MobileIron Access Cookbook

Access with Workday and Microsoft ADFS

09 February 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 Workday 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 Workday. This guide serves as step-by-step configuration manual for users using ADFS as an authentication provider with Workday 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.

Prerequisites

Verify that you have the following components in your environment:

- ADFS version 3.0
- Existing working direct federation between ADFS and Workday
- **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

- **Workday Metadata Files**
  You must download the metadata files for Workday (SP)

  In the Workday administration portal, navigate to **Generate Workday SAML Metadata**. Copy the text starting with "<md:EntityDescriptor>” and save it as a metadata file with .xml extension. This is the Workday metadata file.

Configuring Workday and Microsoft ADFS with MobileIron Access

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

- Register Sentry to Access
- Configure Access to create a Federated Pair
- Configure the ADFS environment
- Configure the Workday 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. **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.

Task Result

This configuration lets you fetch the latest configuration from Access.

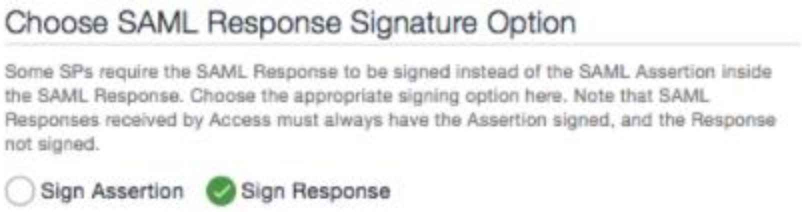
Configure Access to create a Federated Pair

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 **Custom Service Provider** 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 Workday (SP) downloaded in the Prerequisites section.
   - Under Choose SAML Response Signature option, select **Sign Response**.

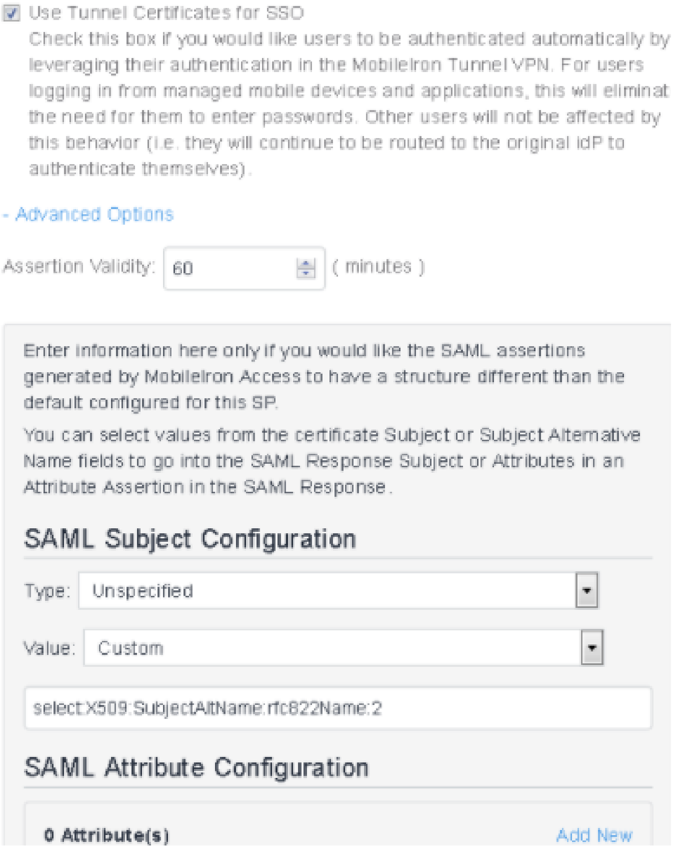


Choose SAML Response Signature Option

Some SPs require the SAML Response to be signed instead of the SAML Assertion inside the SAML Response. Choose the appropriate signing option here. Note that SAML Responses received by Access must always have the Assertion signed, and the Response not signed.

