Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Okta Integration

Release 24.1
F97450-01
June 2024

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Okta Integration, Release 24.1

F97450-01

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

Contents

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 configuration guide explains the steps required for integrating Okta with OPERA Cloud Identity Management.

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
June 2024	Initial Publication

1

Okta Integration with OPERA Cloud Identity Management – Overview

OPERA Cloud Identity Management's OCI IAM Identity Domains provide the capability of integrating with Okta where Okta will be the identity provider for OPERA Cloud Identity Management. This integration ensures customers who are using Okta as their identity provider can centrally manage their users and groups in Okta, and those users, groups, and user group memberships are seamlessly synchronized into OPERA Cloud Identity Management. This integration also supports SAML 2.0 based identity federation, which provides a seamless single-sign-on experience for customers by allowing them to use their Okta user credentials during login to OPERA Cloud Services.

Prerequisites for Okta Integration with OPERA Cloud Identity Management

- An Okta account with administrator privileges.
- OPERA Cloud Identity Management's OCI IAM Identity Domains provisioned for the customer.
- User account in OCI IAM Identity Domain with Administrator role.

2

Configuring Identity Lifecycle Management between Okta & OCI IAM Identity Domain

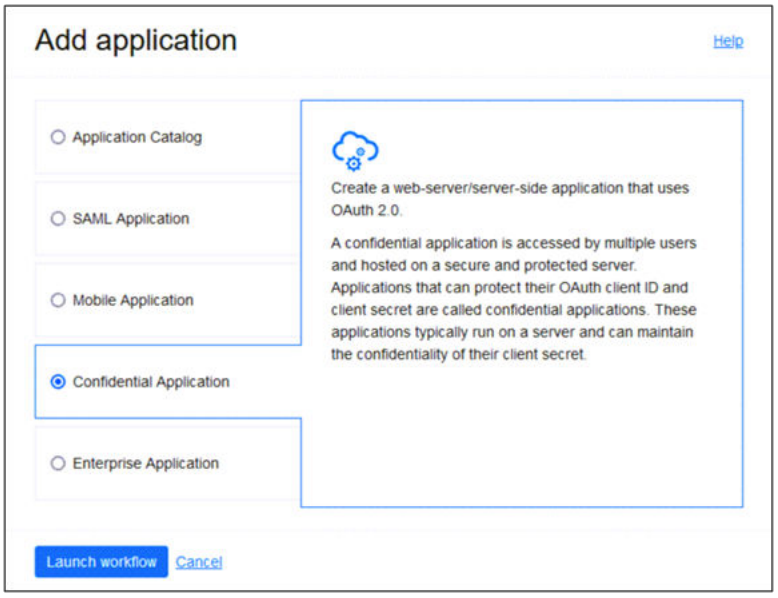
This section provides the steps to configure Okta as the authoritative identity store to manage identities in OPERA Cloud Identity Management's customer OCI IAM Identity Domain.

Below are the high-level steps involved in this configuration.

1. Create a confidential application in OCI IAM.
2. Obtain the identity domain URL and generate a secret token.
3. Create an app in Okta.
4. Update Okta's settings.
5. Test identity provisioning from Okta to OCI IAM.

