

Cisco Spark Control Hub

(Management, Security, Compliance, and Analytics)

Contents

1. Cisco Spark Control Hub and Pro Pack	3
2. Service Management	3
3. Identity and Access Management	10
4. Data Security and Encryption	14
5. Application and Mobile Device Security Controls	18
6. Compliance (e-discovery, retention, DLP, archival)	20
7. Analytics	27
8. Cisco Capital	30

1. Cisco Spark Control Hub and Pro Pack

Overview

The Cisco Spark™ Control Hub is included with any paid subscription for Cisco Spark and provides visibility and control for Cisco Spark and Cisco WebEx®.

Cisco Spark Control Hub is a web-based, intuitive, single-pane-of-glass service that enables you to provision, administer, and manage Cisco Spark and Cisco WebEx¹ services. The Cisco Spark Control Hub also provides the ability to manage the Cisco Spark Hybrid Services (Hybrid Call Service, Hybrid Calendar Service, Hybrid Directory Service, and Hybrid Media Service).

The Pro Pack for Cisco Spark Control Hub is a premium offer for customers that require more advanced capabilities or even integrations with their existing security, compliance, and analytics software. Access can be provided specifically to those that need these more advanced capabilities – for example, information security professionals or compliance officers.

2. Service Management

User and Device Management

Cisco Spark Control Hub makes user onboarding simple. The service provides customers and partners the ability to manage identities during the creation, update, and deletion process, either manually, via a CSV upload, with the Active Directory synchronization tool,² or via APIs that follow the industry-standard System for Cross-Domain Identity Management (SCIM). There is also a Convert Users flow for bringing free users who already have a Cisco Spark account into the paid Cisco Spark organization to be managed by the customer.

¹ The Cisco Spark Control Hub supports Cisco WebEx customer sites that are net-new Cisco WebEx customer sites purchased with A-SPK. All A-SPK renewals, A-WX renewals, and A-WX net-new Cisco WebEx customer sites will need to go through a process to allow Cisco Spark Control Hub to view Cisco WebEx reports.

² Organizations can synchronize their Microsoft Active Directory on-premises with the Cisco Spark service in the cloud. This directory synchronization automatically adds and deletes users and securely eliminates the need to manage multiple directory databases for services from the Cisco Spark Platform.

Manage Users

Add Services for Users
Select the service entitlements that you want to provide to users.

Message	Meeting	Call
Free Public Collaboration Services		
Message Free	Meeting Free 3 Party	Call Free
Licensed Collaboration Services		
Message <input type="checkbox"/> Cisco Spark Messaging Named User License	Basic Meetings <input type="checkbox"/> Cisco Spark 25 party Meetings Named User License •	Call
	Advanced Meetings <input type="checkbox"/> WebEx Meeting Center 200 Named User License • <input type="checkbox"/> WebEx Collaboration Meeting Rooms frontline.my.webex.com	

Back Save

Once users are added, it is very easy to manage all user settings from Cisco Spark Control Hub. All the service settings for each user provisioned on the Cisco Spark Platform can be managed from the user detail pane. Cisco Spark Control Hub also provides a simple interface to manage all Cisco Spark services (Meetings, Messaging, Calling, Cisco Spark Hybrid Services, and Cisco WebEx) from the Services tab.


Cisco Spark Control Hub also provides role-based access so that different levels of administrator access can be set up for customers and partners. The roles assigned are listed in the user detail pane for each user.

Cisco Spark Control Hub also provides a simple interface to onboard and activate devices (personal and shared devices). The device onboarding can be done easily using a 16-digit activation code or QR code generated in Control Hub. Once the devices are onboarded, the device listing in Cisco Spark Control Hub provides visibility into device details and state. If there are any issues with the device that need attention (cable unplugged, upgrade requirements), the message is clearly listed on the device details page.


New Device

What kind of device do you want to set up in this place?

A new device requires a unique activation code to be input during setup. What kind of device do you want to activate?



Desk Phone
e.g. 8845, 8865 or 8800



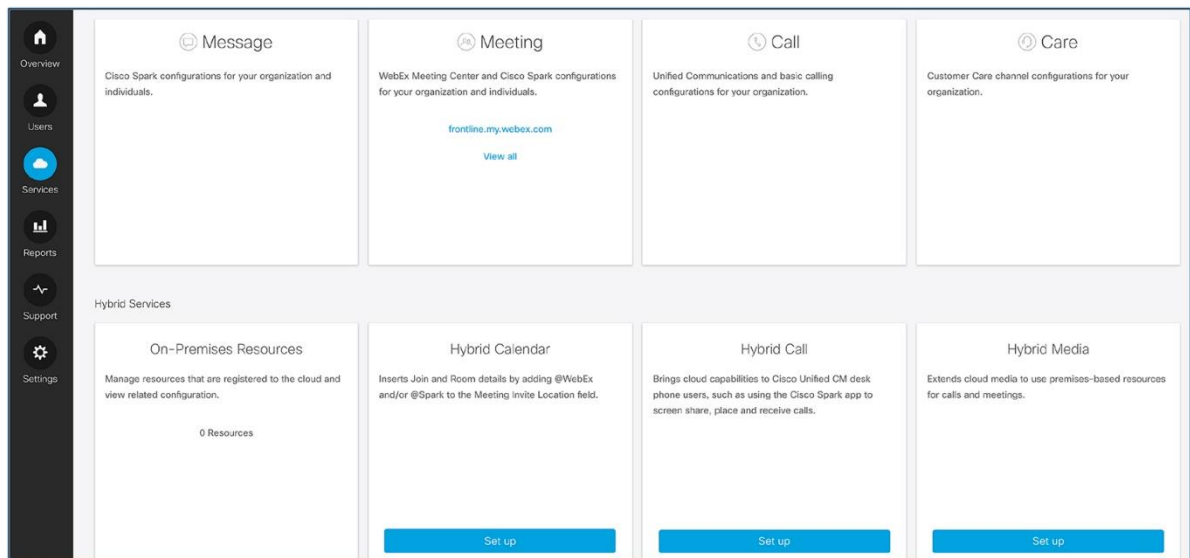
Room Device
Cisco Spark Board, DX, MX and SX series

Single Sign-On

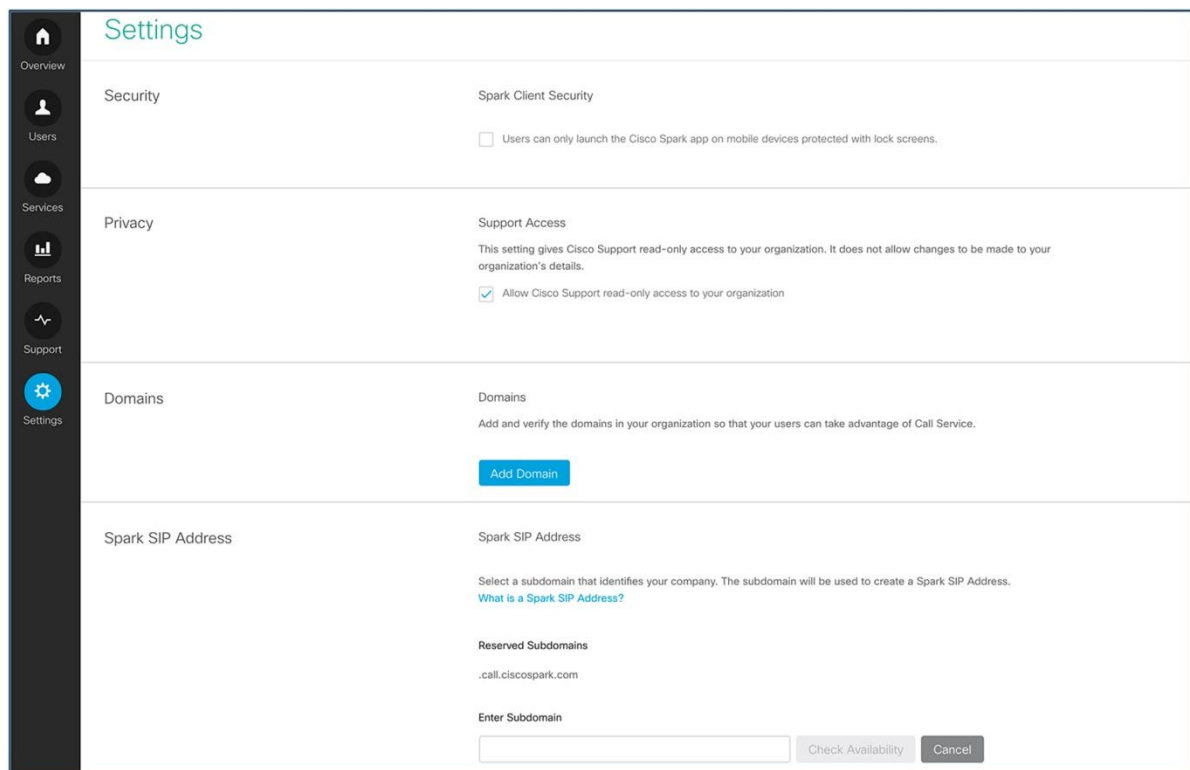
Integrating Single Sign-On (SSO) services helps ensure that users enter their IT-approved password to access Cisco Spark. Role-based access creates access rights and usage levels for different personas in an organization, such as administrators, support personnel, and end users. And if desired, you can outsource the management and setup to your Cisco partner.

