Configuring Microsoft ADFS

Table of Contents

Configuring Microsoft ADFS 1

Step 1: Prepare ADFS metadata 1

ADFS MEX Metadata 2

ADFS Active Logon URL 3

Step 2: Configuring Access with ADFS Metadata 4

1. Microsoft ADFS SAML with Salesforce, G Suite and other as service provider. 4

2. ADFS SAML with Office 365 SAML. 5

3. ADFS as WS-Fed with Office 365 WS-Fed service provider. 6

MEX Metadata: Office 365 (WS-Fed) with ADFS 8

Active Logon URL: Office 365 (SAML) or Office 365 (WS-Fed) with ADFS 9

Step 3: Configure ADFS using PowerShell script generated by MobileIron Access if you are federating with Office 365 10

Execute ADFS PowerShell Script 10

Configuring fallback or rollback procedure for Office 365 and Microsoft ADFS. 12

Supported versions: ADFS v3.0, v4.0, v5.0

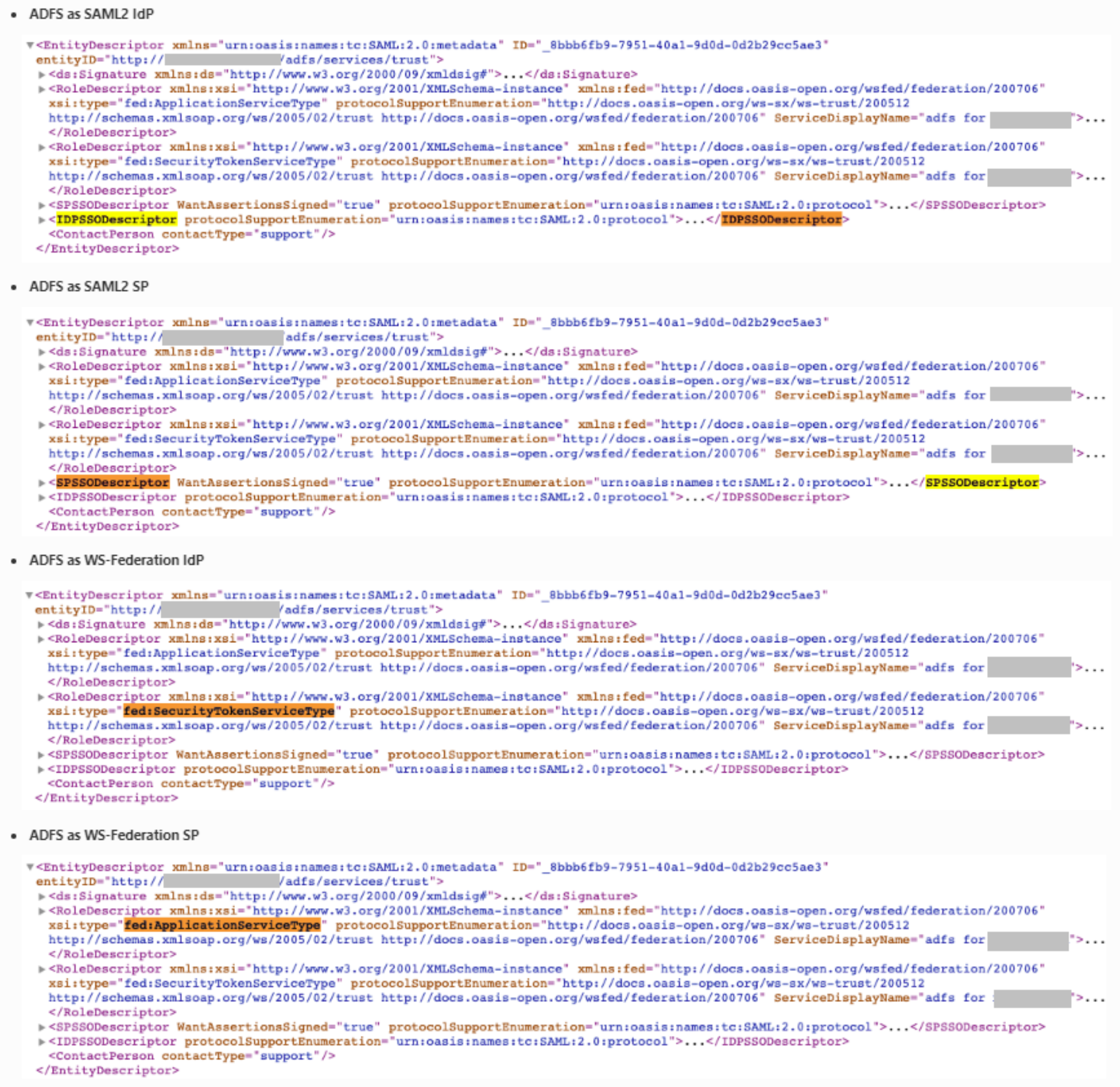
The following steps lets you prepare Microsoft ADFS for creating a federated pair in Access:

- Step 1: Prepare ADFS metadata
- Step 2: Configuring Access with ADFS metadata
- Step 3: Configure ADFS using PowerShell script generated by MobileIron Access.

Step 1: Prepare ADFS metadata

ADFS by default exposes an URL at **https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml** where federation metadata can be accessed.

- You must replace the <FQDN> in the URL with the ADFS hostname. For example: adfs.mi.com
- You can download the metadata file or simply use this URL when configuring Access



- ADFS as SAML2 IdP

```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_8bbb6fb9-7951-40a1-9d0d-0d2b29cc5ae3"
 entityID="http://[redacted]/adfs/services/trust">
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</SPSSODescriptor>
  ▶<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</IDPSSODescriptor>
   <ContactPerson contactType="support"/>
 </EntityDescriptor>
```

- ADFS as SAML2 SP

```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_8bbb6fb9-7951-40a1-9d0d-0d2b29cc5ae3"
 entityID="http://[redacted]adfs/services/trust">
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</SPSSODescriptor>
  ▶<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</IDPSSODescriptor>
   <ContactPerson contactType="support"/>
 </EntityDescriptor>
```

