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 24.1
F96777-02
July 2024

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 24.1

F96777-02

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
July 2024	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 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: 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 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.

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_preferredlanguage	User Preferred Language	No
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 enterprise level. <CHAINCODE>:C for multi-chain customers derived from the user profile. For customers having only a single chain, the source value can be set to constant <CHAINCODE>:C for all users. <CHAINCODE> will be oc_orgcode.	Yes
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

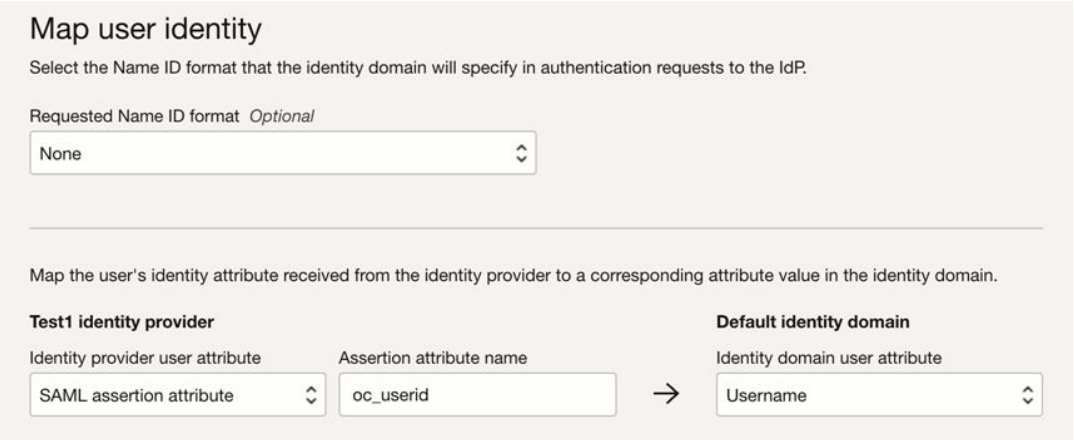
Step 3: Downloading the Identity Provider SAML Metadata Document

1. 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: Adding the Identity Provider in OCI IAM Identity Domains

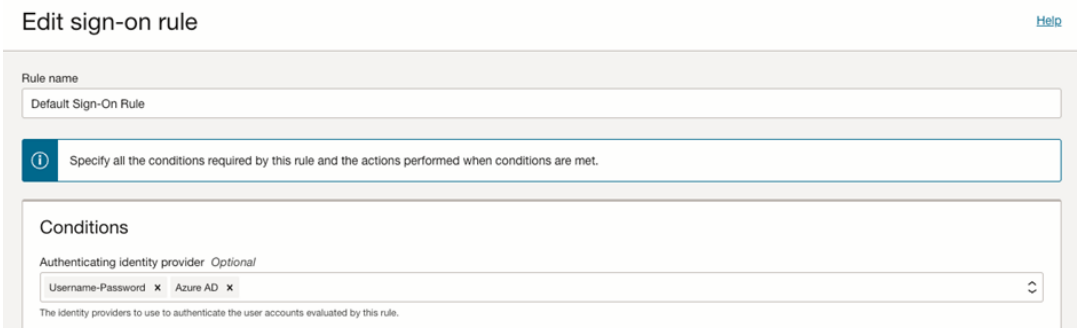
Enter the identity provider details by following these steps:

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 image.



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**.

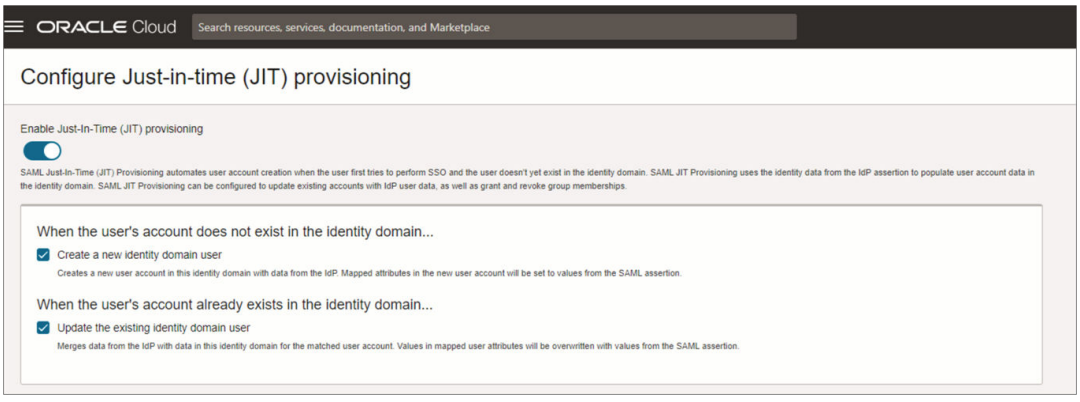
13. Click **Assign identity providers** and then click the Identity provider name to add it to the list.
14. Click **Save Changes**.
15. Go back to Security and click **Sign-on policies**.
16. Click **Default Identity Provider Policy** to open it, and in the Sign-on rules from the context (vertical ellipsis)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



18. Save your changes.

Step 5: Configuring Just In Time Provisioning in OCI IAM Identity Domains

1. In the Identity Provider just created, click **Configure JIT**.
2. On the Configure Just-in-time (JIT) provisioning page:
   a. Select **Enable Just-In-Time (JIT) provisioning**.
   b. Select **Create a new identity domain user**.
   c. Select **Update the existing identity domain user**.



