# MobileIron Access Cookbook

## Access with Cisco WebEx and Microsoft ADFS

**25 June 2018**

# Contents

Overview ... 3
Prerequisites ... 3
Configuring Cisco WebEx and Microsoft ADFS with MobileIron Access ... 4
Register Sentry to Access ... 4
Configure Access to create a Federated Pair ... 5
Configure the ADFS environment ... 6
Configure the Cisco WebEx environment ... 8

# 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 Microsoft ADFS for authentication. The user gets authenticated by ADFS and obtains a token for accessing applications in a cloud environment, such as Cisco WebEx.

This guide serves as step-by-step configuration manual for users using ADFS 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

Verify that you have the following components in your environment:

- ADFS version 3.0
- **ADFS (IDP) Metadata Files**
  You must download the ADFS metadata files for ADFS (IdP)
  - Download ADFS metadata file from https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
- **Cisco WebEx (SP) Metadata Files**
  You must download the metadata files to configure Cisco WebEx:
  1. Login to Cisco WebEx as an administrator.
  2. Click **Configuration** > **Common Site Settings** > **SSO Configuration**
  3. Click **Export** under “You can export a SAML metadata WebEx SP configuration file”.

# Configuring Cisco WebEx and Microsoft ADFS with MobileIron Access

You must perform the following tasks to accomplish the configuration between Cisco WebEx and Microsoft ADFS:

- Register Sentry to Access
- Configure Access to create a Federated Pair
- Configure the ADFS environment
- Configure the Cisco WebEx environment

## Register Sentry to Access

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

### Prerequisite

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

### Procedure

1. **SSH** to Sentry CLI. 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. Click **OK**.
6. **SSH** to Sentry CLI 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 Cisco WebEx as the service provider and Microsoft ADFS as the identity provider. This configuration lets you fetch the latest configuration from Access.

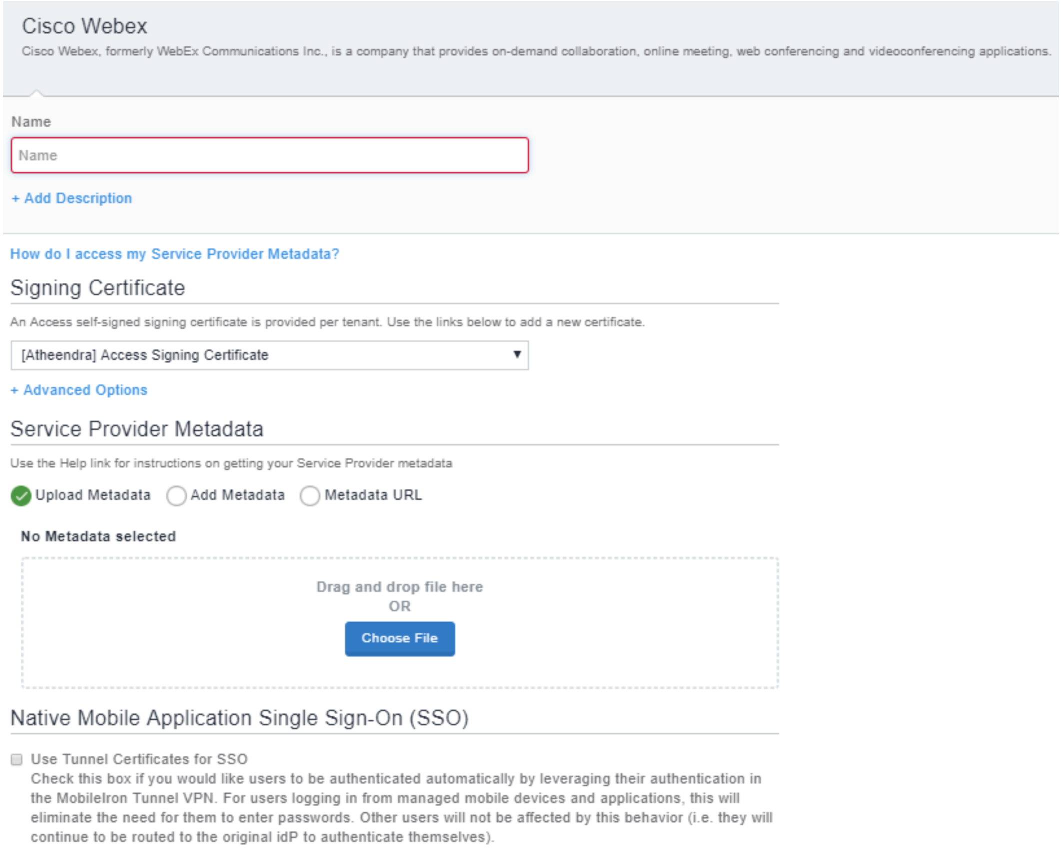
## Configure Access to create a Federated Pair

You must configure Access to select your service provider and the identity provider to create a federated pair.