○ Sign Assertion ● Sign Response

   - **(Optional)** Select Use Tunnel Certificates for SSO for users to be authenticated automatically. This leverages the user's authentication in the MobileIron Tunnel VPN.
     Note: Ensure that the field required to login to Workday (such as the employee id) is a part of the certificate (such as a Subject Alternative Name of type Rfc822Name). Specify a custom SAML Subject Configuration that pulls the value from the certificate and provides it to Workday in the SAML assertion generated by MobileIron Access.



☑ 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 eliminat 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).

- Advanced Options

Assertion Validity: 60 (minutes)

Enter information here only if you would like the SAML assertions generated by MobileIron Access to have a structure different than the default configured for this SP.

You can select values from the certificate Subject or Subject Alternative Name fields to go into the SAML Response Subject or Attributes in an Attribute Assertion in the SAML Response.

SAML Subject Configuration

Type: Unspecified

Value: Custom

select:X509:SubjectAltName:rfc822Name:2

SAML Attribute Configuration

0 Attribute(s)

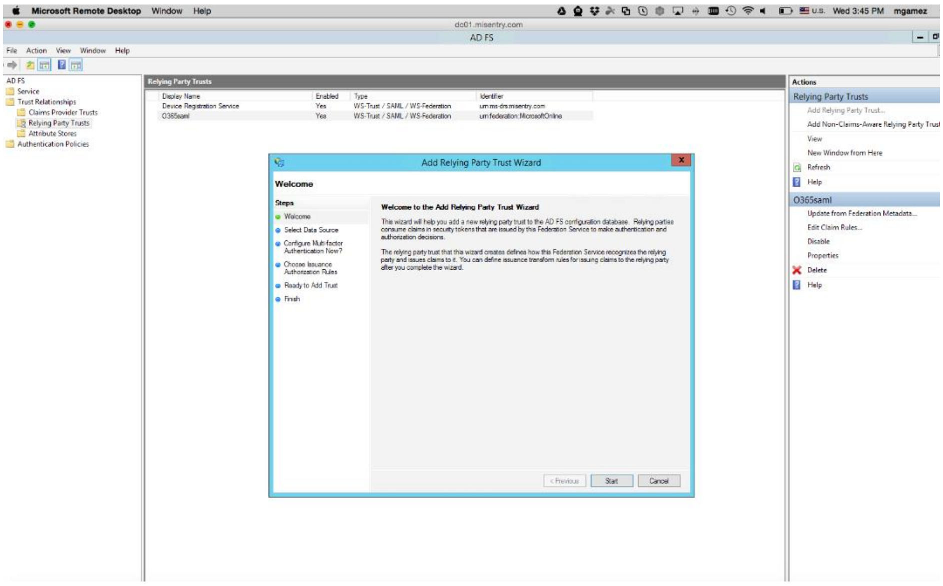
6. Click **Next** and select **Microsoft** as the identity provider.
7. Select the **Access Signing Certificate** or use the **Advanced Options** to create and upload a new self-signed Access Signing Certificate.
8. Add or Upload the **IdP metadata** file that you downloaded in the Prerequisites section.
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

