Oracle Hospitality OPERA Cloud Identity Management

Administrator Guide for Configuring Microsoft Azure AD Synchronization with OPERA Cloud Identity Management

Release 23.1.1
F83071-01
March 2024

Oracle Hospitality OPERA Cloud Identity Management Administrator Guide for Configuring Microsoft Azure AD Synchronization with OPERA Cloud Identity Management, Release 23.1.1

F83071-01

Contents

Notices

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 guide explains the Microsoft Azure Active Directory (AD) Synchronization feature of Oracle Hospitality OPERA Cloud. Customers who are using Microsoft Azure AD as their identity provider can utilize the Microsoft Azure AD Synchronization feature.

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
March 2024	Initial Publication

1
Microsoft Azure AD Synchronization Overview

OPERA Cloud Identity Management's OCI IAM Identity Domains provide the capability of synchronizing users and groups from Microsoft Azure Active Directory (Azure AD). This feature ensures customers who are using Microsoft Azure AD as their identity provider can centrally manage their users and groups in Microsoft Azure AD, and those users, groups, and user group memberships are seamlessly synchronized into OPERA Cloud Identity Management.

Prerequisites for Microsoft Azure AD Synchronization

- An operational Microsoft Azure AD tenant
- A user account in Microsoft Azure AD with permission to configure provisioning (for example, Application Administrator, Cloud Application Administrator, Application Owner, or Global Administrator).
- OPERA Cloud Identity Management's OCI IAM Identity Domains provisioned for the customer.
- User account in OCI IAM Identity Domain with Administrator permissions.

2

Configuring Microsoft Azure AD Synchronization in OCI IAM Identity Domain

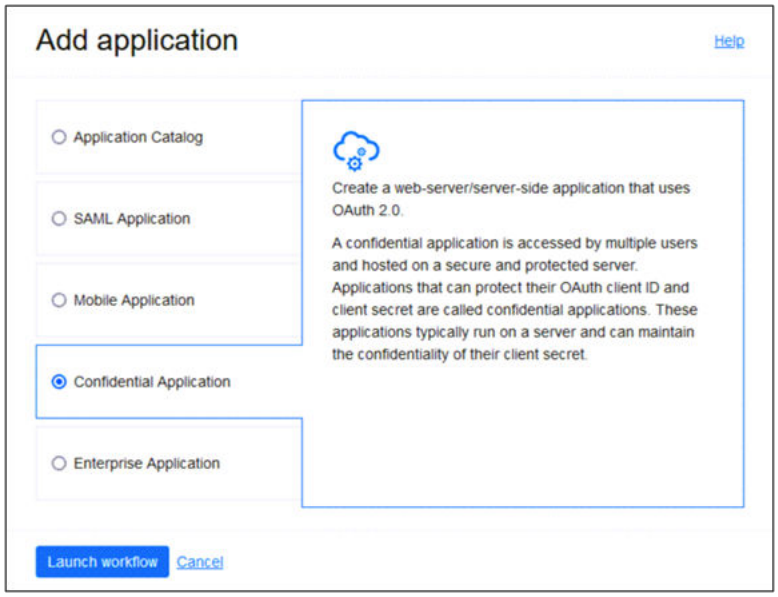
This section provides the steps to configure Microsoft Azure AD as the authoritative identity store to manage identities in OPERA Cloud Identity Management. Microsoft Azure AD is configured using an application template from Microsoft Azure AD Gallery.

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

1. Configure OCI IAM so that Microsoft Azure AD is the identity store to manage identities in OCI IAM. In OCI IAM, create a confidential application.
2. Generate a secret token from the OCI IAM identity domain's client ID and client secret. Use this along with the domain URL in Azure AD.
3. Create an app in Microsoft Azure AD and use the secret token and identity domain URL to specify the OCI IAM identity domain and prove that it works by pushing users from Microsoft Azure AD to OCI IAM.
4. Assign the users and groups you want to provision to OCI IAM in the Microsoft Azure AD application.

