Cisco Webex Control Hub (Compliance)

Contents

Compliance overview

Enterprises require controls to ensure that their employees don't accidentally or maliciously send sensitive and critical information via collaboration tools. Examples of such information are credit card numbers, social security numbers, intellectual property, patient records, etc. Cisco Webex Teams™ has integrated with several Data Loss Prevention (DLP) solutions (powered by APIs from Webex Teams).

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

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

For customers that require the ability to search and extract the content generated by their employees for legal reasons, the e-discovery search and extraction capability lets the compliance administrator extract this information in reports.

In addition, compliance officers can add exceptions to retention policies and put users on a legal hold when those users are under investigation. This helps to ensure that users' content can be preserved and not purged by an organization-wide retention policy during investigations.

Enterprises also prefer to control exposure and limit their liability by constantly purging data that has no business value. The retention feature provides the ability to do that.

Cisco Webex Teams also allows IT administrators the flexibility to enable Microsoft OneDrive and SharePoint Online as an Enterprise Content Management (ECM) solution to their users, in addition to Webex Teams existing native file sharing and storage. Users can share, edit, and grab the latest OneDrive and SharePoint Online files right within Webex Teams work spaces, while files are kept safe and secure in ECM and protected via a customer's existing DLP/CASB and anti-malware solution.

Space ownership

Webex Teams enables communications across the boundaries of organizations. As such, it is possible that users can communicate with colleagues in other companies. To deal with this, Webex Teams uses the concept of space ownership. The ownership rules differ between group spaces and communications with individuals.

Group spaces

For group spaces, a single organization is the owner of that space. The organization whose user creates the space is the owner of the space. The organization that owns the space has certain rights. When an organization has users that are participants in a group space not owned by that organization, the organization is said to be a participating organization.

Table 1 summarizes the content rights for Compliance officer.

Table 1. Compliance Officer Content Rights for Group Spaces

Privilege	Owning organization	Participating organization
Create		
Post content into the space	No	No
Read		
Read content (messages and files) posted by its own users into the space	Yes	Yes
Read content posted by any user in the space	Yes	No
Update		
Modify content posted by users into the space	No	No
Delete		
Define retention policies for the space	Yes	No
Delete content posted by any user into the space	Yes	No
Delete content posted by its own users in the space	Yes	Yes

Cisco Webex Teams 1-to-1 spaces with participants from two different organizations do not have an owning organization. Rather, there are two participating organizations, depending on whether the users in the space are controlled by the organization or not. Table 2 outlines the privileges for each participating organization in a 1-to-1 space (communications between individuals) for space content rights.

Both organizations can have independent retention policies. When the retention policy for one organization expires, messages sent by its user are deleted. When the retention policy for the second organization expires, messages sent by its user are deleted.

Table 2. Compliance Officer Content Rights for 1-to-1 Spaces (communications between individuals)

Privilege	Each participating organization
Create	
Post content into the space	No
Read	
Read content (messages and files) posted by its own users into the space	Yes
Read content posted by any user in the space	Yes
Update	
Modify content posted by users into the space	No
Delete	
Define retention policies for the space	Yes
Delete content posted by any user into the space	No
Delete content posted by its own users in the space	Yes

Events API

Webex Teams allows users to communicate with users outside their company by inviting them to their company-owned space or by joining another company's space. The Events API provides visibility into users' activities even in spaces not owned by the monitoring organization. Using the Events API, DLP software can even take action to remediate issues in such content. https://developer.webex.com/resource-events.html.

E-discovery: Search and extraction

Compliance officers can use the e-discovery search and extraction console to extract data created by users in their Webex Teams Organizations on Demand when required for legal investigations. Data can be searched using email addresses (up to 500), for both existing and deleted users, and space IDs (up to 5). The interface also allows compliance officers to specify a time window for the report.

The search report can be downloaded as an encapsulated zip file where all the activities are in an EML format organized by space. Optionally, the administrator can ingest the output files, which are in an EML format, into a downstream e-discovery tool for further querying or post processing the data. Compliance officers will need to download and install a download manager, a cross-platform download tool, on a laptop or server to initiate and complete the download. Optionally, compliance officers can exclude attachments from the report download and inspect only the messages generated by users. This will help them save time and network bandwidth and facilitate iterative future searches to specific users or spaces of interest.

Access to this feature is restricted to compliance officers as defined by an organization within role-based access control. E-discovery searches and reports are accessible from Webex Control Hub. The report summary shows information such as the number of users, activity, file, whiteboard count, space IDs, etc.

