Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Identity Federation with Okta

Release 25.5
G47681-01
November 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation with Okta, Release 25.5

G47681-01

Contents

Notices

Preface

Purpose

This guide explains the steps to configure Identity Federation to set up OPERA Cloud Services single sign on (SSO) with customer identity provider. This document must be followed only if the customer identity provider is **Okta**.

Audience

This document is intended for OPERA Cloud Services application administrators.

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at the following URL:

https://iccp.custhelp.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

http://docs.oracle.com/en/industries/hospitality/

Revision History

Table Revision History

Date	Description of Change
November 2025	Initial Publication

1

Configuring Identity Federation in OCI IAM Identity Domain when using Okta as the Identity Provider

OPERA Cloud Identity Management provides the capability of identity federation by determining which customers can integrate their identity provider with OPERA Cloud to implement single sign on (SSO) with OPERA Cloud. Leveraging OPERA Cloud Identity Management's identity federation feature, customers can use their corporate credentials to log on to OPERA Cloud, which eliminates the necessity to separately manage users and their access to OPERA Cloud.

This document provides the steps to set up Okta as an IdP, with OCI IAM Identity Domain acting as SP. By setting up federation between Okta and OCI IAM Identity Domain, you enable users' access to OPERA Cloud Services using user credentials that Okta authenticates.

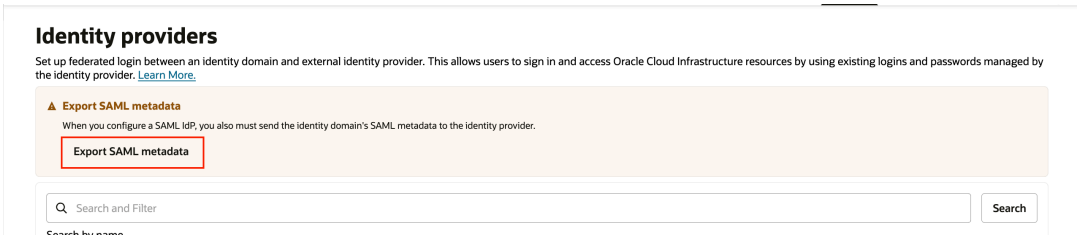
1. First, gather the information needed from OCI IAM.
2. Configure Okta as an IdP for OCI IAM.
3. Configure OCI IAM so Okta acts as IdP.
4. Create IdP policies in OCI IAM.
5. Test that federated authentication works between OCI IAM and Okta.

> **Note**
>
> Follow this document only if your identity provider is **Okta**.

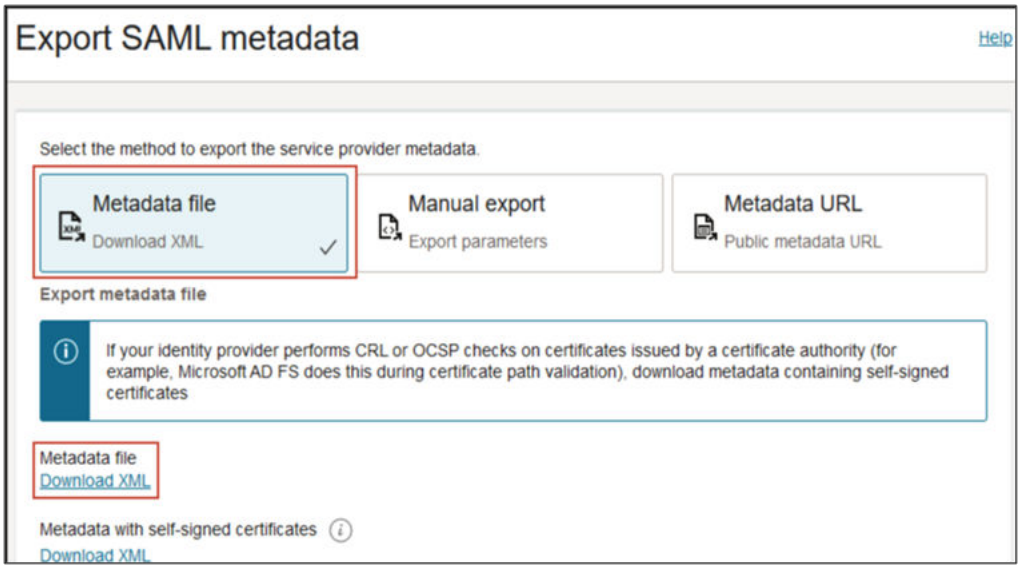
1. Download the SAML Metadata in OCI IAM Identity Domain

You need the IdP SAML metadata from your OCI IAM identity domain to import into the Okta application you create. OCI IAM provides a direct URL to download the metadata of the identity domain you are using. Okta uses the OCI domain URL to connect to OCI IAM.

1. Open a supported browser and enter the following Console URL: https://cloud.oracle.com.
2. Enter your Cloud Account Name, also referred to as your tenancy name, and click **Next**.
3. Select the identity domain to sign in to. This is the identity domain that is used to configure SSO, for example Default.
4. Sign in with your username and password.
5. Open the navigation menu and click **Identity & Security**. Under Identity, click **Domains**.
6. Select the Identity Domain in which you want to configure Okta Federation.
7. Click the **Federation** tab. Under Identity Providers, click **Export SAML metadata**.



