files and messages are stored in an encrypted database that is replicated for redundancy. For files, customers can choose to deploy an Enterprise Content Management service, such as Microsoft OneDrive or SharePoint Online for Webex Teams file storage and distribution.

Any customers who are concerned about Cisco storing their message and file encryption keys and content, can choose to deploy an on-premises (encryption) Key Management Server (KMS), which is a component of the Webex Hybrid Data Security platform. The KMS controls and manages the encryption keys for content stored in Webex data centers. Encryption keys for content are created, distributed and stored on the customer's premise. KMS has a secure (TLS) connection to the Webex cloud and can distribute keys to Webex Teams over a dedicated TLS connection between the KMS and Webex Teams. As shown in the following figure, the on-premises KMS service can run on one, or more Hybrid Data Security nodes in your data center.

Figure 8: On-Premises Hybrid Data Security Services



When Hybrid Data Security Nodes are deployed in the customer premises, encrypted files and content are stored in Webex Teams data centers while their encryption keys are stored and managed locally.

To read any file, or message sent to the Webex cloud, two pieces of information are required:

- The encrypted file, or message
- The encryption key used to secure it.

All customer data within Webex Teams is encrypted and is inaccessible to Cisco personnel without authorization. Attempts to access encrypted customer content without authorization by any employee would be a violation of Cisco policy, would be investigated, and the employee would be subject to disciplinary action up to and including termination of employment.

If government agencies, request any customer data from Cisco, we take an open and transparent approach, including the steps outlined here <https://www.cisco.com/c/en/us/about/trust-center/transparency.html> to protect our customers' interests.

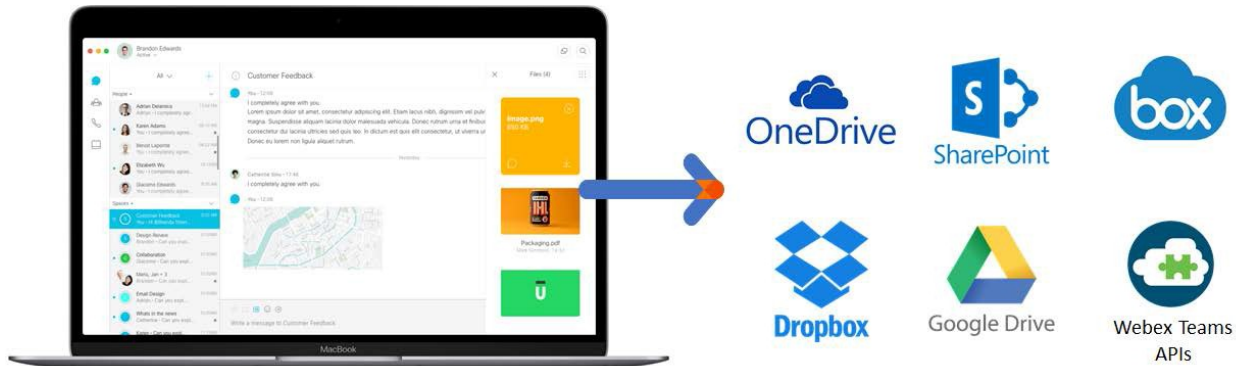
Question: Can I archive content?

Answer: By default, all content (messages and files) sent to Webex Teams spaces is securely stored in Webex Teams data centers. Using Webex Teams APIs, customers have the option to archive a copy of this content with a third-party data archival company. For example, Actiance, Global Relay, or Verint Verba. Customers can retrieve and store content on their own archival system.

Question: Can I store and manage files shared by Webex Teams outside of the Webex cloud?

Answer: Cisco has developed a Webex Teams API framework that allows enterprise customers to store all their files with their preferred Enterprise Content Management (ECM) provider instead of in the Webex cloud. For example, OneDrive, Box, or Google Drive. Customers can also use the API for Enterprise Content Management to store files within their enterprise network. For more information, see the *Connect Cisco Webex Teams to Microsoft OneDrive and SharePoint Online* article here: <https://help.webex.com/article/nuz39yeb>

Figure 9: Webex Teams API for Enterprise Content Management



Question: Does ECM include the storage of Webex board files?

Answer: This is not supported now. However, we plan to support creating an ECM specific folder in a Webex Teams space for whiteboard files.

Question: With ECM integration to Webex Teams, how is file version control implemented?

Answer: File version control is maintained by the ECM application. Webex Teams use Microsoft standard Graph API for ECM integration to Microsoft OneDrive or SharePoint Online. For more information, see <https://docs.microsoft.com/en-us/onedrive/developer/rest-api/?view=odsp-graph-online>.

Question: How long are messages stored on the Webex Teams Indexing Service?

Answer: The Webex Teams Indexing Service enables rapid searches of messages, files (filenames), people (usernames) and places (space names and team names) by Webex Teams users.

Typically, the Webex Teams Indexing Service resides in the Webex cloud (Figure 10), but it can also be deployed on a customer's premises as a component of the Hybrid Data Security Service (Figure 11). This service parses, stems, and hashes terms in all messages and filenames in spaces, as well as usernames and space names to create a series of hashed indexes. These hashed indexes are stored in the Search Service in the Webex cloud. Indexing takes place for each message and file (name) posted by a Webex Teams user. Indexing involves decrypting the posted content, followed by the indexing process. Decrypted messages and filenames are deleted immediately after the indexing process is completed. User search requests use the Search service in the Webex cloud to find either content in spaces and team spaces that the user is a member of; or names of other users and spaces.

