

# Oracle Hospitality OPERA Cloud Identity Management

## Administrator Guide for Configuring Identity Federation (When using Microsoft Entra ID Synchronization for User Provisioning)



Release 25.5  
G47677-01  
November 2025

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation (When using Microsoft Entra ID Synchronization for User Provisioning), Release 25.5

G47677-01

Copyright © 2023, 2025, Oracle and/or its affiliates.

# Contents

## 1 Steps to Configure Identity Federation in OCI IAM Identity Domain

---

Step 1: Download the SAML Metadata in OCI IAM Identity Domain	1
Step 2: Add OCI IAM Identity Domains as an Enterprise Application in Entra ID	1
Step 3: Configure OCI IAM Identity Domain as an Enterprise Application in Entra ID	2
Step 4: Configure User Attributes and Claims	2
Step 5: Download the Entra ID SAML Metadata Document	7
Step 6: Assign User Groups to the Application	7
Step 7: Add Microsoft Entra ID as an Identity Provider in OCI IAM Identity Domains	7
Step 8: Configuring Just In Time Provisioning Attribute Mapping	8
Step 9: Configure OCI IAM Identity Domain Policies	9

# Notices

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Preface

## Purpose

This guide explains the steps to configure Identity Federation to setup OPERA Cloud services SSO with customer identity provider. This document is required to be followed only if the customer identity provider is **Microsoft Entra ID**

## 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

Date	Description of Change
November 2025	Initial Publication

# 1

## Steps to Configure Identity Federation in OCI IAM Identity Domain

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.

### **Note**

Only follow these steps if the customer identity provider is Microsoft Entra ID.

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

1. Log in to Oracle IAM Domain Admin Console.
2. Open the navigation menu and click **Identity & Security**.
3. Under Identity, click **Domains**.
4. Click the name of the identity domain in which you want to work.
5. Click the **Federation** tab.
6. Under Identity Providers, click **Export SAML metadata**.
7. Select **Download XML** next to Metadata with self-signed certificates.

## Step 2: Add OCI IAM Identity Domains as an Enterprise Application in Entra ID

### **Note**

You can skip this step if the enterprise application for OCI is already created as part of setting up Entra ID synchronization with OCI.

1. Log in to the Azure portal and select **Microsoft Entra ID**.
2. Click **Manage** on the left navigation menu and select **Enterprise applications**. A sample of the applications in your Entra ID tenant appears.

3. Click **New application**.
4. Search for and select **Oracle Cloud Infrastructure Console**.
5. Enter a name or accept the default of Oracle Cloud Infrastructure Console.
6. Click **Create**.

The Application Overview page appears with the options for configuring the application for your organization.

## Step 3: Configure OCI IAM Identity Domain as an Enterprise Application in Entra ID

1. On the Application Overview page, under the Manage section, select **Single sign-on**.
2. Select **SAML** to configure the single sign-on. The Set up Single Sign-On with SAML page appears.
3. At the top of the page, click **Upload metadata file**.
4. Locate the **federation metadata file** (Metadata.xml) you downloaded from Oracle Cloud Infrastructure in Step 1 and upload it here. After you upload the file, the following Basic SAML Configuration fields are automatically populated:
  - Identifier (Entity ID)
  - Reply URL (Assertion Consumer Service URL)
5. In the **Basic SAML Configuration** section, enter the following required information:
  - **Sign on URL:**
    - a. Enter the OPERA Cloud User Interface URL for your OPERA Cloud Environment if you have a single OPERA Cloud environment.  
**For example:** `https://customerocua.oraclehospitality.eu-frankfurt-1.ocs.oraclecloud.com/IDENTITY/operacloud/` where **IDENTITY** is the ENTERPRISE ID of the customer.  
Or
    - b. Enter the OPERA Cloud Identity Management Portal URL if you have multiple OPERA Cloud environments.  
**For example:** `https://ocimqa.oraclehospitality.us-phoenix-1.ocs.oraclecloud.com/IDENTITY/ocimportal/` where **IDENTITY** is the ENTERPRISE ID of the customer.
6. Click **Save**.

## Step 4: Configure User Attributes and Claims

The Oracle Cloud Infrastructure Console enterprise application template is seeded with the required attributes, so there is no need to add any. However, you must make the following customizations:

1. In the User Attributes & Claims section, click **Edit**. The Manage Claim panel appears.
2. Click the **Name identifier** value field to edit.
3. Select **Email address** next to the Name identifier format and change it to "Persistent."
4. For Source, select **Attribute**.

5. For Source attribute, select **user.userprincipalname** and click **Save**.
6. Configure additional claims by referring to the below table. **Note:** Only `oc_primaryworklocation` is mandatory and other additional claims are optional.
7. Once all the SAML claims are configured, return to the Set up Single Sign-On with SAML page.



