Oracle Cloud Infrastructure Okta Configuration for Federation and Provisioning

For Tenancies in Regions That Do Not Use Identity Domains

February 2022, version 2.0

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 *not* been updated to use identity domains
November 2021	Updated with the new URL format for SCIM
April 2018	Initial publication

Table of Contents

Overview 4

Audience 4

Supported Features 4

Requirements 4

Configuration Steps 5

Known Issues and Troubleshooting 8

Overview

This document describes the steps required to configure Oracle Cloud Infrastructure (OCI) for federation and provisioning with Okta. Provisioning allows you to add API keys and other OCI credentials for your federated users. Okta is a fully supported identity provider (IdP) for OCI because it supports SAML 2.0.

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 Okta as the identity provider to authenticate with the Oracle Cloud Console
- Consultants and solutions architects who want to demonstrate OCI functionality in a customer environment

Supported Features

Oracle Cloud Infrastructure (OCI) supports the following provisioning features:

- Create users: New or existing users in Okta are pushed to OCI and displayed in the Oracle Cloud Console as federated users.
- Deactivate users: Users deactivated in Okta are automatically deactivated in OCI.
- Push groups: Okta groups can be mapped to groups in OCI.

The following features are not supported in OCI:

- Import users
- Import groups
- Sync password
- Update user attributes

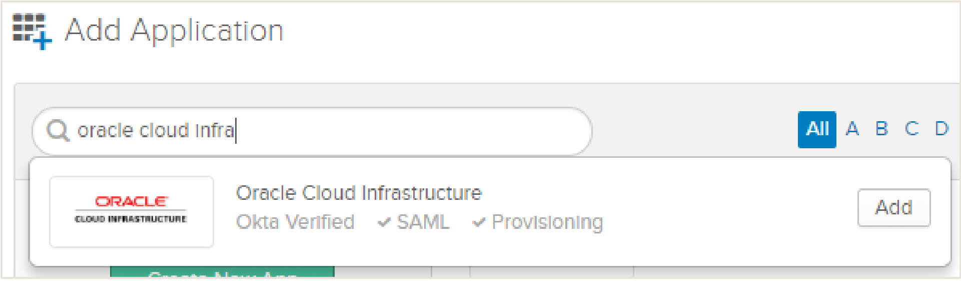
Requirements

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

- You have an Okta account in which you can create an Okta application. Either an enterprise account or a developer account is acceptable.
- You have an OCI tenancy with at least one administrative user and at least one group set up.
- In Okta, we recommend setting up groups for OCI access with an easily recognizable prefix, such as OCIAdmins or OCIUsers. Also, have users in each of the groups that you created.
- You're familiar with the general concepts of identity federation.

Configuration Steps

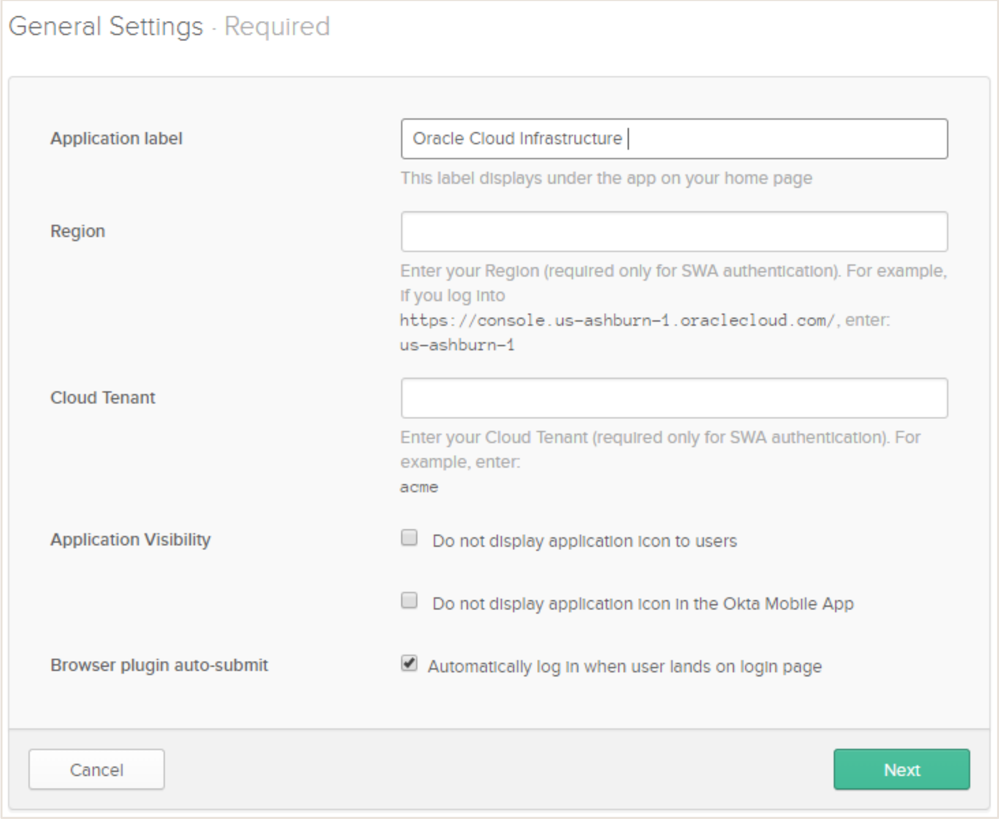
1. Log in to your Okta account.
2. Click **Add Application**, search for "Oracle Cloud Infrastructure," and click **Add**.