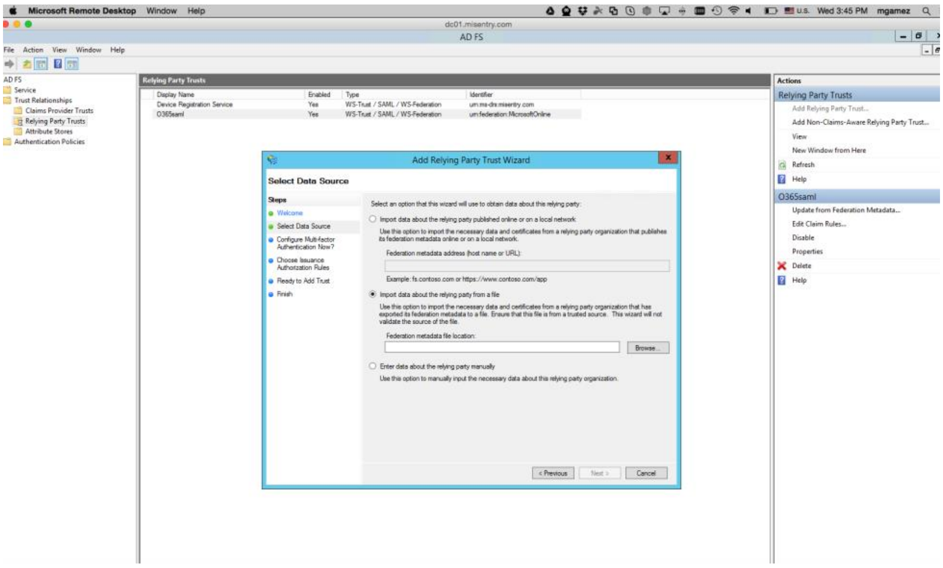
Welcome

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**.



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.

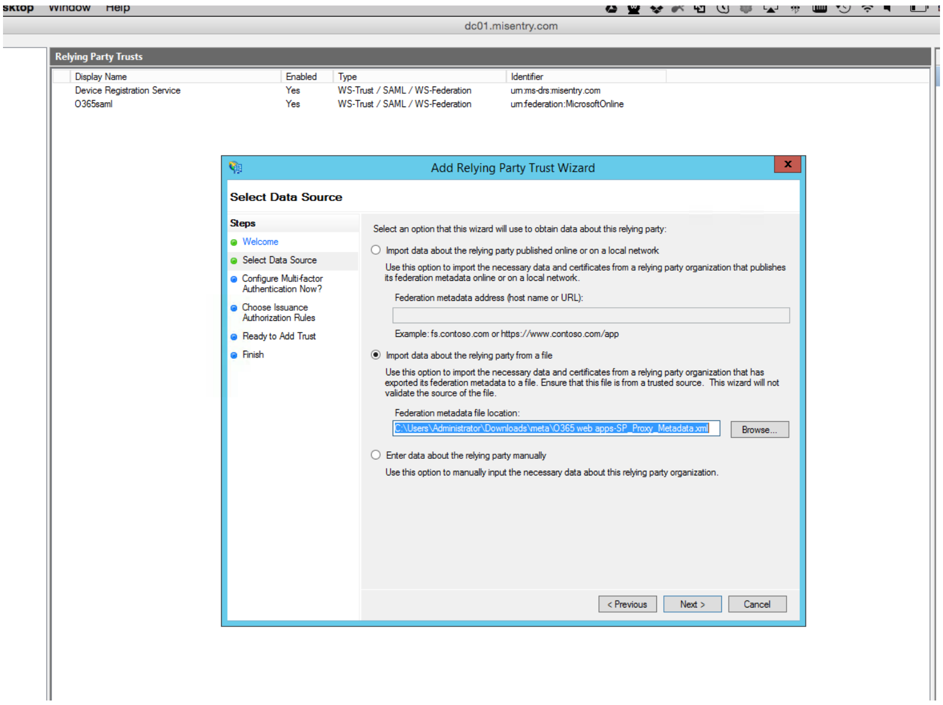
Federation metadata file location:

○ 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*.



