

Federating Oracle Access Manager to Oracle Cloud Infrastructure

ORACLE WHITE PAPER | AUGUST 2018





Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. 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 for Oracle's products remains at the sole discretion of Oracle.

Revision History

The following revisions have been made to this white paper since its initial publication:

Date	Revision
August 31, 2018	Initial publication

You can find the most recent versions of the Oracle Cloud Infrastructure white papers at <https://cloud.oracle.com/iaas/technical-resources>.



Table of Contents

Overview	4
Audience	4
Prerequisites	4
Process for Federating Oracle Cloud Infrastructure to Oracle Access Manager	4
Step 1: Collect Federation Metadata and Configure the Trust Relationship	5
Step 2: Download the IdP Metadata and Configure the Service Provider	5
Step 3: Set Up Federation with Oracle Access Manager	10
Step 4: Test the Configuration	11



Overview

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

Audience

This document is intended for the following audiences:

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

Prerequisites

Before you begin the process, ensure that you have met the following prerequisites:

- You have Oracle Access Manager 11gR2PS3 or 12cPS3.
- You have an Oracle Cloud Infrastructure tenancy with at least one administrative user and at least one group set-up. We recommend setting up groups for Oracle Cloud Infrastructure 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 Oracle Cloud Infrastructure to Oracle Access Manager

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

1. In the Oracle Cloud Infrastructure Console, collect the required federation metadata to configure the trust relationship with Oracle Access Manager.
2. In the Oracle Access Management Console, configure an Oracle Cloud Infrastructure service partner for your tenancy (that is, a trusted relying party) and assert group membership.

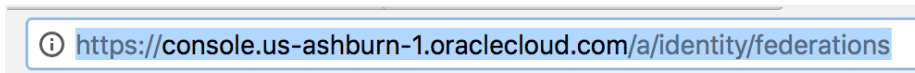
3. In the Oracle Cloud Infrastructure Console, set up federation with Oracle Access Manager and map the appropriate Oracle Access Manager groups to Oracle Cloud Infrastructure groups.
4. Test the configuration by logging in to Oracle Cloud Infrastructure using identities from Oracle Access Manager.

Detailed steps are provided in the following sections.

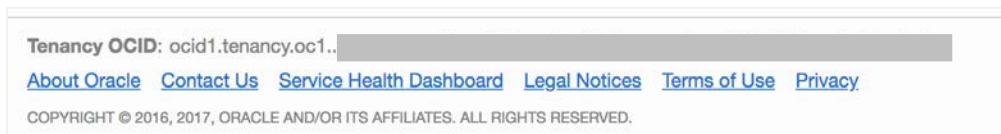
Step 1: Collect Federation Metadata and Configure the Trust Relationship

1. In the Oracle Cloud Infrastructure Console, open the navigation menu. Under **Governance and Administration**, go to **Identity** and click **Federation**.

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

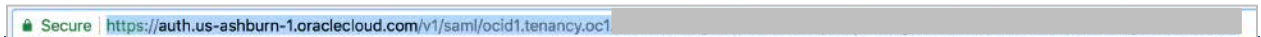


At the bottom of the Federation page, the tenancy OCID is displayed.



2. Click the link near the bottom of the page to download the XML document that describes Oracle Cloud Infrastructure endpoint and certificate information. The URI looks as follows, with your region and tenancy OCID:

`https://auth.us-<region>-1.oraclecloud.com/v1/saml/<tenancy_OCID>/metadata.xml`

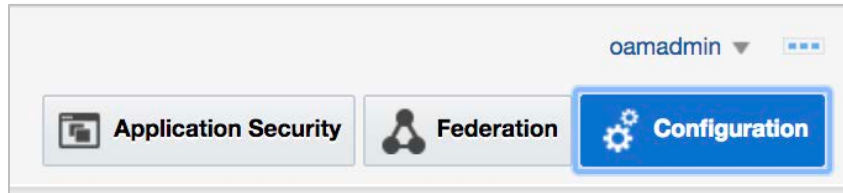


3. Save the page as `OCImetadata.xml` for import into Oracle Access Manager in the next section.

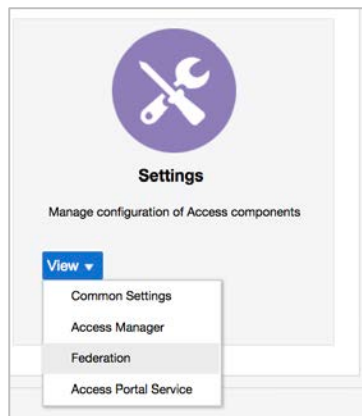
Step 2: Download the IdP Metadata and Configure the Service Provider

1. Sign in to your Oracle Access Manager account (`http://<your_oam_host>/oamconsole/faces/admin.jspx`) as an administrator.