1. Create a Confidential Application

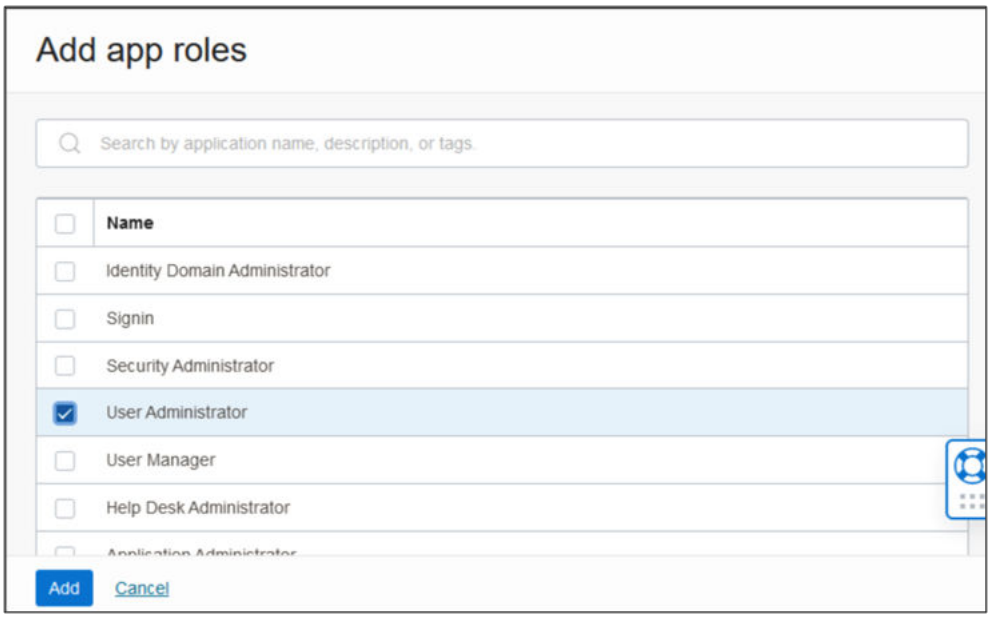
1. Open a supported browser and enter the following Console URL: https://cloud.oracle.com
2. Enter your **Cloud Account Name**, also referred to as your tenancy name, and click **Next**.
3. Sign in with your **username** and **password**.
4. Open the navigation menu and click **Identity & Security**. Under Identity, click **Domains**.
5. Select the identity domain in which you want to configure Okta provisioning and click **Integrated Applications**.
6. Click **Add Application** and choose **Confidential Application** and then click **Launch workflow**.



7. Enter a name for the confidential application, for example, “OktaOPERAClient.” Click **Next**.
8. Under Client configuration, select **Configure this application as a client now**.

9. Under Authorization, select **Client credentials**.

10. Scroll to the bottom and click **Add app roles**.
11. Under App roles click **Add roles**, and in the Add app roles page, select **User Administrator** and click **Add**.



12. Click **Next** and then click **Finish**.
13. On the application details page, click **Activate** and confirm that you want to activate the new application.

2. Find the Domain URL and Generate a Secret Token

You need the following pieces of information for the connection settings of the enterprise app you create:

- The domain URL
- A secret token generated from the client ID and client secret.

1. Return to the identity domain overview by clicking the **identity domain name** in the breadcrumbs. Click **Copy** next to the Domain URL in Domain information and save the URL to an app where you can edit it. The OCI IAM GUID is part of the domain URL: https://<IdentityDomainID>.identity.oraclecloud.com:443/fed/v1/idp/sso

2. In the confidential app in OCI IAM, click the **OAuth** configuration under Resources.
3. Scroll down and find the **Client ID** and **Client secret** under General Information.
4. Copy the **client ID** and store it.
5. Click **Show secret** and copy the secret and store it.

The secret token is the base64 encoding of <clientID>:<clientsecret> or base64(<clientID>:<clientsecret>).

The following examples show how to generate the secret token on Microsoft Windows and Apple MacOS.

In a Microsoft Windows environment:

a. Open CMD and use this powershell command to generate base64:

- [Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes('client_id:secret'))

In an Apple MacOS, use the following:

a. echo -n <clientID>:<clientsecret> | base64

b. Make a note of the secret token value.

3. Create the OCI Application in Okta

Configure Okta to enable Okta to be the authoritative identity store to manage identities in your OCI IAM Identity Domain.

