

Oracle® Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Identity Federation (When using SCIM APIs for User Provisioning)



Release 23.1.1
F87711-01
March 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation (When using SCIM APIs for User Provisioning), Release 23.1.1

F87711-01

Copyright © 2023, Oracle and/or its affiliates.

Contents

1 Steps to Configure Identity Federation in OCI IAM Identity Domain without Just-In-Time Provisioning

Step 1: Download the SAML Metadata in OCI IAM Identity Domain	1-1
Step 2: Add OCI IAM Identity Domain as a Service Provider (SP) in the Identity Provider (IDP)	1-1
Step 3: Download the Identity Provider SAML Metadata Document	1-2
Step 4: Add the Identity Provider in OCI IAM Identity Domains	1-2
Step 5: Test SSO Between Identity Provider and OCI IAM	1-3

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 set up OPERA Cloud services SSO with 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
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.

Step 1: Download 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: Add OCI IAM Identity Domain as a Service Provider (SP) in the Identity Provider (IDP)

1. It is required to add OCI IAM Identity Domain as the service provider in your identity using the metadata downloaded earlier.
2. It is required to map the name the Name identifier(Name ID) value field as the username.

Step 3: Download the Identity Provider SAML Metadata Document

- 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: Add the Identity Provider in OCI IAM Identity Domains

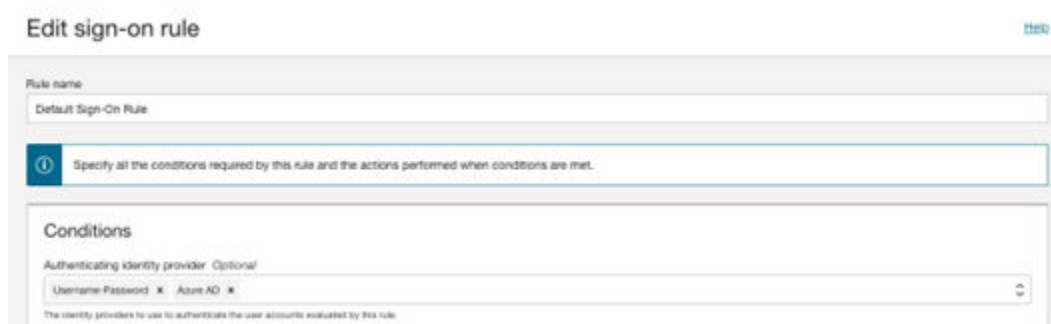
Enter the identity provider details by following these steps:

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 screenshot.

The screenshot displays the 'Identity Provider Metadata' configuration interface. At the top, there is a status message 'Metadata is saved.' and an 'Upload' button. Below this, several configuration fields are visible: 'Issuer ID *' (with a blurred input field), 'Signature Hashing Algorithm' (set to 'SHA-256'), 'Include Signing Certificate' (checkbox is unchecked), and 'Requested NameID Format' (set to '<None Requested>'). A red rectangular box highlights the 'Identity Provider User Attribute' and 'Oracle Identity Cloud Service User Attribute' dropdown menus, both of which have blurred selection options.

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: Test SSO Between Identity Provider and OCI IAM

In this section, you can test that federated authentication works between OCI IAM and customer's identity provider.

1. Open a [supported browser](https://cloud.oracle.com) 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.