

# Federating Oracle Access Manager to Oracle Cloud Infrastructure

---

For Tenancies in Regions That Do Not Use Identity Domains

February 2022, version 1.3  
Copyright © 2022, Oracle and/or its affiliates  
Public

## Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

## Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
February 2022	Added note that this document is applicable only to tenancies in regions that have <i>not</i> been updated to use identity domains
August 2021	Updated template and steps
August 2019	Corrected error in attribute mapping value
August 2018	Initial publication

## Table of Contents

---

<b>Overview</b>	<b>4</b>
<b>Audience</b>	<b>4</b>
<b>Prerequisites</b>	<b>4</b>
<b>Process for Federating OCI to Oracle Access Manager</b>	<b>4</b>
Step 1: Collect Federation Metadata and Configure the Trust Relationship	4
Step 2: Download the IdP Metadata and Configure the Service Provider	5
Step 3: Set Up Federation with Oracle Access Manager	8
Step 4: Test the Configuration	8

## Overview

This document provides the steps required to configure Oracle Cloud Infrastructure (OCI) federation with Oracle Access Manager. Oracle Access Manager is a fully supported identity provider (IdP) for OCI that supports the SAML 2.0 protocol.

---

**Note:** This document is applicable to tenancies in regions that have *not* been updated to use identity domains.

---

## Audience

This document is intended for the following audiences:

- Customers who want to evaluate OCI and use Oracle Access Manager as the IdP to authenticate with the Oracle Cloud Console.
- Consultants and solutions architects who want to demonstrate OCI functionality in a customer environment.

## Prerequisites

Before you begin the process, ensure that you meet the following prerequisites:

- You have Oracle Access Manager 11gR2PS3 or 12cPS3.
- You have an OCI tenancy with at least one administrative user and at least one group set up. We recommend setting up groups for OCI access with an easily recognizable prefix, such as OCI\_Admins or OCI\_Users. You should also have users in each of the groups that you created.
- You are familiar with the general concepts of identity federation.

## Process for Federating OCI to Oracle Access Manager

At a high level, the process to set up federation of OCI with Oracle Access Manager is as follows:

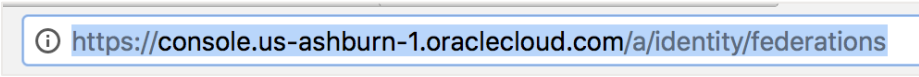
1. In the Oracle Cloud Console, collect the required federation metadata to configure the trust relationship with Oracle Access Manager.
2. In the Oracle Access Management Console, configure an OCI service partner for your tenancy (that is, a trusted relying party) and assert group membership.
3. In the Oracle Cloud Console, set up federation with Oracle Access Manager and map the appropriate Oracle Access Manager groups to OCI groups.
4. Test the configuration by logging in to OCI using identities from Oracle Access Manager.

Detailed steps are provided in the following sections.

### Step 1: Collect Federation Metadata and Configure the Trust Relationship

1. In the Oracle Cloud Console, open the navigation menu. Click **Identity & Security**, and under **Identity**, click **Federation**.

The URL for your data center is displayed in your browser.

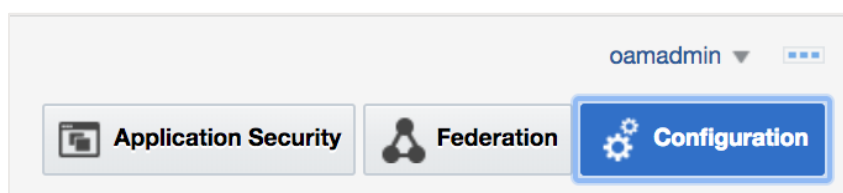


<https://console.us-ashburn-1.oraclecloud.com/a/identity/federations>

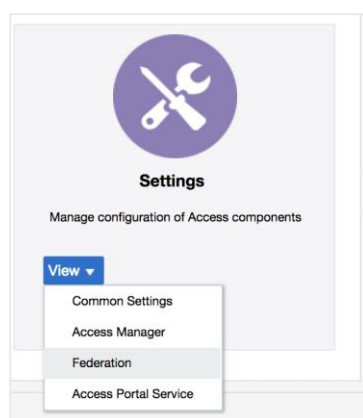
2. In the message on the page, click the **Download this document** link to download the Oracle Cloud Infrastructure Federation Metadata document.
3. Save the document as `OCImetadata.xml` for import into Oracle Access Manager in the next section.