Service Management and Global Settings

The Services tab in Cisco Spark Control Hub provides an interface to manage all the collaboration services you have signed up for, whether trials or purchased, on the Cisco Spark Platform. This tab also allows you to set up and manage Cisco Spark Hybrid Services.



Global Settings allow you to enable and manage settings that affect the entire organization, including security and privacy settings, SIP domain, and branding settings. You can also manage your directory synchronization and SSO settings, and enable or disable SSO from this page.



My Company (account and subscriptions)

You can also get access to account settings to manage your subscriptions. The My Company page provides access to the subscriptions and licenses you own and visibility into usage levels for each. This page also provides details on your account (company name, account number, etc.), as well as a detailed order history.

My Company

Subscriptions Info Order History

Standard Team Spaces

Standard Team Spaces

Standard Team Spaces Spark 25 Party Meetings Spark Call

License Summary

Message	1	Standard Team Spaces Usage: 1/100
Meeting	2	Spark 25 Party Meetings Usage: 2/100
Call	2	Spark Call Usage: 2/100
Room Devices	0	DX, MX or SX system Usage: 0/5

Help Desk

The Help Desk feature enables you to support questions and solve issues for your end users. Help desk or support agents can look up users, customers, orders, or devices, and view service settings in read-only mode.

Help Desk Support
Search Help

Acme

Users Customers Orders

Enter at least three characters per word. To search by name or email, enter two words, for example John Doe or john.doe. Refer to [Search Help](#).

ACME ACADEMY

ACME Anvil Company

Acme Anvil Co

Acme Auto detailing

ACME c/o Atomos

[Show more results](#)

Partners can use the Help Desk feature to provide Tier 1 support to their customers' user bases. Search results provide relevant details at a glance, along with the ability to deploy the customer's Cisco Spark Control Hub.

Partner Portal (for customer trials and customer management)

With Cisco Spark trials, partners can easily demonstrate the business value of Cisco Spark by creating 30-, 60-, and 90-day trials free of charge for potential customers through Cisco Spark Control Hub. The full collaboration suite of services offered within Cisco Spark is available for trial, including Cisco Spark Meetings, Messaging, and Calling (with public-switched telephone network [PSTN] services). Partners can also include devices (endpoints) with the trial through the Cisco Spark Hardware Try and Buy program.

The screenshot shows a web form titled "Start New Trial" with a close button (X) in the top right corner. The form is divided into two main sections: "Customer Information" and "Trial Services".

Customer Information:

- Company Name:** A text input field containing "ATLAS_TEST_DEMO_ORG_1111".
- Administrator Email:** An empty text input field.
- Certification:** A checkbox labeled "I certify that this customer is in a supported location for Cisco Spark." which is checked.

Trial Services:

- Message:** A checkbox labeled "Message" which is checked.
- Meeting:** A checkbox labeled "Meeting 25 Party" which is checked, and a checkbox labeled "WebEx Enterprise Edition 200 with CMR/TNU+" which is unchecked.
- Call:** A checkbox labeled "Call" which is checked.
- Care:** A checkbox labeled "Chat and Callback" which is checked. Below it is a text input field containing "15" followed by the word "Licenses".
- Room Devices:** A checkbox labeled "DX, MX or SX system" which is checked.

At the bottom right of the form are two buttons: "Cancel" and "Next".

Partners can view and manage their paying customers and their customer trials through the Customers tab in Cisco Spark Control Hub. The customers list provides a simple way for partner administrators to view their customers' services and account status, and the number of licenses the customer has purchased. Partner administrators can edit the terms of the trial (for example, changing the length of the trial or adding services.), in addition to managing the customer's settings, with the "Set Up Customer" button.

Customer Name	Services	Account Status	Total Licenses	Notes
Demo_All_Hands	[Icons]	Purchased	410	Purchased
Organization for cinemastest-bwebex.com	[Icons]	Purchased	22	Purchased
Atlas_Test_UC_Port_320b	[Icons]	Purchased	20	Purchased
Atlas_Test_UC_Port_320c	[Icons]	Purchased	20	Purchased
Atlas_Test_UC_Port_320d	[Icons]	Purchased	20	Purchased
Atlas_Test_hp251	[Icons]	Expired	115	Expired
Atlas_Test_MikeM135	[Icons]	Expired	105	Expired
Atlas_Test_bradmDE642-Prod	[Icons]	Expired	17	Expired. Purchase now
Star Wars Delivery	[Icons]	Expired	105	Expired
Atlas_Test_bradmUS9751	[Icons]	Expired	125	Expired
Atlas_Test_timrinhprod310	[Icons]	Expired	100	Expired
Atlas_Test_SparkDocsSparkans	[Icons]	Expired	125	Expired

Customer Name	Services	Account Status
Atlas_Test_bradmDE642-Prod	[Icons]	Expired
Star Wars Delivery	[Icons]	Expired
Atlas_Test_bradmUS9751	[Icons]	Expired
Atlas_Test_timrinhprod310	[Icons]	Expired
Atlas_Test_SparkDocsSparkans	[Icons]	Expired
Joe's Tire shop	[Icons]	Expired
Atlas_Test_SparkDocsAlpha	[Icons]	Expired
Atlas_Test_bradm_EE	[Icons]	Expired
Atlas_Test_bradm11718-NoWebex	[Icons]	Expired
Atlas_Test_MikeM189	[Icons]	Expired
Atlas_Test_UCBoulder_CoffeeHaus	[Icons]	Expired
Atlas_Test_timrinhprod302	[Icons]	Expired
Atlas_Test_DR-exercise-2016-11-04-1	[Icons]	Expired

Joe's Tire shop

Overview

[Setup Customer](#)

Trial [Edit Trial](#)

60 Day Trial Expired

Message 100 QTY

Meeting 25 Party 100 QTY

Call 100 QTY

Room Devices 5 QTY

Subscriptions

Order Request [>](#)

Call [Add Numbers](#)

PSTN Orders & Imports [>](#)

Phone Numbers 0 [>](#)

Customer Branding

Partner Logo Enabled

Customer Logo Override ☐

Table 1 summarizes the management features of Cisco Spark Control Hub.

Table 1. Cisco Spark Control Hub Management Features

Feature	Description
User and device management	Users can be onboarded (Invite flow using UI, CSV, DirSync, APIs, Convert Users flow) and managed. Licenses and entitlements for all Cisco Spark services, as well as roles for users, can be managed through Cisco Spark Control Hub.
Single Sign-On (SSO)	Integrating SSO services helps ensure that users enter their IT-approved password to access Cisco Spark.
Service management	The Services tab in Cisco Spark Control Hub provides an interface to manage all the collaboration services you have signed up for, whether trials or purchased, on the Cisco Spark Platform. This tab also allows you to set up and manage Cisco Spark Hybrid Services.
My Company (account and subscriptions)	Access account settings to manage your licenses and subscriptions.
Help Desk	Help Desk or support agents (support administrator role) can look up users, devices, etc. and view service settings in read-only mode.

3. Identity and Access Management

Overview

The Identity and Access Management service provides one of the key pillars of security protection for the Cisco Spark Platform. The ability to provision users, authenticate, and authorize them to the service and the appropriate spaces is what underpins the industry-leading security model used by the Cisco Spark Platform. Only users who successfully authenticate and are authorized to join a space or meeting are given the unique keys provided by the Key Management Services (KMS) to encrypt or decrypt content in that space.