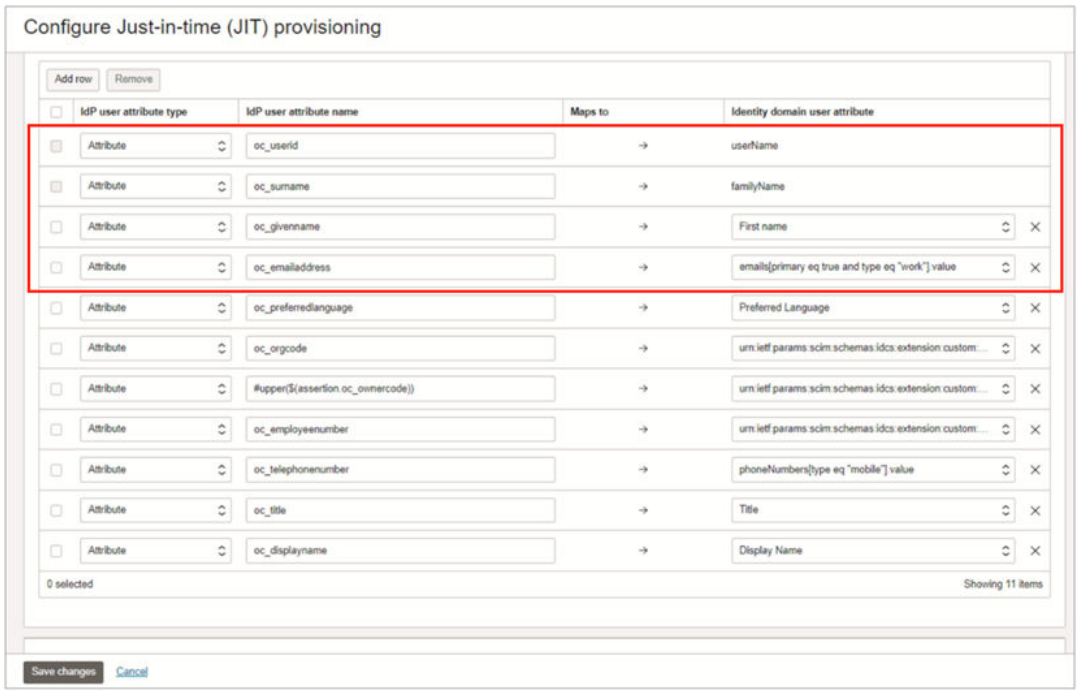
3. Under **Map user attributes**, provide the IdP user attribute name per the mapping below:

Table 1-2 SAML User Attributes

SAML User Attribute Type	SAML User Attribute Name	IAM Domain User Attribute	Mandatory Attribute
Attribute	oc_userid	userName	Yes
Attribute	oc_surname	familyName	Yes
Attribute	oc_emailaddress	emails[primary eq true and type eq "work"].value	Yes. However, if the IAM Domain setting is set to make the primary email address not required, then email address is not a mandatory attribute in the mapping.
Attribute	oc_givenname	givenName	No
Attribute	oc_preferredlanguage	Preferred Language	No
Attribute	oc_primaryworklocation	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_PrimaryWorkLocation	Yes
Attribute	#upper($(assertion.oc_ownercode))	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserOwnerCode	No
Attribute	oc_employeenumber	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserEmployeeNo	No
Attribute	oc_telephonenumber	phoneNumbers[type eq "mobile"].value	No
Attribute	oc_title	Title	No
Attribute	oc_displayname	displayName	No
Attribute	oc_usertype	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserType	No
Attribute	oc_orgcode	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_Department	No
Attribute	oc_workphonenumber	phoneNumbers[type eq "work"].value	No
Attribute	oc_userinitial	name.honorificPrefix	No
Attribute	oc_middlename	name.middleName	No
Attribute	oc_honorificsuffix	urn:ietf:params:scim:schemas:core:2.0:User:name.honorificSuffix	No
Attribute	oc_timezone	urn:ietf:params:scim:schemas:core:2.0:User:timezone	No