### Procedure

1. In Access, click **Profile** > **Get Started**.
2. Enter the Access host information and upload the ACCESS SSL Certificate. The other fields retain their default values. Click **Save**.
3. Click **Profile** > **Federated Pairs** > **Add New Pair.**
4. Select **Cisco WebEx** as the service provider.
5. Enter the following details:

   - Name
   - Description
   - Select the Access Signing Certificate or use the **Advanced Options** to create and upload a new Access Signing Certificate.
   - Upload the metadata file of the service provider.
   - (Optional) 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/.



Cisco Webex

Cisco Webex, formerly WebEx Communications Inc., is a company that provides on-demand collaboration, online meeting, web conferencing and videoconferencing applications.

Name

Name

+ Add Description

How do I access my Service Provider Metadata?

Signing Certificate

An Access self-signed signing certificate is provided per tenant. Use the links below to add a new certificate.

[Atheendra] Access Signing Certificate ▾

+ Advanced Options

Service Provider Metadata

Use the Help link for instructions on getting your Service Provider metadata

● Upload Metadata ○ Add Metadata ○ Metadata URL

No Metadata selected

Drag and drop file here
OR
Choose File

Native Mobile Application Single Sign-On (SSO)

□ Use Tunnel Certificates for SSO

Check this box if you would like users to be authenticated automatically by leveraging their authentication in the MobileIron Tunnel VPN. For users logging in from managed mobile devices and applications, this will eliminate the need for them to enter passwords. Other users will not be affected by this behavior (i.e. they will continue to be routed to the original idP to authenticate themselves).

6. Click **Next** and select **Microsoft** as the identity provider.

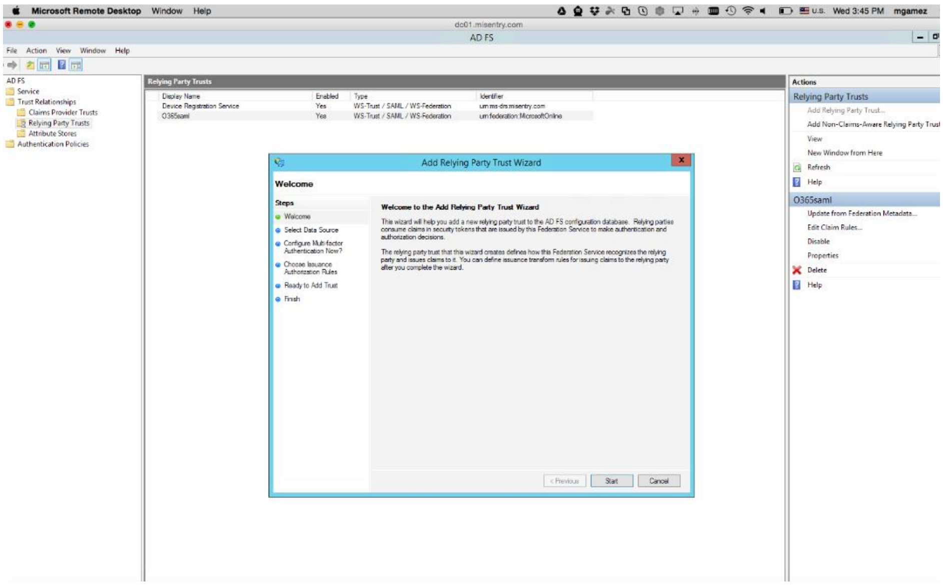
7. Select the **Access Signing Certificate** or use the **Advanced Options** to create and upload a new self-signed Access Signing Certificate.
8. Add or Upload the **IdP metadata** file that you downloaded.
9. Click **Done**.
10. Download the **Access SP Metadata (Upload to IDP)** and **ACCESS IDP Metadata (Upload to SP)** metadata files.
11. Click **Publish** to publish the profile.