Figure 10: Webex cloud-based Indexing and Search Services

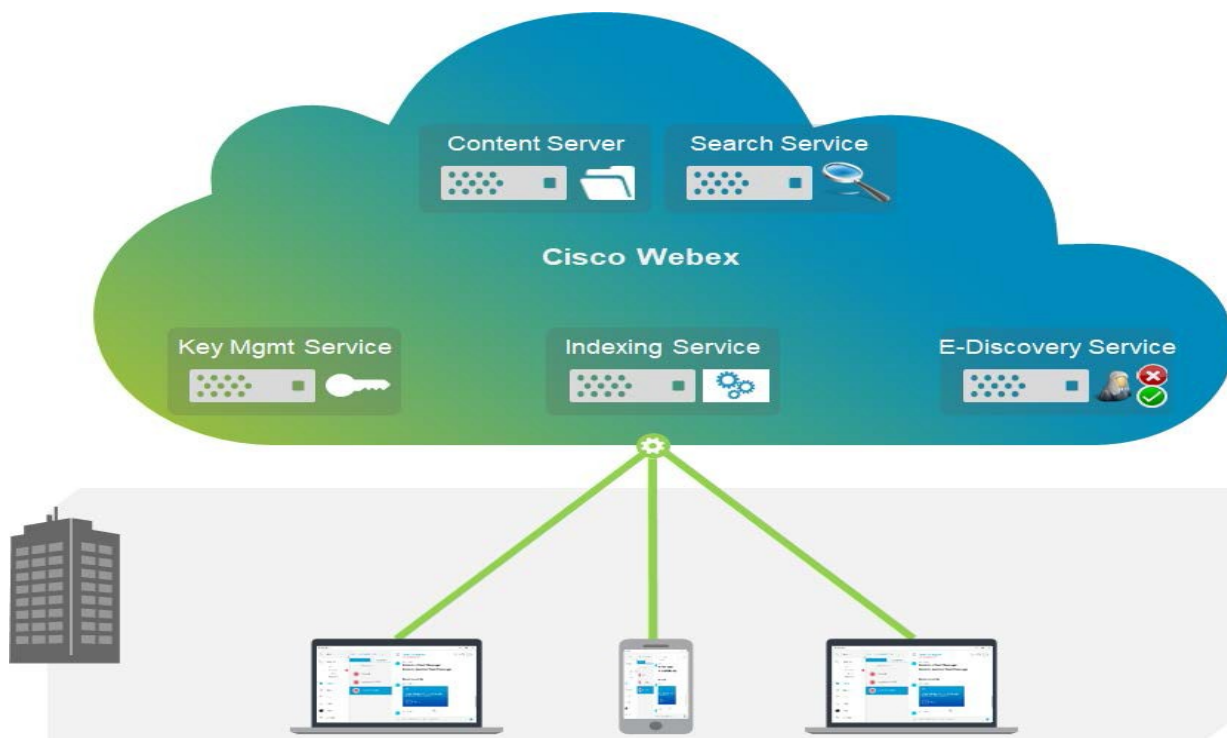
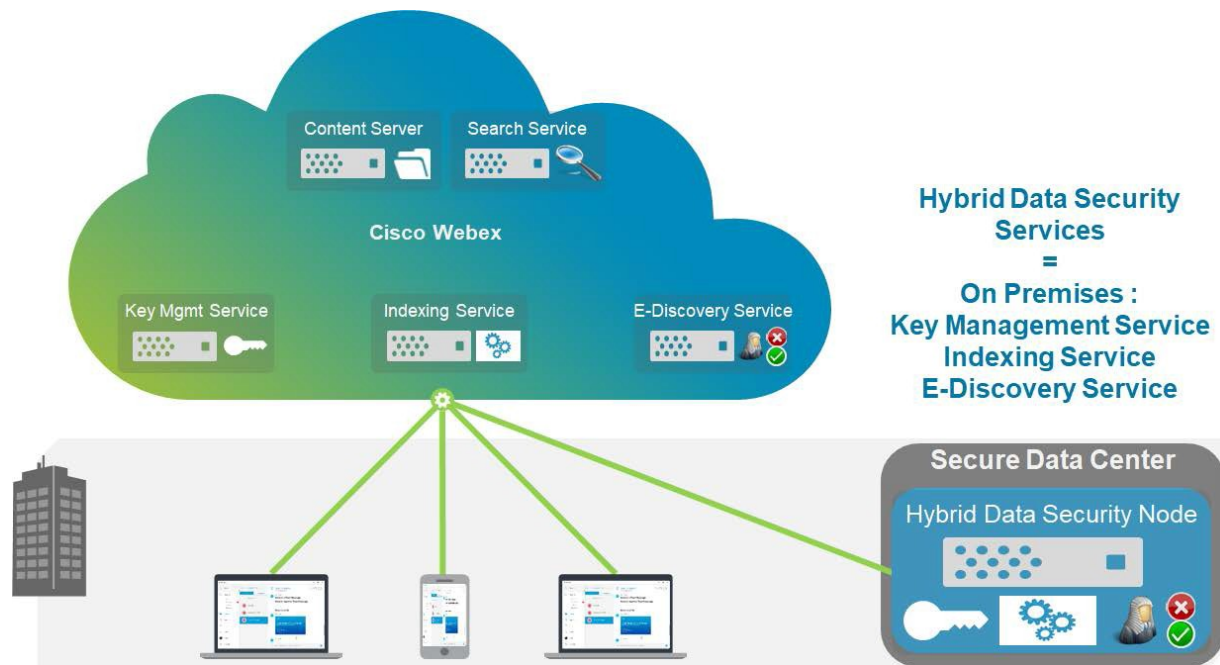


Figure 11: Customer Premises–Based Indexing and Search Services for Webex Teams Hosted on a Hybrid Data Security Node