The service provides customers and partners the ability to manage identities during the creation, update, and deletion process, either manually, via a CSV upload, with the Active Directory synchronization tool, or via APIs that follow the industry-standard SCIM. In today's security-conscious environment, the ability to deprovision users and remove access is critical, and so each of those mechanisms can be used to delete or remove access for a user or device.

Authentication to the Cisco Spark Platform is easy once a user has been provisioned to the platform. Depending on a choice made at the administrator level, a user can either authenticate with a username and password stored in the Cisco Spark Platform or authenticate to another identity provider and, through the Security Assertion Markup Language (SAML) v2.0 protocol, use federated authentication to gain access. Federated SSO improves usability and security for customers, as the Cisco Spark Platform does not store a password for the user. Federated SSO also reduces the total cost of ownership for enterprises, as it reduces lost productivity of users and the number of calls to help desks related to password reset or lockout events because of forgotten passwords.



Cisco Spark also can provide authentication via MultiFactor Authentication (MFA) by integrating with SAML v2 identity Providers (IdPs) that support this mechanism. This capability is critical, as many organizations deploy MFA mechanisms across their enterprise for all services or for services that require special additional factors during the authentication: something you know – your password – and something you have – x509 certificate, HMAC-based One-Time Password (HOTP), Time-based One-Time Password (TOTP), device fingerprinting, or other mechanisms supported by the IdP.

The Cisco Spark Platform uses the OAuth 2.0 protocol to provide authorization across services, allowing for longer-lived user sessions and more specific security when accessing APIs. The OAuth 2.0 implementation provides API security used for devices and integration of third-party APIs, bots, and integrations. This critical protocol allows the Cisco Spark Depot and Cisco Spark developers to extend the Cisco Spark Platform to use additional services such as Box, IFTT, Salesforce, Github, and many other bots or integrations.

Features

Table 2 summarizes the features that are available to manage users, authentication, and authorization for the enterprise.

Table 2. Identity and Access Management Features and Benefits

Feature	Standard offer/Pro Pack required	Benefits
User provisioning	Standard offer	Users can be provisioned into the Cisco Spark Platform in several ways. A user can be created via manual entry or CSV upload into Cisco Spark Control Hub. You can also create a user via Cisco Spark Directory Connector, which synchronizes users from your on-premises Active Directory.
SCIM	Standard offer	User provisioning can also be performed from a number of enterprise identity providers that support the SCIM v1 protocol. This allows enterprise administrators to provision users just in time and, more importantly, to deprovision users so that they no longer have access to the service.
Active Directory (AD) synchronization with the Cisco Spark Directory Connector	Standard offer	Use this software in a Virtual Machine (VM) or on a bare-metal Windows machine to provision and deprovision users based on a synchronization schedule that meets your enterprise requirements. You can choose from your AD containers and use Lightweight Directory Access Protocol (LDAP) filters to select smaller groups of users to start a proof of concept quickly and expand when ready to roll out to the entire organization.
AD synchronization Multidomain and multiforest with the Cisco Spark Directory Connector	Standard offer	Organizations that have users in multiple forests or across multiple domains can use the Cisco Spark Active Directory Connector to synchronize users into the cloud.
Room synchronization	Standard offer	Managing devices such as Cisco Spark Boards or scheduling a meeting in a room that contains a Cisco Spark room device is much easier when you can use rooms that already exist in AD. Use the Cisco Spark Directory Connector to synchronize rooms to the cloud.
Profile picture synchronization	Standard offer	Use Cisco Spark Directory Connector to synchronize profile pictures to the cloud so users can see who they are inviting to Cisco Spark spaces or searching for from within the directory. All user attributes imported from AD are unalterable by the end user on the Cisco Spark Platform.
Basic authentication	Standard offer	Cisco Spark supports authentication via username (email) and password.
Password policy enforcement	Standard offer	The default password policy requires a user to enter 1 uppercase letter, 1 number, and 1 special character and must be 8 characters long. It also filters out common names and words that might be used in creating a strong password with entropy.
SAML 2.0 federated SSO	Standard offer	Cisco Spark supports federated SSO with the SAML 2.0 protocol. After the Cisco Spark Platform and the IdP exchange metadata that creates a circle of trust between them, all authentication for the users in the Cisco Spark tenant will be redirected to the IdP for authentication. This gives you the freedom to define an authentication method that is appropriate for your users and that meets industry security requirements.
MultiFactor Authentication (MFA)	Standard offer	Cisco Spark supports MFA via SAML 2.0 federated SSO. If you require this feature, you usually require it for more than just one application. Therefore, supporting this capability through the IdP enables you to apply the MFA method across multiple applications, reducing cost and increasing security.
Authorization (OAuth 2.0)	Standard offer	Cisco Spark supports OAuth 2.0 to allow users, after authentication, to receive an industry-standard OAuth 2.0 token that has the appropriate scopes for role, license, and micro-service the user is accessing on the Cisco Spark Platform. This capability also allows devices, bots, and integrations to access the appropriate APIs and micro-services to provide the capabilities needed on the Cisco Spark Platform.
Role-Based Access Control (RBAC)	Standard offer	Cisco Spark Control Hub uses RBAC to make sure the administrator has access to the right set of features and functions in the different Cisco Spark services to perform the task their role requires. Cisco Spark supports the following roles: full administrator, read-only administrator, support administrator, sales administrator and compliance officer.

Cisco Spark Directory Connector

Provisioning and deprovisioning users in an enterprise environment is critical to managing access, especially in large organizations. In these cases, Cisco Spark Directory Connector can manage that process for you. This small-footprint application can be installed in a VM or on a bare-metal Windows PC and can be configured to synchronize users on an hourly, daily, or weekly basis. It can provision up to 22 profile attributes to the Cisco Spark Platform from the more than 265 AD attributes available. Administrators can use LDAP filters to select a small group of users to start a Proof Of Concept (POC) and then expand the filters to include all of the users in the organization. Cisco Spark Directory Connector allows a full administrator to perform a dry run before finalizing the configuration to ensure that the data is imported accurately for their Cisco Spark organization. Additionally, an administrator can synchronize attributes such as directory profile image and room objects to manage devices and improve scheduling of meetings. Lastly, Cisco Spark Directory Connector also supports multidomain and multiforest implementations of AD.

You can install Directory Connector on these Windows Server versions:

- Windows Server 2003
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2016

Directory Connector works with:

- Active Directory 2008, 2008 R2, 2012, and 2012 R2
- In addition, .NET Framework v3.5 must be installed on the machine where Directory Connector is installed
- If your machine has Windows 2003, make sure that you have .NET Framework v3.5
- If your machine has Windows 2008 R2, verify that v3.5 is preinstalled on it

Minimum requirements

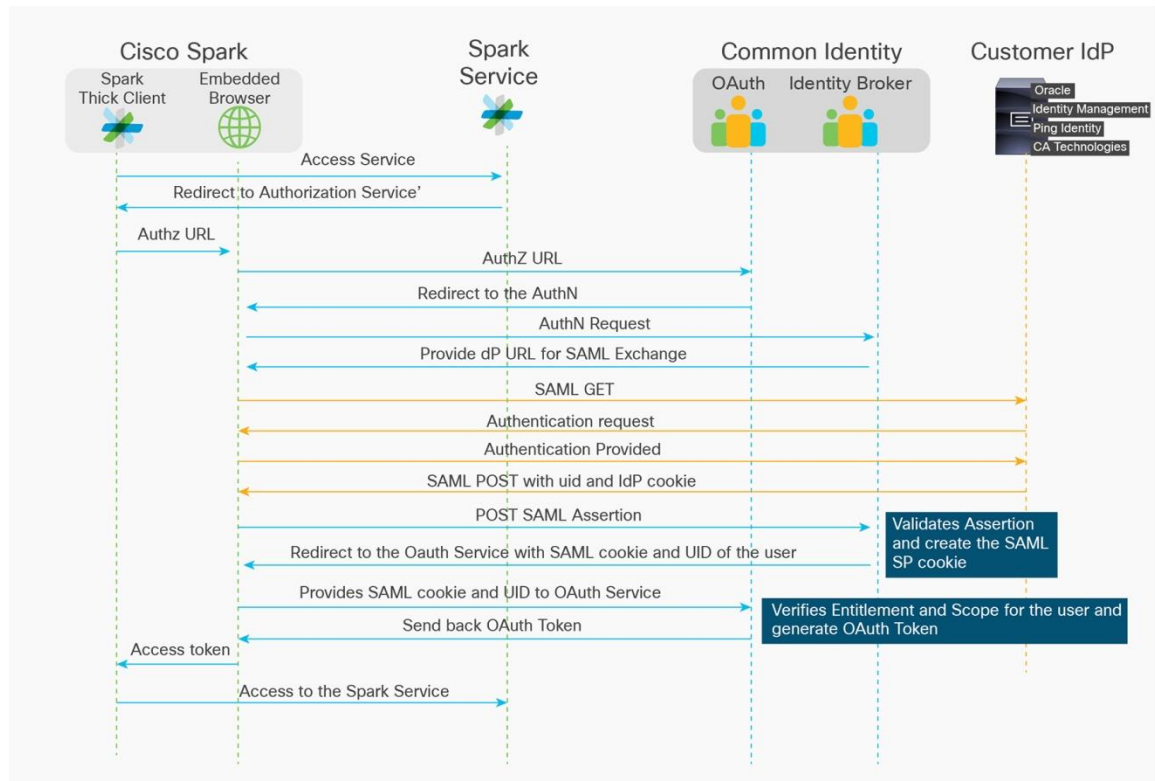
Directory Connector requires a computer with:

