MobileIron Access Cookbook

Access with Office 365 and SecureAuth

08 February 2018

Contents

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

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	1. Select the appropriate ECP Backend Type from the drop-down. This option lets Access connect to the IdP. Select **WS-Trust 2005**. 2. Enter the value for Federated Domain for Office 365. For example: orange.com. 3. Enter the Active Logon URL for Original IDP Active Logon Url. For example: https://<fqdn of secureauth server>/<O365 Realm for WSFed>/webservice/wstrust.svc/2005/usernamemixed **Note**: For active authentication, a pre-defined Microsoft Office 365 application must be available in SecureAuth. Use the above URL from this application.

    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

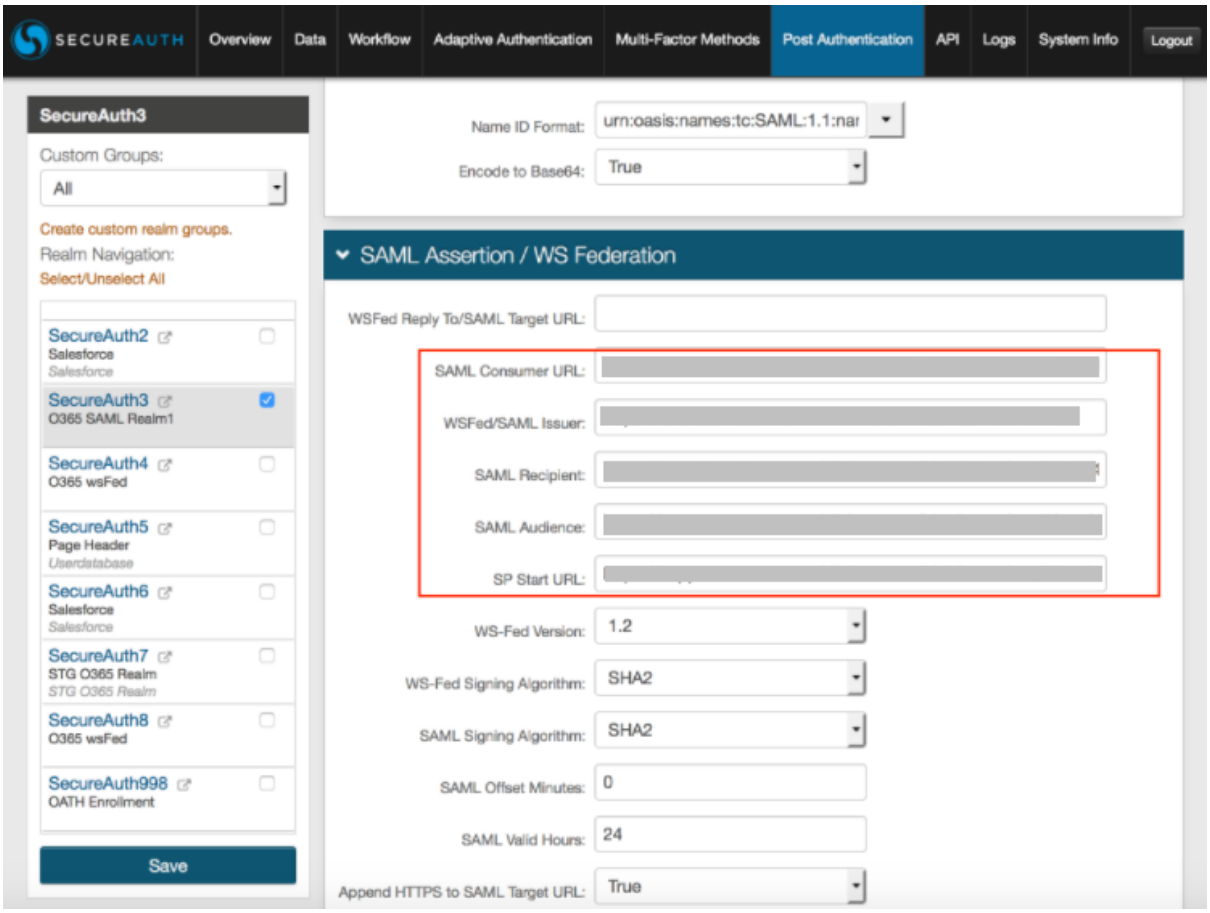
The Federated Pair is created.