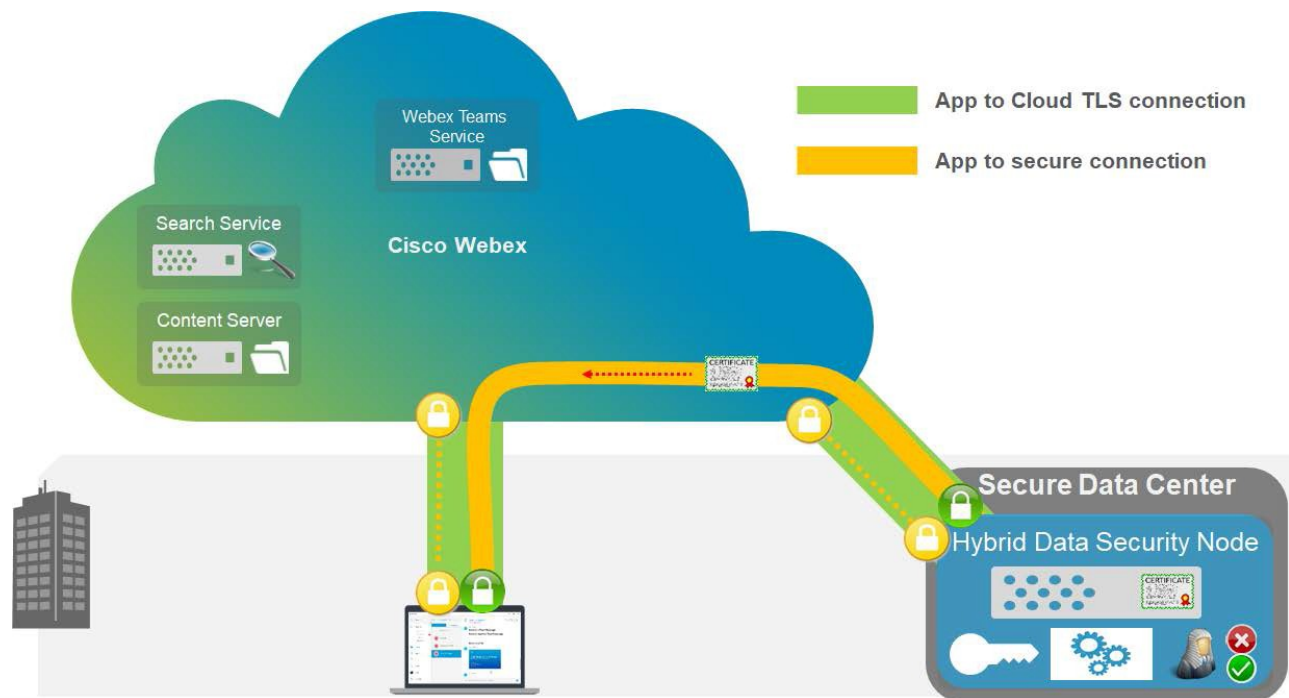
When deployed on-premises, Hybrid Data Security (HDS) services provide an additional benefit, in that decryption of posted content for indexing takes place on the customer premises, not in the Webex cloud. Additionally, the encryption keys for messages and files are also owned, stored, and managed on the customer's premises as part of the Hybrid Data Security service.

Question: When deploying KMS on-premises, what data flows remain in the cloud?

Answer: Webex Teams and Webex devices establish TLS connections to the Webex cloud, these encrypted connections are used for all communication to Webex cloud services and on-premises services such as the Hybrid Data Security service. To ensure that communication between Webex Teams and on-premises HDS services remain confidential, an additional encrypted connection is established between Webex Teams and the on-premises HDS service.

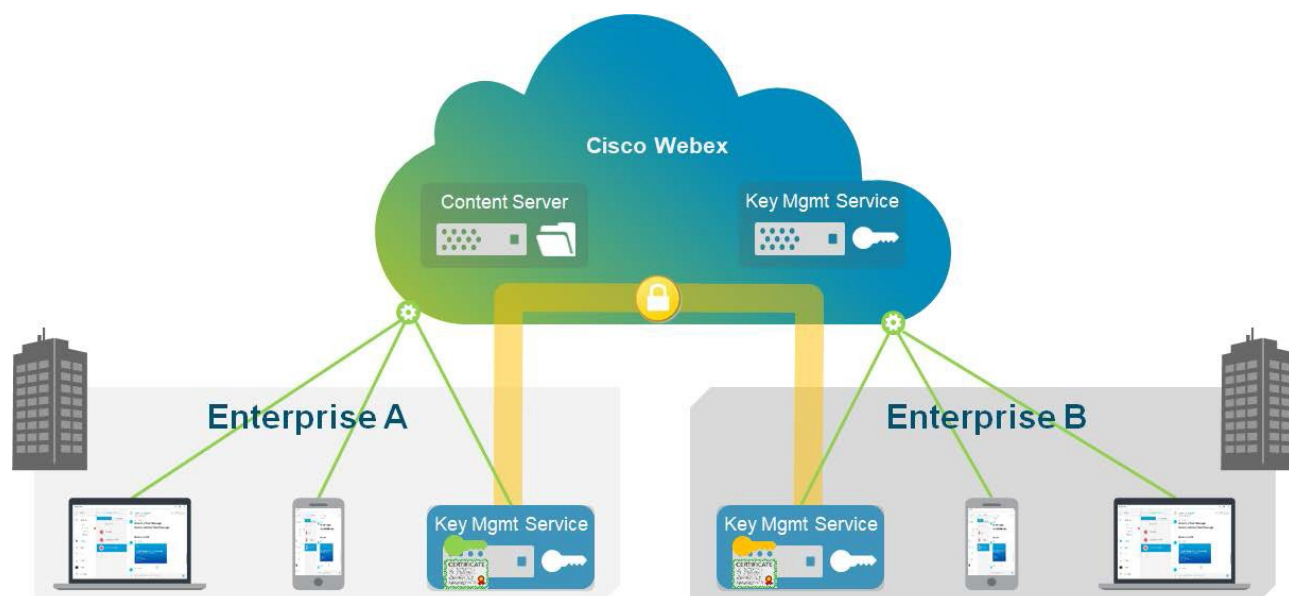
This secure connection uses ECHDE for key negotiation and AES-256_GCM for authenticated encryption of data.

Figure 12: Webex Teams – Webex Cloud and HDS Connections



Key Management Services in HDS nodes automatically federate with the KMS services of other organizations when Webex Teams users from two, or more, organizations participate in a Webex Teams space. This KMS to KMS connection is established by using mutual TLS between the HDS nodes in each organization.

Figure 13: KMS Federation between two Organizations using Webex Teams and HDS



Question: Where I can learn about the encryption and key management capabilities of Webex Teams?

Answer: For information about the encryption and security capabilities of Webex Teams, see:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/whitepapers/cisco-spark-firewall-traversal-white-paper.pdf

For details of encryption and key management features and services supported today, see:

<https://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/webex-room-series/datasheet-c78-740770.html>

Question: Does KMS encrypt media?

Answer: No, the Key Management Server does not perform an encryption function; it creates and distributes encryption keys to Webex Teams that use End to End encryption for content (messages and files). The KMS does not create and distribute encryption keys for Webex Teams media streams, these keys are generated by the Webex Teams, devices, and media servers participating in a call or conference.

Question: Are the Key libraries and keys stored on Cisco dedicated storage? How are the encryption and decryption keys in these key libraries protected? How do we protect the KMS data? Is the database encrypted? What are the Security Controls on our KMS data stores?

Answer: All encryption keys used by Webex Teams are securely stored. Encryption keys for messages and content shared in Webex Teams spaces and the details of these spaces are held in a database and encrypted before being stored. The space details include the space name, space owner or moderator, and participants.

For Webex Teams organizations using the Webex cloud KMS service, their encryption keys and space details are securely stored on Cisco dedicated database servers.