oracle cloud infra

Oracle Cloud Infrastructure
Okta Verified ✓ SAML ✓ Provisioning

3. On the **General** tab, enter an application label that makes sense to you, such as "Oracle Cloud Infrastructure," as shown in the following screenshot. You can ignore the **Region** and **Cloud Tenant** fields. Click **Next**.



General Settings · Required

Application label: Oracle Cloud Infrastructure
This label displays under the app on your home page

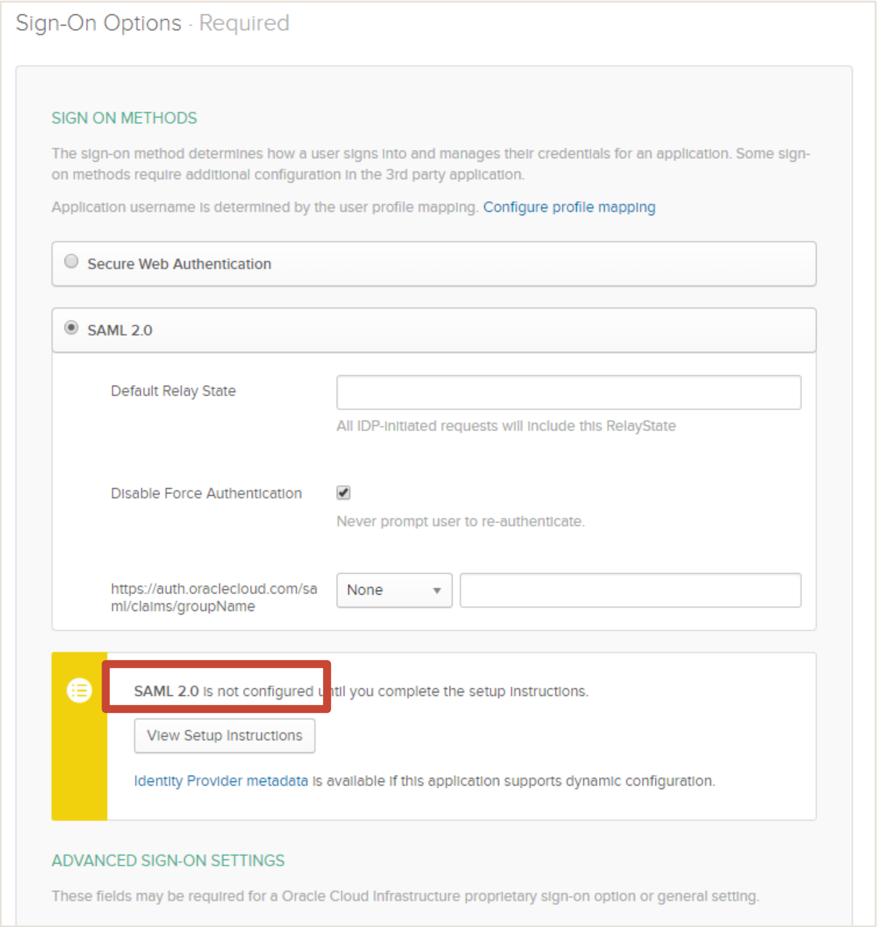
Region:
Enter your Region (required only for SWA authentication). For example, if you log into `https://console.us-ashburn-1.oraclecloud.com/`, enter: `us-ashburn-1`

Cloud Tenant:
Enter your Cloud Tenant (required only for SWA authentication). For example, enter: `acme`

Application Visibility:
☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile App

Browser plugin auto-submit:
☑ Automatically log in when user lands on login page

4. On the **Sign On** tab, click **Edit**. Then, click **View Setup Instructions** to see detailed instructions for completing the SAML setup. Follow the instructions.



