



# Identity Lifecycle Management Between OCI IAM and Entra ID

Provisioning enablement for the integration of OCI IAM and Entra ID

---

**Roberto Raspatella**

Cloud Security Black Belt

# Safe harbor statement

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, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

# Disclaimer

Best practices and techniques utilized in this presentation may not be applicable to a production environment. This presentation and anything provided hereunder, including without limitation use cases and any deliverables, may not be used in a production or commercial environment and may not be distributed to any third party.

THIS PRESENTATION AND ANYTHING PROVIDED HEREUNDER ARE PROVIDED ON AN “AS IS” BASIS WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED

ORACLE SPECIFICALLY DISCLAIMS ANY LIABILITY WITH RESPECT TO THE PRESENTATION AND ANYTHING PROVIDED HEREUNDER

# **Introduction to Identity Lifecycle Management between OCI IAM and Entra ID**

---

# Overall Benefits

- Federating the two solutions has several advantages that can improve security, user experience, and make managing digital identities inside an organization easier.
- From administration perspective, administrators can easily manage entitlements, permissions, and user lifecycles throughout the entire company. It is possible to update a user's access permissions in one location when joining, moving within, or departing the company, guaranteeing uniform and suitable access controls.
- Organizations can then save IDM operating expenses by integrating the two solutions. For example, help desk operations can be more efficiently run, password management overhead can be decreased, and licensing costs for numerous IDM solutions can be lowered with the central administration and automation of user accounts.
- All things considered, the above operations provide a more efficient, safe, and controllable integrate solution, which is advantageous to both users and IT administrators in an enterprise.

# Identity Lifecycle Management between OCI IAM and Entra ID

## **Pushing user accounts from Entra ID to OCI IAM**

By pushing user accounts from Entra ID to OCI IAM, Entra ID is the authoritative identity store, by using a prebuilt application template from the Entra ID Apps Gallery

## **Pulling user accounts, groups and group membership from Entra ID to OCI IAM**

By pulling user accounts, groups and group membership from Entra ID to OCI IAM, Entra ID is the authoritative identity store, by using the template from the OCI IAM Application Catalog

## **Pushing user accounts, groups and license from OCI IAM to Entra ID**

By pushing user accounts, groups and license from OCI IAM to Entra ID, OCI IAM will be configured as the authoritative identity store

# Requirements

## OCI Identity Domain

*Administration Role User*

OCI Domain URL

<https://<domainURL>/admin/v1>

## MS Entra ID account with at least one of the following roles

*Global Administrator, Cloud Application Administrator, Application Administrator*

Sign-On URL

[https://console.\[REGION\].oraclecloud.com/](https://console.[REGION].oraclecloud.com/)

## Secret token generated from

*client ID*

*client secret*

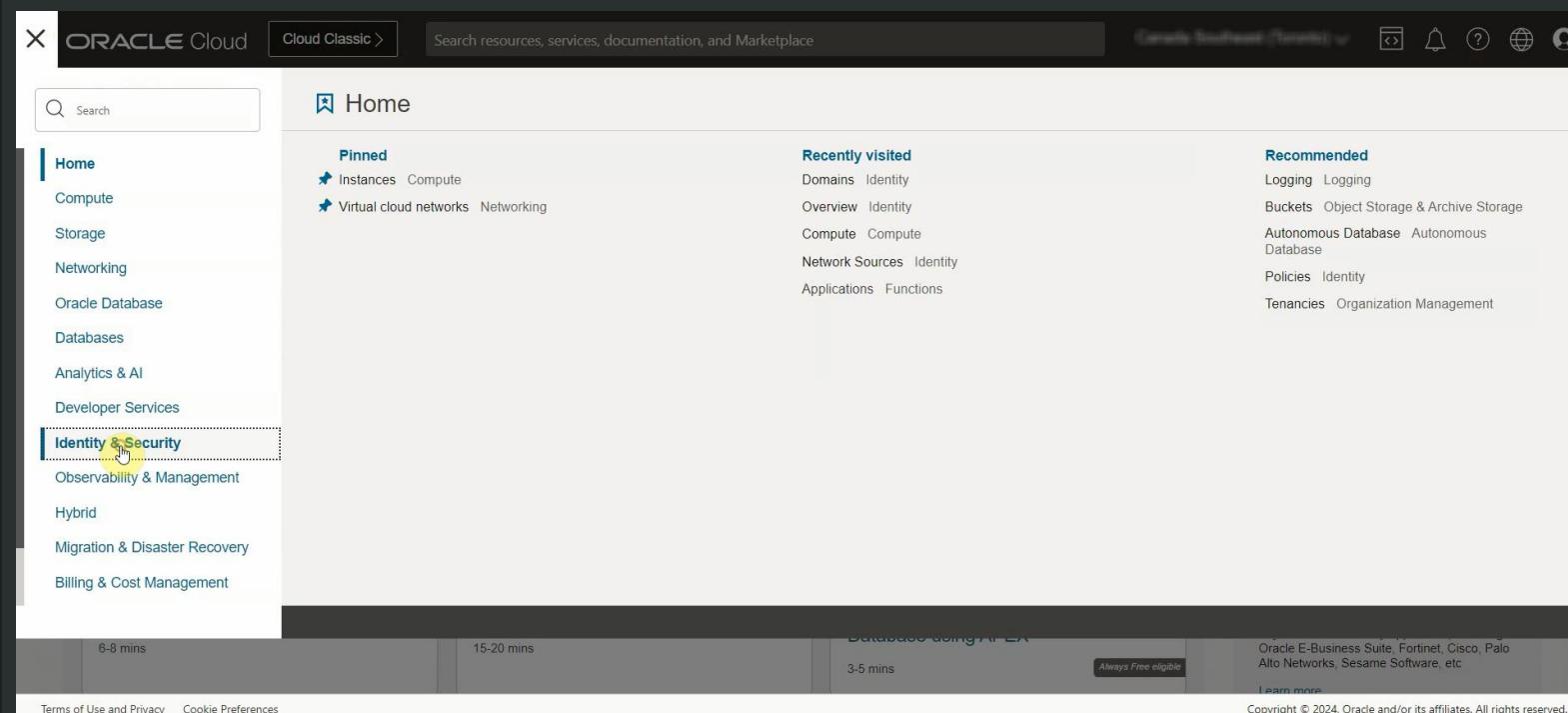
# Pushing user accounts from Entra ID to OCI IAM

---

# Pushing user accounts from Entra ID to OCI IAM

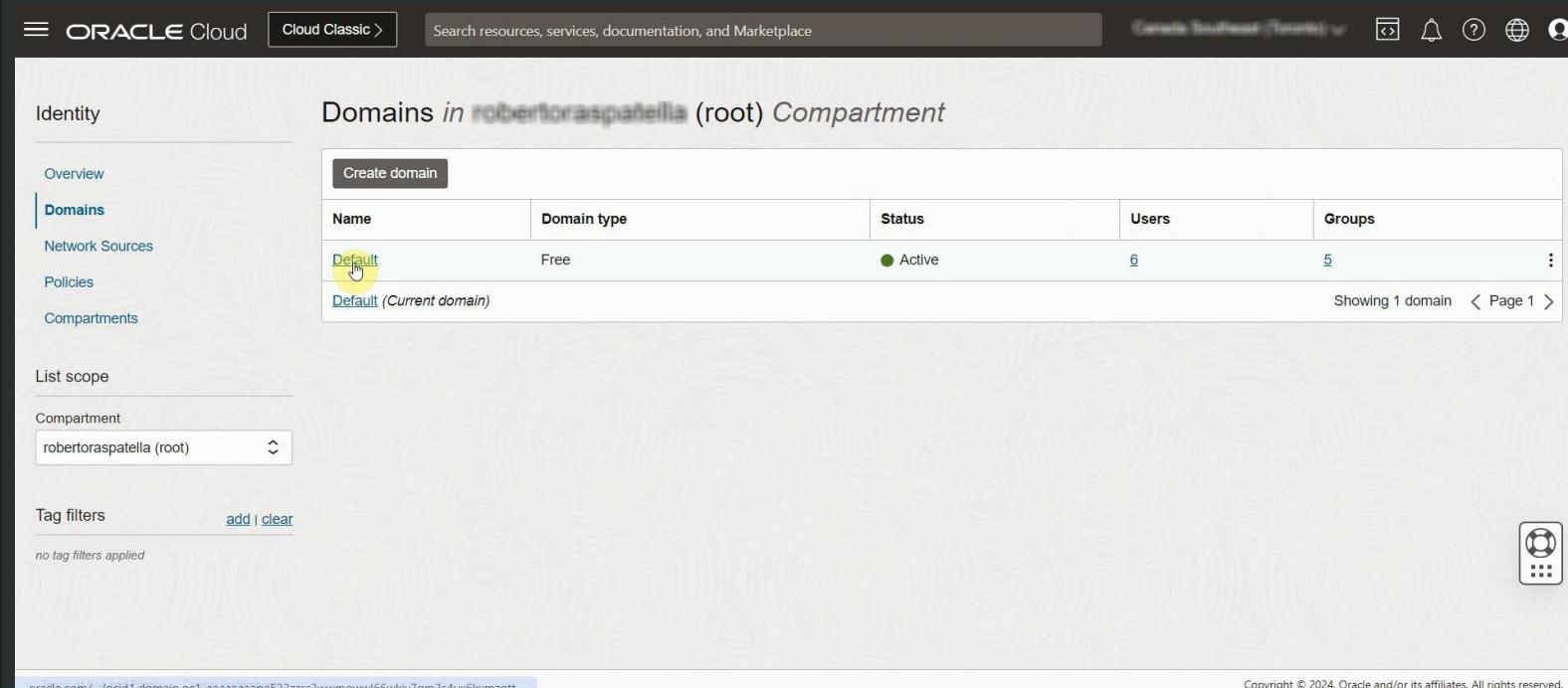
At first, it is needed to configure Entra ID to act as the identity manager so that user accounts are synchronized from Entra ID to OCI IAM.

In OCI, select *Identity & Security* from the top left menu.



# Pushing user accounts from Entra ID to OCI IAM

Then select the domain of the users that is intended to federate



The screenshot shows the Oracle Cloud Identity Domains page. The left sidebar has 'Identity' selected, with options for Overview, Domains (which is highlighted), Network Sources, Policies, and Compartments. The main area displays a table titled 'Domains in robertoraspalena (root) Compartment'. The table has columns for Name, Domain type, Status, Users, and Groups. One row is visible: 'Default' (Free, Active, 6 users, 5 groups). A tooltip 'Default (Current domain)' appears over the 'Default' link. Below the table, it says 'Showing 1 domain < Page 1 >'. At the bottom, there's a URL 'oracle.com/.../ocid1.domain.oc1....' and a copyright notice 'Copyright © 2024, Oracle and/or its affiliates. All rights reserved.'