## Step 2: Download the IdP Metadata and Configure the Service Provider

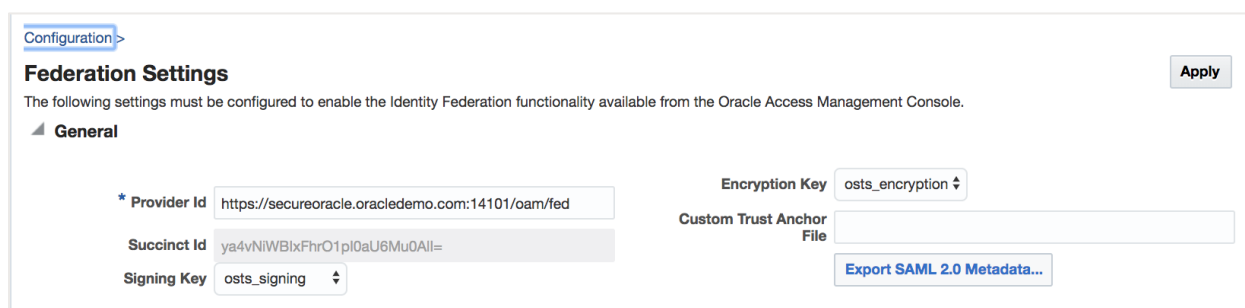
1. Sign in to your Oracle Access Manager account ([http://<your\\_oam\\_host>/oamconsole/faces/admin.jspx](http://<your_oam_host>/oamconsole/faces/admin.jspx)) as an administrator.
2. At the top of the page, click **Configuration**.



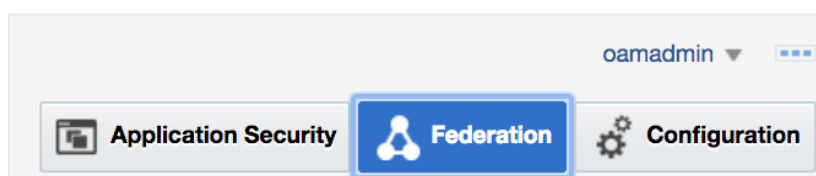
3. Under **Settings**, click **View** and then click **Federation**.



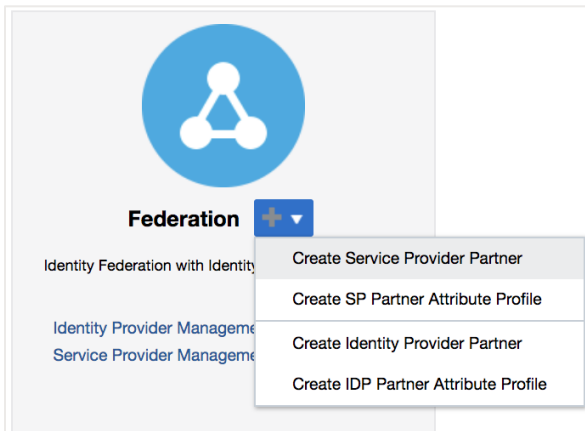
4. Click **Export SAML 2.0 Metadata**. You import this metadata into OCI in a later step.



5. Edit the exported file and remove the `<md:RoleDescriptor> ...</md:RoleDescriptor>` section. Save the file.
6. At the top of the console page, click **Federation**.