For Webex Teams organizations using the Webex Teams HDS service, their encryption keys and space details are securely stored in the organizations premises on customer owned database servers, for example, MSSQL or Postgres.

Access to KMS/HDS related data is tenanted through a combination of the following:

- Access tokens that identify the user, the organization that they belong to and the scope of Webex Teams services that they are authorized to access.
- Data structures for Webex Teams spaces, meetings etc. that define their authorized participants.

Question: When KMS is deployed on-premises what information is sent to the Webex cloud? Please describe inbound and outbound traffic types.

Answer: The Webex Hybrid Data Security (HDS) platform makes outbound TLS connections only and uses HTTPS and Secure Web Socket (WSS) connections for signaling. The signaling connections from HDS to the Webex cloud are used for:

- HDS provisioning and management functions
- Software Upgrades
- Key distribution to Webex Teams used by employees in your organization
- Key distribution to federated KMSs in other organizations
- Key distribution to the Webex cloud for encryption/decryption of content used by other services (e.g. document transcoding, calendaring services)

Question: If the KMS goes down (especially for HDS) how long do keys remain in the client cache?

Answer: The encryption keys for Webex Teams spaces and content (messages and files) are securely stored and cached by Webex Teams.

For Webex Teams for iOS and Android, resetting user access in Cisco Webex Control Hub deletes the cached content. Resetting user access also revokes the user's OAuth access token across all Webex Teams apps, requiring users to sign in again.

For Webex Teams for Web, cached content is deleted when the user signs out or closes the browser or the browser tab.

Question: When multiple HDS nodes are deployed in a cluster for load balancing and redundancy, what determines which one is used for a specific KMS, indexing, or eDiscovery request?

Answer: Each node in an HDS cluster contains a single KMS, indexing and eDiscovery instance, and the aggregate of these nodes represents a single logical HDS cluster. KMS, indexing and eDiscovery requests sent to an HDS cluster are delivered to the individual HDS nodes using round-robin distribution. HDS nodes are stateless.

Question: How do I replace the certificate used by an on-premises KMS?

Answer: For more information, see the *Change the Node Configuration* section in the Deployment Guide for Cisco Webex Hybrid Data Security here:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/datasecurity/cmgt_b_hybrid-data-security/cmgt_b_deployment-guide-for-hybrid-data_chapter_011.html#task_92BAB13CD98665E92B3B2AB9D6B29BF0

Question: On the Hybrid Data Security service, the master key used to encrypt the database content. Where or how is this key generated?

Answer: The Master Key for HDS is generated by the set-up tool when creating ISO file – this can run as a docker container on a local machine

Question: What processes and procedures are in place to manage and recover from the compromise of End to End encryption keys used by Webex Teams?

Answer: Webex Teams uses End to End Encryption to secure messages and files shared in spaces. In addition to the encryption keys used to secured messages and files, encryption keys are used for several other purposes:

- KMS certificate private key is used to secured connections between KMS clusters in different organizations. If compromised, a new certificate can be installed.
- KMS session keys secure the communications between Webex Teams and the KMS cluster. Encryption keys are created for every session using Elliptical Curve Diffie Hellman Ephemeral (ECHDE) key negotiation. They expire in 2 hours and can be explicitly revoked using APIs.
- The KMS master key is used to secure the content stored in the database used by KMS. The KMS master key cannot be “revoked”, however we are currently implementing a means for rotating this key and reducing exposure to compromise.
- KMS application key or KMS keys, these keys are used to secure user messages and content, they cannot be “revoked”, however we are currently working to enable rotation any time a user leaves a space

Question: Is it possible to enable hybrid services when bulk provisioning new users?

Answer: Yes, you can add or modify users and their service assignments by creating or updating the CSV template file available in Cisco Webex Control Hub. For more information, see the *Modify Users in Cisco Webex Control Hub with the CSV Template* article here: <https://help.webex.com/article/e2okky>

Question: Does your organization support the use of PGP for asymmetric data exchange?

Answer: No, Webex Teams uses end-to-end encryption and only authorized participants in a Webex Teams space can access the encryption keys that are used to encrypt or decrypt messages and content. Webex Teams does not use PGP. To learn about the key management architecture that we use to implement end-to-end encryption see: <https://datatracker.ietf.org/doc/draft-abiggs-saag-key-management-service/>

Question: What IdPs does Webex Teams support for Single Sign-on?

Answer: Webex Teams supports any Identity Provider (IDP) that complies with SAML v2. Webex Teams works with the leading identity providers for both on-premises and Identity as a Service (IaaS) integration for the purpose of SAML v2 federated single sign-on. We have created integration guides for some of these partners and have posted them on our Help site at <https://help.webex.com/article/lfu88u>

We have integration guides or confirmed customer integrations for the following identity providers:

- On-premises identity providers
 - Microsoft ADFS
 - Oracle Access Manager
 - Ping Identity
 - OpenAM
 - IBM Security Access Manager
 - CA Siteminder
 - F5 – BigIP
 - Shibboleth
- Identity-as-a-service vendors
 - Okta
 - PingOne
 - Salesforce
 - Microsoft Azure
 - Oracle Identity Cloud Service
 - Centrify
 - OneLogin
- Multi-Factor Authentication

Webex Teams provides authentication through multifactor authentication (MFA) by integrating with SAML v2 identity providers that support this mechanism. Many organizations deploy MFA mechanisms across their enterprise for all services that require special additional factors during authentication (something you know – your password – and something you have – x509 certificate, HMAC-Based-One-Time Password (HOTP), Time-Based One-Time Password (TOTP), device fingerprinting, or other supported mechanisms by the IdP).

- IDP and MDM/MAM with Webex Teams
Enterprise customers are building new architectures to address the security of mobile devices, authentication, and authorization of cloud-based SaaS. Enterprise customers look to the identity provider vendors to provide authentication and authorization to web apps, as well as access control to mobile apps (also known as Mobile Application Management (MAM)). These same IdPs also include Mobile Device Management (MDM) features, or integrations to make sure that trusted devices are used by employees when accessing applications. Many IDPs use features such as device registration or certificate-based authentication to achieve these goals.

Question: Does Webex Teams support multifactor authentication?

Answer: Yes, Webex Teams can support the customer's multi-factor authentication flow using their IdP, as long as the flow can work within an embedded browser. To take advantage of this capability, the customer must setup SSO and integrate their IdP with Webex Teams.