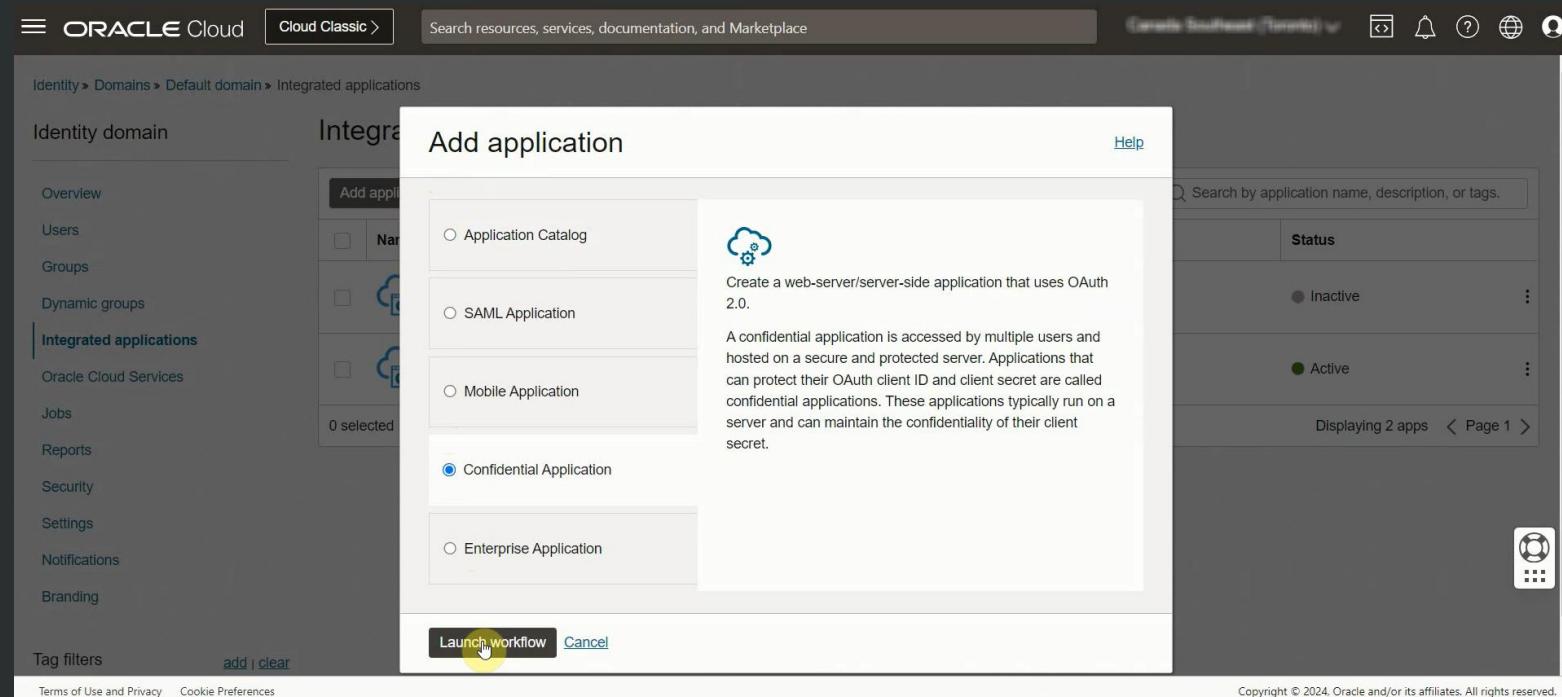
Name	Domain type	Status	Users	Groups
Default	Free	Active	6	5

# Pushing user accounts from Entra ID to OCI IAM

In the identity domain, select *Applications*

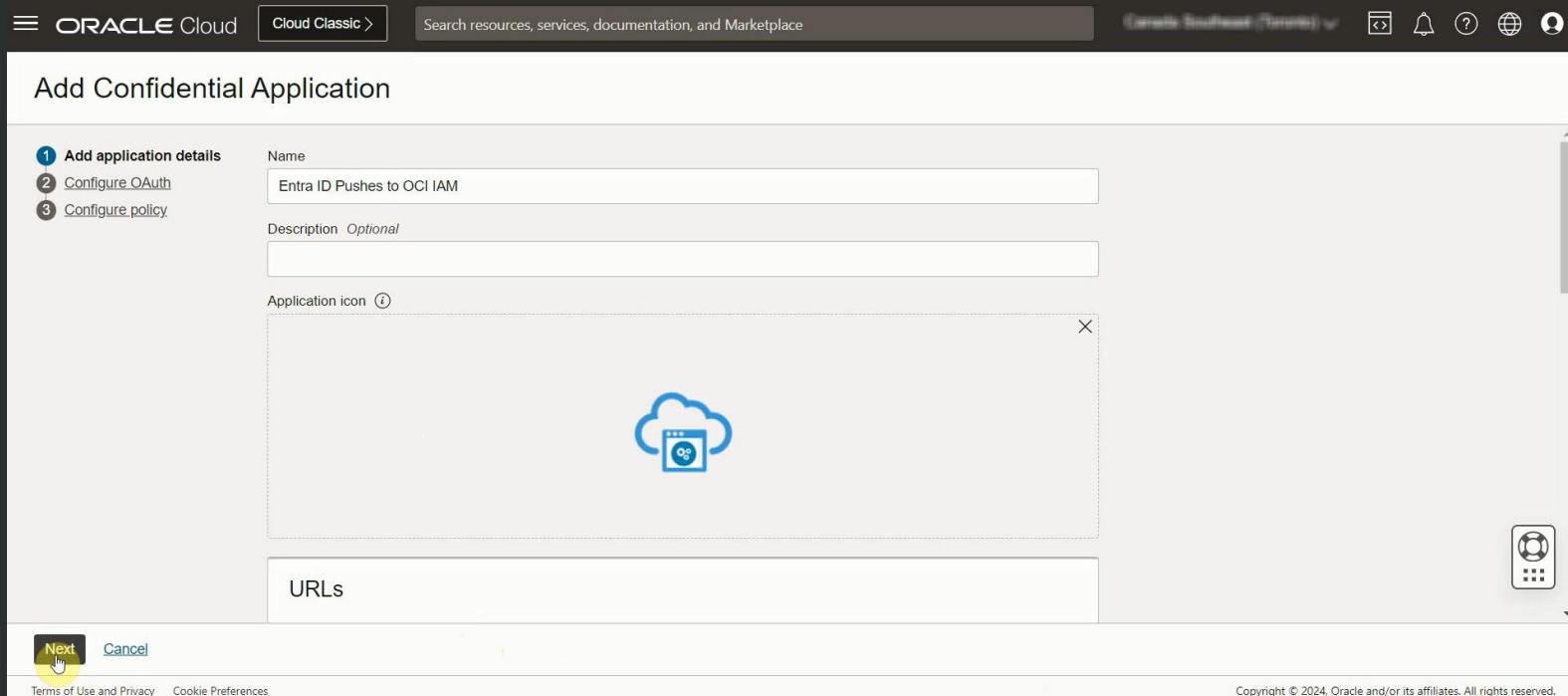
Select *Add Application* and choose *Confidential Application*

Then select *Launch workflow*



# Pushing user accounts from Entra ID to OCI IAM

Enter a name for the application  
and select *Next*



The screenshot shows the 'Add Confidential Application' wizard in Oracle Cloud. The title bar includes the Oracle Cloud logo, 'Cloud Classic >', and a search bar. The main form is titled 'Add Confidential Application' and is on step 1: 'Add application details'. It has three numbered steps: 1. Add application details (current), 2. Configure OAuth, and 3. Configure policy. The 'Name' field contains 'Entra ID Pushes to OCI IAM'. The 'Description' field is optional and empty. An 'Application icon' section shows a placeholder for a cloud icon with a small 'og' logo. Below is a 'URLs' section which is currently empty. At the bottom, there are 'Next' and 'Cancel' buttons, with 'Next' being highlighted.

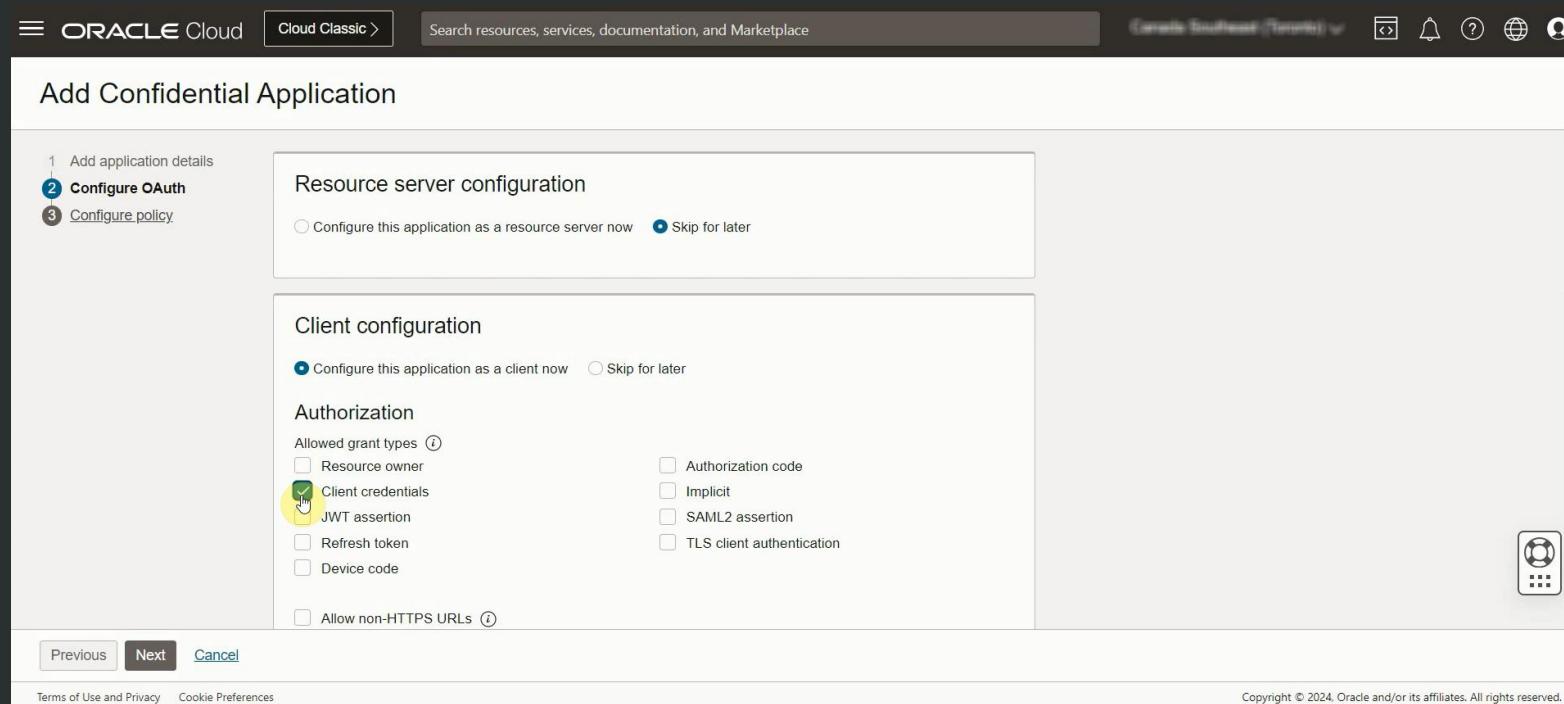


# Pushing user accounts from Entra ID to OCI IAM

Under *Client configuration*, select *Configure this application as a client now*

