Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Okta Integration

Release 25.5
G47682-01
November 2025

ORACLE

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Okta Integration, Release 25.5

G47682-01

Contents

Notices

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
November 2025	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. Log in to the Oracle Cloud Infrastructure (OCI) Console using https://cloud.oracle.com.
2. Open the navigation menu and select **Identity & Security**. Under Identity, select **Domains**. Select the Identity Domain in which you want to configure Okta provisioning.
3. Click **Integrated Applications.**
4. Click **Add Application** and choose **Confidential Application** and then click **Launch workflow**.
5. Enter a name for the confidential application, for example, "OktaOPERAClient." Click **Submit**.
6. Click the **OAuth Configuration** tab and then click **Edit OAuth Configuration**.
7. Under **Client configuration**, select **Configure this application as a client now**.
8. Under Authorization, select **Client credentials**.
9. Scroll to the bottom and enable the **Add app roles** button.
10. Under App roles, click **Add roles**, and in the Add app roles page, select **User Administrator** and then click **Add**.
11. Click **Submit**.
12. On the application details page, click the **Actions** menu and 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 details for the connection settings of the Enterprise application that you create in Okta:

- The Identity Domain ID
- A secret token generated from the Client ID and Client secret.

Find the Identity Domain ID from the Domain URL:

1. Return to the Identity Domain where you are configuring Okta provisioning.
2. On the Identity Domain Details page, click **Copy** next to the Domain URL.

The **Identity Domain ID** is a part of the domain URL: https://<IdentityDomainID>.identity.oraclecloud.com:443

Make note of the **Identity Domain ID** from the Domain URL. For example, if your domain URL is https://idcs-123456.identity.oraclecloud.com:443, then your Identity Domain ID is **idcs-123456**.

Generate Secret Token:

1. Click **Integrated Applications**.
2. Click the confidential application you created for Okta provisioning.
3. Click **OAuth Configuration**.
4. Under **General Information**, copy the value next to **Client ID** and make a note of it.
5. Under **Client Secret**, locate the three dots (ellipsis) next to **Show secret** and then select **Copy**. Make a note that this value is the **Client Secret**.
6. The secret token is the base64 encoding of <clientID>:<clientsecret>.
   In a Microsoft Windows environment, open Powershell and use thiscommand to generate the base64 encoded value:

   ```
   [Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes('<client_id>:<clientsecret>'))
   ```

   In an Apple MacOS, use the following command in a terminal window:

   ```
   echo -n <clientID>:<clientsecret> | base64
   ```

   > **Note**
   >
   > Substitute the <clientID> and <clientsecret> in the command with the values noted in the previous steps. Ensure there are no blank spaces when entering the client ID and client secret values.

7. Copy the value returned by the command and make a note of this value. This value is the **Secret Token**.

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**.

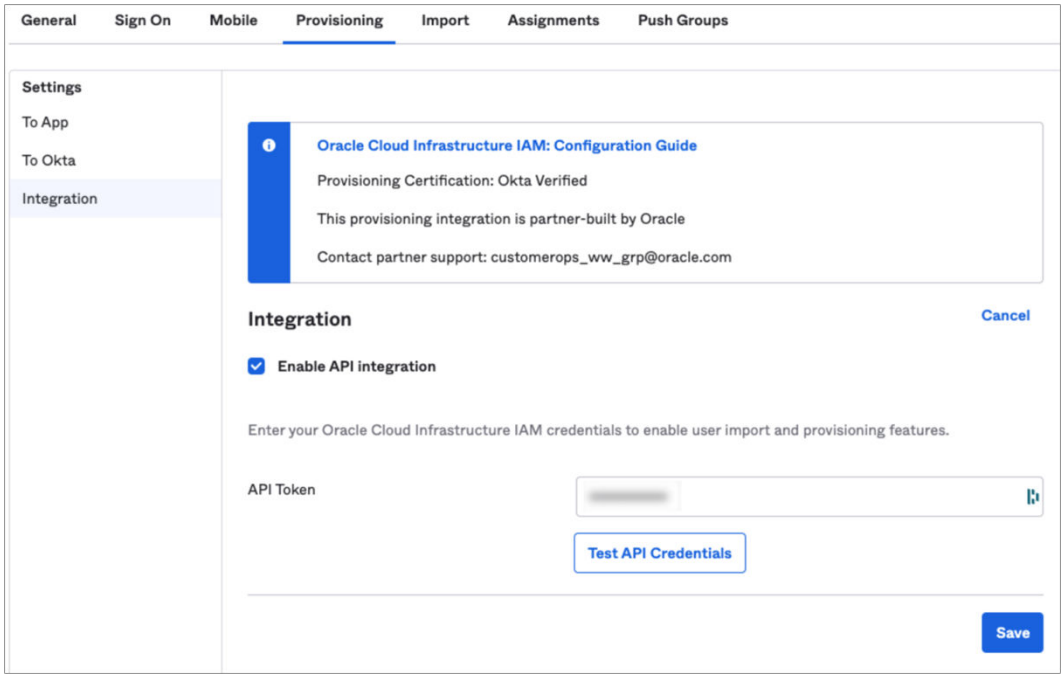
If you already have an application that you created when you went through SSO with OCI and Okta, you can use it. Just click to open it and edit it, and then go to 4. Change Okta Settings. If not, then follow the below steps.

