Oracle® Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Identity Federation (When using SCIM APIs for User Provisioning)

Release 24.1
F97448-01
June 2024

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation (When using SCIM APIs for User Provisioning), Release 24.1

F97448-01

Contents

1 Steps to Configure Identity Federation in OCI IAM Identity Domain without Just-In-Time Provisioning

Step 1: Download the SAML Metadata in OCI IAM Identity Domain 1-1

Step 2: Add OCI IAM Identity Domain as a Service Provider (SP) in the Identity Provider (IDP) 1-1

Step 3: Download the Identity Provider SAML Metadata Document 1-2

Step 4: Add the Identity Provider in OCI IAM Identity Domains 1-2

Step 5: Test SSO Between Identity Provider and OCI IAM 1-3

Notices

Preface

Purpose

This guide explains the steps to configure Identity Federation to set up OPERA Cloud services SSO with customer identity provider.

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
June 2024	Initial Publication

1

Steps to Configure Identity Federation in OCI IAM Identity Domain without Just-In-Time Provisioning

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 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 configure identity federation.

Step 1: Download the SAML Metadata in OCI IAM Identity Domain

1. Log on to Oracle IAM Domain Admin Console.
2. Open the navigation menu, select **Security** and then click **Identity providers**.
3. Open an identity provider.
4. Click **Export SAML metadata**.
5. Select one of the following options:
   - **Metadata File**: Select download the SAML XML metadata file or select download the SAML XML metadata with self-signed certificates.
   - **Manual Export**: Manually exporting the metadata enables you to choose from multiple SAML options. For example, the Entity ID or Logout response URL. After you copy the export file, you can download the service provider signing certificate or the service provider encryption certificate.
   - **Metadata URL**: If your IdP supports downloading SAML metadata directly, click **Access signing certificate** to allow clients to access the signing certificate without the need to log on to an IdP.

Step 2: Add OCI IAM Identity Domain as a Service Provider (SP) in the Identity Provider (IDP)

1. It is required to add OCI IAM Identity Domain as the service provider in your identity using the metadata downloaded earlier.
2. It is required to map the name the Name identifier(Name ID) value field as the username.

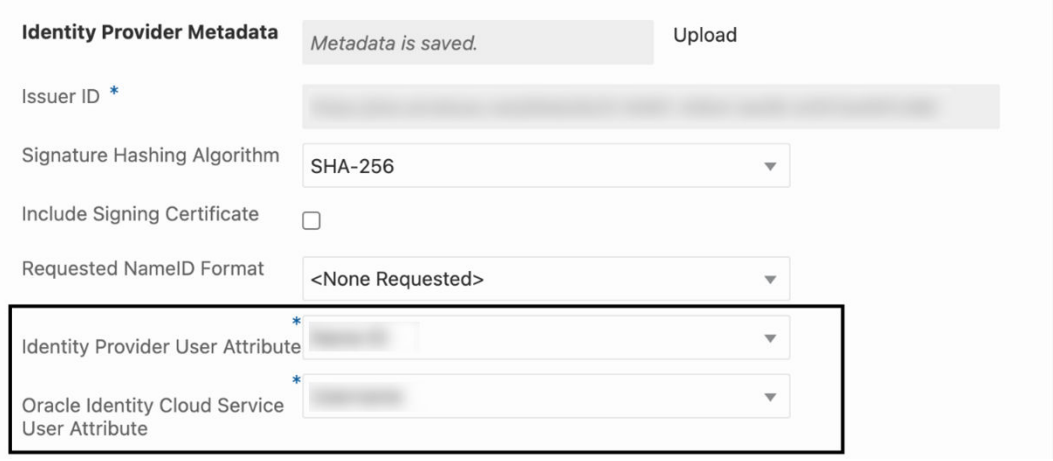
Step 3: Download the Identity Provider SAML Metadata Document

- Download this metadata XML file and make a note of where you save it. You will upload this document to the IAM Domain Console in the next series of steps.

Step 4: Add the Identity Provider in OCI IAM Identity Domains

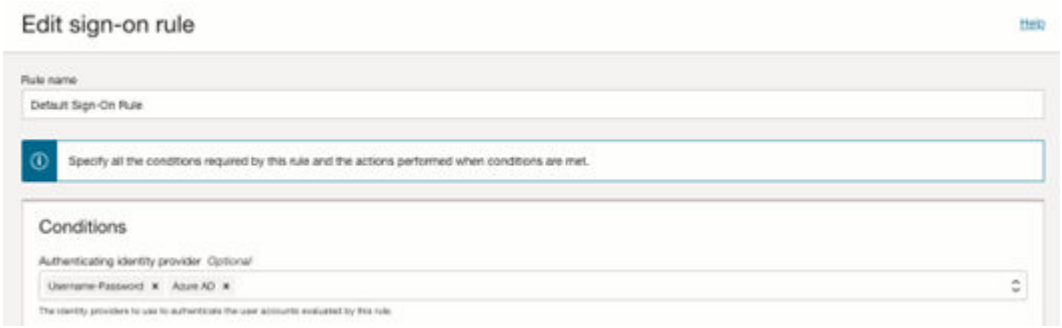
Enter the identity provider details by following these steps:

1. Navigate to the Oracle IAM domain console.
2. On the navigation menu, click **Security** and then click **Identity providers**.
3. Click **Add IdP** and then click **Add SAML IdP**.
4. Enter the following information:
   - **Name**: Enter the name of the IdP.
   - (Optional) **Description**: Enter a description of the IdP.
   - (Optional) **Identity provider icon**: **Drag and drop** a supported image or click **select one** to browse for the image.
5. Click **Next**.
   Verify the **Import identity provider metadata** is selected and browse and select or drag and drop the metadata XML file onto the Identity provider metadata. This is the metadata file you saved earlier from your identity provider.
6. Click **Next**.
7. In Map user identity, set the values as shown in the following screenshot.



8. Click **Next**.
9. Under Review and Create, verify the configurations, and then click **Create IdP**.
10. Click **Activate**.
11. Click **Add to IdP Policy Rule**.
12. Click **Default Identity Provider Policy** to open it, and from the context (vertical ellipsis) menu, select **Edit IdP rule**.

13. Click **Assign identity providers** and then click the Identity provider name to add it to the list.
14. Click **Save Changes**.
15. Go back to Security and click **Sign-on policies**.
16. Click **Default Identity Provider Policy** to open it, and in the Sign-on rules from the context (vertical ellipsis) menu on the right, select **Edit IdP rule**.
17. Select the identity provider.



18. Save your changes.

Step 5: Test SSO Between Identity Provider and OCI IAM

In this section, you can test that federated authentication works between OCI IAM and customer's identity provider.

1. Open a supported browser and enter the OCI 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 in which Identity provider has been configured.
4. On the sign-in page, you can see an option to sign in with identity provider.
5. Select the identity provider. You are redirected to the Microsoft login page.
6. Provide your identity provider user credentials.
7. On successful authentication, you are logged in to the OCI Console.