Datasheet

Control Hub

Extended Security Pack (ESP)

webex by CISCO

Contents

Webex® connects people with each other and their work, whether you are collaborating with partners or working with your own customers.

Webex delivers highly secure world-class messaging, meetings, and calling experiences from your pocket to the boardroom, to optimize and modernize employee and customer experiences.

Product overview

Enterprises require controls to ensure their employees don't accidentally or intentionally send sensitive and critical information via collaboration tools. Examples of such information include intellectual property, patient records, credit card numbers, and social security numbers.

IT administrators also need to protect against malware and ransomware that may get distributed when sharing files externally or when using devices that aren't managed by their corporate IT teams.

The Extended Security Pack for Control Hub can help you protect your company's data, your partners, and your customers by bundling data loss prevention and anti-malware capabilities in an add-on flex collaboration offer.

The Extended Security Pack provides collaboration administrators with agility and peace of mind so they can more securely deploy Webex in their enterprises by addressing all information security concerns in one tightly integrated solution.

Data Loss Prevention (DLP)

The Extended Security Pack includes the full set of functionalities from Cisco Cloudlock® for Webex. Cloudlock enables organizations to more securely adopt Webex by providing full visibility and control over sensitive data stored in Webex. Cloudlock identifies critical information such as Personally Identifiable Information (PII), Personal Health Information (PHI), and Payment Card Information (PCI) as well as other proprietary information to adhere to regulatory compliance and internal data protection mandates. When sensitive information is detected in violation of customer policies, Cloudlock triggers incidents and automatically takes risk-appropriate actions such as notifying end users and admins of violations and deleting violating content (file or message) from a Webex space as well as Webex Meetings post-meeting transcripts and highlights. Figure 1 is a screenshot of an incident view within Cloudlock.

