Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Identity Federation (When using Microsoft Azure AD Synchronization for User Provisioning)

Release 25.2
G33278-01
June 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation (When using Microsoft Azure AD Synchronization for User Provisioning), Release 25.2

G33278-01

Contents

Notices

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 Azure AD**

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
June 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 Azure AD.

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 **Security** on the left navigation and then click **Identity providers**.
6. Click **Export SAML metadata**.
7. Select **Download XML** under Metadata with self-signed certificates.

Step 2: Add OCI IAM Identity Domains as an Enterprise Application in Azure AD

> **Note:**
>
> You can skip this step if the enterprise application for OCI is already created as part of setting up Azure AD synchronization with OCI.

1. In the Azure portal, on the left navigation panel, select **Azure Active Directory**.

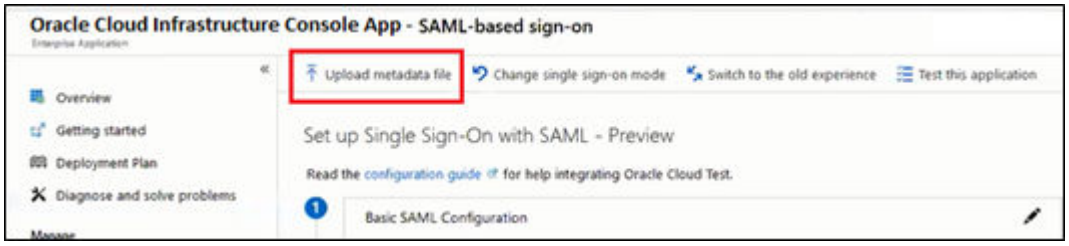
2. In the Azure Active Directory pane, select **Enterprise applications**. A sample of the applications in your Azure AD tenant appears.
3. At the top of the All applications pane, click **New application**.
4. In the Add from gallery region, enter **Oracle Cloud Infrastructure Console** in the search box.
5. Select the **Oracle Cloud Infrastructure Console** application from the results.
6. In the application-specific form, you can edit information about the application. For example, you can edit the name of the application.
7. When you are finished editing the properties, select **Create**.

The getting started page appears with the options for configuring the application for your organization.

Step 3: Configure OCI IAM Identity Domain as an Enterprise Application in Azure AD

1. 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**.



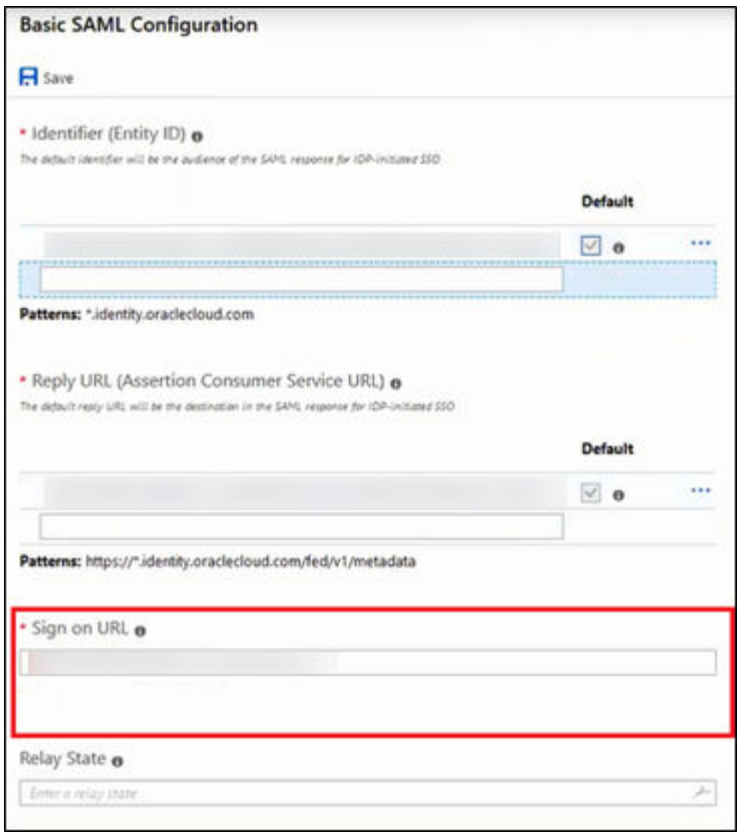
4. Locate the **federation metadata file** (metadata.xml) you downloaded from Oracle Cloud Infrastructure in Step 1 and upload it here. After you upload the file, the following Basic SAML Configuration fields are automatically populated:
   - Identifier (Entity ID)
   - Reply URL (Assertion Consumer Service URL)
5. In the **Basic SAML Configuration** section, click **Edit**. On the Basic SAML Configuration pane, 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.