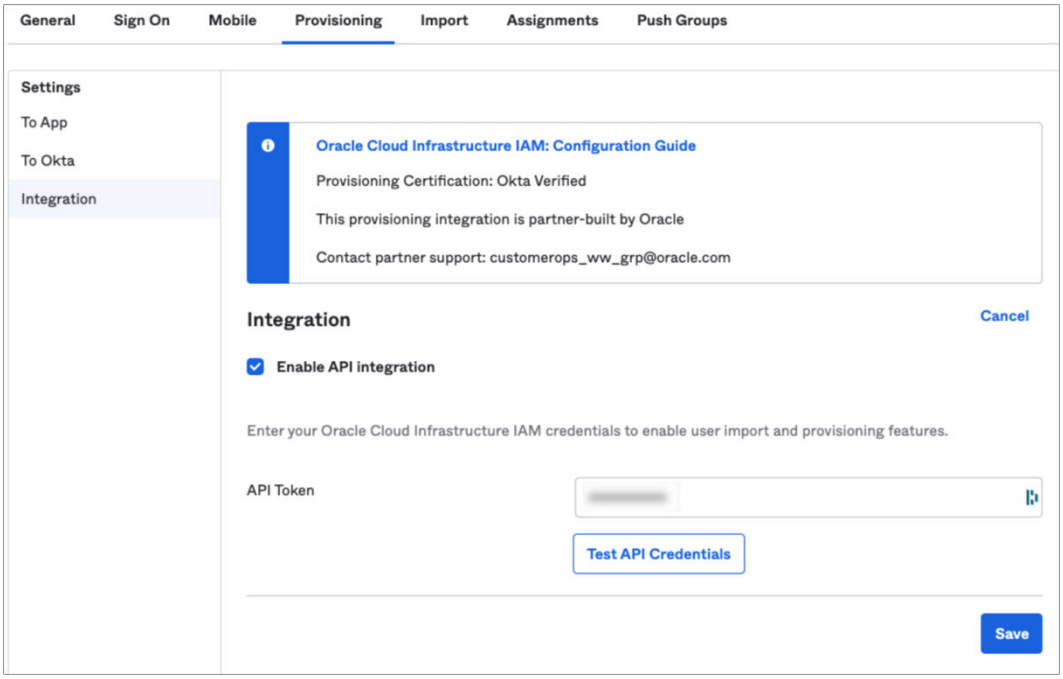
1. In the browser, sign into Okta using the following URL where <okta-org> is the prefix for your organization with Okta:
https://<Okta-org>-admin.okta.com
2. In the menu on the left, click **Applications**.
If you already have an application that you created when you went through SSO with OCI and Okta, you can use it. Just click to open it and edit it, and then go to 4. Change Okta Settings. If not, then follow the below steps.
3. Click **Browse App Catalog** and search for Oracle Cloud. 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**.

4. Change Okta Settings

Connect the Okta app to the OCI IAM confidential app using the domain URL and secret token from an earlier step.

1. In the newly created application page, click the **Sign On** tab.
2. In Settings, click **Edit**.
3. Scroll down to Advanced Sign-on Settings.

   Enter the domain URL in Oracle Cloud Infrastructure IAM GUID.
4. Click **Save**.
5. Near the top of the page, click the **Provisioning** tab.
6. Click **Configure API Integration**.
7. Select **Enable API Integration**.



8. Enter the secret token value you copied earlier in **API Token**.
9. Click **Test API Credentials**.
   If you get an error message, check the values that you have entered and try again.

   Okta has successfully connected to the OCI IAM SCIM endpoint when you get the '*Oracle Cloud Infrastructure IAM was verified successfully!*' message.
10. Click **Save**.

    The Provisioning to App page opens, where you can create users, update user attributes, and map attributes between OCI IAM and Okta.
11. Under Setting list, Provisioning to App screen, Click **Edit**.
12. Enable Create Users, Update User Attributes & Deactivate Users. Click **Save**
13. Scroll down to the **Attribute Mappings** section.
14. Click **Go to Profile Editor**; the Attribute section lists OCI IAM Attributes.
    Refer to the **User Mapping** table below to map user attributes between OCI IAM and Okta, adding any required attributes including the mandatory attributes.