- ADFS as WS-Federation IdP

```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_8bbb6fb9-7951-40a1-9d0d-0d2b29cc5ae3"
 entityID="http://[redacted]/adfs/services/trust">
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</SPSSODescriptor>
  ▶<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</IDPSSODescriptor>
   <ContactPerson contactType="support"/>
 </EntityDescriptor>
```

- ADFS as WS-Federation SP

```
▼<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" ID="_8bbb6fb9-7951-40a1-9d0d-0d2b29cc5ae3"
 entityID="http://[redacted]/adfs/services/trust">
  ▶<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...</ds:Signature>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:ApplicationServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<RoleDescriptor xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:fed="http://docs.oasis-open.org/wsfed/federation/200706"
   xsi:type="fed:SecurityTokenServiceType" protocolSupportEnumeration="http://docs.oasis-open.org/ws-sx/ws-trust/200512
   http://schemas.xmlsoap.org/ws/2005/02/trust http://docs.oasis-open.org/wsfed/federation/200706" ServiceDisplayName="adfs for [redacted]">...
   </RoleDescriptor>
  ▶<SPSSODescriptor WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</SPSSODescriptor>
  ▶<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">...</IDPSSODescriptor>
   <ContactPerson contactType="support"/>
 </EntityDescriptor>
```

Depending on the use-cases of the federation setup, Access uses one or more sections of the metadata. For example:

- When configuring Salesforce (a SAML2 SP) with ADFS, Access will use **ADFS as SAML2 IdP**.
- When configuring Office365 with ADFS using WS-Federation protocol, Access will use **ADFS as WS-Federation IdP**.
- When configuring ADFS in Delegated IdP mode, Access will use **ADFS as WS-Federation SP** and **ADFS as WS-Federation IdP** (to support unmanaged device login).

Because ADFS combines description of all these roles into a single URL or file, you must provide the same URL or file to Access in all use-cases.

ADFS MEX Metadata

ADFS describes all its supported endpoints in an XML document according to the "Web Service Metadata Exchange" protocol. Certain legacy apps and use-cases rely on the MEX endpoint for its functions.

ADFS by default exposes an URL at **https://<FQDN>/adfs/services/trust/mex** where MEX metadata can be accessed. If you are configuring Office 365 and ADFS as a Federated Pair on Access (as opposed to Delegated IdP), and need to support use-cases requiring MEX, then you must provide ADFS MEX URL or metadata file to Access.

NOTE:

- MEX metadata is only for certain use cases between Office 365/Azure AD and ADFS. If your service provider is not Office 365, MEX Metadata is not required.
- If you configure ADFS as Delegated IdP, then MEX Metadata is not required to configure Access (Access is not a full proxy between Azure AD and ADFS).

ADFS Active Logon URL

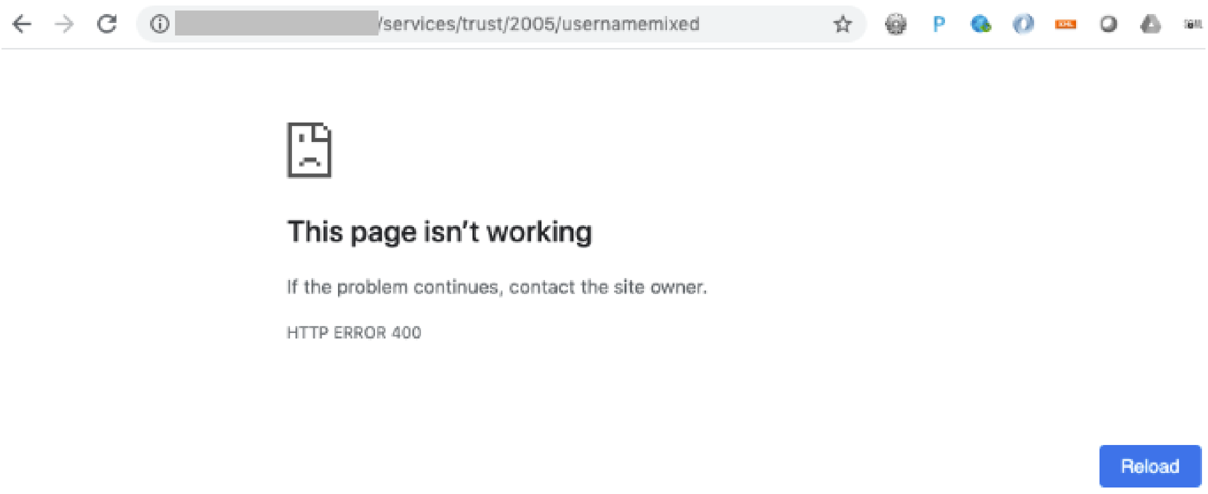
Applications supporting *modern authentication* (Passive Logon) assumes that user may be guided through a series of steps and visit more than one authority. Consequently, the application must support browser-like behaviour during user login process. In fact, such applications commonly leverage an embedded browser, or a separate browser or authenticator application to accomplish such complex interactions.

There are, however, still legacy applications that do not support modern authentication. Typically, these applications acquire users' credential in the application and sends the credentials as BASIC auth header to the backend. "Active Logon" is a message protocol for such interactions. Legacy email applications is a primary example of Active Logon, but other legacy apps, command lines, and background jobs may have similar behaviour.

NOTE: As an administrator, if an application supports both modern authentication and Active Logon, whenever possible, consider configuring the application with modern authentication.

ADFS by default exposes an URL for at **https://<FQDN>/adfs/services/trust/2005/usernamemixed** to support Active Logon. A valid URL must be provided to Access if you need to support Active Logon.

NOTE: Verify that this endpoint returns HTTP Error 400 (Bad Request) as we have not provided the correct payload. However, ensure that it does not return HTTP Error 404 (Not Found).



[redacted]/services/trust/2005/usernamemixed

This page isn't working

If the problem continues, contact the site owner.