- 8 GB of RAM
- 50 GB of storage
- No minimum for the CPU

Authentication and Authorization Flow

When you configure Cisco Spark for authentication and authorization with a SAML IdP for federated SSO, the flow between the user on a Cisco Spark app, the Cisco Spark service, and your IdP is illustrated in Figure 1. This is a typical industry standard for SSO authentication.

Figure 1. Authentication and Authorization Flow for Cisco Spark



Users gain access to Cisco Spark after successful authentication and authorization, as illustrated in Figure 1. Administrators must consider employee lifecycle use cases to maintain the overall security of their use of the Cisco Spark service. You can use features such as the manual delete via Cisco Spark Control Hub, Cisco Spark Directory Connector, or the SCIM API to help ensure that users are deprovisioned and lose access after an HR event.

Cisco Spark Identity Management Partners

Cisco has worked with the leading IdPs in the market for both on-premises and identity-as-a-service integration for the purpose of SAML v2 federated SSO. Cisco has created integration guides for some of these partners and has posted them on the Cisco Spark Help site.

We have either created integration guides or confirmed customer integrations for the following partners:

On-premises identity providers

- Microsoft ADFS
- Oracle Access Manager
- Ping Identity
- OpenAM
- IBM Security Access Manager
- CA Siteminder
- F5 – BigIP
- Shibboleth

Identity-as-a-service vendors

- OKTA
- PingOne
- Salesforce
- Microsoft Azure
- Oracle Identity Cloud Service
- Centrify
- OneLogin

4. Data Security and Encryption

Overview

One of the key benefits for enterprises of consuming cloud services is the ability to leverage value-added features and functionality as quickly as the cloud service provider can deploy them. But for many cloud providers, “adding value” often means having full access to user data and content. For collaboration applications, most cloud providers directly access message, call, and meeting content in order to offer features such as message search, content transcoding, and integration with third-party applications. On the other hand, modern consumer collaboration services tend to be geared toward protecting consumer privacy by offering end-to-end encryption at the expense of features that add value.

Cisco Spark provides the best of both worlds: an end-to-end encrypted cloud collaboration platform that offers enterprises the ability to choose which, if any, value-added integrations Cisco and third parties provide. Cisco Spark uses an open architecture for the secure distribution of encryption keys, allowing enterprises to gain control over the management of their encryption keys and the confidentiality of their data. This means that content is encrypted on the user’s Cisco Spark app and remains encrypted until it reaches the recipient, with no intermediaries having access to decryption keys for content unless the enterprise explicitly chooses to grant such access.

Cisco Spark Differentiation

- Cisco Spark baseline security for user-generated data is differentiated in the market for collaboration solutions. Generally, security is provided through piecemeal encryption of data during transit, while at rest on devices, and during storage, using different solutions. No enterprise messaging offer today supplies the end-to-end encryption provided by Cisco Spark.
- Our offer for customers to hold keys on-premises (Hybrid Data Security or HDS) is an industry-leading solution because we are not only enabling our customers to manage their key storage, but also allowing them to host key compliance and search services on-premises. Accordingly, for the compliance and search services, HDS handles unencrypted content on behalf of the organization in the customer’s secure data centers instead of on the Cisco Spark Platform.
- The Cisco Spark Platform always stores encrypted content in a realm separate from the storage of keys and services that handle unencrypted content. Despite having achieved this level of data security, Cisco Spark has not compromised on enterprise-grade features such as content searches, e-discovery, archival, and Data Loss Prevention (DLP).

Cisco Spark Data Security Using Cloud Key Management Services

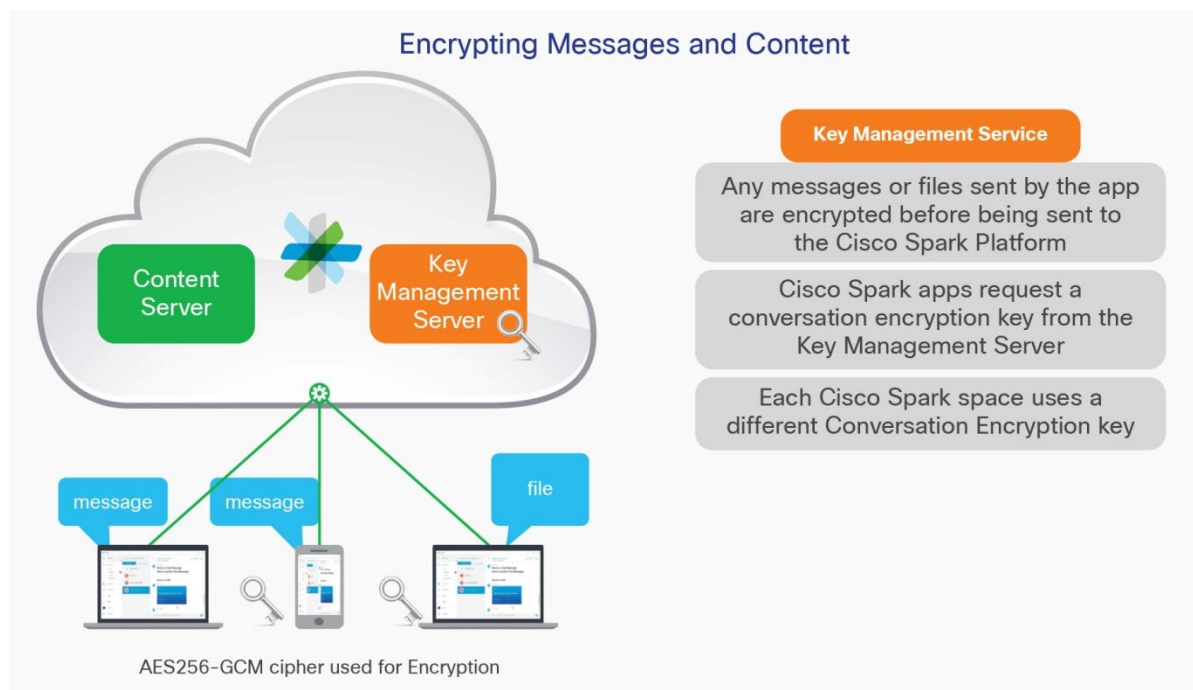
Cisco Spark Platform–based Key Management Services (cloud KMS) are available by default to all customers to encrypt their content before it leaves a user's Cisco Spark app. The baseline for all customers, including online offer consumers, helps ensure that Cisco always provides KMS and end-to-end encryption.

With cloud KMS, every Cisco Spark user gets:

- Clear separation between the services that handle storage and transport of encrypted content and the services that handle encryption and security key management
- An end-to-end encrypted channel between the cloud KMS and the Cisco Spark app or Cisco Spark registered device for exchanging keys
- Industry-standard encryption of user-generated content using symmetric keys managed by the cloud KMS (minimum of one key per Cisco Spark space)
- Controlled authorization to access keys using users' access tokens
- Encrypted search capabilities
- Enterprise capabilities such as e-discovery, DLP APIs, and archival, with decryption done at the perimeter, authorized by the administrator

Figure 2 shows Cisco Spark data security using cloud KMS.