Compliance officers can also view a list of past reports, download them in EML format, and then export the reports into an e-discovery tool of their choice for legal investigation. The reports are available for 10 days.

Retention

Organizations can manage risks and align with global retention policies by setting a custom retention period in Webex Teams for the entire organization. With the Pro Pack for Webex Control Hub, full administrators can set the retention period for Webex Teams to align with the organizational retention policies and purge data older than that period.

An administrator can define an organization-wide data retention policy so that all relevant contents are permanently deleted at the configured retention timeframe. This reduces the risk of confidential information being accessible for a long time and also helps with alignment to retention policies across email and other applications.

Data Loss Prevention (DLP)

Cisco Webex Teams has a twofold DLP strategy. First, it informs users about potential data loss by making them aware of the context in which they are communicating. Users are informed about space ownership, retention, and the presence of external participants. End users are further empowered by propagation control features such as message deletion, read receipts, space locks, and moderator inheritance.

The second part of the strategy involves making events such as posting or deleting a message, attaching a file, and adding a user to or removing a user from a space in Webex Teams accessible via APIs so that they can be consumed by DLP software to check for violations and take action to remediate any issues. An administrator can use the Webex Events API to poll for events and content in order to monitor and respond to user behavior.

There are three ways to approach DLP integration.

- Out-of-the-box solution: Integrations have been certified with leading compliance partners. Cloud Access Security Brokers (CASB), DLP ISVs, and Cisco CloudLock® have integrated with Webex Teams via the Webex Events API to offer turnkey DLP capabilities for Webex Teams. They check for policy violations and take action to remediate them.
- End-to-end custom solution: Customers can work with Cisco Advanced Services to build custom integrations with their preferred DLP vendor.
- Do-it-yourself: The Webex Events API is exposed publicly. Customers are able to use the API to integrate with homegrown solutions or other third-party DLP vendors.

Block External Communications (BEC) – space membership

Cross-organization collaboration (collaboration with users who belong to a different organization, such as customers, partners, vendors, etc.) is a critical feature of the Webex Teams chat platform and is extremely valuable in improving workforce productivity. However cross-organization collaboration also exposes a surface area, for data loss and unauthorized communication, that needs to be protected. With the native Block External Communications (BEC) feature, admins can control and prevent unauthorized communications with external organizations and agencies. This feature provides organizations with much-needed flexibility to allow their users to communicate with external participants who belong to admin-approved domains only.

Webex Teams admins can configure a whitelist of trusted and authorized external domains (currently in controlled availability / trial mode) for users of an organization to collaborate. When users attempt to create a space and invite participants from external organizations who do not belong to a domain that is part of their organization's configured whitelist, the invited users will not be added to the space (e.g., the membership add action will fail). The policy decisions are executed inline and enforced proactively before the violating user is added to the space. This inline execution and enforcement of the BEC policy greatly minimizes the risk of data loss and protects the organization from exposure to users who belong to unapproved or untrusted domains.

The BEC policy always protects the space-owning organization. Any external user who is invited to join a space must belong to a domain that is part of the space-owning organization's domain whitelist. In cross-organization spaces, where the space owner, inviter, and invitee belong to different organizations, the domain whitelist policy of all three organizations (if BEC is turned on) will be evaluated and any of the three parties can veto the membership addition. Under certain circumstances, admins may want a highly restrictive policy and not allow their users to join group spaces that are owned by other organizations. Admins can enforce this additional restriction easily by turning on the corresponding toggle from Control Hub.

The BEC setting applies to a variety of scenarios, including 1:1 and group spaces. The policy is enforced when users are added to existing spaces and also during new space creations that involve membership additions.

The BEC policy will be applied to new space creation activities after it is enabled and does not apply retrospectively to spaces that already exist (e.g., spaces that were created prior to the BEC policy being turned on for an organization). Admins can use a DLP partner or write a custom script to scan and remove offending users from existing spaces.

Integrations management

Control Hub has the capability to allow administrators to set policies regarding access to integrations by their users. With this capability, a customer can whitelist third-party applications created using APIs from developer.webex.com, ensuring only the apps meeting their security and data handling standards will be enabled for their users. This capability is rish with many features You can review more details at the Webex Help Center online.