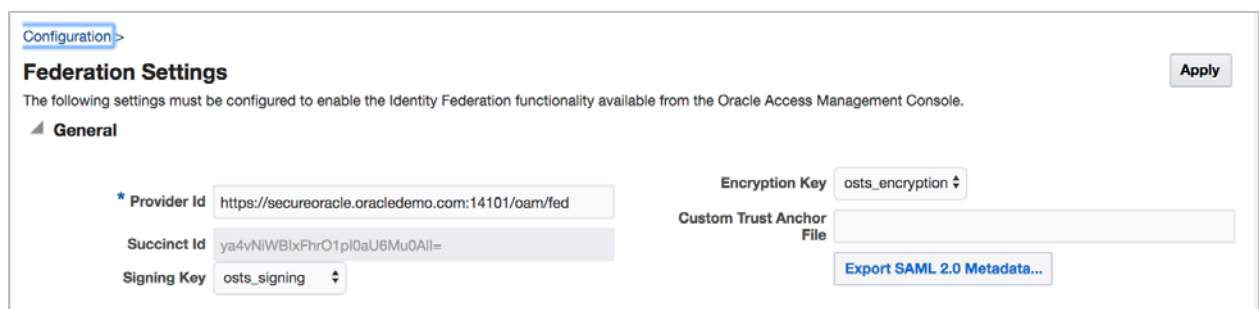
- At the top of the page, click **Configuration**.



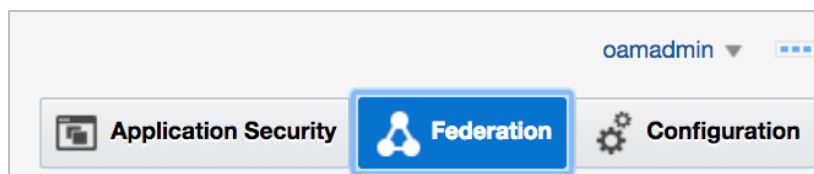
- Under **Settings**, click **View** and then click **Federation**.



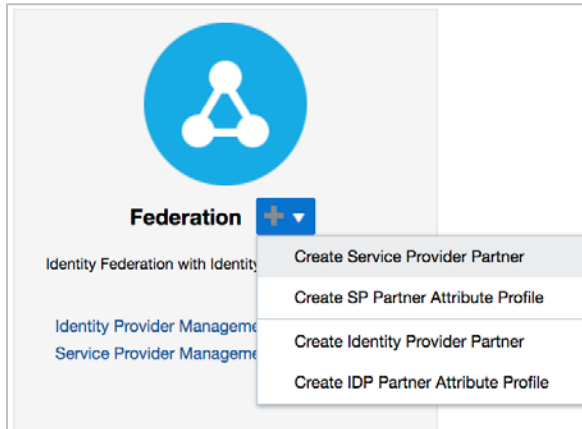
- Click **Export SAML 2.0 Metadata**. You import this metadata into Oracle Cloud Infrastructure in a later step.



- Edit the exported file and remove the `<md:RoleDescriptor> ...</md:RoleDescriptor>` section. Save the file.
- 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**.

Launch Pad **Create Service Provider R...** x

Federation >

Service Provider Partners Service Provider Partner

Save

General

* Name OCI Enable Partner

Description Baremetal Federation

Service Information

Protocol SAML2.0

Service Details Load from provider metadata Enter Manually

Metadata has been loaded from file. **Load Metadata**

Provider ID https://auth.us-ashburn-1.oraclecloud.com/v1/saml/ocid1.tenancy.oc1... [REDACTED]

Signing Certificate Subject CN=Oracle Cloud Infrastructure, OU=Oracle Cloud Infrastructure, O=Oracle, L=Seattle, ST=WA, C=US