8. Select the **Metadata file** option and click **Download XML**.



9. Return to the Identity Domain where you are configuring Okta provisioning. On the Identity Domain Details page, click **Copy** next to the Domain URL.
The Identity Domain ID is part of the domain URL: https://<IdentityDomainID>.identity.oraclecloud.com:443.

   Note the **Identity Domain ID** from the Domain URL. For example, if your domain URL is https://idcs-123456.identity.oraclecloud.com:443, then your Identity Domain ID is **idcs-123456**.

2. Create an Application in Okta for OCI IAM Identity Domain

> **Note**
>
> You can skip this step if the enterprise application for OCI is already created as part of Okta Integration with OCI IAM Identity Domain for user lifecycle.

Create an app in Okta and make note of the values you will need later.

1. In the browser, sign into Okta using the following URL where **<OktaOrg>** is the prefix for your organization with Okta: https://<OktaOrg>-admin.okta.com
2. In the left menu, click **Security** and choose **Applications** and then click **Browse App Catalog**.

3. Search for Oracle Cloud and select **Oracle Cloud Infrastructure IAM** from the available options.
4. Click **Add Integration**.
5. Under General settings, enter a name for the application, for example OCI IAM, and click **Done**.
6. Click the **Sign on** tab. Under the About section on the right side of the page, click **View SAML setup instructions** under SAML Setup.
7. Make a note of the following information:
   - **Identity provider issuer URI**
   - **SSO service URL**
   - **IdP logout request URL and IdP Logout Response URL**
   - **Signing certificate**: Click the provided link and **Save** the file as "okta.pem"

3. Configure Okta as an Identity Provider in OCI IAM Identity Domain

1. In the OCI Console, go to the Identity Domain in which you want to configure Okta Federation.
2. Click the **Federation** tab. Under Identity Providers, click the **Actions** menu and select **Add SAML IdP**.
3. Enter a name for the **SAML IdP**. For example, Okta. Click **Next**.
4. On the Exchange metadata page, ensure that **Enter IdP metadata - Enter Parameters manually** is selected.
5. Enter the following from step 7 in 2. Create an Application in Okta for OCI IAM Identity Domain.
   - For **Identity provider issuer URI**: Enter the **Entity/Issuer ID**.
   - For **SSO service URL**: Enter the **SingleSignOnService URL**.
   - For **SSO service binding**: Select **POST**.
   - For **Upload identity provider signing certificate**: Use the **.pem** file of the Okta certification.
6. On the Map User Identity page:
   - For **Requested NameId** format: Choose **None**.
   - For **Identity provider user** attribute: Choose **SAML assertion Name ID**.
   - For **Identity Domain user** attribute: Choose **UserName**.
7. Click **Next**.
8. Review and click **Create IDP**.
9. Click the newly created Identity Provider to open the IdP Details page.
10. Click the **Actions** menu and click **Activate**.
11. Under **Service Provider Metadata**, scroll down and click **Download** next to **Service provider signing certificate** and save it.

4. Configure Okta

1. In the Okta console, click **Application** and then click the new application **OCI IAM**.
2. Go to the **Sign On** tab and click **Edit**.
3. Select **Enable Single Logout**.
4. Browse to the certificate you downloaded from the OCI IAM Console in the previous step and click **Upload**.
5. Scroll down to **Advanced Sign-on Settings** and enter the following:
   - **Oracle Cloud Infrastructure IAM GUID**: Enter the Identity Domain ID from step 9 in 1. Download the SAML Metadata in OCI IAM Identity Domain.
   - Set the Application username format to **Email**.
6. Click **Save**.
7. Go to the Assignments tab, assign users who you want to have access to this application.
8. Click **Next**.

5. Add Okta Identity Provider to IdP Policy in OCI Console

1. In the OCI Console, go to the Identity Domain in which you want to configure Okta Federation.
2. Click the **Federation** tab. Under Identity Providers, scroll down to **Identity provider policies.**
3. Click **Default Identity Provider Policy** and select the **Identity provider rules** tab.
4. Click the three dots (ellipsis) next to Default IdP rule and select **Edit IdP rule**.
5. Under Assigned Identity Providers, select the IdP that was created for Okta and save your changes.
6. Go back to the Identity Domain page. Click the **Domain Policies** tab.
7. Under **Sign-on policies**, click the **Default Sign-On Policy**.
8. Click the **Sign-on rules** tab. Click the three dots (ellipsis) next to **Default sign-on rule** and select **Edit Sign-on rule**.
9. Under **Conditions**, **Authenticating identity provider**, add the Okta Identity Provider.
10. Click **Edit Sign-on rule** to save your changes.

6. Test Single Sign On

1. Enter the following Console URL: https://cloud.oracle.com
2. Enter your **Cloud Account Name**, also referred to as your tenancy name and click **Next**.
3. Select the **domain** for which you configured Okta IdP.
4. On the sign-in page, click the **Okta** icon.
5. Enter your **Okta** credentials. You are now signed in to the OCI Console.