Oracle Hospitality OPERA Cloud Identity Management

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

Release 23.1.1
F83068-01
March 2024

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation (When using Microsoft Azure AD Synchronization for User Provisioning), Release 23.1.1

F83068-01

Contents

Notices

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 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
March 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.

> **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

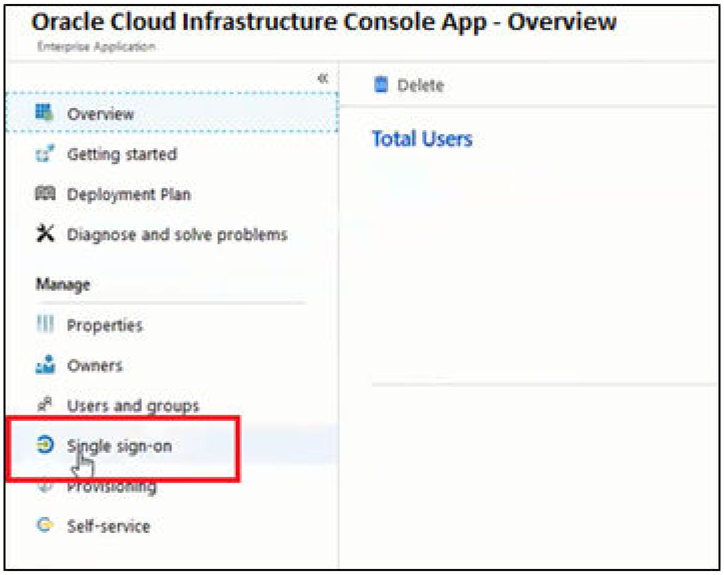
> **Note:**
>
> You can skip this step if the enterprise application for OCI is already created as part of setting up Azure AD synchronization with OCI.

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

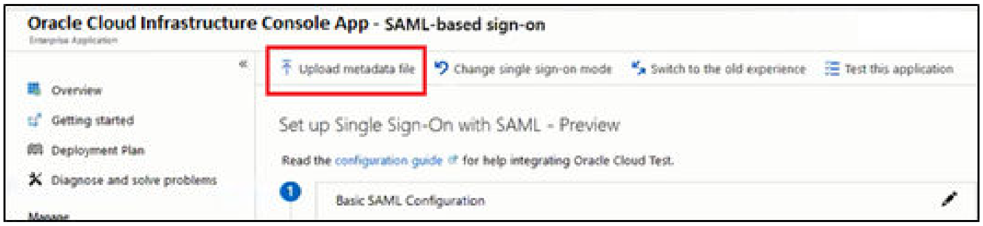
1. Under the Manage section, select **Single sign-on**.



Oracle Cloud Infrastructure Console App - Overview

Enterprise Application

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**.



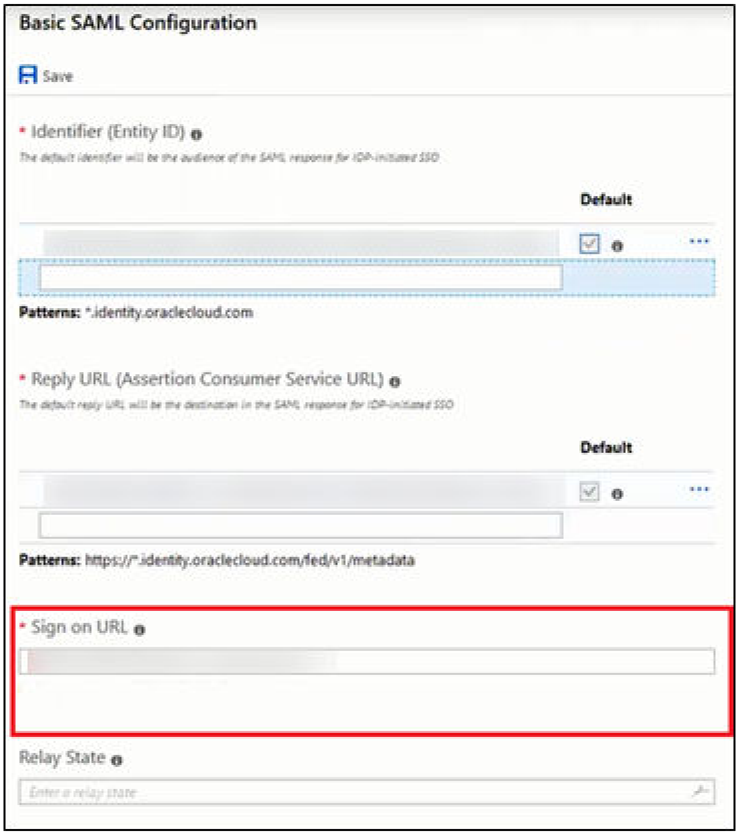
Oracle Cloud Infrastructure Console App - SAML-based sign-on