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. Configure Provisioning and User Attribute Mappings in the Identity Provider (Okta)

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. Click **Edit** next to Settings.
3. Scroll down to Advanced Sign-on Settings and enter the **Identity Domain ID** under the 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 the 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.
15. Under Attributes, click **Add Attribute**.
16. Refer to the *Table 2-1 User Mapping* and add all the mandatory attributes one by one. Some attributes may have already been created by default, so you do not need to add them.
    To Add an attribute, enter the following details on the **Add Attribute** window:
    - **Data Type**: Add the value from the Mapping Type column from the User Mapping Table.
    - **Display Name**: Add the value from the IAM Domain (IDCS) User Attribute column from the User Mapping Table.
    - **Variable Name**: Add the value from the IAM Domain (IDCS) User Attribute column from the User Mapping Table.
    - **External Name**: Automatically populated by the value of the variable name.
    - **External Namespace**: Add the value from the External Namespace column from the User Mapping Table. If there is no value in the column, leave it blank.
    - **Attribute Type**: Select **Personal**.

    Click **Save and add another**. Repeat this process until all the mandatory attributes have been added.

Table 2-1 User Mapping

Okta Attribute	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
login	userName		Direct	Map from Okta profile	User name	Yes
lastName	name.familyName		Direct	Map from Okta profile	Last name	Yes
email	emails[type eq "work"].value		Direct	Map from Okta profile	Email address	Yes

Table 2-1 (Cont.) User Mapping

Okta Attribute	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
(user.email != null && user.email != '') ? 'work' : ''	emailType		Expression	(user.email != null && user.email != '') ? 'work' : ''	Email Type	Yes
extensionAttributePrimaryWorkLocation	OC_PrimaryWorkLocation	urn:ietf:params:scim:schemas:idcs:extension:custom:User	Expression	Same value for all Users. Refer description	Mandatory Single Valued User Attribute. Indicates the User primary work location. Primary Work Location can have values <CHAINCODE>:C for multi chain customers derived from the User profile. For customers having only a single chain, the source value can be set to constant <CHAINCODE>:C for all users.	Yes
isFederatedUser	isFederatedUser	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User	Expression	true	Enable Federated User flag in Identity Domain.	Yes

Table 2-1 (Cont.) User Mapping

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

Table 2-1 (Cont.) User Mapping

Okta Attribute	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
employeeNumber	OC_UserEmployeeNo	urn:ietf:params:scim:schemas:idcs:extension:custom:User	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	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	Direct	Map from Okta profile	Specifies the User's department.	No
primaryPhone	phoneNumbers[type eq "work"].value		Direct	Map from Okta profile	The User's work phone number.	No
extensionAttributeUserOwnerCode	OC_UserOwnerCode	urn:ietf:params:scim:schemas:idcs:extension:custom:User	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	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
extensionAttribute HonorificPrefix	name.honorificPrefix		Direct	Map from Okta profile	User Initials	No
extensionAttribute MiddleName	name.middleName		Direct	Map from Okta profile	User Middle name	No
extensionAttribute HonorificSuffix	name.honorificSuffix		Direct	Map from Okta profile	Suffix	No
extensionAttribute Timezone	timezone		Direct	Map from Okta profile	User's timezone	No
extensionAttribute Locale	locale		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