Configure SecureAuth with MobileIron Access

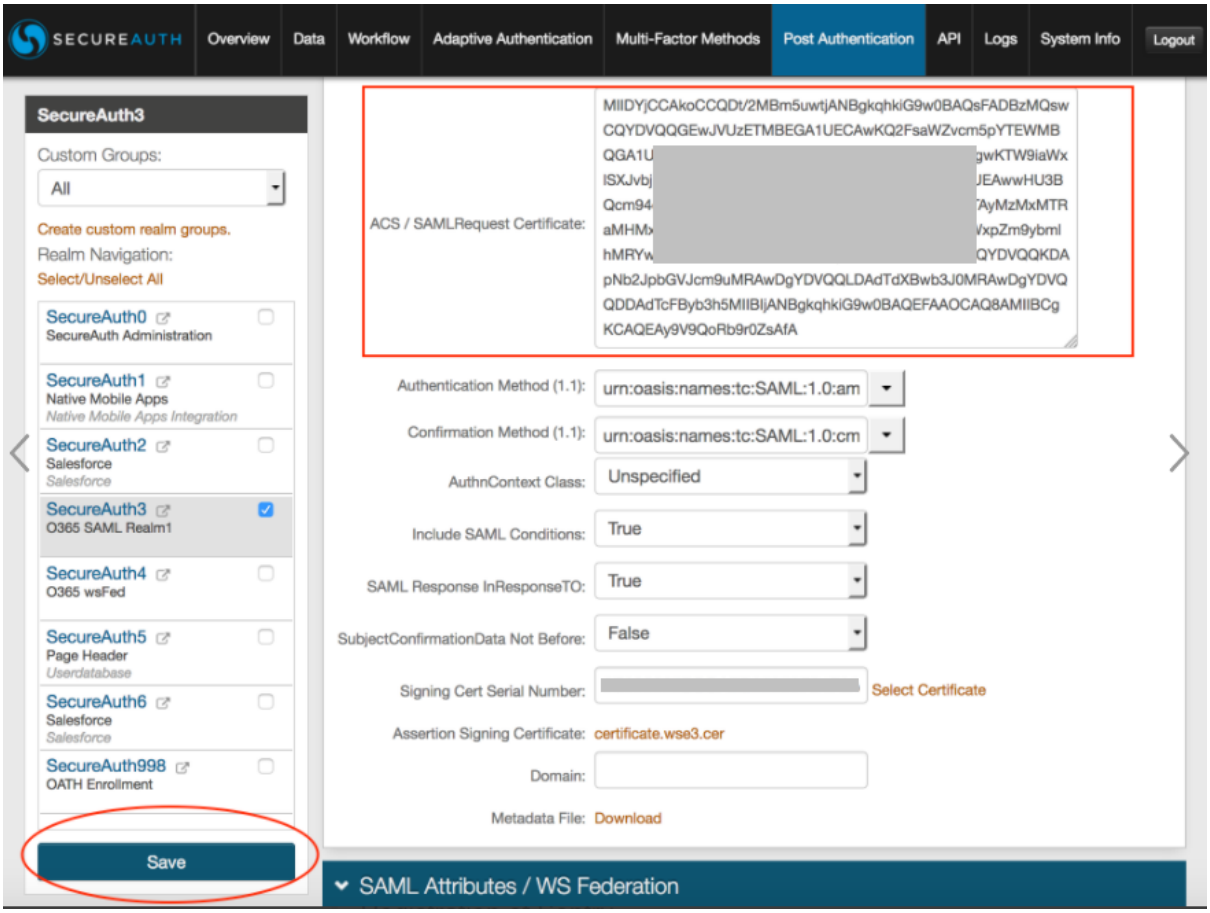
You must configure the identity provider with the service provider metadata file. This builds the trust relationship with the service provider.

