MobileIron Access Cookbook

Access with Office 365 and Shibboleth

24th November, 2017

Contents

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 Shibboleth for authentication. The user gets authenticated by Shibboleth and obtains a SAML token for accessing applications in a cloud environment, such as Office 365. This guide serves as step-by-step configuration manual for users using Shibboleth as an authentication provider with Office 365 in a cloud environment.

This cookbook is to configure Office 365 and Shibboleth for passive authentication in SAML protocol. WS-Fed for Office 365 and Shibboleth pair is not supported.

Prerequisites

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

- Ensure that you have a working setup between Office 365 and Shibboleth without MobileIron Access.

- **Metadata files for Office 365**
  Download Office 365 metadata file from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

- **Metadata files for Shibboleth**
  curl -o shib-metadata.xml https://<adfs_hostname>/idp/shibboleth

Configuring Office 365 and Shibboleth with MobileIron Access

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

- Configure Access to create a Federated Pair
- Configure the Shibboleth environment with MobileIron Access
- Configure the Office 365 environment with MobileIron Access
- Registering Sentry to Access

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** for Office 365.
    b. Enter an appropriate Description.
    c. Select the Access generated default **Signing Certificate** from the drop-down list.
    d. Select **WS-Trust 2005** in Office 365 specifics.
    e. Enter value for Federated Domain: <domain_name>.com
    f. Enter the original IdP Active Logon URL
    You can find the value in **Office365** > **Sign On** >**WS-Federation View** setup instruction.
    Note: For active authentication, a pre-defined Microsoft Office 365 application must be available in Shibboleth. Use the above URL from this application.
    g. Upload the metadata file of service provider downloaded from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
    h. 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 **Microsoft ADFS** as the identity provider. Click **Next**.
9. Select the Access generated default **Signing Certificate** from the drop-down list.

10. Upload the **IdP metadata file** for Shibboleth downloaded in Prerequisites. Click **Done**.
11. Download the **ACCESS SP Metadata (Upload to IDP)** and the **ACCESS IDP Metadata (Upload to SP)** files from the federated pair page.
12. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

Configure the Shibboleth environment with MobileIron Access

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

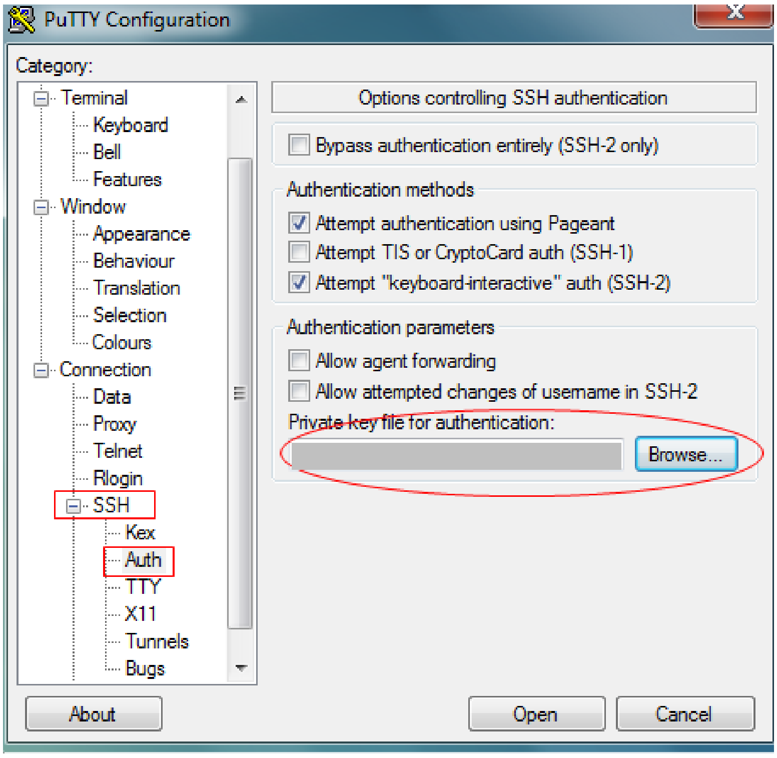
Login to Shibboleth Machine from MAC

ssh -i "/Users/<User>/Downloads/<user>.pem" user@adfs-plugin.<domain_name>

OR

Login to Shibboleth Machine from Windows

1. Open the **Putty** and enter hostname.
2. Select the certificate location in Putty. Expand **SSH** under **Connections**, select **Auth** and point to certificate location.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

