Configuring Office365

Contents

Prerequisites

- Ensure that you have the Office 365 subscription.

Complete the following steps to configure Office 365:

- Download metadata for Office 365
- Create a federated pair in MobileIron Access
- Executing PowerShell scripts to configure Office 365

Download metadata for Office 365

- Office 365 (Azure) SAML 2.0 Metadata URL

https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

- Office365(Azure) WS-Federation

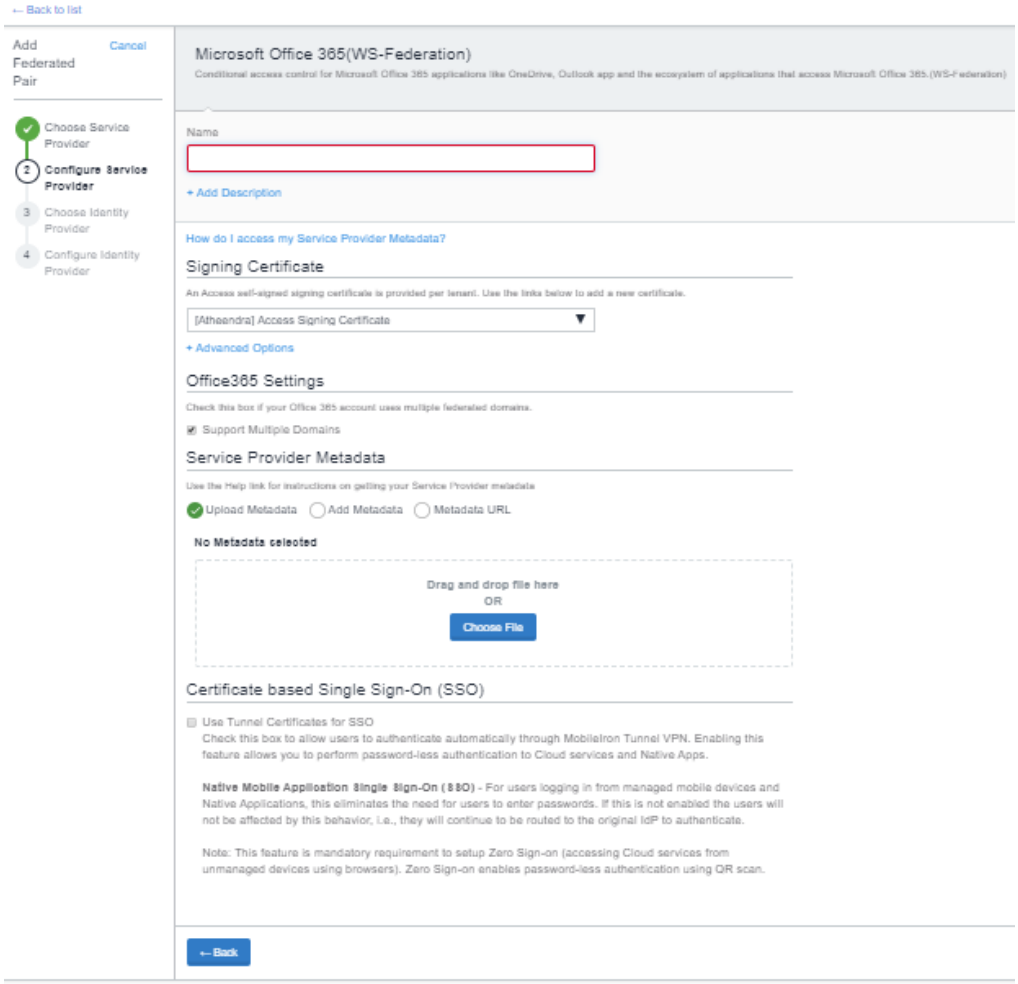
https://nexus.microsoftonline-p.com/federationmetadata/2007-06/federationmetadata.xml

