Datasheet

Control Hub

Compliance

webex by CISCO

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 merger and acquisition information, credit card numbers, social security numbers, intellectual property, patient records, etc. Webex, via its open API ecosystem, has integrated with several Data Loss Prevention (DLP) and archival solutions to ensure your data security and integrity. The impact of a breach can be severe, so Webex has introduced Control Hub visibility and controls via partner integrations to allow customers to manage the adherence to their compliance policies. Control Hub is a web-based, intuitive, single-pane-of-glass management portal that enables you to provision, administer, and manage Webex services.

The Pro Pack for Control Hub is a premium offer for customers that require more advanced capabilities and fine-grained controls in coordination 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 into easy to search reports.

Enterprises also prefer to control exposure and limit their liability by automatically purging data that has no business value, in regular intervals. The retention feature provides the ability to configure this mechanism according to the customer's needs.

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 be purged by an organization-wide retention policy during investigations.

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

Webex Space ownership

Webex supports and encourages collaboration across the boundaries of organizations. As such, it is possible that users can communicate with colleagues in other companies. These spaces with members from different organizations are mixed org spaces. For reasons of compliance assertions any space, including mixed org spaces, are always attributed to a specific org. To deal with this, Webex uses the concept of space ownership. The ownership rules differ between group spaces and direct spaces where two individuals communicate.

Webex 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 space	Yes	Yes
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 in Control Hub	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

Webex 1-to-1 (direct) spaces with participants from two different organizations provide shared ownership between the two organizations. 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 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 in Control Hub	Yes
Delete content posted by any user into the space	No
Delete content posted by its own users in the space	Yes

Events API

The events API is a Compliance Officer accessible REST endpoint. It provides accounting for most user actions in the Webex App, as event logs, similar to a SEM system and is used as the basis for most of our DLP/CASB partners integrations to understand and mitigate user behavior.

Webex allows users to communicate with others 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.

Webex Meetings allows users to invite participants from within their company or outside the organization as guests to a meeting they host.

For Common-Identity (CI) linked and enabled sites, the Webex Events API provides the compliance officer of the host organization with access to meeting events, recordings, and transcripts. Meeting-related data (and metadata) is accessible only by the compliance officer of the host's organization.

Other meeting specific events in support of enterprises' demand to archive and account for any eCommunication, includes in-meeting chat messages (including breakout sessions), in-meetings poll and Q&A, in-meeting closed captions retrieval as well as a ledger of meeting invitees and who got dropped from the invitation verses who participated.

Webex Calling allows users in an organization to make and receive internal and PSTN calls from devices or the Webex App. These call events can be retrieved using the Events API for analysis or archival. Data in the events include call participants and numbers, call duration, call date and time, and other call information.

E-discovery: Search and extraction

Compliance officers can use the web accessible e-discovery search and extraction console to extract data created by users in their 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 a compacted 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. The search report will also include transcripts generated for meetings hosted by users in the compliance officer's organization. Compliance officers have the option to include Webex Messaging, Webex Meetings or Webex Calling content in the eDiscovery report.

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 Control Hub. The report summary shows information such as the number of users, activity, file, whiteboard count, space IDs, meetings, recording information, call records, and other metadata 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 and separate retention period for Webex Messaging and Webex Meetings which will apply to the entire Organization. Call records will follow a preset 13 month retention period. This is not configureable by the admin. With the Pro Pack for Control Hub, full administrators can set the retention period 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 align retention policies across email and other applications.

Organizations can set separate retention values for 1-on-1 and Group chat spaces in the Webex App. This setting applies to all space content created by users in the Organization. This granular retention setting allows organizations to stay compliant with corporate policies without compromising employee productivity in Group spaces. Organizations have more control over the lifecycle of content generated in Webex App spaces and can manage retention policies in accordance with

Data Loss Prevention (DLP)

Webex has a twofold DLP strategy. First, users are in the know about the environment they collaborate in. Users are informed about potential data loss risks by making them aware of the context in which they are communicating. Specifically, users are informed about space ownership, retention policies applied, space classification and the presence of external participants.

The second part of the strategy involves monitoring user actions such as posting or deleting a message, attaching a file, and adding a user to or removing a user from a space in Webex App, as events, via APIs

so that they can be consumed by DLP software to check for and remediate violations. A Compliance Officer administrator can use the Webex Events API to poll for events to retrieve user content in order to monitor and respond to user behavior.

