Oracle® Cloud

Configuring Single Sign-On for Oracle Enterprise Performance Management Cloud

In this Document

- Overview
- Configuring Single Sign-On Between EPM Cloud and Oracle Fusion Cloud
- Configuring Single Sign-On Between EPM Cloud and NetSuite

Overview

Single Sign-On (SSO) enables users belonging to a Security Assertion Markup Language 2 (SAML2) compliant identity provider to access multiple services offered by Oracle service providers such as Oracle Enterprise Performance Management Cloud, NetSuite, and Oracle Fusion Cloud. Users use their corporate credentials to authenticate once; for example, to an EPM Cloud instance, and then seamlessly access other configured service providers such as Oracle Fusion Cloud or NetSuite without being challenged for credentials.

You may use any SAML2.0 identity provider, for example, Oracle Identity Federation, Microsoft Active Directory Federation Services 2.0+, Okta, Ping Identity PingFederate, and Shibboleth Identity Provider, to establish SSO.

See Managing Oracle Single Sign-On *in Administering Oracle Cloud Identity Management* for information on how users can access multiple Oracle Cloud services using one set of credentials.

Configuring Single Sign-On Between EPM Cloud and Oracle Fusion Cloud

This section lists the steps to establish SSO between Oracle Enterprise Performance Management Cloud and Oracle Fusion Cloud deployments that use Oracle Identity Federation as the identity provider.

Prerequisites

- The identity provider must be SAML2 compliant.
- User accounts must exist in the Oracle Fusion Cloud identity store, and the EPM Cloud identity domain. Both must be configured for SSO.

If you use an identity provider such as Okta, instead of the Oracle Identity Federation of Oracle Fusion Cloud, you must configure your users in the identity provider as well.

SSO access between Oracle Fusion Cloud and EPM Cloud is permitted only for users who have an account in the identity store of Oracle Fusion Cloud and EPM Cloud identity domain.

Configuring Oracle Fusion Cloud for SSO

The procedures in this section set up SSO between Oracle Fusion Cloud and the organization's identity provider. The configuration process involves these steps:

- Configuring Oracle Fusion Cloud for SSO Using Oracle Identity Federation
- Creating Oracle Fusion Cloud Users in Oracle Identity Federation

Configuring Oracle Fusion Cloud for SSO Using Oracle Identity Federation

Open a service request with Oracle Support to configure Oracle Identity Federation as the identity provider for SSO with Oracle Fusion Cloud. Oracle imports the required metadata to enable Oracle Fusion Cloud to work with Oracle Identity Federation.

Note:

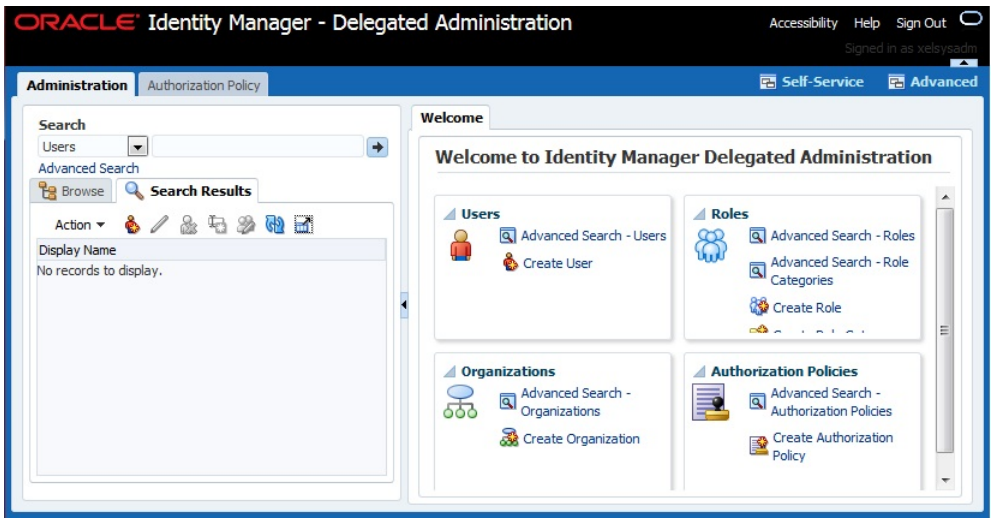
Be sure to provide the metadata of your identity provider in the service request, especially if you are not using the Oracle Identity Federation of Oracle Fusion Cloud as the identity provider. In this scenario, Oracle will provide the metadata of Oracle Fusion Cloud service provider to your identity provider administrator to import it into your identity provider.

Creating Oracle Fusion Cloud Users in Oracle Identity Federation

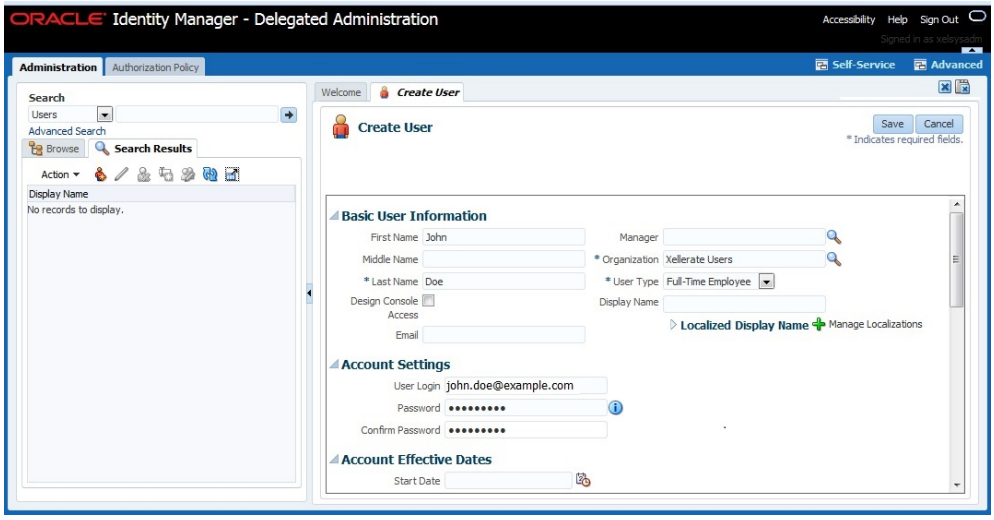
In the Oracle Identity Federation that supports Oracle Fusion Cloud, create an account for each user who needs SSO access to Oracle Fusion Cloud. You can create users by importing user details from a file or by accessing the Oracle Identity Management (OIM) console of the Oracle Identity Federation that supports Oracle Fusion Cloud.

To create a user in Oracle Identity Federation of Oracle Fusion Cloud:

1. Access the OIM console and sign in by entering the user ID and password of an OIM administrator.
2. Click **Administration**, and then **Create User**.



3. Enter basic user information such as first name and last name.
4. Select **Xellerate Users** in organization name.
5. Select a user type.
6. Specify a login name (for example, the email id) and password for the user.



Configuring EPM Cloud for SSO

Configuring Oracle Enterprise Performance Management Cloud for SSO involves these steps:

- Enabling SSO
- Creating EPM Cloud Users and Assigning Roles

Enabling SSO in EPM Cloud

Identity Domain Administrators use My Services to enable SSO for a service instance.

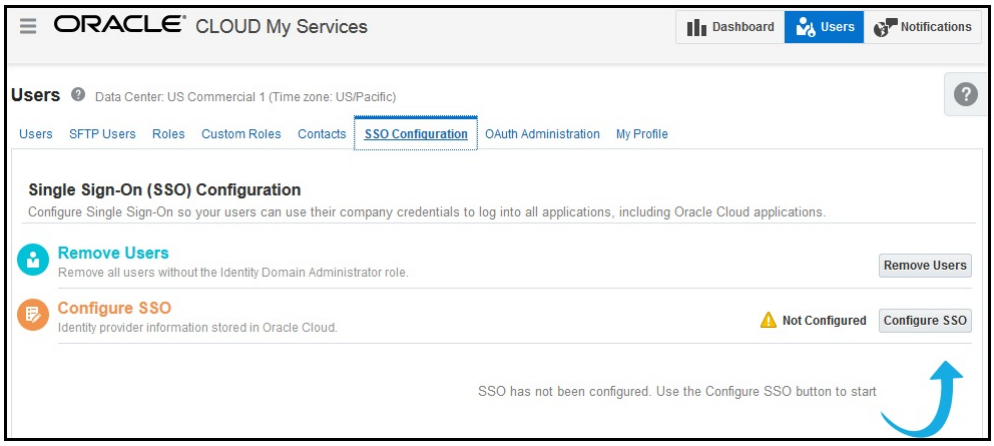
To enable SSO for an Oracle Enterprise Performance Management Cloud instance:

1. Go to the Oracle Cloud website (`http://cloud.oracle.com`), and sign in to your service as an Identity Domain Administrator.