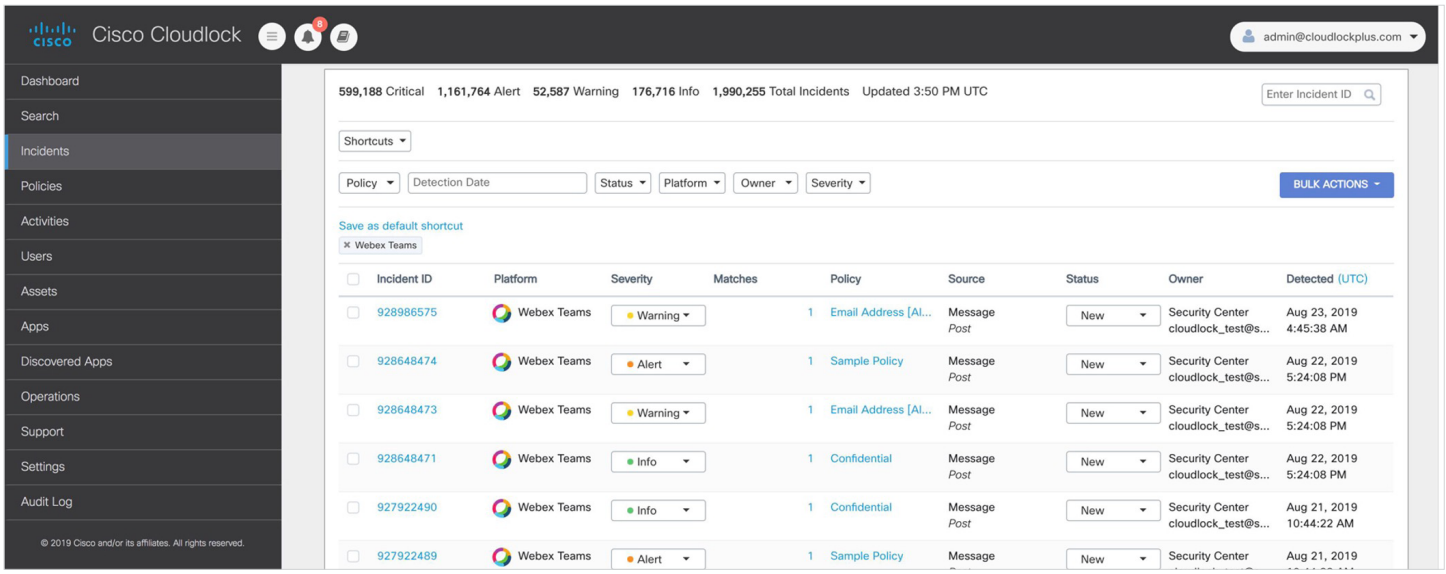


Figure 1. Cisco Cloudlock for Webex – Incident View

Key functionality highlights

Mitigate increased risk of data exposure in cloud applications

Combating data leakage in the cloud can be challenging given the collaborative nature of cloud environments and the ease with which they enable users to access, create, and share sensitive information. Organizations struggle to bridge the gap between legacy data protection tools and the limited level of visibility and control they provide within cloud environments. This is particularly true when cloud applications are being accessed by external users or remote and roaming employees who are not on the corporate network.

Identify sensitive data in cloud environments

Cloudlock continuously monitors Webex environments with a powerful cloud Data Loss Prevention (DLP) engine that can identify when sensitive information stored in cloud environments is in violation of policy. With Cloudlock, security professionals enforce out-of-the-box policies focused on common sensitive information sets, such as Payment Card Industry Data Security Standard (PCI-DSS) and HIPAA compliance, as well as custom policies to identify proprietary data such as intellectual property. Advanced capabilities such as custom Regular Expression (RegEx) input, threshold settings, and proximity controls help to ensure high true positive and low false positive rates.

Mitigate risk through automated responses

Cloudlock takes cloud DLP beyond discovery by offering configurable, cross-platform, automated response actions. Through an API-driven Cloud Access Security Broker (CASB) architecture, Cloudlock supports deep, integrated response workflows that leverage the native capabilities of Webex—from end user and admin notifications to the automated deletion of sensitive data. Figure 2 shows the web interface of Cloudlock's Automated Response.

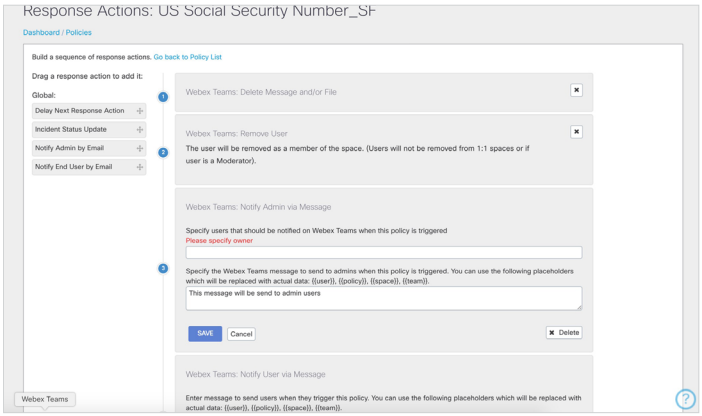


Figure 2. Cisco Cloudlock for Webex - Automated Response

Anti-malware capabilities

The Extended Security Pack includes a built-in anti-malware engine that scans all file uploads for Trojan attacks, viruses, malware, and other malicious threats. All files in spaces that you designate will be scanned and remediated, even if they are uploaded by external users.

Infected files will be marked clearly and end users will not be able to download them on both corporate-managed and personally managed devices. There is no limit on the number of files that can be scanned as part of this Extended Security Pack subscription. Figure 3 shows an instance of the Extended Security Pack blocking a file.

