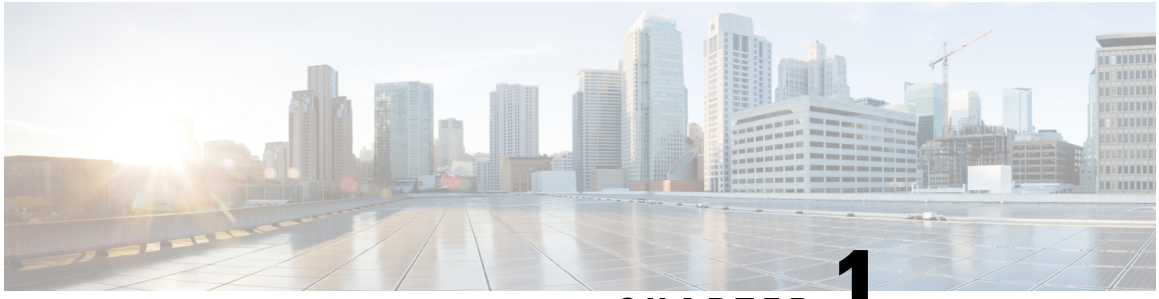
Webex for Government Administration Guide

First Published: 2020-12-21

Last Modified: 2021-03-03

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Get Started with Control Hub

Access

Use https://admin-usgov.webex.com to sign in to Control Hub.

Control Hub Overview

With Control Hub, administrators will be able to manage calling, meetings, messaging and devices in a single pane.

As soon as your site upgrades, you'll be able to start using Control Hub immediately to:

- Familiarize yourself with the new Analytics in Control Hub.
- Troubleshoot meetings with advanced diagnostics (link takes you to help.webex.com)
- Configure Webex App Security, Data Retention, and Compliance Settings in Control Hub.
- Register Webex devices to the cloud (link takes you to help.webex.com).

Analytics in Control Hub

The following tables describe, at a high level, the analytics that are available to explore in this Early Field Trial.

Table 1: Meeting Analytics

Feature	Help Article	Considerations for Government Organizations
Quickly gauge Key Performance Indicators for meeting activity.	Analytics for Your Webex for Government Portfolio	To view your meeting analytics data, from https://admin-usgov.webex.com, go to **Analytics**, then click **Meetings**.
View historical trends for business insights: • User adoption and engagement. • Quality of service (average join time, VoIP quality). • Service utilization. • Resource optimization		
Monitor current activity with in-meeting diagnostics.		
View post-meeting diagnostics.		
Drill down to participant details. (Requires Pro Pack.)		

Table 2: Webex App Messaging Analytics

Feature	Help Article	Considerations for Government Organizations
Quickly gauge Key Performance Indicators for messaging activity.	Analytics for Your Webex for Government Portfolio	To view your messaging analytics data, from https://admin-usgov.webex.com, go to **Analytics**, then click **Messaging**.
Monitor the number of people actively engaged with Webex app.		
View the top 30 most active messaging users in the app.		
Monitor the total number of messages users send each day over time.		
Compare desktop and mobile messaging usage over time.		
Monitor space usage over time.		
Monitor file sharing over time.		

Webex App Security, Data Retention, and Compliance Settings in Control Hub

As an administrator, you can configure the following settings for data handling and security in the Webex app.

Table 3: Content Management

Feature	Help Article	Considerations for Government Organizations
Enable **Microsoft OneDrive and SharePoint Online (Office 365 GCC Moderate)** or **Box** as your enterprise content management platform.	Enterprise Content Management in Cisco Webex Control Hub	—

Table 4: Custom Security Settings (Available on Request with Pro Pack)

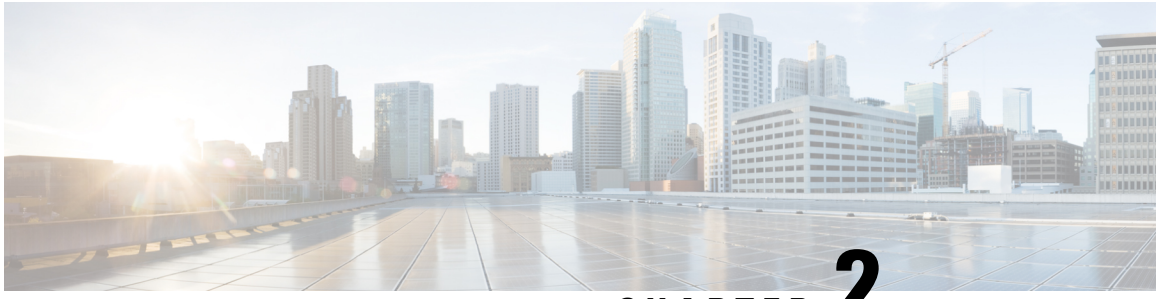
Feature	Help Article	Considerations for Government Organizations
Block External Communication controls whether people can communicate in spaces with users outside of your organization.	Block External Users in Webex Spaces for Your Organization	For government organizations, by default, external communication is **blocked** for all domains. If you choose to allow external communication, your users can communicate only with other organizations that use the Webex for Government multi-tenant service.
PIN lock enforcement requires Webex mobile app users to secure devices with PINs or lock screens.	Set Up Security for Mobile Devices	—
Revoke access remotely and wipe any cached Webex app content from a mobile phone.	Revoke a User's Access to Cisco Webex	—
File share controls restrict users from downloading, previewing, and uploading files to the Webex app.	Prevent People Sharing Files	—

