Configuring SSO Using SAML Cookbook

Concur and Microsoft ADFS

May 02, 2017

Contents

Overview

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

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 the ADFS metadata file from https://<ADFS Server FQDN> /FederationMetadata/2007-06/FederationMetadata.xml
- **Concur Metadata Files**
  Verify that you have the metadata files for Concur (SP):
  - **Entity ID -** https://concursolutions.com
  - **Assertion Consumer Service URL -** https://concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx

Configuring Concur and Microsoft ADFS with MobileIron Access

You must perform the following tasks to accomplish the configuration between Concur and ADFS:

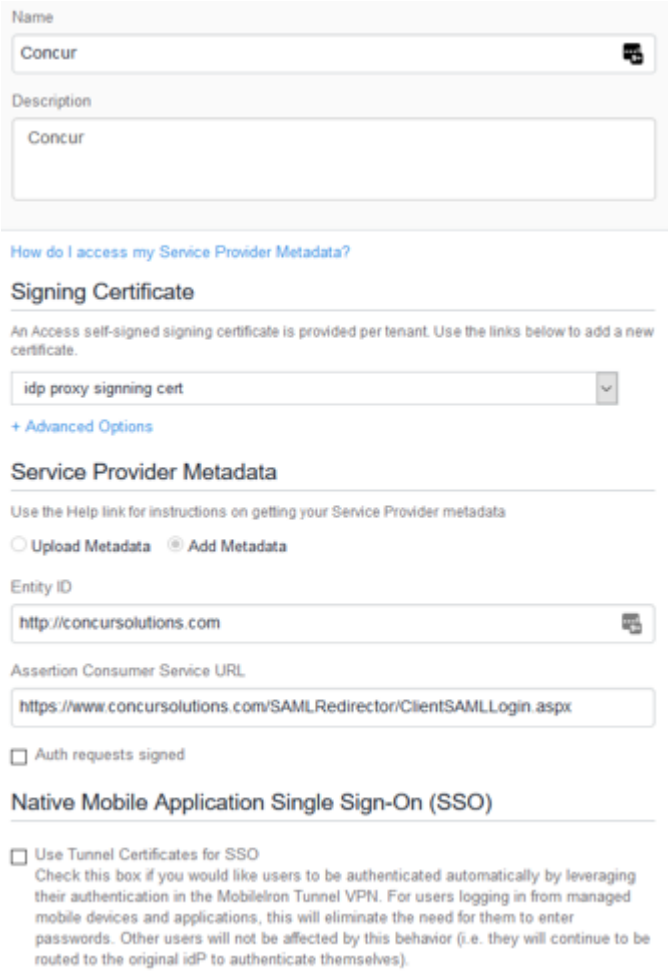
Configure Access to create a Federated Pair

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. It creates a federated pair.

Procedure

1. In Access, click **Profiles** > **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 **Profiles** > **Federated Pairs** > **Add.**
4. Select **Concur** as the service provider.
5. Enter the following details:

    a) Enter a **Name** for Concur.
    b) Enter an appropriate **Description**.
    c) Select the Access generated default **Signing Certificate** from the drop-down list.
    d) Select **Add Metadata** manually.
        - Enter the Entity ID - https://concursolutions.com
        - Enter the Assertion Consumer Service URL - https://concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx
    e) (Optional): Select **Use Tunnel Certificates for SSO** for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN.



6. Click **Next** and select **Microsoft ADFS** as the identity provider. Click **Next**.
7. Select the default **Signing Certificate** from the drop-down list.
8. Upload **IdP metadata** file that you downloaded from https://<ADFS Server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml
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.
    MobileIron Access setup for Concur is complete.