Figure 2. Cisco Spark Data Security Using Cloud KMS



Cisco Spark Data Security with Hybrid Data Security

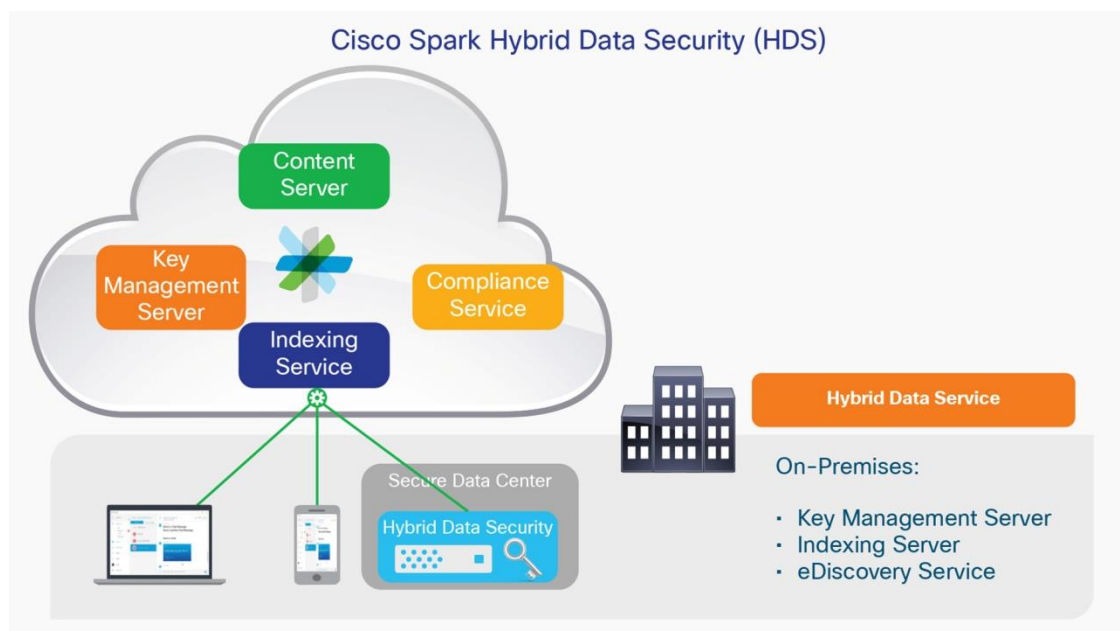
Security-conscious enterprise customers may choose to deploy the security realm services, including KMS, on their own premises. This works no differently than using the cloud KMS, except that keys are obtained and accessed through an on-premises deployment of the servers.

Hybrid Data Security (HDS) includes:

- On-premises deployment and management of the security realm through the Pro Pack for Cisco Spark Control Hub
- KMS and storage
- Search indexer: Ability to securely search encrypted Cisco Spark content
- E-discovery on-premises engine: Although the e-discovery user interface will be hosted in the cloud, the engine remains on-premises for customers who opt to deploy HDS in their own data centers
- Automatic upgrades, alerts, and notifications
- Local logs/audits of access to keys using an on-premises “bring-your-own” syslog

Figure 3 shows Cisco Spark data security using HDS.

Figure 3. Cisco Spark Hybrid Data Security



Cisco Spark Data Security Features

Table 3 summarizes Cisco Spark's data security features.

Table 3. Cisco Spark Data Security Features

Feature	Standard offer/Pro Pack required	Description
End-to-end encryption of content Note: Includes user-generated content such as messages, file uploads, space names, meeting subjects, device nicknames, and Cisco Spark Board content	Standard offer	Cisco Spark uses industry-leading encryption to help ensure that Cisco Spark messages, files, and whiteboards remain confidential, available, and secure at all times. The Cisco Spark app encrypts your data before it leaves your device, using dynamic keys from the KMS. Data stays encrypted when it's in transit to our cloud servers, when we process your data (data in use), and when we store it (data at rest). The KMS is responsible for creating, maintaining, and authorizing access to the encryption keys that the Cisco Spark app uses to encrypt and decrypt content.
Encryption in transit	Standard offer	We use secure HTTPS for all web transactions between Cisco Spark for Mac, Windows, iPhone, Android, and web and our cloud. Similarly, HTTPS is used for all web transactions from Cisco Spark devices (for example, Cisco Spark room devices, IP phones, Cisco Spark Board). Web APIs on the Cisco Collaboration Cloud (at developer.ciscospark.com) use HTTPS. There is no support for HTTP. Consequently, all transport in and out of the Cisco Collaboration Cloud is encrypted. HTTPS is also used to protect data in transit from or to Cisco Spark Control Hub. All media in Cisco Spark, such as voice, video, desktop share, and whiteboarding are transmitted using Secure Real-Time Transport Protocol (SRTP, defined in RFC 3711). Currently, the Cisco Spark Platform decrypts real-time media for mixing, distribution, PSTN trunking, and demarcation purposes.
Search on encrypted content	Standard offer	Search indexes for all user-generated messages are created when encrypted content is received in the Cisco Collaboration Cloud. Search indexes are one-way hashed using dynamic keys before being stored. When the end user searches for a word in Cisco Spark, the word is encrypted before leaving the app. Words are appropriately hashed and searched against previously stored encrypted search words. Matches are retrieved and sent to the app for decryption and display to the end user.
Hybrid Data Security (customer-controlled data security)	Pro Pack required	Enterprises can opt to deploy both the services that manage and store the keys used for encrypting content and the services that operate on generating search index hashes. With these capabilities, enterprise customers have the additional assurance of choosing the location where their users' keys are physically stored. This capability, once it is deployed, should be run in a trial mode first for a select set of users, to help ensure a smooth rollout of the service. More details are in the deployment guide here . Disclaimer: <ul style="list-style-type: none"> • Certain cloud services will continue to have access to the customer keys, specifically, the API servers and the preview capability in the Cisco Spark Platform. • Authorizations for end users to access keys are provided through OAuth tokens, which are generated and stored in the Cisco Collaboration Cloud. If the tokens are compromised, it introduces a vulnerability that allows access to the keys and content accessible by the authorized token.

Frequently Asked Questions

- Q.** What encryption algorithm is used for encrypting content?
- A.** The symmetric cipher used in Cisco Spark is AES256-GCM.
- Q.** Is there a Internet Engineering Task Force (IETF) protocol defined for Key Management Services (KMS)?
- A.** Cisco Spark builds on open standards and protocols for securing data, including key management specifications designed by Cisco and openly submitted for consideration as Internet standards.

Q. How can I obtain Hybrid Data Security?

A. HDS is one of the many features available for purchase as part of the Pro Pack for Cisco Spark Control Hub.

Q. Is a detailed deployment guide available for HDS?

A. Please see <https://www.cisco.com/go/hybrid-data-security>.

Q. What additional security does HDS guarantee?

A. HDS gives you physical control of the keys that are generated and owned by your organization. Although certain cloud services can access those keys, separating the keys from the encrypted content in the cloud assures security-conscious organizations that their content cannot be compromised by outside attacks unless the attacker can access both the encrypted content and the keys.

5. Application and Mobile Device Security Controls

Overview

Cisco Spark is enterprise grade, and Cisco is committed to meeting customer security needs with the Cisco Spark Platform. Enterprise IT require basic controls on the security of the applications it deploys to users. With Cisco Spark, the controls to be provided will include capabilities such as PIN lock enforcement, token revocation and remote wipe of Cisco Spark cached content on mobile devices, and Cisco Spark for Web idle session timeout.

Enterprise Application Security Policies

Enterprise administrators are provided security controls that will allow them to customize Cisco Spark usage:

- In the user profile, an administrator has the ability to revoke the user's access. This will remove all access and refresh the tokens of that user and will also remotely wipe all cached content on the mobile devices that the user is authenticated into (Figure 4). The typical use case for this is when a user loses a mobile device or when a user is terminated but not yet deprovisioned from Cisco Spark.
- An enterprise administrator can also customize the Cisco Spark for Web idle session timeout for both in-network usage and out-of-network usage. The typical use case for this is when an administrator logs in from a public network vs. when they log in from the company network.

