MobileIron Access Cookbook

Access with Office 365 and Okta

Revised: April 05, 2018

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 Okta for authentication. The user gets authentication from Okta 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 Okta as an authentication provider with Office 365 in a cloud environment.

This cookbook is to configure Office 365 and Okta for passive authentication in SAML protocol. WS-Fed for Office 365 and Okta pair 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:

- Verify that you download the deployment guide for Okta with Office 365: https://support.okta.com/help/Documentation/Knowledge_Article/Office365-Deployment-Guide
- Download the metadata files for Okta.
    1. Login to Okta with admin credentials.
    2. On the **Application** tab, click **Sign On** tab.
    3. Click **Identity Provider metadata** and download the metadata file.
- Download the metadata files for Office 365.
    1. Download Office 365 metadata file from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml

Configuring Office 365 and Okta with MobileIron Access

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

- Configure Access to create a Federated Pair
- Configure the Okta environment
- Configure the Office 365 environment
- Configure Office 365 with IDP Proxy Settings
- Configure Okta with SP Proxy Settings
- Register 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. Upload the SPProxy Certificate.
    e. Select **WS-Trust 2005** in Office 365 specifics.
    f. Enter value for Federated Domain: <domain_name>.com
    g. 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 Okta. Use the above URL from this application.
    h. Upload the metadata file of service provider downloaded from https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml
    i. 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 **Okta** as the Identity provider. Click **Next**.
9. Upload the **IdP certificate** and the **IdP metadata file** download. Click **Done**.
10. Download the **ACCESS SP Proxy** and the **ACCESS IDP Proxy** metadata file.
11. On the **Profile** tab, click **Publish** to publish the profile.

Task Result

The Federated Pair is created.

Configure the Okta environment

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 Okta with Admin credentials.
2. Click **Add Application**.
3. Click **Create New App**.
4. Select **SAML 2.0** and click **Create**.
5. Enter an **App name** for the application and click **Next**.
6. Enter the configuration values.

SAML Settings	Values
Single sign on URL	Extract the single sign on URL from the SP metadata file. Select the check box for **Use this for Recipient URL and destination URL**.
Audience URI(SP Entity ID)	Enter the above single sign on URL.
Default RelayState	Enter the above single sign on URL. If no value is set, a blank relay is sent.
Name ID format	Persistent
Application username	Okta username

7. Click **Show Advanced Settings**.

Settings	Values
Response	Unsigned
Assertion Signature	Signed
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	Deselect the check box for Allow application to initiate Single Logout
Authentication context class	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/$(org.externalKey)

Add the screen, ATTRIBUTE STATEMENTS (optional).
   - user.email for IDPEmail
   - UPN
8. Configure the **Feedback Settings** and click **Finish**.
   - Are you a customer partner: Select **I'm an Okta customer adding an internal app**.
   - Select the **This is an internal app that we have created** check box.
9. Click **Directory** >**People** > **Add Person** > **Create User**.
10. On the **Applications** tab, click **Assign Application**.
11. Select the Application and the User that you have created and click **Next**.
12. Click **Confirm Assignment**.

Testing a single user

The following instructions are used for testing with a single user.
You must follow Okta documentation to sync your directory with Okta and use the appropriate user mappings.

Note: Okta is not configured to be synced with Active Directory. To test a single user, you must get the immutable property value of the user from Office 365 and replace the user name with immutable ID of the user in Okta user name value.

1. Open PowerShell and execute the following command:

```
PS C:\Users\Administrator> Get-MsolUser -UserPrincipalName <User_Name> | select ImmutableId |
fl
```

2. On Okta portal, click **Applications** > **Office 365** > **People**.
   Edit the **User Name** and enter the **ImmutableID**.