## Configure the ADFS environment

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

### Procedure

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Click **Start** > **Administrative tools** > **ADFS Management** > Expand **Trust Relationships.**
3. Click **Relying Party Trust.** In the right-hand pane, click **Add Relying Party Trust** and follow the prompts.



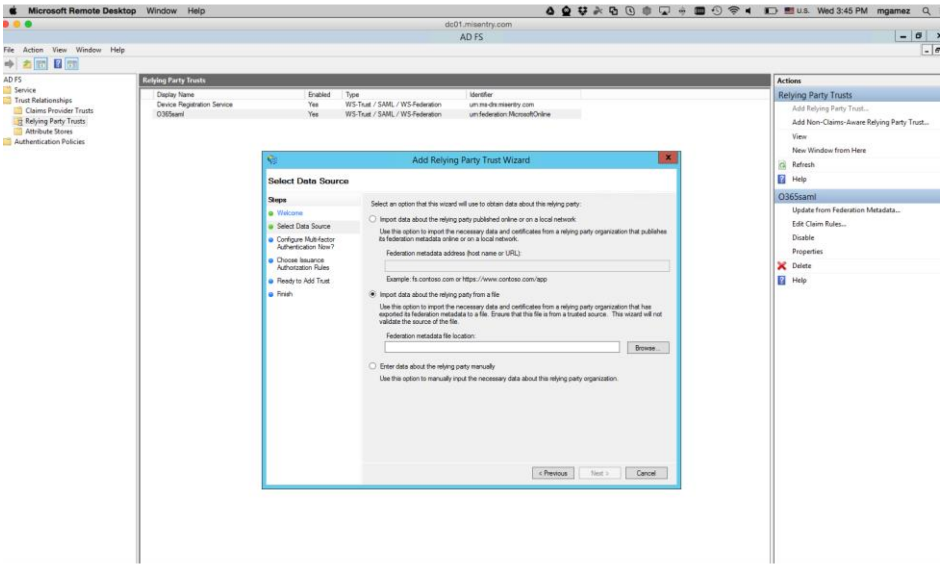
| Display Name | Enabled | Type | Identifier |
|---|---|---|---|
| Device Registration Service | Yes | WS-Trust / SAML / WS-Federation | urn:ms-drs:misentry.com |
| O365saml | Yes | WS-Trust / SAML / WS-Federation | urn:federation:MicrosoftOnline |

**Welcome to the Add Relying Party Trust Wizard**

This wizard will help you add a new relying party trust to the AD FS configuration database. Relying parties consume claims in security tokens that are issued by this Federation Service to make authentication and authorization decisions.

The relying party trust that this wizard creates defines how this Federation Service recognizes the relying party and issues claims to it. You can define issuance transform rules for issuing claims to the relying party after you complete the wizard.

4. Click **Start** and select **Import data about the relying party from a file**. Click **Next**.



Relying Party Trusts

| Display Name | Enabled | Type | Identifier |
|---|---|---|---|
| Device Registration Service | Yes | WS-Trust / SAML / WS-Federation | urn:ms-drs:misentry.com |
| O365saml | Yes | WS-Trust / SAML / WS-Federation | urn:federation:MicrosoftOnline |