Mobile Device Security Controls

The Cisco Spark for iPhone and Android apps benefit from the following enterprise-grade security features:

- All supported Cisco Spark authentication – password based or SSO based – establishes OAuth tokens for authorizations. Once established, the client refreshes the access tokens, never requiring a reauthentication unless specific events such as deprovisioning or token revocation occur.
- End-to-end encryption using dynamic keys.
- Secure Transport Layer Security (TLS) connection to the Cisco Spark service and to the user's organization-defined KMS (Cisco Spark Platform or HDS).
- PIN lock requirement when enabled (Pro Pack for Cisco Spark Control Hub required). This capability requires a user to secure their device with PIN lock or a passcode, helping ensuring that enterprise content in the Cisco Spark app is not accessible if the device is misplaced, lost, or in the wrong hands (Figure 5).
- Remote wipe of content cached on mobile devices when either the user is deprovisioned from Cisco Spark or the user's access tokens are revoked by an administrator.
- Encryption at rest on Cisco Spark for iPhone.

Figure 4. Error Message Seen On iOS and Android Devices When Either the User is Deprovisioned or the User's Tokens are Revoked

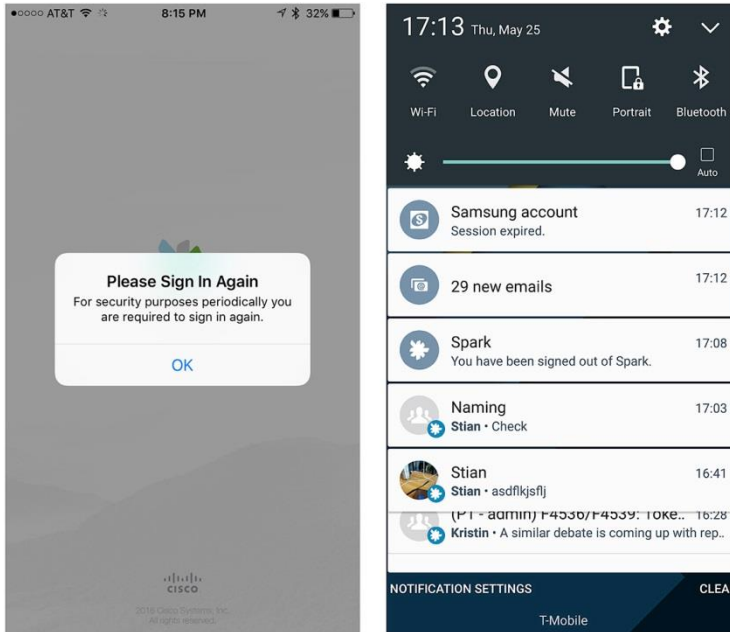
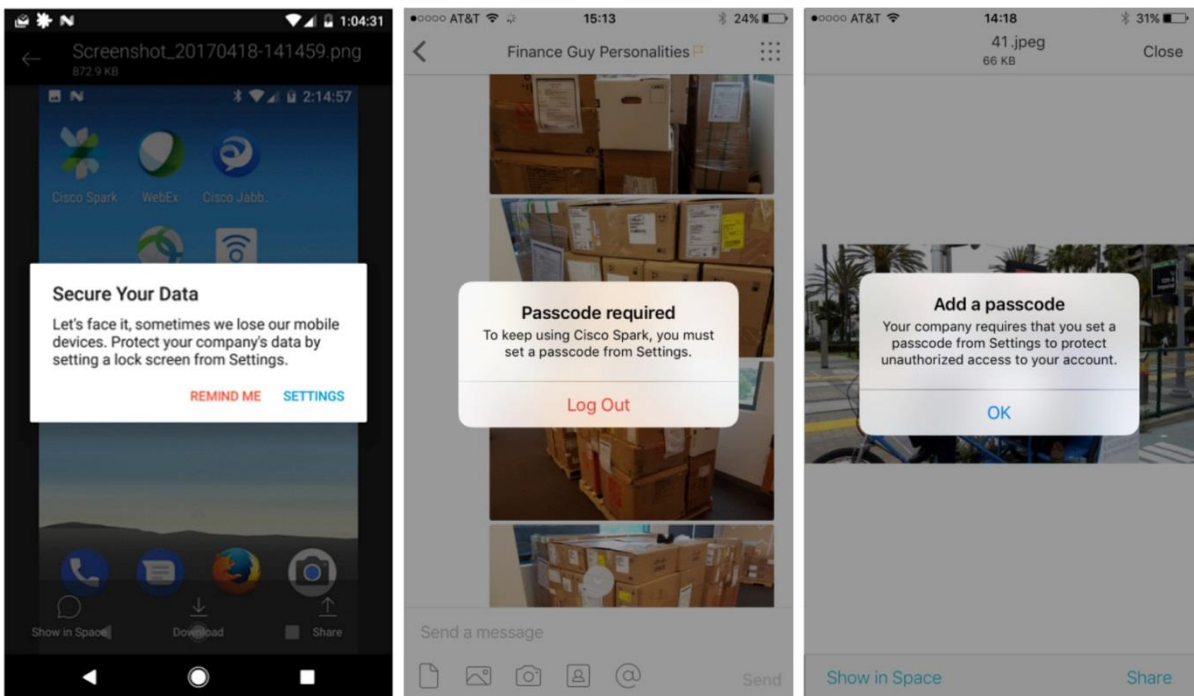


Figure 5. Error Message pop-ups When PIN Lock is Enabled but the User has not Changed the Device Settings



Features

Table 4 summarizes the application and mobile device security controls.

Table 4. Application and Mobile Device Security Control Features

Feature	Standard offer/ Pro Pack required	Benefit
PIN lock enforcement Note: Only for iOS and Android smartphones; does not include Chromebook	Pro Pack required	This is a Cisco Spark Mobile Device Management (MDM) feature that an enterprise administrator can enable. Once enabled, PIN lock enforcement will require the user of Cisco Spark for iPhone and Android to enable the device's PIN lock when using certain features in the mobile app, in order to continue using the app. This feature helps ensure the security of the content in the Cisco Spark app.
Remote wipe and access reset by administrator	Pro Pack required	When a user loses their mobile device, or a user who has left the organization potentially has access to Cisco Spark content through their mobile device, an administrator can revoke all access and wipe Cisco Spark cached content on the mobile devices (iPhone and Android), helping ensure content security for the enterprise.
Customizable Cisco Spark for Web idle timeout (on-net and off-net)	Pro Pack required	An enterprise can customize its intranet and extranet idle timeout for both Cisco Spark for Web and Cisco Spark Control Hub. For example, the extranet idle timeout could be much shorter, such as 10 minutes, reducing the vulnerability of users who are in a public location or logged in from public computers, while a user logged in to the intranet could get up to 60 minutes of idle time before being logged out.

Frequently Asked Questions

Q. Is Cisco Spark certified for specific Mobile Device Management (MDM) providers?

A. No.

Q. How can an administrator access the PIN lock enablement feature?

A. This is a premium feature enabled through the Pro Pack for Cisco Spark Control Hub. It becomes available under Settings when you purchase the add-on offer.

Q. Will more security controls be added?

A. Yes. Cisco Spark is a cloud service and will constantly be adding new features to help ensure ongoing control and visibility.

6. Compliance (e-discovery, retention, DLP, archival)

Overview

For customers who 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 the form of JSON reports. 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. 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, SSNs, intellectual property, patient records, etc. By providing access to content-generating events via the Events API, Cisco Spark gives enterprise IT the ability to monitor data loss and take action in the event that data loss occurs.

Search Ownership

Cisco Spark 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, Cisco Spark has the notion of Cisco Spark 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 5 summarizes the content rights.

Table 5. 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 Spark 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 6 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 org one 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 6. 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

Privilege	Each participating organization
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

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 and then exported into e-discovery software. Access to this feature is restricted to compliance officers as defined by an organization within Role-Based Access Control. Only a user with the compliance officer role has access to this feature. It is accessible from Cisco Spark Control Hub (Support -> View Activity Reports).

Search Cisco Spark Space Activity

Search messages, file content

Compliance Officer role

Search

Choose to search for specific users or spaces. Add more than one by separating with commas

Email Address

e.g. johnsmith@email.com, jansmit@email.com

Date Range

2017-03-18 to 2017-04-17

Where **Messages** contains

e.g. project AND manager

Search

The report summary shows information such as the number of users, messages, files, and space IDs.