1. Create a Confidential Application

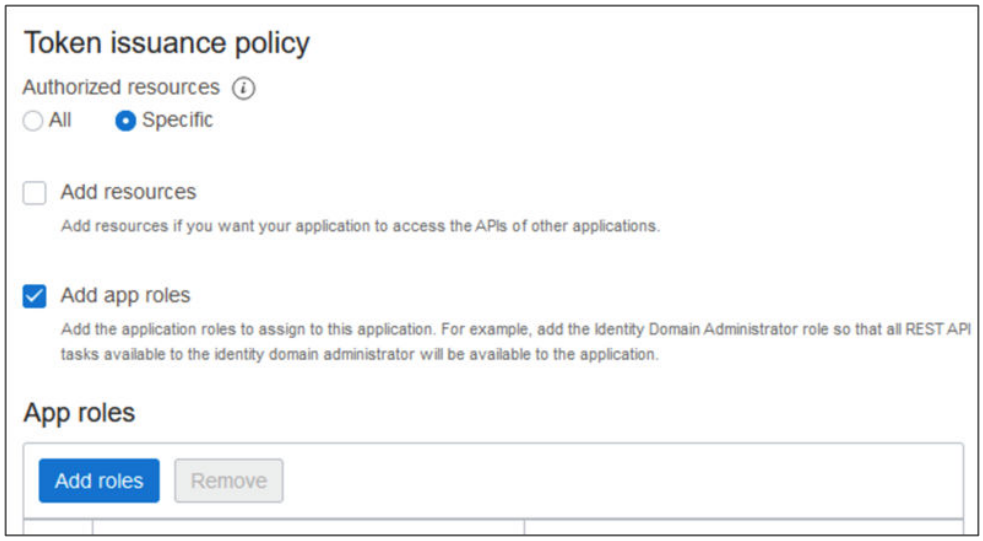
1. In the OCI Identity Domain, open the navigation menu and click **Identity & Security**.
2. Under Identity, click **Domains**.
3. Click **Integrated Applications** in the identity domain in which you are working
4. Click **Add Application** and choose **Confidential Application** and click **Launch workflow**.



5. Enter a name for the application, for example Azure AD, and click **Next**.
6. Under Client configuration, select **Configure this application as a client now**.

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

8. Under Client type, select **Confidential**.
9. Scroll down and in the Token issuance policy section, set Authorized resources to **Specific**.



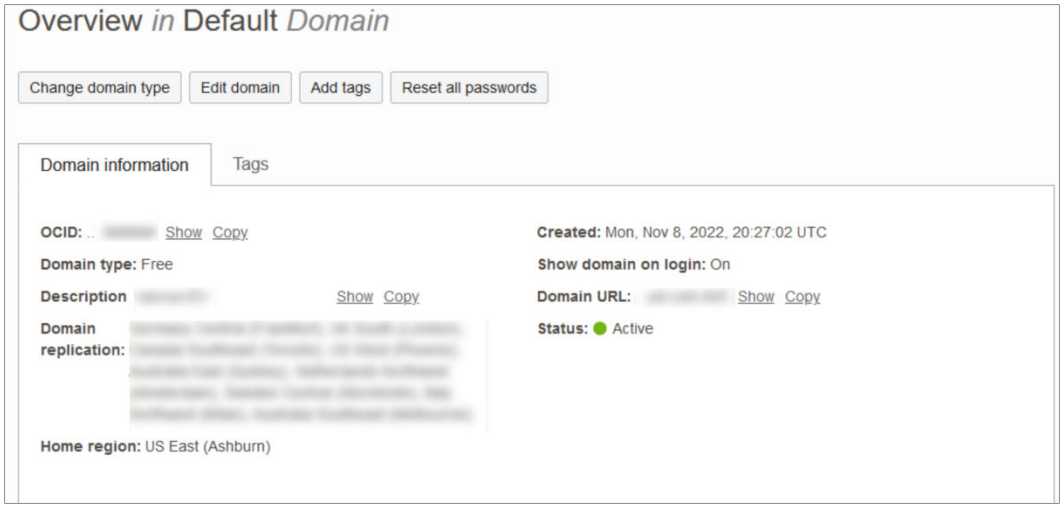
10. Select **Add app roles**.
11. In the App roles section, click the **Add roles** button.
12. On the Add app roles page, select **User Administrator** and then click **Add**.
13. Click **Next** and then click **Finish**.
14. On the Application Overview page, click **Activate** and confirm that you want to activate the application. The confidential application is now activated.

2. Find the Domain URL and Generate a Secret Token

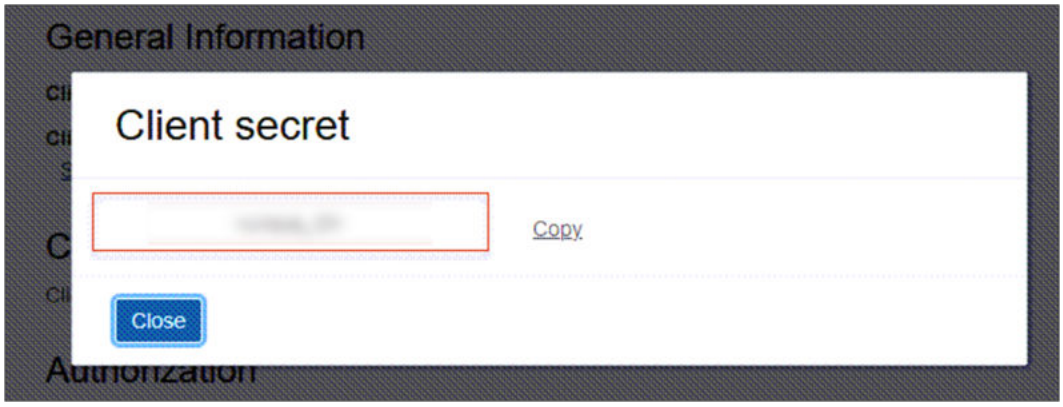
You need the following pieces of information for the connection settings of the enterprise app you create:

- 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.



