



# MobileIron Access Cookbook

## Access with Office 365 and SecureAuth

**08 February 2018**



## Contents

Overview.....	3
Prerequisites.....	3
Configuring Office 365 and SecureAuth with MobileIron Access .....	4
Register Sentry to Access .....	4
Configure Access to create a Federated Pair .....	4
Configure SecureAuth with MobileIron Access.....	5
Configure Office 365 with MobileIron Access .....	7
Verification .....	9



# Overview

SAML/WSFed 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 SecureAuth for authentication. The user gets authenticated by SecureAuth and obtains a SAML/WSFed token for accessing applications in a cloud environment, such as Office 365.

This guide serves as step-by-step configuration manual for users using SecureAuth as an authentication provider with Office 365 in a cloud environment.

This cookbook is to configure Office 365 and SecureAuth for passive authentication in SAML protocol.

## Note the following:

- SecureAuth supports applications which prompts MODERN AUTHENTICATION.
- MODERN AUTHENTICATION: The app uses Passive Auth flow initially. Subsequent SAML renewals follows Active Auth flow.
- In WS-Fed environment, only passive auth flow is tested. Active Auth is not supported.

## 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

You must perform the following steps before you configure Office 365:

- Download the metadata files for Office 365.
  1. Download Office 365 metadata file from <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>
- Download the metadata files for SecureAuth:
  1. Login to SecureAuth with admin credentials.
  2. Click on the Office 365 realm > Post Authentication tab and scroll down.
  3. Click **Download** at the **Metadata File** field and save the file.



# Configuring Office 365 and SecureAuth with MobileIron Access

You must perform the following tasks to configure Office 365 and SecureAuth with MobileIron Access:

- [Register Sentry to Access](#)
- [Configure Access to create a Federated Pair](#)
- [Configure SecureAuth with MobileIron Access](#)
- [Configure Office 365 with MobileIron Access](#)

## [Register Sentry to Access](#)

You must register Sentry to Access to fetch the latest configuration from Access.

### **Prerequisites**

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. Enter the tenant password for the profile.
6. Click **OK**.
7. **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.

## [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 to create a federated pair.



## Procedure

1. Log in to **Access**.
2. Click **Profiles > Get Started**.
3. Enter Access host information and upload the **ACCESS SSL certificate**. The other fields retain the default values. Click **Save**.
4. Click **Profiles > Federated Pairs > Add**.
5. Select **Office 365** as the service provider.
6. Enter the following details:
  - a. Enter a **Name**.
  - b. Enter an appropriate **Description**.
  - c. Select the Access generated default **Signing Certificate** from the drop-down list.
  - d. In Office 365 specifics, select SAML from Office 365 Domain Federation:

Protocol	Settings
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. Select <b>WS-Trust 2005</b>.</li><li>2. Enter the value for Federated Domain for Office 365. For example: orange.com.</li><li>3. Enter the Active Logon URL for Original IDP Active Logon Url. For example: <a href="https://&lt;fqdn of secureauth server&gt;/&lt;O365 Realm for WSFed&gt;/webservice/wstrust.svc/2005/usernamemixed">https://&lt;fqdn of secureauth server&gt;/&lt;O365 Realm for WSFed&gt;/webservice/wstrust.svc/2005/usernamemixed</a></li></ol> <p><b>Note:</b> For active authentication, a pre-defined Microsoft Office 365 application must be available in SecureAuth. Use the above URL from this application.</p>

- e. Upload the metadata file of service provider downloaded from <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>
  - f. (Optional) Select *Use Tunnel Certificates for SSO* to configure Cert SSO on MobileIron Core. See *Appendix* in the *MobileIron Access Guide* at <https://support.mobileiron.com/docs/current/accs/> .
7. Click **Next**.
8. Select **SecureAuth** as the Identity provider. Click **Next**.
9. Upload the **IdP certificate** and the **IdP metadata file** download. Click **Done**.
10. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** metadata files.
11. On the **Profile** tab, click **Publish** to publish the profile.

## Task Result

The Federated Pair is created.