In addition to Webex Messaging, events and metadata related to Webex Meetings and transcripts are also available via the Events API. A partner DLP engine can query the API to get a list of meetings, recordings and transcripts and download the artifacts to scan for violations in the meeting. In addition, we also provide Compliance Officers with the ability to redact the meeting transcripts or delete the transcripts

We are celebrating our new methodology on how Webex DLP compliance can be consumed with the advent of real-time file DLP. Real-time file DLP allows DLP vendors to scan and assess files before they are seen and can be downloaded by other users. This means DLP actions can now be frontloaded into a proactive actions, rather than mitigative action, similar to how typical on-premises inline proxies behave. We are intending to extend our real-time features to other users' actions in the coming months.

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 Messaging and Webex Meetings via the Events API to offer turnkey DLP capabilities for Webex. 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 Webex Messaging 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 admins can configure a permitted list of trusted and authorized external domains 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 permitted list, 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 permitted list. In cross-organization spaces, where the space owner, inviter, and invitee belong to different organizations, the domain permitted list 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.

In addition to the Org wide policy settings above, admins can also create granular policies to be applied to users in specific Active Directory (AD) groups. We currently support BEC policies backed by AD Groups only, Org admins need to ensure that Directory Connector is enabled (Directory Connector Deployment Guide) and AD Group information for users is synced from the Organization's Active Directory servers.

With this enhancement, admins can open external collaboration to users from select AD groups only, while conforming to the Organization's security posture and external collaboration rules. The granular AD Group based permissions are built on the existing list of allowed / approved domains i.e. users from selected AD Groups can collaborate with external users who belong to the approved list of domains only. For eg. Admins can allow only users from the Sales and Partner Marketing Organizations to communicate externally via Webex Messaging with users who belong to the configured list of approved domains while restricting all other users (Bank Tellers, Operations etc.) to internal communications.

Policy evaluation and enforcement occurs in real-time (retroactive evaluation and policy enforcement is not supported)

With the bulk domain add workflow, admins can create a list of domains (total of 2000 domains with a 500 domain limit per import) and import it into Control Hub. The workflow allows admins to check for unverified, unclaimed domains or any syntax (RegEx) errors for the list of domains in the import file. Admins can fix any outstanding errors before completing the import.

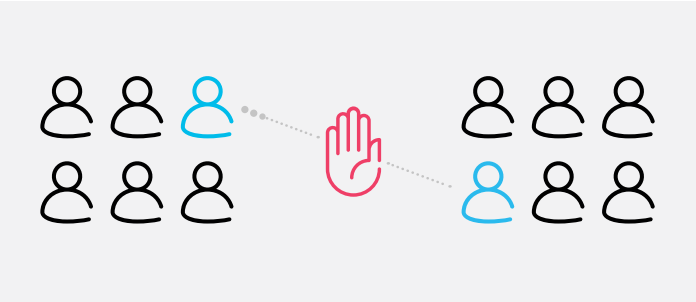
This will greatly reduce the setup time for admins who need to add a large number of domains to their Organizations' list of approved domains.

Granular AD Group based BEC with deny list:

Webex admins can configure a list of untrusted external domains to protect users from their organization communicating with unauthorized and risky external actors. When users attempt to create a space and invite participants from external organizations who belong to a domain that is part of their organization's configured deny list, 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 (i.e., membership denied) 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 can be applied to all users in the Organization or granularly to a specific set of users who belong to certain Active Directory (AD) Groups.

Block Internal Communications (BIC): Ethical Wall

Ethical walls (also known as Block Internal Communication) allow administrators to define simple rules in Control Hub to prevent certain groups of users from collaborating with each other via Webex Spaces. Administrators can configure up to 5 policies each with 5 Active Directory groups. Once policies are defined, restricted groups cannot invite each other to spaces or initiate conversations; however, they can still communicate with users in the rest of the company. Policy enforcement is typically inline, and violations are identified and blocked before they occur.



For example. At a large bank, investment bankers and company research analysts must not communicate to avoid a conflict of interest. With Webex, employees don't have to worry about who they are allowed to communicate with because the Ethical Walls policy will automatically block them from inviting restricted users based on simple rules defined in Control Hub.

This feature ensures that organizations maintain compliance with relevant company standards and regulations (e.g., FINRA), and avoid potential conflicts of interest.