[Back to Search](#)

Search Info

Email Addresses
N/A

Date Range
2017/04/01 - 2017/06/11

Messages
test

Report Summary

Spaces	Messages	Files	Est. Report Size
22	3429	26	12 MB

Generate Report

Enter report information to generate a report. The time to generate the report depends on the estimated report size.


Report Name


Description

Export Format
JSON

























[Generate Report](#)

The compliance officer 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.


eDiscovery Search and Extraction


Prateek Temkar
Compliance Officer, IT

[Search](#)
[Reports](#)

Name	Date Generated	Size	Status	Actions
 HanzoReport	Jul 5, 2017, 11:24 AM	2.16 MB	Completed	 
 file-upload-test	Jun 18, 2017, 3:16 PM	47.76 KB	Completed	 
 TAC training report	Jun 12, 2017, 3:58 PM	2.21 KB	Completed	 
 del	Jun 12, 2017, 2:49 PM	2.21 KB	Completed	 
 report1	Jun 11, 2017, 3:24 PM	12.20 MB	Completed	 
 pjxurm report	Jun 6, 2017, 4:48 PM	10.45 MB	Completed	 
 test reposrt	Jun 6, 2017, 4:48 PM	8.23 MB	Completed	 
 test 26	May 26, 2017, 5:04 PM	2.49 KB	Completed	 

Retention

You can manage risks and align with global retention policies by setting a custom retention period in Cisco Spark for the entire organization. With the Pro Pack for Cisco Spark Control Hub, full administrators can set the retention period for Cisco Spark 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 by setting a minimum retention period in increments of one month. After the retention period is reached, all the content (messages, activities, files) is purged and irretrievable.

Retention

Spark Message Data

Set amount of time before accumulated user data is retired and removed from the system.

There is a 5GB total storage limit per user. After limit is reached, older data will be removed first.

☐ Indefinitely

☒ Default retention time

Past 60 months

▼

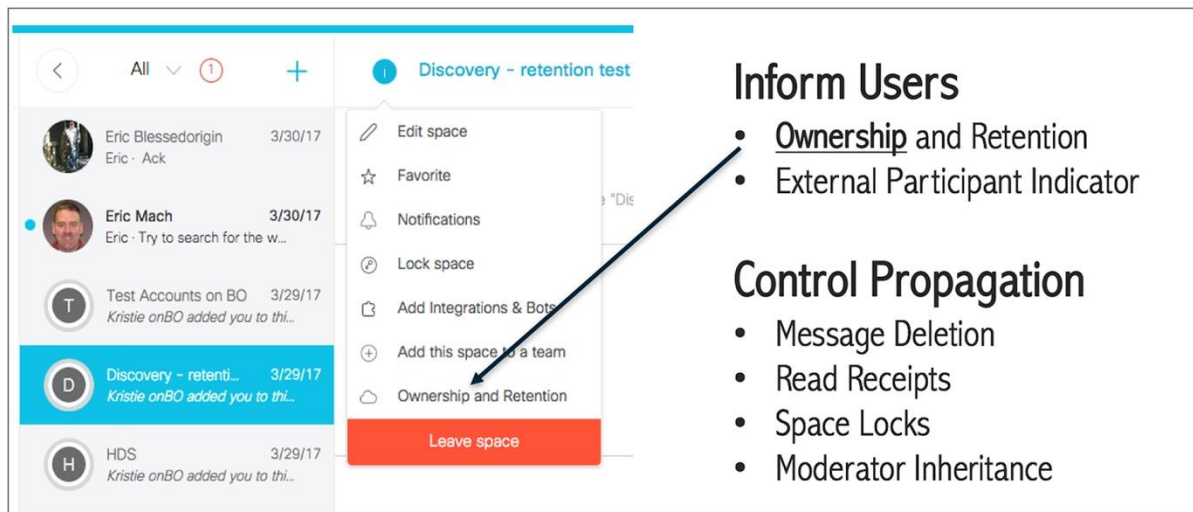
☐ Custom retention time between 1 and 120 months

months

Data Loss Prevention (DLP)

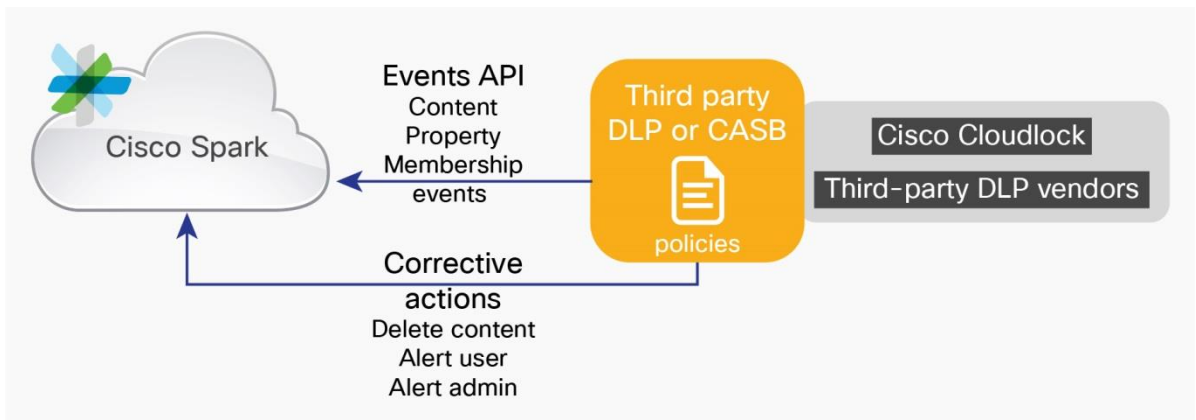
Cisco Spark has a twofold DLP strategy. The first part involves informing users about potential data loss by making them aware of the context in which they are communicating. Users are informed about space ownership, retention, and the presence of external participants. End users are further empowered by propagation control features such as message deletion, read receipts, space locks, and moderator inheritance (Figure 6).

Figure 6. First Part of Cisco Spark's Twofold DLP Strategy



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 Cisco Spark accessible via APIs so that they can be consumed by DLP software to check for violations and take actions to remediate any issues (Figure 7).

Figure 7. Second Part of Cisco Spark's Twofold DLP Strategy



There are three ways to approach DLP integration.

- Out-of-the-box solution: Certified integrations with leading compliance partners. The Cisco Spark team is actively working on building integrations with Cisco Cloudlock and third-party DLP vendors.
- 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 Events API will be exposed publicly. Customers are able to use the API to integrate with homegrown solutions or third-party DLP vendors.

Archival

Customers can use the Cisco Spark Events API to integrate with archival software. The integration with archival vendors is currently in progress. As with DLP, there are three ways to approach the archival integration (out-of-the-box solution, end-to-end custom solution, DIY solution).

Table 7 summarizes Cisco Spark's compliance features.

Table 7. Cisco Spark Compliance Features

Features	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 200, 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 alone or 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. 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 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. Pro Pack: The administrator can set the retention period for data in Cisco Spark. After this period, all content (files, messages, 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 Cisco Spark.
DLP: Enlisting users	The Cisco Spark 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.
Events API: DLP	The Cisco Spark Platform exposes an 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.
Events API: Archival	The Events API can be consumed by archival software to archive Cisco Spark 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.

Cisco Spark Differentiation

Cisco Spark 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. This is a key differentiator. If Cisco Spark restricted such external communication, employees would use other mechanisms to communicate with external users, and the IT team would have no visibility into such communication.

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 Cloud Access Security Broker (CASB) or an archival system that Cisco Spark does not have a certified integration with?
- A.** In that case there are two additional options. You can:
- Build an integration between Cisco Spark and the CASB or archival system using Cisco Spark's Events API
 - Work with Cisco Advanced Services to build the integrations using Cisco Spark's Events API
- Q.** What are the different types of events exposed through the Events API?
- A.** The Events API captures these events.
- Posting a message
 - Posting a file
 - Deleting a message or file
 - Adding a user to a space
 - Removing a user from a space

7. Analytics

Cisco Spark analytics provide usage trends and valuable insights on which to base further adoption strategies to promote and optimize collaboration across teams. Advanced analytics capabilities are integrated as part of Cisco Spark Control Hub. Customers are able to understand how different services are being used across the organization and effectively grow adoption to maximize productivity gains. Administrators are able to monitor capacity and performance to optimize resource utilization as part of proactive management. Administrators or IT help desk staff can diagnose and shorten case resolution time.