Then, under *Authorization*, check *Client credentials*

Scroll Down the page.



# Pushing user accounts from Entra ID to OCI IAM

In the *Token issuance policy* section, set *Authorized resources* to *Specific*

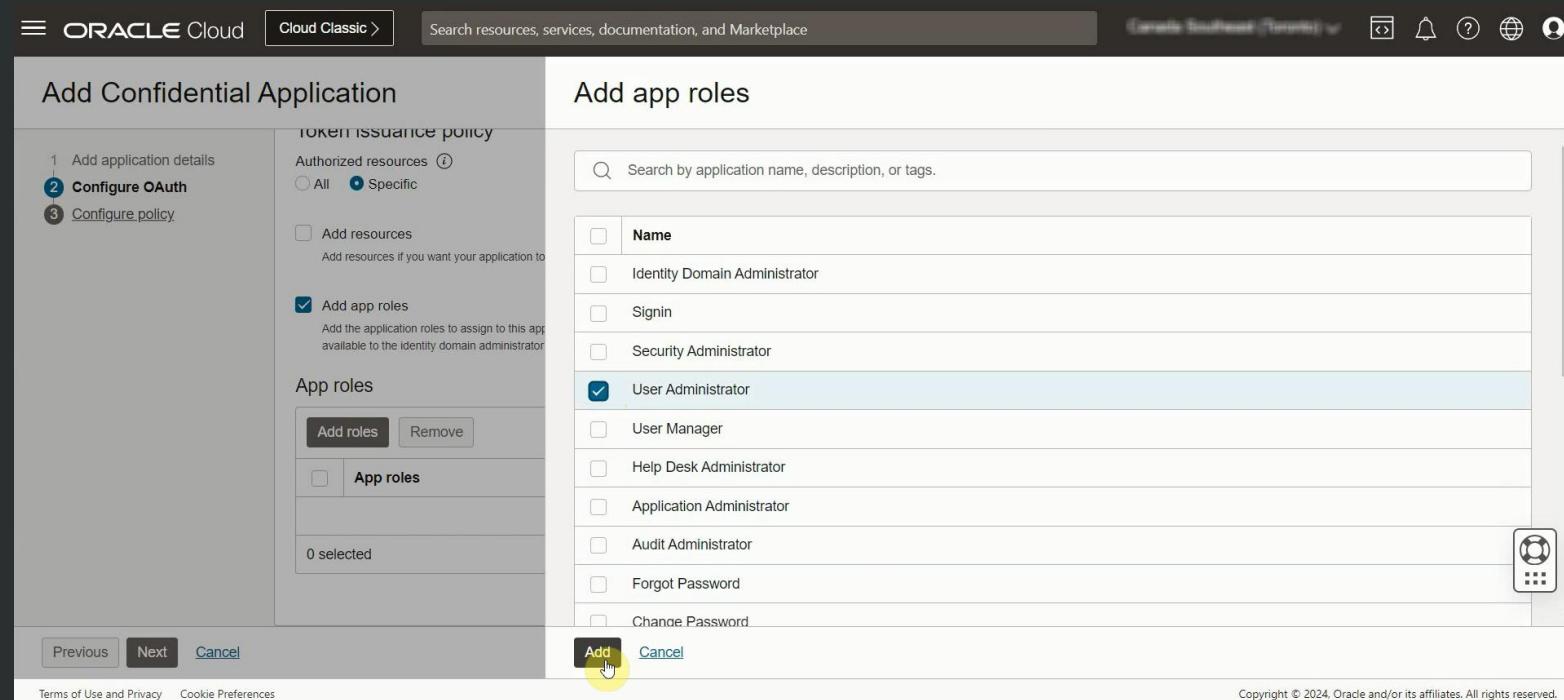
Select then *Add app roles*

The screenshot shows the Oracle Cloud interface for adding a confidential application. The top navigation bar includes 'ORACLE Cloud', 'Cloud Classic >', a search bar, and account information for 'Canada Southeast (Toronto)'. The main window title is 'Add Confidential Application'. The process is at step 2, 'Configure OAuth'. On the left, there's a sidebar with three steps: 1. Add application details, 2. Configure OAuth (which is active), and 3. Configure policy. The main content area has several sections: 'Content encryption algorithm' (with a note about encrypting tokens for third parties), 'Bypass consent' (a toggle switch turned off), 'Client IP address' (radio buttons for 'Anywhere' and 'Restrict by network perimeter'), 'Token issuance policy', 'Authorized resources' (radio buttons for 'All' and 'Specific' - 'Specific' is selected), 'Add resources' (checkbox), 'Add app roles' (button with a hand icon), and 'App roles' (a note about assigning application roles). At the bottom are 'Previous', 'Next' (highlighted in dark grey), and 'Cancel' buttons, along with links for 'Terms of Use and Privacy' and 'Cookie Preferences'. The footer contains the copyright notice 'Copyright © 2024, Oracle and/or its affiliates. All rights reserved.'

# Pushing user accounts from Entra ID to OCI IAM

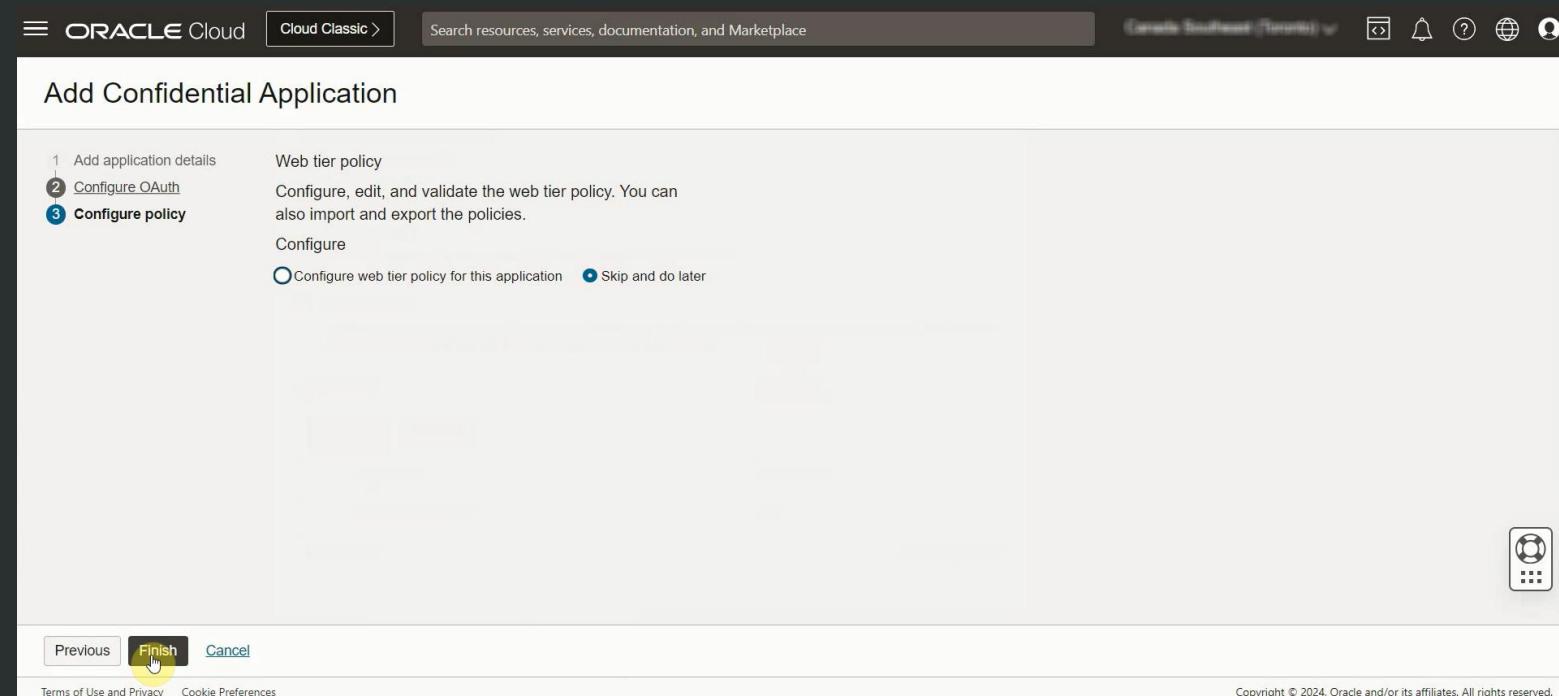
In the *App Roles* section, select *Add roles*, and in the *Add app roles* page select *User Administrator*, then select *Add*

User Administrator will appear on the application roles to assign to this application