The Ethical Walls feature acts in a forward and retroactive manner after it is enabled by the admin in Control Hub. Ethical Walls actively and retroactively scan for existing violations in Webex spaces and enforce the configured policy for those spaces that are out of policy compliance. When violations are found, Webex will try to remedy the situation. This scenario typically occurs when users switch jobs and undergo an AD group membership change. Often when membership changes occur, they may be in violation of the Ethical Wall policies. Ethical Walls policy enforcement applies to both 1-on-1 and Group Spaces but in different ways. The 1-on-1 spaces in violation are set to Read Only mode, which will allow users to read historical content in the space but will not allow either user to post new content. For Group spaces, the violating user(s) will be removed from the space to ensure that the configured policies are adhered to by the users.

Integration management

Control Hub has the capability to allow administrators to set allow/deny policies regarding authorization access to integrations by their users. With this capability, a customer can selectively allow 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. In addition, administrators can revoke access to integrations and prevent future authorization. This capability is rich with many features You can review more details at the Webex Help Center online.

Bot management: Space membership

Like the Integrations management, where administrators can reduce the outflow of information to third-party Integration apps via Control Hub settings, there is an additional capability to manage bots. Control Hub administrators can set global policies to allow or deny bots for their organization. In case of "global deny," individual bots can be allowed 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 allowed list. 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 will be evaluated, and the bot admitted only where none of the organization policies prohibits such action.

Archival integration

Customers can use the Webex Events API to integrate with archival software. As with DLP, there are three ways to approach archival integration: out-of-the-box solutions with partners, end-to-end custom solutions through partner or advanced services engagement, 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 and also exposed via REST API. These admin audit logs can be viewed in Control Hub, where you can search for admin actions during a specific date range or search for 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 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, 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 released, at which time that data becomes subject to deletion based on the organization's retention period.

Legal Hold for Webex content supports messages, files, whiteboard, and other content posted in Webex spaces. Additionally, Webex Meetings content such as recordings, transcripts, and highlights, as well as Webex Calling Call Detail Records (CDRs) are supported.

Enterprise content management integration

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

The setup is configured as a single toggle in 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, eliminating data loss risk, while simultaneously protecting against malware threats. Similarly, admins can also decide which email domains to allow for Google drive.

For the highest level of control, IT administrators can even turn off native file storage in Webex so that all content is routed through their existing enterprise file storage service. New files and folders can be uploaded to OneDrive, SharePoint Online, Google Drive, and Box right from Webex, as well as sharing, viewing, and co-editing (not supported in Box) files within Webex.

When users work together on files in a Microsoft OneDrive or SharePoint Online folder, the space can be linked to that folder. Users can then access the files in the linked folder directly from the Webex space and set as the default storage for the spaces (based on Control Hub settings). In such cases, all files shared in the space (including screen captures) will be stored in the linked ECM folder itself, and not in Webex native storage.

The Webex ECM integration solution:

- Allows IT administrators to enable native file storage or Microsoft OneDrive, SharePoint Online, Box and Google Drive for file sharing and storage
- Allows IT administrators to enable linking of folders to spaces with options for default storage for Microsoft OneDrive and SharePoint Online integration.
- Allows people to share, open, edit, and co-author files from their ECM system, right in their Webex Team space
- Allows collaborators to upload files and folders into their ECM system, right from their Webex space
- Allows people to define who can see and co-edit any shared files for Microsoft OneDrive and SharePoint Online
- Ensures that collaborators will 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 does not create additional copies of files as they are shared in Webex 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.