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 Windows and MacOS:

- In a Windows environment, open CMD and use this powershell command to generate base64:
  encoding[Convert]::ToBase64String([System.Text.Encoding]::Unicode.GetBytes('client_id:secret'))"
- In MacOS, use the following:
  echo -n <clientID>:<clientsecret> | base64

  The secret token is returned. For example:

  echo -n 39235775234752392345743 7:3454-9853-7843-3554 | base64

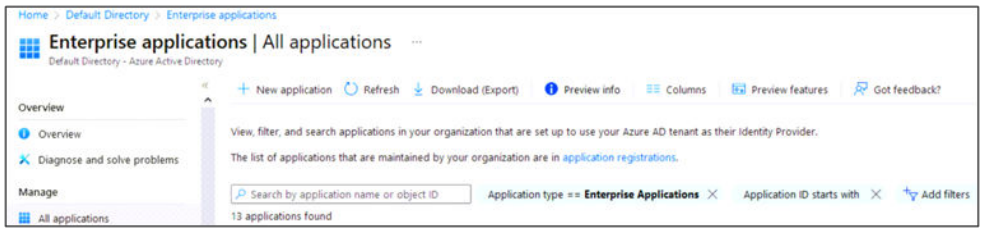
  Nk0NzUyMzcyMzQ1NzMTc0NzUyMzMtNTQzNC05ODc4LTUzNQ==

  Make a note of the secret token value.

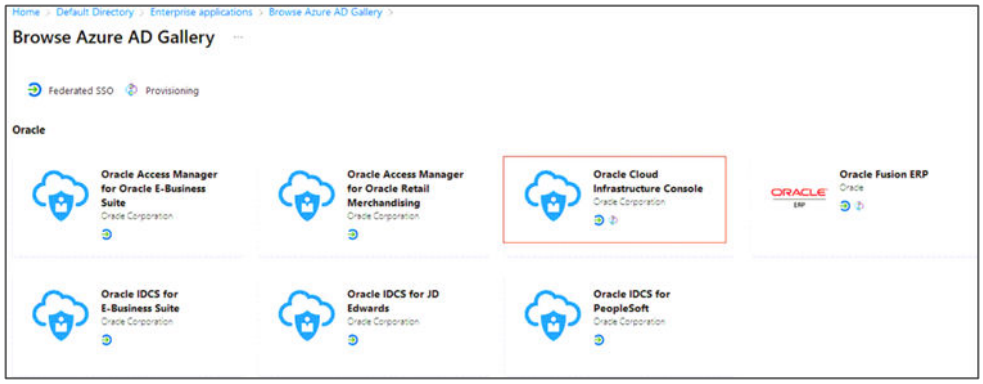
3. Create the OCI Application on Azure AD

Configure Microsoft Azure AD to enable Azure AD to be the authoritative identity store to manage identities in IAM.

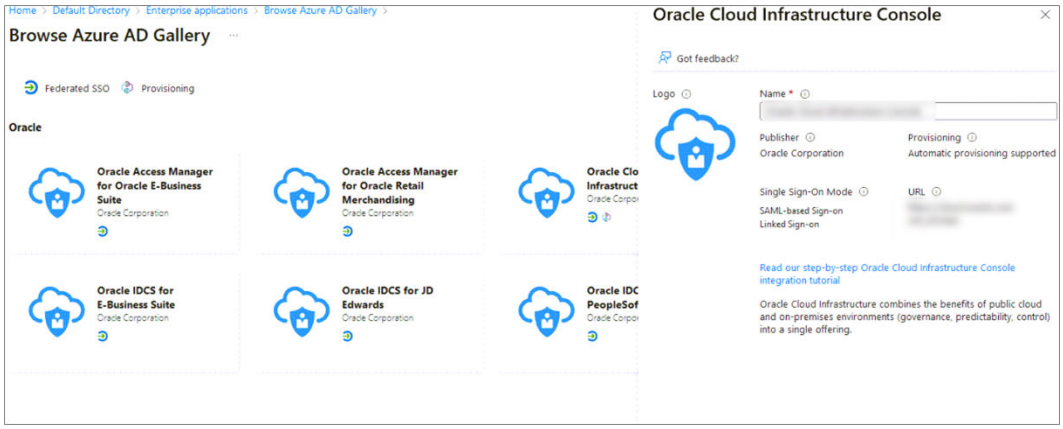
1. In the browser, sign into Microsoft Azure using the URL https://portal.azure.com
2. Click **Azure Active Directory** to open the Azure Active Directory overview page.
3. In the left menu, click **Enterprise applications**.