Sign-On Options · Required

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ Secure Web Authentication

● SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState

Disable Force Authentication ☑

Never prompt user to re-authenticate.

https://auth.oraclecloud.com/saml/claims/groupName None ▾

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a Oracle Cloud Infrastructure proprietary sign-on option or general setting.

5. Use the default values for the rest of the settings on the **General**, **Sign On**, and **Import** tabs.

6. Click the **Provisioning** tab, and then click **Configure API Integration**.

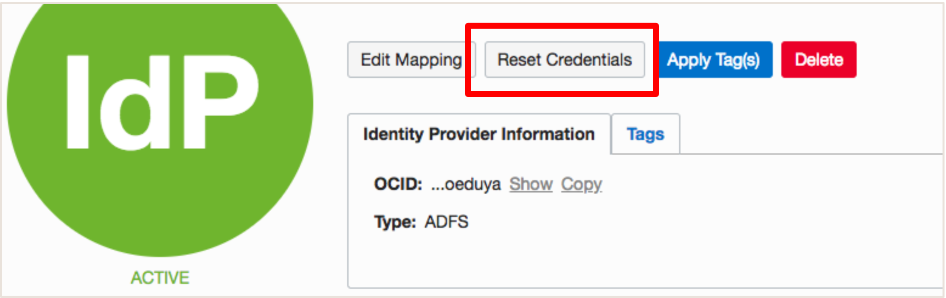
7. Select **Enable API Integration**.

8. To complete the API Integration settings, get the SCIM base URL and credentials (username and password).

   - The SCIM base URL follows the convention, `https://scim.<OCI-home-region-name>.oci.oraclecloud.com/v2`, where `<OCI-home-region-name>` is the same as the region name obtained in step 4 for the ACS location URL. For example, if the ACS location URL is `https://auth.us-ashburn-1.oraclecloud.com/v1/saml/ocid1.tenancy.oc1..aaaaaakdjsk...`, the region name is `us-ashburn-1`. So, the SCIM base URL is `https://scim.us-ashburn-1.oci.oraclecloud.com/v2`.
   - The username and password are the client ID and secret from the OCI setup. Get them as follows:

     A. In the Oracle Cloud Console, open the navigation menu. Under **Governance and Administration**, go to **Identity** and then click **Federation**. Click the name that you assigned to your Okta federation to see the details page.

