

Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Identity Federation with Okta



Release 24.2
G11513-01
July 2024

ORACLE®

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Identity Federation with Okta, Release 24.2

G11513-01

Copyright © 2023, 2024, Oracle and/or its affiliates.

Contents

1 Configuring Identity Federation in OCI IAM Identity Domain when using Okta as the Identity Provider

1. Download the SAML Metadata in OCI IAM Identity Domain	1-1
2. Create an Application in Okta for OCI IAM Identity Domain	1-3
3. Configure Okta as an Identity Provider in OCI IAM Identity Domain	1-3
4. Configure Okta	1-5
5. Add Okta Identity Provider to IdP Policy in OCI Console	1-5
6. Test Single Sign On	1-6

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 single sign on (SSO) with customer identity provider. This document must be followed only if the customer identity provider is **Okta**.

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

Configuring Identity Federation in OCI IAM Identity Domain when using Okta as the Identity Provider

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 (SSO) 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 set up Okta as an IdP, with OCI IAM Identity Domain acting as SP. By setting up federation between Okta and OCI IAM Identity Domain, you enable users' access to OPERA Cloud Services using user credentials that Okta authenticates.

1. First, gather the information needed from OCI IAM.
2. Configure Okta as an IdP for OCI IAM.
3. Configure OCI IAM so Okta acts as IdP.
4. Create IdP policies in OCI IAM.
5. Test that federated authentication works between OCI IAM and Okta.



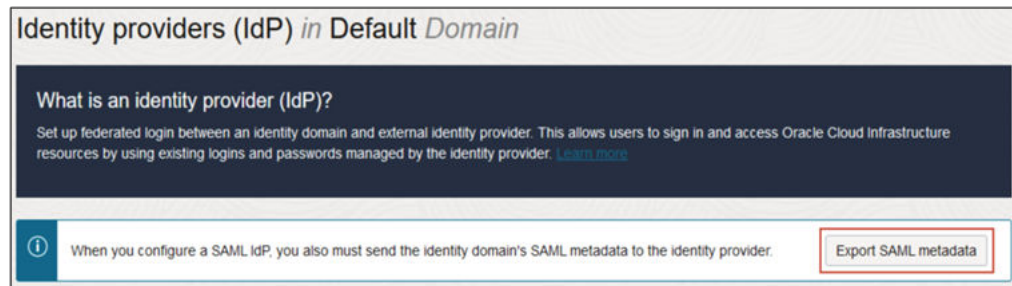
Note:

Follow this document only if your identity provider is **Okta**.

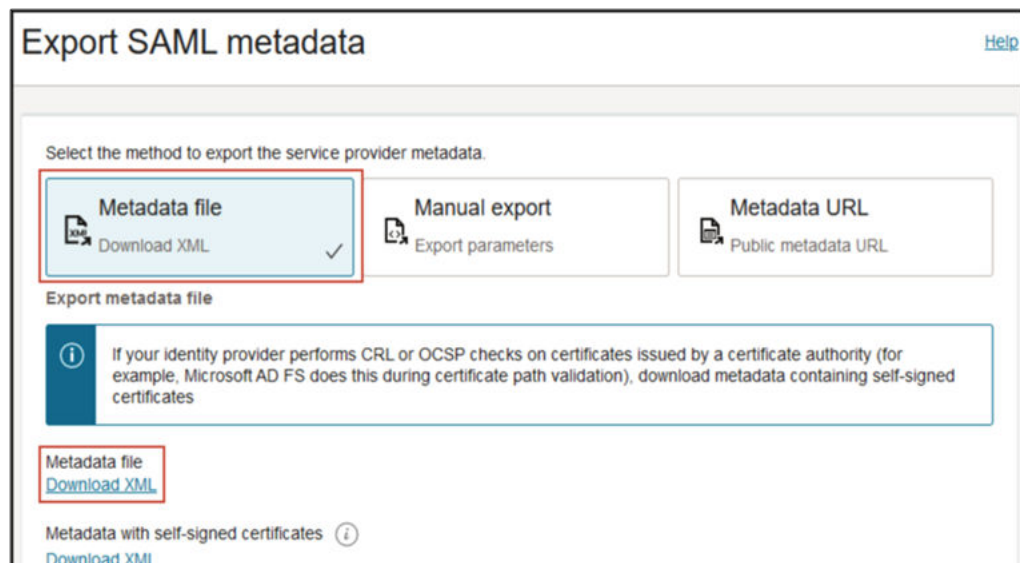
1. Download the SAML Metadata in OCI IAM Identity Domain

You need the IdP SAML metadata from your OCI IAM identity domain to import into the Okta application you create. OCI IAM provides a direct URL to download the metadata of the identity domain you are using. Okta uses the OCI domain URL to connect to OCI IAM.