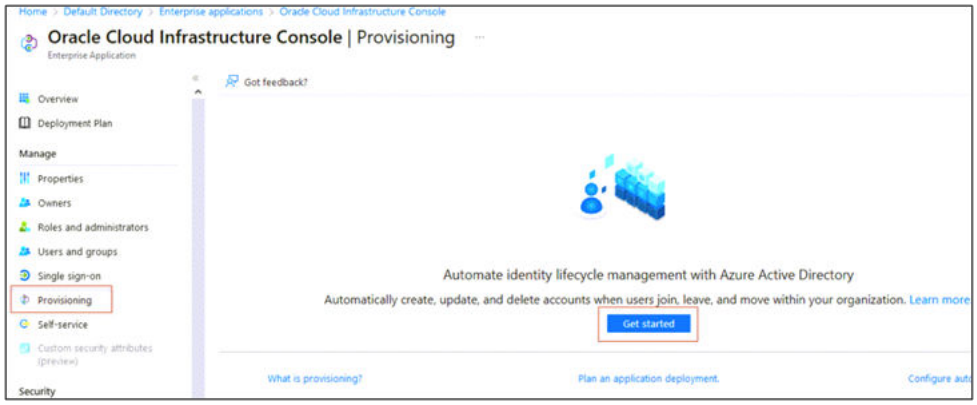
4. On the Enterprise applications page, click **New application**.
5. Select **Oracle Cloud Infrastructure Console**.



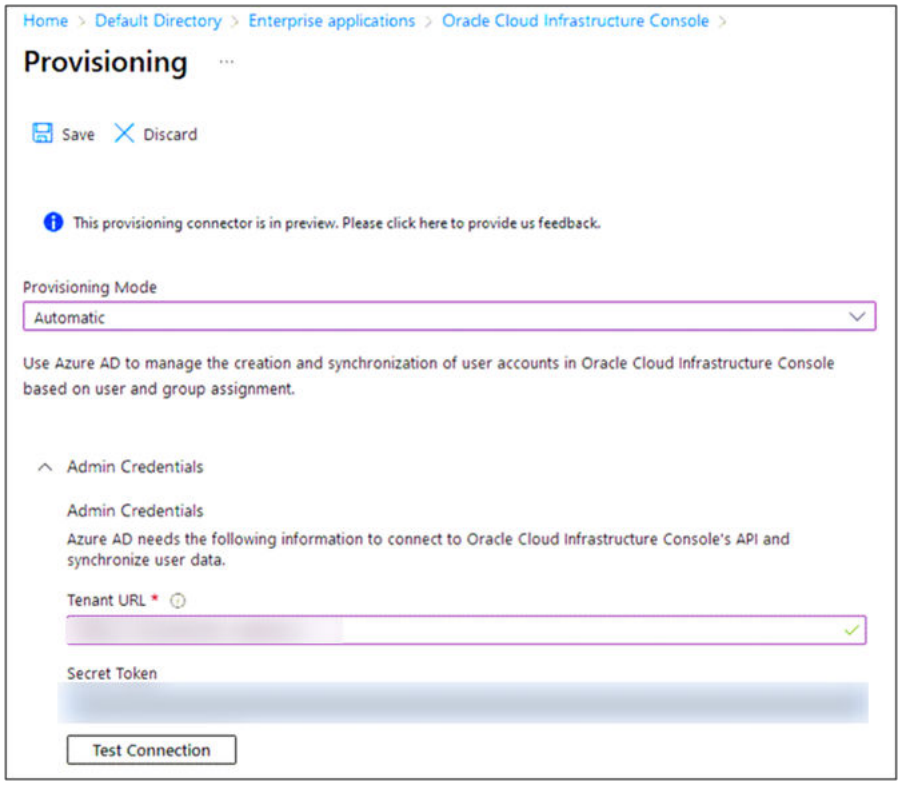
6. Enter a name or accept the default of Oracle Cloud Infrastructure Console.
7. Click **Create**.



