

# Cookbook for Cisco Webex

This guide provides step by step guidelines for administrators to configure Cisco WebEx as Cloud Service with MobileIron Access.

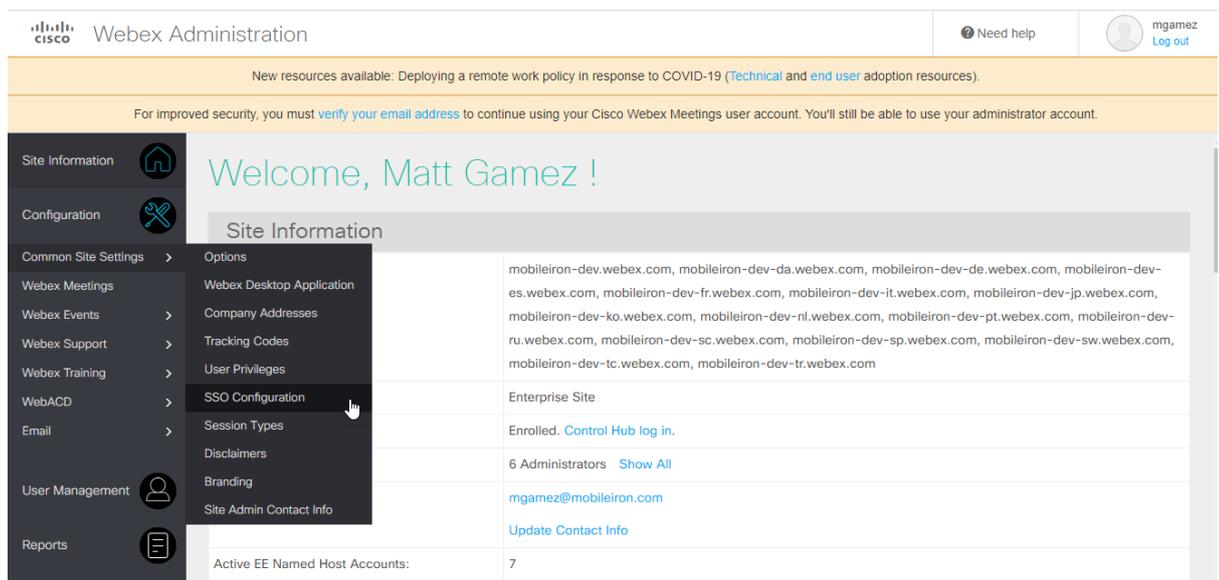
## Prerequisites

Verify that you have the following components in your environment:

- **Cisco Webex (SP) Metadata File**

You must download the metadata files to configure Webex if you have already configured the application:

1. Login to Cisco WebEx with admin credentials.
2. Click **Configuration > Common Site Settings > SSO Configuration**.



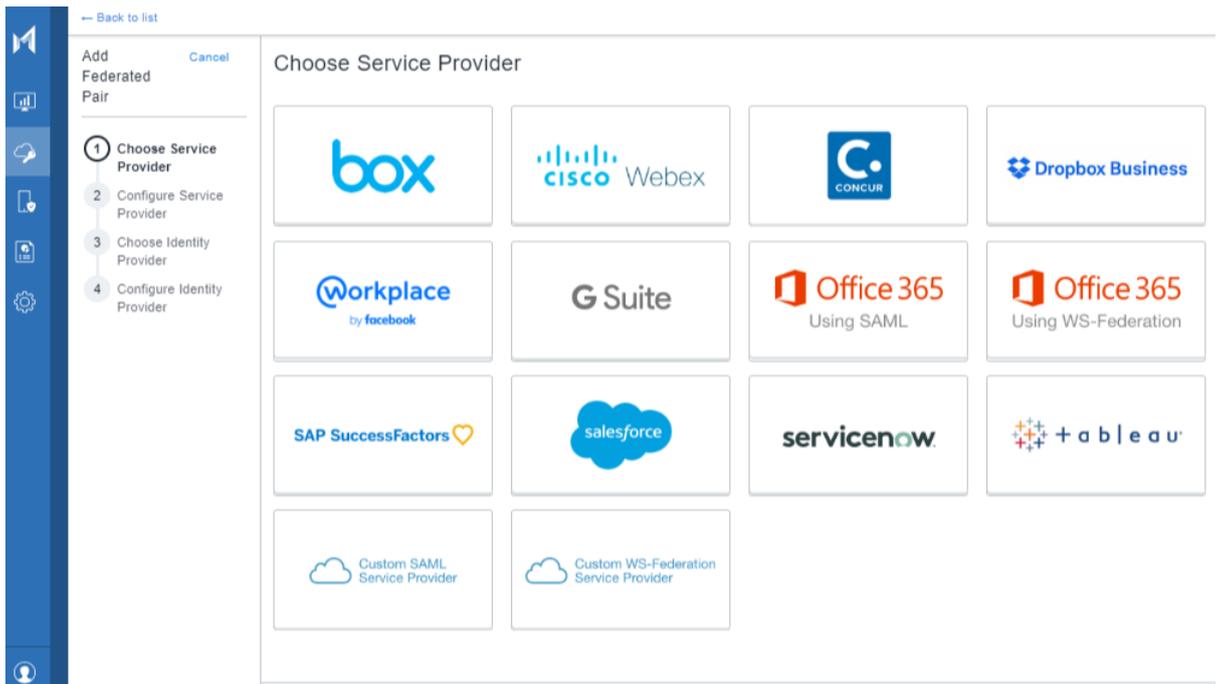
The screenshot shows the Cisco Webex Administration interface. At the top, there is a navigation bar with the Cisco logo, 'Webex Administration', a 'Need help' button, and a user profile for 'mgamez' with a 'Log out' link. Below the navigation bar, a yellow banner contains a message: 'New resources available: Deploying a remote work policy in response to COVID-19 (Technical and end user adoption resources).' Another yellow banner below it states: 'For improved security, you must verify your email address to continue using your Cisco Webex Meetings user account. You'll still be able to use your administrator account.'

