



Configuring SSO Using SAML Cookbook

Concur and Microsoft ADFS

May 02, 2017



Contents

Overview.....	3
Prerequisites.....	3
Configuring Concur and Microsoft ADFS with MobileIron Access.....	4
Configure Access to create a Federated Pair	4
Configure ADFS environment.....	6
Configure Concur environment	7
Register Sentry to Access	8
Working with Concur application on mobile devices.....	9
Working with Concur application on laptops or desktops.....	9



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](#)
- [Configure ADFS environment](#)
- [Configure Concur environment](#)
- [Register Sentry to 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. 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.



Name
Concur

Description
Concur

[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.

idp proxy signing cert

[+ Advanced Options](#)

Service Provider Metadata

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

Upload Metadata Add Metadata

Entity ID
http://concur solutions.com

Assertion Consumer Service URL
https://www.concursolutions.com/SAMLRedirector/ClientSAMLLogin.aspx

Auth requests signed

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 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.

Concur
Concur
Policy Name: Default Policy

SP Metadata [View](#)
Access SP Metadata (Upload to IDP) [View](#) | [Download](#)
IDP Metadata [View](#)
Access IDP Metadata (Upload to SP) [View](#) | [Download](#)

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.

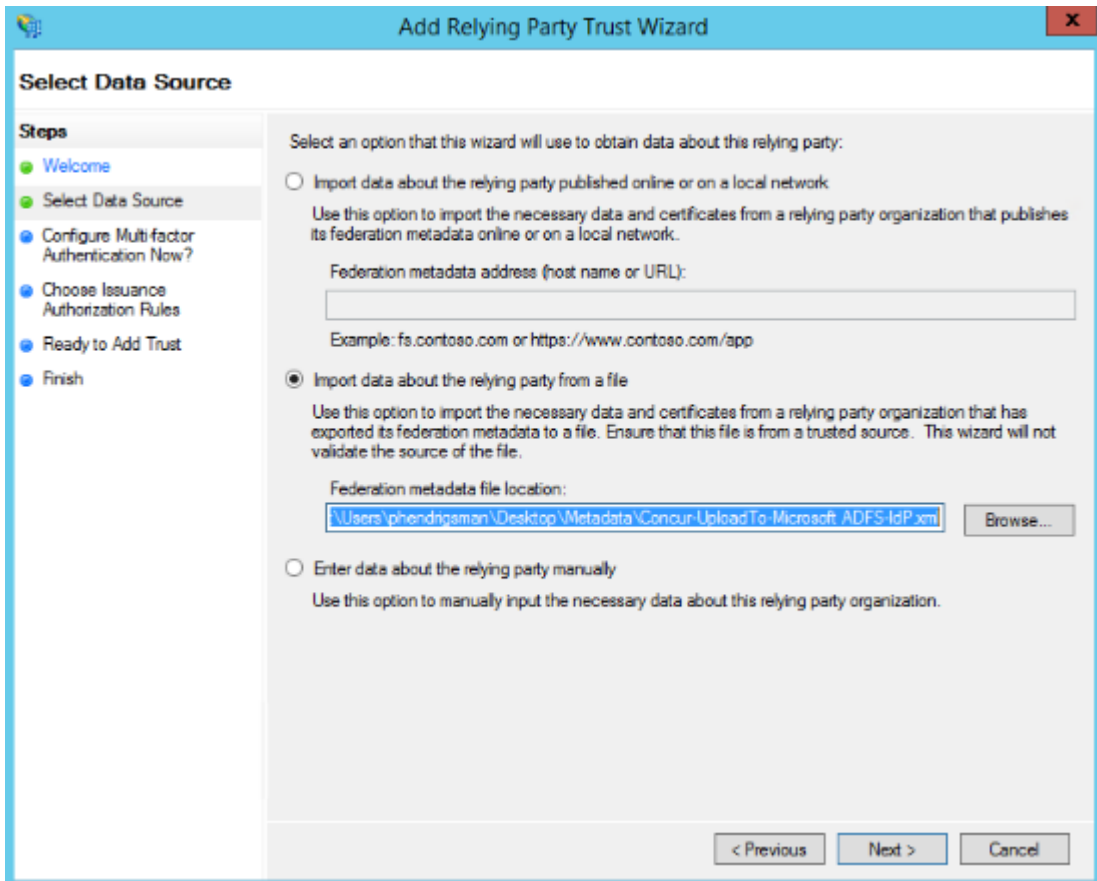


Configure ADFS environment

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.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://eapp192-alt.auto.mobileiron.com/MobileIron/acc/357910ea-04e1-4bdf-94d8-e1b68301b701/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>MIIIDjCCA LKqAwIBAgIEIj/
AgzANBgkqhkiG9w0BAQsFAAD3R0UwEgyYVQ00DAtTawduan5n02VyY0EgNA4A1UECWhU3Vmc09yZDE0DEBGA1UECgwtMTUwLXNkLXJvbjEwMC51b3R0eXN0Y2Vzcm5pYTEuLm
GA1UEBmN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm
TMBAEAAQKQ2FsaWZcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm51b3R0eXN0Y2Vzcm5pYTEuLm
g4L26zFnx8Tb70Yy0ANNZ6oKzJ2BzJUCSvKw8mLQJ1191P6T1Bk1Jot1qGIVERWnhdZ4UFTFRtAC1BngF1hEY0zqfUaUvUx49LFtK85mVGu5zozggnlg0pu+sYc04p5QZ5LefFVoyIn9Uw/0JcK2ncVfLkqCI
+1ZLULYjCFWz7Y75gWjUxMd3HsbhKehPCNeJkGLeRyZhdRgYvDXtGEY7eoG/nyYNgVZqWz8hNYe+oPaR0Jjy+LW1h1TayCSjLALCXmLmZInhyHa9Kda6xBak/6VGoetZ3a7UhbjkhnCJE+06gRP+rzzKohBgj0CnVgqK00
+ndfVg6j/s0cj+7V1Lvgq/65mHtcqXyngd+3LKJjpsSnmz0K7xZB4MZl9sLCZ5mb/1utn9hVYMC913R/pfXpJlI80Aq/QY9406Zu+T1AAWH8KfA0eF7zB6pMJKr+VcHgz03Rk1B55HDBCEHs=</ds:
X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:IDPSSODescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://eapp192-alt.auto.mobileiron.com/MobileIron/acc/357910ea-04e1-4bdf-94d8-