   Immutable ID: cEogWsYJskiVf1MBE7Zi/Q==

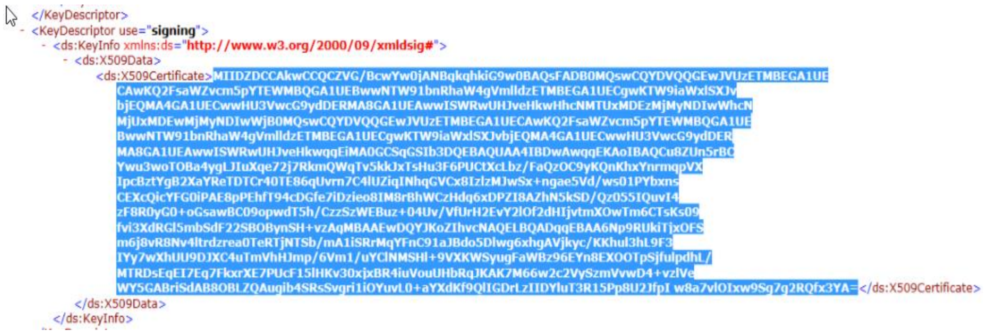
Configure the Office 365 environment

You must configure Office 365 to use with Okta.

Procedure

1. Login to Okta admin portal and click **Applications**.
2. On the **Sign On** tab, click **View Setup Instructions**.
3. Configure the setup instructions:

Settings	URL
Identity Provider Single Sign-on URL	<Single Sign-on URL extracted from the metadata file>

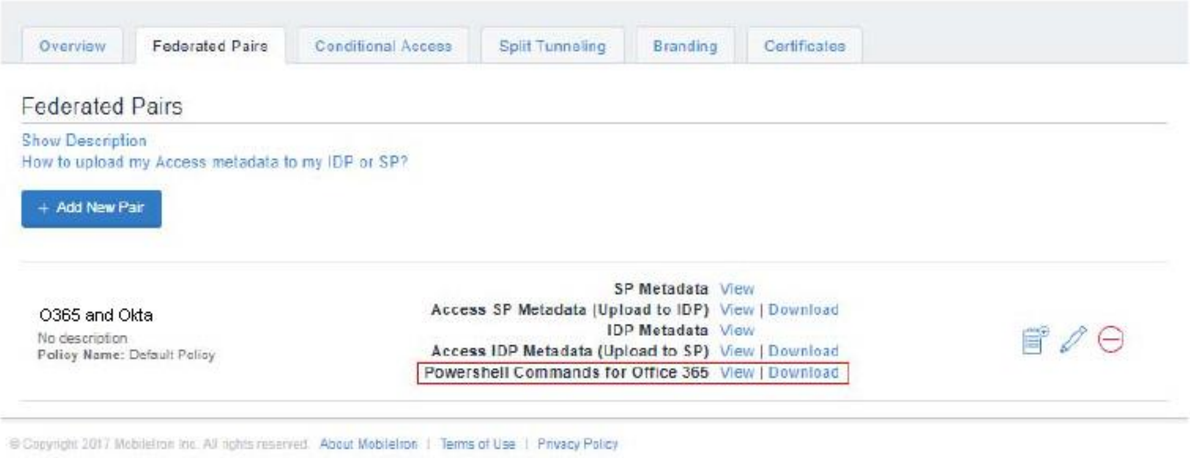
Identity Provider Single Logout URL	<Single Logout URL extracted from the metadata file>
Identity Provider Issuer	http://www.okta.com/exk6airngdrXNmGPr0h7
X.509 Certificate	

```
   </KeyDescriptor>
 - <KeyDescriptor use="signing">
   - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
     - <ds:X509Data>
         <ds:X509Certificate>MIIDZDCCAkwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzETMBEGA1UE
           CAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJv
           bjEQMA4GA1UECwwHU3VwcG9ydDERMA8GA1UEAwwISWRwUHJveHkwHhcNMTUxMDEzMjMyNDIwWhcN
           MjUxMDEwMjMyNDIwWjB0MQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UE
           BwwNTW91bnRhaW4gVmlldzETMBEGA1UECgwKTW9iaWxlSXJvbjEQMA4GA1UECwwHU3VwcG9ydDER
           MA8GA1UEAwwISWRwUHJveHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCu8ZUn5rBC
           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>
```

