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 e-discovery services, signaling services for Webex Teams, 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).

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 at 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)**
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)

Audio/Video
Cascaded Audio/Video

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

Audio/Video
Cascaded Audio/Video

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

Answer: Yes
SSL/TLS/HTTPS signaling 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 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.

For SSL/TLS/HTTPS Inspection for Webex Teams on Window and Mac, Webex Teams relies 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, Webex Teams will trust certificates signed by the enterprise CA, when presented to it by the proxy server. This bypasses the certificate pinning process used by Webex Teams and allows a TLS connection to be established to the proxy server.
For details on Webex Teams and device support for SSL/TLS/HTTPS inspection, see: https://help.webex.com/article/WBX000028782/

Question: What proxy types does Webex Teams support?

Answer: Webex Teams and Webex devices support standard HTTP/TLS Proxies – for more information on the features supported by Proxy devices, see: https://help.webex.com/article/WBX000028782/

Question: How does Webex Teams use Certificates?

Answer: We use certificates to allow Webex Teams and Webex devices to identify and authenticate the Webex Teams services that they connect to. Webex Teams 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, 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 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

- TLS versions 1.2 and 1.1 only are 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 SDES. For more information, see https://tools.ietf.org/html/rfc4568
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 support TLS versions 1.2 and 1.1 only (most enterprises have security concerns about the use of TLS 1.0).

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.

If TLS version 1.2 only is required, an organization could use its Enterprise Proxy server to intercept and modify TLS connection requests from Webex Teams and devices, limiting outbound TLS connections from the Proxy to version 1.2 only.
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 One Drive, or SharePoint Online) for Webex Teams file storage and distribution.

Non-U.S. and U.S. 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 http://www.cisco.com/c/en/us/about/trust-transparency-center/validation/report.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 also have the option to archive a copy of this content with a third-party data archival company (e.g. Actian, Global Relay, Verint Verba), or to 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. For example, OneDrive, Box, Google Drive and so on. Customers can also use the API for Enterprise Content Management to store files within their enterprise network. For more information, see https://help.webex.com/article/nuz39yeb/

Figure 9: Webex Teams API for Enterprise Content Management

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

Answer: Yes

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 OneDrive/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 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
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:
All Webex Teams apps 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.
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 can I learn about the encryption and key management capabilities of Webex Teams?


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: How are the key libraries protected to include encryption and decryption keys?

Answer: All Key Management Server (KMS) encryption keys are encrypted with a master encryption key before being stored in either the Cisco Webex cloud managed database, or a customer-managed database used in conjunction with Hybrid Data Services (and on-premises KMS).

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 the Webex Teams for Web, cached content is deleted, when the user signs out, or closes the browser/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 e-discovery request?

Answer: Each node in an HDS cluster contains a single KMS, indexing and e-discovery instance, and the aggregate of these nodes represents a single logical HDS cluster. KMS, indexing and e-discovery 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 on-premises KMS?

Answer:

Specifically, this section:

Question: On the Hybrid Data Security service, the master key used to encrypt the DB content. Where/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: Does your organization support the use of PGP for asymmetric data exchange?

Answer: No
Webex Teams uses end-to-end encryption so that 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 Center site at https://help.webex.com/article/lfu88u

We have integration guides, or confirmed customer integrations for these 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 via 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: 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 their Webex Teams. 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 them protected? (e.g. full encryption, remote wipe capabilities, etc.)

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 via Webex Teams Control Hub (Reset Access feature). Webex Teams for Web does not store messages and content.

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

Answer: For Webex Teams for Windows, Mac, iOS and Android - the tokens, keys, messages and transcoded docs are securely stored. The folders or database that they are stored in are encrypted. Downloaded files are decrypted and then stored based on user/OS choice e.g. Windows Downloads folder. Messages and transcoded files are decrypted using the space key before being securely stored.

For Webex Teams for Windows and Mac: Content is stored on the device until the organization’s retention time expires, transcoded files may be overwritten as storage is limited.

For Webex Teams for iOS and Android: Content is stored on the device until the organization’s retention time expires, transcoded files may be overwritten as storage is limited. The Administrator of the Webex Teams organization can use the Control Hub “Reset Access” feature to clear the cache on the user’s device.

For Webex Teams for Web: Content isn’t cached, the content is pulled from the cloud after the user has signed in; and deleted when the user signs out, or the tab or browser are closed.

Keys and tokens are generally not cached by default; the exception to this is when the user enables the “remember me” feature, then tokens and keys are cached and only cleared 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 only if the user chooses the “remember me” option 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 Cisco 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: https://help.webex.com/article/WBX000028782/

Question: Do Webex Teams and Endpoints support 802.1X?
Answer: Yes – For details, see 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 16-digit 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 (paid subscription) version of Webex Teams provides the following indications when there are external participants in a space:
- A yellow icon is displayed the space’s text entry panel
- The list of people in the space includes the following text “People outside your company are included in this space”.
- The list of people in the space highlights external users by including their domain id
- When an external user posts content into a space, their name and external domain id are displayed in messaging window.

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 Q3 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 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 PC using their consumer id (e.g. 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 domain(s) that a user can sign into Webex Teams with whilst within 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 Feature

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:


- 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 if:

- The employee is using a corporate email address (matching the organization’s domain)
- And if 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 (e.g. cisco.com), 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, cannot be controlled by the company’s organization administrator.

Question: If an employee is terminated, and their account in AD 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 the Reset Access feature 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

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

Question: How are Webex Teams users signed out?

Answer: Once a Webex Teams user is authenticated, the application downloads and stores OAuth 2 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 choses 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 > Options > Recent session page.

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 who subsequently purchases a Pro Pack subscription search for content beyond 90 days for members within their org?

Answer: Yes, the Compliance officer of a Pro Pack enabled Org can search for content beyond 90 days, including content that was added before Pro Pack was enabled.

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

Answer: Yes
A user with the role of Compliance officer in the org can delete content created by any user.
For more details see:
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 (text). 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 / 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 (e.g. 36 months), after this period user content is purged (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 Webex Teams user deletes content in a space, is this content still discoverable by a Compliance Officer using the eDiscovery feature 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/ 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 (CY 2019).