   Oracle Cloud My Services portal opens.

2. Click **Users**.

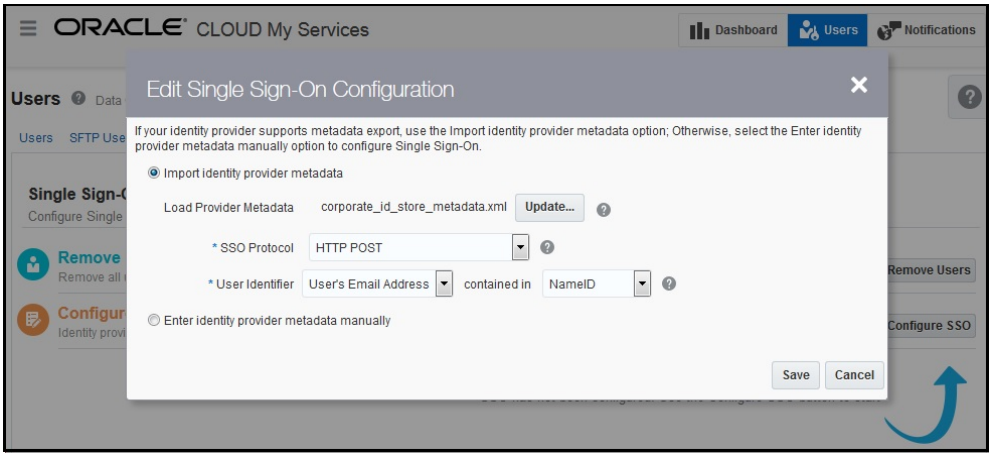
3. Click **SSO Configuration**.



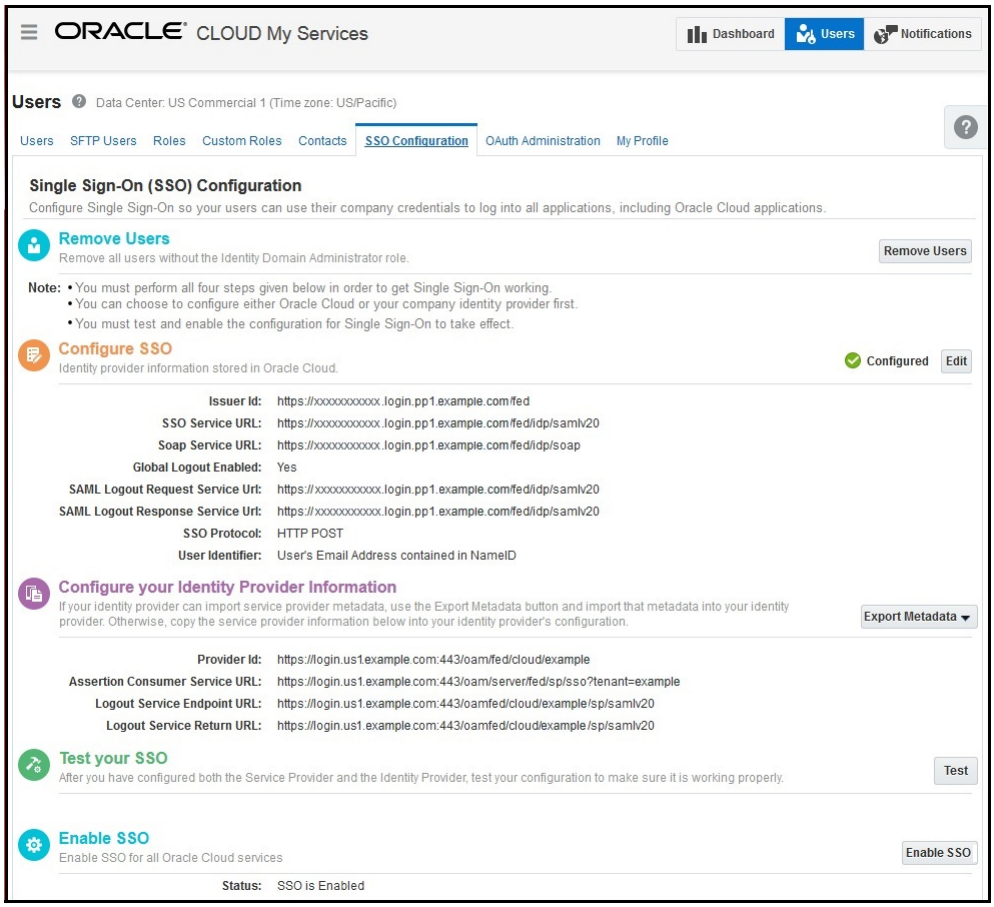
4. Click **Configure SSO**.

   See Configuring Oracle Cloud as the Service Provider in *Administering Oracle Cloud Identity Management*.

5. In **Edit Single Sign-On Configuration**, enter the required information to import identity provider metadata, and then click **Save**. See the following image for an example.



6. Click **Test**.

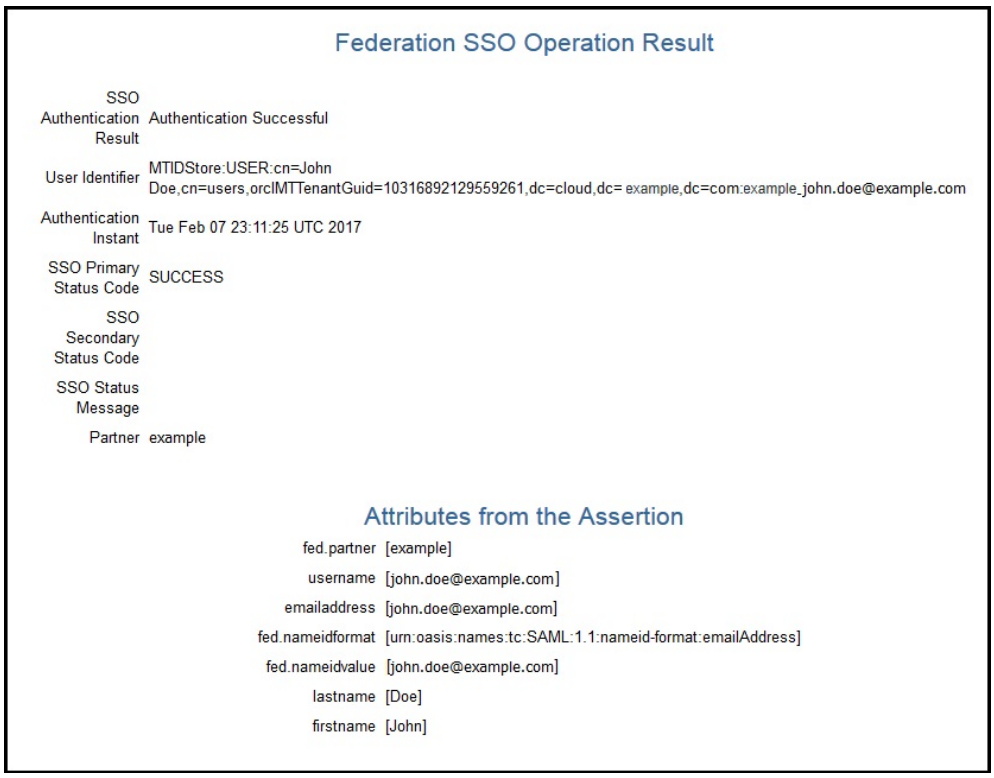


7. In **Initiate Federation SSO**, click **Start SSO**.

   Oracle Fusion Cloud Sign In screen is displayed.

8. Enter the user ID and password of a user available in the identity provider, and then click **Sign In**.

   The Federation SSO Operation Result screen, which indicates whether the SSO was successful, is displayed in a new tab.. SUCCESS is displayed as the SSO Primary Status Code if EPM Cloud has successfully paired with the Oracle Fusion Cloud' Oracle Identity Federation.



9. On Single Sign-On (SSO) Configuration screen, click **Enable SSO**.

10. Click **OK**.

11. Click **Export Metadata** to export the metadata of the service provider (EPM Cloud). An administrator must import this metadata into the identity provider.