# Pushing user accounts from Entra ID to OCI IAM

Select *Next* and then select  
*Finish*

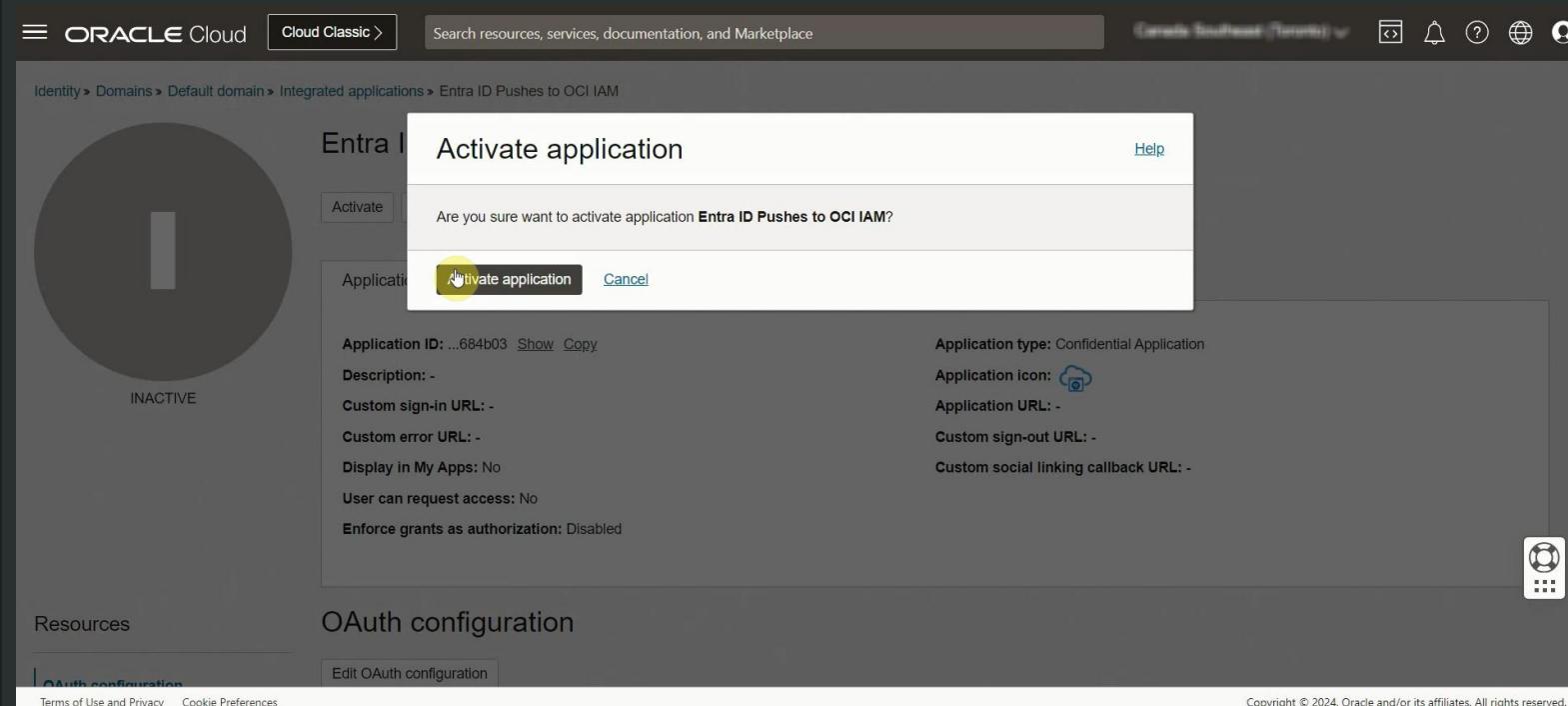


The screenshot shows the 'Add Confidential Application' wizard in the Oracle Cloud interface. The current step is 'Configure OAuth'. The wizard has three steps: 1. Add application details (completed), 2. Configure OAuth (current step), and 3. Configure policy (next step). Step 2 is divided into two sections: 'Web tier policy' and 'Configure'. Under 'Web tier policy', there is a note about configuring, editing, validating policies, and importing/exporting them. Below this is a 'Configure' button and a radio button for 'Configure web tier policy for this application' (selected) or 'Skip and do later' (unchecked). At the bottom of the wizard are 'Previous', 'Finish' (highlighted with a yellow circle), and 'Cancel' buttons. A small note at the bottom left says 'Terms of Use and Privacy' and 'Cookie Preferences'. The bottom right corner contains copyright information: 'Copyright © 2024, Oracle and/or its affiliates. All rights reserved.'

# Pushing user accounts from Entra ID to OCI IAM

On the application overview page, select *Activate* and confirm the activation of the application

The confidential application is now activated.



# Pushing user accounts from Entra ID to OCI IAM

Return to the identity domain overview by selecting the identity domain name in the breadcrumbs

Select *Copy* next to the Domain URL in *Domain information* and save the URL to a text editor

The screenshot shows the Oracle Cloud Identity domain overview page. The left sidebar lists various sections: Overview, Users, Groups, Dynamic groups, Integrated applications, Oracle Cloud Services, Jobs, Reports, Security, Settings, Notifications, and Branding. The main content area is titled "Overview in Default Domain". It includes tabs for "Domain information" and "Tags". Under "Domain information", there are fields for OCID, Domain type (Free), Description (Default domain), Domain replication (-), Home region (Canada Southeast - Toronto), Created (Fri, Jun 9, 2023, 08:13:38 UTC), Show domain on login (On), Domain URL (ecloud.com:443), Regional URL (...ud.com:443), and Status (Active). A yellow box highlights the "Copy" button next to the Domain URL. Below this is an "Audit log report" section with a "Review" icon and a link to "Review identity domain activity, including successful and failed logins, and creation, modification, and deletion of user accounts.". To the right, there's a "Get the most out of your domain" section with a "Learn more" link. The bottom of the page includes links for "Terms of Use and Privacy" and "Cookie Preferences", and a copyright notice: "Copyright © 2024, Oracle and/or its affiliates. All rights reserved.".

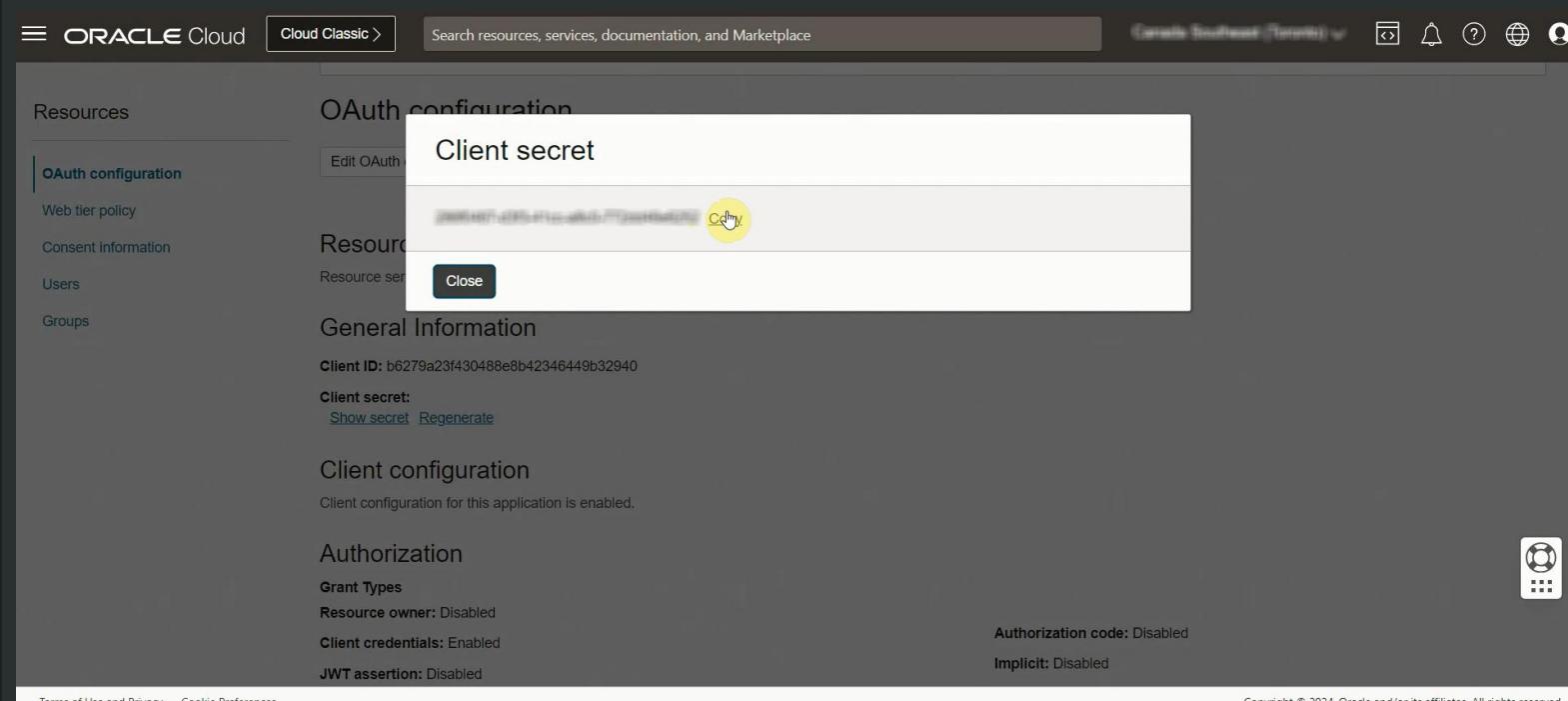
# Pushing user accounts from Entra ID to OCI IAM

In the confidential app in OCI IAM, select *OAuth configuration* under *Resources*

Scroll down and find the Client ID and Client secret under *General Information*

Copy the client ID and store it

Select *Show secret* and copy the secret and store it



# Make a note of the secret token value

The secret token is the base64 encoding of <clientID>:<clientsecret>

or

base64(<clientID>:<clientsecret>)



In Windows, open CMD and use powershell

```
[Convert]::ToString([System.Text.Encoding]::Unicode.GetBytes('client_id:secret'))
```