Enterprise Application

Set up Single Sign-On with SAML - Preview

Read the configuration guide for help integrating Oracle Cloud Test.

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 field:
    - **Sign on URL**: Enter the URL in the following format: https://cloud.oracle.com.



Basic SAML Configuration

* Identifier (Entity ID)

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Patterns: *.identity.oraclecloud.com

* Reply URL (Assertion Consumer Service URL)

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Patterns: https://*.identity.oraclecloud.com/fed/v1/metadata

* Sign on URL

Relay State

Enter a relay state

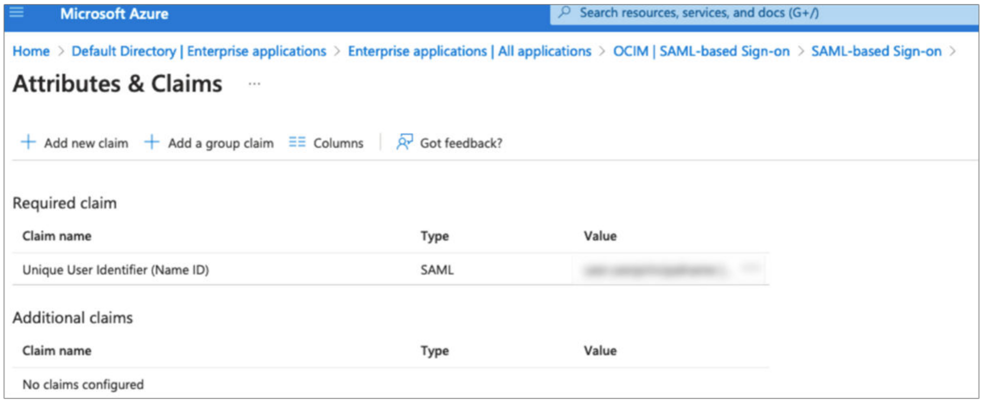
6. Click **Save**.

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**.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory | Enterprise applications > Enterprise applications | All applications > OCIM | SAML-based Sign-on > SAML-based Sign-on >
Attributes & Claims ...
+ Add new claim
+ Add a group claim
Columns
Got feedback?

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	[redacted]

Additional claims

Claim name	Type	Value
No claims configured		

7. Click **Save**.

Table 1-1 SAML Attribute Mapping

SAML User Attribute Type	SAML User Attribute Name	IAM Domain User Attribute	Value	Mandatory Attribute
Attribute	#upper($(assertion.oc_ownercode))	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserOwnerCode	N/A	No
Attribute	oc_employeenumber	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserEmployeeNo	N/A	No

