



# MobileIron Access Cookbook

## Access with Office 365 and Microsoft ADFS

**Revised: 07 Febuary 2018**



## Contents

Overview.....	3
Prerequisites.....	3
Configuring Office 365 and Microsoft ADFS with MobileIron Access .....	4
Register Sentry to Access .....	4
Configure Access to create a Federated Pair .....	5
Configure the ADFS environment .....	6
Configure the Office 365 environment .....	8



# Overview

SAML provides single sign-on capability for users accessing their services hosted in a cloud environment. Generally, a service provider such as Office 365 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 Office 365. This guide serves as step-by-step configuration manual for users using ADFS as an authentication provider with Office 365 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
- Office 365 subscription
- Existing working direct federation between ADFS and Office 365
- **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>

- **Office 365 Metadata Files**

You must download the metadata files for Office 365 (SP)

- Download Office 365 metadata file from <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>



# Configuring Office 365 and Microsoft ADFS with MobileIron Access

You must perform the following tasks to accomplish the configuration between Office 365 and ADFS:

- [Register Sentry to Access](#)
- [Configure Access to create a Federated Pair](#)
- [Configure the ADFS](#)
- [Configure the Office 365](#)

## [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**

Single-sign-on service is now configured using SAML with Office 365 as the service provider and Microsoft ADFS as the identity provider. 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 **Office 365** 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.
  - In Office 365 specifics, select one of the following Office 365 Domain Federation:

Protocol	Settings
WS-Fed	The WS-Fed protocol allows only Microsoft ADFS as an IdP selection. This is the default option. <ol style="list-style-type: none"><li>1. Enter the Original IDP Active Logon Url. For example: <a href="https://[ADFS server domain]/adfs/services/trust/13/usernamemixed">https://[ADFS server domain]/adfs/services/trust/13/usernamemixed</a>.</li></ol>
SAML	<ol style="list-style-type: none"><li>1. Select the appropriate ECP Backend Type from the drop-down. This option lets Access connect to the IdP.</li><li>2. Enter the value for Federated Domain for Office 365. For example, &lt;domain_name&gt;.com.</li><li>3. Enter the ADFS Active Logon URL for Original IDP Active Logon URL. For example: <a href="https://[ADFS server domain]/adfs/services/trust/13/usernamemixed">https://[ADFS server domain]/adfs/services/trust/13/usernamemixed</a></li></ol>

- Upload the metadata file of the service provider downloaded in **Office 365 Metadata Files** section.
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.
  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.