Table 5: Data Retention and Compliance (Available on Request with Pro Pack)

Feature	Help Article	Considerations for Government Organizations
Configurable retention period for user-generated content (messages, files and whiteboards shared in spaces).	Set the Retention Policy for Your Organization	—
eDiscovery Search and Extraction allows compliance officers to search and view conversation content and manage compliance reports.	Ensure Regulatory Compliance of Cisco Webex Content	—
Legal hold to ensure that information relevant to legal matters is not purged by your retention policy.	Manage Compliance Data for Legal Hold in Cisco Webex Control Hub	—

Table 6: Extended Security Features (Available on Request)

Feature	Help Article	Considerations for Government Organizations
Data Loss Prevention through Cisco CloudLock	Cisco CloudLock for Webex Teams	—
Cisco Talos Clam AV anti-malware protection	Anti-Malware Scanning of Files in Webex	—



CHAPTER 2

Set Up the App for Webex for Government

To verify that you can use the app on your device or web browser, see the Webex | System Requirements and Support Policy help article.

The Webex app is available for the following platforms, each of which has slightly different considerations for government organizations:

- Windows Desktop, on page 5
- Mac Desktop, on page 7
- Mobile, on page 8
- Web, on page 9

Windows Desktop

Enable FIPS Registry Key (Recommended)

Note Your organization may require you to run the Webex app in FIPS mode. To do so, set the following registry key to 1 (DWORD value) on user machines:

```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled
```

To change this setting, you must have HKLM registry access. Typically, an administrator or user with admin privileges has this access.

Since this is an OS-level setting, we recommend that you evaluate its impact on your other Windows applications before rolling it out across your organization.

If you don’t enable the registry key, note the following:

- You don't lose any app functionality.
- We’ll still support your organization.
- The app still uses FIPS-compatible algorithms and TLS 1.2. However, operating system libraries (such as WinHTTP) don't run in FIPS mode.

Choose a Windows App Deployment Option

To enable the app to connect to the Webex for Government cloud for your users, choose one of the following options, according to your needs:

Option 1: MSI

Do these steps if you prefer deploying the app as an administrator-controlled MSI install.

Note To perform this action, you must have HLKM registry access. Typically, an administrator or user with admin privileges has this access. The FEDRAMPENABLED setting causes the installer to write to the HLKM area of the registry.

Before you begin

Enable the FIPS registry key, if required.

Step 1 Download the installer using the applicable link.

- Localized versions:
  - 32-bit version https://binaries.webex.com/WebexTeamsDesktop-Windows-Gold/Webex_x86.msi
  - 64-bit version https://binaries.webex.com/WebexTeamsDesktop-Windows-Gold/Webex.msi
- Non-localized versions:
  - 32-bit version https://binaries.webex.com/WebexTeamsDesktop-Windows-Gold/Webex_x86_en.msi
  - 64-bit version https://binaries.webex.com/WebexTeamsDesktop-Windows-Gold/Webex_en.msi

Step 2 To enable usage of the Webex for Government cloud environment, run msiexec with the `FEDRAMPENABLED=1` option along with any other options that you need.

Example:

```
msiexec /i WebexTeams.msi FEDRAMPENABLED=1 ALLUSERS=1
```

Option 2: FedRampEnabled RegKey

Do this task if you plan to let users download and install the Webex app MSI themselves, but want to ensure that they connect to the Webex for Government cloud.

Note To perform this action, you must have HLKM registry access. Typically, an administrator or user with admin privileges has this access.

Before you begin

Enable the FIPS registry key, if required.

Step 1 Set the following registry key to 1 (DWORD value):

```
HKLM\Software\Cisco Spark Native\FedRampEnabled
```

Step 2 If the user has installed and signed in to the Webex app before the registry key was set, have the user sign out and sign back in.

Mac Desktop

To enable the Webex app to connect to the FedRAMP government cloud for your Mac users, choose one of the following options, according to your needs:

Option 1: (Recommended) MDM

This is the recommended mechanism to configure FIPS and FedRAMP modes for MacOS. Deploy an MDM configuration profile that contains the following settings. The exact details for configuring this will depend on your MDM solution.