**Table 1-1 SAML Attribute Mapping**

Claim Name	Type	Value	Mandatory Claim (Yes/No)
oc_primaryworklocation	Attribute	<p>Mandatory Single Valued User Attribute.</p> <p>Indicates the user's primary work location.</p> <p>Possible Values:</p> <ol style="list-style-type: none"> <li>1. &lt;ENTERPRISE_ID&gt;:E where &lt;ENTERPRISE_ID&gt; is the OPERA Cloud enterprise ID for the customer. This can be the value if users are at enterprise level specially for users who need access to multiple chains. For example, ENTERPRISE1:E where ENTERPRISE1 is the enterprise code for the customer.</li> <li>2. &lt;CHAIN_CODE&gt;:C where &lt;CHAIN_CODE&gt; is chain code in OPERA Cloud for that customer. This can be the value if users are at chain level specially for users who need access to multiple properties. For example, CHAIN1:C where CHAIN1 is the chain code for the customer in OPERA Cloud.</li> <li>3. &lt;PROPERTY_CODE&gt;:P where &lt;PROPERTY_CODE&gt; is the property code in OPERA Cloud. This can be the value for users at a specific</li> </ol>	Yes

Table 1-1 (Cont.) SAML Attribute Mapping

Claim Name	Type	Value	Mandatory Claim (Yes/No)
		property level. For example, PROPERTY1:P where PROPERTY1 is the property code for the customer in OPERA Cloud.	
		<b>Note:</b> Ensure this claim is created and if it is not created in Entra ID, it will significantly impact OPERA Cloud operations.	
#upper\$(assertion.oc_ownercode))	Attribute	This is the owner code for the user in OPERA Cloud Sales and Event Management.	No
oc_employee_number	Attribute	Employee number is the unique employee number in the customer's employee management system.	No
oc_actas	Attribute	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: <ul style="list-style-type: none"> <li>Reservation Sales Person</li> <li>Conference Sales Person</li> <li>External System</li> </ul>	No

**Table 1-1 (Cont.) SAML Attribute Mapping**

Claim Name	Type	Value	Mandatory Claim (Yes/No)
oc_actat	Attribute	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: <ul style="list-style-type: none"> <li>Property</li> <li>Central</li> </ul>	No
oc_hubs	Attribute	This SAML claim enables customer to map HUB(s) to a user in OPERA Cloud. This claim is mapped to string array attribute in OCI IAM Identity Domain and allows multiple values. If the identity provider system does not support string array data type then please use the claim oc_hubs_string as described below. If no value passed, the user is assigned to default hub in OPERA Cloud.	No
oc_hubs_string	Attribute	This SAML claim enables customer 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 either of oc_hubs or oc_hubs_string need to be used based on data type supported in the identity provider. If no value passed, the user is assigned to default hub in OPERA Cloud.	No

## Step 5: Download the Entra ID SAML Metadata Document

1. In the SAML Certificates section, click the **Download** link next to Federation Metadata XML.
2. Download this document 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 6: Assign User Groups to the Application

To enable Entra ID users to log in to Oracle Hospitality OPERA Cloud, you must assign the appropriate user groups to your new enterprise application.

1. On the left navigation pane, under Manage, select **Users and Groups**.
2. Click **Add User/Group** at the top of the Users and Groups list to open the Add Assignment pane.
3. Click the **Users or groups** selector.
4. Enter the name of the group you want to assign to the application into the **Search by name** or **email address** search box.
5. Hover over the group in the results list to see a check box appear. Select the **check box** to add the group to the Selected list.
6. When you are finished selecting groups, click **Select** to add them to the list of users and groups to be assigned to the application.
7. Click **Assign** to assign the application to the selected groups.

## Step 7: Add Microsoft Entra ID as an Identity Provider in OCI IAM Identity Domains

Enter the Entra ID Identity Provider details by following these steps:

1. Navigate to the OCI IAM Identity domain.
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**.
5. Ensure that Import IdP metadata is selected, and browse and select, or drag and drop the Entra ID metadata XML file. This is the metadata file you saved earlier from Entra ID.
6. Click **Next**.
7. Under Map user identity, set the values as below:
  - **Requested Name ID Format:** None
  - **Identity Provider user attribute:** SAML Assertion Name ID

- **Identity Domain user attribute:** Username

### Map user identity

Select the Name ID format that the identity domain will specify in authentication requests to the IdP.

Requested Name ID format  
None

### Map user attribute

Map the user's identity attribute received from the identity provider to a corresponding attribute value in the identity domain.

Identity provider user attribute  
SAML assertion Name ID

Maps to

Identity domain user attribute  
Username

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

## Step 8: Configuring Just In Time Provisioning Attribute Mapping

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 must 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 Entra ID Identity Provider.

### Confirm the JIT Mappings are Created

1. Go to the OCI IAM Identity Domain and navigate to the Entra ID Identity Provider that you created under the **Federation** tab.
2. Click the **Actions** menu and select **Configure JIT** and confirm the JIT is enabled and the attribute mappings have been created.
3. Click **Save changes**.

**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 9: 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 the **Assign Identity Providers** field and then select the **Entra ID 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 the **Entra ID Identity provider** to add it to the list.
5. Click **Edit Sign-on Rule** to save the changes.