### [Configure SecureAuth with MobileIron Access](#)

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



## Procedure

1. Login to SecureAuth with admin credentials.
2. Click on Office 365 realm > Post authentication tab.
3. Edit the SAML Assertion/WS Federation settings and replace SAML recipient, SP start URL values with entity id available in the **Access SP Metadata (Upload to IDP)** file downloaded at step 10 of [Configure Access to create a Federated Pair](#).

The screenshot shows the SecureAuth Admin Console interface. The top navigation bar includes 'Overview', 'Data', 'Workflow', 'Adaptive Authentication', 'Multi-Factor Methods', 'Post Authentication', 'API', 'Logs', 'System Info', and 'Logout'. The main content area is titled 'SecureAuth3' and shows a list of realms on the left. The 'SecureAuth3' realm is selected, and its settings are displayed on the right. The 'SAML Assertion / WS Federation' section is expanded, showing various configuration fields. A red box highlights the 'SAML Consumer URL', 'WSFed/SAML Issuer', 'SAML Recipient', 'SAML Audience', and 'SP Start URL' fields, which are currently empty. Other visible fields include 'Name ID Format' (urn:oasis:names:tc:SAML:1.1:nar), 'Encode to Base64' (True), 'WSFed Reply To/SAML Target URL', 'WS-Fed Version' (1.2), 'WS-Fed Signing Algorithm' (SHA2), 'SAML Signing Algorithm' (SHA2), 'SAML Offset Minutes' (0), 'SAML Valid Hours' (24), and 'Append HTTPS to SAML Target URL' (True).

4. Edit the ACS/SAML Request Certificate and copy-paste the certificate from Access SP Metadata (Upload to IDP) file downloaded at step 10 of [Configure Access to create a Federated Pair](#).



SecureAuth3

Custom Groups: All

Create custom realm groups.

Realm Navigation: Select/Unselect All

- SecureAuth0 SecureAuth Administration
- SecureAuth1 Native Mobile Apps Native Mobile Apps Integration
- SecureAuth2 Salesforce Salesforce
- SecureAuth3 O365 SAML Realm1**
- SecureAuth4 O365 wsFed
- SecureAuth5 Page Header Userdatabase
- SecureAuth6 Salesforce Salesforce
- SecureAuth998 OATH Enrollment

ACS / SAMLRequest Certificate: MIIDYjCCAKoCCQDt/2MBm5uwtjANBgkqhkiG9w0BAQsFADBzMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEwWwQGA1UgwkTW9iaWxISXJvbjJEAwwHU3BQcm94AyMzMxMTRaMHMxvxpZm9ybmlhMRYwQYDVQQKDApNb2JpbGVJcm9uMRAwDgYDVQQLDAdTdXBwb3J0MRAwDgYDVQOQDAdTcFByb3h5MIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAy9V9QoRb9r0ZsAFA

Authentication Method (1.1): urn:oasis:names:tc:SAML:1.0:am

Confirmation Method (1.1): urn:oasis:names:tc:SAML:1.0:cm

AuthnContext Class: Unspecified

Include SAML Conditions: True

SAML Response InResponseTO: True

SubjectConfirmationData Not Before: False

Signing Cert Serial Number: [Field] Select Certificate

Assertion Signing Certificate: certificate.wse3.cer

Domain: [Field]

Metadata File: Download

Save

SAML Attributes / WS Federation

## [Configure Office 365 with MobileIron Access](#)

Office 365 does not provide provision to upload the metadata file. The information must be extracted from IDP Proxy Metadata file downloaded at step 10 of [Configure Access to create a Federated Pair](#).

### Procedure

1. Open Windows PowerShell.
2. Execute the following command in PowerShell downloaded at step 10 of [Configure Access to create a Federated Pair](#):

```
PS C:\> powershell -ExecutionPolicy ByPass -File .\MICROSOFT_OFFICE_365_SP-SAML-script.ps1
```

**Note:** Download the PowerShell script from MobileIron Access for Office 365 and SecureAuth federated pair to avoid manual editing.



Overview Federated Pairs Conditional Access Split Tunneling Branding Certificates

### Federated Pairs

Show Description  
How to upload my Access metadata to my IDP or SP?