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

Add Relying Party Trust Wizard
Select Data Source
Steps
Welcome
Select Data Source
Configure Multi-factor Authentication Now?
Choose Issuance Authorization Rules
Ready to Add Trust
Finish

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. All other fields are set to defaults. Follow the prompts.
8. At the end, select **Open Edit Claim rules dialog for relying party trust**.
9. In the **Claim Rule Template** drop-down, select **Send Claims Using a Custom Rule** and click **Next.**
10. Add **Claim rules** as follows:

    a) **<u>Rule 1:</u>**
    Name: Query AD for ObjectGUID
    Custom Rule Value:
    c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
    => add(store = "Active Directory", types = ("ObjectGuid"), query = ";objectGUID;{0}", param = c.Value);

    b) **<u>Rule 2:</u>**
    Name: Issue ObjectGUID as Name Id claim
    Custom Rule Value:
    c:[Type == "ObjectGuid"]
    => issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] = "urn:oasis:names:tc:SAML:2.0:nameid-format:persistent");

    c) **<u>Rule 3:</u>**
    Name: IDPEmail
    Custom Rule Value:
    c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"]

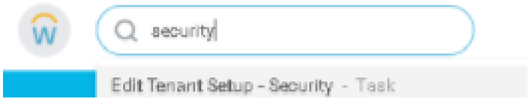
=> issue(Type = "IDPEmail", Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType = c.ValueType);

11. Click **Apply** and **OK.**

Configure the Workday environment

Procedure

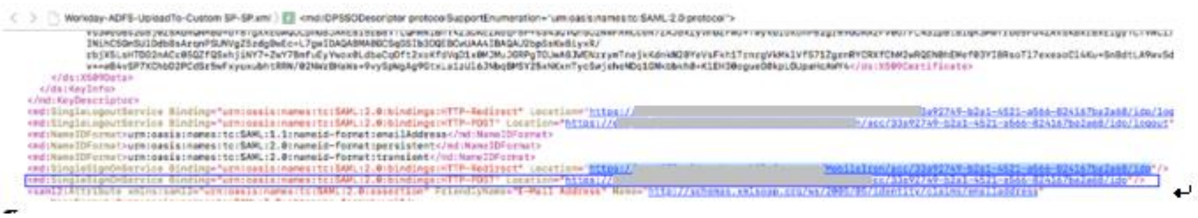
1. Navigate to the Workday tenant security page.



security

Edit Tenant Setup - Security - Task

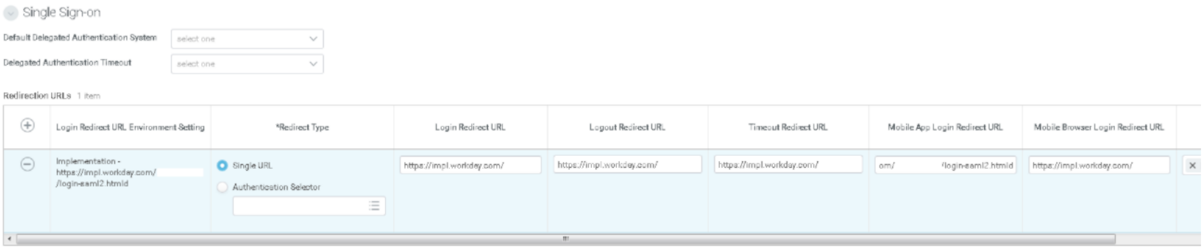
2. Edit the Access IDP metadata file and copy the URL for the value of the attribute *Location* of the XML tag <md:SingleSignOnService>



Workday-ADFS-UploadTo-Custom SP-SP.xml <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

```
        [illegible]
        INiHCS0nSU1Odb8sAronPSUNVgZ5zdg0wEc+L7gwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAJ0bpdSsKeBiLy+R/
        [illegible]
        [illegible]</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[redacted]3a92749-b2a1-4521-a566-82416 7ba2a68/idp/log
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted]/acc/33a92749-b2a1-4521-a566-82416 7ba2a68/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>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[redacted]MobileIron/acc/33a92749-b2a1-4521-a566-82416 7ba2a68/idp"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[redacted]cc/33a92749-b2a1-4521-a566-82416 7ba2a68/idp"/>
  <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"
```

3. Copy the single sign-on URL and paste it in the *Mobile App Login Redirect URL* and *Mobile Browser Login Redirect URL* field in the *Single Sign On* section.