Step 1 Download the DMG installer from the following link.

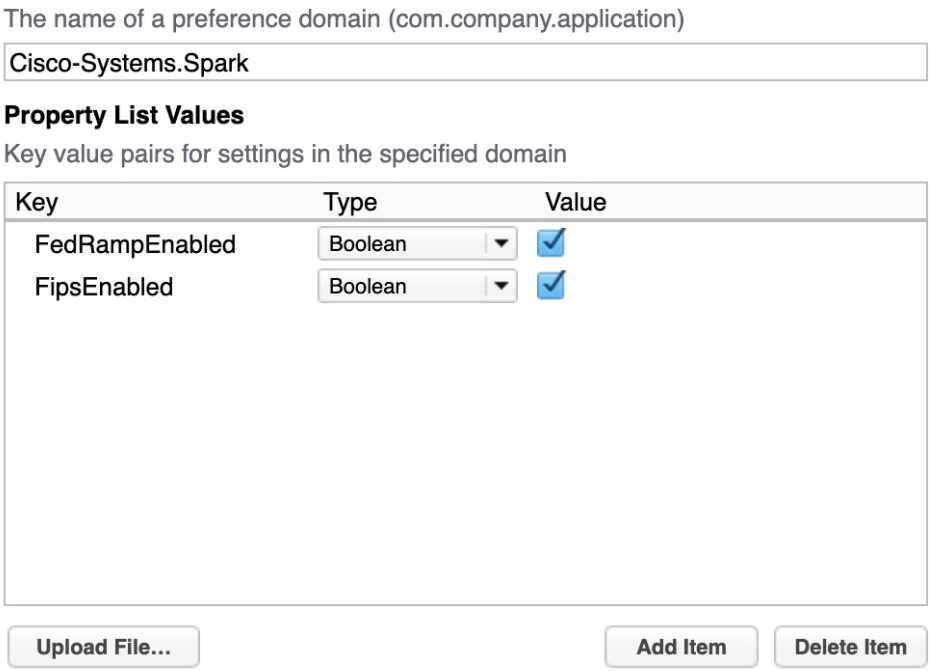
- https://binaries.webex.com/WebexTeamsDesktop-MACOS-Gold/WebexTeams.dmg

Step 2 Set the following two **Boolean** keys to true in preference domain `Cisco-Systems.Spark`:

```
FipsEnabled
```

```
FedRampEnabled
```

Example:



Option 2: Defaults Command

If you do not have access to an MDM solution, you can change the default values for FIPS and FedRAMP using the defaults command. The end user can potentially override values set via defaults, so we recommend using MDM if you have the option.

Enter the following commands:

```
defaults write Cisco-Systems.Spark FedRampEnabled -bool true

defaults write Cisco-Systems.Spark FipsEnabled -bool true
```

Mobile

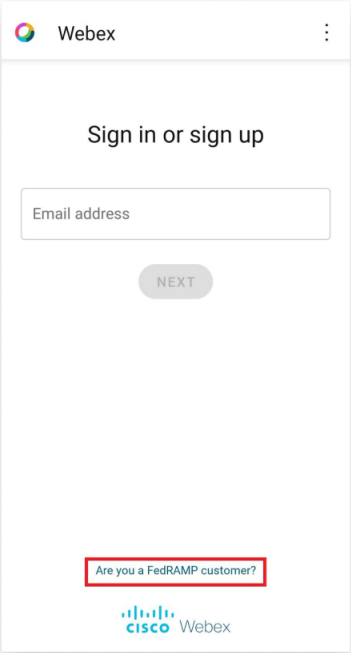
No special administrator action is required to set up or connect to the Webex for Government cloud from the mobile app, although users must sign in using the method below. To use MDM/MAM or app wrapping options on user mobile devices, see the Webex | Secure Mobile Devices help article.

Step 1 Download the Webex app:

- iPhone and iPad—App Store for iPhone and iPad
- Android—Google Play

Step 2 Start the app, tap **Get Started**, and then tap **Are you a FedRAMP customer?**

Example:



This link takes you to the FedRAMP sign-in page, which directs the authentication to the Webex for Government identity service and enables FIPS 140-2 mode.

Step 3 Enter your email address and check **I agree to terms and conditions**, then click **Next** to sign in.

The first time you sign in, you are directed to set up a passcode.

Web

No special administrator action is required to connect to the Webex for Government cloud from the web app. The Webex for Government Cloud has a dedicated URL.

Step 1 In a web browser, navigate to https://teams-usgov.webex.com/.

Step 2 Sign in with the Webex for Government user account.