HTTP ERROR 400

Step 2: Configuring Access with ADFS Metadata

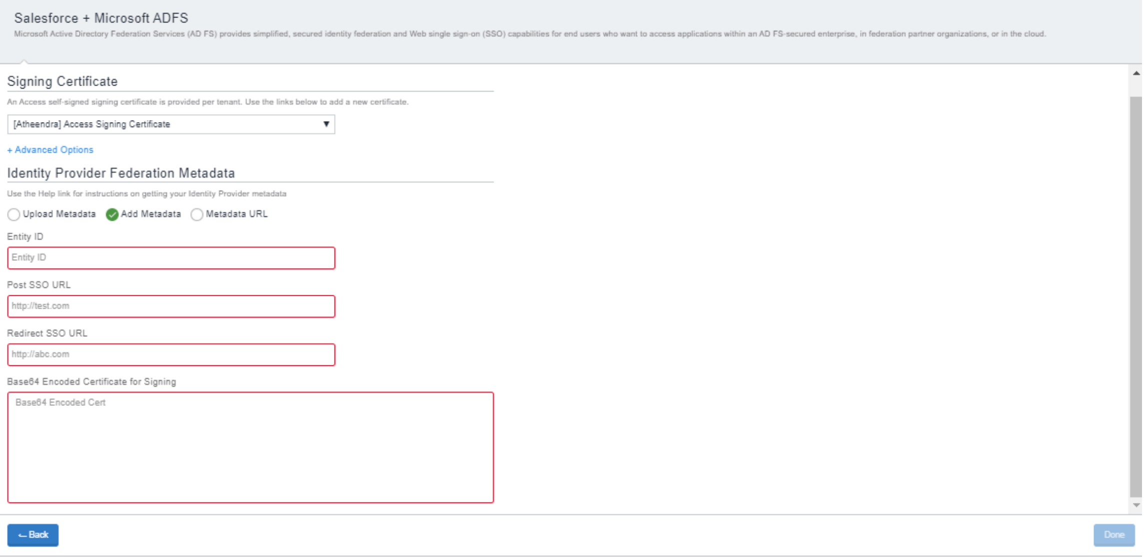
To configure a federated pair, follow the description in "**Creating Federated Pair in Access**" in **Overview**.
Microsoft ADFS metadata can be updated in the following ways for various service providers:

1. Microsoft ADFS SAML with Salesforce, G Suite and other as service provider.

Enter the following details for ADFS when configuring in Access:

- **Signing certificate**: Select the signing certificate from the drop-down list.
- **Identity Provider Federation Metadata**: Select **"Metadata URL"** and provide the https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml URL. Alternatively, you can also download the metadata file and upload by selecting **“Add Metadata” or "Upload Metadata"**

Add Metadata



Salesforce + Microsoft ADFS

Microsoft Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud.

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

Identity Provider Federation Metadata

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

○ Upload Metadata ● Add Metadata ○ Metadata URL

Entity ID: Entity ID

Post SSO URL: http://test.com

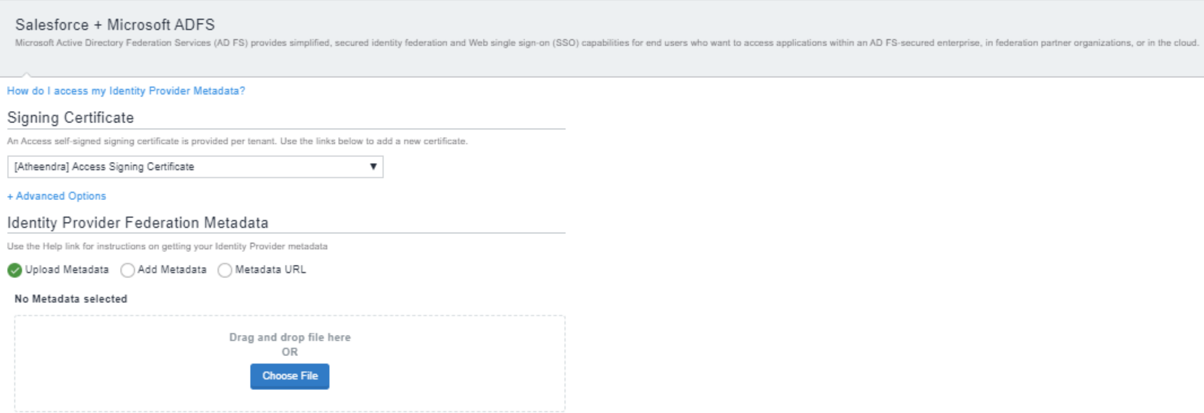
Redirect SSO URL: http://abc.com

Base64 Encoded Certificate for Signing: Base64 Encoded Cert

Download the metadata xml using https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml. Open the xml file and enter the following details:

- Enter the Entity ID, Post SSO URL, and Redirect SSO URL – All the URLs are the same – entity ID.
- Enter the “Base 64 Encoded Certificate for Signing” – Copy the content between the <X509Certificate> tag.

Upload Metadata



Salesforce + Microsoft ADFS

Microsoft Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud.

How do I access my Identity 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