Question: For customers using the Webex Teams Common Identity service to store usernames and passwords for authentication, or organizations that are not using an IdP and SSO for authentication, are the user passwords stored in the Common Identity service encrypted?

Answer: Yes. For more information on how Webex Teams stores and manages personal data, see the Webex Teams Privacy Data sheet:

https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

Question: Does Single Sign On (SSO) apply to Control Hub users?

Answer: If SSO is enabled for a Webex Teams organization it applies to Webex Teams users and Control Hub users.

Question: Can you revoke the OAuth tokens of an employee whose contract has been terminated?

Answer: Yes, token revocation and remote wipe on mobile devices are available through [Pro Pack for Webex Control Hub](#). With Control Hub, an enterprise admin can revoke all existing user tokens from the user profile. When tokens are revoked, all user sessions through endpoints and apps become invalid. On mobile devices, all cached content is erased.

When a user's token is revoked, users must re-authenticate to use Webex Teams. On mobile devices, once authenticated, Webex Teams also refreshes its data cache.

An OAuth access token is valid for 6 hours.

An OAuth refresh token that is valid for 60 days. The refresh token allows a user to request a new access token, without re-authenticating. The Refresh token's lifetime is renewed every time the user gets a new access token.

If a terminated user's account is deleted in Webex Teams, their access and refresh tokens are revoked which disables access to Webex Teams services.

Question: If devices are lost or stolen, is the data on the devices protected?

Answer: Data is encrypted at rest on Webex Teams for Windows, Mac, iOS and Android. In addition to this, data stored by Webex Teams for iOS and Android can be remotely wiped in Webex Control Hub using Reset Access. Webex Teams for Web doesn't store messages and content.

Question: Are OS platform administrator rights required to install and update Webex Teams?

Answer: As an administrator you can install Webex Teams using the MSI file on Windows, or the DMG file on Mac. Webex Teams checks for newer versions and automatically upgrades the application, administrator rights are not required to upgrade Webex Teams. For more information, see *Cisco Webex Teams Installation and Automatic Upgrade* <https://help.webex.com/article/nw5p67g>.

Question: How long does the cache remain valid in Webex Teams? Is it per device?

Answer: For Webex Teams on desktop and mobile the tokens, keys, messages and transcoded documents are securely stored. The folders or database that they are stored in are encrypted. Downloaded files are decrypted and then stored based on user or OS choice, for example the Windows downloads folder. Messages and transcoded files are decrypted using the space key before being securely stored.

For Webex Teams for Windows and Mac, the content is stored on the device until the organization's retention period expires, transcoded files may be overwritten as storage is limited.

For Webex Teams for iOS and Android, the content is stored on the devices until the organization's retention period expires, transcoded files may be overwritten as storage is limited. The administrator of the Webex Teams organization can reset access in Control Hub to clear the cache on the user's device.

For Webex Teams on Web, the content or messages isn't cached, the content is retrieved from the cloud after the user has signed in and deleted when the user signs out or closes the browser. Keys and tokens are not cached by default, except when a user selects **remember me**. Then, the Web app caches tokens and keys and only clears the details when the user signs out.

Question: Does Webex Teams use persistent cookies? If so, how are those secured?

Answer: Cookies are only used by Webex Teams for Web and are persisted when the user chooses **remember me** in the browser. Cookies are locally stored and non-persistent cookies are deleted along with all other information when the user signs out.

Question: Despite the 16Digits/QR Code for first registration, does Webex Teams have a mechanism in place for identity check or re-validation when a device disconnects or reconnects?

Answer: The on-boarding process for Webex devices is a one-time operation. Once authenticated with the Webex Teams service, the device receives and uses OAuth access and refresh tokens from the Webex cloud. The OAuth access token includes scopes that define which Webex Teams services the device is authorized to use. To establish a secure connection to a Webex Teams service, the device must first send its access token to the service, which checks the scope of permissions assigned to the device before allowing a secure connection to be established.

Device OAuth tokens are held in NVRAM but can be revoked by deleting the device in Webex Control Hub. If further identity checks are required when a device disconnects and reconnects to the corporate network, we recommend using 802.1X as the Network Access Control protocol. For details on 802.1X support by Webex devices, see *Network Requirements for Webex Teams Services* <https://help.webex.com/article/WBX000028782>

Question: For Webex Teams device onboarding, is the 16-digit activation code linked to the org? How is device communication secured during the onboarding process?

Answer: Part of the 16digit activation code used by Webex Teams devices during the onboarding process identifies the device's organization. All connections to the cloud use TLS to secure data in transit.

Question: Does Webex Teams provide notification if users external to their organization are also space participants?

Answer: Yes. The non-consumer or paid subscription version of Webex Teams provides the following indications when there are external participants in a space:

1. A yellow icon is displayed the space's text entry panel
2. The list of people in the space includes the following text "People outside your company are included in this space".
3. The list of people in the space highlights external users by including their domain id
4. When an external user posts content into a space, their name and external domain id are displayed in messaging window.

For more information, see the *External Users in the Cisco Webex Teams App* article here:

<https://help.webex.com/article/no3o617>

Question: Is it possible to restrict the ability to add external people to Webex Teams spaces?

Answer: Yes, there are multiple ways that external users can be blocked from Webex Teams spaces:

- Using the Block External Communication feature in Control Hub. This feature blocks all users in the organization from inviting external contacts to Webex Teams spaces and from joining external Webex Teams spaces.
- With Block all external communication enabled, specific external domains can be added to an "Allowed Domains List" from Webex Control Hub (This feature is scheduled to be delivered in Q4 CY 2019).
- For fine grained control of communication between users in your Webex Teams organization and external users (and other internal users if required for ethical wall functionality); the Webex Teams Events API supports membership events in Webex Teams spaces. A DLP/CASB application can use the Events API to monitor the addition of users to a space and remove users if their membership of a space falls outside of policy. See <https://developer.webex.com/docs/api/guides/compliance>.

Question: How is file storage secured during document transcoding?

Answer: Files are never stored by the document transcoding application; they are processed by the application (converted to a PNG image). After the content is transcoded, the original document is deleted.