Creating EPM Cloud Users and Assigning Roles

In the identity domain that supports the Oracle Enterprise Performance Management Cloud service instance, create and provision an account for each user who needs SSO access to EPM Cloud.

The Identity Domain Administrator can create users individually or use an upload file containing user data to create many users at once. See these topics in *Getting Started with Oracle Cloud*:

- Creating a User and Assigning a Role
- Importing a Batch of User Accounts

Testing the SSO Configuration

Test the SSO configuration by accessing Oracle Fusion Cloud and then navigating to Oracle Enterprise Performance Management Cloud, and vice versa.

To verifying SSO between Oracle Fusion Cloud and EPM Cloud:

1. Sign in to the EPM Cloud that is configured for SSO. For example, use a URL similar to the following to access an Oracle Planning and Budgeting Cloud instance:

   `https://<servicename>-<identity_domain>.pbcs.<dc>.oraclecloud.com/workspace`

2. Enter your identity domain, and then click **Go**.

   Oracle Fusion Cloud Sign In screen is displayed.

3. Enter the credentials of a user (for example, `john.doe@example.com`) that you created in the Oracle Identity Federation of Oracle Fusion Cloud, and then click **Sign In**.

   The EPM Cloud resource that you requested is displayed.

4. From a different browser window or tab, access the URL of an Oracle Fusion Cloud.

   The requested resource is displayed without going through a sign in process.

5. Sign out of the Oracle Fusion Cloud resource.

   You are signed out from Oracle Fusion Cloud and fromEPM Cloud.

   Oracle Fusion Cloud Sign In screen is displayed.

6. Close the browser.

7. Start a new browser session and access an Oracle Fusion Cloud resource.

   Oracle Fusion Cloud Sign In screen is displayed.

8. Sign in using the credentials (for example, `john.doe@example.com`) that you previously used to test EPM Cloud SSO.

   The Oracle Fusion Cloud resource that you requested is displayed.

9. From a different browser window or tab, access the URL of an EPM Cloud resource; for example, an Oracle Planning and Budgeting Cloud instance.

   The screen to specify an identity domain is displayed.

10. Enter the identity domain, and then click **GO**.

Note:

If you work within this EPM Cloud identity domain most of the time, select **Remember my choice**. In the future, you will not be prompted to enter an identity domain when you access the service.

The requested EPM Cloud resource is displayed without going through a sign in process.

Configuring Single Sign-On Between EPM Cloud and NetSuite

This section lists the steps to establish SSO between Oracle Enterprise Performance Management Cloud and NetSuite deployments using user identities stored in an identity provider such as Okta.

Note:

The procedures in this section have been tested using Okta as the identity provider that stores user identities. You can use any SAML 2.0 compliant identity provider to enable SSO.

SSO access between NetSuite and EPM Cloud is permitted only for users who have accounts in the user directories of NetSuite, Okta, and EPM Cloud identity domain.

Prerequisites

- All users of NetSuite and EPM Cloud are available in the SAML 2.0 compliant identity provider that you are using.
- EPM Cloud users who need SSO access were created and provisioned in the identity domain that services EPM Cloud. For detailed instructions to create and provision users, see Adding Users and Assigning Roles in *Getting Started with Oracle Cloud*.

  Before starting the SSO configuration process, make sure that only the users who need SSO access can sign in to EPM Cloud.

  After enabling SSO, all EPM Cloud users will be able to navigate to NetSuite without being challenged for credentials. For these users, functional access is controlled by NetSuite roles and permissions.
- Users who need SSO access have been created and provisioned in NetSuite. For detailed information, see NetSuite documentation.

  After enabling SSO, only the users NetSuite who have been granted a NetSuite role that assigns `SAML Single Sign-on` access will be able to navigate to EPM Cloud without going through an additional sign in process.

  Before starting the SSO configuration process, make sure that all users who need SSO access to EPM Cloud can access and work in NetSuite.

Tasks to Complete in Okta

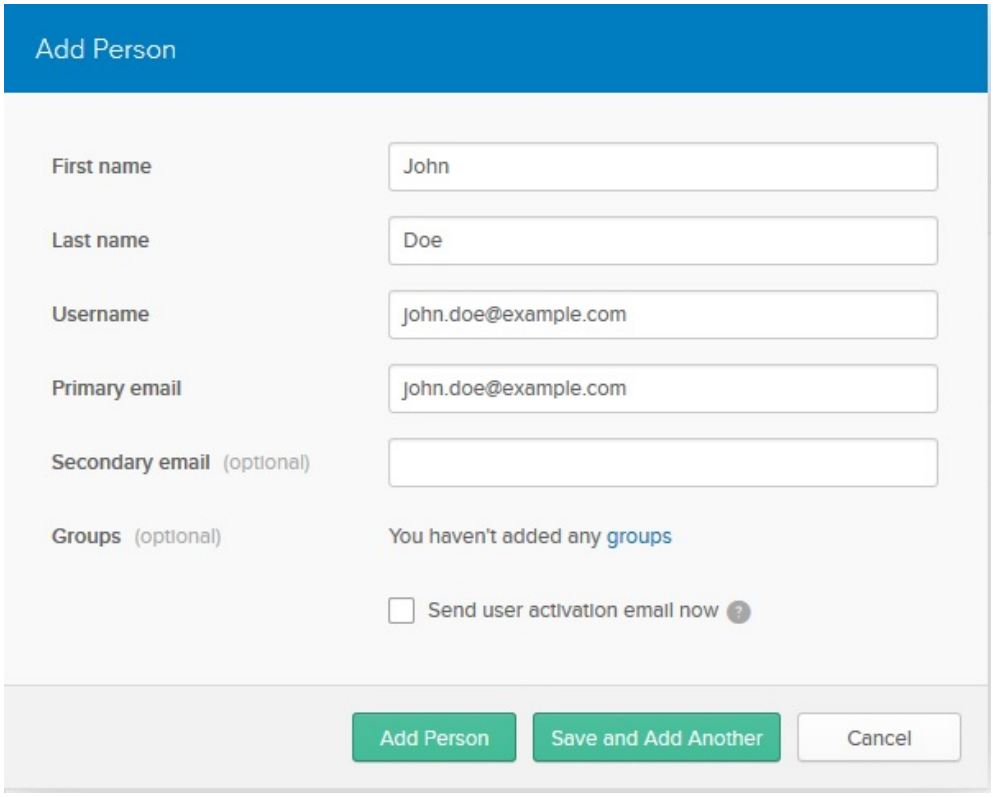
- Creating Users in the Identity Provider
- Add NetSuite as an Application
- Add EPM Cloud as an Application in the Identity Provider

Creating Users in the Identity Provider

This document assumes that you created and activated all users who need SSO access between NetSuite and Oracle Enterprise Performance Management Cloud resources as users in your organization's identity provider.

To create and activate users in Okta:

1. Sign in to the Admin dashboard as a user with Okta Administrator privileges.
2. Click **Admin**.
3. On **Dashboard**, click **Add People** under **Shortcuts**.
4. Click **Add Person**.
5. Enter user information such as first name, last name, user name (must be an email ID), and the primary email ID if it is not identical to the username.



6. Click **Add Person** to create the user and close the screen or **Save and Add Another**
7. Repeat the preceding procedure to create all the users who needs SSO access between NetSuite and EPM Cloud.
8. Activate the users that you created.
   a. On **People**, click **Pending Activation** under **Filters**.
   b. Click **Bulk activate**.
   c. Click **Activate All**.
   d. On **Activate People**, click **Activate**.

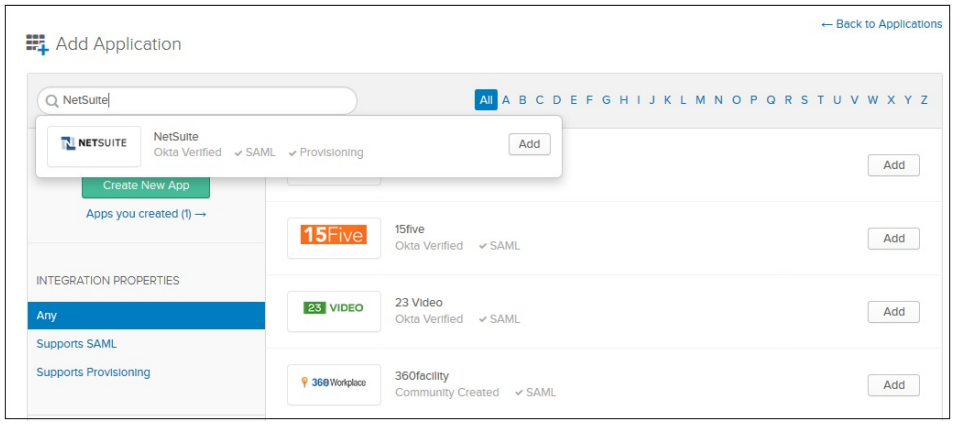
Okta sends an activation email to each user.