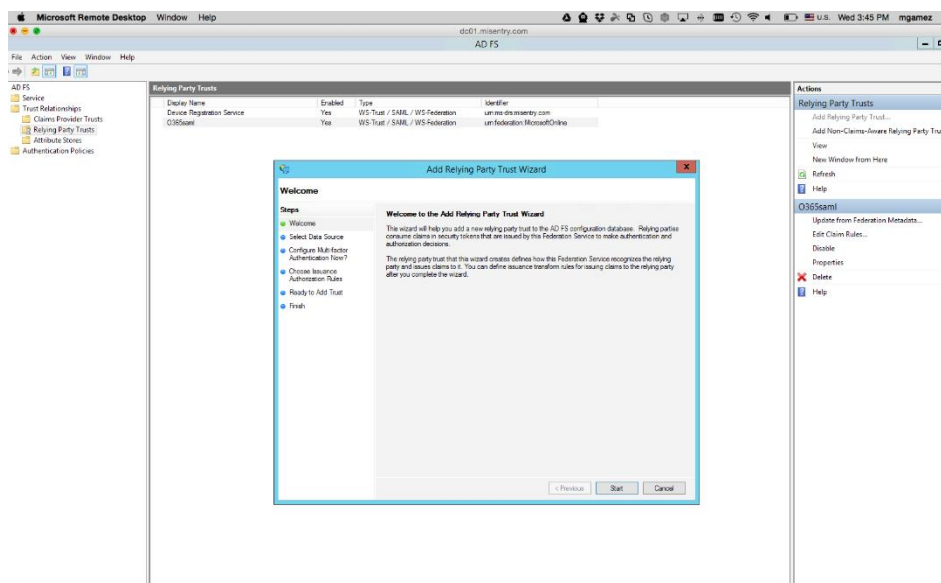


## Configure the ADFS environment

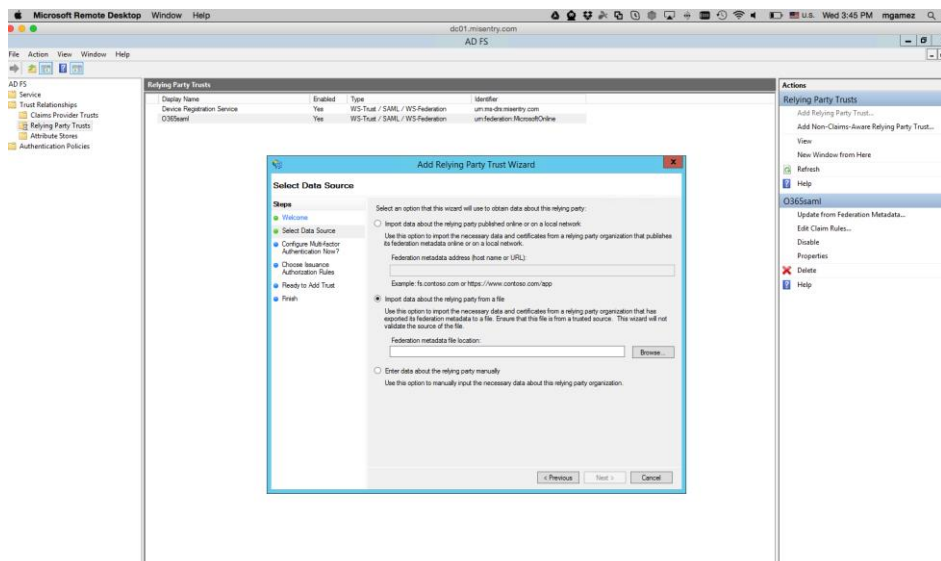
You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

### 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.



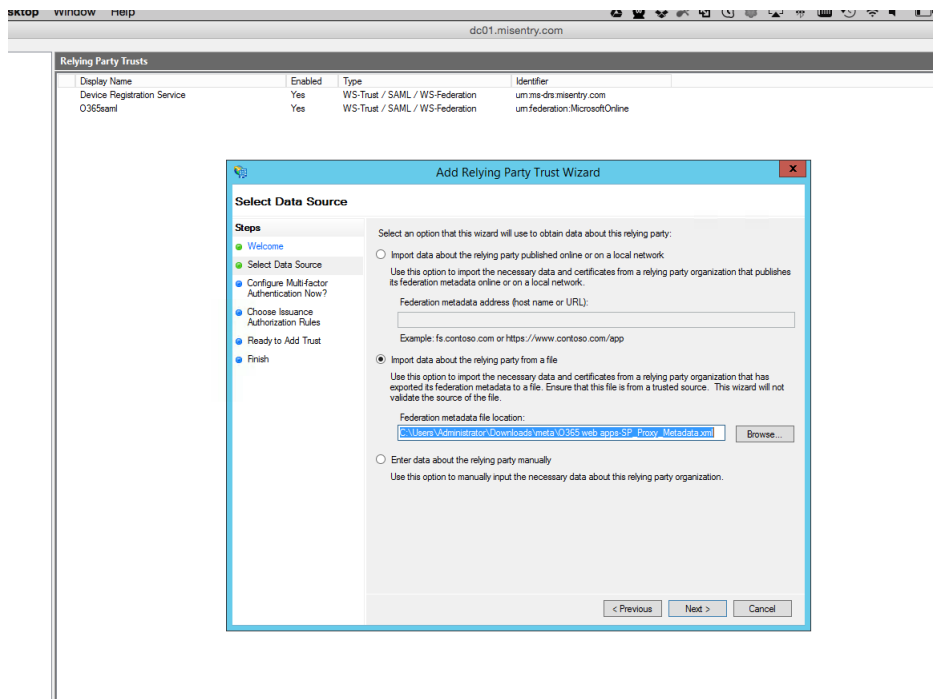
4. Click **Start** and select **Import data about the relying party from a file**. Click **Next**.



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*.



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) **Rule 1:**

*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) **Rule 2:**

*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) **Rule 3:**

*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 Office 365 environment](#)

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. Use Remote Desktop Services to log in to an ADFS machine with admin credentials.
2. In the PowerShell command window, connect to the Office 365 Tenant:  
*Connect-MsolService*

3. Download the PowerShell script from MobileIron Access for Office 365 and Microsoft ADFS federated pair to avoid manual editing.