8. Select **Provisioning** from the left menu under Manage.



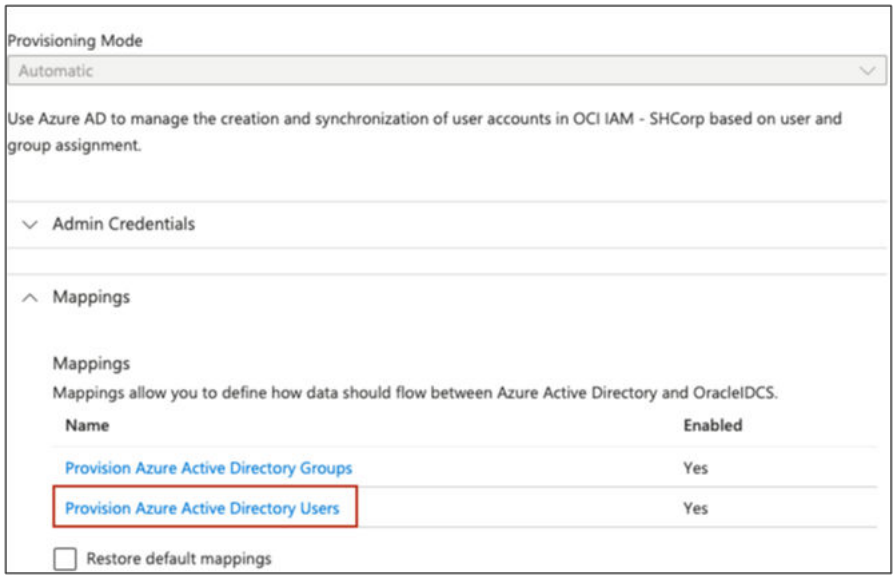
9. Click **Get started** and change the Provisioning Mode to **Automatic**.
10. In the **Tenant URL**, enter the **OCI IAM Domain URL** from 2. Find the Domain URL and Generate a Secret Token followed by **/admin/v1**. That is, the tenant URL is https://<domainURL>/admin/v1
11. Enter the secret token you generated in 2. Find the Domain URL and Generate a Secret Token.



12. Click **Test Connection** and verify if the test is successful.

4. Additional Configurations for Federated Users

1. In the browser, log in to Microsoft Azure using the URL.
2. Click **Azure Active Directory** to open the Azure Active Directory overview page.
3. In the left menu, click **Enterprise applications**.
4. Click the application you created earlier, Oracle Cloud Infrastructure Console.
5. In the left menu under Manage, click **Provisioning** and then click **Edit Provisioning**.
6. In the Provisioning page, click **Mappings**.
7. Under Mappings, click **Provision Azure Active Directory Users**.



8. Under Attribute Mappings, scroll down and click **Add New Mapping**.

Table 2-1 User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
userPrincipal Name	userName	Direct	N/A	User name	Yes
surname	name.family Name	Direct	N/A	Last name	Yes
mail	emails[type eq "work"].value	Direct	N/A	Email address	Yes

Table 2-1 (Cont.) User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
extensionAttributePrimaryWorkLocation	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_PrimaryWorkLocation	Direct	N/A	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 the User profile. For customers having only a single chain, the source value can be set to constant <CHAINCODE >:C for all users.	Yes
CBool(true)	isFederatedUser	Expression	CBool("true")	Enable Federated User flag in Identity Domain.	Yes

Table 2-1 (Cont.) User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
CBool(true)	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:bypassNotification	Expression	CBool("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 and this disables user account activation notification in IAM Identity Domain for the user.	Yes
active	active	Expression	Not([IsSoftDeleted])	User status. The attribute IsSoftDeleted is often part of the default mappings for an application in Azure AD. It is not recommended to remove the IsSoftDeleted attribute from your attribute mappings.	Yes
givenName	name.givenName	Direct	N/A	First name	No

Table 2-1 (Cont.) User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
perferredLanguage	preferredLanguage	Direct	N/A	User's preferred written or spoken language used for localized user interfaces.	No
displayName	displayName	Direct	N/A	Display name	No
jobTitle	title	Direct	N/A	Title	No
mobile	phoneNumbers[type eq "mobile"].value	Direct	N/A	User's mobile phone number	No
extensionAttributeUserOwnerCode	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_User OwnerCode	Direct	N/A	Unique code (typically, the sales manager's initials) for the owner. For example, oc_ownercode=First_Last_Initial.	No
employeeId	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_User EmployeeNo	Direct	N/A	Numeric or alphanumeric identifier assigned to a person, typically based on order of hire or association with an organization.	No