Identity Provider Federation Metadata

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

● Upload Metadata ○ Add Metadata ○ Metadata URL

No Metadata selected

Drag and drop file here
OR

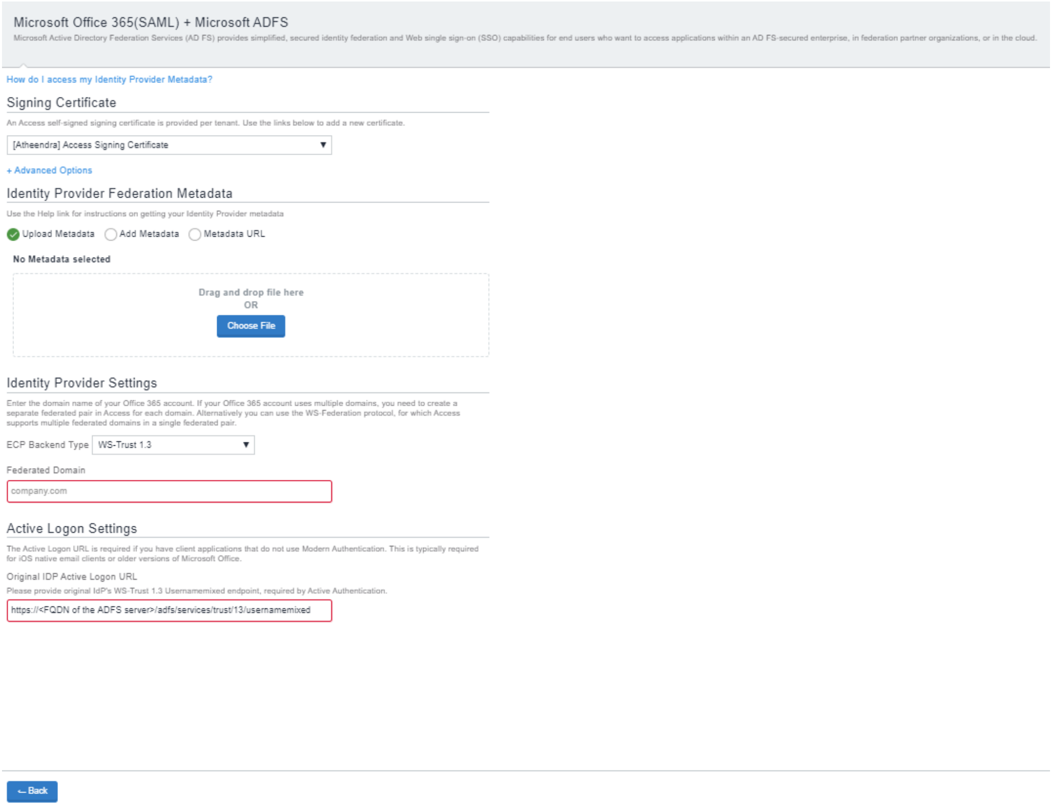
2. ADFS SAML with Office 365 SAML.

Enter the following details for ADFS when configuring in Access:

- **Signing certificate**: Select the signing certificate from the drop-down list.
- **Identity Provider Federation Metadata**: Select **"Metadata URL"** and provide the https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml URL. Alternatively, you can also download the metadata file and upload by selecting "**Upload Metadata**" or “**Add Metadata**”.

- **Identity provider settings with Upload Metadata**
    - Select the **ECP Backend Type** from the drop-down: WS-Trust 1.3, WS_Trust 2005, or SAML 2.0.

      Enter the domain name of Office 365 account in **Federated Domain**.



Microsoft Office 365(SAML) + Microsoft ADFS

Microsoft Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud.

How do I access my Identity 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

Identity Provider Federation Metadata

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

● Upload Metadata ○ Add Metadata ○ Metadata URL

No Metadata selected

Drag and drop file here
OR
Choose File

Identity Provider Settings

Enter the domain name of your Office 365 account. If your Office 365 account uses multiple domains, you need to create a separate federated pair in Access for each domain. Alternatively you can use the WS-Federation protocol, for which Access supports multiple federated domains in a single federated pair.

ECP Backend Type: WS-Trust 1.3 ▼

Federated Domain: company.com

Active Logon Settings

The Active Logon URL is required if you have client applications that do not use Modern Authentication. This is typically required for iOS native email clients or older versions of Microsoft Office.

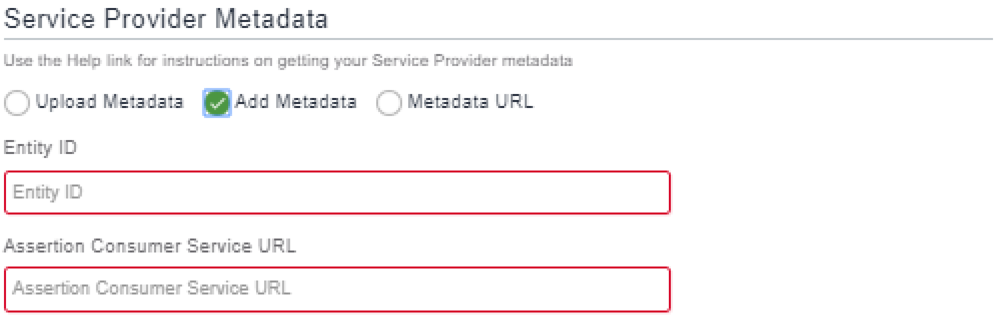
Original IDP Active Logon URL

Please provide original IdP's WS-Trust 1.3 Usernamemixed endpoint, required by Active Authentication.

https://<FQDN of the ADFS server>/adfs/services/trust/13/usernamemixed

← Back

- **Identity Provider Settings with Add Metadata**



Service Provider Metadata

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

○ Upload Metadata ● Add Metadata ○ Metadata URL

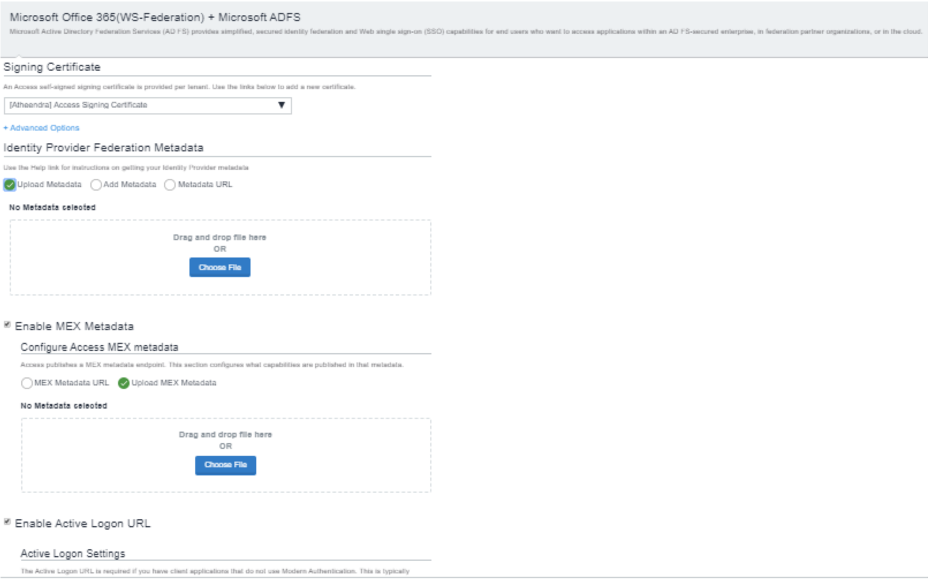
Entity ID: Entity ID

Assertion Consumer Service URL: Assertion Consumer Service URL

Open the xml file and copy the Entity ID and Assertion Consumer URL which remain the same.