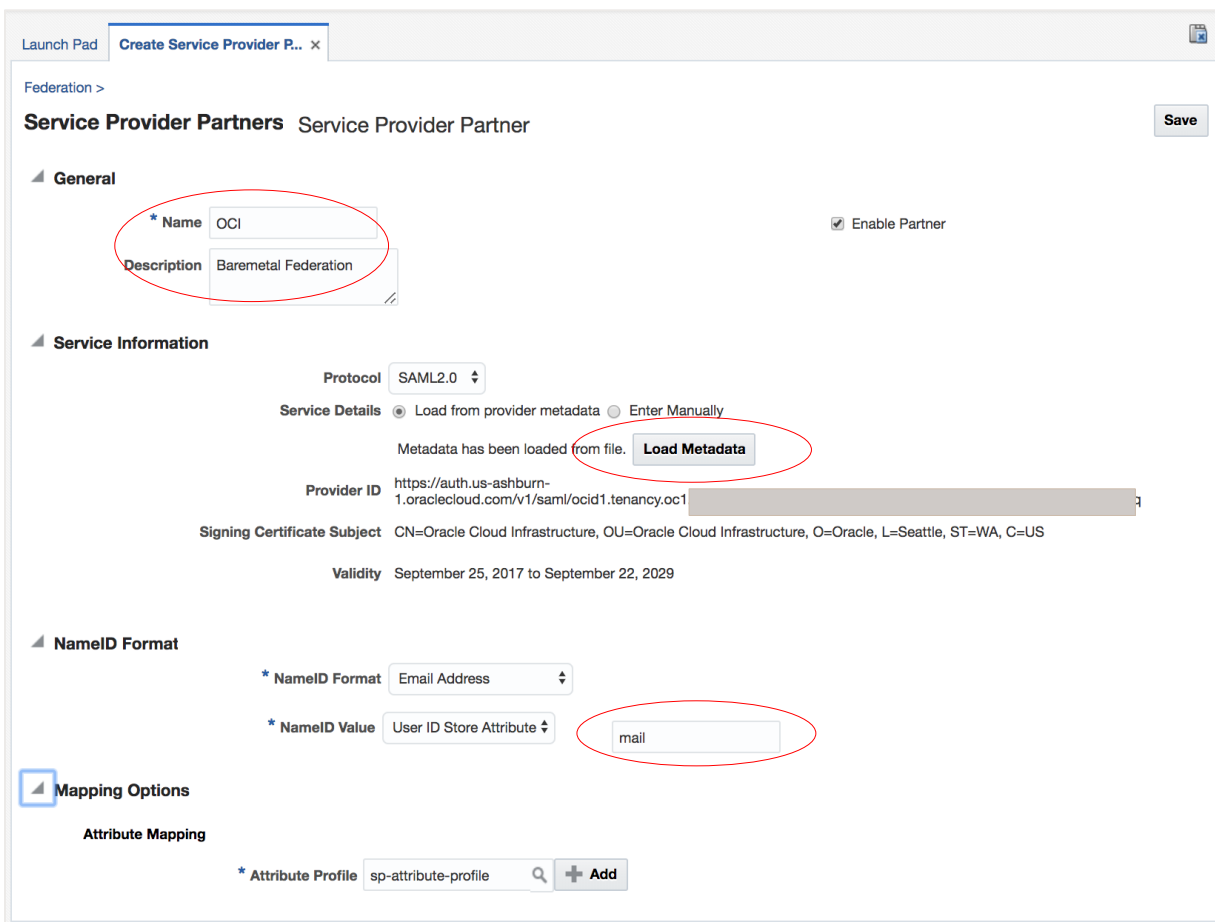


7. Click the plus (+) symbol next to **Federation** and select **Create Service Provider Partner**.

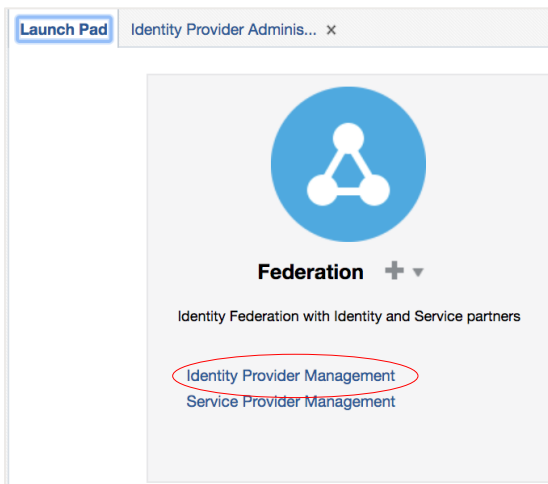


8. Enter the following values:

- For **Name**, enter **OCI**.
- Provide a brief description.
- Click **Load Metadata** and upload the OCImetadata.xml file.
- For **NameID Format**, select **Persistent**.
- For the **NameID Value**, enter **mail**.



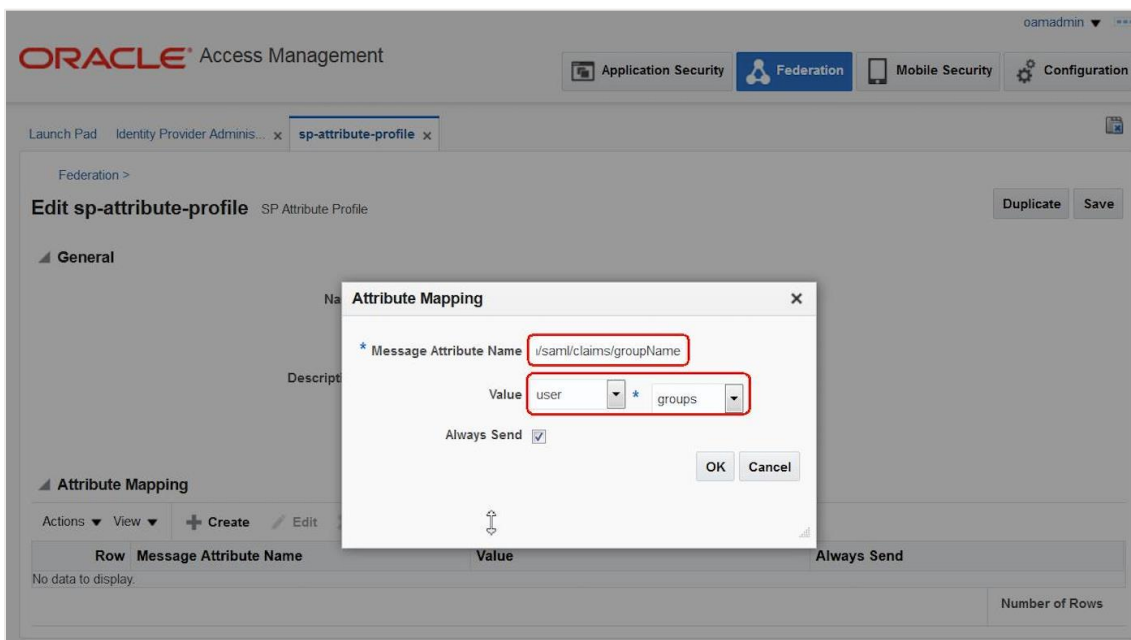
9. Click the **Launch Pad** tab, and then click **Identity Provider Management**.