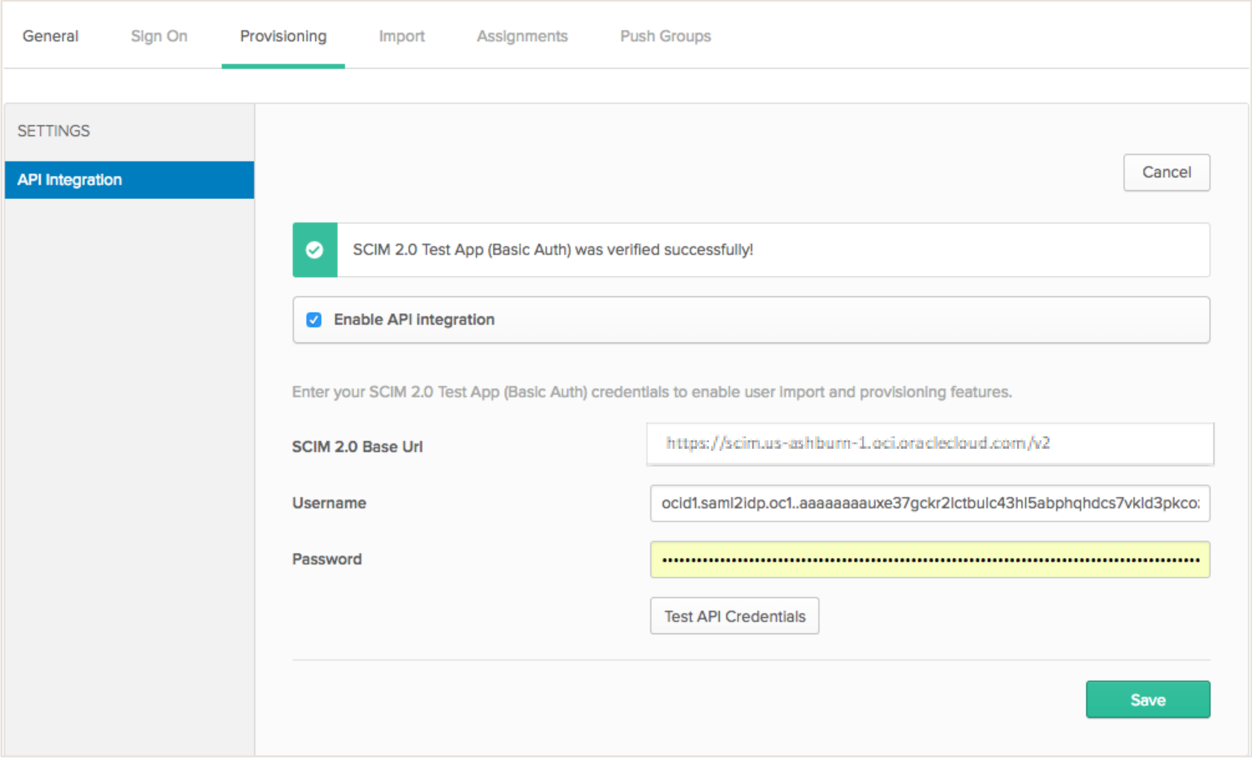
     B. Click **Reset Credentials**, as shown in the following screenshot, to display the credentials. Copy the client ID and secret.



OCID: ...oeduya

Type: ADFS

9. In the **API Integration** settings in Okta, enter the SCIM base URL, enter the client ID in the **Username** text box, and enter the secret in the **Password** text box.



SCIM 2.0 Test App (Basic Auth) was verified successfully!

☑ Enable API integration

Enter your SCIM 2.0 Test App (Basic Auth) credentials to enable user import and provisioning features.

SCIM 2.0 Base Url: https://scim.us-ashburn-1.oci.oraclecloud.com/v2

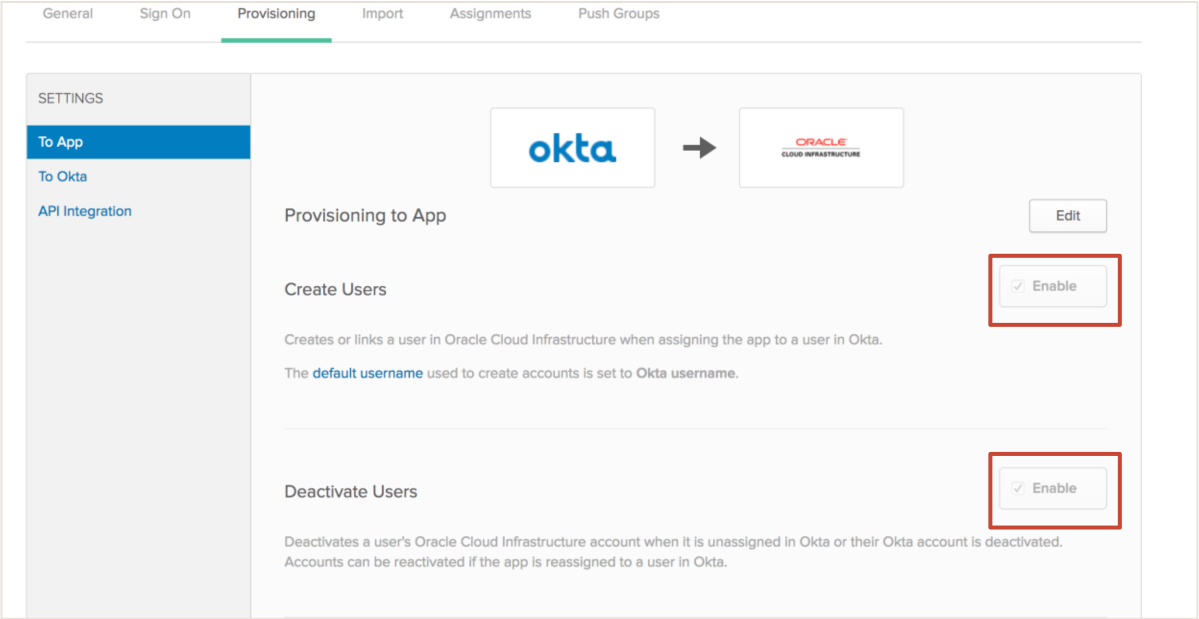
Username: ocid1.saml2idp.oc1..aaaaaaaauxe37gckr2lctbulc43hl5abphqhdcs7vkld3pkco:

Password: ••

10. Click **Test API Credentials** to ensure that the credentials are correct. You know that it works if you see a successful confirmation message (as shown in the preceding screenshot).

11. Click **Save**.

12. After you complete the previous step, the **To App** and **To Okta** configurations are created under **Settings**. In the **Provisioning to App** settings, enable **Create Users** and **Deactivate Users**.



Provisioning to App

Create Users ☑ Enable

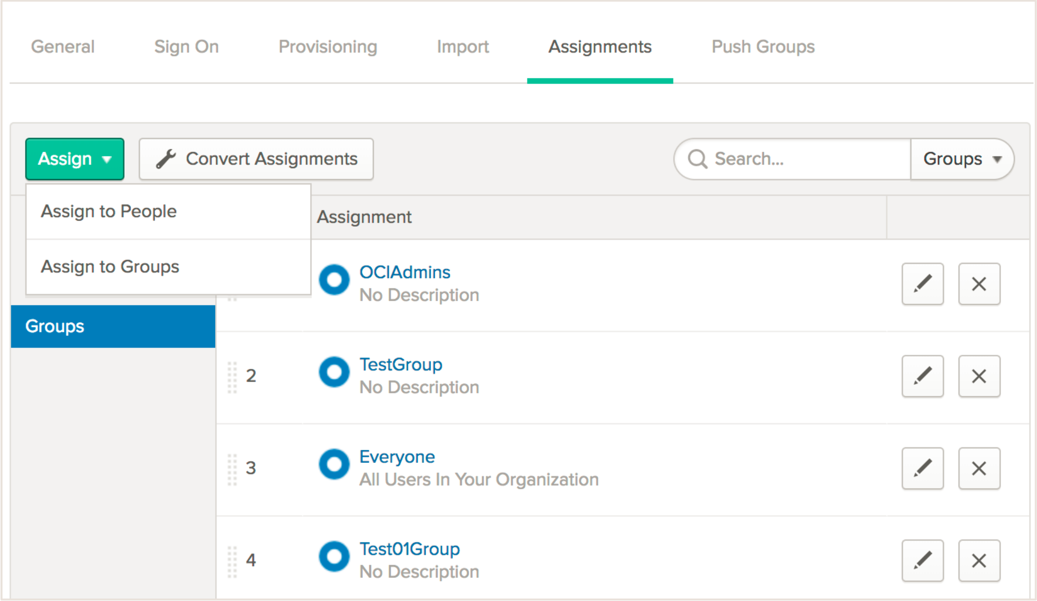
Creates or links a user in Oracle Cloud Infrastructure when assigning the app to a user in Okta.

The default username used to create accounts is set to Okta username.

Deactivate Users ☑ Enable

Deactivates a user's Oracle Cloud Infrastructure account when it is unassigned in Okta or their Okta account is deactivated. Accounts can be reactivated if the app is reassigned to a user in Okta.

13. On the **Assignments** tab, assign this app to groups or to individuals that you want to be able to log in to OCI, as shown in the following screenshot.



	Assignment
	OCIAdmins No Description
2	TestGroup No Description
3	Everyone All Users In Your Organization
4	Test01Group No Description

Known Issues and Troubleshooting

- You don't see a list of Okta groups in the OCI group mapping dialog box unless you manually push that group to OCI. For more information, see the Okta help topic Using Group Push.
- When the group push is done, the group doesn't readily appear in the Oracle Cloud Console. Manually map the group to an OCI group by clicking **Edit Mappings**.
- When a user is deactivated in Okta, the user continues to exist in OCI but can't use the Okta credentials.
- When pushing a group, OCI doesn't support linking existing groups that were created in Oracle Cloud Infrastructure to groups created in Okta.

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 facebook.com/oracle twitter.com/oracle