4. Extract the certificate and save in a *idp-proxy.cer* file.
5. Execute the following commands in Office 365 PowerShell:

Task	**Commands**
Office 365 settings	• $ActiveLogOnUri="https://dev-565215.oktapreview.com/app/mobileirondev565215_okataccso365_1/exk6airngdrXNmGPr0h7/sso/saml" • $IssuerUri="http://www.okta.com//exk6airngdrXNmGPr0h7" • $LogOffUri="https://dev-565215.oktapreview.com/app/mobileirondev565215_okataccso365_1/exk6airngdrXNmGPr0h7/slo/saml" • $PassiveLogOnUri="https://dev-565215.oktapreview.com/app/mobileirondev565215_okataccso365_1/exk6airngdrXNmGPr0h7/sso/saml" • $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\idp-proxy.cer") $certData = [system.convert]::tobase64string($cert.rawdata) $SigningCertificate=$certData
Unfederated the domain	ps c:\>Set-MsolDomainAuthentication -DomainName misentry.com -Authentication Managed
Refederate the domain	ps c:\>Set-MsolDomainAuthentication -DomainName <domain name> -FederationBrandName $saml.FederationBrandName -Authentication Federated -PassiveLogOnUri $saml.PassiveLogOnUri -ActiveLogOnUri $saml.ActiveLogonUri -SigningCertificate $saml.SigningCertificate -IssuerUri $saml.IssuerUri -LogOffUri $saml.LogOffUri -PreferredAuthenticationProtocol "SAMLP"
Verify the new settings	ps c:\>Get-MsolDomainFederationSettings -DomainName misentry.com

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



Federated Pairs

Show Description

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

O365 and Okta

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

© Copyright 2017 MobileIron Inc. All rights reserved. About MobileIron | Terms of Use | Privacy Policy

6. Login to the mail box from a browser, App (iOS native email app), or Outlook. Verify that the email sync is successful.

Configure Office 365 with IDP Proxy Settings

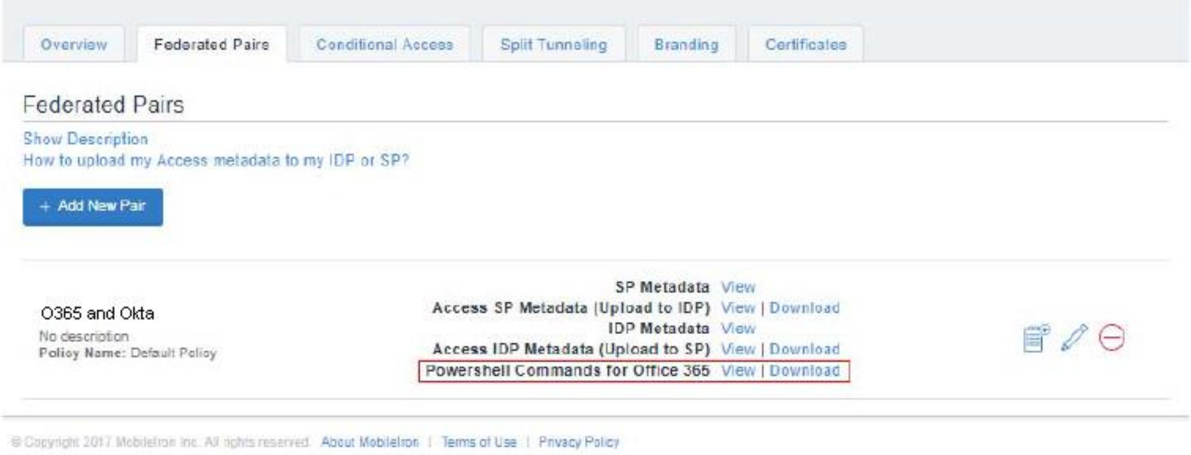
Office 365 does not provide provision to upload the metadata file. The information must be extracted from IDP Proxy Metadata file downloaded at Step 10 of Configure Access to create a Federated Pair.