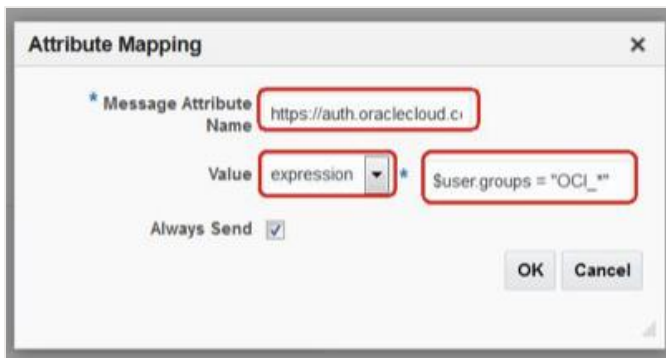
10. Search for and then click **sp-attribute-profile**.

11. Create an attribute mapping with the following values:

- **Message Attribute Name:** `https://auth.oraclecloud.com/saml/claims/groupName`
- **Value:** `user * groups`



Oracle Cloud Infrastructure can accept only 50 group memberships. If users have more than 50 group memberships, we recommend sending groups related to OCI only (hence the recommendation to prepend **OCI** to OCI groups). You can do this in Oracle Access Manager by changing from **user** to **expression** and entering the following expression: `$user.groups = "OCI_*`



Oracle Access Manager's default behavior is to send the group attributes in comma-separated format if the user belongs to multiple groups. Additionally, **Always Send** is set to **true**.

12. To change this behavior to send multiple-value attributes across in single entries, follow the [instructions in the Oracle Access Management documentation](#).
13. Restart the Oracle Access Manager server.

### Step 3: Set Up Federation with Oracle Access Manager

Go back to the Oracle Cloud Console and configure federation with Oracle Access Manager for your tenancy.

1. In the navigation menu, click **Identity & Security**, and under **Identity**, click **Federation**.
2. Click **Add Identity Provider**.
3. In the **Add Identity Provider** panel, enter the following values:
  - o Enter a name, for example, **OAM**.
  - o Provide a description.
  - o For **Type**, select **Microsoft Active Directory Federation Service (ADFS)** or **SAML 2.0 Compliant Identity Provider**.
  - o Upload the federation metadata XML file that you exported from Oracle Access Manager and edited (in Step 2).
4. Click **Continue**.
5. Map your Oracle Access Manager groups to your OCI groups. For example, map identity provider group **OCIAdmins** to OCI group **Administrators**.
6. Click **Add Provider**.

### Step 4: Test the Configuration

Now that you have set up federation with Oracle Access Manager, perform the following few steps to verify that the federation is configured correctly.

1. Sign out of the Oracle Cloud Console and sign out of Oracle Access Manager.
2. Go to the signin page for your Oracle Cloud Infrastructure tenancy.  
You should see a new option to sign in using SSO.
3. In the **Identity Provider** list, select **OAM** (or whatever you named the IdP), and then click **Continue**.  
The sign-in page redirects to Oracle Access Manager.




4. Sign in using one of your users' Oracle Access Manager credentials.
5. On the next page, confirm that your user is successfully signed in to the Oracle Cloud Console.
6. Confirm that this user has access to the appropriate resources.

For example, if the user was in the OCIAdmins group in Oracle Access Manager and you mapped that group to the Administrators group in Oracle Cloud Infrastructure, that user should be able to accomplish any task in the Oracle Cloud Console, such as creating users or compartments.

---

## Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at **oracle.com/contact**.

 [blogs.oracle.com](https://blogs.oracle.com)

 [facebook.com/oracle](https://facebook.com/oracle)

 [twitter.com/oracle](https://twitter.com/oracle)

---

Copyright © 2022, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0120