Validity September 25, 2017 to September 22, 2029

NameID Format

* NameID Format Persistent

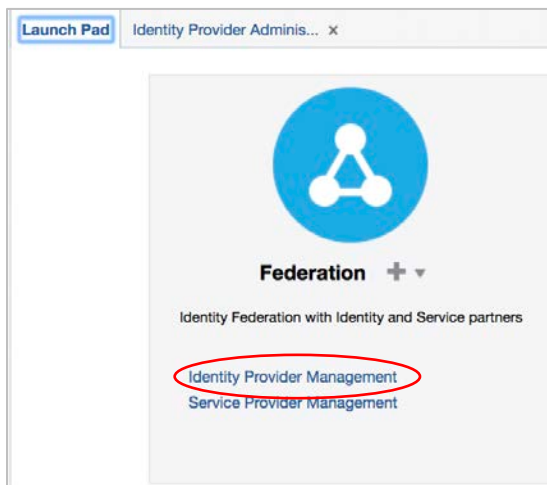
* NameID Value User ID Store Attribute

Mapping Options

Attribute Mapping

* Attribute Profile sp-attribute-profile

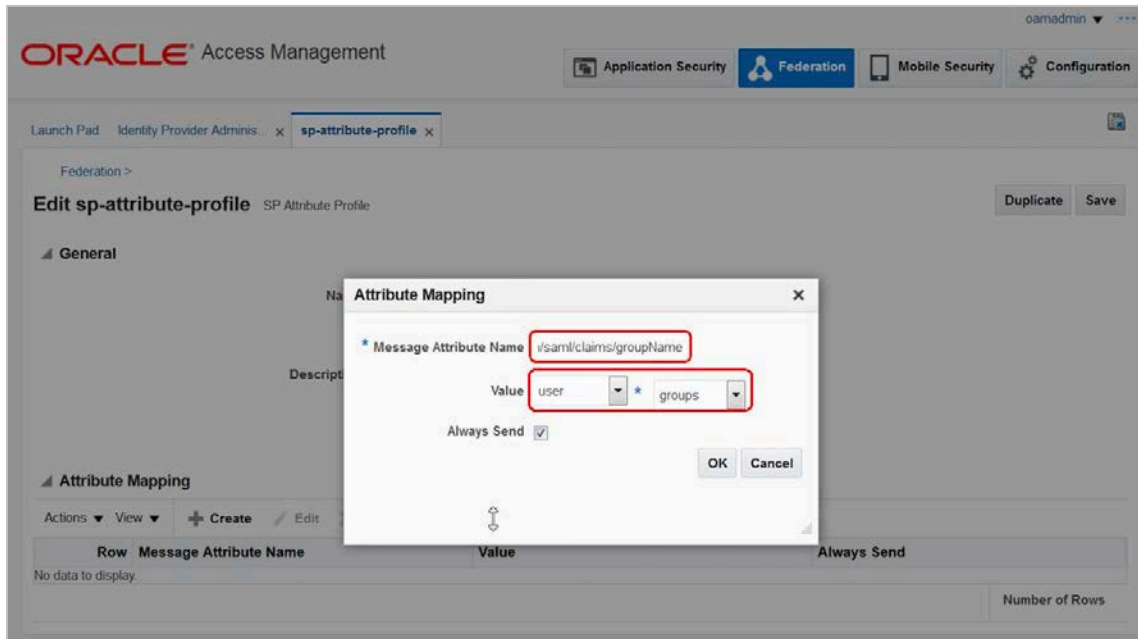
9. Click the **Launch Pad** tab, and then click **Identity Provider Management**.



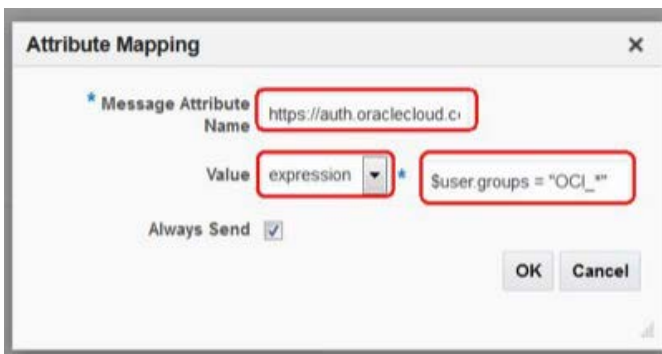
10. Search for and then click **sp-attribute-profile**.


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 Oracle Cloud Infrastructure only (hence the recommendation to prepend **OCI** to Oracle Cloud Infrastructure 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 Infrastructure Console and configure federation with Oracle Access Manager for your tenancy.

1. Under **Governance and Administration** in the navigation menu, go to **Identity** and click **Federation**.
2. Click **Add Identity Provider**.
3. In the **Add Identity Provider** dialog box, enter the following values:
 - Enter a name, for example, **OAM**.
 - Provide a description.
 - For **Type**, select **Microsoft Active Directory Federation Service (ADFS) or SAML 2.0 Compliant Identity Provider**.
 - In the **XML** section, upload the federation metadata XML file that you exported from Oracle Access Manager and edited (in Step 2).
4. Click **Continue**.


- In the **Mapping** section of the **Add Identity Provider** dialog box, map your Oracle Access Manager groups to your Oracle Cloud Infrastructure groups. For example, identity provider group **OCIAdmins** could be mapped to Oracle Cloud Infrastructure group **Administrators**.

- Click **Submit**.

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.

- Sign out of the Oracle Cloud Infrastructure Console and sign out of Oracle Access Manager.
- Go to the sign-in 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 Infrastructure Console.
6. Confirm that this user has access to the appropriate resources.




For example, if the user was in the OCIAAdmins 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 Infrastructure Console, such as creating users or compartments.



Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, 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. 0818

Federating Oracle Access Manager to Oracle Cloud Infrastructure
August 2018
Author: David Lee



Oracle is committed to developing practices and products that help protect the environment.