Procedure

1. Use Remote Desktop services to log into an ADFS machine with Admin credentials.
2. Execute the following command in PowerShell to connect to Office 365 tenant:

   ```
   PS c:\>Connect-MsolService
   ```

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

   Federated Pairs

   Show Description

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

   O365 and Okta

   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

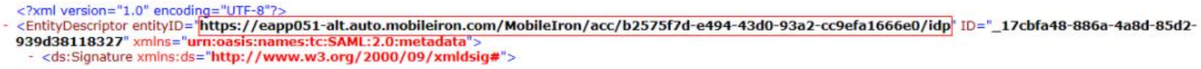
   © Copyright 2017 MobileIron Inc. All rights reserved. About MobileIron | Terms of Use | Privacy Policy

3. Execute the following command to fetch the existing settings:

   ```
   PS C:\> $saml = Get-MsolDomainFederationSettings -DomainName <domain name>
   ```

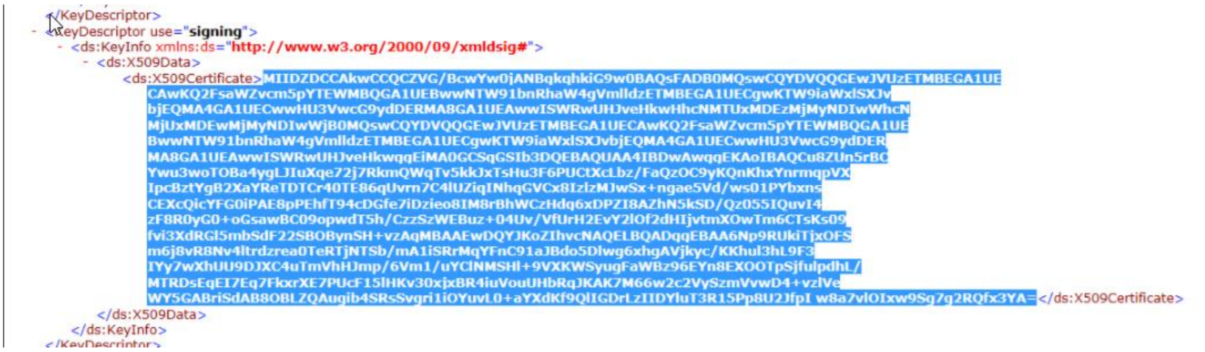
4. Edit the settings for ActiveLogOnUri, IssuerUri, LogOffUri, PassiveLogonUri
   - PSC:\>$saml = New-Object -TypeName PSObject
   - PSC:\>$saml | Add-Member -MemberType NoteProperty -Name ActiveLogOnUri -Value $saml.ActiveLogOnUri
   - PSC:\>$saml.ActiveLogOnUri="https://eapp051-alt.auto.mobileiron.com/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp/active"
   - PSC:\>$saml | Add-Member -MemberType NoteProperty -Name IssuerUri -Value $saml.IssuerUri
   - PSC:\>$saml.IssuerUri="https://eapp051-alt.auto.mobileiron.com/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp"
   - PSC:\>$saml | Add-Member -MemberType NoteProperty -Name LogOffUri -Value $saml.LogOffUri
   - PSC:\>$saml.LogOffUri="https://eapp051-alt.auto.mobileiron.com/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp/logout"
   - PSC:\>$saml | Add-Member -MemberType NoteProperty -Name PassiveLogOnUri -Value $saml.PassiveLogOnUri
   - PSC:\>$saml.PassiveLogOnUri="https://eapp051-alt.auto.mobileiron.com/MobileIron/acc/a5158d28-0f7c-4579-8ddc-aa59a1f28d13/idp