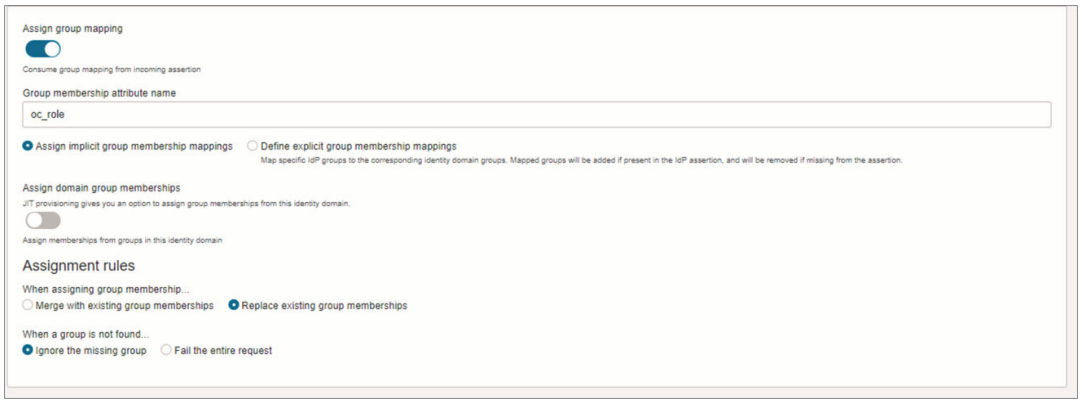
Table 1-2 (Cont.) SAML User Attributes

SAML User Attribute Type	SAML User Attribute Name	IAM Domain User Attribute	Mandatory Attribute
Attribute	oc_locale	urn:ietf:params:scim:schemas:core:2.0:User:locale	No



> **Note:**
>
> Ensure the mapping for the required user attributes (highlighted in the above image) are added before you save your changes. The remaining attributes can be added through the Postman in Step 7.

4. Select **Assign group mapping**.
5. Apply the changes as shown in the image below:



6. Click **Save changes**.

Step 6: Creating 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 in which you want to work. You might need to change the compartment to find the domain that you want.
4. Next, click **Integrated applications**.
5. Click **Add application**.
6. On the Add Application screen, select **Confidential Application** and then click **Launch workflow**.
7. On the Add Application details page, enter an application name and description, and then click **Next**.
8. On the Configure OAuth page, under Client configuration, select **Configure this application as a client now**.
9. Under Authorization, select only **Client Credentials** as the Allowed Grant Type.
10. At the bottom of the page, select **Add app roles** and then click **Add roles**.
11. On the Add app roles panel, select **Identity Domain Administrator** and then click **Add**.
12. Click **Next** and then click **Finish**.
13. On the application detail page, scroll down to General Information and copy the **Client ID** and the **Client Secret** and store it in a safe place.
14. Click **Activate** after the application is created.

    The confidential application is now activated.

> **Note:**
>
> Once JIT Configuration is completed, this Client application can be deactivated.

Step 7: Configuring Just In Time Provisioning Attribute Mapping using Postman

To configure the part of JIT attribute Mapping through Postman, follow these steps:

Set the Environment Parameters in Postman

1. Open Postman, select **Environments**, and click **Import**.
2. On the **Import** screen, import the file **OCI IAM Identity Domain.postman_environment.json**. For the JSON file downloads, refer to the following Customer Support Portal article: https://iccp.custhelp.com/app/answers/answer_view/a_id/1016088.
3. In the imported environment, update the environment variables by entering the following values, and then click **Save**.

a. **HOST**: The Oracle IAM Domain URL.

b. **CLIENT_ID and CLIENT_SECRET**: The Client ID and the Client Secret from the confidential application.

Import the OCIM Federation Postman Collection

1. On the Postman main page, select **Collection** and click **Import**.
2. In the Import dialog box, import the file **OCIM Federation.postman_collection.json**. For the JSON file downloads, refer to the following Customer Support Portal article: https://iccp.custhelp.com/app/answers/answer_view/a_id/1016088.

Request an Access Token

1. On the Collections tab, expand **OCIM Federation** and select **Obtain access_token** (client credentials). Click **Send**.

   The access token is returned in the response from Oracle Identity Domain.
2. Highlight the access token content between the quotation marks and then right-click.
3. In the shortcut menu, select **Set: OCI IAM Identity Domain**. In the secondary menu, select **access_token**. The highlighted content is assigned as the access token value.

Get the Identity Provider Name

1. Select **Get the Identity Provider Name** and click **Send**.
2. Note the partnerName in the response for the type: SAML. The partnerName should be the Identity Provider configured in Identity Domain.

Get the Identity Provider Id by passing the Identity Provider Name

1. Select **Get the Identity Provider Id** by passing the Identity Provider Name.
2. Replace partnerName in the URI with the partnerName from the 'Get the Identity Provider Name' section (see previous steps).
3. Click **Send**.
4. Note the **jitUserProvAttributes.value**.

Update the JIT Attribute Mapping

1. Select **Update the JIT Attribute Mapping**.
2. Replace the **<jitUserProvAttributes.value>** in the URL with the value from the ‘Get the Identity Provider Id by passing the Identity Provider Name’ section (see previous steps).
3. Click **Send**.

> **Note:**
>
> Status: 200 OK should be received in the response.

Confirm the JIT Mappings are Created

1. Go to the OCI Identity Domain console, navigate to Identity Provider, and select the provider.
2. Click **Configure JIT** and confirm the JIT mappings have been created.

Step 8: 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 Microsoft login page.
6. Provide your identity provider user credentials.
7. On successful authentication, you are logged in to the OCI Console.