Table 2-1 User Mapping

Okta Attribute	OCI User Attribute	External Namespace	Data type	Mapping Type	Attribute Value	Description	Mandatory Attribute
login	userName		String	Direct	Map from Okta profile	User name	Yes

Table 2-1 (Cont.) User Mapping

Okta Attribute	OCI User Attribute	External Namespace	Data type	Mapping Type	Attribute Value	Description	Mandatory Attribute
lastName	name.familyName		String	Direct	Map from Okta profile	Last name	Yes
email	emails[type eq "work"].value		String	Direct	Map from Okta profile	Email address	Yes
(user.email != null && user.email != '') ? 'work' : ''	emailType		String	Expression	(user.email != null && user.email != '') ? 'work' : ''	Email Type	Yes
extensionAttributePrimaryWorkLocation	OC_PrimaryWorkLocation	urn:ietf:params:scim:schemas:idcs:extension:custom:User	String	Expression	Same value for all Users. Refer description	Mandatory Single Valued User Attribute. Indicates the user's primary work location. Primary Work Location can have values <ENTERPRISE_ID>:E for multi chain customers derived from user profile. For customers having only a single chain, the source value can be set to constant <ENTERPRISE_ID>:E for all users.	Yes
isFederatedUser	isFederatedUser	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User	Boolean	Expression	True	Enable Federated User flag in Identity Domain.	Yes

Table 2-1 (Cont.) User Mapping

Okta Attribute	OCI User Attribute	External Namespace	Data type	Mapping Type	Attribute Value	Description	Mandatory Attribute
bypassNotification	bypassNotification	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User	Boolean	Expression	True	The bypass notification flag controls whether an email notification is sent after creating or updating a user account in Identity Domain. bypassNotification to be set to "true" for Federated users. This disables user account activation notification in IAM Identity Domain for the user.	Yes
firstName	name.givenName		String	Direct	Map from Okta profile	First name	No
perferredLanguage	preferredLanguage		String	Direct	Map from Okta profile	User's preferred written or spoken language used for localized user interfaces.	No
displayName	displayName		String	Direct	Map from Okta profile	Display name	No
title	title		String	Direct	Map from Okta profile	Title	No
mobilePhone	phoneNumbers[type eq "mobile"].value		String	Direct	Map from Okta profile	User's mobile phone number	No

Table 2-1 (Cont.) User Mapping

Okta Attribute	OCI User Attribute	External Namespace	Data type	Mapping Type	Attribute Value	Description	Mandatory Attribute
employeeNumber	OC_UserEmployeeNo	urn:ietf:params:scim:schemas:idcs:extension:custom:User	String	Direct	Map from Okta profile	Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization.	No
userType	OC_UserType	urn:ietf:params:scim:schemas:idcs:extension:custom:User	String	Direct	Map from Okta profile Possible Values: FULL-TIME EMPLOYEE PART-TIME EMPLOYEE TRAINEE CONTRACTOR CONSULTANT OTHER	Used to identify the organization-to-user relationship.	No
department	OC_Department	urn:ietf:params:scim:schemas:idcs:extension:custom:User	String	Direct	Map from Okta profile	Specifies the user's department.	No
primaryPhone	phoneNumbers[type eq "work"].value		String	Direct	Map from Okta profile	The user's work phone number.	No
extensionAttributeUserOwnerCode	OC_UserOwnerCode	urn:ietf:params:scim:schemas:idcs:extension:custom:User	String	Direct	Map from Okta profile	Unique code (typically, the sales manager's initials) for the owner. For example, oc_ownercode=First_Last_Initial	No