Single Sign-on

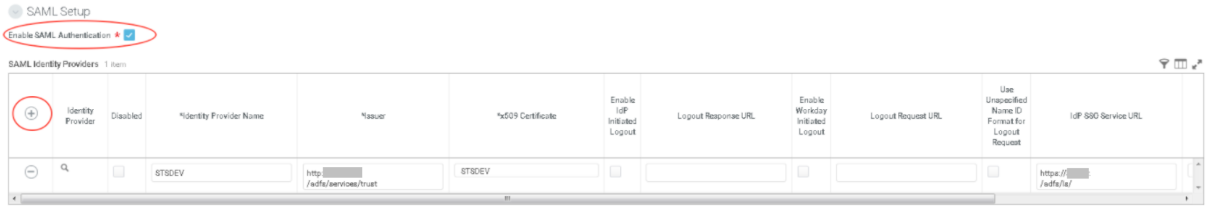
Default Delegated Authentication System: select one

Delegated Authentication Timeout: select one

Redirection URLs 1 item

⊕	Login Redirect URL Environment Setting	*Redirect Type	Login Redirect URL	Logout Redirect URL	Timeout Redirect URL	Mobile App Login Redirect URL	Mobile Browser Login Redirect URL	
⊖	Implementation - https://impl.workday.com/ /login-saml2.htmld	● Single URL ○ Authentication Selector	https://impl.workday.com/	https://impl.workday.com/	https://impl.workday.com/	om/ /login-saml2.htmld	https://impl.workday.com/	×

4. In the SAML Setup section, check *Enable SAML Authentication* and expand the identity providers list in the below table. A new row appears. Enter a name for the new identity provider.



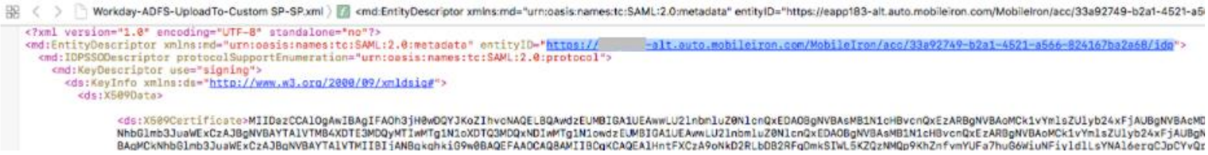
SAML Setup

Enable SAML Authentication * ☑

SAML Identity Providers 1 item

⊕	Identity Provider	Disabled	*Identity Provider Name	*Issuer	*x509 Certificate	Enable IdP Initiated Logout	Logout Response URL	Enable Workday Initiated Logout	Logout Request URL	Use Unspecified Name ID Format for Logout Request	IdP SSO Service URL
⊖	🔍	□	STSDEV	http[redacted] /adfs/services/trust	STSDEV	□		□		□	https://[redacted] /adfs/ls/