Table 2-1 (Cont.) User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
employeeType	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserType	Direct	Possible Values: • FULL-TIME EMPLOYEE • PART-TIME EMPLOYEE • TRAINEE • CONTRACTOR • CONSULTANT OTHER	Used to identify the organization-to-user relationship.	No
department	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_Department	Direct	N/A	Specifies the user's department	No
telephoneNumber	phoneNumbers[type eq "work"].value	Direct	N/A	User's work phone number	No
extensionAttributeHonorificPrefix	name.honorificPrefix	Direct	N/A	User’s Initials	No
extensionAttributeMiddleName	name.middleName	Direct	N/A	User’s Middle name	No
extensionAttributeHonorificSuffix	name.honorificSuffix	Direct	N/A	Suffix	No
extensionAttributeTimezone	urn:ietf:params:scim:schemas:core:2.0:User:timezone	Direct	N/A	User's timezone	No

Table 2-1 (Cont.) User Mappings

Azure AD User Attribute Name	OCI IAM Domain User Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
extensionAttributeLocale	urn:ietf:params:scim:schemas:core:2.0:User:locale	Direct	N/A	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


Attribute Mappings
Attribute mappings define how attributes are synchronized between Azure Active Directory and OracleIDCS

Azure Active Directory Attribute	OracleIDCS Attribute	Matching precedence	Remove
Item(Split([userPrincipalName], "@"), 1)	userName	1	Delete
Not([IsSoftDeleted])	active		Delete
displayName	displayName		Delete
jobTitle	title		Delete
mail	emails[type eq "work"].value		Delete
preferredLanguage	preferredLanguage		Delete
givenName	name.givenName		Delete
surname	name.familyName		Delete
CBool("true")	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:bypassNotification		Delete
CBool("true")	urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:isFederatedUser		Delete
employeeId	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserEmployeeNo		Delete
extensionAttributeUserOwnerCode	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_OwnerCode		Delete
extensionAttributePrimaryWorkLocation	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_PrimaryWorkLocation		Delete
employeeType	urn:ietf:params:scim:schemas:idcs:extension:custom:User:OC_UserType		Delete

Add New Mapping

Custom Attribute Mapping

To add mapping for target attributes, such as custom attributes and attributes not defined by default in the provisioning connector schema, you can edit the JSON representation of the schema to add these attribute mappings.

> **Note:**
>
> Editing the list of supported attributes is only recommended for administrators who have customized the schema of their applications and systems and have first-hand knowledge of how their custom attributes are defined or if a source attribute is not automatically displayed in the Microsoft Entra admin center UI. This sometimes requires familiarity with the APIs and developer tools provided by an application or system. The ability to edit the list of supported attributes is locked down by default, but customers can enable this capability by navigating to the following URL: https://portal.azure.com/?Microsoft_AAD_Connect_Provisioning_forceSchemaEditorEnabled=true.

You can navigate to your application to view the attribute list. For more information, see the "Editing the list of supported attributes" section of the Microsoft article *Tutorial - Customize user provisioning attribute-mappings for SaaS applications in Microsoft Entra ID*.

1. Under Provisioning, select **Mappings**, and then select **Provision Azure Active Directory Users**.
2. Select the **Show advanced options** check box at the bottom of the Attribute Mapping screen, and then select **Edit attribute list for OracleIDCS**.

3. **Save** the mapping.

Group Attribute Mapping

1. On the Provisioning page, click **Mappings**.
2. Under Mappings, click **Provision Azure Active Directory Groups**. Refer to the below table to update and add the mappings for Group attributes.

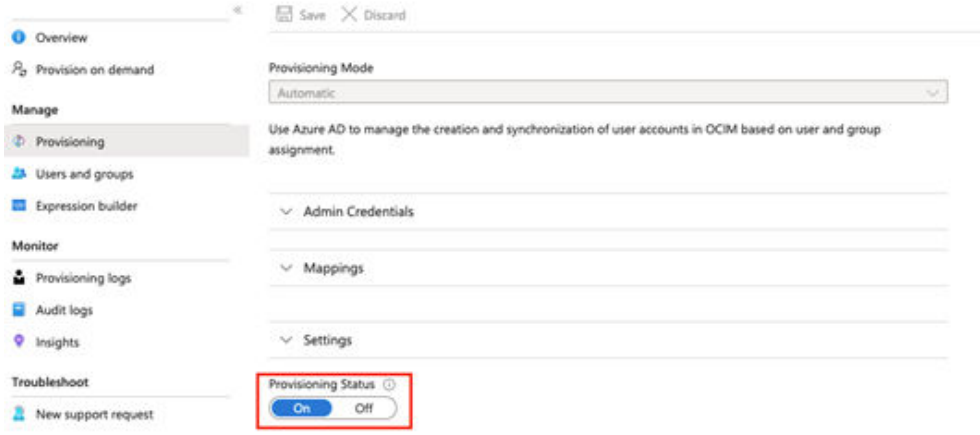
Table 2-2 Group Attribute Mappings

Azure AD Attribute	IAM Domain Group Attribute Name	Mapping Type	Value	Description	Mandatory Attribute
displayName	displayName	Direct	N/A	Group display name	Yes
members	members	Direct	N/A	Members of the group	No
objectId	externalId	Direct	N/A	External Group Id	No
description	urn:ietf:params:scim:schemas:oracle:idcs:extension:group:Group:description	Direct	N/A	Group description	No

Group Attribute Mapping in Azure AD

Follow the below steps to add the IDCS Group Description attribute.