What's Next

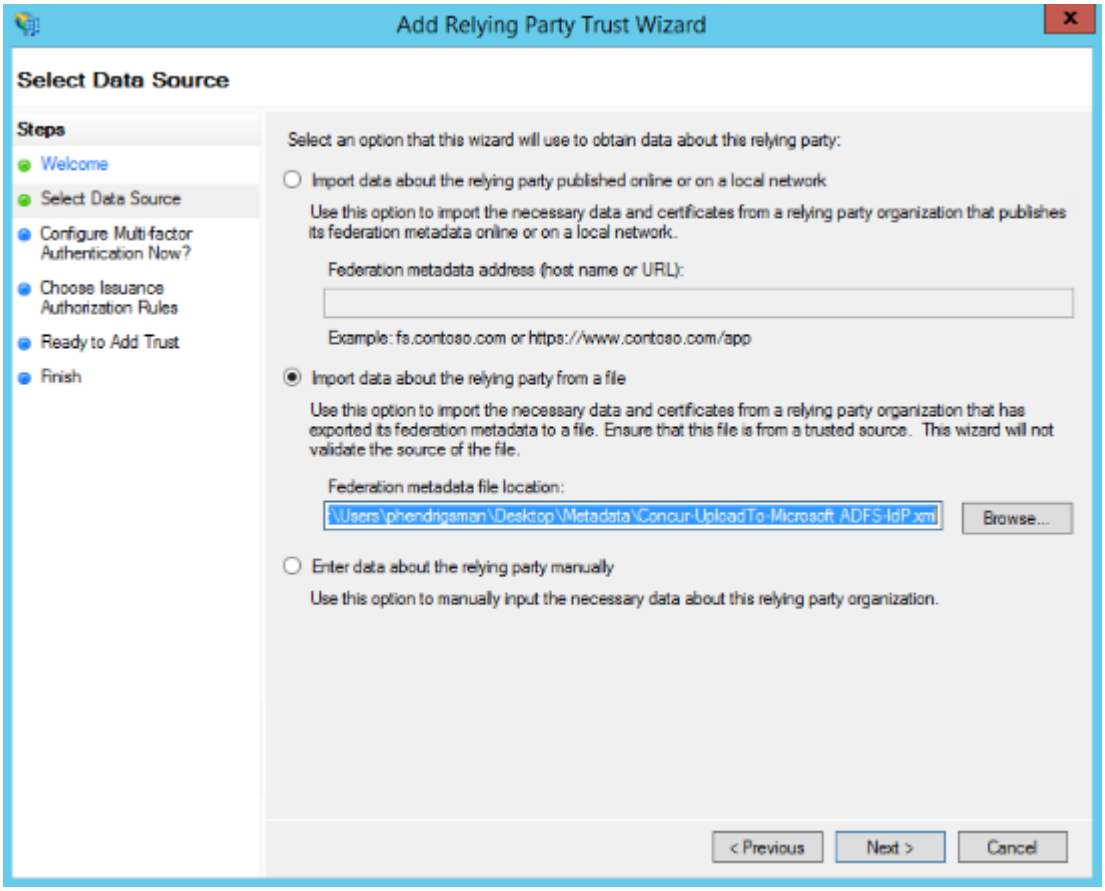
Contact your Concur support representative to request that they complete the SAML connection in Concur. You must provide the *Access IDP Metadata* to upload it to the Concur server.

Configure 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.
4. Click **Start** and select **Import data about the relying party from a file**. Click **Browse** to upload the metadata file that you downloaded from Access.



   a) On **Specify Display Name**, enter a unique **Display Name** and click **Next.**
   b) On **Configure Multi-factor Authentication Now?**, select *I do not want to configure multi-factor authentication settings for this relying party trust at this time*.
   c) On **Issuance Authorization Rules**, select *Permit all users to access the relying party*.
   d) Click **Next** and retain all default values on further prompts. Click **Finish**.
5. Right-Click **Relying Party Trust** and select **Edit Claim Rules**.

6. Click **Add Rule** and select **Send LDAP Attributes as Claims** from the Claim rule template drop-down list. Click **Next**.
7. Configure the **Claim Rule** and click **OK**.
    a) Enter a **Claim rule name**.
    b) Select **Active Directory** from the **Attribute store** drop-down list.
    c) Map the **Email Addresses** to **Name ID**.

    Note: If you choose to enable Native SSO using MobileIron Access, map **User-Principal-Name** to **Name ID**.

8. Edit the federated pair: On **Concur Properties** tab > **Advanced** tab, select the secure hash algorithm to use SHA-1 from the drop-down list.
9. On endpoints tab, select the Endpoints and add the SAML logout endpoints.
    a) Trusted URL - https://<ADFS Server FQDN>/adfs/ls
    b) Response URL - https://<ADFS Server FQDN>/logout
10. Click **Apply** and **OK.**

Configure Concur environment

You must configure Concur to build the trust relationship with the Identity Provider.

Procedure

1. Download the Access IDP Metadata from Access that is available in the step 10 of **Configure Access to create a Federated Pair**.
2. Copy the SAML 2.0 Endpoint (HTTP) URL from the metadata file from SingleSignOnService tag for HTTP-Redirect.

    For example: Copy the highlighted string.

3. Copy the X.509 certificate string from the metadata file into a text file.

    For example: Copy the highlighted string into a text file.

4. Contact your Concur support representative to complete the SAML connection in Concur.
   The representative requires the SAML 2.0 Endpoint (HTTP) and X.509 certificate from step 2 and step 3.

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. **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. Click **OK**.
6. **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.

What's Next

Contact your Concur support representative to request that they complete the SAML connection in Concur. You must provide the SAML 2.0 Endpoint (HTTP) and X.509 certificate that you copied to your Concur support representative.

Task Result

Single-sign-on service is now configured using SAML with Concur as the service provider and Microsoft ADFS as the identity provider. This configuration lets you fetch the latest configuration from Access.

You are now ready to test your Concur SSO login from your ADFS sign-in page.

Working with Concur application on mobile devices

Procedure

1. Download Concur as a managed application from Apps@work app to any iOS or other devices registered to MobileIron Core or MobileIron Cloud.
2. Launch the Concur application.
   Verify that the **Settings** page displays when you double-click the Concur logo.
3. Edit the server URL to https://concursolutions.com and click **Save**.
4. Click **SSO Company Code Sing-in** on the application and add the company code.
   You are now re-directed to the ADFS sign-in page with username and password. However, if you have selected **Use Tunnel Certificates for SSO** option in MobileIron Access, then you are signed-in automatically without a prompt for username or password.
5. The Report and Expense page displays.

Working with Concur application on laptops or desktops

Procedure

1. Navigate to https://<ADFS Server FQDN>/adfs/ls/idpinitiatedsignon in a browser.
2. Select **Concur**.
3. Enter the username and password in the ADFS page.
4. The Reports and Expense page displays with sign-on.