3. ADFS as WS-Fed with Office 365 WS-Fed service provider.

Enter the following details for ADFS when configuring in Access:



Microsoft Office 365(WS-Federation) + Microsoft ADFS

Microsoft Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities for end users who want to access applications within an AD FS-secured enterprise, in federation partner organizations, or in the cloud.

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

Identity Provider Federation Metadata

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

● Upload Metadata ○ Add Metadata ○ Metadata URL

No Metadata selected

Drag and drop file here
OR
Choose File

☑ Enable MEX Metadata

Configure Access MEX metadata

Access publishes a MEX metadata endpoint. This section configures what capabilities are published in that metadata.

○ MEX Metadata URL ● Upload MEX Metadata

No Metadata selected

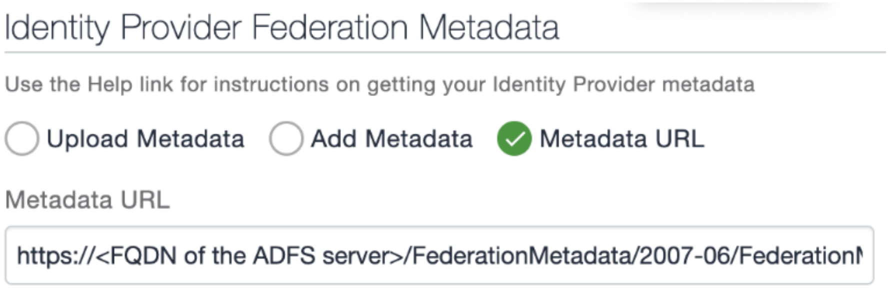
Drag and drop file here
OR
Choose File

☑ Enable Active Logon URL

Active Logon Settings

The Active Logon URL is required if you have client applications that do not use Modern Authentication. This is typically

- **Signing certificate**: Select the signing certificate from the drop-down list.
- **Identity Provider Federation Metadata**: Select **"Metadata URL"** and provide the **https://<FQDN>/FederationMetadata/2007-06/FederationMetadata.xml** URL. Alternatively, you can also download the metadata file and upload by selecting "**Upload Metadata**". Using metadata URL is preferred, allowing Access to monitor any changes to the metadata over time (for example, signing certificate expiration).



Identity Provider Federation Metadata

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

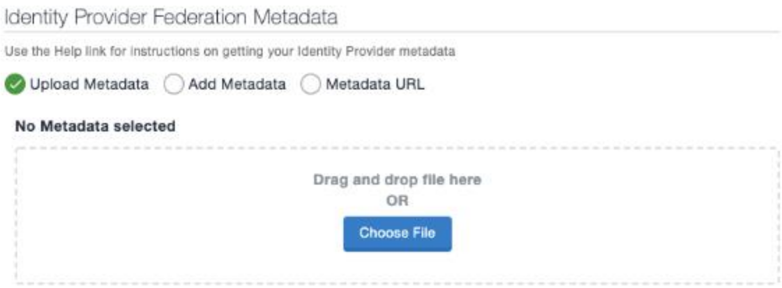
○ Upload Metadata ○ Add Metadata ● Metadata URL

Metadata URL

https://<FQDN of the ADFS server>/FederationMetadata/2007-06/FederationM

OR

Upload Metadata



Identity Provider Federation Metadata

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

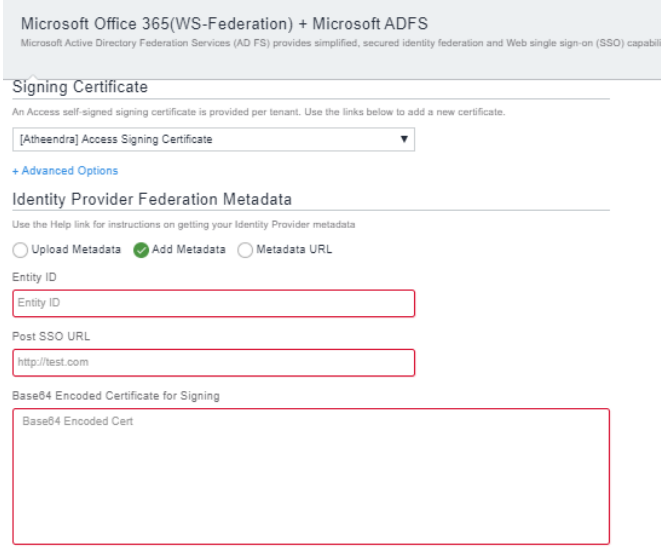
● Upload Metadata ○ Add Metadata ○ Metadata URL

No Metadata selected

Drag and drop file here
OR
Choose File

OR

Add Metadata



Microsoft Office 365(WS-Federation) + Microsoft ADFS

Microsoft Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabili

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

Identity Provider Federation Metadata

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

○ Upload Metadata ● Add Metadata ○ Metadata URL

Entity ID: Entity ID

Post SSO URL: http://test.com

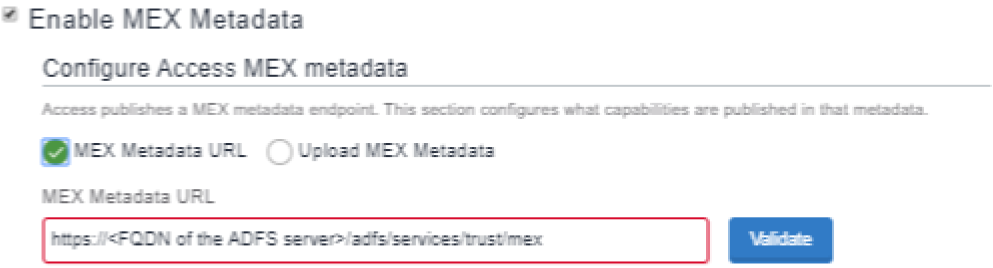
Base64 Encoded Certificate for Signing: Base64 Encoded Cert

Open the xml file and enter the Entity ID, Post SSO URL which remains the same as entity ID. For the “Base64 Encoded Certificate for Signing” , enter the content in the tag <X509Certificate>.

