Federating Okta and Oracle Cloud Infrastructure
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.
Table of Contents

Overview 4
Audience 4
Prerequisites 4
Process for Federating Okta and Oracle Cloud Infrastructure 4
  Step 1: Collect Required Federation Metadata 5
  Step 2: Configure the Console Login Page for Your Tenancy 5
  Step 3: Assign Users or Groups to the New Application 7
  Step 4: Set Up Federation with Okta 7
  Step 5: Test the Configuration 8
Overview

This document describes the steps required to configure Oracle Cloud Infrastructure federation with Okta. Okta is a fully supported identity provider (IDP) for Oracle Cloud Infrastructure because it supports SAML 2.0.

Audience

This document is intended for the following audiences:

- Customers who want to evaluate Oracle Cloud Infrastructure and use Okta as the identity provider 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 an Okta tenancy in which you can create an Okta application. Either an Enterprise account or a Developer account is acceptable.
- 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 OCIAdmins or OCIUsers. 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 Okta and Oracle Cloud Infrastructure

At a high level, the process to set up federation with Okta is as follows:

1. In the Oracle Cloud Infrastructure Console, collect the required federation metadata to configure the trust relationship with Okta.
2. In Okta, configure the console login page for your Oracle Cloud Infrastructure tenancy as an application (that is, a trusted relying party) and add the claim rules required to convey group memberships to Oracle Cloud Infrastructure.
3. In Okta, assign users and/or groups to your new Oracle Cloud Infrastructure Console application.
4. In the Oracle Cloud Infrastructure Console, set up federation with Okta and map the appropriate Okta groups to Oracle Cloud Infrastructure groups.

5. Test the configuration by logging in to Oracle Cloud Infrastructure using identities from Okta.

The following sections provide detailed instructions for each step.

**Step 1: Collect Required Federation Metadata**

In the Oracle Cloud Infrastructure Console, collect the required federation metadata to configure the trust relationship with Okta.

1. In the Oracle Cloud Infrastructure Console, click **Identity** and then click **Federation**.

2. Click the link at the bottom of the page to download the XML document that describes Oracle Cloud Infrastructure endpoint and certificate information. The URI looks as follows:

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

3. Record the following values from the XML file:
   - The **entityID** value
   - The **AssertionConsumerService Binding** value.

   These values are URIs that look as follows:

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

**Step 2: Configure the Console Login Page for Your Tenancy**

In Okta, you need to configure the console login page for your tenancy as an application (that is, a trusted relying party).

1. Sign in to your Okta account. We recommend using the Okta Classic UI.

2. From the **Applications** menu at the top of the page, select **Applications**.

3. Click **Add Application**.

4. Click **Create New App**.
5. In the **Create a New Application** dialog box, select the following values:
   - **Platform**: Web
   - **Sign on method**: SAML 2.0

6. Click **Create**.

7. On the **General Settings** page of the **Create SAML Integration** screen, perform the following actions and then click **Next**:
   - Type a name for the application, such as OCI Console.
   - *(Optional)* Upload a logo.
   - Ensure that the **App visibility** check boxes are *not* selected.

8. On the next page, set up the following SAML configuration parameters:
   - **Single sign on URL**: Enter the AssertionConsumerService Binding location URI that you copied from the Oracle Cloud Infrastructure federation metadata XML document.
   - **Audience URI**: Enter the entityID that you copied from the Oracle Cloud Infrastructure federation metadata XML document.
   - **Default Relay State**: Leave blank.
   - **Name ID format**: Leave as **Unspecified**.
   - **Application username**: Leave as **Okta username**.

9. In the **Group Attribute Statements** section at the bottom of the page, set up the claim rules to convey group membership of the user to the Oracle Cloud Infrastructure Console. Create a new statement with the following parameters:
   - **Name**: https://auth.oraclecloud.com/saml/claims/groupName
   - **Name format**: basic
   - **Filter**: Use a filter that ensures that the groups you want conveyed to Oracle Cloud Infrastructure when the user logs in are in the claim. If you used our recommendation for groups names, you could use a filter such as “Starts with” “OCI”.

10. Click **Next**.

11. Select the option indicating that you’re an Okta customer adding an internal app.
12. Click **Finish**.

   You should be taken to the **Sign on** tab in the application configuration page. If not, then go there.

13. In the **Settings** section, click the **Identity Provider metadata** link.

   The Federation Metadata XML for your application from Okta is downloaded. You will need this file in “Step 4: Set Up Federation with Okta.”

### Step 3: Assign Users or Groups to the New Application

1. In the Okta Classic UI, select **Applications** from the **Applications** menu.

2. Select the new application that you just created (for example, OCI Console).

3. On the **Assignments** tab, click **Assign** and select **Assign to Groups**.

   We recommend that you choose **Assign to Groups** and select the groups from which you want users to log in to the Oracle Cloud Infrastructure Console. If you used our recommendation, all these groups are prefixed with **OCI** (for example, OCIAdmins or OCIUsers).

4. In the **Assign to Groups** dialog box, select the group and click **Assign**.

5. Click **Done**.

### Step 4: Set Up Federation with Okta

1. In the Oracle Cloud Infrastructure Console, click **Identity** and then click **Federation**.

2. Click **Add Identity Provider**.

3. Give the identity provider a name (for example, Okta) and provide a description.

4. Under **Type**, select **Microsoft Active Directory Federation Services (ADFS)**.

5. In the XML section, upload the federation metadata XML file that you saved from Okta in “Step 2: Configure the Console Login Page for Your Tenancy.”

6. Click **Continue**.
7. Map your Okta groups to your Oracle Cloud Infrastructure groups. For example, the identity provider group OCIAdmins could be mapped to the Oracle Cloud Infrastructure group Administrators.

8. Click Submit.

Step 5: Test the Configuration

Now that you have set up federation with Okta, perform a few steps to verify that it is configured correctly.

1. Log out of the Oracle Cloud Infrastructure Console, and log out of Okta.

   On the Oracle Cloud Infrastructure sign-in page for your tenancy, you should see a new option for signing in using SSO.

2. In the Identity Provider drop-down list, select Okta or whatever you named the identity provider. Then, click Continue.

   The sign-in page redirects to Okta.

3. Sign in by using one of your users’ Okta credentials.

4. Confirm that your user is successfully logged in to the Oracle Cloud Infrastructure Console.

5. Confirm that this user has access to the appropriate resources. For example, if the user was in the OCIAdmins group in Okta and you mapped that group to Administrators in Oracle Cloud Infrastructure, that user should be able to accomplish any task in the Console (for example, create new users, create new compartments, and so on).
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.

Federating Okta and Oracle Cloud Infrastructure
April 2018
Author: Martin Sleeman