In Linux, use

```
echo -n <clientID>:<clientsecret> | base64 --wrap=0
```



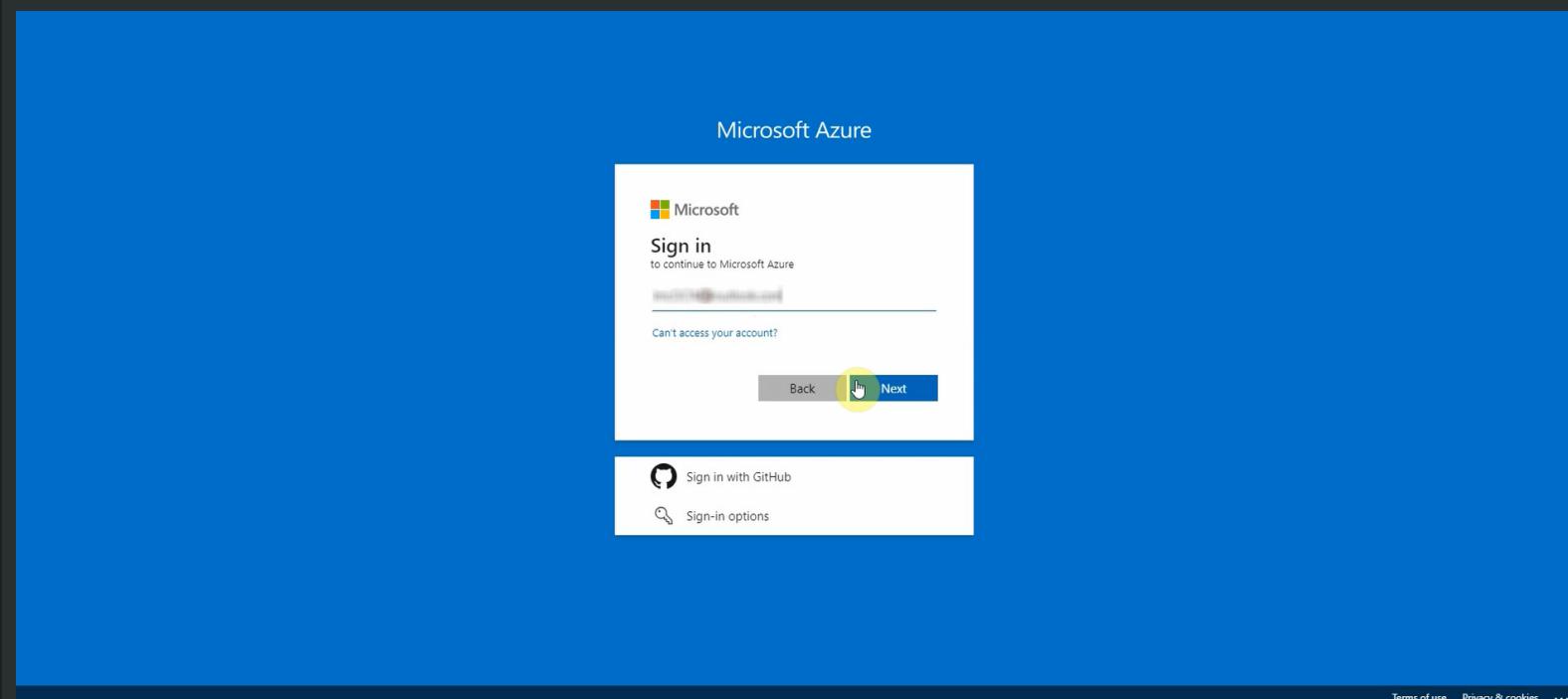
In MacOS, use

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

# Pushing user accounts from Entra ID to OCI IAM

It is now needed to configure Entra ID to enable it to be the authoritative identity store to manage identities in IAM

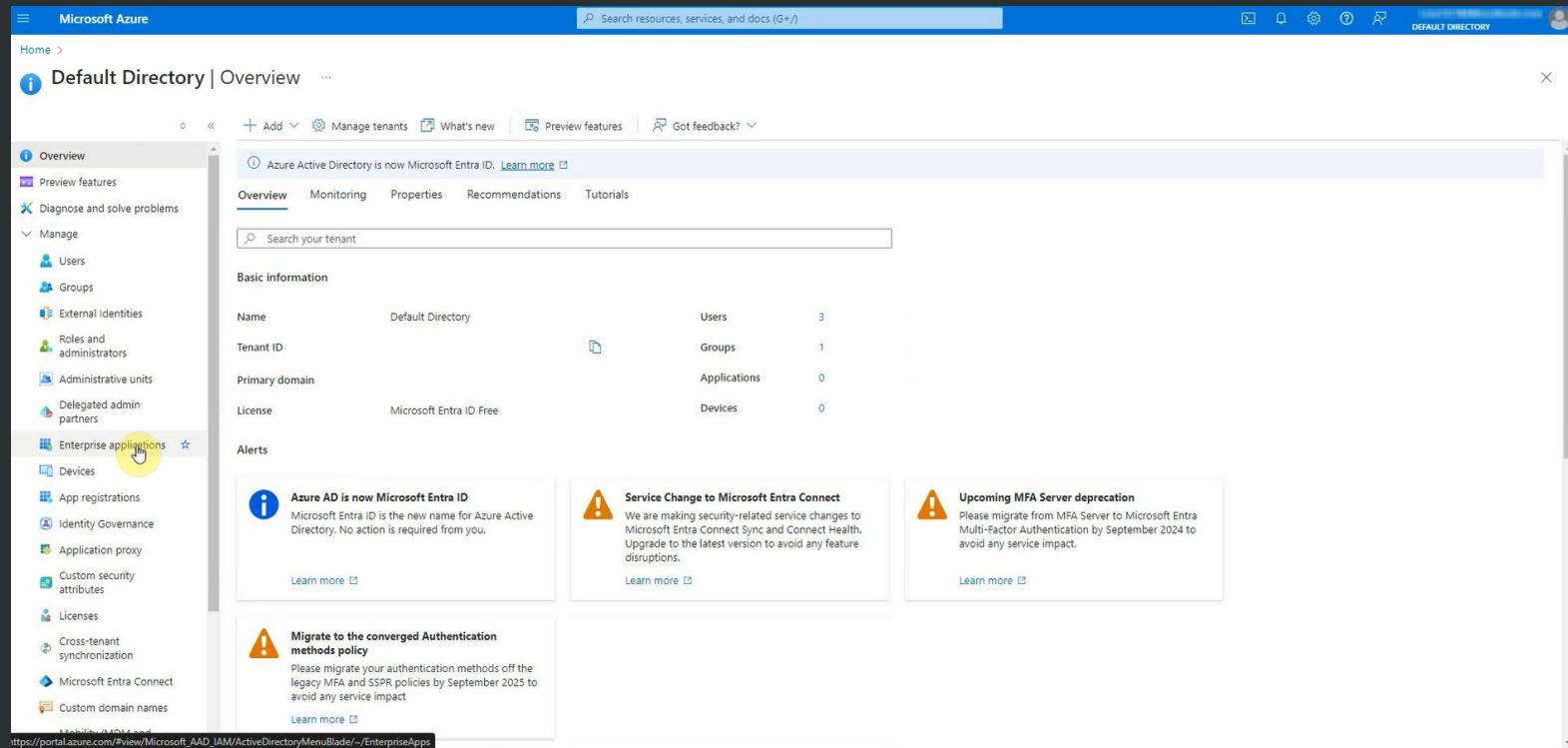
In the browser, sign in to Microsoft Entra ID using username and password on the URL: <https://portal.azure.com>



# Pushing user accounts from Entra ID to OCI IAM

Select *Identity* then *Applications*

Select *Enterprise applications*



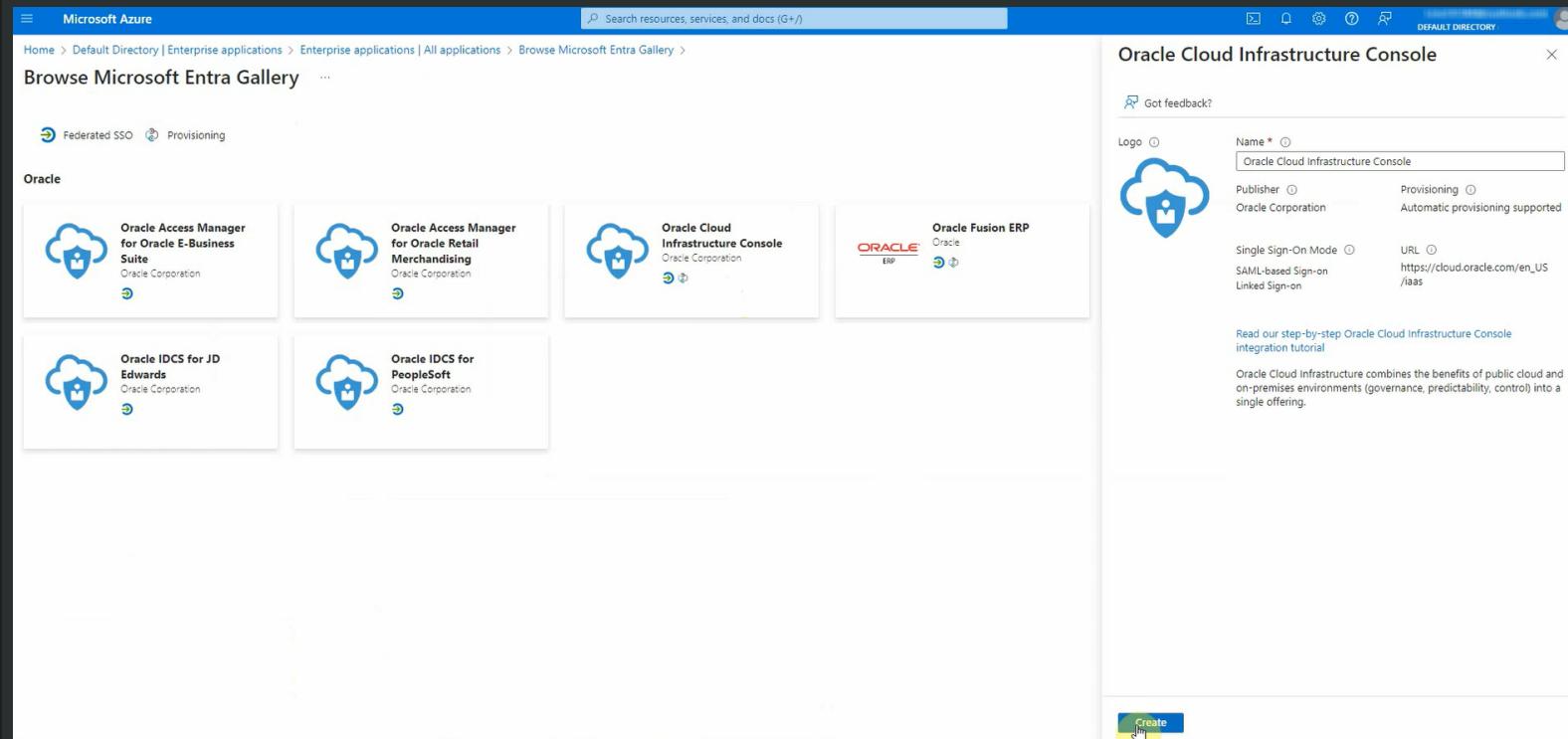
The screenshot shows the Microsoft Azure portal's 'Default Directory | Overview' page. On the left, there is a navigation sidebar with various options like 'Overview', 'Manage tenants', 'What's new', 'Preview features', 'Diagnose and solve problems', 'Manage' (with sub-options 'Users', 'Groups', 'External identities', 'Roles and administrators', 'Administrative units', 'Delegated admin partners'), 'Enterprise applications' (which is highlighted with a yellow circle), 'Devices', 'App registrations', 'Identity Governance', 'Application proxy', 'Custom security attributes', 'Licenses', 'Cross-tenant synchronization', 'Microsoft Entra Connect', and 'Custom domain names'. The main content area displays 'Basic information' for the tenant, including the name 'Default Directory', users (3), groups (1), primary domain (0), license (Microsoft Entra ID Free), and devices (0). Below this, there are three 'Alerts' sections: 'Azure AD is now Microsoft Entra ID' (info icon), 'Service Change to Microsoft Entra Connect' (warning icon), and 'Upcoming MFA Server deprecation' (warning icon). At the bottom of the page, the URL 'https://portal.azure.com/#view/Microsoft\_AAD\_IAM/ActiveDirectoryMenuBlade/~/EnterpriseApps' is visible.