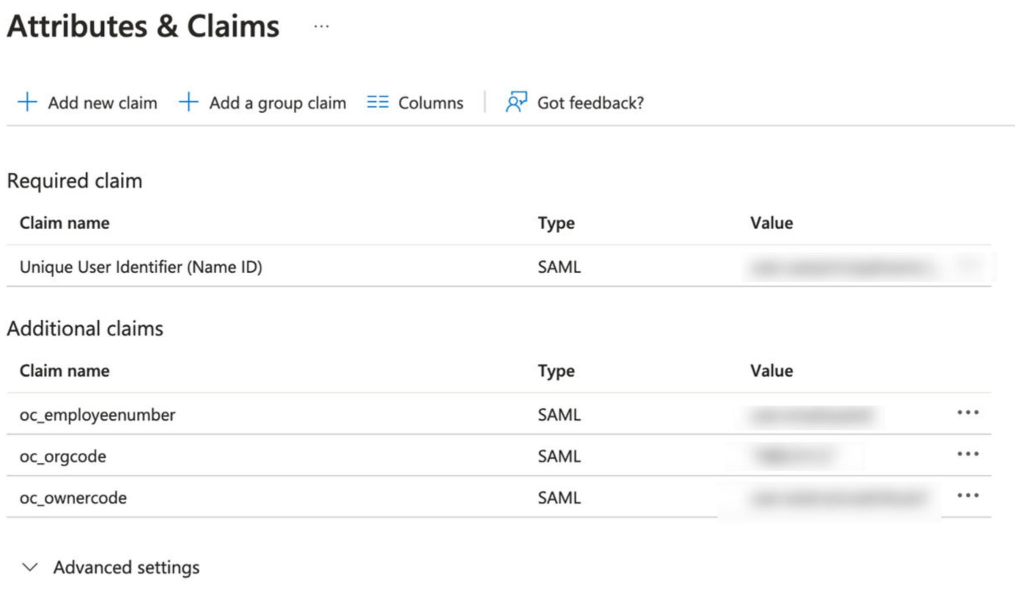
Table 1-1 (Cont.) SAML Attribute Mapping

SAML User Attribute Type	SAML User Attribute Name	IAM Domain User Attribute	Value	Mandatory Attribute
Attribute	oc_orgcode:C	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_PrimaryWorkLocation	Mandatory Single Valued User Attribute. Indicates the user's primary work location. Primary Work Location can have values <ENTERPRISE_IDCHAINCODE>:EC for multi chain customers derived from the user profile. For customers having only a single chain, the source value can be set to constant <ENTERPRISE_ID>:E <CHAINCODE>:C for all users. <ENTERPRISE_ID><CHAINCODE> will be oc_orgcode. This mapping is required and mandatory only if oc_primaryworklocation cannot	Yes

Table 1-1 (Cont.) SAML Attribute Mapping

SAML User Attribute Type	SAML User Attribute Name	IAM Domain User Attribute	Value	Mandatory Attribute
			be sent in the SAML claims from IdP.	

Figure 1-1 Attributes & Claims



Attributes & Claims ···

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	[redacted]

Additional claims

Claim name	Type	Value
oc_employeenumber	SAML	[redacted]
oc_orgcode	SAML	[redacted]
oc_ownercode	SAML	[redacted]

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.

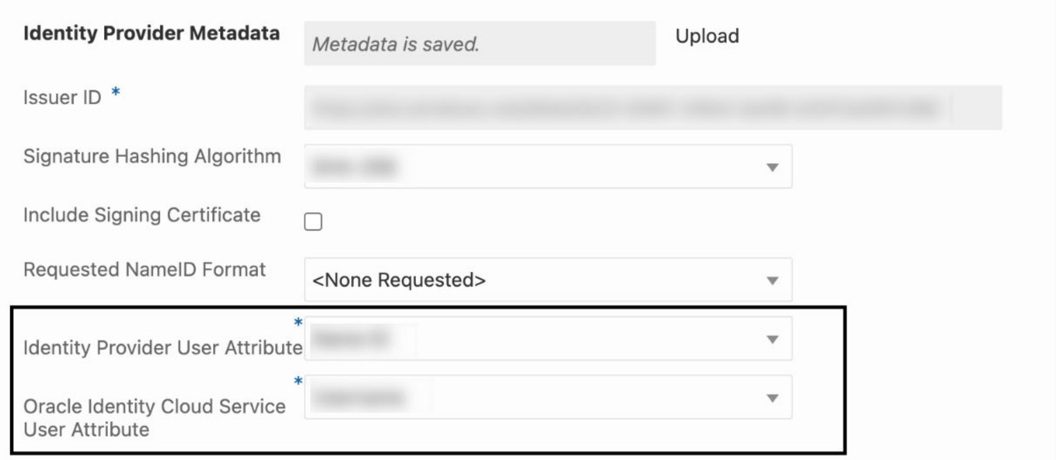
1. On the left navigation pane, under Manage, select **Users and Groups**.
2. Click **Add** at the top of the Users and Groups list to open the Add Assignment pane.