□ Allow attempted changes of username in SSH-2

Private key file for authentication:

3. Run the following command

   [hostname]$ sudo docker exec -it containet_shib_office /bin/bash

4. Create a **Directory** with Sentry name by executing the following command:

   [root@<username> /]# mkdir hostname

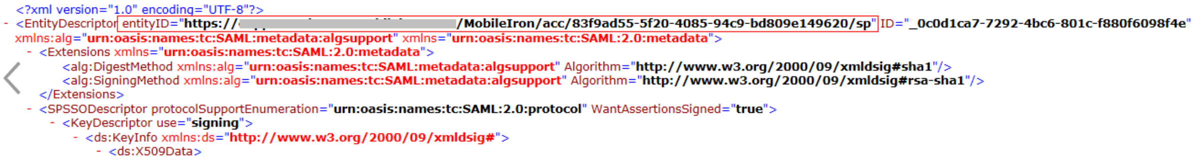
   [root@<username> /]# chmod 777 -R hostname

   [root@<username> /]# cd hostname/

5. Create an xml file and copy the contents of the SP Proxy Metadata file downloaded at **Step 11** in Configure Access to create a Federated Pair.

6. Edit the metadata file: */opt/shibboleth-idp/conf/metadata-providers.xml*
   a. Search for the below file
      <MetadataProvider id="LocalMetadata"
      xsi:type="FilesystemMetadataProvider"
      metadataFile="PATH_TO_YOUR_METADATA"/>
   b. Add the following line in this section:
      <MetadataProvider id="LocalMetadata"
      xsi:type="FilesystemMetadataProvider"
      metadataFile="/<hostname>/mex.xml"/>

7. Extract the Entity ID from the **ACCESS SP Metadata (Upload to IDP**) downloaded at **Step 11** in Configure Access to create a Federated Pair.



```
<?xml version="1.0" encoding="UTF-8"?>
- <EntityDescriptor entityID="https://[redacted]/MobileIron/acc/83f9ad55-5f20-4085-94c9-bd809e149620/sp" ID="_0c0d1ca7-7292-4bc6-801c-f880f6098f4e"
  xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <Extensions xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
      <alg:DigestMethod xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport" Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <alg:SigningMethod xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport" Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    </Extensions>
  - <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true">
    - <KeyDescriptor use="signing">
      - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        - <ds:X509Data>
```

8. In the Shibboleth machine, edit Relying party metadata file *"/opt/shibboleth-idp/conf/<xml file>"*. Search and add the SP Entity ID information in below line.

    <bean parent="RelyingPartyByName"
   c:relyingPartyIds="https://<hostname>/<organization>/acc/<path>/sp">

9. Edit the attribute filter file:
   /opt/shibboleth-idp/conf/attribute-filter.xml

10. Add the SP Entity ID in the following line:
    <afp:PolicyRequirementRule xsi:type="basic:AttributeRequesterString" value="https://<hostname>/<org>/acc/<path>/sp />

11. Restart the Shibboleth container.
    [root@username/]# exit

```
[user@adfs-plugin ~]$ sudo docker restart containet_shib_office
```