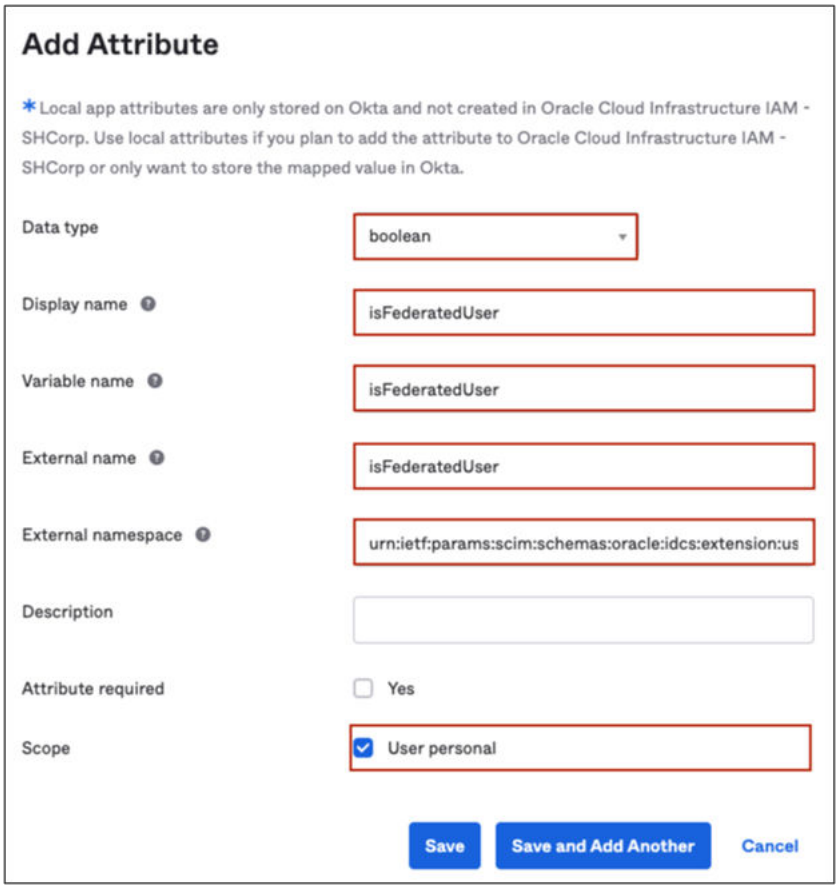
Table 2-1 (Cont.) User Mapping

Okta Attribute	OCI User Attribute	External Namespace	Datatype	Mapping Type	Attribute Value	Description	Mandatory Attribute
extensionAttributeHonorificPrefix	name.honorificPrefix		String	Direct	Map from Okta profile	User Initials	No
extensionAttributeMiddleName	name.middleName		String	Direct	Map from Okta profile	User's Middle name	No
extensionAttributeHonorificSuffix	name.honorificSuffix		String	Direct	Map from Okta profile	Suffix	No
extensionAttributeTimezone	urn:ietf:params:scim:schemas:core:2.0:User:timezone		String	Direct	Map from Okta profile	User's timezone	No
extensionAttributeLocale	locale		String	Direct	Map from Okta profile	Used to indicate the user's default location for purposes of localizing items such as currency, date and time format, numerical representations, and so on.	No