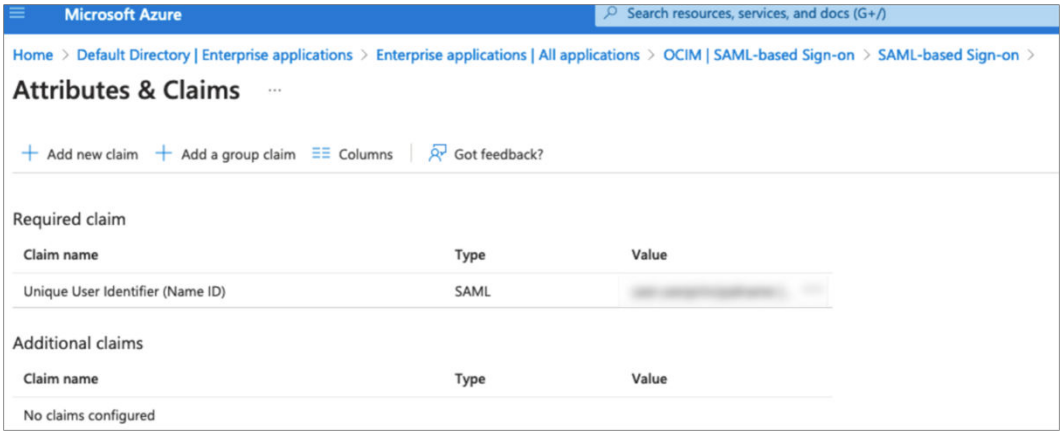


6. Click **Save**.

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** in the upper-right corner. The Manage Claim panel appears.
2. Next to the Name identifier value field, click **Edit**.
3. Under Required claim, select **Unique User Identifier** (Name ID).
4. Select **Email address** and change it to “Persistent.”
5. For Source, select **Attribute**.
6. For Source attribute, select **user.userprincipalname**.



7. Configure additional claims by referring to the below table. **Note**: Only oc_primaryworklocation is mandatory and other additional claims are optional.

Table 1-1 SAML Attribute Mapping

Claim Name	Type	Value	Mandatory Claim (Yes/No)
oc_primaryworklocation	Attribute	Mandatory Single Valued User Attribute. Indicates the user's primary work location. Possible Values: 1. <ENTERPRISE_ID>:E where <ENTERPRISE_ID> 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 whereENTERPRISE1 is the enterprise code for the customer. 2. <CHAIN_CODE>:C where <CHAIN_CODE> 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. 3. <PROPERTY_CODE>:P where <PROPERTY_CODE> is the property code in OPERA Cloud. This can be the value for users at a specific	Yes

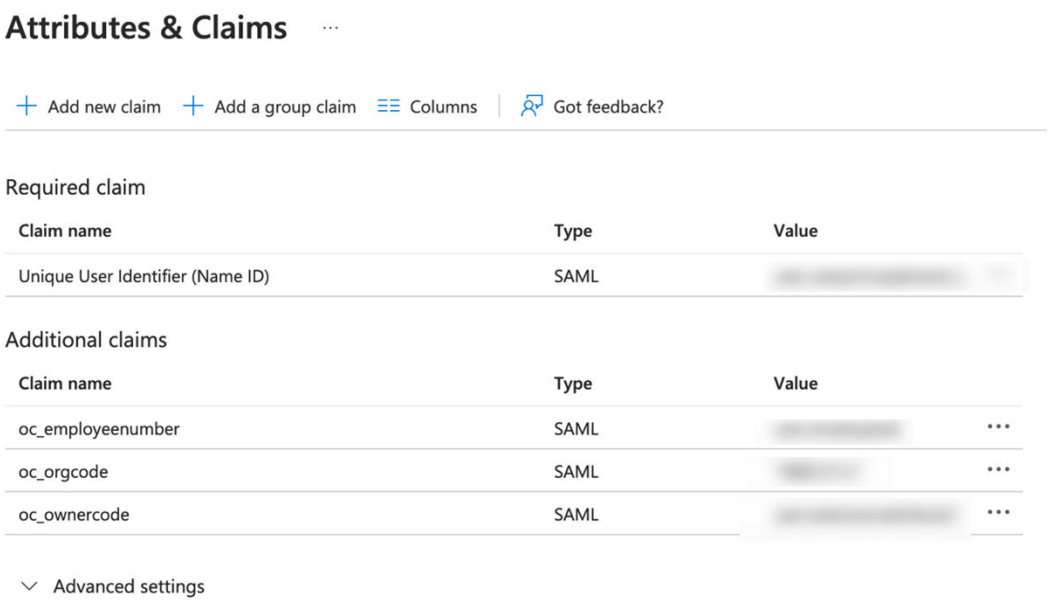
Table 1-1 (Cont.) SAML Attribute Mapping

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. **Note**: Ensure this claim is created and if it is not created in Azure AD, 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_employeenumber	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: • Reservation Sales Person • Conference Sales Person • External System	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: • Property • Central	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

Figure 1-1 Attributes & Claims



The claim values in the above image are only examples.

Step 5: Download the Azure AD SAML Metadata Document

1. In the SAML Signing Certificate 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 IAM Domain Console in the next series of steps.