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.



Identity Provider Metadata: *Metadata is saved.*

Issuer ID *: [redacted]

Signature Hashing Algorithm: [redacted]

Include Signing Certificate: □

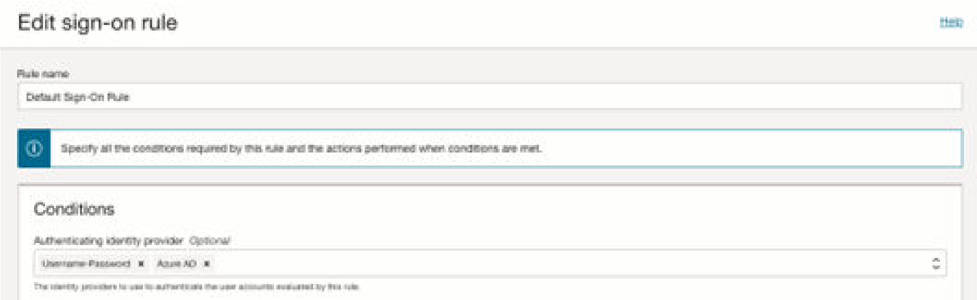
Requested NameID Format: <None Requested>

Identity Provider User Attribute *: [redacted]

Oracle Identity Cloud Service User Attribute *: [redacted]

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**.



Edit sign-on rule

Rule name

Default Sign-On Rule

Specify all the conditions required by this rule and the actions performed when conditions are met.

Conditions

Authenticating identity provider Optional

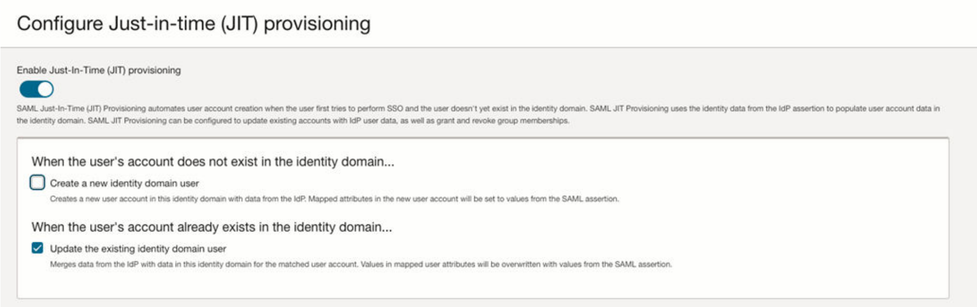
Username-Password ✕ Azure AD ✕

The identity providers to use to authenticate the user accounts evaluated by this rule.

18. Save your changes.

JIT Attribute Mapping

1. In the OCI console, open the navigation menu and click **Identity & Security**.
2. Under Identity, click **Domains**.
3. In the respective domain, navigate to **Security** and then navigate to **Identity Provider**.
4. Under the respective Identity Provider, click **Configure JIT**.
5. Turn on the **Enable Just-In-Time (JIT) provisioning** option and select the **Update the existing identity domain user option**.



Configure Just-in-time (JIT) provisioning

Enable Just-In-Time (JIT) provisioning

SAML Just-In-Time (JIT) Provisioning automates user account creation when the user first tries to perform SSO and the user doesn't yet exist in the identity domain. SAML JIT Provisioning uses the identity data from the IdP assertion to populate user account data in the identity domain. SAML JIT Provisioning can be configured to update existing accounts with IdP user data, as well as grant and revoke group memberships.

When the user's account does not exist in the identity domain...