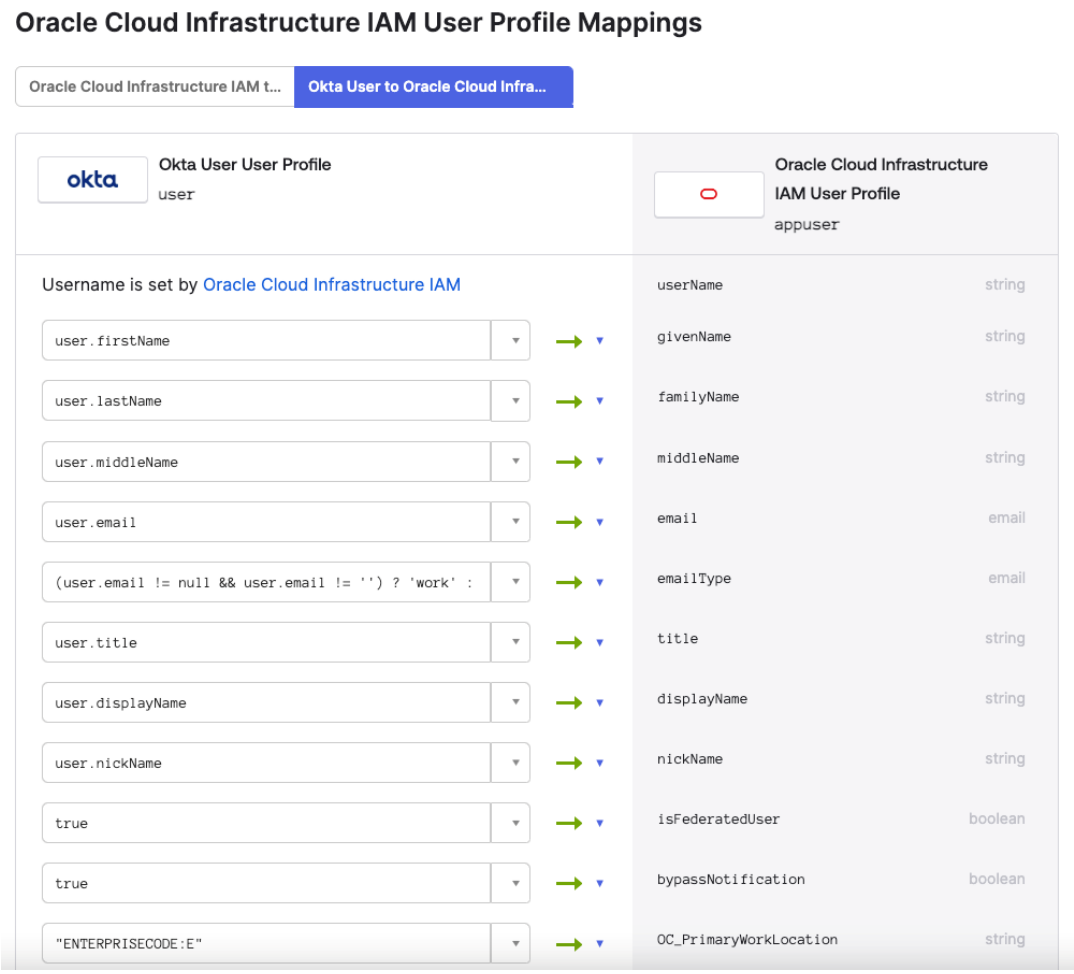
15. Follow the steps below to add required attributes from those attributes listed in the above user mapping table.
16. Under Attributes, click **Add Attributes**.
17. In the Add Attribute page, enter the following values from the User Mapping table above:
    - For **Data Type**, enter the corresponding value from the **Data Type** column.
    - For **Display Name**, enter the corresponding value from the **OCI User Attribute** column.
    - For **Variable Name**, enter the corresponding value from the **OCI User Attribute** column.

> **Note:**
>
> The external name is automatically populated by the value of the variable name.

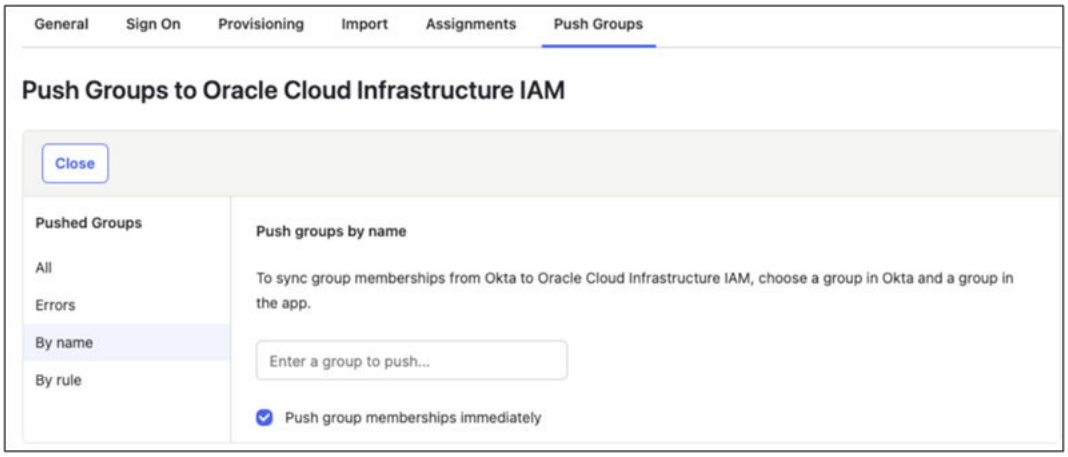
18. For External namespace, enter **urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User**.
19. Under Scope, check **User personal**.