Add NetSuite as an Application

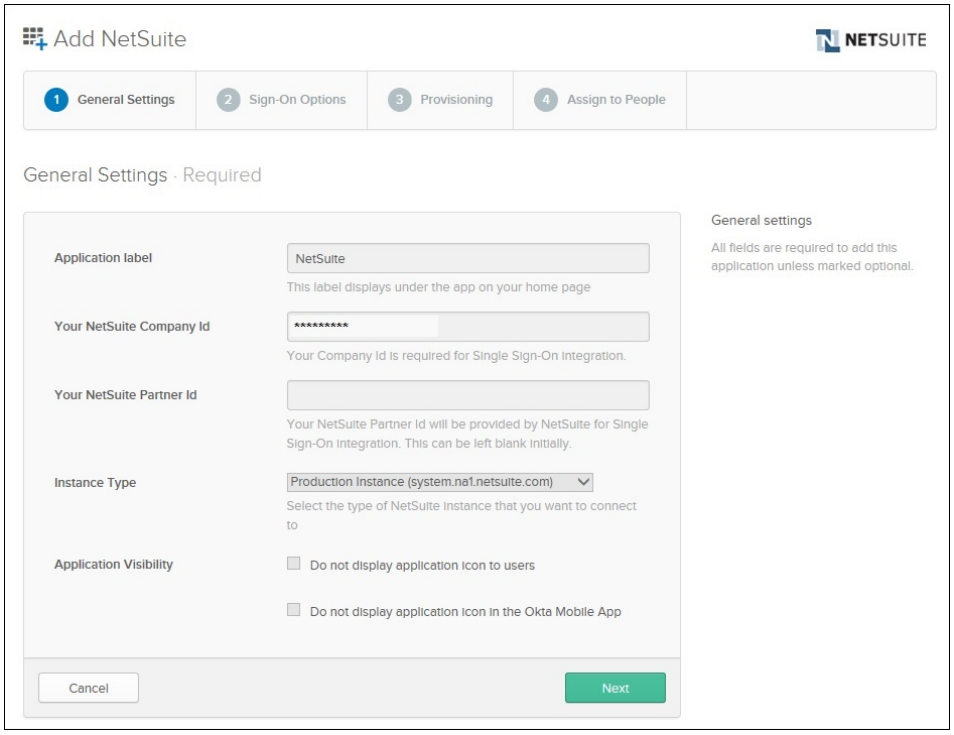
In this step, you add NetSuite as an application in the identity provider, and provision the users who can use SSO.

To add NetSuite as an application using Okta Admin Console:

1. Sign in to the Admin dashboard as a user with Okta Administrator privileges, and then click **Admin**.
2. Add NetSuite as an Application.
   a. Click **Applications**, and then **Add Application**.
   b. In **Add Application**, search for NetSuite.
   c. Select **NetSuite** and click **Add**.

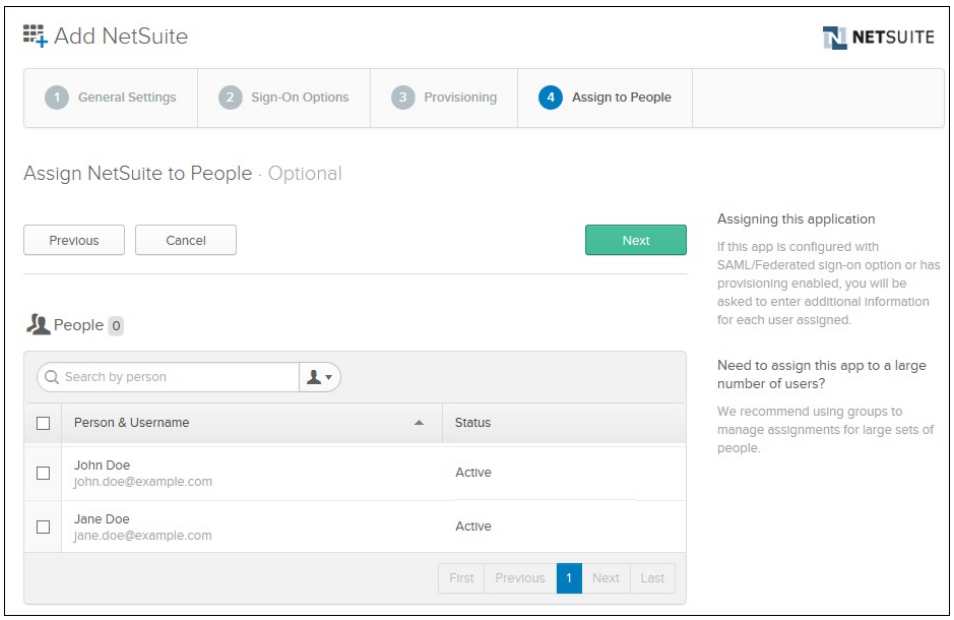


   d. Specify General Options for NetSuite integration, and then click **Next**. You must initially specify, at a minimum, the company id and the instance type. Contact your NetSuite administrator for the company Id and instance type to use.



e. On **Sign-On Options** and **Provisioning Settings**, click **Next**.

f. On **Assign NetSuite to People**, select all the users who need SSO access between NetSuite and Oracle Enterprise Performance Management Cloud, and then click **Next**.

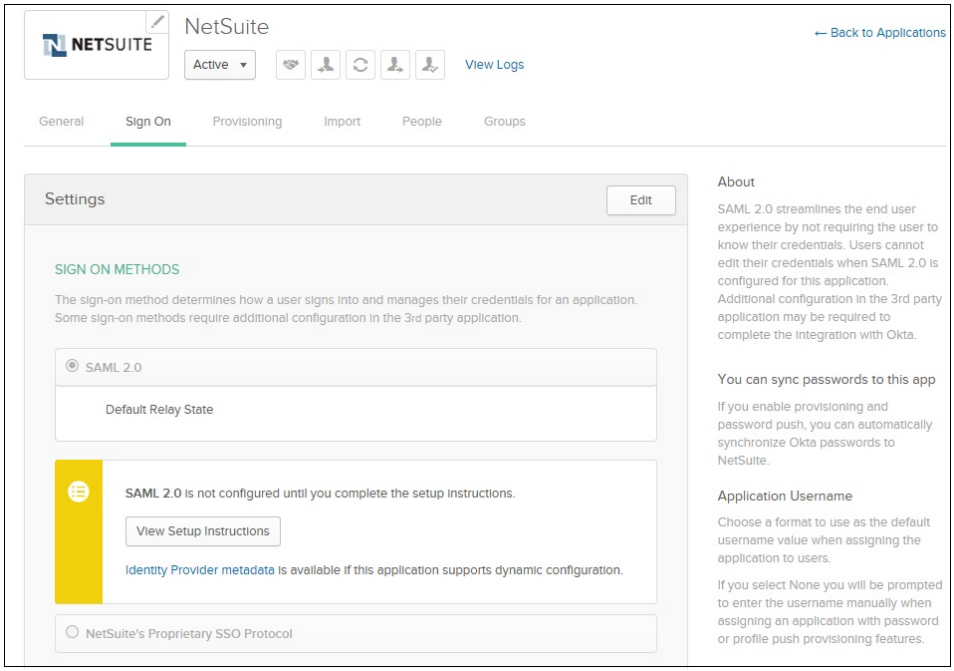


g. On **Assign NetSuite to People Optional**, click **Done**.

3. Obtain pre-populated Okta URLs and instructions for configuring SAML2 for NetSuite.

   a. Click **Applications**, and then the NetSuite application that you added in the preceding step.

   b. Click **Sign On**, and then **View Setup Instructions**.



   A web page that details instructions to configure SAML2 for your NetSuite instance and the URLs to use during the configuration process is displayed. You can also access the setup instructions, without the pre-populated URLs, from this URL: http://saml-doc.okta.com/SAML_Docs/How-to-Configure-SAML-2.0-for-Netsuite.html.

   c. Copy the following information from the web page to a local file. You will need this information to configure SAML for NetSuite.