- Click **Done**.

MEX Metadata: Office 365 (WS-Fed) with ADFS

If you are federating **Office 365 using WS-Federation with Microsoft ADFS**, then you have the option to "**Enable MEX Metadata**". Enter the MEX metadata URL **https://<FQDN>/adfs/services/trust/mex** and click **Validate**. It validates and displays the endpoints present in the metadata.



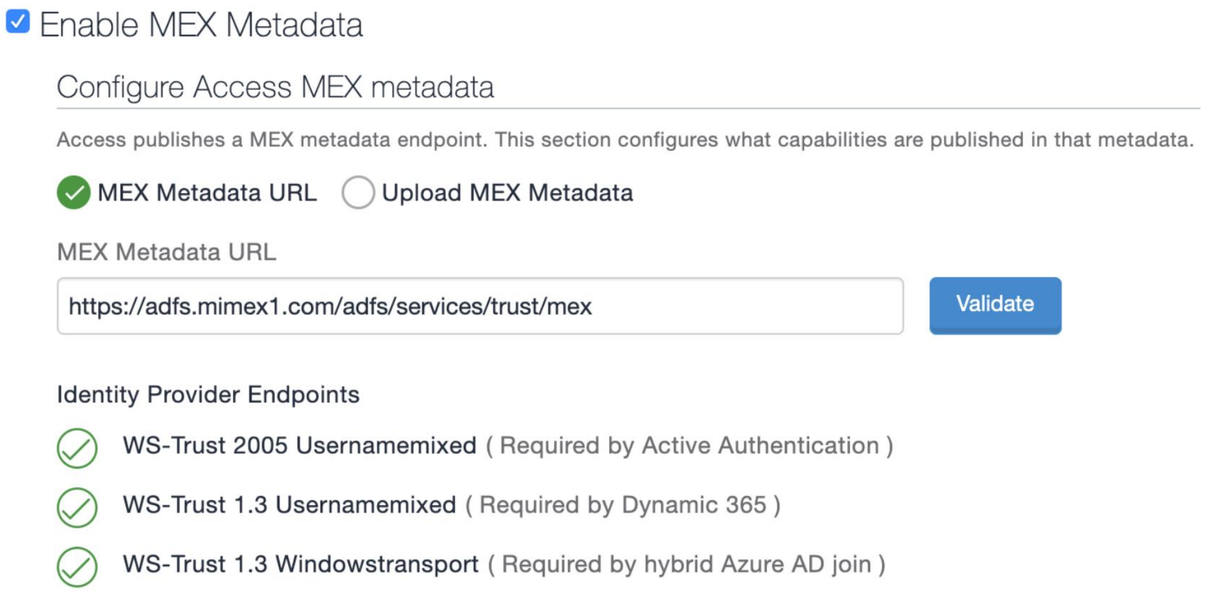
☑ Enable MEX Metadata

Configure Access MEX metadata

Access publishes a MEX metadata endpoint. This section configures what capabilities are published in that metadata.

● MEX Metadata URL ○ Upload MEX Metadata

MEX Metadata URL: https://<FQDN of the ADFS server>/adfs/services/trust/mex



☑ Enable MEX Metadata

Configure Access MEX metadata

Access publishes a MEX metadata endpoint. This section configures what capabilities are published in that metadata.

● MEX Metadata URL ○ Upload MEX Metadata

MEX Metadata URL

https://adfs.mimex1.com/adfs/services/trust/mex

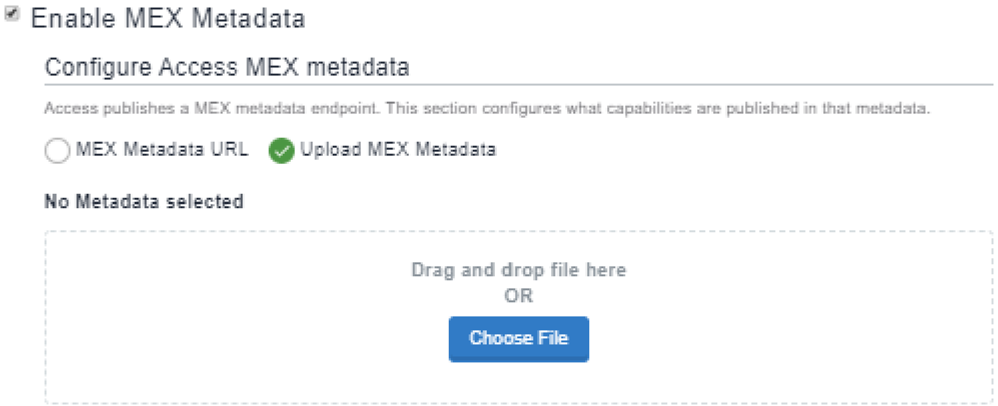
Identity Provider Endpoints

✓ WS-Trust 2005 Usernamemixed (Required by Active Authentication)

✓ WS-Trust 1.3 Usernamemixed (Required by Dynamic 365)

✓ WS-Trust 1.3 Windowstransport (Required by hybrid Azure AD join)

Alternatively, you can also upload the MEX metadata by selecting "**Uploading MEX Metadata**".



☑ Enable MEX Metadata

Configure Access MEX metadata

Access publishes a MEX metadata endpoint. This section configures what capabilities are published in that metadata.

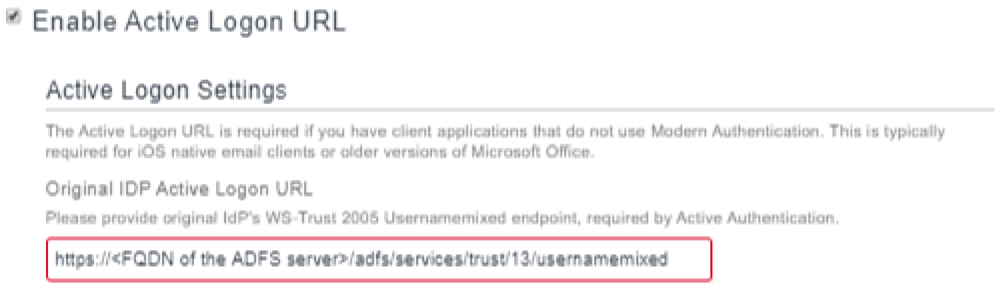
○ MEX Metadata URL ● Upload MEX Metadata

No Metadata selected

Note: Windows Transport feature is only supported in Legacy tenants with Sentry.
For more information, see TBD.