# Pushing user accounts from Entra ID to OCI IAM

On the Enterprise applications page, select *New application* then type “Oracle” and then select Oracle Cloud Infrastructure Console

Choose Oracle Cloud Infrastructure Console and enter a name or accept the default one of *Oracle Cloud Infrastructure Console*

Select *Create*



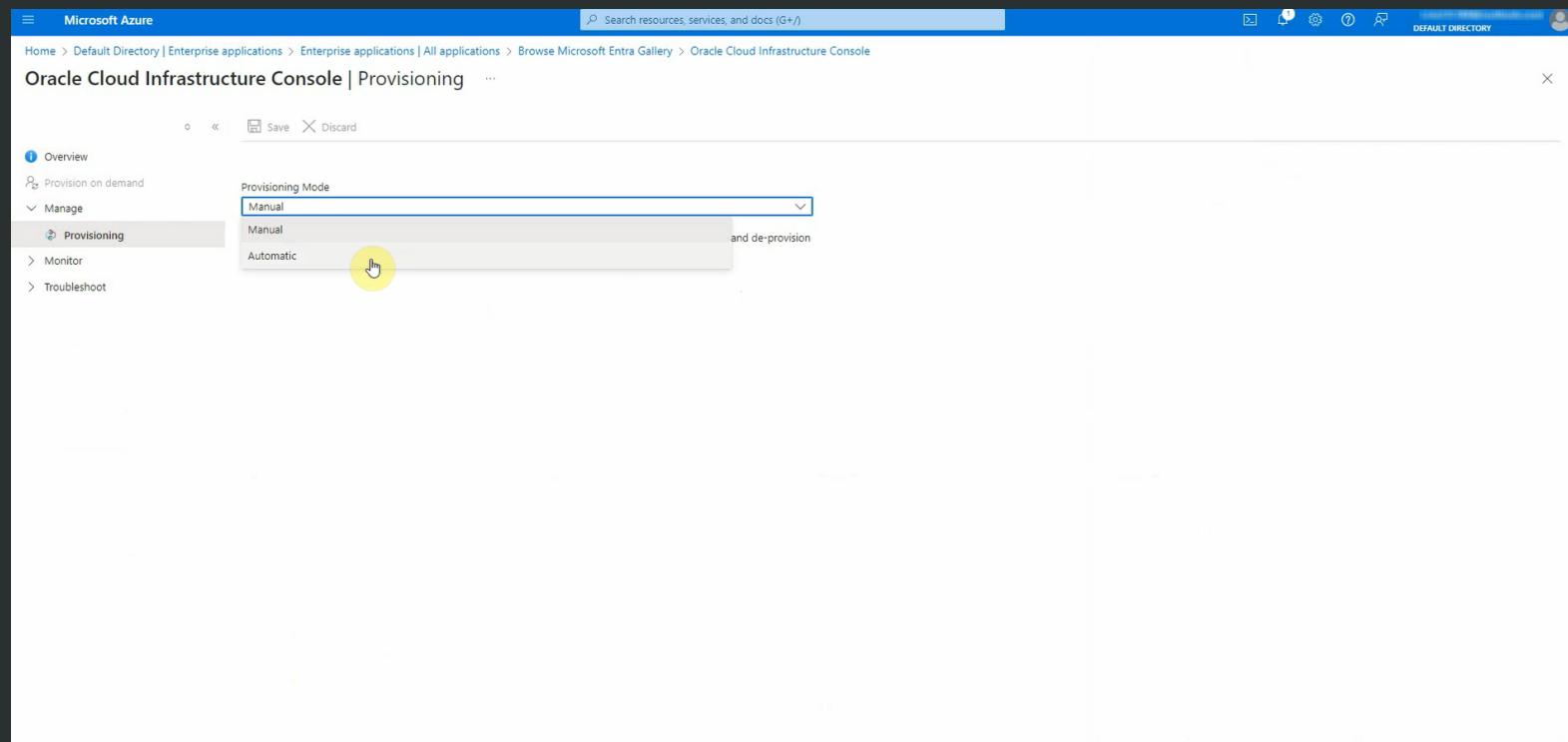
# Pushing user accounts from Entra ID to OCI IAM

Choose *Provisioning* from the left menu under *Manage*

The screenshot shows the Microsoft Azure Oracle Cloud Infrastructure Console Overview page. In the top navigation bar, there are links for Home, Default Directory, Enterprise applications, Enterprise applications, All applications, Browse Microsoft Entra Gallery, and a search bar. On the right side, there is a message: "Adding application Application Oracle Cloud Infrastructure Console added successfully". The main content area has a sidebar titled "Properties" with sections for Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups), Single sign-on (Provisioning, Self-service, Custom security attributes), Security, Activity, and Troubleshooting + Support. The "Provisioning" link is highlighted with a yellow circle and a cursor icon. Below the sidebar, there is a "Getting Started" section with five numbered steps: 1. Assign users and groups, 2. Set up single sign on, 3. Provision User Accounts, 4. Conditional Access, and 5. Self service. At the bottom, there is a "What's New" section with two items: "Sign in charts have moved!" and "Delete Application has moved to Properties".

# Pushing user accounts from Entra ID to OCI IAM

Select *Get started* and change  
Provisioning Mode to *Automatic*



# Pushing user accounts from Entra ID to OCI IAM

In Tenant URL, enter the OCI IAM Domain URL followed by /admin/v1

Tenant URL is

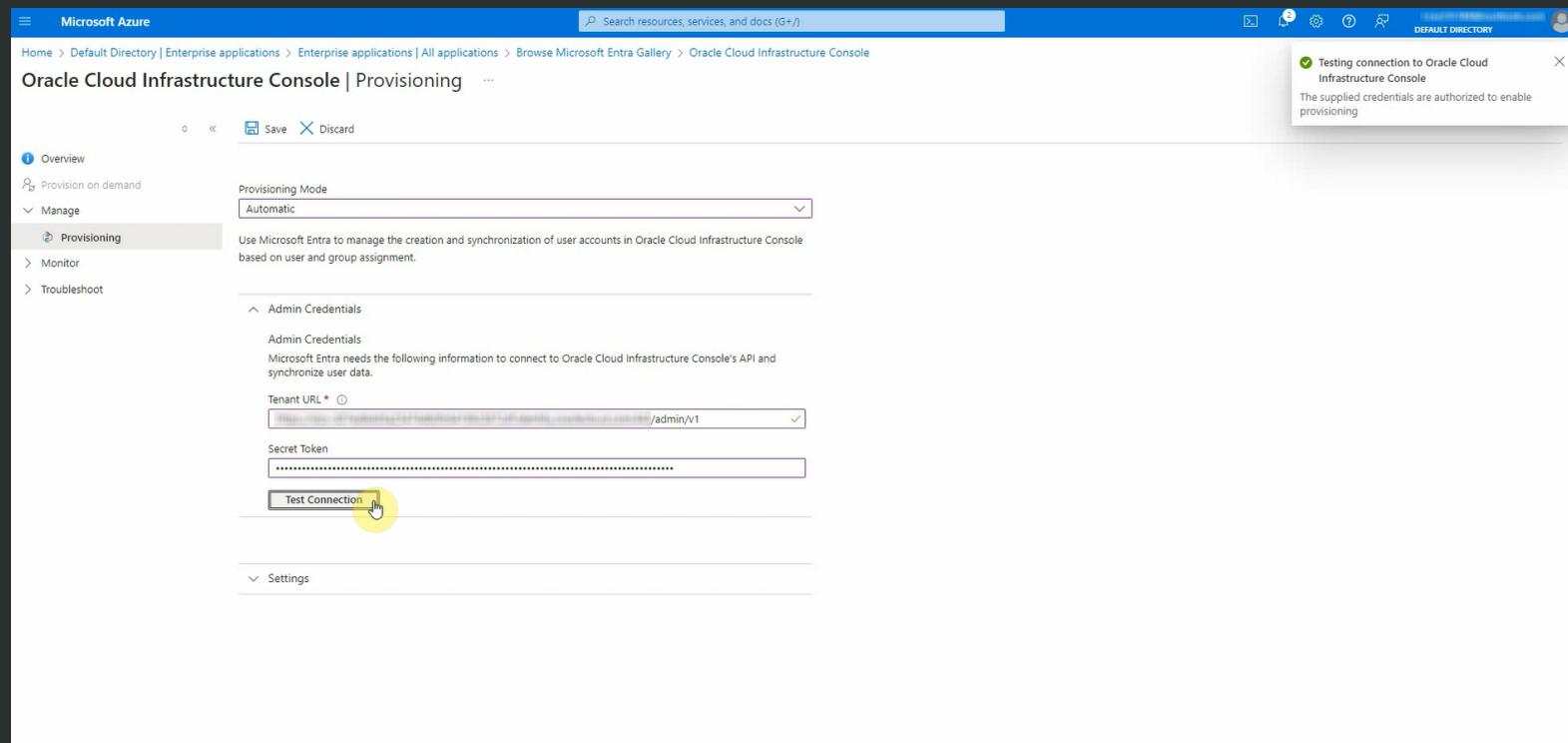
<https://<domainURL>/admin/v1>

Enter the secret token and select *Test Connection*

When this message appears, the connection is successful:

Testing connection to Oracle Cloud Infrastructure Console

The supplied credentials are authorized to enable provisioning

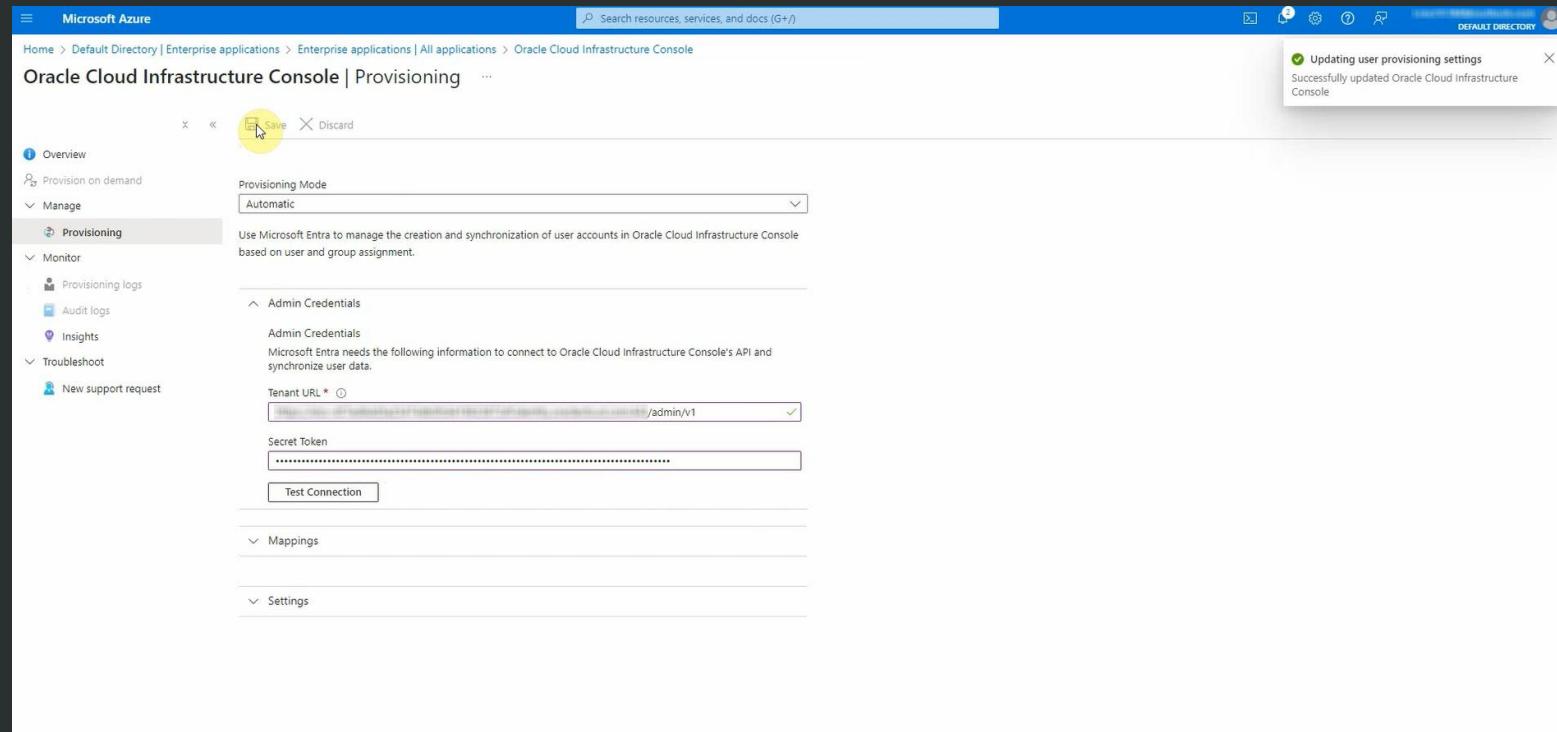


# Pushing user accounts from Entra ID to OCI IAM

## Select Save

The environments are now correctly configured. It is possible to assign the users that are needed to be provisioned, by choosing them on Entra ID from the Oracle application previously created, selecting and then assigning them

The automatic provisioning will do the job. Please keep in mind that removing users from the Oracle Cloud Infrastructure application on Entra ID, they will be just deactivated on OCI IAM



# Pushing user accounts from Entra ID to OCI IAM

At this point, users don't have credentials to sign in directly to OCI. By setting the federated attribute to *TRUE*, they'll be able to use their federated accounts to sign in to OCI.

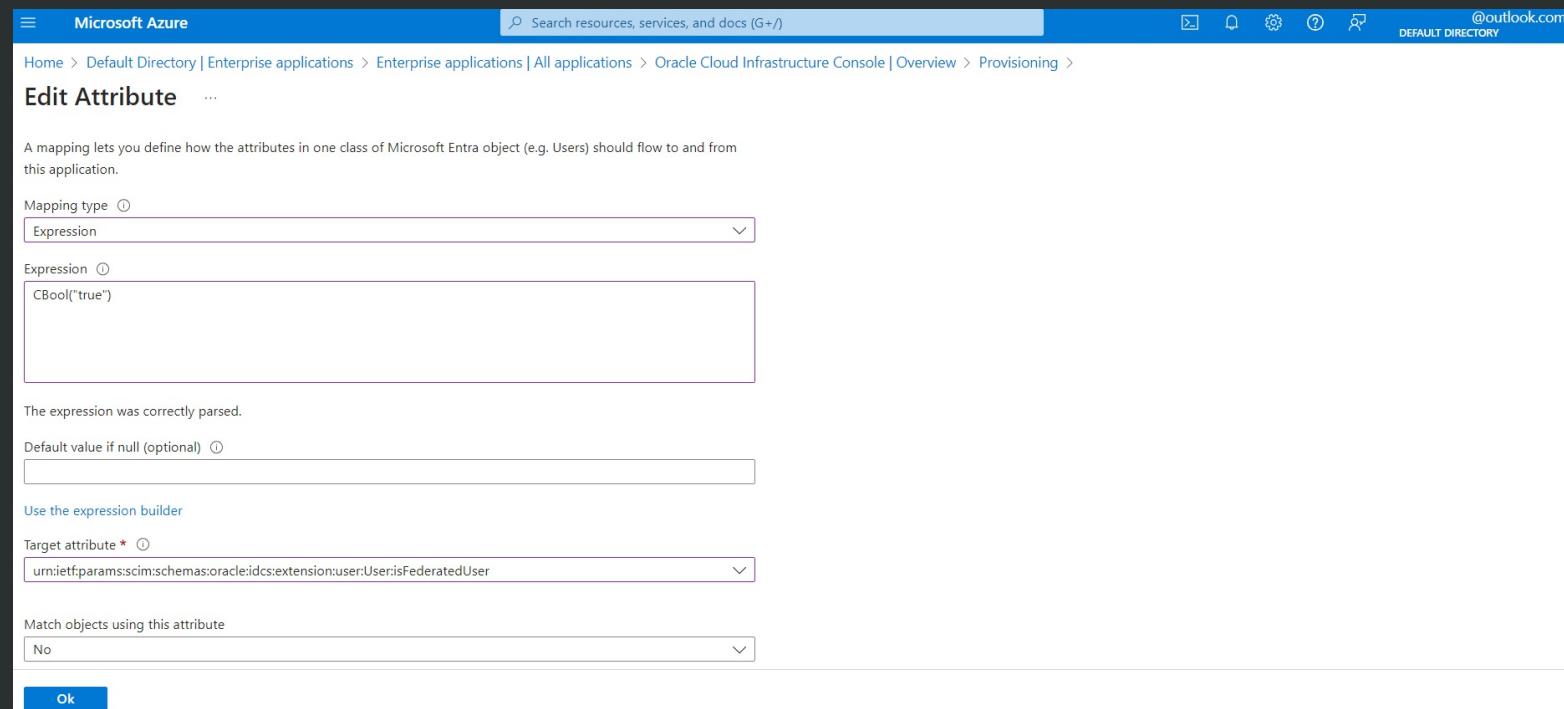
In the Provisioning page, select *Mappings* and add a *New Mapping*. This mapping type will be as *Expression*. Provide the following parameters:

Expression: `CBool("true")`

Target Attribute:

`urn:ietf:params:scim:schemas:oracle:idcs:extension:user:User:isFederatedUser`

Select *OK* and *Save*



# Pushing user accounts from Entra ID to OCI IAM

In Entra ID, in the left menu select *Enterprise applications*

Select the application created earlier, Oracle Cloud Infrastructure Console

In the left menu under *Manage*, select *Users and groups*

In the *Users and groups* page, select *Add user/group*

In the *Add Assignment* page, on the left under *Users and groups*, select *None Selected*