Table 2-1 (Cont.) User Mapping

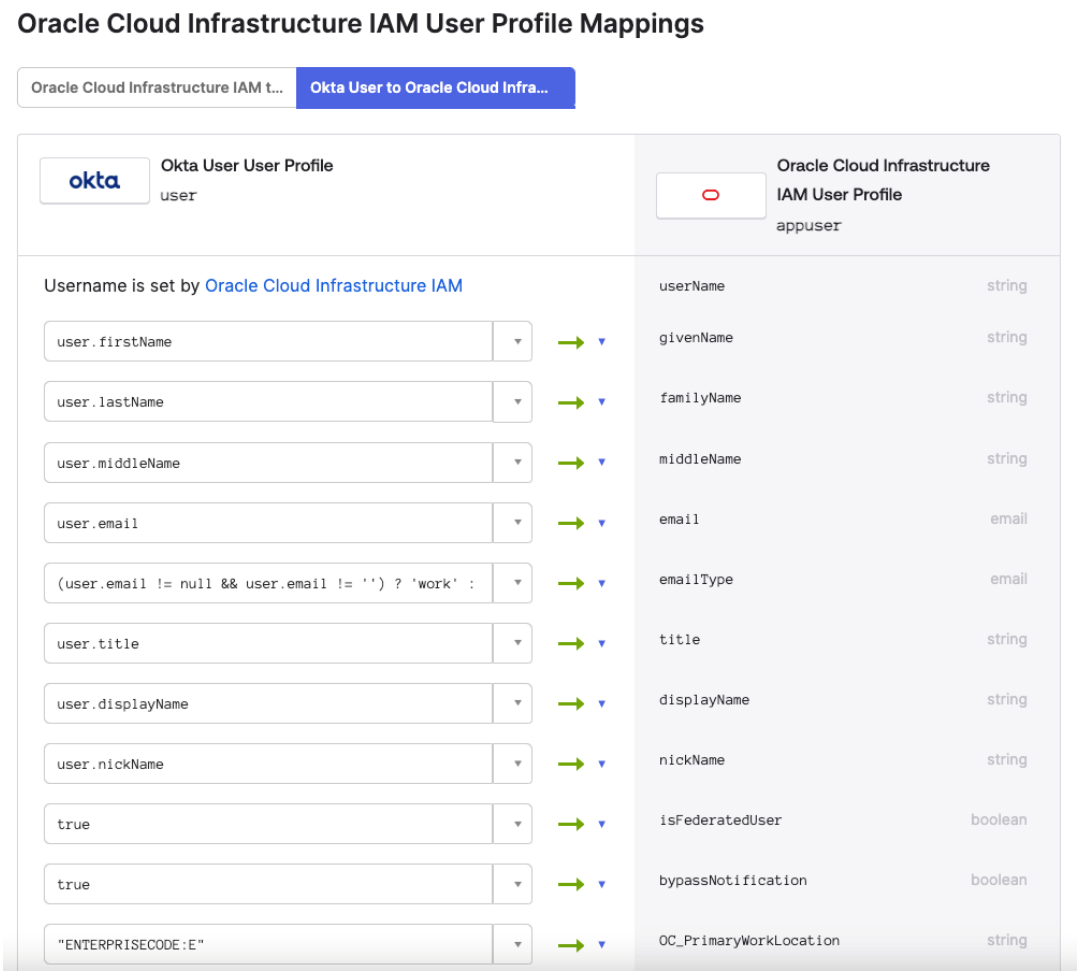
Okta Attribute	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
extensionAttributeActAs	oc_actas	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_ActAs	Direct	Map from Okta profile Possible Values: • Reservation Sales Person • Conference Sales Person • External System	OPERA Cloud attribute. Determines the Originating Application value in Blocks and Manage Block (see Managing Blocks) referenced by the Origin list field in Group Rooms Control (see Using Group Rooms Control) search and in reports.	No
extensionAttributeActAt	oc_actat	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_ActAt	Direct	Map from Okta profile Possible Values: • Property • Central	OPERA Cloud attribute. Determines the Originating Application value in Blocks and Manage Block (see Managing Blocks) referenced by the Origin list field in Group Rooms Control (see Using Group Rooms Control) search and in reports.	No