Bot management – space membership

Similar to the already existing Integrations management, where administrators can reduce the outflow of information to third-party Integration systems via Control Hub toggles, there is now the ability to manage bots, currently in controlled availability / trial mode, in an equivalent way. Administrators can set global policies to allow or deny bots for their organization. In case of "global deny," individual bots can be whitelisted and therefore made available in group and direct spaces for org employees to communicate with. All an IT admin needs to know is the globally unique email address for the bot to put them onto the whitelist. For now, bot management does not apply to existing bot memberships, (e.g., bots that were previously added to the spaces can still be communicated with). In mixed spaces, where the space owner, the inviter, and the bot potentially belong to different organizations policies from all three entities, they will be evaluated, and the bot admitted only where none of the organization policies prohibits such action.

Archival integration

Customers can use the Cisco Webex Events API to integrate with archival software. As with DLP, there are three ways to approach archival integration: an out-of-the-box solution, and end-to-end custom solution, or a DIY solution.

Audit administrator activity

A log of admin actions is a requirement for compliance in many organizations and industries. Full administrators can now view significant actions (such as changes to organizational settings) done by any administrator via the admin audit log stored in Control Hub. These admin audit logs can be viewed in Control Hub, where you can search for admin actions during a specific date range or search a specific action or specific administrator. You can also download the logs to a Comma-Separated Values (CSV) file.

Legal Hold

The Legal Hold feature gives users who hold a compliance officer role the ability to preserve all forms of relevant Cisco Webex Teams content associated with users when litigation is reasonably anticipated, regardless of the organization's retention policy. Compliance officers can create a legal matter and put custodians (users) on legal hold, view and download matters, and release matters. Data on legal hold is not subject to deletion based on the organization’s retention period. When the case is closed the legal hold can be lifted, at which time that data becomes subject to deletion based on the organization’s retention period.

Enterprise content management integration

In addition to its native file sharing and storage, Cisco Webex Teams also allows IT administrators the flexibility to enable Microsoft OneDrive and SharePoint Online as an enterprise content management (ECM) solution to their users. Users can share, edit, and grab the latest OneDrive and SharePoint Online files right within Webex Teams work spaces.

The setup is a single toggle in Webex Control Hub. And it requires no change to the existing file-sharing permissions and Data Loss Prevention (DLP) policies. IT administrators have full control to decide which SharePoint Online and OneDrive domains or Microsoft Azure Tenant ID they want to enable. This ensures that only IT-approved domains are available and users cannot use personal OneDrive folders. This not only eliminates data loss risk, but also protects against malware threats.

For the highest level of control, IT administrators can even turn off native file storage in Webex Teams so that all content is routed through their existing enterprise file storage service. New files and folders can be uploaded to OneDrive and SharePoint Online right from Webex Teams, as well as sharing, viewing, and co-editing files within Webex Teams.

The Cisco Webex Teams ECM integration solution:

- Allows IT administrators to enable Webex Teams native file storage or Microsoft OneDrive and SharePoint Online, or both, for file sharing and storage
- Allows people to share, open, edit, and co-author files from their ECM system, right in their Webex Team space
- Allows people to upload files and folders into their ECM system, right from their Webex Team space
- Allows people to define who can see and co-edit any shared files
- Ensures that people can always see the latest version of any file
- Encrypts links to ECM files, messages, and whiteboard drawings, end to end
- Works with existing DLP and doesn't create additional copies of files as they are shared in Webex Teams spaces
- Blocks personal or shadow IT OneDrive or SharePoint Online folders, and only allows approved instances

Summary of compliance features

Table 3 summarizes the compliance features of Webex Teams.

Table 3. Compliance features

Feature	Description
E-discovery report: Email- and space-based search	Compliance administrators can search and extract content using user email addresses or space names. Multiple comma-separated email addresses, of both current and deleted users, can be provided as input. The hard limit for the number of email addresses is 500 with the ability to generate large reports in the multi GB range.
E-discovery report: Time window	Compliance administrators can provide a time window to which they would like to restrict their search. **Standard offer:** Search data generated during the last 90 days. **Pro Pack:** Search data beyond the past 90 days.
E-discovery report download	Compliance administrators can view a list of past reports and download them in EML format. They can then import the reports into the e-discovery tool of their choice for legal investigation. Optionally compliance administrators can also exclude attachments from their downloads to inspect only messages and identify spaces or users of interest. The reports are available for 10 days. Large reports in the multi GB range can be generated and downloaded.