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

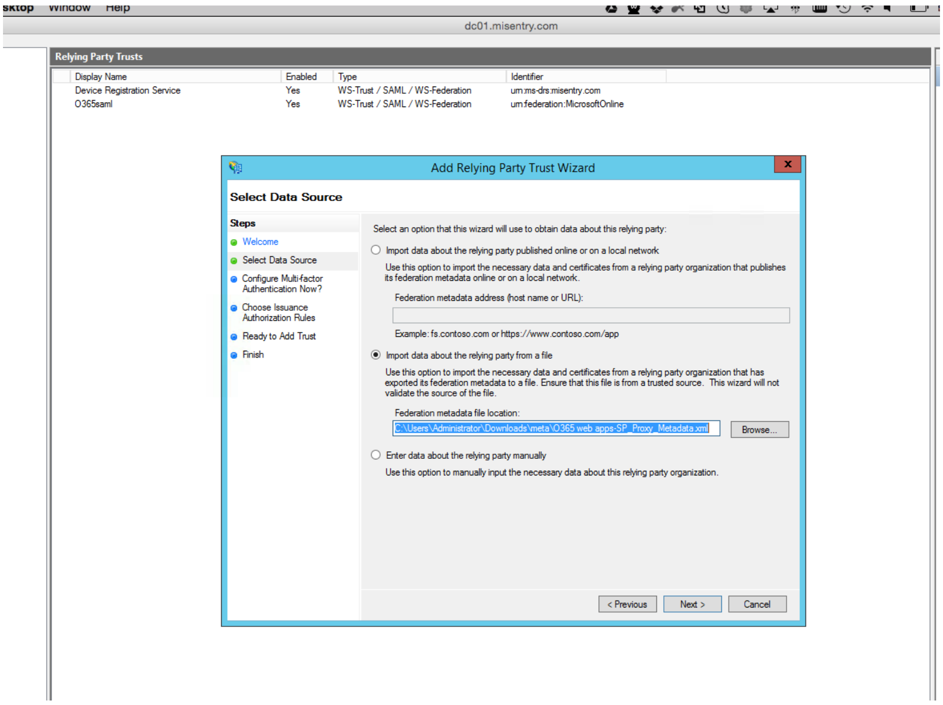
Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

5. Click **Browse** and select the service provider proxy metadata file that you downloaded and click **Next**.

   **Note**: The filename for the proxy metadata file name ends with *UploadTo-Microsoft ADFS-IdP.xml*.



Relying Party Trusts

| Display Name | Enabled | Type | Identifier |
|---|---|---|---|
| Device Registration Service | Yes | WS-Trust / SAML / WS-Federation | urn:ms-drs:misentry.com |
| O365saml | Yes | WS-Trust / SAML / WS-Federation | urn:federation:MicrosoftOnline |

Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

● Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location: C:\Users\Administrator\Downloads\meta\O365 web apps-SP_Proxy_Metadata.xml

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

6. Enter the **Display Name** and click **Next.**
7. Select "I do not want to configure multi-factor authentication settings for this relaying party trust at this time." and click **Next**.
8. Select "Permit all users to access this relying party" and click **Next**.
9. At the end, select **Open Edit Claim rules dialog for relying party trust**.

10. In the **Claim Rule Template** drop-down, select **Send Claims Using a Custom Rule** and click **Next.**
11. Add **Claim rules** as follows:

- **Claim rule name**: Name ID Mapping
- **Attribute store**: Active Directory
- **LDAP Attribute**: E-Mail-Addresses
- **Outgoing Claim Type**: Name ID

12. Click **Add Rule** to add an Auto Account Create rule.

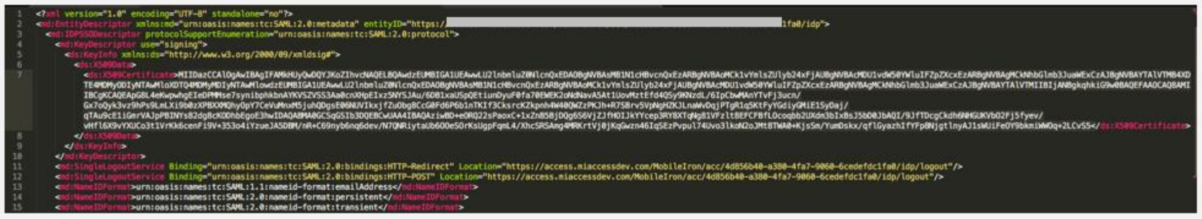
- **Claim rule name**: AutoAccountCreate
- **Attribute store**: Active Directory
- **LDAP Attribute**:
    - E-Mail_Attributes: email
    - Given-Name: firstname
    - Surname: lastname