12. View the Shibboleth log file:

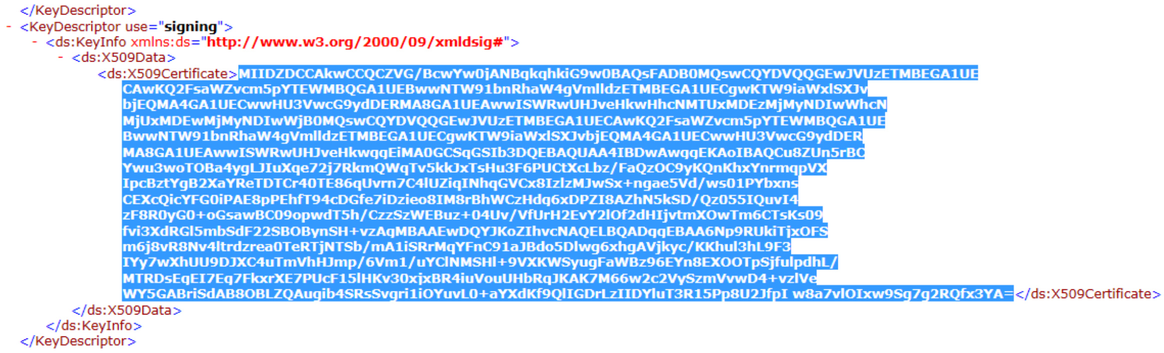
```
[user@adfs-plugin ~]$ sudo docker exec -it container_shib_office /bin/bash
[root@username/]# tail -f /opt/shibboleth-idp/logs/idp-process.log
```

Configure the Office 365 environment with MobileIron Access

You must configure Office 365 to use with Shibboleth.

Procedure

1. Extract the Entity ID from the metadata file downloaded in **Step 11** of Configure Access to create a Federated Pair.
2. Login to Office 365 tenant using Windows Azure PowerShell.
   PS c:\>Connect-MsolService
3. Execute the following commands in PowerShell and replace the Entity ID with the ID that is extracted in **Step 1**.
   - PS C:\Windows\system32> $FederationBrandName="<Test>"
   - PS C:\Windows\system32> $ActiveLogOnUri="https://<hostname>/<org>/acc/<path>/idp/active"
   - PS C:\Windows\system32> $IssuerUri=" https://<hostname>/<org>/acc/<path>idp"
   - PS C:\Windows\system32> $LogOffUri=" https://<hostname>/<org>/acc/<path>/idp/logout"
   - PS C:\Windows\system32> $PassiveLogOnUri=" https://<hostname>/<org>/acc/<path>/idp"
4. Extract the certificate from **ACCESS IDP Metadata (Upload to SP)** and save in a *.cer* file.



```
  </KeyDescriptor>
- <KeyDescriptor use="signing">
  - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:X509Data>
        <ds:X509Certificate>MIIDZDCCAkwCCQCZVG/BcwYw0jANBqkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzETMBEGA1UE
          CAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJv
          bjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTUxMDEzMjMyNDIwWhcN
          MjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
          BwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER
          MA8GA1UEAwwISWRwUHJveHkwqqEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwqqEKAoIBAQCu8ZUn5rBC
          Ywu3woTOBa4ygLJIuXqe72j7RkmQWqTv5kkJxTsHu3F6PUCtXcLbz/FaQzOC9yKQnKhxYnrmqpVX
          IpcBztYgB2XaYReTDTCr40TE86qUvrn7C4lUZiqINhqGVCx8IzlzMJwSx+ngae5Vd/ws01PYbxns
          CEXcQicYFG0iPAE8pPEhfT94cDGfe7iDzieo8IM8rBhWCzHdq6xDPZI8AZhN5kSD/Qz055IQuvI4
          zF8R0yG0+oGsawBC09opwdT5h/CzzSzWEBuz+04Uv/VfUrH2EvY2lOf2dHIjvtmXOwTm6CTsKs09
          fvi3XdRGl5mbSdF22SBOBynSH+vzAqMBAAEwDQYJKoZIhvcNAQELBQADqqEBAA6Np9RUkiTjxOFS
          m6j8vR8Nv4ltrdzrea0TeRTjNTSb/mA1iSRrMqYFnC91aJBdo5Dlwg6xhgAVjkyc/KKhul3hL9F3
          IYy7wXhUU9DJXC4uTmVhHJmp/6Vm1/uYClNMSHl+9VXKWSyugFaWBz96EYn8EXOOTpSjfulpdhL/
          MTRDsEqEI7Eq7FkxrXE7PUcF15lHKv30xjxBR4iuVouUHbRqJKAK7M66w2c2VySzmVvwD4+vzlVe
          WY5GABriSdAB8OBLZQAugib4SRsSvgri1iOYuvL0+aYXdKf9QlIGDrLzIIDYluT3R15Pp8U2JfpI w8a7vlOIxw9Sg7g2RQfx3YA=</ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </KeyDescriptor>
```