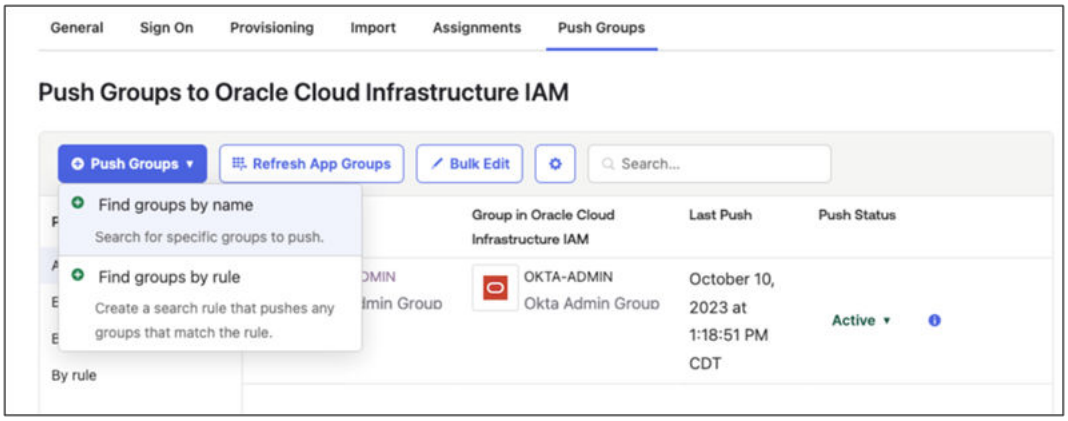
20. Click **Save and Add Another** attribute.
21. In the Attributes list, click **Mapping** and choose the tab **Okta User to Oracle IAM User Profile**.
22. Add mappings referring to the **User Mapping** table.



23. Save mappings.
24. Return to the OIC Application.
25. Syncing Groups from Okta to Oracle Identity Domain can be done manually or can be automated by selecting the **Push Group** tab under the OCI IAM application to define a rule.
26. Select the **Push Group** tab.
    You can manually push the group by entering the group name and selecting the group to be pushed.



27. Enter the group name to push from Okta to OCI IAM Domain.
28. You can also define a rule to automate Group synchronization.



5. Test User and Group Provisioning for Okta

1. In the newly created application, click the **Assignments** tab.
2. Click **Assign** and select **Assign to People**.
3. Search for the user to provision from Okta to OCI IAM.
4. Click **Assign** next to the user.
5. Click **Save** and then click **Go Back**.
6. Now provision Okta groups into OCI IAM. In the **Assignments** tab, click **Assign** and select **Assign to Groups**.
7. Search for the groups to be provisioned to OCI IAM. Next to the group name, click Assign.
8. Click **Done**.
9. Sign in to OCI.
10. Open a supported browser and enter the following OCI Console URL: https://cloud.oracle.com.
11. Enter your **Cloud Account Name**, also referred to as your tenancy name, and click **Next**.

12. Select the identity domain in which Okta has been configured.
13. Click **Users**.
    The user which was assigned to the OCI IAM application in Okta is now present in OCI IAM.
14. Click **Groups**.
    The group which was assigned to the OCI IAM application in Okta is now present in OCI IAM.