13. Click **Apply** and **OK.**

## Configure the Cisco WebEx environment

### Prerequisites

- Open the exported **ACCESS IDP Metadata** and extract the signing certificate. Save it as x509 format as shown below



```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https:/[redacted]1fa0/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIIDazCCAlOgAwIBAgIFAMkHUyQwDQYJKoZIhvcNAQELBQAwdzEUMBIGA1UEAwwLU2lnbmluZ0NlcnQxEDAOBgNVBAsMB1N1cHBvcnQxEzARBgNVBAoMCk1vYmlsZUlyb24xFjAUBgNVBAcMDU1vdW50YWluIFZpZXcxEzARBgNVBAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XD
          TE4MDMyODIyNTAwMloXDTQ4MDMyMDIyNTAwMlowdzEUMBIGA1UEAwwLU2lnbmluZ0NlcnQxEDAOBgNVBAsMB1N1cHBvcnQxEzARBgNVBAoMCk1vYmlsZUlyb24xFjAUBgNVBAcMDU1vdW50YWluIFZpZXcxEzARBgNVBAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMI
          IBCgKCAQEApGBL4eKwpwhgEIeDPMMse7synibphkbnAYKVSZVSS3Aa0cnXHpEIxzSNYSJAu/6DB1xaUSpQEtiunDyuF0fa70EWEK2oNdNavA5At1UovMztEfd4QSy9KNzdL/6IpCbwMAnYTvFj3ucn/
          Gx7oQyk3vz9hPs9LmLXi9b0zXPBXXMQhyOpY7CeVuMnxM5juhQDgsE06NUVIkxjfZuObgBCcG0Fd6P6b1nTKIf3CksrcKZkpnh4W40QWZzPKJh+R75Brv5VpNgHZKJLnaWvOqjPTgR1q5KtFyYGdiyGMiE1SyDaj/
          qTAu9cE1iGmrVAJpPBINYs82dg8cKODhbEgoE3hwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAziwBD+eORQ22sPaoxC+1xZn858jDQg6S6VjZJfHOIJkYYcep3RY8XTqNg81VFzltBEFCFBfLOcoqbb2UXdm3bIxBsJ5bD0JbAQI/9JfTDcgCkdh6NMGUKVbO2Fj5fyev/
          vHfl6X9vYXUCo3t1VrKk6cenFi9V+353o4iYzueJA5DBM/nR+C69nyb6nq6dev/N7QNRiytaUb6O0e5OrKsUgpFqmL4/XhcSRSAmg4MRKrtVj0jKqGwzn46IqSEzPvpul74Uvo3lkoN2oJMtBTWA0+KjsSm/YumDskx/qflGyazhIfYFpBNjgtlnyAJ1sWUiFeOY9bkmiWWOq+2LCvS5</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://access.miaccessdev.com/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp/logout"/>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://access.miaccessdev.com/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp/logout"/>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
```

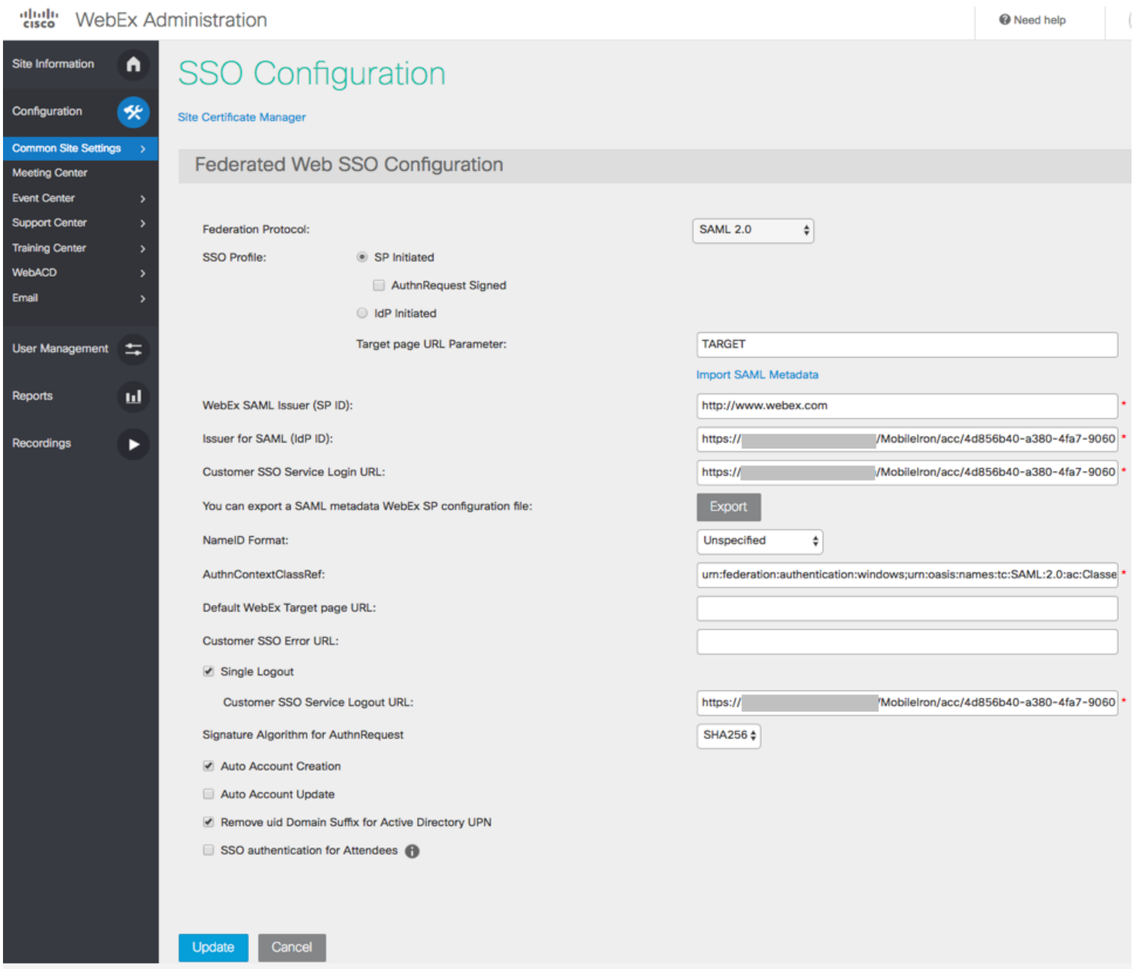
- Note the Entity ID and the Single Logout URL in the exported Access IdP metadata.

