Set up SSO between Azure AD and Oracle Identity Cloud Service for PeopleSoft

Technologies
IAM
Service Categories
Multicloud, Networking
Released
Jan 10, 2020

Set Up Federation Trust Between Azure AD and Identity Cloud Service

For setting up federation trust, you need to add Oracle Identity Cloud Service as a gallery application in Azure AD tenant. After an application is added to the tenant, add Azure AD as an identity provider (IDP) in Oracle Identity Cloud Service, and then configure single sign-on in Azure AD.

Before You Begin

Before you set up federation trust between Azure AD and Oracle Identity Cloud Service, prepare the following:

- You should have Azure subscription with a Contributor or greater privileged account. You must also have hands-on experience working with the Azure platform. This solution does not cover Azure IaaS and security best practices to create and run VMs and applications.
- Get Azure AD subscription and create a user with the Application Administrator or Global Administrator role in the Azure AD portal.
- You should know how to create a security group in Azure and also add users to it.
- User synchronization between Azure AD and PeopleSoft applications is a prerequisite for SSO to work. You can even use Oracle Identity Cloud Service feature to keep users synchronized between Azure AD and Oracle Identity Cloud Service. At least one attribute must match among all three systems. For example, user principal name (UPN or any other unique attribute) in Azure AD must match with the username or any other attribute in Oracle Identity Cloud Service, and that attribute must also match with the PeopleSoft application username.

Add Oracle Identity Cloud Service as a Gallery Application in Azure AD

You need admin credentials for your Oracle Identity Cloud Service tenancy to add as a gallery application in Azure AD.

You'll need the metadata file later in the steps. So go to your Oracle Identity Cloud Service tenancy-specific metadata URL and download the metadata. The URL looks like: `https://<your_tenancy>.identity.oraclecloud.com/fed/v1/metadata`.

1. In the Azure portal, select **Azure Active Directory** on the left navigation pane.
2. Select **Enterprise applications** in **Azure Active Directory**.
3. Select **New Application**.
4. Navigate to **Add from the gallery** and enter "Oracle Identity Cloud Service for PeopleSoft" in the search box. Select the matching application from the search results and add your application.
5. Select your application to configure single sign-on and under **Manage**, navigate to **Single sign-on** on the left pane.
6. Select **SAML** as the single sign-on method.
7. In the **Set up Single Sign-On with SAML - Preview** page, navigate to the **Basic SAML Configuration** section and click **Upload metadata file**.
8. Select the Oracle Identity Cloud Service metadata file that you downloaded earlier and then click **Add**.
9. In the **Sign-on URL** properties box enter the Oracle Identity Cloud Service myconsole URL.
10. Verify the SAML configuration. Add the Oracle Identity Cloud Service **Logout Url** if it's missing. In the **User Attributes & Claims** section, keep the default values.
11. In the **SAML Signing Certificate** section, click **Download** next to **Federation Metadata XML** to download the Azure AD federation metadata file.
    This application provides a SAML 2.0 federation link between Azure AD and Oracle Identity Cloud Service, but PeopleSoft application users should see only the PeopleSoft application in the **My Apps** portal.
12. If you want to hide the application in the **My Apps** portal, set the **Visible to users?** property to **No**.

Add Azure AD as an Identity Provider in Oracle Identity Cloud Service

When you add an identity provider, you'll import the metadata content of the identity provider, which you downloaded while adding the gallery application. Make sure that you have the metadata XML file or the URL readily available.

1. Log in to the Oracle Identity Cloud Service admin console.
2. Navigate to **Security**, select **Identity Provider** and then add an Identity Provider.
3. In the **Add Identity Provider** wizard, enter a name and click **Next**.
4. Import the **Azure AD Federation Metadata XML** file, which you downloaded while adding your application to the gallery.
5. In the **Configure** pane of the wizard, use the default value for **Requested NameID Format**. The value for **Identity Provider User Attribute** should be `Name ID`.
6. Set the value for Oracle Identity Cloud Service **User Attribute** to `Primary Email Address` or to any other attribute in Identity Cloud Service that might hold the user principal name in Azure AD.
7. Set up an IDP policy and add Webgate-App created earlier to use Azure AD for authentication.
   a. In the navigation pane, click **Security**, and then click **IDP Policies** to add.
   b. In the wizard, enter the name for the policy, and then click **Next**.
   c. Click **Assign**, select **Azure AD IDP** from the list, and then exit the wizard. You can assign more than one application that might use this IDP.

Complete Single Sign-On Configuration in Azure AD

Complete the single sign-on configuration to establish a connection between Oracle Cloud Infrastructure and Azure AD.

1. Sign in to the Azure portal.
2. Create a security group and give a name. For example, `oracle-Users`.
3. Create a test user by navigating to **Azure Active Directory** and selecting **Users** and then create a user.
4. Add the user to the security group.
5. Assign the group to the Oracle Identity Cloud Service SSO application. For example, the Oracle-Users group contains all the users who might access a PeopleSoft application through Oracle Identity Cloud Service.
6. Open the Oracle Identity Cloud Service admin console.
   For testing purposes, you can either create a user in Oracle Identity Cloud Service manually or synchronize Azure AD users in Oracle Identity Cloud Service. The users should be created or synchronized such that a user principal name in Azure AD matches the user's primary email address (or some other attribute) in Oracle Identity Cloud Service. For example, joe.smith@example.com would be the user's principal name in Azure AD and the Oracle Identity Cloud Service primary email address.
7. In Azure AD, navigate to the IDCS-SSO enterprise application and test single-sign on by using the test account.

Previous Page
Next Page