Create a federated pair in MobileIron Access

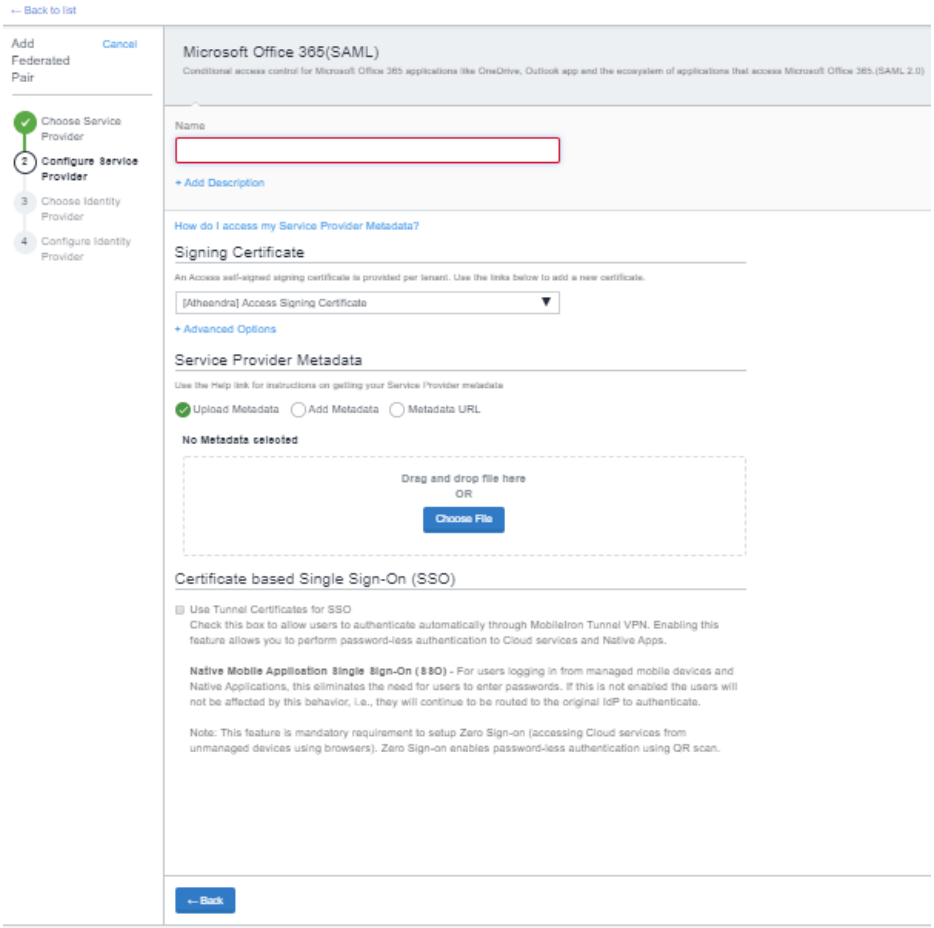
You must configure a federated pair in MobileIron Access with Office 365 WS-Federation (recommended) or SAML 2.0 as the service provider.

1. Login to the MobileIron Access administrator portal.
2. Click **Profile** > **Federation** > **Add Pair > Federated Pair.**
3. Select **Office 365 WS-Federation (Recommended) or SAML 2.0** as the service provider.

   Office 365 (WS-Federation)


← Back to list
Add Federated Pair
Cancel
Choose Service Provider
2 Configure Service Provider
3 Choose Identity Provider
4 Configure Identity Provider
Microsoft Office 365(WS-Federation)
Conditional access control for Microsoft Office 365 applications like OneDrive, Outlook app and the ecosystem of applications that access Microsoft Office 365.(WS-Federation)
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
Office365 Settings
Check this box if your Office 365 account uses multiple federated domains.
Support Multiple Domains
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
Certificate based Single Sign-On (SSO)
Use Tunnel Certificates for SSO
Check this box to allow users to authenticate automatically through MobileIron Tunnel VPN. Enabling this feature allows you to perform password-less authentication to Cloud services and Native Apps.
Native Mobile Application Single Sign-On (SSO) - For users logging in from managed mobile devices and Native Applications, this eliminates the need for users to enter passwords. If this is not enabled the users will not be affected by this behavior, i.e., they will continue to be routed to the original IdP to authenticate.
Note: This feature is mandatory requirement to setup Zero Sign-on (accessing Cloud services from unmanaged devices using browsers). Zero Sign-on enables password-less authentication using QR scan.
← Back

Office 365 (SAML)



- 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.
- In Office 365 specifics (WS Federation): Select the checkbox "*Support Multiple Domains*" if your account uses multiple federated domains.
- **Add** or **Upload Metadata** downloaded in the prerequisites section or enter the **Metadata URL**.
  To Add Metadata: Download the metadata file and extract the Entity ID and the Assertion Consumer Service URL from the file.
- (Optional): Select "*Use Tunnel Certificates for SSO*" in the **Certificate based Single Sign-on**.

4. Click **Next** and select the identity provider. Enter the details for the identity provider.
   For more information, see Access Cookbooks to set up the appropriate identity provider.
5. Click **Done**.
6. On the Federation page, download the PowerShell scripts and run on the appropriate identity provider set up.

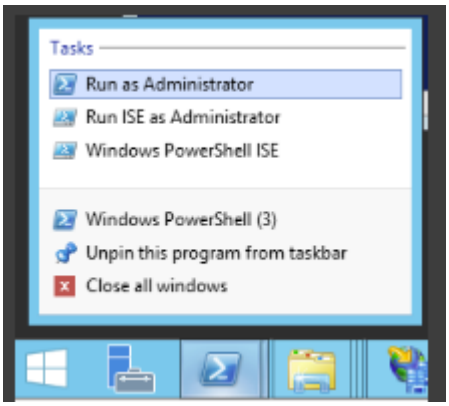
7. Click **Publish** to publish the profile.

Executing PowerShell scripts to configure Office 365

Office 365 does not let you upload a metadata file. The information must be extracted from the IDP Proxy metadata file. Extract the Entity ID from the IDP Proxy metadata file.

Procedure

1. Configure Office 365 and the identity provider.
   See, Create a federated pair in MobileIron Access.
2. Download the PowerShell scripts on the Federation page.
3. Run the PowerShell script in a Windows server as an Administrator.



Note: The scripts can also by run using the following command:
./MICROSOFT_OFFICE_365_SP-WSFED-script.ps1 -domain misentry.com

4. Verify the new settings.
   # Get-MsolDomainFederationSettings -DomainName

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