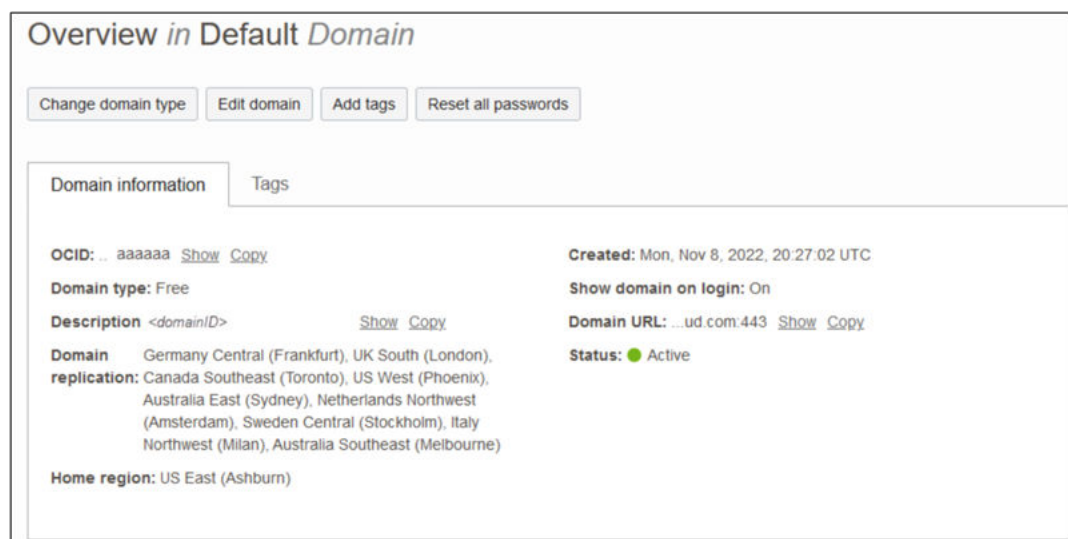
1. Open a [supported browser](#) and enter the following Console URL: <https://cloud.oracle.com>.
2. Enter your Cloud Account Name, also referred to as your tenancy name, and click **Next**.
3. Select the identity domain to sign in to. This is the identity domain that is used to configure SSO, for example Default.
4. Sign in with your username and password.
5. Open the navigation menu and click **Identity & Security**. Under Identity, click **Domains**.
6. 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. Next, click **Security** and then click **Identity providers**.
7. Click **Export SAML metadata**.



8. Select the **Metadata file** option and click **Download XML**.



9. Rename the downloaded XML file to OCIMetadata.xml.
10. Return to the identity domain overview by clicking the identity domain name in the breadcrumb navigation trail. Click **Copy** next to the Domain URL in Domain information and save the URL. This is the OCI IAM domain URL that you will use later.



2. Create an Application in Okta for OCI IAM Identity Domain



Note:

You can skip this step if the enterprise application for OCI is already created as part of Okta Integration with OCI IAM Identity Domain for user lifecycle.

Create an app in Okta and make note of the values you will need later.

1. In the browser, sign into Okta using the following URL where **<OktaOrg>** is the prefix for your organization with Okta: <https://<OktaOrg>-admin.okta.com>
2. In the left menu, click **Security** and choose **Applications** and then click **Browse App Catalog**.
3. Search for Oracle Cloud and select **Oracle Cloud Infrastructure IAM** from the available options.
4. Click **Add Integration**.
5. Under General settings, enter a name for the application, for example OCI IAM, and click **Done**.
6. In the application details page for your new application, click the **Sign On** tab, and under SAML Signing Certificates, click **View SAML setup instructions**.
7. On the View SAML setup instructions page, make note of the following:
 - Entity ID
 - SingleLogoutService URL
 - SingleSignOnService URL
8. Download and save the certificate with a file extension of “.pem.”

3. Configure Okta as an Identity Provider in OCI IAM Identity Domain

Create an IdP for Okta on the OCI Console.

1. In the OCI Console in the domain you are working in, click **Security** and then click **Identity providers**.
2. Click **Add IdP** and then click **Add SAML IdP**.
3. Enter a name for the SAML IdP, for example, Okta. Click **Next**.
4. On the Exchange metadata page, ensure that Enter IdP metadata is selected.
5. Enter the following from step 6 in [2. Create an Application in Okta for OCI IAM Identity Domain](#).
 - For Identity provider issuer URI: Enter the **ID**.
 - For SSO service URL: Enter the **SingleSignOnService URL**.
 - For SSO service binding: Select **POST**.

