Data Sheet

# 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, and 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 user 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. So 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 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. Ref: 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 that may be required for legal investigations. Data can be searched using email addresses, space IDs, or keywords. The interface also allows the compliance officer to specify a time window.

The search report can be downloaded in JSON format. Optionally, the administrator can use the reference script provided by Webex Teams to convert the JSON output into Concordance format and then export it into e-discovery software. 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, messages, files, and space IDs.

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

You 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. While the default retention period is indefinite, enterprises can override this default by setting a minimum retention period in increments of one month. After the retention period is reached, all the content (messages, activities, and files) is purged and becomes irretrievable.

## 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.

## 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.

## Retention

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.

## 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. So 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 CASB

- 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 users’ email addresses or space IDs. Multiple comma-separated email addresses can be provided as input. The hard limit for the number of email addresses is 5, but the aggregate size of the report is limited to 5 GB. |
| **E-discovery report: Keyword-based search** | Compliance administrators can provide one or more comma-separated keywords of interest when they’re searching. These keywords could be entered in combination with an email address or a space ID. |
| **E-discovery report: Time window** | Compliance administrators can provide a time window to which they would like to restrict their search.<br>**Standard offer:** Search data generated during the last 90 days<br>**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 JSON format. They can then export the reports into the e-discovery tool of their choice for legal investigation. The reports are available for 10 days. The size of the report is limited to 5 GB. |
| **Retention** | **Standard offer:** Indefinite retention. Not configurable.<br>**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.<br>**ProPack**: 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. |

| Feature | Description |
|---|---|
| **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.<br>**Standard offer:** Real-time API usage. Custom data range should be within the past 90 days.<br>**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.<br>**Standard offer:** Real-time API usage. Custom data range should be within the past 90 days.<br>**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.<br>**Standard offer:** Microsoft OneDrive and SharePoint Online Integration but no ability to disable Webex native file storage.<br>**Pro Pack:** Microsoft OneDrive and SharePoint Online integration with the ability to disable Webex Teams' native file storage. |

## 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 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 USAs C78-740772-01 03/19