Feature	Description
Retention	**Standard offer:** Indefinite retention. Not configurable. **Pro Pack:** The administrator can set the retention period for data in Webex Teams. After this period, all content (files, messages, and events) will be purged and irretrievable. The minimum retention period is 1 month. The default retention period is indefinite. The retention period can be set in increments of 1 month up to 120 months. The retention policies apply to all spaces in Webex Teams.
Legal Hold	**Standard offer**: Not available. **Pro Pack**: Users with a compliance officer role in an organization can preserve all forms of relevant Cisco Webex Teams content associated with users when litigation is reasonably anticipated, regardless of the organization's retention policy. Compliance officers can create a legal matter and put custodians (users) on legal hold, view and download matters, and release matters.
DLP: Enlisting users	The Webex Teams app has features that enable you to enlist users in the process of DLP. Users are informed about space ownership, retention, and the presence of external participants. Message propagation is controlled via message deletion, read receipts, space locks, and moderator inheritance.
Webex Events API: DLP	The Webex platform exposes the Webex Events API. This API can be integrated with DLP software to check for policy violations and take action to remediate any issues. Events include posting of messages and files and addition of users to spaces. The action taken could be alerting the user or administrator, deleting the message, etc. **Standard offer:** Real-time API usage. Custom data range should be within the past 90 days. **Pro Pack:** Real-time API usage. Custom data range within the period of time data retention is set for and available.
Webex Events API: Archival integration	The Webex Events API can be consumed by archival software to archive Webex Teams data. **Standard offer:** Real-time API usage. Custom data range should be within the past 90 days. **Pro Pack:** Real-time API usage. Custom data range has no limits.
Enterprise content management integration	Cisco Webex Teams also allows IT administrators the flexibility to enable **Microsoft OneDrive and SharePoint Online** as an Enterprise Content Management (ECM) solution, in addition to its own native file sharing and storage. The result is that users can share, edit, and grab the latest OneDrive and SharePoint Online files, right within Webex Teams work spaces. **Standard offer:** Microsoft OneDrive and SharePoint Online Integration but no ability to disable Webex native file storage. **Pro Pack:** Microsoft OneDrive and SharePoint Online integration with the ability to disable Webex Teams' native file storage.

Feature	Description
Block External Communication (BEC)	Webex Teams administrators can enable cross-organization (by allowing space memberships with users from a different organization) collaboration and leverage the full power of the collaboration platform while protecting their organization and users from exposure to untrusted domains. Admins can easily create a whitelist of approved domains and ensure that users can communicate with participants from trusted domains only. Admins can configure up to **1000** domains as part of their whitelist. The inline policy enforcement (addition of users to spaces is allowed only after determining that the user belongs to a domain that is part of the organization's whitelist) minimizes exposure to users from untrusted domains and data leakage. **Standard offer**: BEC is not included as part of the standard offer. **Pro Pack:** Full features with the ability to whitelist up to **1000** domains
Bot management	Webex Teams administrators can set bot management policies to globally allow or deny bots. In case of global deny individual bots may be whitelisted by their unique email address. Mixed spaces with the participation of different org members are evaluated based on the most restrictive policy as it relates to space owner, inviter and invitee org (bot). **Standard offer:** Global allow or deny for bot management. **Pro Pack:** Individual bot whitelist where the global flag is set to deny.
Integration management	**Standard offer:** An administrator can enable or disable access to all integrations by their users. **Pro Pack:** An administrator can choose to enable or disable specific integrations for all users or a specific set of users, monitor the adoption of integrations by their users, revoke access of integrations, and download the list of email address for users who are actively using an integration. When an integration is disabled for an organization, a user will not be able to authorize an integration to be added to a space and take action on behalf of the user.

Frequently asked questions

Q. As a compliance officer, can I search for content posted by my company employees in spaces that my company does not own?

A. Yes, compliance officers can search for content posted by their organization's employees in any space that their employees belong to.

Q. What if the customer has deployed a CASB or an archival system that Webex Teams does not have a certified integration with?

A. In that case there are two additional options. You can:

- Build an integration between Webex Teams and the CASB or archival system using the Events API
- Work with Cisco Advanced Services to build the integrations using the Events API

Q. What are the different types of events exposed through the Events API?

A. The Events API captures the following events:

- Posting a message
- Posting a file
- Deleting a message or file
- Adding a user to a space
- Removing a user from a space
- Whiteboard snapshots

Cisco Capital

Flexible payment solutions to help you achieve your objectives

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

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA

C78-740772-02 09/19