The main content area is titled 'Welcome, Matt Gamez !' and 'Site Information'. On the left, a dark sidebar menu is open, showing a tree view of navigation options. The 'SSO Configuration' option is highlighted with a mouse cursor. The main content area displays a table of site information:

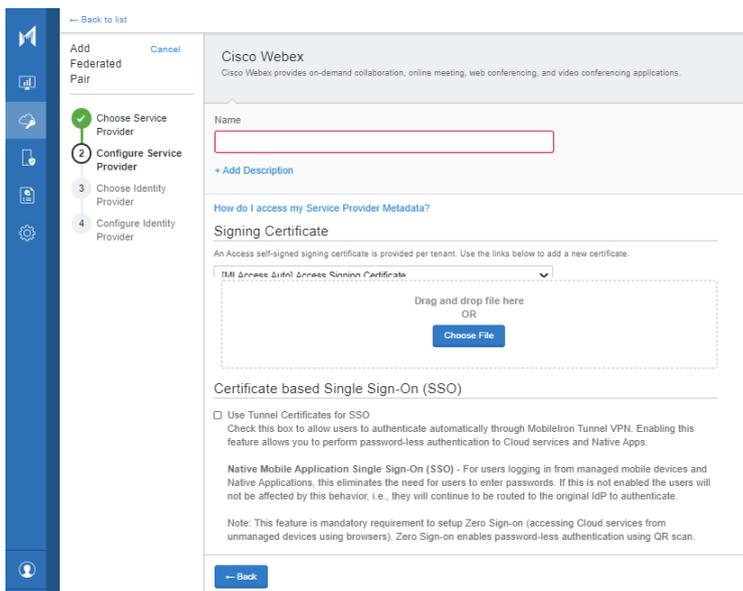
Site Information	
Options	mobileiron-dev.webex.com, mobileiron-dev-da.webex.com, mobileiron-dev-de.webex.com, mobileiron-dev-es.webex.com, mobileiron-dev-fr.webex.com, mobileiron-dev-it.webex.com, mobileiron-dev-jp.webex.com, mobileiron-dev-ko.webex.com, mobileiron-dev-nl.webex.com, mobileiron-dev-pt.webex.com, mobileiron-dev-ru.webex.com, mobileiron-dev-sc.webex.com, mobileiron-dev-sp.webex.com, mobileiron-dev-sw.webex.com, mobileiron-dev-tc.webex.com, mobileiron-dev-tr.webex.com
Webex Desktop Application	
Company Addresses	
Tracking Codes	
User Privileges	
SSO Configuration	Enterprise Site
Session Types	Enrolled. <a href="#">Control Hub log in.</a>
Disclaimers	6 Administrators <a href="#">Show All</a>
Branding	<a href="#">mgamez@mobileiron.com</a>
Site Admin Contact Info	<a href="#">Update Contact Info</a>
Active EE Named Host Accounts:	7

3. Click **Export** in "You can export a SAML metadata WebEx SP configuration file".





4. Select **Cisco Webex** as the service provider from the catalog and click **Next** to configure.
5. Enter the following details to configure Cisco Webex:



- Enter a **Name** and **Description**.
- Select the Access signing certificate from the drop-down or click **Advanced Options** to **Generate Certificate** or **Add a New Certificate**.
- Click **Upload Metadata** to upload the metadata that was downloaded in [Prerequisites](#).

OR

Click **Add Metadata** to enter the **Entity ID** and **Assertion Consumer Services URL**. Open the metadata file downloaded in [Prerequisites](#) and copy the Entity ID.

- (Optional) ) Select "**Use Tunnel Certificates for SSO**" to configure Cert SSO on MobileIron Core. See **Appendix** in the [MobileIron Access Guide](#).
6. Click **Next** to select and configure the appropriate identity provider.
  7. Click **Done** when the identity provider is configured. The Federated Pair is now created.
  8. On the Federation page, download the **Access SP Metadata (Upload to IDP)** and **Access IDP Metadata (Upload to SP)** files.
  9. On the Federation page, click **Publish** to publish the changes to the profile.

