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.

disco Webex Administration			Need help	mgamez Log out
	New resources available: Deploying a remo	te work policy in response to COVID-19 (Technical and end user adoption res	ources).	
For impro	ved security, you must verify your email address to con	tinue using your Cisco Webex Meetings user account. You'll still be able to us	e your administrator acco	unt.
Site Information	Welcome, Matt Ga	amez !		
Configuration	Site Information			
Common Site Settings >	Options	mobileiron-dev.webex.com, mobileiron-dev-da.webex.com, mobileiron	-dev-de.webex.com, m	obileiron-dev-
Webex Meetings	Webex Desktop Application	es.webex.com, mobileiron-dev-fr.webex.com, mobileiron-dev-it.webex		o.webex.com,
Webex Events >	Company Addresses	mobileiron-dev-ko.webex.com, mobileiron-dev-nl.webex.com, mobileiron-	ron-dev-pt.webex.com,	mobileiron-dev-
Webex Support >	Tracking Codes	ru.webex.com, mobileiron-dev-sc.webex.com, mobileiron-dev-sp.web	ex.com, mobileiron-dev	-sw.webex.com,
Webex Training >	User Privileges	mobileiron-dev-tc.webex.com, mobileiron-dev-tr.webex.com		
WebACD >	SSO Configuration	Enterprise Site		
Email >	Session Types	Enrolled. Control Hub log in.		
	Disclaimers	6 Administrators Show All		
User Management	Branding Site Admin Contact Info	mgamez@mobileiron.com		
Reports		Update Contact Info		
	Active EE Named Host Accounts:	7		

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

Site Information	SSO Configuration			
Configuration	Site Certificate Manager			
Common Site Settings >	Endorsted Web SSO C	opfiguration		
Webex Meetings	rederated web 550 C	onngulation		
Webex Events >				
Webex Support >	Federation Protocol:		SAML 2.0 V	
Webex Iraining >	SSO Profile:	SP Initiated		
Fmail >		AuthnRequest Signed		
		O IdP Initiated		
User Management		Target page URL Parameter:	TARGET	
			Import SAML Metadata	
Reports	Webex SAML Issuer (SP ID):		http://www.webex.com	
	Income for CANH (HD ID).			
Liser Management	Issuer for SAME (IdP ID):		http://www.okta.com/exxco.sxxmwiu2G/Nx4x6	
	Customer SSO Service Login URL:		https://dev-667069.okta.com/app/abcdev667069_clscowebex_1/exkco3xxxl *	
Reports	You can export a SAML metadata We	bex SP configuration file:	Export	
Ĭ	NameID Format:		Unspecified V	
User Management	AuthnContextClassRef:		um:federation:authentication:windows;um:oasis:names:to:SAML:2.0:ac:Class	
<u> </u>	Default Webex Target page URL:			
Reports User Management	Customer SSO Error URL:			
	Single Logout			
Reports	Auto Account Creation			
December 0	Auto Account Update			
Recordings	Remove uid Domain Suffix for Act	ive Directory UPN		
Analytics Dol	SSO authentication for Attendees 👔			
Troubleshooting				
	Update Cancel			

4. Save the metadata file.

Configuring Cisco Webex in MobileIron Access

You must now create a federated pair in MobileIron Access.

Prerequisites

• Download and open the metadata file for Cisco Webex as downloaded in <u>Prerequisites</u>. Copy the Entity ID from the metadata file.

Procedure

- 1. Login to MobileIron Access administrative portal with admin credentials.
- 2. Click **Profile** > **Federation**.
- 3. Click Add Pair > Federated pair. The Choose Service Provider window opens.