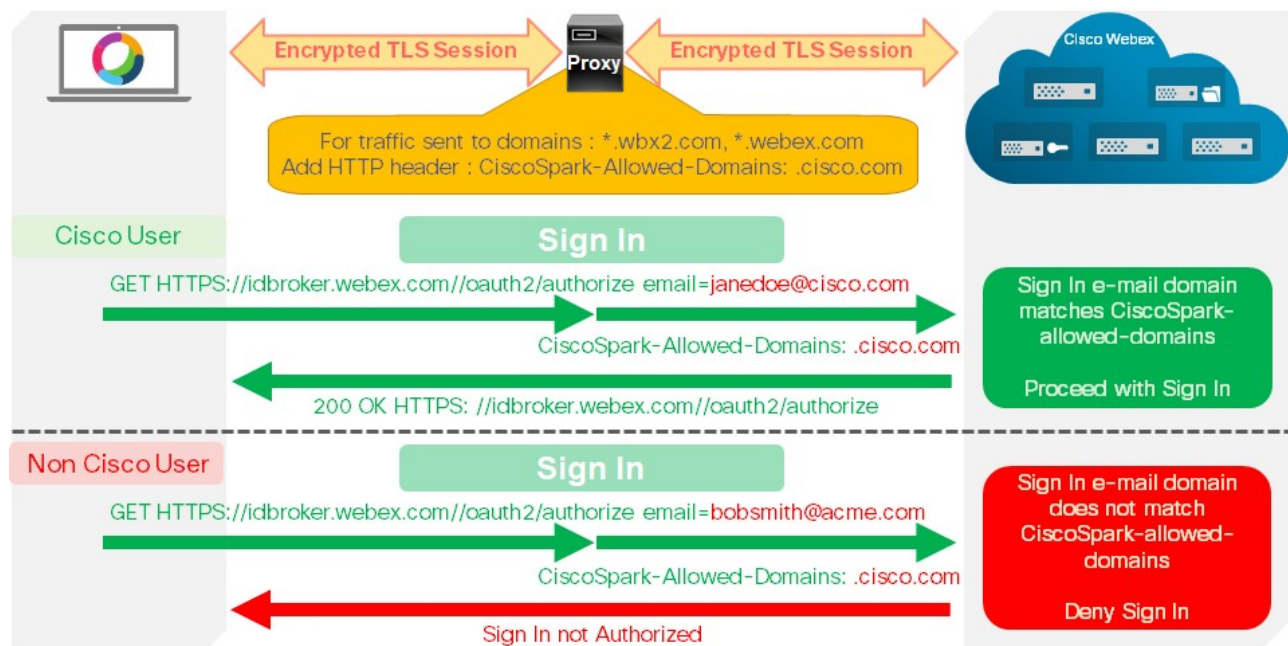
Native document and file transcoding in the Webex cloud was introduced in Q2 CY 2019. File and document transcoding in the Webex cloud, removes the requirement to use third party transcoding services and improves transcoding performance.

Question: For an organization that is using DLP to track documents that users are sending to Webex Teams spaces. If a user signs in to Webex Teams on their organization's computer using their consumer id, for example their Gmail account; can this user send internal docs into any space that they create?

Answer: By default, yes this is possible as the DLP application is only monitoring users within their organization.

However, Webex Teams does allow an organization to limit the domains that a user can sign into Webex Teams with when they are in their Enterprise network. This Allowed Domains feature (see figure 14) works in conjunction with the Enterprise's Proxy server, which injects HTTP headers into Webex Teams sign in requests, indicating the domains that can be used to sign into Webex Teams from within the Enterprise network.

Figure 14: Webex Teams– Proxy TLS – Allowed Domains



Question: Describe Webex Teams eDiscovery capabilities

Answer: Webex Teams eDiscovery and compliance capabilities are described in the *Ensure Regulatory Compliance of Cisco Webex Teams Content* article here: <https://help.webex.com/article/nr70c1m>

Question: Can eDiscovery be turned off?

Answer: eDiscovery is performed by the Webex Teams compliance officer within your organization. The compliance officer role is a setting that is assigned to a user by the Webex Control Hub administrator for your organization. By default, no user has compliance officer privileges and the administrator cannot assign this privilege to their own profile.

Question: How is the Webex Teams service protected?

Answer: For more information, see the following:

- Webex Teams Privacy and Security whitepaper: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/esp/cisco-spark-security-white-paper.pdf
- Privacy data sheet: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-service-privacy-data-sheet.pdf
- Additional information is also available in other questions and answers in this document.

Question: Can we enforce policies using a disclaimer?

Answer: Links to the standard Terms of Service, Privacy Statement and Notices and Disclaimers for Webex Teams are displayed on the sign in page for Webex Teams. Customized Disclaimers and sign in banners are not supported today.

Question: Can you prevent employees from creating Webex Teams accounts?

Answer: Within an organization, Webex Teams is available for use by all employees when:
The employee is using a corporate email address, matching the organization's domain
The organization is active within Webex Teams.

If the company's Webex Teams organization is not active, employees can use their corporate email address to create a public account and use Webex Teams. When a Webex Teams organization is created using the corporate domain, the Webex Teams administrator has the ability to import all those employee accounts using the organization's domain, from the public organization to their own organization.

Employees using their personal email addresses to create an account and use Webex Teams, these employees can't be controlled by the company's administrator.

Question: If an employee is terminated and their account in Active Directory is deactivated or removed; how long until their Webex Teams account is deactivated?

Answer: The addition and deletion of employees from the Webex Teams Common Identity service occurs during directory synchronization, Webex Teams uses a default interval of 10 minutes between incremental synchronizations.

If immediate off-boarding is needed, the users OAuth Tokens can be deleted by using Reset Access in Control Hub.

Question: What is the shortest interval for directory synchronization?

Answer: 5 minutes

Question: What is the difference between disabling a user and deleting a user in Active Directory in terms of user status in the Webex Teams organization after a directory synchronization?

Answer: Deleting a user deletes the Unique User ID (UUID) to Active Directory user mapping in the Webex Teams identity service. Deleting the UUID makes the user's content irretrievable.

Disabling a user maintains the UUID assigned to the Active Directory user. When the user is re-activated their UUID is restored and all their conversations and interactions in Webex Teams are restored.

Question: How are Webex Teams users signed out?

Answer: Once a Webex Teams user is authenticated, the application downloads and stores OAuth2 access and refresh tokens. These tokens are used to provide proof of authorized access to Webex Teams services. An OAuth access token is valid for 6 hours. An OAuth refresh token is valid for 60 days. The refresh token allows a user to request a new access token, without re-authenticating. The refresh token's lifetime is renewed every time the user gets a new access token.