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.



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.



Configure Office 365 with MobileIron Access

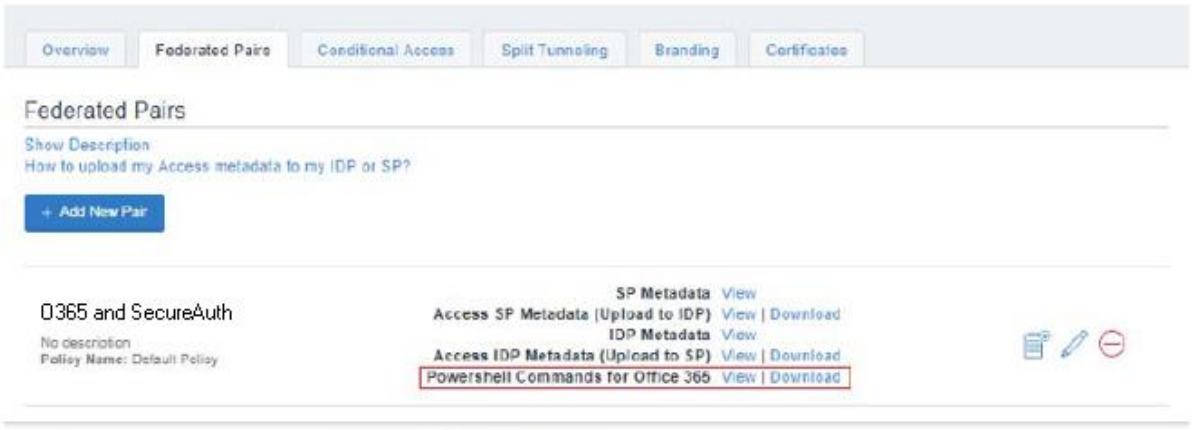
Office 365 does not provide provision to upload the metadata file. The information must be extracted from IDP Proxy Metadata file downloaded at step 10 of Configure Access to create a Federated Pair.

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.



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
     VQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwN
     TW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UEC
     wwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTUxMDEzMj
     MyNDIwWhcNMjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMB
     EGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmlld
     zETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER
     MA8GA1UEAwwISWRwUHJveHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwA
     wggEKAoIBAQCu8ZUn5rBCYwu3woTOBa4ygLJIuXqe72j7RkmQWqTv5kkJxTs
     Hu3F6PUCtXcLbz/FaQzOC9yKQnKhxYnrmqpVXIpcBztYgB2XaYReTDTCr40TE
     86qUvrn7C4lUZiqINhqGVCx8IzlzMJwSx+ngae5Vd/ws01PYbxnsCEXcQicYFG0iP
     AE8pPEhfT94cDGfe7iDzieo8IM8rBhWCzHdg6xDPZI8AZhN5kSD/Qz055IQuvI4z
     F8R0yG0+oGsawBC09opwdT5h/CzzSzWEBuz+04Uv/VfUrH2EvY2lOf2dHIjvtmX
     OwTm6CTsKs09fvi3XdRGl5mbSdF22SBOBynSH+vzAgMBAAEwDQYJKoZIhvc
     NAQELBQADggEBAA6Np9RUkiTjxOFSm6j8vR8Nv4ltrdzrea0TeRTjNTSb/mA1i
     SRrMqYFnC91aJBdo5Dlwg6xhgAVjkyc/KKhul3hL9F3IYy7wXhUU9DJXC4uTmV
     hHJmp/6Vm1/uYClNMSHl+9VXKWSyugFaWBz96EYn8EXOOTpSjfulpdhL/MTR
     DsEgEI7Eg7FkxrXE7PUcF15lHKv30xjxBR4iuVouUHbRqJKAK7M66w2c2VySzm
     VvwD4+vzlVeWY5GABriSdAB8OBLZQAugib4SRsSvgri1iOYuvL0+aYXdKf9QlI

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.