**Note:** Run the PowerShell script in a Windows server as an Administrator.

Name	Description	Policy Name	SP Metadata	Access SP Metadata (Upload to IDP)	IDP Metadata	Access IDP Metadata (Upload to SP)	PowerShell Commands for Office 365
O365+ADFS	No description	Policy Name: Default Policy	View	View   Download	View	View   Download	View   Download

OR

4. Execute the following commands /steps in PowerShell. Edit the settings for ActiveLogOnUri, IssuerUri, LogOffUri, and PassiveLogonUri before executing the commands.
  - *PSC:\>\$saml = New-Object -TypeName PSObject*
  - *PSC:\>\$saml | Add-Member -MemberType NoteProperty -Name ActiveLogOnUri -Value \$saml.ActiveLogOnUri*





- `PSC:\>$saml.ActiveLogOnUri=https://<domain_name>/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp/active`
- `PSC:\>$saml | Add-Member -MemberType NoteProperty -Name IssuerUri -Value $saml.IssuerUri`
- `PSC:\>$saml.IssuerUri=https://<domain_name>/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp`
- `PSC:\>$saml | Add-Member -MemberType NoteProperty -Name LogOffUri -Value $saml.LogOffUri`
- `PSC:\>$saml.LogOffUri=https://<domain_name>/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp/logout`
- `PSC:\>$saml | Add-Member -MemberType NoteProperty -Name PassiveLogOnUri -Value $saml.PassiveLogOnUri`
- `PSC:\>$saml.PassiveLogOnUri=https://<domain_name>/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp`

**Note:** You can extract the above information from Access IDP metadata file. For example,

```
<?xml version="1.0" encoding="UTF-8"?>
- <EntityDescriptor entityID="https://<domain_name>/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp" ID="e0/ldp" ID="*_17cfa48-886a-4a8d-85d2-939d38118327" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" >
- <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
```

5. Extract the certificate from the IDP Proxy metadata file and save it in the .cer file.

```
</KeyDescriptor>
- <KeyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#" >
- <ds:X509Data >
- <ds:X509Certificate>MIIDZDCCAkwwCQCZVG/BcwYwIjANBgkqhkiG9w0BAQsFADBOMQswCQYDVQOCEwJVUzEIMBECA1UE
bG9QMAAQA1UECwwwHU3YwC69yDERMA8CA1UEAwWISWRwUHVhHkwwqEIMAGCCSgCSStb3DOEBAQUAA41BDwAwggEKAoIBAQCu8ZUinr8C
YwU3wo1OBo4yglJluXqe7Z7JRkmQWq1vSgdxTShu3F6PUCdC1bz/FaQzOC9yKqndoxYnrmqpVx
TpcBztYgB2kaYReFDTC40TEB6qtUvm7C4IUZlqIMhqCvCxbTzLzMDwSx+ngae5Vd/wS01PYbxxz
CEXcQicTFG0IPAE8pPEhfT94cDGFz7IDzise8IM8rrhWCzHdq6xDPZ18AZhNSkSD/Qz0551Quv14
zFBR0yGd+oG5awBc09opwd1Sh/Cz25zWEbuz+04Uv/VUuH2EYVZlOf2dHlJvtmX0wTmeCT5Ks09
fv3XdRcL5mbSdf225BOBvynSH+VzAqMBAALwDQYJKoZIhvcNAQELBQADggEBAAGNp9RUKlTpxDFS
m6jvR8Nv4lrdzrea0TeRTJNTsb/mA1ISRrMqYFnC91aJBdoSDlw6xhgAVjkyc/KKhul3hL9F3
1Yy7wXhUu9DIXC4uImVhUdmp/eVm1/uyCINMSHI+9V3KWSyugfawBz96EYn8FX00TpsJhulpdhl
MTRDSEqeL7Lq7flocrXE7PUCF15IHkV30xpBR4iuVoutJlIbRqJKAK7M66wzC2VyszmVwwD4+VzV6
WY5GABrisdABB0BLZQAuqgl4SRsSvqr110YuvL0+aYXdkf9QlIGDrL2IIDYluT3R15Pp8U2Jfplw8a/vl0Dxw9Sg7q2RQfx3YA</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
```

6. Upload the Access IDP Proxy signing cert in PowerShell.

- `PSC:\>$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\idp-proxy.cer")`
- `PSC:\>$certData = [system.convert]::tobase64string($cert.rawdata)`
- `PSC:\>$saml | Add-Member -MemberType NoteProperty -Name SigningCertificate -Value $saml.SigningCertificate`
- `PSC:\>$saml.SigningCertificate=$certData`

7. Unfederate the domain by executing the command in PowerShell.

```
PSC:\>Set-MSolDomainAuthentication -DomainName <domain_name>.com -Authentication Managed
```

8. Re-federate the domain.

```
ps c:\>Set-MSolDomainAuthentication -DomainName -FederationBrandName $saml.FederationBrandName -Authentication Federated -PassiveLogOnUri
```



```
$saml.PassiveLogOnUri -ActiveLogOnUri $saml.ActiveLogonUri -SigningCertificate  
$saml.SigningCertificate -IssuerUri $saml.IssuerUri -LogOffUri $saml.LogOffUri -  
PreferredAuthenticationProtocol "SAML"
```

9. Verify the new settings.

```
ps c:\>Get-MsolDomainFederationSettings -DomainName
```



Copyright © 2016 - 2018 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.