Oracle® Hospitality OPERA Cloud Identity Management

Administrator Guide for Setting Up Identity Federation with Just-In-Time Provisioning (JIT) in OCI IAM Identity Domains

Release 25.5
G47676-01
November 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Setting Up Identity Federation with Just-In-Time Provisioning (JIT) in OCI IAM Identity Domains, Release 25.5

G47676-01

Contents

Notices

Preface

Purpose

This guide explains the steps to configure Identity Federation to set up OPERA Cloud services single sign-on (SSO) with a 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
November 2025	Initial Publication

1

Steps to Configure Identity Federation in OCI IAM Identity Domains with 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 explains the steps required to configure identity federation with Just In Time (JIT) user provisioning in a customer's OCI IAM Identity Domains.

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

1. Log on to OCI IAM Identity Domain.
2. Open the navigation menu, select **Identity and Security** and then click **Domains**. Click the Identity Domain in which you want to work.
3. Click the **Federation** tab.
4. Under Identity Providers, 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: Adding OCI IAM Identity Domain as a Service Provider (SP) in the Identity Provider (IdP)

1. Add the OCI IAM Identity Domain as the service provider in your Identity Provider using the metadata downloaded earlier.
2. Map the Name identifier (Name ID) value field as the **Username**.

3. The below table lists the SAML attributes that must be configured in Identity Provider to pass as assertion during the SAML response. Ensure all the mandatory attributes are added in the Identity Provider.

Table 1-1 SAML Attributes

SAML Attribute Name	Attribute Description	Mandatory Attribute
oc_userid	User Name	Yes
oc_surname	Family Name	Yes
oc_emailaddress	Primary Email	Yes
oc_userid	User Name	Yes
oc_surname	Family Name	Yes
oc_primaryworklocation	User's primary work location. This is a mandatory single value user attribute that indicates the user's primary work location. The primary work location can have the following values: <ENTERPRISE ID>:E for multi-chain customers derived from the user profile for those users who are at the enterprise level. For customers having only a single chain, the source value can be set to constant <CHAIN CODE>:C for all users. Assign <PROPERTY CODE>:P derived from the user profile in the identity provider to assign users with a property code as their primary work location.	Yes
oc_role	Group memberships (role memberships) of the user.	Yes
oc_actas	You can send values for a new user's Act As field from your identity provider, which eliminates overhead for an admin to manually assign Act As for a new user in OPERA Cloud Role Manager. Possible Values: • Reservation Sales Person • Conference Sales Person • External System	No

Table 1-1 (Cont.) SAML Attributes

SAML Attribute Name	Attribute Description	Mandatory Attribute
oc_actat	You can send values for a new user's Act At field from your identity provider, which eliminates overhead for an admin to manually assign Act At for a new user in OPERA Cloud Role Manager. Possible Values: • Property • Central	No
oc_preferredlanguage	User Preferred Language	No
oc_givenname	Given Name	No
oc_employeenumber	Employee Number	No
oc_telephonenumber	Mobile Number	No
oc_title	Title	No
oc_displayname	Display Name	No
oc_usertype	User Type. The possible values are: • FULL-TIME EMPLOYEE • PART-TIME EMPLOYEE • TRAINEE • CONTRACTOR • CONSULTANT • OTHER	No
oc_orgcode	Enterprise or Chain Code	No
oc_workphonenumber	Work Phone Number	No
oc_userinitial	Honorific Prefix	No
oc_middlename	Middle Name	No
oc_honorificsuffix	Honorific Suffix	No
oc_timezone	User Timezone	No
oc_locale	User Locale	No
oc_ownercode	Owner code of the user	No
oc_hubs	This SAML claim enables customers to map HUB(s) to a user in OPERA Cloud. This claim is mapped to a string array attribute in OCI IAM Identity Domain and allows multiple values. If the identity provider system does not support string array data types, then use the claim oc_hubs_string as described below. If no value is passed, the user is assigned to the default hub in OPERA Cloud.	No

Table 1-1 (Cont.) SAML Attributes

SAML Attribute Name	Attribute Description	Mandatory Attribute
oc_hubs_string	This SAML claim enables customers to map HUB(s) to a user in OPERA Cloud. This claim is mapped to a string attribute in OCI IAM Identity Domain. Please note, only oc_hubs or oc_hubs_string can be used based on the data type supported in the identity provider. If no value is passed, the user is assigned to the default hub in OPERA Cloud.	No