Step 6: Assign User Groups to the Application

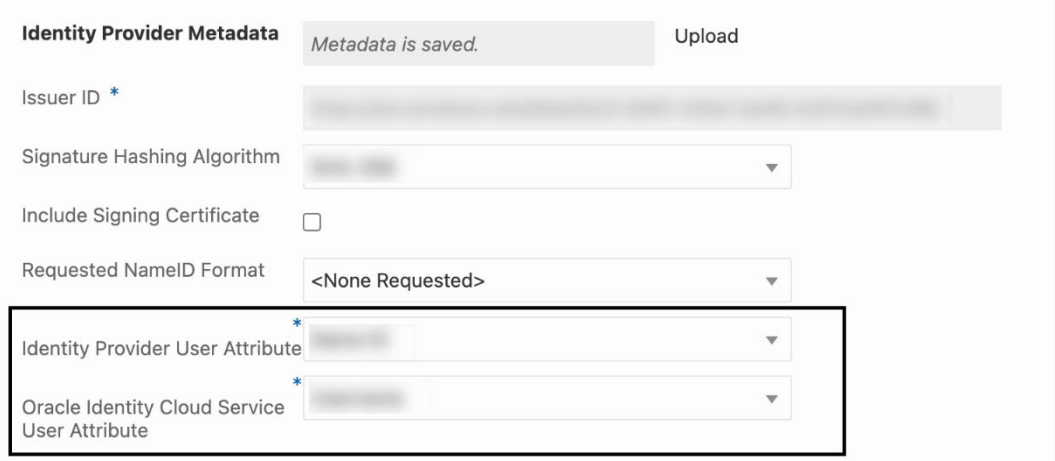
To enable Azure AD users to log in to Oracle Hospitality OPERA Cloud, you must assign the appropriate user groups to your new enterprise application.

1. On the left navigation pane, under Manage, select **Users and Groups**.
2. Click **Add** at the top of the Users and Groups list to open the Add Assignment pane.
3. Click the **Users and 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 Azure AD as an Identity Provider in OCI IAM Identity Domains

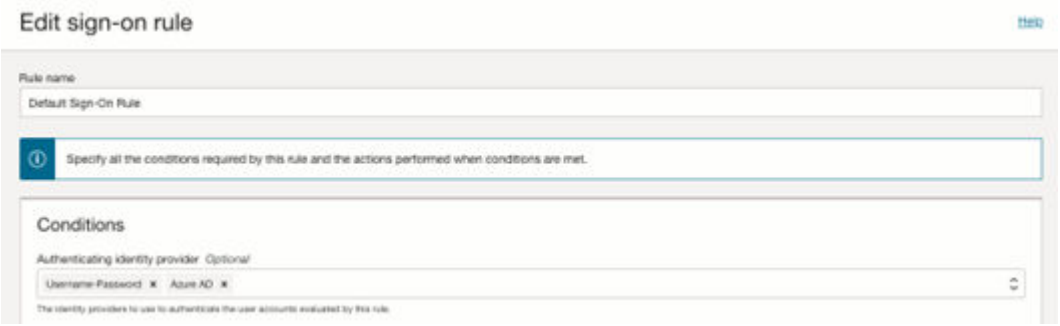
Enter the Azure AD identity provider details by following these steps:

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**.
   Ensure that Import identity provider metadata is selected, and browse and select, or drag and drop the Azure AD metadata XML file into Identity provider metadata. This is the metadata file you saved earlier from Azure AD.
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 (three dots) menu choose **Edit IdP rule**.
13. Click **Assign identity providers** and then click **Azure AD** Identity provider 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 (three dots) menu on the right, select **Edit IdP rule**.
17. Select **Azure AD**.



18. Save your changes.

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 Mappings for Azure AD Identity Provider

1. Log in to OPERA Cloud Identity Management Portal as an enterprise administrator.
2. Click the **Tools** tile on the Homepage.

> **Note:**
>
> Only enterprise and chain-level administrators have access to the Tools tile.

The Tools page consists of a list of available tools including **Configure Identity Providers**.

3. Select **Configure Identity Providers**.
4. All active Identity Providers in the respective OCI IAM Identity Domain are shown.

> **Note:**
>
> User must have the Identity Domain Administrator or Security Administrator role in Oracle Cloud Infrastructure Identity and Access Management to perform this operation. For more information, refer to Understanding Administrator Roles in the Oracle Cloud Infrastructure Documentation.

5. Click the **Configure JIT** button next to the respective Azure AD Identity Provider. This enables JIT for the respective Identity Provider and adds all the attribute mappings including the custom attributes needed for provisioning.

Confirm the JIT Mappings are Created

1. Go to the OCI console and navigate to the Azure AD Identity Provider.
2. Click **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: Test SSO Between Azure AD and OCI IAM

> **Note:**
>
> The configurations in the 'Setting Up Synchronization with Microsoft Azure AD' guide must be completed before you can test the SSO between Azure AD and OCI IAM.

In this section, you can test that federated authentication works between OCI IAM and Azure AD.

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 AzureAD federation has been configured.
4. On the sign-in page, you can see an option to sign in with Azure AD.
5. Select Azure AD. You are redirected to the Microsoft login page.
6. Provide your AzureAD credentials.
7. On successful authentication, a ‘Connection Successful’ message appears.