## Updating Cisco Webex (Service Provider) configuration

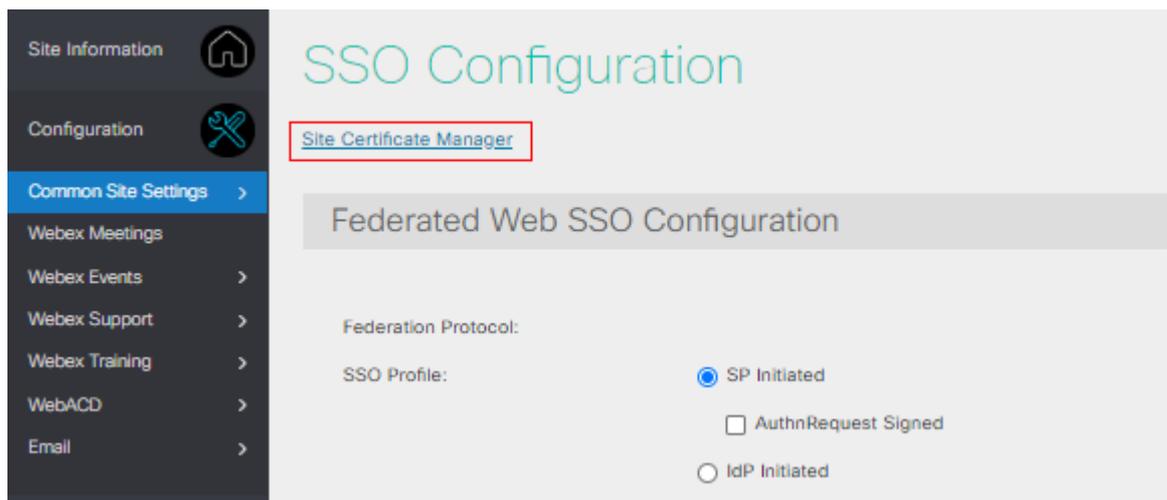
You must configure the Cisco Webex (service provider) settings with the IdP Proxy settings to build a trust relationship.

### Prerequisites

Extract the Entity ID from **Access IDP Metadata (Upload to SP)** downloaded in [Configuring Cisco Webex in MobileIron Access](#).

### Procedure

1. Login to Cisco Webex portal with admin credentials.
2. Click **Configuration > Common Site Settings > SSO Configuration**.
3. Click **Site Certificate Manager**.



4. Click **Import** to import the **Access IDP Metadata (Upload to SP)** downloaded in [Configuring Cisco Webex in MobileIron Access](#).
5. On the **SSO Configuration** page, configure the following fields:

Field	Value
Federation Protocol	SAML 2.0
SSO Profile	SP Initiated
Webex SAML Issuer (SP ID)	<a href="https://www.webex.com">https://www.webex.com</a>
Issuer for SAML (IdP ID)	<a href="https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp">https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp</a>
Customer SSO Service Login URL	<a href="https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp">https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp</a>
NameID Format	Unspecified
AuthnContextClassRef:	ur:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Classes:PasswordProtectedTransport
Single Logout	Customer SSO Service Logout URL: <a href="https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp/logout">https://access.&lt;domainname&gt;/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp/logout</a>
Signature Algorithm for AuthnRequest	SHA256
Auto Account Creation	Selected
Remove uid Domain Suffix for Active Directory UPN	Selected

The screenshot shows the 'Federated Web SSO Configuration' page in a web application. The left sidebar contains navigation options like Site Information, Configuration, Common Site Settings, Webex Meetings, Webex Events, Webex Support, Webex Training, WebACD, Email, User Management, Reports, and Troubleshooting. The main content area is titled 'SSO Configuration' and 'Site Certificate Manager'. The configuration form includes the following fields and options:

- Federation Protocol:** SAML 2.0 (dropdown)
- SSO Profile:**
  - SP Initiated
  - AuthnRequest Signed
  - IdP Initiated
- Target page URL Parameter:** TARGET (text input)
- Webex SAML Issuer (SP ID):** <http://www.webex.com> (text input)
- Issuer for SAML (IdP ID):** <http://www.okta.com/exkco3xxmwl0Z7N4x6> (text input)
- Customer SSO Service Login URL:** [https://dev-667069.okta.com/app/abcdev667069\\_ciscowebex\\_1/exkco3xxmwl0Z7N4x6](https://dev-667069.okta.com/app/abcdev667069_ciscowebex_1/exkco3xxmwl0Z7N4x6) (text input)
- Export:** Export button
- NameID Format:** Unspecified (dropdown)
- AuthnContextClassRef:** urn:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Classes:PasswordProtectedTransport (text input)
- Default Webex Target page URL:** (text input)
- Customer SSO Error URL:** (text input)
- Single Logout:**  Single Logout
- Auto Account Creation:**  Auto Account Creation
- Auto Account Update:**  Auto Account Update
- Remove uid Domain Suffix for Active Directory UPN:**  Remove uid Domain Suffix for Active Directory UPN
- SSO authentication for Attendees:**  SSO authentication for Attendees ⓘ

At the bottom of the configuration form, there are 'Update' and 'Cancel' buttons.