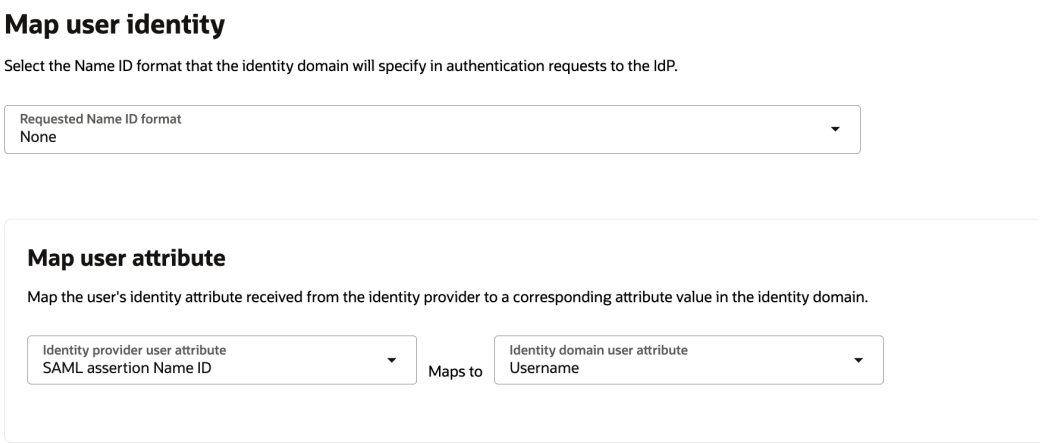
Step 3: Downloading the Identity Provider SAML Metadata Document

1. Download the SAML metadata XML file from the Identity Provider and make a note of where you save it. You will upload this document to the OCI IAM Identity Domain in the next series of steps.

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

Enter the identity provider details by following these steps:

1. Navigate to the OCI IAM Identity domain overview page.
2. Click the **Federation** tab. Under **Identity providers**, click the **Actions** menu and select **Add SAML IdP**.
3. 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.
4. 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.
5. Click **Next**.
6. Under Map user identity, set the values below:
   - **Requested Name ID Format**: None
   - **Identity Provider user attribute**: SAML Assertion Name ID
   - **Identity Domain user attribute**: Username



7. Click **Next**.
8. Under Review and Create, verify the configurations and then click **Create IdP**.
9. Click the name of the IdP you just created to open the IdP Overview page.
10. Click the **Actions** menu and select **Activate**.

Step 5: Configuring Just In Time Provisioning in OPERA Cloud Identity Management Portal

The Configure Identity Providers tool in OPERA Cloud Identity Management portal configures attribute mappings for Just-in-time (JIT) provisioning in the selected SAML Identity Provider of the respective Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) Identity Domain.

Enterprise administrators have access to this feature in the OPERA Cloud Identity Management portal Tools page. In addition, the customer administrator should also have the Identity Domain Administrator or the Security Administrator Application Roles in Oracle Cloud Infrastructure Identity and Access Management to configure the Identity Provider.

Configure JIT from OPERA Cloud Identity Management Portal

Refer to the steps mentioned in Configure Identity Providers to Configure JIT Mappings for the Identity Provider.

Confirm the JIT Mappings are Created

1. Go to the OCI console and navigate to the Identity domain in which you want to work and select the **Identity Provider**.
2. Click **Configure JIT** and confirm the JIT is enabled and the attribute mappings have been created.
3. Click **Cancel**.

> **Note**
>
> Oracle does not recommend that customers make any customization to the JIT configuration from the Oracle Cloud Infrastructure console. Any updates made in the OCI console will not be saved or captured by the Configure Identity Providers tool.

Step 6: Configure OCI IAM Identity Domain Policies

Configure Identity Provider (IdP) Policies

1. Navigate to the Identity Domain Overview page and click the **Federation** tab under the Identity Domain.
2. Under **Identity provider policies**, click the **Default Identity Provider policy** to open it.
3. Click the **Identity Provider Rules** tab. Click the **ellipsis** (three dots) next to the **Default IDP Rule** and select **Edit IDP Rule**.
4. Click **Assign Identity Providers** field and then select your Identity provider to add it to the list.
5. Click **Save Changes**.

Configure Single Sign-on (SSO) Policies

1. Navigate to the Identity Domain Overview page and click **Domain Policies**.
2. Under **Single Sign-on policies**, click the **Default Sign-on policy** to open it.
3. Click the **Sign-on Rules** tab. Click the **Ellipsis** (three dots) next to the **Default Sign-on Rule** and select **Edit Sign-on Rule**.
4. Click the **Authenticating Identity Providers** field and then select your Identity provider to add it to the list.
5. Click **Edit Sign-on Rule** to save your changes.

Step 7: Testing SSO between Identity Provider and OCI IAM

In this section, you can test that federated authentication works between OCI IAM and the 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 Identity Provider login page.
6. Provide your identity provider user credentials.
7. On successful authentication, you are logged in to the OCI Console.