Active Logon URL: Office 365 (SAML) or Office 365 (WS-Fed) with ADFS

If you are federating **Office 365 (SAML) or Office 365 (WS-Fed) with Microsoft ADFS**, then you have the option to "Enable Active Logon URL" **https://<FQDN>/adfs/services/trust/2005/usernamemixed** .



☑ Enable Active Logon URL

Active Logon Settings

The Active Logon URL is required if you have client applications that do not use Modern Authentication. This is typically required for iOS native email clients or older versions of Microsoft Office.

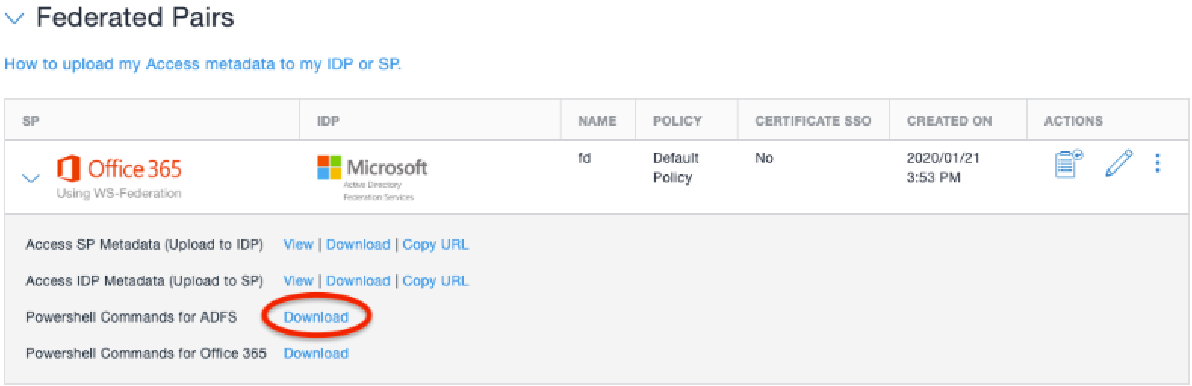
Original IDP Active Logon URL

Please provide original IdP's WS-Trust 2005 Usernamemixed endpoint, required by Active Authentication.

https://<FQDN of the ADFS server>/adfs/services/trust/13/usernamemixed

Step 3: Configure ADFS using PowerShell script generated by MobileIron Access if you are federating with Office 365

After the federated pair is created, you must configure ADFS with Access metadata. Access automates this process by providing a PowerShell script that displays in the Federation page. The administrator can download and run the script on the ADFS machine as an administrator. From your ADFS Management Console, you should also find the corresponding "Relying Party".



Federated Pairs

How to upload my Access metadata to my IDP or SP.

SP	IDP	NAME	POLICY	CERTIFICATE SSO	CREATED ON	ACTIONS
Office 365 Using WS-Federation	Microsoft Active Directory Federation Services	fd	Default Policy	No	2020/01/21 3:53 PM	

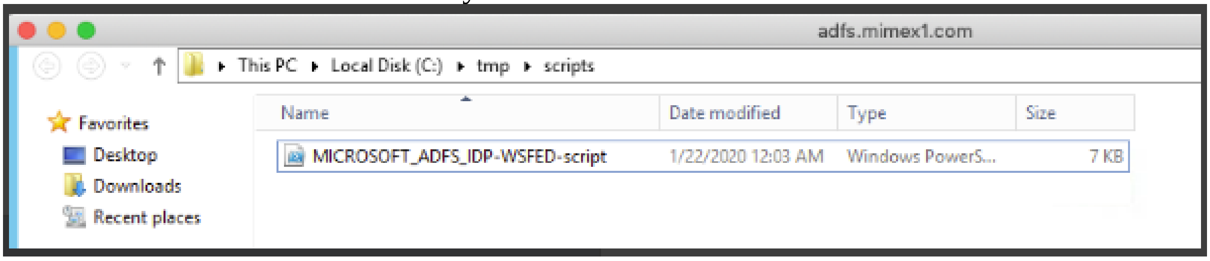
Access SP Metadata (Upload to IDP) View | Download | Copy URL

Access IDP Metadata (Upload to SP) View | Download | Copy URL

Powershell Commands for ADFS Download

Powershell Commands for Office 365 Download

This file must be downloaded locally to the ADFS machine.



adfs.mimex1.com

This PC ▸ Local Disk (C:) ▸ tmp ▸ scripts

Name	Date modified	Type	Size
MICROSOFT_ADFS_IDP-WSFED-script	1/22/2020 12:03 AM	Windows PowerS...	7 KB

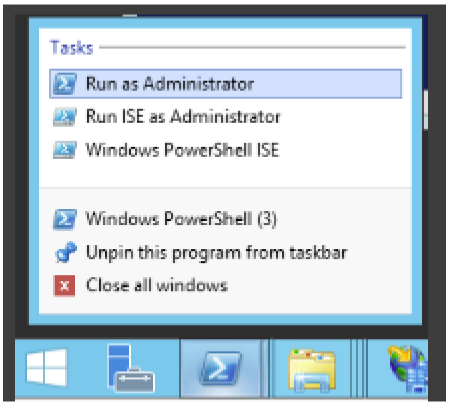
If you are not using Office 365 to federate, you must upload the proxy metadata for ADFS listed in the Federation page to the appropriate service provider.

Execute ADFS PowerShell Script

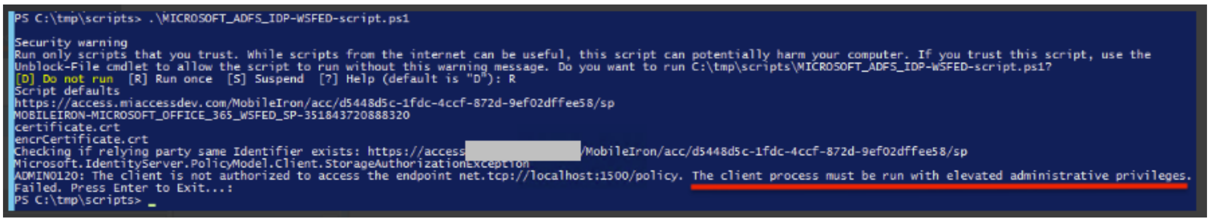
The script requires elevated privilege and must be run as an admin.