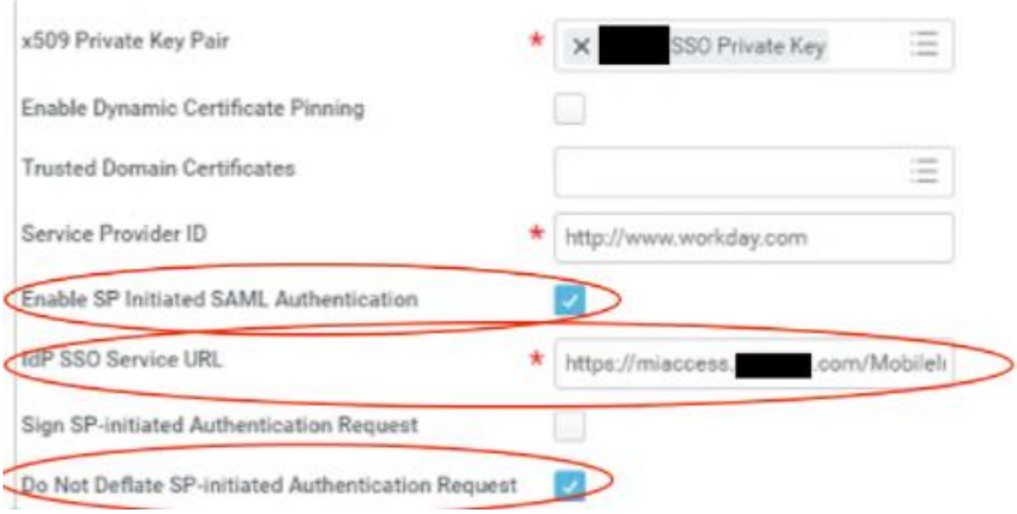
5. Paste the Single Sign-on URL copied in Step 3. Open the Access IdP metadata file again, and copy the entityID from this file.



Workday-ADFS-UploadTo-Custom SP-SP.xml 〉 <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://eapp183-alt.auto.mobileiron.com/MobileIron/acc/33a92749-b2a1-4521-a5

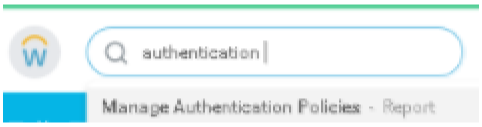
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://[redacted]-alt.auto.mobileiron.com/MobileIron/acc/33a92749-b2a1-4521-a566-824167ba2a68/idp">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>

            <ds:X509Certificate>MIIDazCCAlOgAwIBAgIFAOh3jH0wDQYJKoZIhvcNAQELBQAwdzEUMBIGA1UEAwwLU2lnbmluZ0NlcnQxEDAOBgNVBAsMB1N1cHBvcnQxEzARBgNVBAoMCk1vYmlsZUlyb24xFjAUBgNVBAcMD
            NhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE3MDQyMTIwMTg1N1oXDTQ3MDQxNDIwMTg1N1owdzEUMBIGA1UEAwwLU2lnbmluZ0NlcnQxEDAOBgNVBAsMB1N1cHBvcnQxEzARBgNVBAoMCk1vYmlsZUlyb24xFjAUBgN
            BAgMCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlHntFXCzA9oNkD2RLbDB2RFqDmkSIWL5KZQzNMQp9KhZnfvmYUFa7huG6WiuNFiyldlLsYNAl6erqCJpCYvQr
```

6. Copy the entityID and paste it in the Issuer column of the new row. In the x509 Certificate column of this row, choose the *Access IdP Signing Certificate*.
7. Configure the SAML Parameters:
   - Check *Enable SP Initiated SAML Authentication*.
   - The IdP SSO Service URL is set to the same value as the *IdP SSO Service URL* in the new row of the SAML Identity Providers table.
   - Enable *Do Not Deflate SP-initiated Authentication Request*.



x509 Private Key Pair *	× [redacted] SSO Private Key
Enable Dynamic Certificate Pinning	☐
Trusted Domain Certificates	
Service Provider ID *	http://www.workday.com
Enable SP Initiated SAML Authentication	☑
IdP SSO Service URL *	https://miaccess.[redacted].com/Mobilel
Sign SP-initiated Authentication Request	☐
Do Not Deflate SP-initiated Authentication Request	☑

8. Click OK.
9. Navigate to the Manage Authentication Policy screen.



authentication

Manage Authentication Policies - Report

10. On the Authentication Whitelist table, ensure that the authentication type named SAML: <name as in step 4> is an allowed authentication type.

Verification

From of managed mobile device, launch the Workday application. It must navigate to MobileIron Access upon launch.

- If certificate-based SSO is not enabled, then you are redirected to the original identity provider.
- If certificate-based SSO is enabled, then you are logged into Workday automatically.