1. Under Provisioning, select **Mappings** and then select **Provision Azure Active Directory Groups**.
2. Select the **Show advanced options** check box at the bottom of the Attribute Mapping screen and then select **Edit attribute list for OracleIDCS**.
3. Add the attribute.
4. Save the mapping.
5. Navigate to **Provision Azure Active Directory Groups** and add the mapping for the Group description and save the changes.
6. Select **Provisioning** from the left menu and set the **Provisioning Status** to “On.”



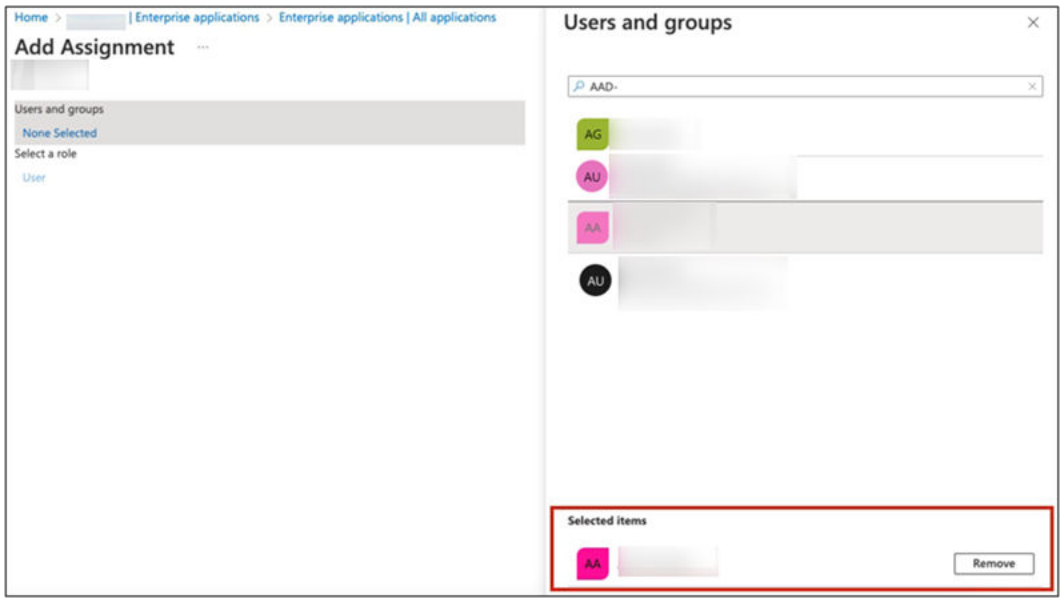
7. Save the changes.

5. Assign Users and Groups to the Microsoft Azure AD Application

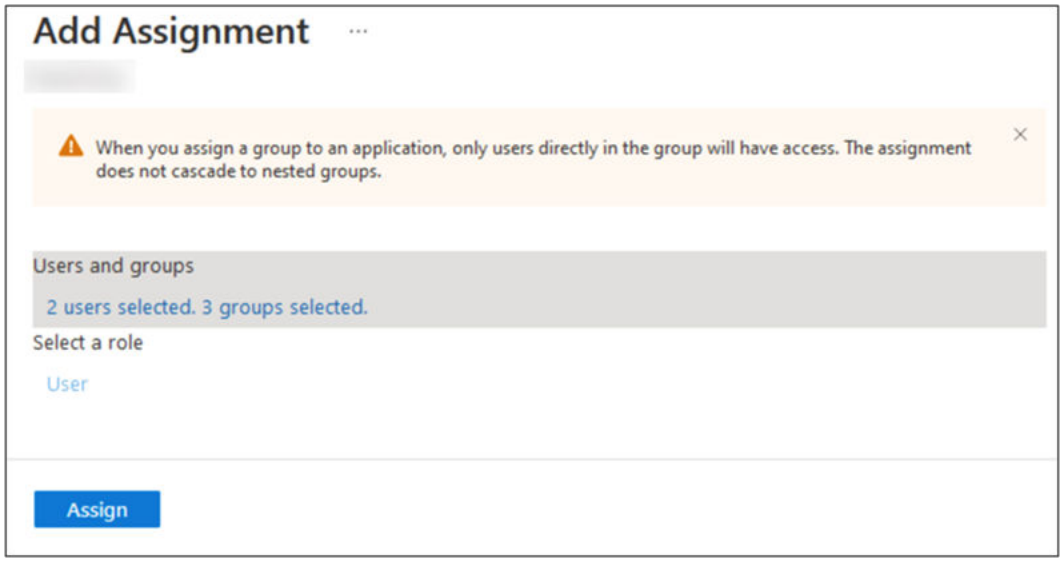
Assign the users you want to provision to OCI IAM.