- For Upload identity provider signing certificate: Use the .pem file of the Okta certification.

- On the Map attributes page:
 - For Requested NameId format, choose **None**.
 - For Identity provider user attribute: Choose **SAML assertion Name ID**.
 - For Identity Domain user attribute: Choose **UserName**.
- Click **Next**.
- Review and click **Create IDP**.
- On the What's Next page, click **Activate** and then click **Add to IdP policy**.
- Click **Default Identity Provider Policy** to open it and then click the **Actions** menu () for the rule and click **Edit IdP rule**.
- Click in **Assign identity providers** and then click **Okta** to add it to the list.
- Click **Save** changes.
- Download the SP Certificate.
- In the OCI Console in the domain in which you are working, click **Security** and then click **Identity providers**.
- Click **Okta**.
- On the Okta IdP page, click **Service Provider metadata**.

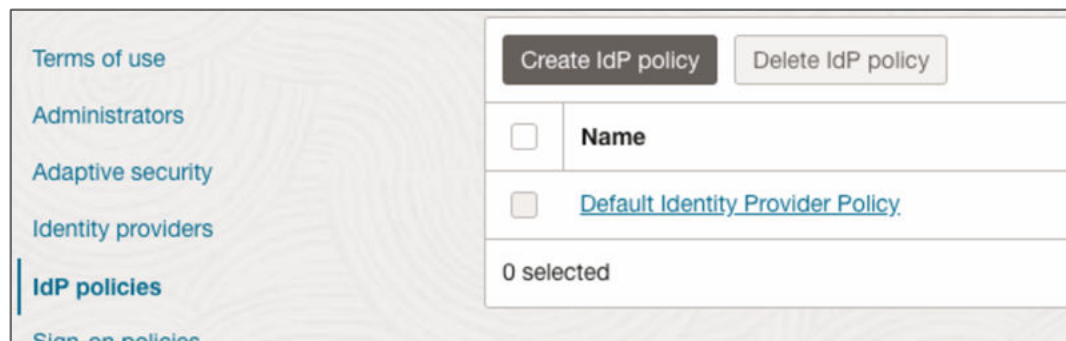
17. Click **Download** next to Service Provider signing certificate to download the SP signing certificate and save it.

4. Configure Okta

1. In the Okta console, click **Application** and then click the new application **OCI IAM**.
2. Go to the **Sign On** tab and click **Edit**.
3. Select **Enable Single Logout**.
4. Browse to the certificate you downloaded from the OCI IAM Console in the previous step and click **Upload**.
5. Scroll down to Advance Sign-on Settings and enter the following:
 - Oracle Cloud Infrastructure IAM GUID: Enter the **OCI IAM domain URL** from step 10 in 1. [Download the SAML Metadata](#) in OCI IAM Identity Domain.
 - Set the Application username format to **Email**.
6. Click **Save**.
7. Go to the Assignments tab, assign users who you want to have access to this application.
8. Click **Next**.

5. Add Okta Identity Provider to IdP Policy in OCI Console

1. In the OCI Console in the domain you are working in, click **Security** and then click **IdP policies**.
2. Click **Default Identity Provider Policy** and edit the **Default IDP Rule**.



3. Under Assigned Identity Providers, add the IdP that was created for Okta and Save your changes.

Edit identity provider rule

Rule name

Default IDP Rule

Assign identity providers

Username-Password x

4. Add IdP to Sign-on policy in IAM Domain:
 - a. Navigate to **Sign-on policies** under Security.
 - b. Edit the **Default Sign-On Policy**.
 - c. Under Sign-on rules, edit the **Default Sign-On Rule**.
 - d. Under Conditions, Authenticating identity provider, add the **Okta Identity Provider**.

Security

Sign-on policies in OCIMVBE Domain

In order to further improve the security posture of your tenancy, Oracle recommends that you keep multi-factor authentication enabled. See [OCI Security recommendations](#).

Create sign-on policy Actions

☐	Name	Description
☐	Default Sign-On Policy	Default Sign on Policy for Tenant
☐	OPERA Cloud OCI Console Login Policy	Restrict Access to OCI Console
☐	Security Policy for OCI Console	The Security Defaults to secure OCI Console

6. Test Single Sign On

1. Enter the following Console URL: <https://cloud.oracle.com>
2. Enter your **Cloud Account Name**, also referred to as your tenancy name and click **Next**.
3. Sign in with your **username** and **password**.
4. Select the **domain** for which you configured Okta IdP.
5. On the sign-in page, click the **Okta** icon.
6. Enter your **Okta** credentials. You are now signed in to the OCI Console.