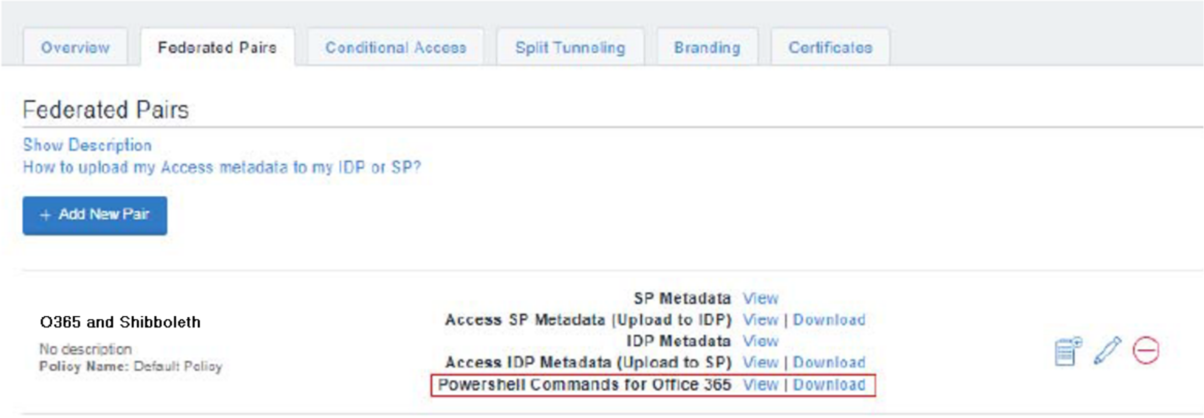
5. Execute the following commands in Office 365 PowerShell:

    - PS C:\Windows\system32> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\shibbo-idp-proxy.cer")

    - PS C:\Windows\system32> $certData = [system.convert]::tobase64string($cert.rawdata)

    - PS C:\Windows\system32> $SigningCertificate=$certData

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



Federated Pairs

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

O365 and Shibboleth
No description
Policy Name: Default Policy

SP Metadata View
Access SP Metadata (Upload to IDP) View | Download
IDP Metadata View
Access IDP Metadata (Upload to SP) View | Download
Powershell Commands for Office 365 View | Download

6. Unfederating and Federating the domain:
   Execute the following commands in PowerShell:

    - PS C:\Windows\system32> Set-MsolDomainAuthentication -DomainName -<domain_name> Authentication Managed

    - PS C:\Windows\system32> Set-MsolDomainAuthentication -DomainName <domain_name> -FederationBrandName $FederationBrandName -Authentication Federated -PassiveLogOnUri $PassiveLogOnUri -ActiveLogOnUri $ActiveLogonUri -SigningCertificate $SigningCertificate -IssuerUri $IssuerUri -LogOffUri $LogOffUri -PreferredAuthenticationProtocol "SAMLP"

7. View the configuration settings for Office 365 domain:

    - PS C:\Windows\system32> Get-MsolDomainFederationSettings -DomainName <domain_name>

Registering 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.

Verification

- Open a browser and login to Office 365 account. Check the Sentry Logs for SAML Request and Responses.
- Configure Native Email App on iOS/Android/Windows device and check the Sentry Logs for SAML Request and Responses.