An intuitive graphical interface allows administrators access to usage, adoption, and other important information. Interactive data visualizations explore data as it automatically adapts to parameters specified in real time.

Access to historical data for the last 90 days is standard. Data is aggregated and presented in multiple reports. Administrators may access these reports at any time within Cisco Spark Control Hub.

The Pro Pack for Cisco Spark Control Hub offers additional features that allow you to further explore data and correlate insights that would otherwise be unknown. It enables data exploration with different dimensions, such as time, location, and person. It also offers a diagnostic feature that allows real-time access to Cisco WebEx meeting details, such as meeting duration and participants list.

Cisco Spark Analytics Features

Table 8 summarizes Cisco Spark's analytics features.

Table 8. Cisco Spark Analytics Features

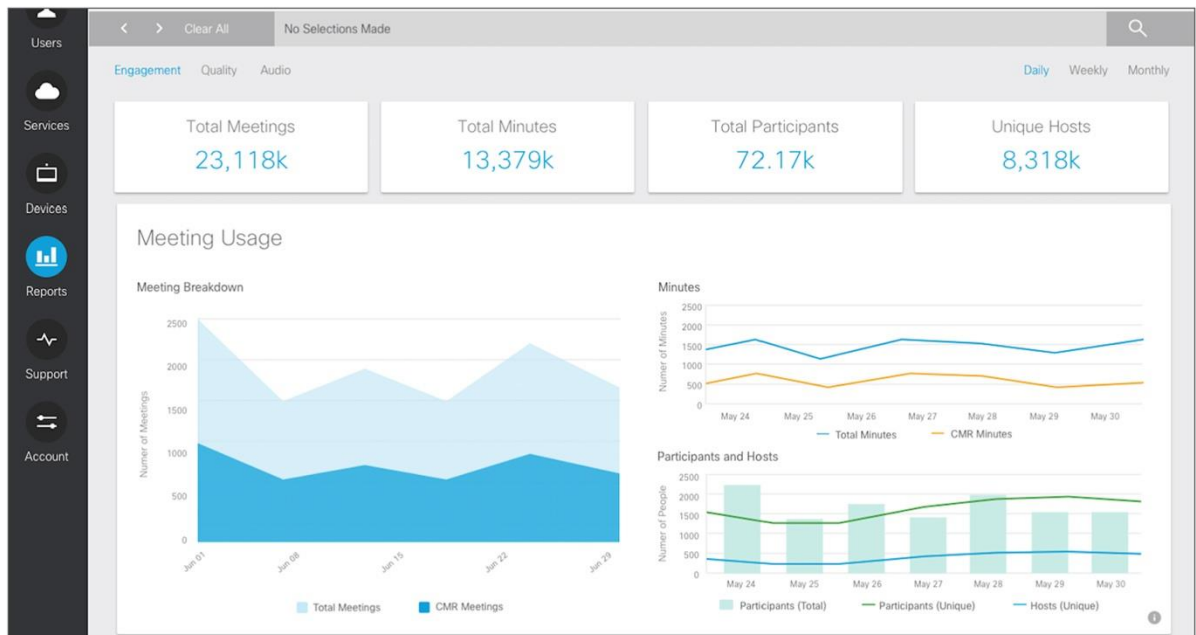
Feature	Standard offer/Pro Pack required	Description
Flexible historical reports	Standard offer	Daily aggregated metrics of up to 90 days are visualized in summary reports for Cisco WebEx, Cisco Spark, Hybrid Media Service, and devices. Engagement and quality reports are available.
Customized reports with drill down	Pro Pack required	This capability is available for Cisco WebEx reports in this release. Individual session and user level metrics are available. You can zoom in from a monthly report to an individual meeting record. Cisco WebEx usage metrics are available for up to 365 days. Cisco WebEx quality metrics are available for 90 days initially. This will be extended to 365 days as data is accumulated
Multidimensional pivots and data exploration	Pro Pack required	This capability is available for Cisco WebEx reports in this release. The new analytics engine allows users to manipulate data in real time via the reporting interface. Selection of any data set will update all associated reports.
Diagnostic	Pro Pack required	This capability is available for Cisco WebEx reports in this release. Real-time search of the last 7 days of Cisco WebEx meeting details. Locate meetings with participant details by searching for the host email or meeting ID.

Flexible Historical Reports

Historical reports are standard in Cisco Spark Control Hub. They are available in daily, weekly, and monthly format. Up to 90 days of daily aggregated metrics are accessible by users with full administrator, or read-only privileges. Administrators may view different types of reports for Cisco Spark, Cisco WebEx, Hybrid Media Service, and Cisco Spark devices when applicable to the deployed configuration.

- Cisco WebEx reports include meeting and audio usage, average meeting join time, and media quality.
- Cisco Spark reports include space usage, active users, registered devices, and media quality.
- Hybrid Media Service reports include total calls, resource utilization, and cluster status.
- Cisco Spark device reports include usage, and most and least used devices.

Identify recurring anomalies with historical trends. Engagement, quality, and diagnostic data are readily available. To help you understand your system at a glance, top metrics are easily visible. Trending and visualizations make key patterns clear and apparent.



Drill Down

With the Pro Pack for Cisco Spark Control Hub, Cisco WebEx meeting session and user level details are available. Administrators can zoom from monthly total meeting usage to individual call details with a simple click. This capability allows administrators to filter unwanted data so that they can focus on the information that matters most to them.

Meeting Number	Meeting Name	Start Time	End Time	OS	Browser	Duration	
209006036	ESP Program - Sync up ...	01 Jun 2017 20:23:23	01 Jun 2017 20:43:41	MAC	Firefox	20	
209006036	Pro Pack Feature team	01 Jun 2017 20:23:23	01 Jun 2017 20:43:41	MAC	Firefox	20	
209006036	UX Weekly Meeting	01 Jun 2017 20:23:23	01 Jun 2017 20:43:41	MAC	Firefox	20	
209006036	PCIA 2.0 Program Meeting	01 Jun 2017 20:23:23	01 Jun 2017 20:43:41	MAC	Firefox	20	
209006036	ESP Program - Sync up ...	01 Jun 2017 20:23:23	01 Jun 2017 20:43:41	MAC	Firefox	20	

Data Exploration

With the Pro Pack for Cisco Spark Control Hub, root-cause analysis is easy. The advanced analytics data architecture captures information in an internal data model that allows real-time, on-the-fly data exploration. Any manipulation or selection of a data set will automatically update all associated reports. For example, to analyze a department's Cisco WebEx meeting usage trends, an administrator can simply select the department's users from the meeting details table. Meeting, audio, and minutes usage reports will be updated instantly to display the usage of the specific department. Multidimensional pivots change how information is visualized, enabling boundless manipulation of data in real time.

Diagnostics

The Pro Pack for Cisco Spark Control Hub also offers a Cisco WebEx meeting diagnostic capability. Technical staff can quickly resolve support requests and search for meetings in real time as they occur. Administrators can access meeting diagnostics by selecting the “Diagnostic” option on the Cisco WebEx Reports page. Both host email address and meeting ID are valid search criteria, with an optional date selection of the last 7 days. When a meeting is located, the start time, end time, duration, host information, and feature usage are reported. Administrators may further zoom in to retrieve participants and session-level details, such as each participant’s join and end time.

The screenshot displays the Cisco Cloud Collaboration Management interface. The left sidebar contains navigation icons for Overview, Users, Places, Services, Devices, Reports, and Support. The main content area is titled 'Reports' and includes a search bar with the email 'mcdue@blessedorigin.com'. Below the search bar is a table with columns for Start Date, Status, and Meeting Name. The table lists two meetings, both with a status of 'Ended'. The right sidebar shows a detailed view of 'Matt Duke's Personal Room' (Meeting Number: 924109258). This view includes an Overview section with meeting details, a Meeting Session section with a timeline of events, a Participants section with host information, and a Features section with a table of feature usage.

Start Date	Status	Meeting Name
July 20th, 2017 4:09:42 PM	Ended	Matt Duke's P
July 24th, 2017 4:29:50 PM	Ended	Matt Duke's P

Features		
Chat	Poll	Flash
Yes	Yes	No
App Share	File Share	Doc Share
Yes	Yes	No

8. Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. [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>.

 Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)