A Webex Teams user can be signed out using the following methods:

- The user chooses to sign out of Webex Teams.
- The user doesn't connect to the Webex Teams platform for more than 60 days, thus expiring the Refresh Token.
- The Webex Team Administrator revokes the user's tokens using the Reset Access Feature in Control Hub.
- The user ends Webex Team sessions by revoking tokens on specific devices using the Webex Teams App, under Settings > Recent Sessions (on Windows) or Preferences > Recent Sessions (on Mac.)

Question: Is it possible to have an automatic sign out for Webex Teams app?

Answer: Webex Teams supports a configurable timeout for Webex Teams for Web. The timeout can be set for Webex Teams on Web running on devices on enterprise networks and external networks. Webex Teams for desktop and mobile don't have a configurable timeout, they rely on the inactivity timers that are used by the operating system to lock the device.

Question: For the eDiscovery search and extraction tool, standard Cisco Webex Teams customers have access to only 90 days of content. Pro Pack customers can access unlimited data within Webex Teams spaces. Can a customer purchase a Pro Pack subscription and then search for content beyond 90 days for members in their organization?

Answer: Yes, the Compliance officer of an organization with Pro Pack can search for content beyond 90 days, this includes content that was added before Pro Pack was enabled.

Question: Can a Webex Teams user with the compliance officer role, search content posted by a subset of users? For example, users from a certain domain?

Answer: Yes, as part of Webex Control Hub eDiscovery, the compliance officer can perform a search of user-generated content based on users' email addresses. For more information, see figure 15.

Figure 15: Webex Control Hub – eDiscovery

Search & Generate Compliance Report

Search Information
Enter information to search and include in your report. When generating a report, the 'AND' operation will be used to gather data.

Search Type
Manually enter up to 500 users or space names separated by commas or bulk add with a CSV file. Multiple users or spaces entered here will use the 'OR' operation.

Email Address
user1@email.com, user2@email.com, user3@email.com, user4@email.com,
user5@email.com, user6@email.com, user7@email.com, user8@email.com,
user9@email.com, user10@email.com, user11@email.com, user12@email.com
e.g. johndoe@email.com, jane.williams@email.com [Clear](#) [CSV Bulk Add](#)

Space Names
Space Name 1, Space Name 2, Space Name 3, Space Name 4
e.g. Developer Collaboration, Ask Help Desk. [Clear](#) [CSV Bulk Add](#)

Date Range @
02/09/18 to 02/19/18

Where Messages contains
Enter comma separated values
e.g. project, manager. Values entered here will use the 'OR' operation.

Question: Does the audit event log in Control hub capture the creation of a compliance officer role?

Answer: Today, the Control Hub audit tracks changes to user entitlements, but does not log the specific change of a user's role, for example adding a compliance officer role. The Webex Control Hub Compliance Officer Audit Log is currently in Early Field Trials.

Question: Is there a process/procedure to enable the Events API for a customer's Org?

Answer: The Webex Teams Events API, is one of several REST API endpoints that can be used by a Webex Teams organization. To use a Webex Teams REST API, you need to use or create a Webex Teams account in your organization for the user. You can then use the APIs to build Bots and Integrations for Webex Teams users or to perform administrative tasks. To fully use the Events API, your user will need to be assigned with the Compliance Officer role which gives them access to and management of all data created by their organization including messages, content attachments, etc. in order to monitor data and to mitigate compliance issues that could arise.

Question: Is there a way for an administrator to delete content created by a user?

Answer: Yes, a user with the Compliance officer role in the organization can delete content created by any user.

For more details see the following:

<https://developer.webex.com/docs/api/guides/compliance.html>

<https://developer.webex.com/endpoint-messages-messageId-delete.html>

Question: Does the Webex Teams service support SCIM?

Answer: Yes, Webex Teams supports SCIM v1.0 today, SCIM v2.0 which adds support for user groups and other objects is currently in development.

Question: How does the DLP inspect files to ensure it does not contain violations?

Answer: Most DLP/CASB applications can inspect files by file name and file content. Files and messages sent to DLP/CASB applications via the Webex Teams Events API use TLS as a securely encrypted transport channel.

Question: If a customer is using a DLP/CASB. When the DLP/CASB deletes a message, is this message fully purged, or is it still held for archival or retention reasons?

Answer: Messages are soft deleted and archived for the retention period specified by the organization. Note – If a user's content is placed on legal hold, the organization's retention policy is overridden, and the content is archived until legal hold has been removed.

Question: How long is a Webex Teams user's data retained for when they are placed on Legal Hold?

Answer: Content for Webex Teams users not placed on legal hold is stored until the retention period set for the organization is reached, for example: 36 months. After this retention period user content is purged or hard deleted.

If a Webex Teams user's content is put on legal hold, the organization's retention policy is ignored, and the user's content is retained until legal hold is released. When legal hold on the user's content is released, all data older than the retention period is deleted.

Question: If a user is put on legal hold and they delete messages in a space, is the content retained or lost?

Answer: When a user is placed on legal hold, all messages, files and whiteboards are retained; even if the user subsequently deletes them or they exceed the content retention period set by the organization.

Question: If a Webex Teams user deletes content in a space, is this content still discoverable by a Compliance Officer using eDiscovery in Control Hub?

Answer: Yes, provided that the content has not been deleted in accordance with the organization's retention policy.

Question: Is it possible to track who has previewed or downloaded a specific file from a space?

Answer: We plan to add the capability for DLP/CASB applications to track file downloads and file previews via the Webex Teams Events API later this year (Q4 CY 2019).

Question: If the moderator of a space leaves the organization and no other moderator exists within the space, can a new moderator be assigned?

Answer: Yes, if the moderator leaves the space or leaves the organization and no other moderator exists within the space, the space becomes unmoderated. In an unmoderated space, any participating user can assign themselves the role of moderator.

Question: Is the retention policy on archived spaces the same as all other spaces?

Answer: Yes, the retention policy configured for your organization in Control Hub, applies to active and archived spaces.

Question: Does Webex Teams support ephemeral messages or messages with very short retention period?

Answer: The retention period for a Webex Teams organization can be set in Control Hub, the minimum retention period is 1 month. By request, retention periods of less than one month with a minimum of 24 hours can be configured for an organization by Cisco's Webex Teams system administrator.

Question: Is the Cisco Webex assistant always in listening mode, whereby the Webex Teams device could capture sensitive conversations in the room?