   - **Logout Landing Page**: see item 14 in the web page.
   - **Identity Provider Login Page**: see item 15 in the web page

   d. Click **Identity Provider metadata** and save the Okta SAML metadata in a TXT file, for example, `okta_netsuite_metadata.txt`.

   You need this metadata to configure NetSuite SAML. See Configure SAML in NetSuite.

Add EPM Cloud as an Application in the Identity Provider

In this step, you add Oracle Enterprise Performance Management Cloud as an application in the identity provider and provision the users who can use SSO.

To add EPM Cloud as an application using Okta Admin Console:

1. Sign in to the Admin dashboard as a user with Okta Administrator privileges, and then click **Admin**.
2. Add EPM Cloud as an application.
   a. Click **Applications**, and then **Add Application**.

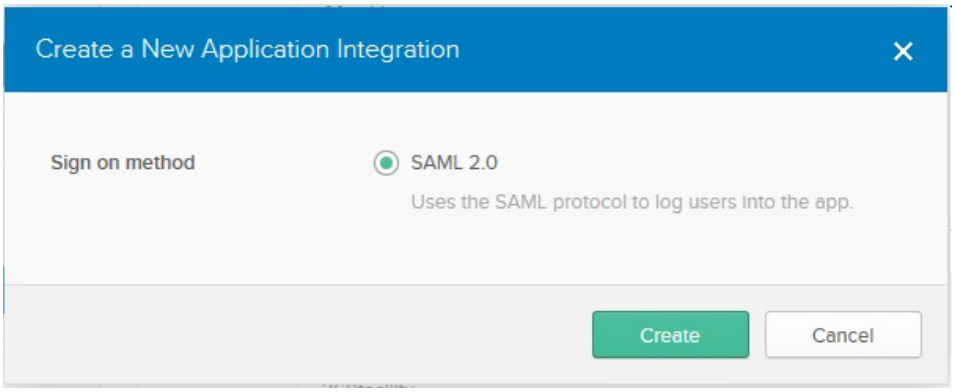
Note:

Because EPM Cloud is not yet integrated in Okta, you must add it as a generic application.

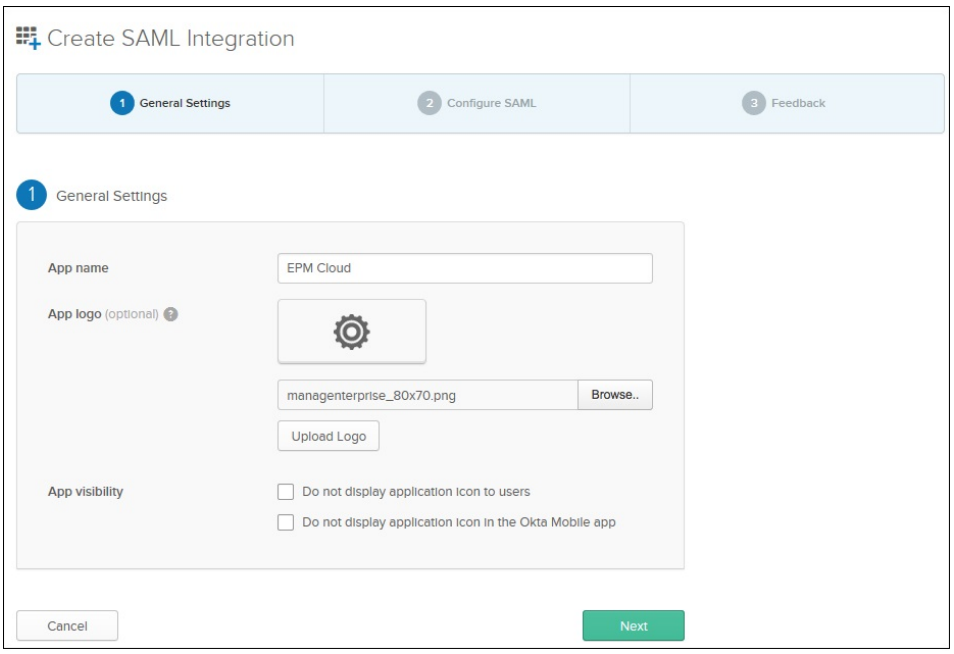
A search will show on-premises Oracle Hyperion EPM, but do not select it.

---

   b. Click **Create New App**.
   c. In **Create a New Application Integration**, click **Create**.



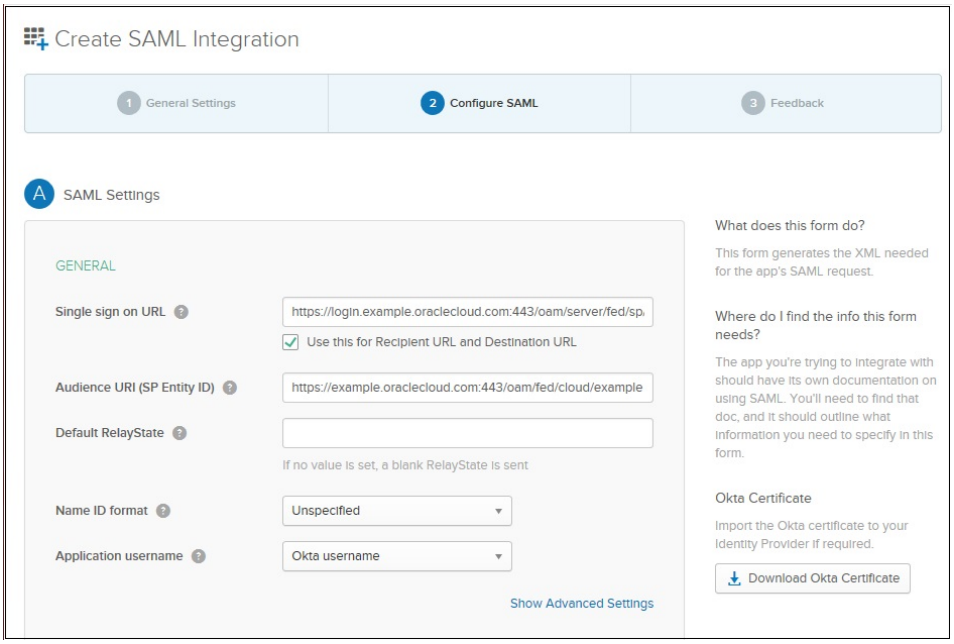
   d. On **General Settings** enter an application name (for example, EPM Cloud) and select an optional application logo, and then click **Next**.



e. On **Configure SAML**, enter the following information. Contact your Service Administrator for this information.

- **Single sign on URL**: The URL for signing in to an EPM Cloud instance. This is the location where the SAML assertion is sent with an HTTP POST.
- **Audience URI (SP Entity ID)**: The intended audience of the SAML assertion; usually the Entity ID of the application.

Also, ensure that **Use this for Recipient URL and Destination URL** is selected.



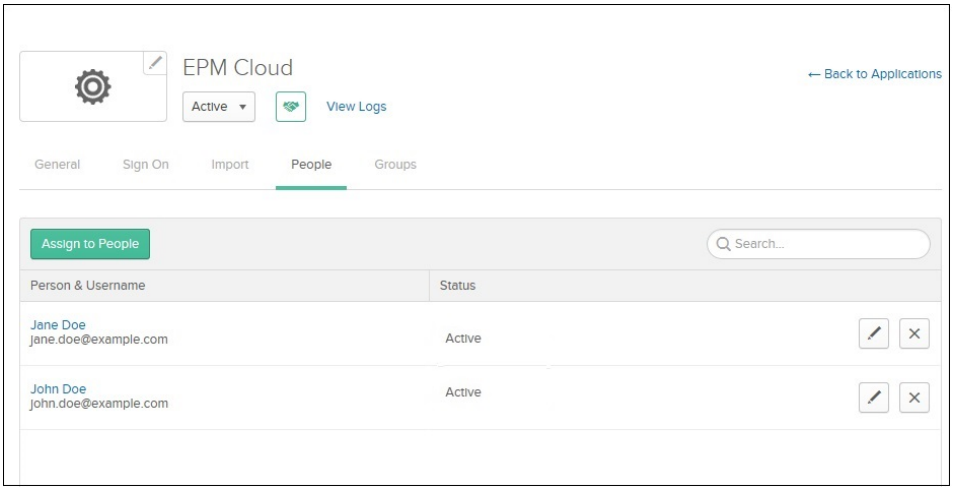
f. Click **Next**.

g. On **Feedback**, select the feedback to provide to Okta, and then click **Finish**.

h. Click **People**, and then **Assign to People**.

i. In **Assign EPM Cloud to People**, click **Assign** for each user who needs SSO access.