Procedure

1. Run Windows PowerShell **as Administrator.**



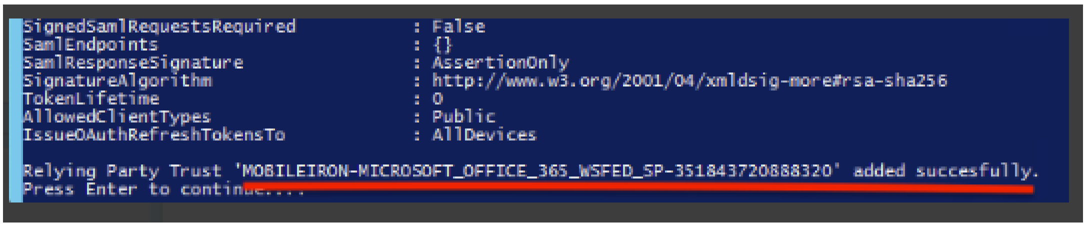
2. If you do not execute the PowerShell as Administrator, the following error displays:



```
PS C:\tmp\scripts> .\MICROSOFT_ADFS_IDP-WSFED-script.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your computer. If you trust this script, use the
Unblock-File cmdlet to allow the script to run without this warning message. Do you want to run C:\tmp\scripts\MICROSOFT_ADFS_IDP-WSFED-script.ps1?
[D] Do not run  [R] Run once  [S] Suspend  [?] Help (default is "D"): R
Script defaults
https://access.miaccessdev.com/MobileIron/acc/d5448d5c-1fdc-4ccf-872d-9ef02dffee58/sp
MOBILEIRON-MICROSOFT_OFFICE_365_WSFED_SP-351843720888320
certificate.crt
encrCertificate.crt
Checking if relying party same Identifier exists: https://access[redacted]/MobileIron/acc/d5448d5c-1fdc-4ccf-872d-9ef02dffee58/sp
Microsoft.IdentityServer.PolicyModel.Client.StorageAuthorizationException
ADMIN0120: The client is not authorized to access the endpoint net.tcp://localhost:1500/policy. The client process must be run with elevated administrative privileges.
Failed. Press Enter to Exit...:
PS C:\tmp\scripts> _
```

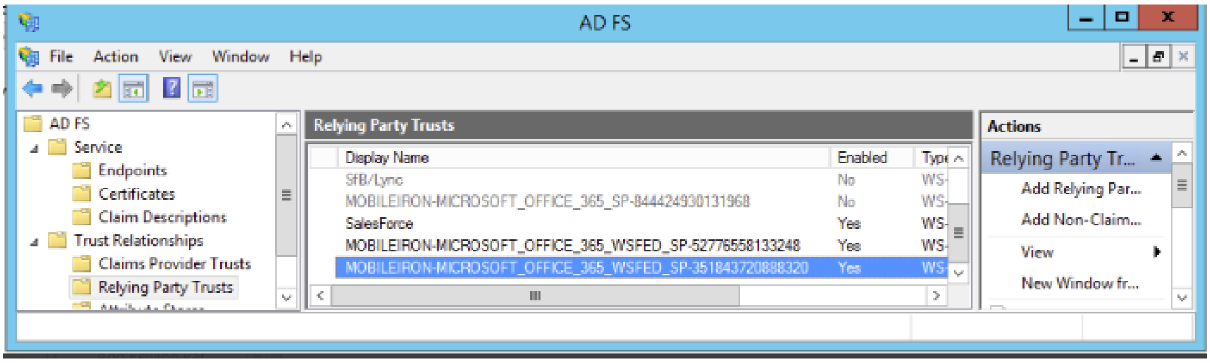
3. If the script is executed successfully, you will see a confirmation similar to the following:



```
SignedSamlRequestsRequired                 : False
SamlEndpoints                              : {}
SamlResponseSignature                      : AssertionOnly
SignatureAlgorithm                         : http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
TokenLifetime                              : 0
AllowedClientTypes                         : Public
IssueOAuthRefreshTokensTo                  : AllDevices

Relying Party Trust 'MOBILEIRON-MICROSOFT_OFFICE_365_WSFED_SP-351843720888320' added succesfully.
Press Enter to continue....
```

4. From your ADFS Management Console, you should also find the corresponding "Relying Party".



Relying Party Trusts

Display Name	Enabled	Type
SfB/Lync	No	WS-
MOBILEIRON-MICROSOFT_OFFICE_365_SP-844424930131968	No	WS-
SalesForce	Yes	WS-
MOBILEIRON-MICROSOFT_OFFICE_365_WSFED_SP-52776558133248	Yes	WS-
MOBILEIRON-MICROSOFT_OFFICE_365_WSFED_SP-351843720888320	Yes	WS-

Configuring fallback or rollback procedure for Office 365 and Microsoft ADFS

The fallback or rollback feature lets an administrator revert the federation setup to Microsoft ADFS if there are any outages.

1. Run the following command in PowerShell to log into Office 365.
   PS C:\> Connect-MsolService
2. Enter the Office 365 tenant admin username and password.
3. Set the MSOL ADFS context server to ADFS server.
   PS C:\>Set-MsolADFSContext -Computer <FQDN of the ADFS server>.
4. Enter the ADFS server admin username and password.
5. Unfederate the domain.
   PS C:\>Set-MsolDomainAuthentication -DomainName <domain name> -Authentication Managed
6. Convert the domain to a federated domain.
   PS C:\> Convert-MsolDomainToFederated –DomainName <domain name>
7. Verify that "*Successfully updated <domain name>*" is displayed.
8. Verify Federation.

   PS C:\> Get-MsolFederationProperty –DomainName <domain name>

   For Example: PS C:\> Get-MsolFederationProperty –DomainName abcd.com