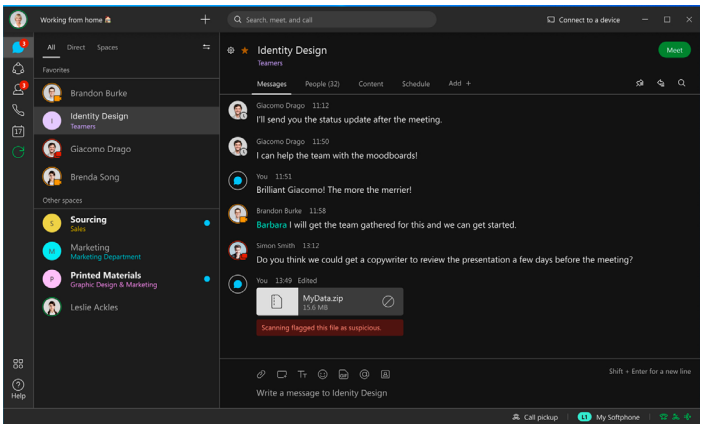
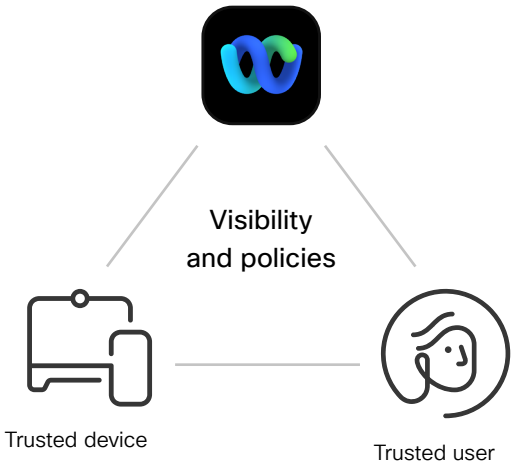


Figure 3. Anti—malware capabilities

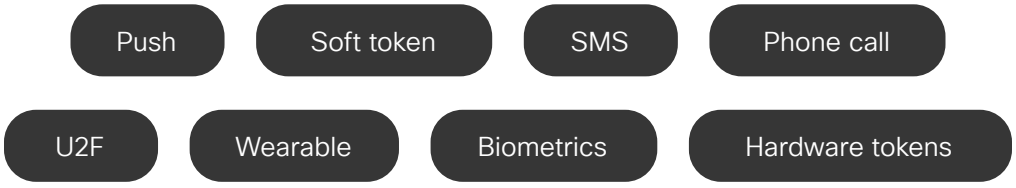
Zero trust multi-factor authentication

The Extended Security Pack (ESP) includes Duo Essentials. With this, customers can utilize Single Sign-On (SSO) and Multi-Factor Authentication for Webex to verify user trust quickly and securely, in every access attempt to keep your data secure. This helps not only improve end user productivity & experience but also enterprise security and risk posture while ensuring regulatory compliance. Duo provides the broadest range of MFA options such as Duo Push, Security Keys, Universal 2nd factor (U2F), one-time password (OTP), Phone callback, SMS and HW tokens.

With Duo, the MFA can be configured for the entire organization or specific groups of Webex users for ease of use and flexibility. Duo also delivers passwordless authentication, a term used to describe identity verification methods that do not rely on passwords. Biometrics, security keys, and specialized mobile applications are all considered “passwordless” or “modern” authentication methods and makes it more user friendly and as secure as traditional methods of MFA. Learn more about detailed instructions on how to setup Duo Single Sign-On for Cisco Webex.



Zero Trust Duo Multi-Factor Authentication



Ethical wall

Ethical walls (also known as Block Internal Communication) allows Webex administrators to define simple rules in Control Hub to prevent certain groups of users from collaborating with each other within Webex Spaces. Administrators can configure up to 5 policies each with AD (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 in line (i.e., violations are identified and blocked before they occur).

For example, at a large bank, investment bankers and company research analysts shouldn't communicate to avoid a conflict of interest.

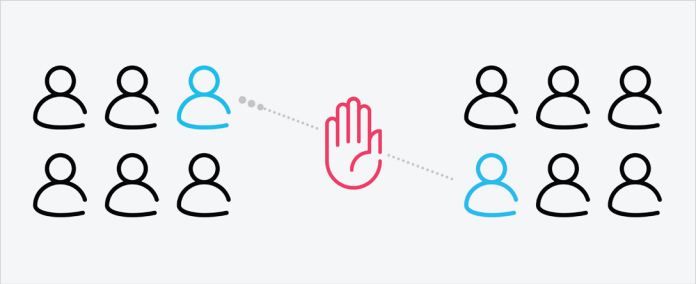


Figure 4. Ethical walls

With Webex, the end user does not have to worry about who they are allowed to communicate with because the Ethical Walls corporate policy Webex will automatically block them from inviting restricted disallowed users before it happens based on simple rules defined in the Webex Control Hub.

