MobileIron Access Cookbook

Access with Cisco WebEx and Okta

25 June 2018

Contents

Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Cisco WebEx is federated with an identity provider such as Okta for authentication. The user gets authentication from Okta and obtains a SAML token for accessing applications in a cloud environment, such as Cisco WebEx. This guide serves as step-by-step configuration manual for users using Okta as an authentication provider with Cisco WebEx in a cloud environment.

Disclaimer:

- This cookbook is informational to help with the setup flow and actual screenshots. The steps might vary in your deployment scenario due to changes in SP/IdP versions.
- This cookbook provides information for MobileIron Access with Standalone Sentry. For more information on Access as a service, see *MobileIron Access Guide*.

Prerequisites

You must perform the following steps before you configure Cisco WebEx:

- Download the metadata files for Okta.
    1. Login to Okta with admin credentials.
    2. Click **Admin** > **Add Applications** > **Create New App**.
    3. Select SAML 2.0 and click **Create**.
    4. In General Settings, enter "**Example SAML Application**" in the App name field and click **Next**.
    5. Configure SAML > SAML Settings, enter the following URL in the Single Sign-on URL and Audience URI (SP Entity ID).
       http://example.com/saml/sso/example-okta-com
    6. Click **Next**.
    7. In Feedback, select "I'm an Okta customer adding an internal app" and "This is an internal app that we have created".
    8. Click **Finish**.
       The Sign-on section for the new application appears. Save the identity provider metadata link from this page.

- Download the metadata files for Cisco WebEx.
    1. Login to the WebEx admin portal.
    2. In the site management menu, click **Common Site Settings** > **SSO Configuration**.
    3. On the SSO configuration screen, select SAML 2.0 as the federation protocol.
    4. Click **Export** and **Save** the XML file.

Configuring Cisco WebEx and Okta with MobileIron Access

You must perform the following tasks to configure Cisco WebEx and Okta with MobileIron Access:

Register Sentry to Access

You must register Sentry to Access to fetch the latest configuration from Access.

Prerequisites

Verify that you have registered Sentry earlier. If so, then do not perform this step.

Procedure

1. **Clish** Sentry. In the configuration mode, execute the following command for registration.
   (config)#accs registration https:/<FQDN of Access server><Admin Username of Access Server>
2. Enter the **Tenant password** and complete the registration.
3. In **Access**, click the **Sentry** tab.
4. Select the appropriate Sentry instance, then click **Action** > **Assign**.
5. Enter the tenant password for the profile.
6. Click **OK**.
7. **Clish** Sentry and execute the following command in configuration mode to fetch the latest configuration from Access immediately:

   (config)# accs config-fetch update

   Note: All the published configuration changes are fetched by Sentry assigned to the profile in fifteen minutes. However, if you want to see the changes immediately, then perform Step 6.

Task Result

Single sign-on service is now configured using SAML with WebEx Meetings and Okta. This configuration lets you fetch the latest configuration from Access.

Configure Access to create a Federated Pair

You must configure Access to select your service provider and the identity provider. You can apply the configuration settings for the service provider and the identity provider to create a federated pair.

Procedure

1. Log in to **Access**.
2. Click **Profiles** > **Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. The other fields retain the default values. Click **Save**.
4. Click **Profiles** > **Federated Pairs** > **Add**.
5. Select **Cisco WebEx** as the service provider.
6. Enter the following details:
    a. Enter a **Name**.
    b. Enter an appropriate Description.
    c. Select the Access generated default **Signing Certificate** from the drop-down list.
    d. Upload the metadata file of service provider downloaded from the Prerequisites section.
    e. Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at https://support.mobileiron.com/docs/current/accs/ .
7. Click **Next**.
8. Select **Okta** as the Identity provider. Click **Next**.
9. Add or Upload the **IdP metadata file** download. Click **Done**.
10. Download the **ACCESS SP Proxy** and the **ACCESS IDP Proxy** metadata file.
11. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

Configure the Okta environment

You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

Procedure

1. Login to Okta with Admin credentials.
2. Click **Add Application**.
3. Click **Create New App**.
4. Select **SAML 2.0** and click **Create**.
5. Enter an **App name** for the application and click **Next**.

6. Enter the configuration values.

SAML Settings	Values
Single sign on URL	Extract the single sign on URL from the SP metadata file. Select the check box for **Use this for Recipient URL and destination URL**.
Audience URI (SP Entity ID)	Enter the above single sign on URL.
Default RelayState	Enter the above single sign on URL. If no value is set, a blank relay is sent.
Name ID format	EmailAddress
Application username	Okta username

7. Click **Show Advanced Settings**.

Settings	Values
Response	Unsigned
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	Deselect the check box for Allow application to initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/$(org.externalKey)

8. Configure the **Feedback Settings** and click **Finish**.
    - Are you a customer partner: Select **I'm an Okta customer adding an internal app**.
    - Select the **This is an internal app that we have created** check box.
9. Click **Directory** >**People** > **Add Person** > **Create User**.
10. On the **Applications** tab, click **Assign Application**.
11. Select the Application and the User that you have created and click **Next**.
12. Click **Confirm Assignment**.

Configure the Cisco WebEx environment

You must configure Cisco WebEx to use with Okta.

Prerequisites

- Open the **Access IdP Metadata (Upload to SP)** file exported from Access and copy the signing certificate. Save it in x509 format.

- Note the Entity ID and the Single Logout URL in the exported Access IdP metadata.

Procedure

1. Login to Cisco WebEx admin portal.
2. Click **Configuration** > **Common Site Settings** > **SSO Configuration**.
3. Click **Site Certificate Manager** and browse for the metadata file exported from **Okta** and click **OK** to import.
4. On the **SSO Configuration** page, configure the following fields:

Settings	Description
Federation protocol	SAML 2.0
SSO Profile	SP initiated
WebEx SAML Issuer	http://www.webex.com
Issuer for SAML (IdP ID):	https://<domain_name>/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp Note: Enter the entityID URL that noted in the Prerequisites section.
Customer SSO Service Login URL	https://<domain_name>/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp Note: Enter the entityID URL that noted in the Prerequisites section.
NameID Format	Unspecifed
AuthnContextClassRef	urn:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Classes:PasswordProtectedTransport
Signature Algorithm for AuthnRequest	SHA256
Auto Account Creation	Selected
Remove uid Domain Surffix for Active Directory UPN	Selected