### Procedure

1. Login to the Cisco WebEx portal with admin credentials.
2. Click **Configuration** > **Common Site Settings** > **SSO Configuration**.
3. Click **Site Certificate Manager**.
4. Browse for the Token Signing Certificate exported from Microsoft ADFS and click **OK** to import.
5. On the SSO Configuration page, configure the following fields:

| | |
|---|---|
| Federation Protocol | SAML 2.0 |
| SSO Profile | SP Initiated |

| | |
|---|---|
| WebEx SAML Issuer (SP ID): | http://www.webex.com |
| Issuer for SAML (IdP ID): | https://access.<domain name>/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp<br>**Note**: This URL is the entityID saved in the Prerequisites section above. |
| Customer SSO Service Login URL: | https://access.<domain name>/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp<br>**Note**: This URL is the entityID saved in the Prerequisites section above |
| NameID Format | Unspecifed |
| AuthnContextClassRef: | urn:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Classes:PasswordProtectedTransport |
| Single Logout | Customer SSO Service Logout URL:<br>https://access.<domain name>/MobileIron/acc/4d856b40-a380-4fa7-9060-6cedefdc1fa0/idp/logout<br>**Note**: This URL is the Single Logout URL saved in the Prerequisites section above |
| Signature Algorithm for AuthnRequest | SHA256 |
| Auto Account Creation | Selected |
| Remove uid Domain Surffix for Active Directory UPN | Selected |



SSO Configuration

Federated Web SSO Configuration

Federation Protocol: SAML 2.0

SSO Profile: ● SP Initiated

□ AuthnRequest Signed

○ IdP Initiated

Target page URL Parameter: TARGET

Import SAML Metadata

WebEx SAML Issuer (SP ID): http://www.webex.com *

Issuer for SAML (IdP ID): https://[redacted]/MobileIron/acc/4d856b40-a380-4fa7-9060 *

Customer SSO Service Login URL: https://[redacted]/MobileIron/acc/4d856b40-a380-4fa7-9060 *

You can export a SAML metadata WebEx SP configuration file: Export

NameID Format: Unspecified

AuthnContextClassRef: urn:federation:authentication:windows;urn:oasis:names:tc:SAML:2.0:ac:Classe *

Default WebEx Target page URL:

Customer SSO Error URL:

☑ Single Logout

Customer SSO Service Logout URL: https://[redacted]/MobileIron/acc/4d856b40-a380-4fa7-9060 *

Signature Algorithm for AuthnRequest: SHA256

☑ Auto Account Creation

□ Auto Account Update

☑ Remove uid Domain Suffix for Active Directory UPN

□ SSO authentication for Attendees

Update Cancel