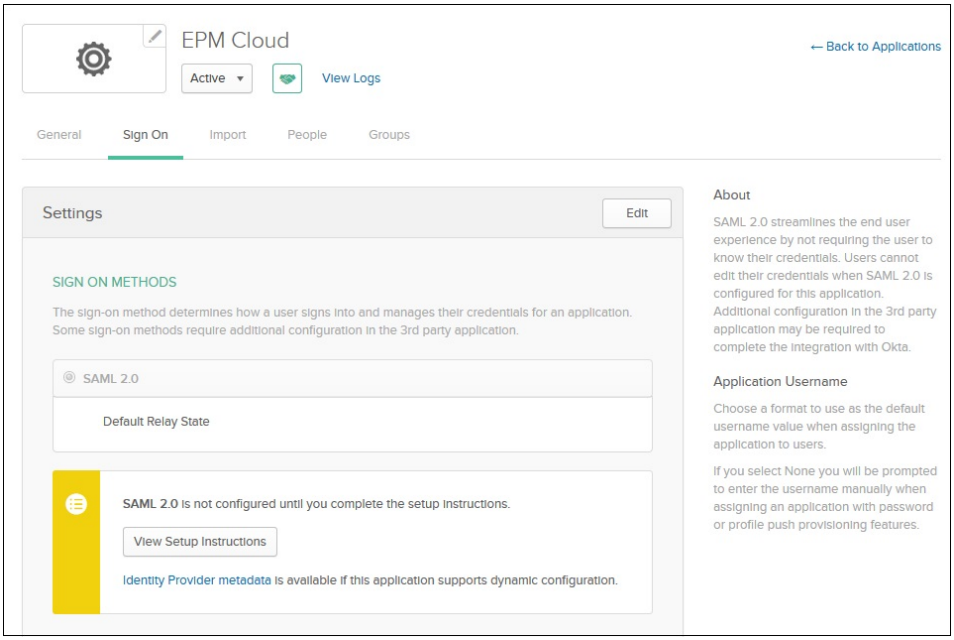
Click **Save and Go Back** to return to **Assign EPM Cloud to People**. Click **Done** when you are finished.



j. On **Assign NetSuite to People Optional**, click **Done**.

3. Obtain Okta identity provider metadata.

   a. Click **Sign On**, and then **Identity Provider metadata**.



   b. Save the Okta SAML metadata in an XML file, for example, `okta_epm_metadata.xml`.

      An Identity Domain Administrator must import this metadata into the identity provider of EPM Cloud while configuring it for SSO. See Configuring SSO in EPM Cloud.

Configure SAML in NetSuite

To configure SAML for NetSuite:

1. Sign into NetSuite as an Administrator.
2. Click **Setup**, and then **Setup Manager**.
3. Configure SAML 2.0 for NetSuite using the instructions available in How to Configure SAML 2.0 for Netsuite.

   You need the following information, which was saved locally while creating NetSuite application in Okta. See Step 3 in Add NetSuite as an Application.

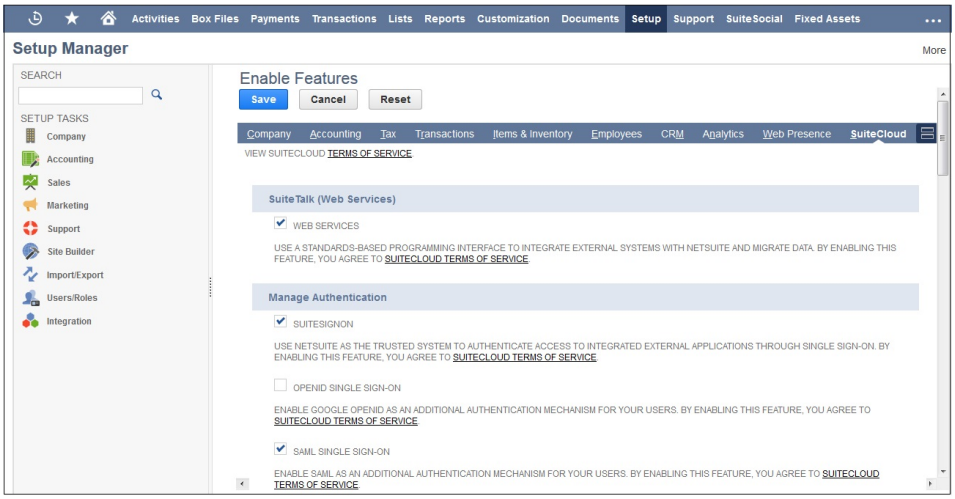
   - Logout Landing Page URL
   - Identity Provider Login Page URL
   - Name of the Okta identity provider metadata file, for example,`okta_netsuite_metadata.txt`

4. Enable NetSuite SAML SSO.

   a. In **Setup Manager**, click **Enable Features** under Company Setup Tasks.

   b. Click **SuiteCloud**.

   c. In the **Manage Authentication** section, select **SAML SINGLE SIGN-ON** . You will need to scroll down to locate this section.



   d. Click **Save** at the bottom of the SuiteCloud page.

5. Click **Save** to save the changes you made in Setup Manager.

6. Create a SAML role in NetSuite that allows users to perform SSO.

Note:

SSO in NetSuite is controlled at the SAML role level. You must assign a SAML role to each NetSuite user who needs SSO access.

A NetSuite Administrator creates SAML roles. See NetSuite documentation for information.

---

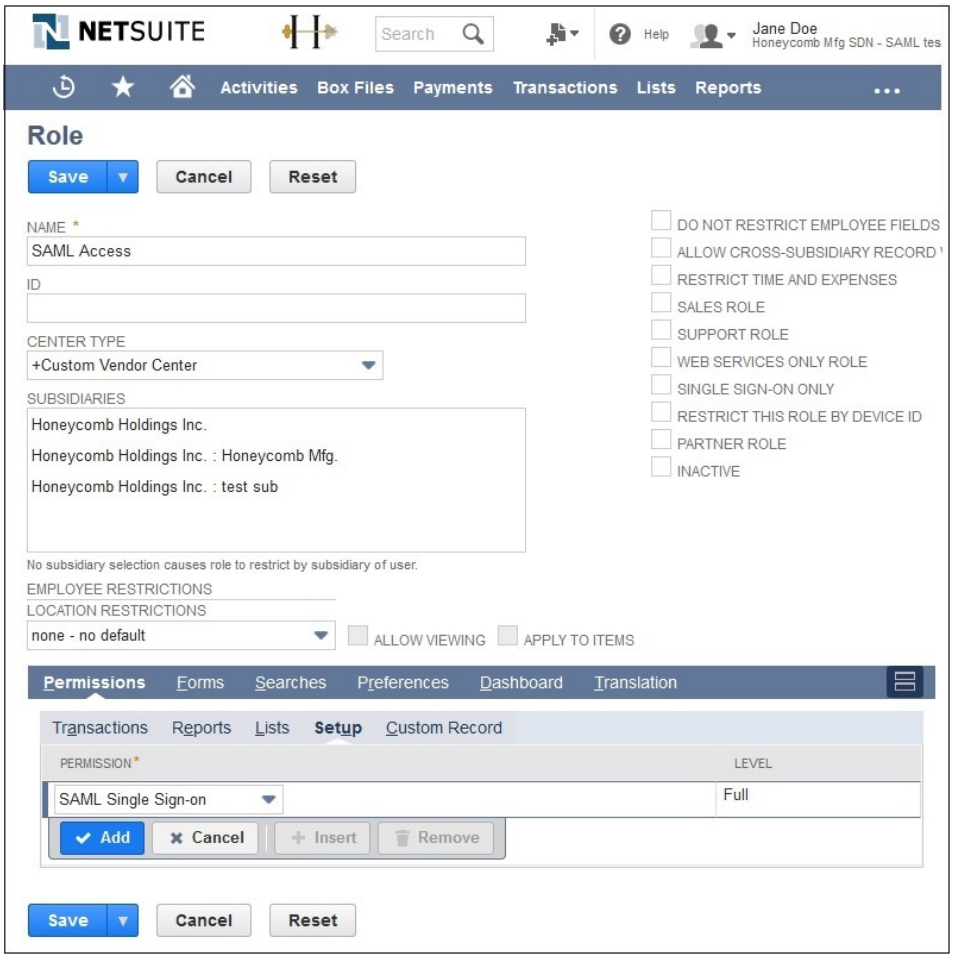
   a. Click **Setup**, then **Users/Roles**, then **Manage Roles**, and then **New**.

   b. Enter a unique role name. To distinguish SAML roles from functional roles, you may prepend role names with SAML; for example, `SAML Access`.

   c. Scroll down, and then click **Permissions** and then **Setup**.

   d. From the list of permissions, select **SAML Single Sign-on**, and then click **Add**.

   e. Click **Save**.