Table 3. Compliance features

FEATURE	DESCRIPTION
E-discovery report: Email and space-based search	Compliance administrators can search and extract messaging, meeting and calling 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 to. **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. 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:** Meetings and Messaging Retention is 360 days. Webex Calling retention is 13 months for CDRs and is not configurable. For current retention details see this link. **Pro Pack:** The administrator can set the retention period for data in Webex Messaging and Webex Meetings. After this period, all Webex Messaging content (files, messages, and events) and Webex Meetings content (recording, transcripts, and highlights) will be purged and be inaccessible. The retention policy applies to all spaces in Webex. The Webex Meetings retention policy applies to all meeting recordings, transcripts, and highlights. Administrators can also set a separate retention policy for content generated by users in 1-on-1 verses Group spaces in the Webex App. Retention of space content generated in 1-on-1 and Group spaces will follow the retention value set for each space type and content will be purged accordingly. The separation of retention settings between 1-on-1, and Group spaces allows admins to exercise more granular control over the lifecycle of content generated by users in their Org.
Legal Hold	**Standard offer:** Not available. **Pro Pack:** Users with a compliance officer role in an organization can preserve all forms of relevant 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. Legal Hold supports Webex Messaging, Webex Meetings and Webex Calling content.
Webex Events API: DLP	The Webex Events REST API can be integrated with DLP software to check for policy violations and take action to remediate any issues. Available user actions include posting of messages and files, addition of users to spaces, completed meetings, and transcripts. The action taken could be alerting the user or administrator, deleting the message (messaging only), throwing an alarm or others as defined by the DLP policy. **Standard offer:** Real-time events API access. Custom data range should be within the past 90 days. **Pro Pack:** Real-time events API access. 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 Messaging, Webex Meetings and Webex Calling data (CDRs). **Standard offer:** Real-time events API access. Custom data range should be within the past 90 days. **Pro Pack:** Real-time events API access. Custom data range has no limits.
Enterprise content management integration	Webex also allows IT administrators the flexibility to enable Microsoft OneDrive, SharePoint Online, Box, and Google Drive 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 (not supported in Box), and grab the latest OneDrive and SharePoint Online files, right within Webex spaces. Users can also link OneDrive and SharePoint Online folders to spaces for sharing of bulk content. Additionally, they can make these folders default storage for the spaces. **Standard offer:** Microsoft OneDrive and SharePoint Online, Box and Google Drive Integration but no ability to disable Webex native file storage. **Pro Pack:** Microsoft OneDrive and SharePoint Online, Box and Google Drive integration with the ability to disable Webex native file storage.

FEATURE	DESCRIPTION
Block External Communication (BEC)	Administrators can enable cross-organization collaboration (by allowing space memberships with users from a different organization) and leverage the full power of Webex while protecting their organization and users from exposure to untrusted domains. Admins can easily create a list of approved or denied domains and ensure that users can communicate only with trusted domains. Admins can configure up to **2000** domains as part of their allowed list. Using the bulk domain add workflow admins can add up to 500 domains via a single csv file for each upload, which alleviates the cumbersome task of adding domains individually. 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 allowed list and not in the deny list) minimizes exposure to users from untrusted domains and data leakage. Admins can also allow external communication to selected users from their Active Directory groups or prevent users in certain AD Groups from communicating externally. **Standard offer:** BEC is not included as part of the standard offer. **Pro Pack:** Fully featured with support for up to **2000** domains.
Block Internal Communication (BIC) – Ethical Wall	Enables IT admins to prevent certain groups of users within their organization from communicating with each other. It helps organizations maintain compliance with relevant industry standards and regulations (e.g., FINRA), and avoid potential conflicts of interest. **Standard offer:** None **Pro Pack:** Fully featured for inline policy check.
Bot management	Administrators can set bot management policies to globally allow or deny bots. In case of global deny, individual bots may be selectively permitted 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-only allow or deny for bot management. **Pro Pack:** Individual bot permitted list 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 act 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. As a compliance officer, can I search for meeting transcripts and recordings for meetings hosted by employees of my company?

A. Yes, compliance officers can search for meeting transcripts and recordings for meetings hosted by their organization's employees on their organization meeting sites.

Q. As a compliance officer, can I search for meeting transcripts and recordings for meetings hosted on external company meeting site?

A. No, compliance officers cannot search for meeting transcripts and recordings for meetings hosted on external organization meeting sites.

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

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

Build an integration between Webex 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
- Downloading a file
- Deleting a message or file
- Adding a user to a space
- Removing a user from a space
- Whiteboard snapshots
- Meeting event
- Transcript event

Frequently asked questions

Q. Are non-Webex Calling Calls included in compliance?

A. Only Webex Calling Calls produce CDRs and Events. Basic “Call on Webex” Calls will not be included.

Q. Is other Webex Calling data included in Compliance?

A. Only CDRs are supported. Voicemails, Voicemail Transcriptions, Call Recordings and Call Transcriptions will be available in the near future.

Cisco environmental sustainability

Information about Cisco's environmental sustainability policies and initiatives for our products, solutions, operations, and extended operations or supply chain is provided in the "Environment Sustainability" section of Cisco's Corporate Social Responsibility (CSR) Report.

Reference links to information about key environmental sustainability topics (mentioned in the "Environment Sustainability" section of the CSR Report) are provided in the following table.

SUSTAINABILITY TOPIC	REFERENCE
Information on product material content laws and regulations	Materials
Information on electronic waste laws and regulations, including products, batteries, and packaging	WEEE compliance

Cisco makes the packaging data available for informational purposes only. It may not reflect the most current legal developments, and Cisco does not represent, warrant, or guarantee that it is complete, accurate, or up to date. This information is subject to change without notice.

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.