Table 2-1 (Cont.) User Mapping

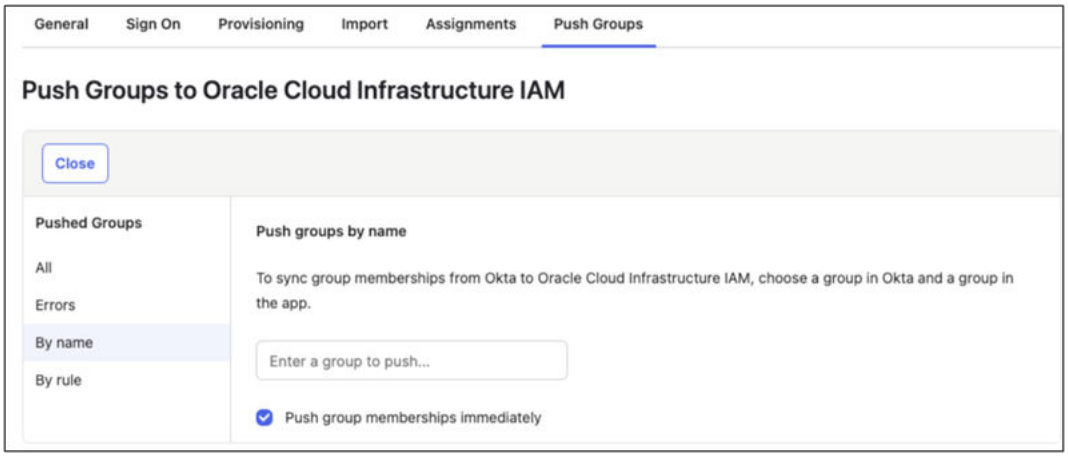
Okta Attribute	IAM Domain (IDCS) User Attribute	External Namespace	Mapping Type	Attribute Value	Description	Mandatory Attribute
extensionAttributeHubs	String array	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_Hubs	Direct	N/A	Assign one or more hubs to a user to determine their property location access in multi-property operations. oc_hubs is a String array in IAM Domain and the Identity Provider should should map a multi valued attribute to oc_hubs. Value for oc_hubs needs to be sent in all uppercase.	No
extensionAttributeHubsString	String	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_Hubs_String	Direct	N/A	Assign one or more hubs to a users to determine their property location access in multi-property operations. OC_Hubs_String needs to be sent in all uppercase as comma separated values.	No

17. Once all the mandatory attributes have been created, click **Mapping**. Click the tab **Okta User to Oracle Cloud Infrastructure**.

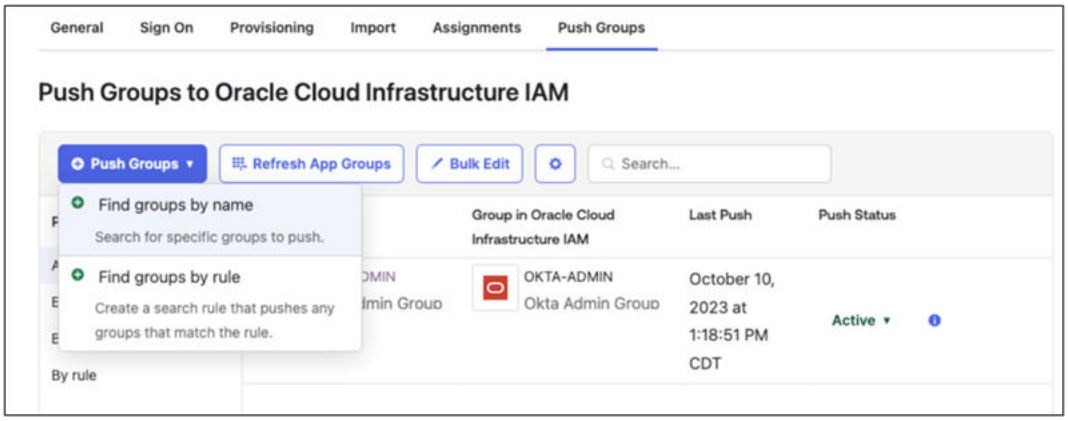
18. Refer to the Attribute Value column in the Table 2-1 User Mapping and update the values for all the mandatory attributes.
19. Save the mappings and return to the Application in Okta.
20. Syncing Groups from Okta to Oracle Identity Domain can be done manually or can be automated by selecting the **Push Group** tab to define a rule. Select the **Push Group** tab and click **Push Group**.
21. Click **Find groups by name** and enter the group name to push from Okta to OCI IAM Domain. Click **Save**.
    You can also define a rule to automate Group synchronization.



22. Save mappings.
23. Return to the OIC Application.
24. 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.
25. Select the **Push Group** tab.
    You can manually push the group by entering the group name and selecting the group to be pushed.



26. Enter the group name to push from Okta to OCI IAM Domain.
27. 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. Log in to the Oracle Cloud Infrastructure (OCI) Console using https://cloud.oracle.com.
10. Open the navigation menu and select **Identity & Security**. Under Identity, select **Domains**.
11. Select the identity domain in which Okta has been configured.

12. Click **Users**.
    The user which was assigned to the OCI IAM application in Okta is now present in OCI IAM.
13. Click **Groups**.
    The group which was assigned to the OCI IAM application in Okta is now present in OCI IAM.