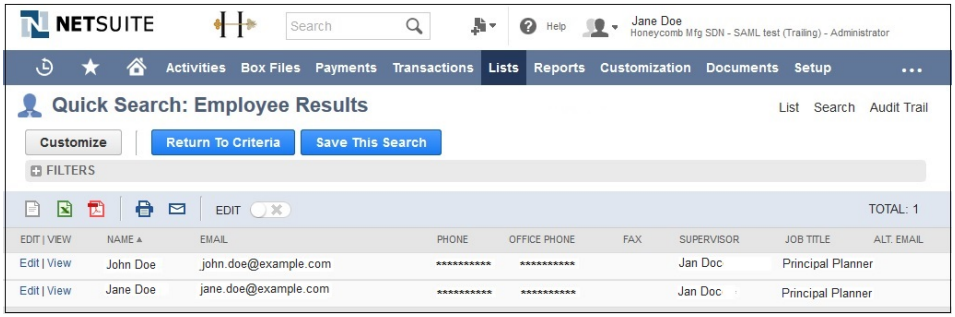
7. Provision NetSuite users with SAML role.

   a. Click **Lists**.

   b. In **Quick Search**, enter a search criterion such as email id or name of the user who is to be granted SAML role. You can use * (asterisk) as a wildcard to find all matching records.

   c. In **SEARCH FOR**, select the search information type, for example, employee to search only for employees that match the search criterion.

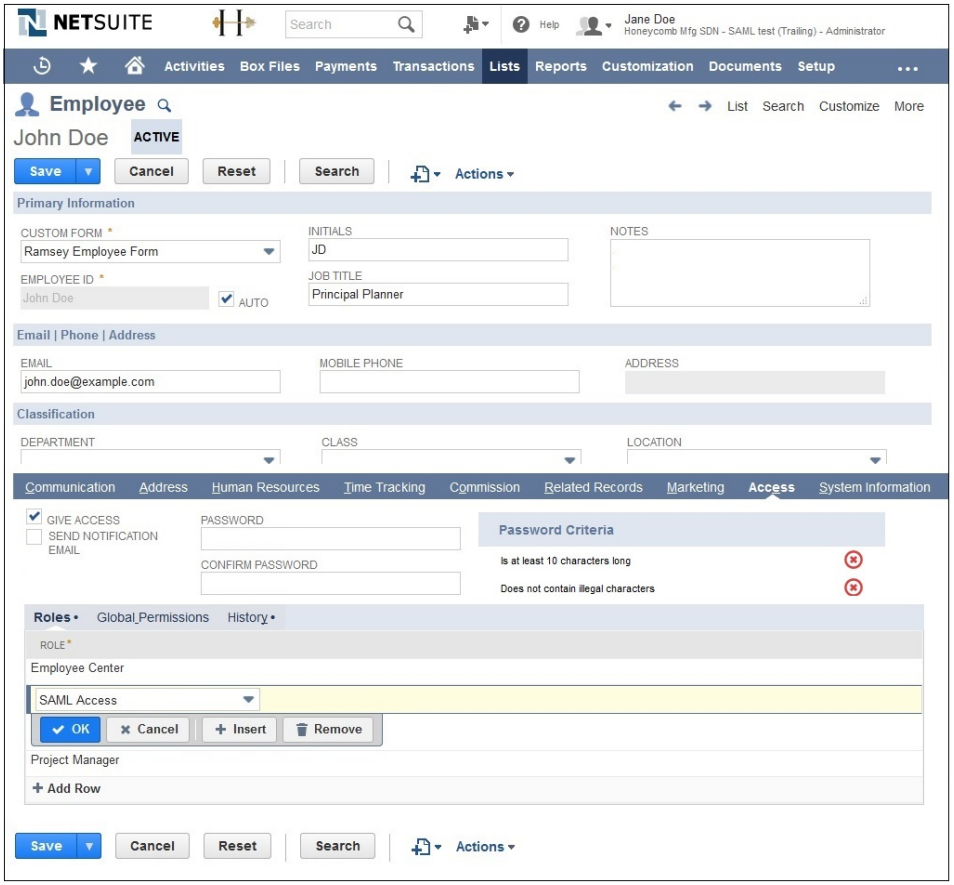
   d. Click **Search**.



e. In the Search results, click **Edit** in the row containing the record of the employee who is to be granted SAML role.

The employee record is displayed.

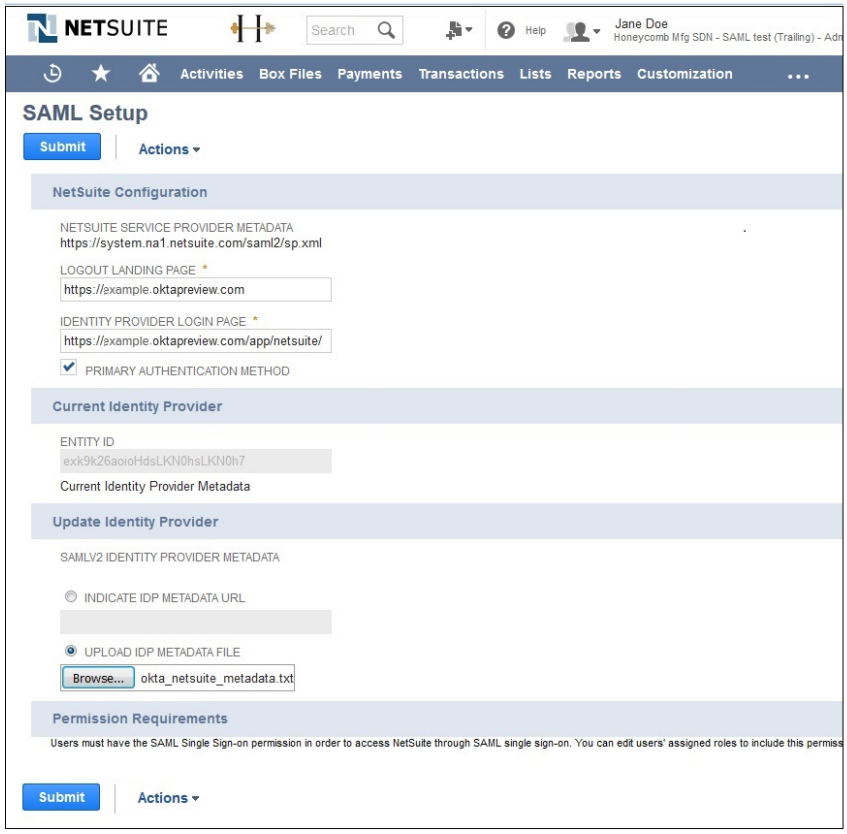
f. Scroll down and click **Access**, and then **Roles**.



g. On **Roles**, select the SAML role you want to assign; for example, the role that you created in the preceding step, and then click **OK**.

h. Click **Save** at the bottom of the screen.

8. Repeat the preceding step to provision additional users with SAML roles.
9. Import Okta metadata file. You created this file as a part of creating the NetSuite application in Okta. See Add NetSuite as an Application.
    a. Click **Setup**, then **Integration**, and then **SAML Single Sign-on**.



    b. Scroll down and then select **UPLOAD METADATA FILE**.
    c. Browse and select the file that contains Okta metadata file.
    d. Click **Submit**.

Configuring SSO in EPM Cloud

Identity Domain Administrators use My Services to enable SSO for a service instance.