5. Edit the entity ID for PassiveLogOnUri, IssuerUri, and ActiveLogOnUri:



```
<?xml version="1.0" encoding="UTF-8"?>
- <EntityDescriptor entityID="https://eapp051-alt.auto.mobileiron.com/MobileIron/acc/b2575f7d-e494-43d0-93a2-cc9efa1666e0/idp" ID="_17cbfa48-886a-4a8d-85d2-
939d38118327" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  - <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

6. Extract the certificate from IDP Proxy metadata file and save it in a .cer file:



```
  </KeyDescriptor>
- <KeyDescriptor use="signing">
  - <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    - <ds:X509Data>
        <ds:X509Certificate>MIIDZDCCAkwCCQCZVG/BcwYw0jANBgkqhkiG9w0BAQsFADB0MQswCQYDVQQGEwJVUzETMBEGA1UE
        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>
```

7. Execute the following commands in PowerShell to upload the proxy signing certificate:
   - ps c:\>$cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("C:\idp-proxy.cer")
   - ps c:\>$certData = [system.convert]::tobase64string($cert.rawdata)
   - ps c:\>$saml.SigningCertificate=$certData
8. Execute the following command in PowerShell to unfederated the domain:
   - ps c:\>Set-MsolDomainAuthentication -DomainName <domain name> -Authentication Managed
9. Execute the following command in PowerShell to refederate the domain:
   - ps c:\>Set-MsolDomainAuthentication -DomainName <domain name> -FederationBrandName $saml.FederationBrandName -Authentication Federated -PassiveLogOnUri $saml.PassiveLogOnUri -ActiveLogOnUri $saml.ActiveLogonUri -SigningCertificate $saml.SigningCertificate -IssuerUri $saml.IssuerUri -LogOffUri $saml.LogOffUri -PreferredAuthenticationProtocol "SAMLP"
10. Execute the following command to verify the new settings:
    - ps c:\>Get-MsolDomainFederationSettings -DomainName misentry.com

Configure Okta with SP Proxy Settings

You must configure the IDP settings with the SP proxy settings to build a trust relationship.

Procedure

1. Login to Okta admin portal and click **Application**.
2. On the **Application** tab, select the application that is created.
3. On the **General** tab, click **SAML Settings** and click **Next**.
4. Extract the entity ID from the SP proxy metadata file and configure the settings as follows:
   - Enter the Single sign on URL
   - Audience URI
   - Name ID format: Persistent
   - Application username: Okta username
5. Click **Next** and click **Finish**.

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.

Task Result

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

What's next

Verify that the following tests are successful:

- Open a browser and login to Office 365 account. Verify that the Sentry logs for SAML request and responses are available.
- Configure Native Email app on iOS device and verify the Sentry logs for SAML request and responses.

ActiveSync email access control

You must enable Office 365 ActiveSync access control using Standalone Sentry and IP claim rules with Okta. This is not a mandatory task for upgrade cycle.

Prerequisites

- Verify that you have configured SSO using SAML between Office 365 as service provider and Okta as the identity provider. See Configuring Office 365 and Okta with MobileIron Access.

Procedure:

1. Login to Okta admin portal with admin credentials.
2. Select **Security** > **Network**.
3. Click **Add Zone** to add Zone tab in test tenants.
   Note: There are two zones that are available by default and can be used as an example to create zones. This lets you allow or block IP addresses.
4. Click **Edit** to modify IP Zone such as LegacyIpZone and enter the IP address of the Sentry.
5. Click **Save**.
6. On the **Applications** tab, select **Office365**.
7. Click **Sign On** and scroll-down to **Signon Policy**.
8. Click **Add Rule** and enter the following information:
   a. Enter the **Rule Name**.
   b. In **Location**, select **Not in Zone**.
   c. In **Network Zones**, enter the name of the zone that you created, such as, LegacyIpZone.
   d. In CLIENT, select Mobile (ActiveSync)
   e. In ACTIONS, select Denied from the drop-down list.
   f. Click Save.
9. The IP Claim Rule is added.