1. In Azure AD, in the left menu, click **Enterprise applications**.
2. Click the application you created earlier, Oracle Cloud Infrastructure Console.
3. In the left menu under Manage, click **Users and groups**.

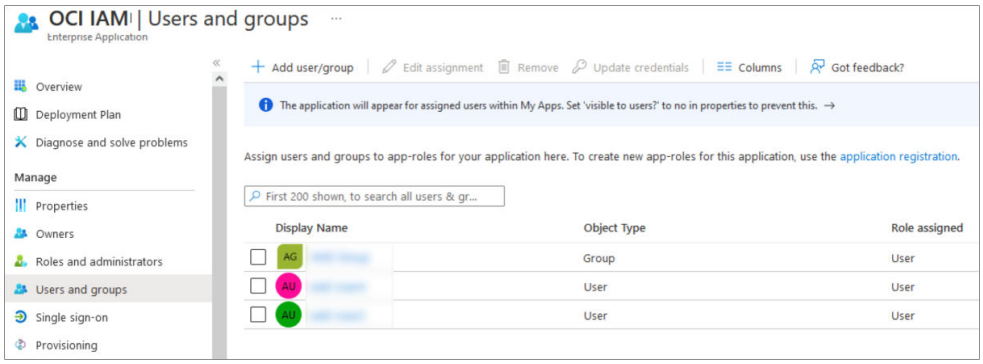
4. In the Users and groups page, click **Add user/group**.
5. On the Add Assignment page, under Users and groups, click **None Selected**. The Users and groups page opens.
6. Select one or more users or groups from the list by clicking them. The ones you select are listed under Selected items.



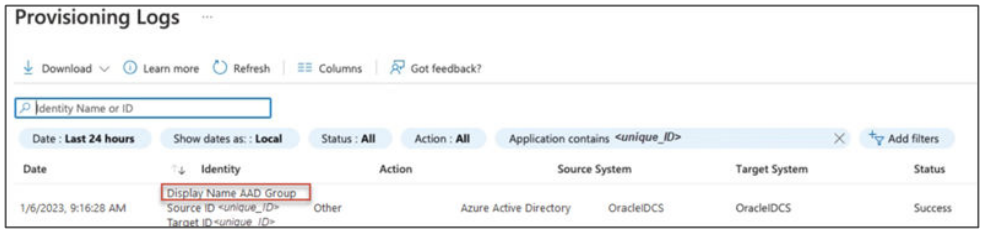
7. Click **Select**. The number of users and groups selected are shown on the Add Assignment page.



8. On the Add Assignment page, click **Assign**.
The Users and groups page now shows the users and groups you have chosen.

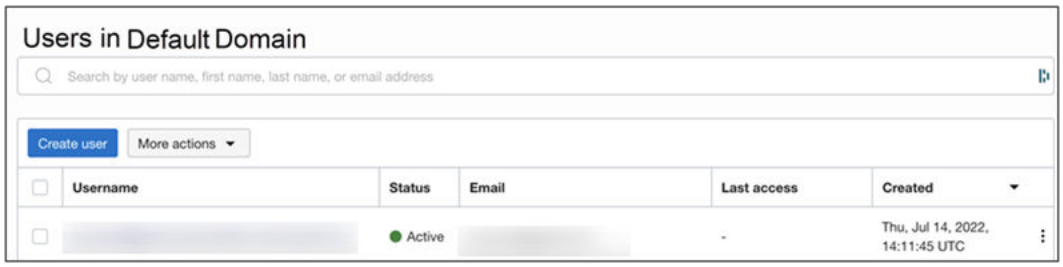


9. Click **Provisioning** in the left menu to provision the groups and users. The provisioning log shows the status.



10. When provisioning is successful, the **Current cycle status** indicates that the incremental cycle has completed, and the number of users provisioned to OCI IAM appears.

In OCI IAM, you can now see the users and groups provisioned from Azure AD.



Note

OC_PrimaryWorkLocation is a custom attribute in OCI IAM Domain. Due to an issue in Microsoft Azure, this does not get synced from Microsoft Azure to Oracle via the provisioning connector in Microsoft Entra. As a work around, we are having the custom attribute sync carried out by JIT attribute mapping as part of the Federation configuration. This custom attribute is updated in OCI IAM Domain at the time of the user's first login to OPERA Cloud.