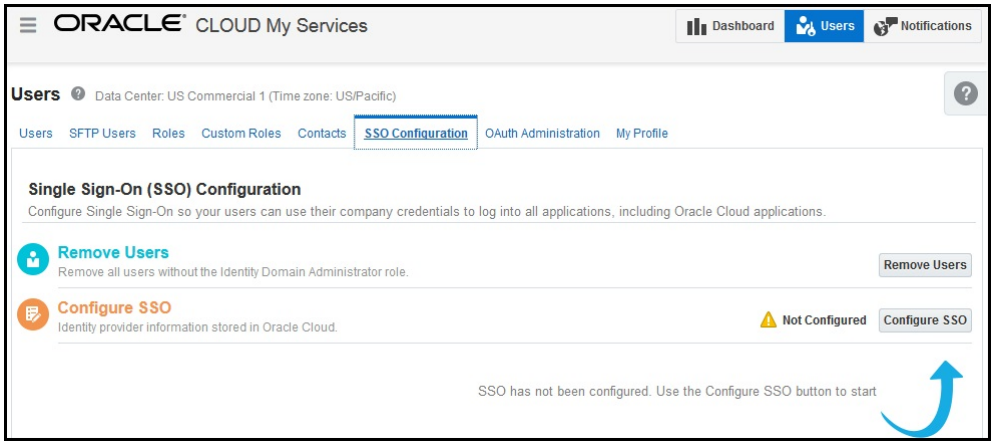
To enable SSO:

1. Go to the Oracle Cloud website (`http://cloud.oracle.com`) and sign in as an Identity Domain Administrator.

    Oracle Cloud My Services portal opens.

2. Click **Users**.

3. Click **SSO Configuration**.

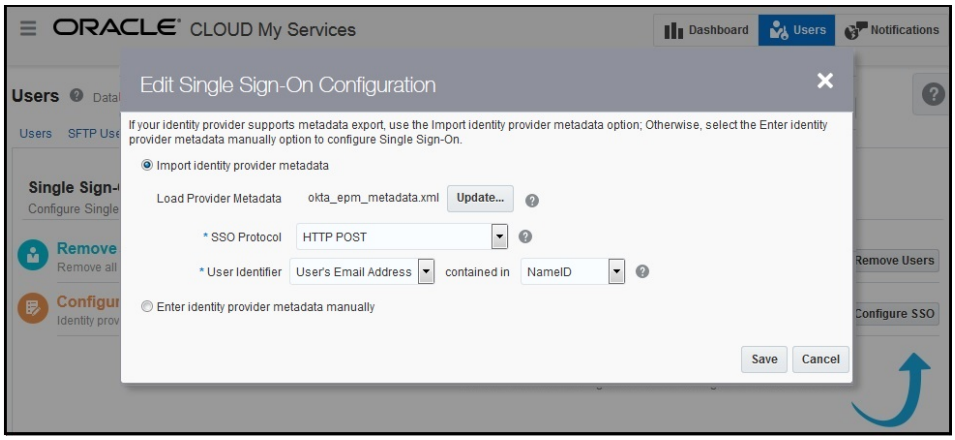


4. Click **Configure SSO**.

5. In **Edit Single Sign-On Configuration**, complete these steps:

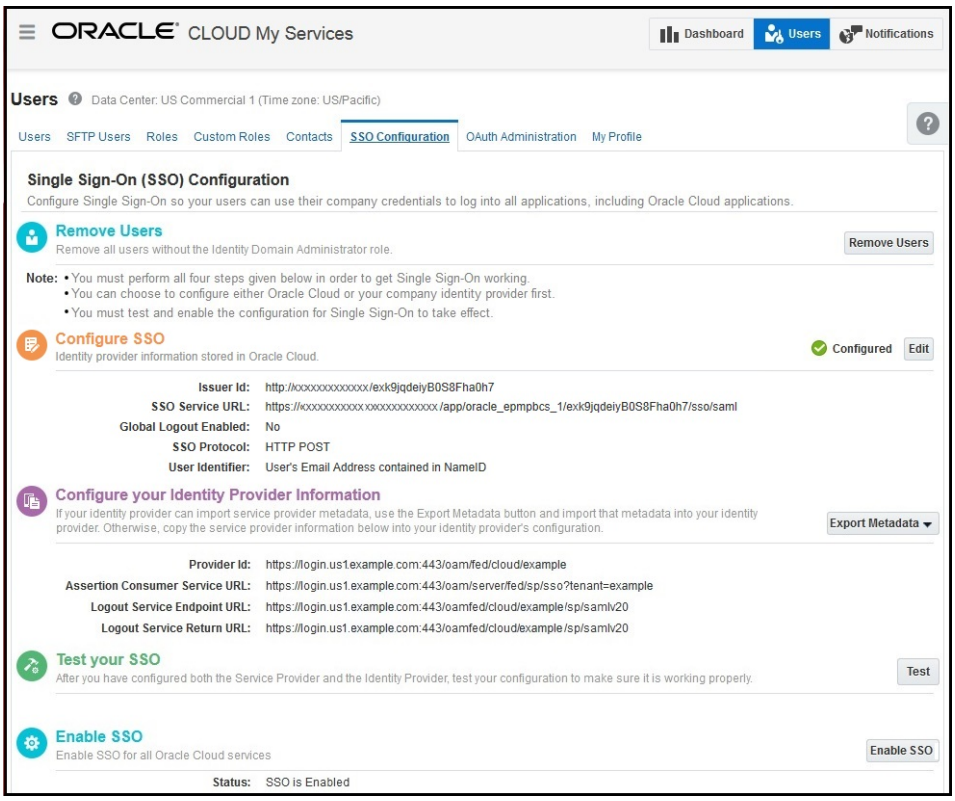
   a. Using **Browse**, select the metadata file that you created when you added Oracle Cloud as an application in Okta.

   b. Select a user identifier that uniquely identifies users who need SSO access. The value of the user identifier must point to the same unique user in Oracle Cloud, Okta, and NetSuite.



   c. Click **Save**.

      SSO Configuration screen displays identity provider Information



6. Click **Test**.
7. In **Initiate Federation SSO**, click **Start SSO**.
8. Enter the user ID and password of a user available in Okta, and then click **Sign In**.

   The Federation SSO Operation Result screen, which indicates whether the SSO was successful, is displayed in a new tab. SUCCESS is displayed as the SSO Primary Status Code if Oracle Enterprise Performance Management Cloud has successfully paired with Okta.

9. On Single Sign-On (SSO) Configuration screen, click **Enable SSO**.
10. Click **OK**.
11. If needed, create and provision EPM Cloud users.

    Identity Domain Administrators create and manage users from My Services while Service Administrators assign roles to them. See Adding Users and Assigning Roles in *Getting Started with Oracle Cloud*.

Creating EPM Cloud Users and Assigning Roles

Create and provision additional Oracle Enterprise Performance Management Cloud users if needed.

The Identity Domain Administrator can create users individually or use an upload file containing user data to create many users at once. See these topics in *Getting Started with Oracle Cloud*:

- Creating a User and Assigning a Role
- Importing a Batch of User Accounts

Additionally, ensure that only the users who need SSO access to NetSuite are present in the identity domain.

Testing SSO

To test the SSO configuration:

1. From a browser, connect to the Oracle Enterprise Performance Management Cloud URL.

2. Enter the name of the identity domain that you configured for SSO with NetSuite, and then click **Go**.

Note:

If you work within this identity domain most of the time, select **Remember my choice**. In future, you will not be prompted to enter an identity domain when you access the service.

---

3. In **Sign In To Oracle Cloud**, click **Remember my choice**, and then **Company Sign In**. to display the Okta sign in page.
4. Enter a user name; (for example, `john.doe@example.com`, and password that you created in Okta, and then click **Sign In**.

   The EPM Cloud resource is displayed.
5. From a different browser window or tab, access the NetSuite URL.

   The requested resource is displayed without going through a sign in process.
6. Sign out of NetSuite and EPM Cloud.
7. Close the browser.
8. Start a new browser session and access NetSuite.

   The Okta Sign In screen is displayed.
9. Sign in using the credentials (for example, `john.doe@example.com`) that you previously used to test EPM Cloud SSO.

   NetSuite is displayed.
10. From a different browser window or tab, access the EPM Cloud URL; for example, that of an Oracle Planning and Budgeting Cloud instance.

    The screen to specify an identity domain is displayed.
11. Enter the identity domain, and then click **GO**.

Note:

If you work within this identity domain most of the time, select **Remember my choice**. In future, you will not be prompted to enter an identity domain when you access the service.

---

12. In **Sign in to Oracle Cloud**, click **Company Sign In**

Note:

Select **Remember my choice** to not display the sign-in screen in the future.

The requested EPM Cloud resource is displayed without going through a sign in process.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Send feedback on this documentation to: epmdoc_ww@oracle.com

Follow EPM Information Development on these social media sites:

LinkedIn - http://www.linkedin.com/groups?gid=3127051&goback=.gmp_3127051

Twitter - http://twitter.com/hyperionepminfo

Facebook - http://www.facebook.com/pages/Hyperion-EPM-Info/102682103112642

Google+ - https://plus.google.com/106915048672979407731/#106915048672979407731/posts

YouTube - https://www.youtube.com/user/EvolvingBI