+ Add New Pair

0365 and SecureAuth	Access SP Metadata (Upload to IDP) View   Download	SP Metadata View
No description Policy Name: Default Policy	Access IDP Metadata (Upload to SP) View   Download	IDP Metadata View
	Powershell Commands for Office 365 View   Download	

### 3. Execute the following commands from Office 365 PowerShell:

- ps c:\>Set-MSolDomainAuthentication -DomainName <domain name>-  
Authentication Managed
- ps c:\>Set-MSolDomainAuthentication -DomainName <domain name>-  
FederationBrandName
- \$saml.FederationBrandName -Authentication Federated
- PassiveLogOnUri <https://<hostname>/MobileIron/acc/736de1f6-2c3e-445f-8d8a-957c0d17db77/idp>
- ActiveLogOnUri <https://<hostname>/MobileIron/acc/736de1f6-2c3e-445f-8d8a-957c0d17db77/idp>
- **SigningCertificate**  
MIIDZDCCAKwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYD  
VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwN  
TW91bnRhaW4gVmllZETMBEGA1UECgwKWTW9iaWxlSXJvbjEQMA4GA1UEC  
wwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMtUxMDEzMj  
MyNDIwWhcNMjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMB  
EGA1UECAwKQ2FsaWZvcn5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmllZ  
zETMBEGA1UECgwKWTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER  
MA8GA1UEAwwISWRwUHJveHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwA  
wggEKAoIBAQCu8ZUn5rBCYwu3woTOBa4ygLJIuXqe72j7RkmQWqTv5kkJxTs  
Hu3F6PUCtXcLbz/FaQzOC9yKQnKhxYnrmqpVXIpcBztYgB2XaYReTDTCr40TE  
86qUvrn7C4IUZiqINhqGVCx8IzlzMJwSx+ngae5Vd/ws01PYbxnsCEXcQicYFG0iP  
AE8pPEhft94cDGfe7iDzieo8IM8rBhWCzHdg6xDPZI8AZhN5kSD/Qz055IQuvI4z  
F8R0yG0+oGsawBC09opwdT5h/CzzSzWEBuz+04Uv/VfUrH2EvY2IOf2dHIjvtmX  
OwTm6CTsKs09fvi3XdRG15mbSdF22SBOBsynSH+vzAgMBAAEwDQYJKoZIhvc  
NAQELBQADggEBAA6Np9RUkiTjxOFSm6j8vR8Nv4ltrdzrea0TeRTjNTSb/ma1i  
SRrMqYFnC91aJBdo5Dlwg6xhgAVjkyC/KKhul3hL9F3IYy7wXhUU9DJXC4uTmV  
hHJmp/6Vm1/uYCINMSHI+9VXKWSyugFaWBz96EYn8EXOOTpSjfulpdhL/MTR  
DsEgEI7Eg7FkxrXE7PUcF15IHKv30xjxBR4iuVouUHbRqJKAK7M66w2c2VySzm  
VvwD4+vz1VeWY5GABriSdAB8OBLZQAugib4SRsSvgr1iOYuvL0+aYXdkf9QII





GDrLzIIDYluT3R15Pp8U2JfpIw8a7vlOIxw9Sg7g2RQfx3YA=

- IssuerUri <https://eapp289-alt.auto.mobileiron.com/MobileIron/acc/736de1f6-2c3e-445f-8d8a-957c0d17db77/idp>
- LogOffUri <https://eapp289-alt.auto.mobileiron.com/MobileIron/acc/736de1f6-2c3e-445f-8d8a-957c0d17db77/idp>
- MetadataExchangeUri <https://eapp289-alt.auto.mobileiron.com/MobileIron/acc/>

### **Task Result**

Single sign-on service is now configured using SAML with Office 365 and SecureAuth. This configuration lets you fetch the latest configuration from Access.

## **Verification**

Verify that the following tests are successful:

1. Register a device to Core.
2. Download Salesforce application from App Store.
3. Open the application. This triggers the VPN.
4. Verify that SAML SSO is working.



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.