e1b68301b701/idp/logout/">
  </md:SingleLogoutService>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://eapp192-alt.auto.mobileiron.com/MobileIron/acc/357910ea-04e1-4bdf-94d8-
e1b68301b701/idp/logout/">
  </md:SingleLogoutService>
  <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>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://eapp192-alt.auto.mobileiron.com/MobileIron/acc/357910ea-04e1-4bdf-94d8-
e1b68301b701/idp/">
  </md:SingleSignOnService>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://eapp192-alt.auto.mobileiron.com/MobileIron/acc/357910ea-04e1-4bdf-94d8-
e1b68301b701/idp/">
  </md:SingleSignOnService>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="E-Mail Address" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-uri"/>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Given Name" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname" NameFormat="urn:
  oasis:names:tc:SAML:2.0:attribute-uri"/>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Name" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attribute-uri"/>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="URN" Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/urn" NameFormat="urn:oasis:names
  tc:SAML:2.0:attribute-uri"/>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="Common Name" Name="http://schemas.xmlsoap.org/claims/COMMON" NameFormat="urn:oasis:names:tc:
  SAML:2.0:attribute-uri"/>
  <saml2:Attribute xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion" FriendlyName="AD FS 1.x E-Mail Address" Name="http://schemas.xmlsoap.org/claims/EmailAddress" NameFormat="urn:
  oasis:names:tc:SAML:2.0:attribute-uri"/>
  </md:EntityDescriptor>
</xml>
```

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.



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://concurolutions.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.

Copyright © 2016 - 2017 MobileIron, Inc. All Rights Reserved.



Any reproduction or redistribution of part or all of these materials is strictly prohibited. Information in this publication is subject to change without notice. MobileIron, Inc. does not warrant the use of this publication. For some phone images, a third-party database and image library, Copyright © 2007-2009 Aeleeta's Art and Design Studio, is used. This database and image library cannot be distributed separate from the MobileIron product.

“MobileIron,” the MobileIron logos and other trade names, trademarks or service marks of MobileIron, Inc. appearing in this documentation are the property of MobileIron, Inc. This documentation contains additional trade names, trademarks and service marks of others, which are the property of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.