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

The Ethical Walls feature acts in a forward looking manner after it is enabled by the admin in Control Hub. Webex has the ability to retroactively scan for existing violations in Webex spaces, and when they are out of policy compliance, evict users and their violations from those spaces. This scenario typically occurs when users switch jobs and in the process undergo an AD group membership change.Due to this membership change, they may be in violation of one or more Ethical Walls policies.

Multiple Identity Providers (IdPs)

Multiple Identity Providers (IdPs) for a Webex Organization can help large enterprise customers solve complex deployments for authentication and authorization. This feature specifically helps customers who need to connect multiple IT organizations with different IDP's when they are undergoing a merger and acquisitions but need to communicate even though both organizations have their own Identity Provider. Government or Universities have various organizations, colleges or agencies that purchase centrally or share the same email domain but have different IT departments.

Multi-national organizations sometimes have subsidiaries that are in a country with their own separate IT organization and need to connect to the same Webex organization.

Webex has solved this problem by building a feature that allows the customer to configure multiple IDP's with the following features.

Choose the Federation Protocol right for your organization. Webex supports OpenID Connect (OIDC) or SAML to federate with Webex.

Webex Identity can be used for users that are not in your IDP. If a user lives outside your organization's IDP and you want them to use a username and password that Webex manages, you can choose Webex Identity as an Identity Provider.

Routing rules provide flexibility and control in your configuration. Routing rules allow administrators to route users to the right identity provider via a Group or Domain.

Security and Auditability: Admins must use a domain that is verified within their organization to route users if using domain-based routing. Admin alerts are on by default. Configuration changes are automatically added to your Audit Log.

Other Considerations for administrators. If you are an SMB or enterprise, you can use external users and external admins if you only have one or two users you need to authenticate outside your organization. Many enterprises have powerful security IDPs that allow you to federate across boundaries between organizations. Collaboration Admins should work in close consultation with their Identity and Security teams to evaluate the applicability of this feature to solve their requirements and ensure this configuration meets your enterprise compliance and security requirements.

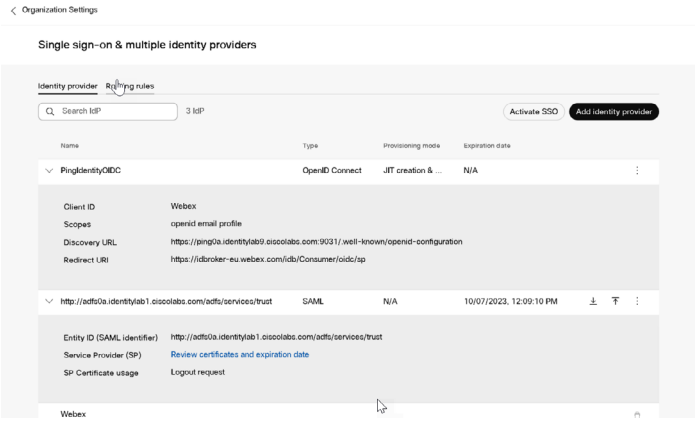


Figure 5. Single sign-on multiple identity providers 1

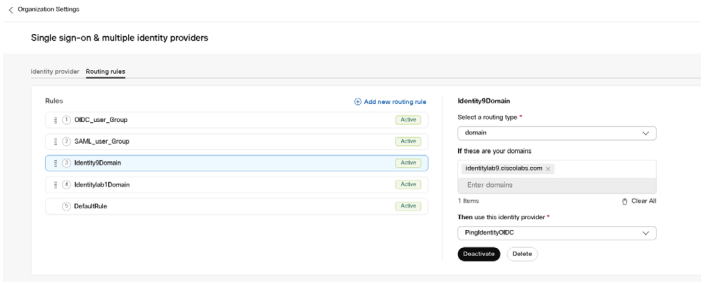


Figure 6. Single sign-on multiple identity providers 2

Summary of features

Table 1 summarizes the compliance features of Webex.