	← Back to list				
M	Add Cancel Federated Pair	Choose Service Provid	er		
9	1 Choose Service Provider	box	ululu cisco Webey	C.	💱 Dropbox Business
Ŀ	2 Configure Service Provider		CISCO WEDEX	CONCUR	
	3 Choose Identity Provider				
ŵ	4 Configure Identity Provider	by facebook	G Suite	Using SAML	Using WS-Federation
		SAP SuccessFactors ♡	salesforce	servicenow	다. · · · · · · · · · · · · · · · · · · ·
		Custom SAML Service Provider	Custom WS-Federation Service Provider		
Ω					

- 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:

	← Back to list	
M	Add Cancel	Cisco Webex
Q.	Pair	Cisco Webex provides on-demand collaboration, online meeting, web conferencing, and video conferencing applications.
φ	Choose Service Provider	Name
D	2 Configure Service Provider	+ Add Description
	3 Choose Identity Provider	How do Laccess my Service Provider Metadata?
	4 Configure Identity Provider	Signing Certificate
		INI Arress Anth' Arress Siminn Certificate Drag and drop file here OR Choose File
		Certificate based Single Sign-On (SSO)
		I use Tunnel Certificates for SSO Check this box to allow users to authenticate automatically through Mobiletron Tunnel VPIL Enabling this feature allows you to perform password-less authentication to Cloud services and Native Apps. Native Mobile Applications Single Sign-On (SSO) - For users logging in from managed mobile devices and Native Applications, this eliminates the need for users to enter passwords. If this is not enabled the users will not be affected by this behavior, i.e., they will continue to be routed to the original IdP to authenticate. Note: This feature is mandatory requirement to setup Zero Sign-on (accessing Cloud services from unmanaged devices using browsers). Zero Sign-on enables password-less authentication using QR scan.
0		Back

- 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 <u>Prerequisites</u>.

Click **Add Metadata** to enter the **Entity ID** and **Assertion Consumer Services URL**. Open the metadata file downloaded in <u>Prerequisites</u> 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 <u>Configuring Cisco Webex in MobileIron Access</u>.

Procedure

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

Site Information	SSO Configu	uration
Configuration	Site Certificate Manager	
Common Site Settings >		
Webex Meetings	Federated Web SS	SO Configuration
Webex Events >		
Webex Support >	Federation Protocol:	
Webex Training >	SSO Profile:	SD Initiated
WebACD	330 Prome.	SF indated
100100		AuthnRequest Signed
Email >		O IdP Initiated

- 4. Click Import to import the Access IDP Metadata (Upload to SP) downloaded in <u>Configuring Cisco Webex in MobileIron Access</u>.
- 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)	https://www.webex.com	
Issuer for SAML (IdP ID)	https://access. <domainname>/MobileIron/acc/4d856b40- a380-4fa7-9060-6cedefdc1fa0/idp</domainname>	
Customer SSO Service Login URL	https://access. <domain name>/MobileIron/acc/4d856b40-a380-4fa7-9060- 6cedefdc1fa0/idp</domain 	
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: https://access. <domainname>/MobileIron/acc/4d856b40- a380-4fa7-9060-6cedefdc1fa0/idp/logout</domainname>	
Signature Algorithm for AuthnRequest	SHA256	
Auto Account Creation	Selected	
Remove uid Domain Surffix for Active Directory UPN	Selected	

Site Information	SSO Configuration			
Configuration	Site Certificate Manager			
Common Site Settings > Webex Meetings	Federated Web SSO Configuration			
Webex Events > Webex Support > Webex Training > WebACD > Email >	Federation Protocol: SSO Profile:	SP Initiated AuthnRequest Signed IdP Initiated	SAML 2.0	
User Management		Target page URL Parameter:	TARGET	
Reports	Webex SAML Issuer (SP ID):		Import SAML Metadata http://www.webex.com *	
Liser Management	Issuer for SAML (IdP ID):		http://www.okta.com/exkco3xxmwI0ZG7Nx4x6	
	Customer SSO Service Login URL:		https://dev-667069.okta.com/app/abcdev667069_ciscowebex_1/exkco3xxi	
Reports	You can export a SAML metadata \	Nebex SP configuration file:	Export	
-	NameID Format:		Unspecified V	
User Management	AuthnContextClassRef:		urn:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Class *	
	Default Webex Target page URL:			
User Management	Customer SSO Error URL:			
Reports	Single Logout			
	Auto Account Update			
Recordings	Remove uid Domain Suffix for A	Ictive Directory UPN		
Analytics Dol	SSO authentication for Attende	es 🚯		
Troubleshooting	Update Cancel			