☐ Create a new identity domain user

Creates a new user account in this identity domain with data from the IdP. Mapped attributes in the new user account will be set to values from the SAML assertion.

When the user's account already exists in the identity domain...

☑ Update the existing identity domain user

Merges data from the IdP with data in this identity domain for the matched user account. Values in mapped user attributes will be overwritten with values from the SAML assertion.

6. Save your changes.

Follow the below steps to create JIT Attribute mapping for custom attributes.

1. Create a Confidential Application
   1. In the OCI identity domain, open the navigation menu and click **Identity & Security**.
   2. Under **Identity**, click **Domains**.
   3. Click the name of the identity domain that you want to work in. You might need to change the compartment to find the domain that you want. Then, click **Integrated applications**.
   4. Click **Add application.**
   5. In the **Add application** screen, select **Confidential Application**, and then click **Launch workflow**.
   6. On the **Add application details** page, enter an application name and description, and then click **Next**.
   7. On the **Configure OAuth** page, under **Client configuration**, select **Configure this application as a client now**.
   8. Under **Authorization**, select only **Client Credentials** as the **Allowed Grant Type**.
   9. At the bottom of the page, select **Add app roles** and then click **Add roles**.
   10. In the **Add app roles** panel, select **Identity Domain Administrator**, and then click **Add**.
   11. Click **Next** and then click **Finish**.
   12. On the application detail page, scroll down to **General Information**. Copy the **Client ID** and the **Client Secret** and save it in a secure place for later.
   13. After the application is created, click **Activate**.

   The confidential application is now activated.
2. Obtain an Access Token.

```
curl --location 'https://<domainURL>/oauth2/v1/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'Authorization: Basic <base64encoded clientid:secret>' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'scope=urn:opc:idm:__myscopes__'
```

3. Get the Identity Provider Name.
   1. In the OCI Console, navigate to the **Domain**, **Security**, and **Identity Providers** to find the Identity Provider Name.
4. Get the Identity Provider Id (jitUserProvAttributes.value) by passing the Identity Provider Name.

```
curl --location 'https://<domainURL>/admin/v1/IdentityProviders?
attributes=jitUserProvAttributes.value&filter=partnerName+eq+<Identity
Provider Name> \
--header 'Authorization: Bearer <ACCESS TOKEN>'
```

5. Update the JIT Attribute Mapping.

CURL to Configure JIT Mapping

```
curl --location --request PATCH 'https://<domainURL>/admin/v1/
MappedAttributes/<jitUserProvAttributes.value>' \
--header 'Authorization: Bearer <ACCESS TOKEN>' \
--header 'Content-Type: application/json' \
--data '{
     "schemas": [
        "urn:ietf:params:scim:api:messages:2.0:PatchOp"
    ],
    "Operations": [
        {
            "op": "replace",
            "path": "attributeMappings",
            "value": [
                {
                    "managedObjectAttributeName": "$
(assertion.oc_userid)",
                    "idcsAttributeName": "userName"
                },
                {
                    "managedObjectAttributeName": "$
(assertion.oc_givenname)",
                    "idcsAttributeName": "name.givenName"
                },
                {
                    "managedObjectAttributeName": "$
(assertion.oc_surname)",
                    "idcsAttributeName": "name.familyName"
                },
                {
                    "managedObjectAttributeName": "$
(assertion.oc_emailaddress)",
                    "idcsAttributeName": "emails[primary eq true and
type eq \"work\"].value"
                },
                {
                    "managedObjectAttributeName": "$
(assertion.oc_orgcode)",
                    "idcsAttributeName":
"urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_PrimaryWork
Location"
                },
                {
                    "managedObjectAttributeName": "#upper($
(assertion.oc_ownercode))",
                    "idcsAttributeName":
"urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserOwnerCo
de"
                },
                {
                    "managedObjectAttributeName": "$
(assertion.oc_employeenumber)",
                    "idcsAttributeName":
```

```
"urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserEmployeeNo"
                }
            ]
        }
    ]
}'
```

Step 8: 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.