Table 1. Compliance features

FEATURE	DESCRIPTION
Data loss prevention	Use Cisco Cloudlock to: • Gain visibility into and control over sensitive information stored in Webex. Admins can leverage 80+ existing policies or create new custom policies • Mitigate the risk of cloud data leakage through powerful, automated response actions when sensitive data is discovered. When policies are violated, Cloudlock will automatically delete files or messages, notify users or admins, and remove users from spaces • Support adherence to compliance regulations within your cloud applications' security incident lifecycle directly from SIEM systems
Anti-malware	The built-in, high-performance anti-malware engine scans all file uploads for Trojans, viruses, malware, and other malicious threats. Infected files will be marked and cannot be downloaded by end users
Ethical Wall	Enables IT admins to prevent certain group of users within their organization from communicating with each other. It helps organization maintain compliance with relevant industry standards and regulations (e.g. FINRA), and avoid potential conflicts of interest
Multi-Factor Authentication	With Duo Essentials, IT administrators can enable Single Sign-On (SSO) and Multi-Factor Authentication for Webex. It can be configured for the entire organization or specific groups of Webex users with the ability to choose from a broad range of MFA options such as Duo Push, Security Keys, Universal 2nd factor (U2F), one-time password (OTP), Phone callback, SMS and HW tokens.
Multiple IDP Support	Webex Administrators can configure more than one federation IDP to authenticate users. Webex supports OIDC, and SAML IDPs. If users cannot use a federated IDP, then Webex Identity can manage the username and password for these users. Users can be routed via their Domain name if verified or claimed within the organization, or by creating a group of users.

Ordering information

The Webex Extended Security Pack can be purchased within the Collaboration Flex Plan subscription (A-FLEX). See the Collaboration Flex Plan Ordering Guide for details on how to add this feature to a Collaboration Calling and/or Meetings subscription.

Table 2. Product SKUs and descriptions

PID	PID DESCRIPTION
A-FLEX-NU-SEC-PK	Extended Security Pack NU add-on
A-FLEX-EA1-SEC-PK	Extended Security Pack EntW add-on for 250-1,999 KWs
A-FLEX-EA2-SEC-PK	Extended Security Pack EntW add-on for 2,000-9,999 KWs
A-FLEX-EA3-SEC-PK	Extended Security Pack EntW add-on for 10,000+ KWs
A-FLEX-AU1-SEC-PK	Extended Security Pack Active User add-on for 250-1,999 KWs
A-FLEX-AU2-SEC-PK	Extended Security Pack Active User add-on for 2,000-9,999 KWs
A-FLEX-AU3-SEC-PK	Extended Security Pack Active User add-on for 10,000+ KWs
A-FLEX-SEC-PK-ENT	Extended Security Pack Entitlement

Frequently asked questions

Q. Are Cloudlock functionality limitations in the Extended Security Pack?

A. No, the full functionality of Cisco Cloudlock is packaged in the Extended Security Pack. All you need to do is provision a compliance officer user in Control Hub and have that user authorize Cloudlock for Webex.

Q. If I like Cloudlock for Webex, can I use it to protect my other SaaS and cloud services such as Box?

A. Yes, you can buy additional licenses for Box and other SaaS services by contacting your account team or partner. Management for all application will be done via a single console.

Q. Can I only enable DLP capabilities because I already have a malware scanner on my devices?

A. Yes, there is a Control Hub setting to enable and disable malware scans.

Q. Will malware scanning delay my file uploads and impact user experience?

A. No, the anti-malware engine has high performance and files will be scanned within a few seconds. The files will be uploaded to spaces instantly, but they cannot be downloaded or previewed until the malware scan is complete. There is no visible difference to the end-user experience.

Q. Will administrators have the option to disable and enable malware scanning for their organization?

A. Yes, administrators will have option to disable malware scanning for their organization in Control Hub.

Q. Can I use Duo Essentials with any application other than Webex?

A. No., Duo Essentials included in Extended Security Pack, only licensed to be used for Webex.

Q. I already have Duo Essentials but would like to use Extended Security Pack (ESP) to make use of other capabilities included in ESP. How can I do this?

A. You can contact your Cisco account team for Webex and they be able to assist with providing Extended Security Pack license, including continued support for your existing Duo Essentials license.

Q. I have Extended Security Pack (ESP) and using Duo Essentials included in the bundle, but would like to use Duo Advantage or Duo Premier, which is not included in ESP. How can I do this?

A. You can contact your Cisco account team and they be able to assist you, so you have continued access to ESP and also able to move to higher editions of Duo.

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.

For more information
Please visit Webex Security

May 2023