Answer: No, when the Webex Assistant is activated using its wake word, "OK Webex," it results in speech being streamed to the cloud-based speech engine. The wake word service only listens for the wake word pattern and does not stream content until it is activated. For additional details on technologies such as conversational artificial intelligence, face recognition and so on, see https://use.webex.com/cognitive_collab_lp

Question: Does Webex Teams allow an administrator to restrict individual users from adding external users to spaces?

Answer: In Control Hub you can globally restrict all external communication and whitelist specific external domains that you wish to allow your users to communicate with. More granular control, such as restricting communication between individual internal and external users can be provided by a Data Loss Prevention (DLP), or Cloud Access Security Broker (CASB) application.

Question: When an administrator converts a user from a free account to one managed by the administrator's organization, what happens to the user's associated content?

Answer: During the account conversion process, free account users are given two options:

1. To create a new private account for their existing content and a new blank account is created in your organization for them.
2. To convert their existing account and its content to one owned and managed by your organization.

Question: When a user's account is disabled, how long does it take before the user is signed out from Webex Teams on their devices?

Answer: When a user's account is disabled, their access and refresh tokens are revoked. Once the tokens are revoked, the process of signing a user out the application can take up to two hours.

Question: Can an administrator be notified proactively should a room device go offline?

Answer: Control Hub device alerts, which includes alerts on device state change from online to offline, is scheduled to become generally available by the end of CY'19.

Question: Can multiple users be deleted by using CSV files or another simple method?

Answer: Today, CSV files can be used to add users, assign services and resource profiles to users. Users cannot be deleted using CSV files. Alternatively, the Webex Teams Directory Service can be deployed to automatically synchronize users between Microsoft Active Directory and Cisco Webex Teams user management.

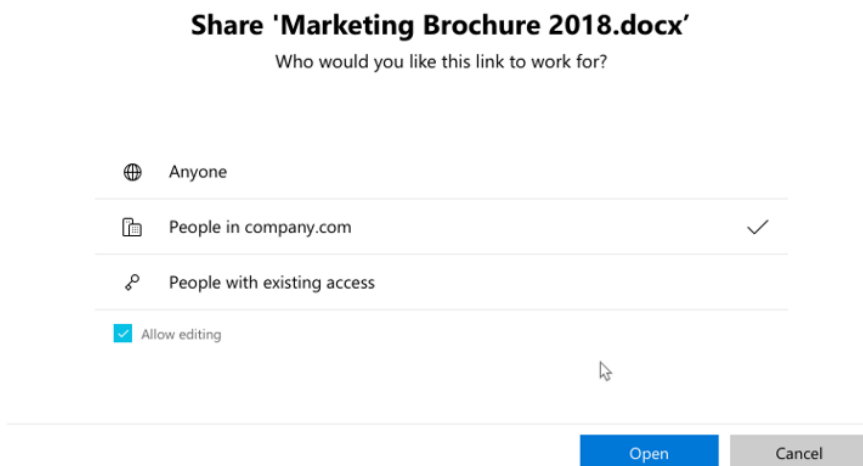
Question: If users are moved from one organization to another, what happens to the user generated content?

Answer: When a user is moved from one organization to another, the user's content is not migrated to the new organization.

Question: Is it possible to allow file sharing between Webex Teams users in my organization only and to block file sharing with external users outside of my organization?

Answer: There are two options for file sharing restrictions:

1. Use the file sharing restrictions available in Webex Teams integrated with an Enterprise Content Management (ECM) application. If file sharing in Webex Teams is limited to files managed by the ECM application only, for example, Microsoft OneDrive, SharePoint Online, or Google Drive. When a file is shared in a Webex Teams space, the user is prompted to select who they wish to share the file with:
 - Anyone in the Webex Teams Space
 - People in my organization only
 - People allowed to access the file based on the ECM platform's file or folder permissions



2. Using the Webex Teams Events API and a DLP/CASB application – files can be removed from spaces that contain external users.

Question: When disabling file sharing by app in Webex Control Hub, does this setting apply to all users no matter what space they join; that is, both internal spaces and external spaces owned by other organizations?

Answer: The file sharing restrictions in Webex Control Hub are applied to the Webex Teams apps or bot and they apply to any space both internal and external that the user is participating in.

Question: How does Cisco protect customer data from being accessed by other customers in the Webex cloud?

Answer: Cisco uses several mechanisms to isolate and protect customer data:

1. User content generated in Webex Teams spaces is end-to-end encrypted with an encryption key that is unique to the space that the users are participating in.
2. Customer data at rest that is stored in the Webex cloud is encrypted, including end-to-end encrypted user generated content.

3. Access to data is tenanted through a combination of the following:

- Access tokens that identify the user, the organization that they belong to and the scope of Webex Teams services that they are authorized to access
- Data structures for Webex Teams spaces, meetings etc. that define their authorized participants

Question: Does Webex Teams support SMTP for archiving?

Answer: No, Webex Teams uses the Events API endpoint to allow third party applications or integrations to archive user generated content. For a list of partners providing archiving solutions, see the *Cisco Webex Teams Integration with Archiving and Data Loss Prevention Solutions* article here:

<https://help.webex.com/article/nmbm0jk>

Question: Can you limit the size of files that can be uploaded in spaces?

Answer: Webex Teams has a maximum file size limit of 100MB for files uploaded to spaces. A DLP/CASB application can detect uploaded files that exceed a specified size and, if required, delete them using the Events API.

Question: Are security and system logs encrypted at rest?

Answer: Yes, for details of the data that Webex Teams stores and encrypts at rest, see the *Webex Teams Privacy and Security datasheet* https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-webex-teams-privacy-data-sheet.pdf

Question: Can a Webex Teams administrator allow file previews to be viewed, but restrict files from being downloaded?

Answer: File sharing controls in Webex Control Hub allow file previews and files to be blocked based on Webex Team app desktop, mobile or web app and bots. The capability to preview files only and block file downloads is not available today in Webex Control Hub. Most MDM and MAM applications offer the capability to block a user from downloading and saving files from managed applications.

Question: Describe the Webex Control Hub administrator roles and configuration settings

Answer: You can set up users in your organization with different administrator roles. Users can become full administrators, or a combination of support administrators, user and device administrators, device administrators, read-only administrators, or compliance officers. For more information, see the *Assign Organization Account Roles in Cisco Webex Control Hub* article here: <https://help.webex.com/article/fs78p5>

Cisco Trademark (all documentation)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Cisco Copyright (all documentation)

© 2019 Cisco Systems, Inc. All rights reserved.