Select one or more users or groups from the list

On the *Add Assignment* page, select *Assign*

The Users and groups page now shows the chosen users and groups

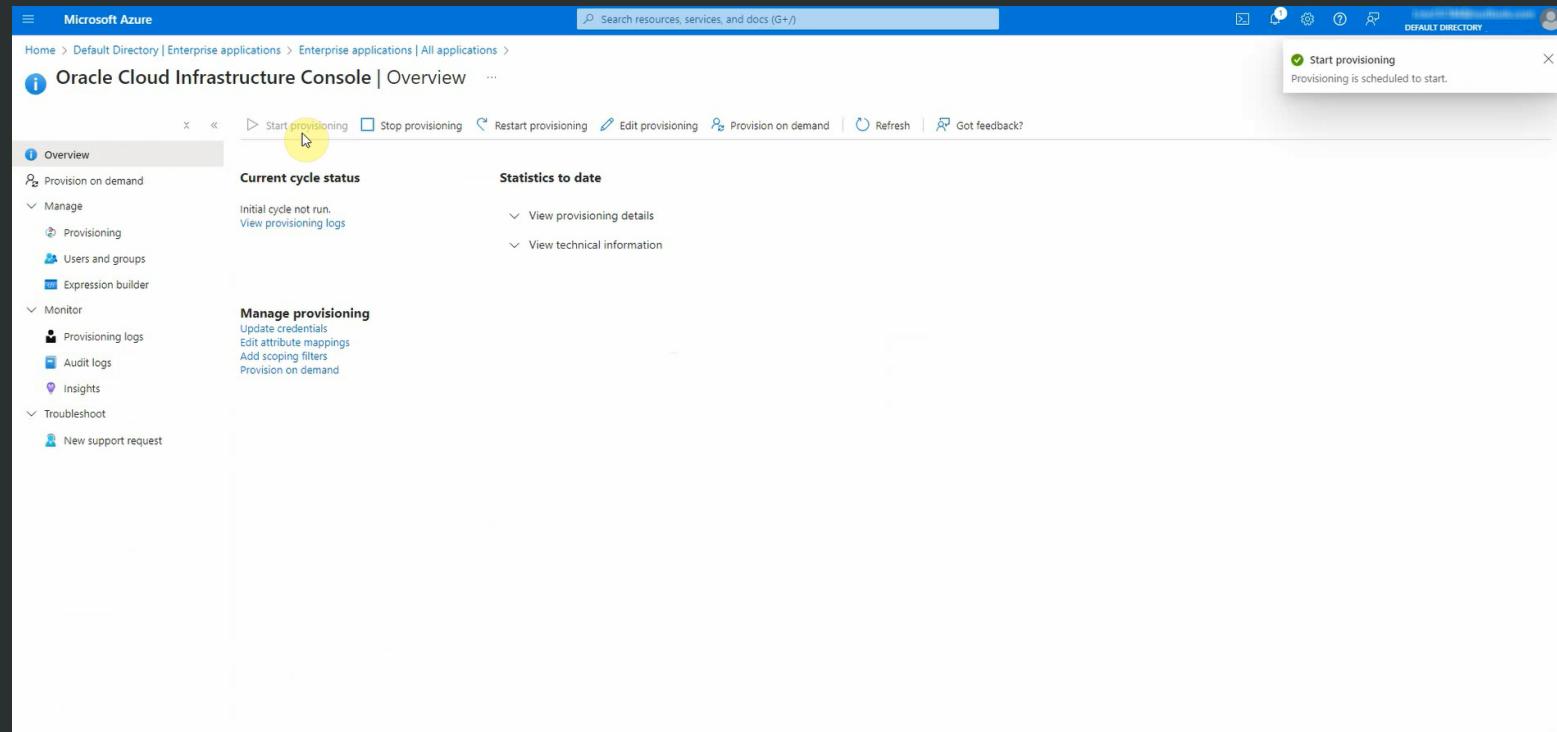
The screenshot shows the Microsoft Azure interface with the Oracle Cloud Infrastructure Console application selected. The left sidebar shows navigation options like Overview, Deployment Plan, Diagnose and solve problems, Manage (Properties, Owners, Roles and administrators, Users and groups), Single sign-on, Provisioning, Self-service, and Custom security attributes. The main content area displays the 'Users and groups' page for the Oracle Cloud Infrastructure Console application. It includes a note about the application appearing in My Apps if 'Visible to users?' is set to yes. A table lists two users assigned to the application:

Display Name	Object Type	Role assigned
OCI-IAM-User01	User	User
OCI-IAM-User02	User	User

# Pushing user accounts from Entra ID to OCI IAM

Choose *Provisioning* from the left menu under *Manage* and select *Start provisioning*

The provisioning cycle starts, and the status of provisioning is displayed



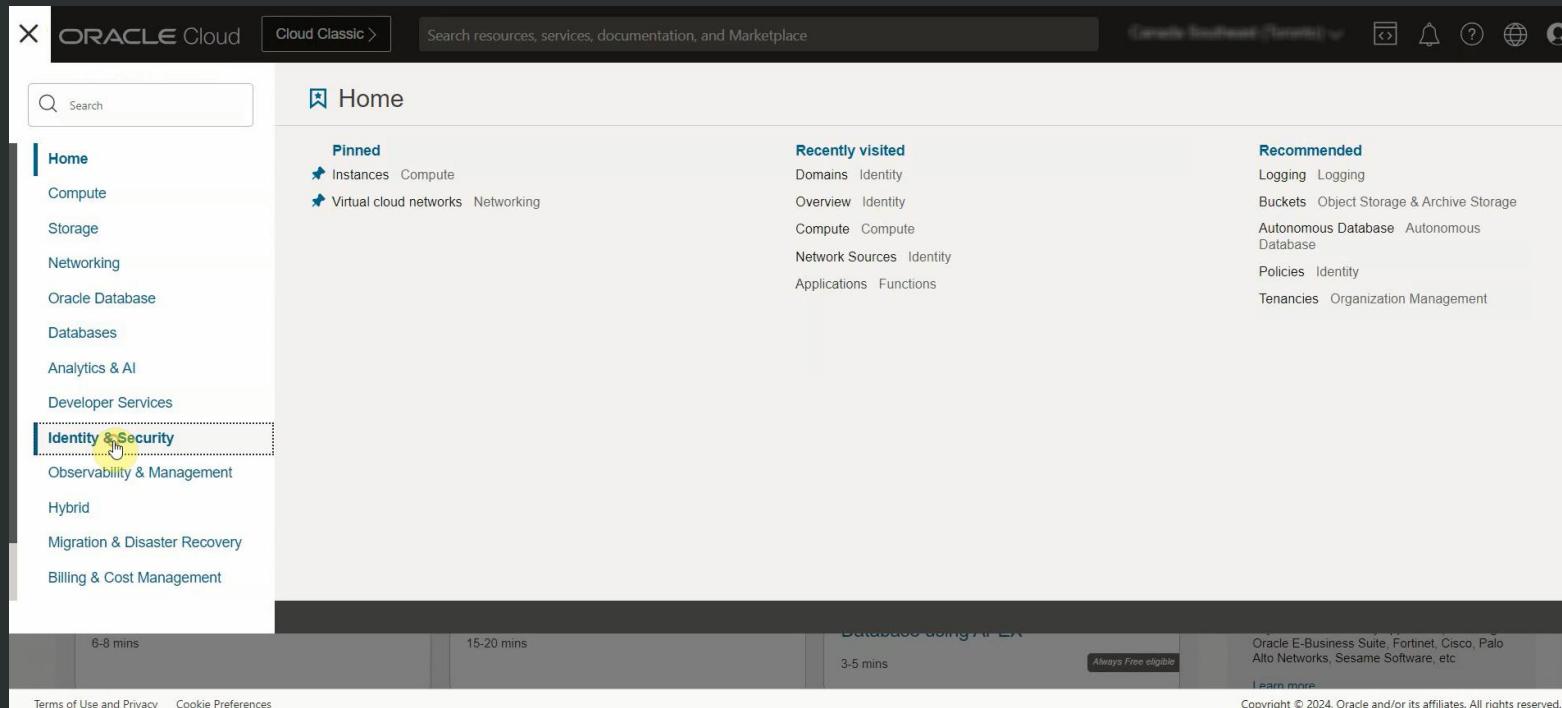
# **Pulling user accounts, groups and group membership from Entra ID to OCI IAM**

---

# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

In this case, Entra ID will use OCI IAM as the identity store

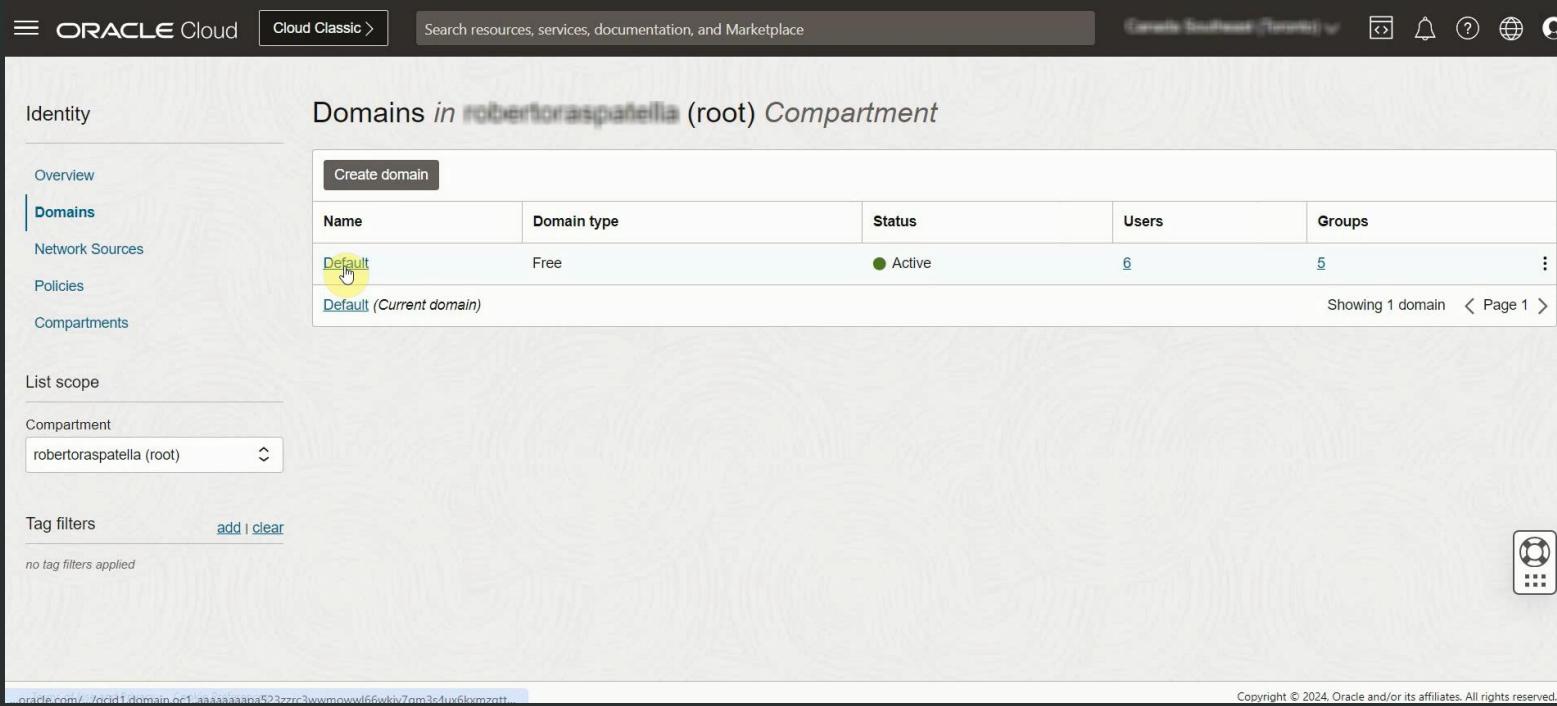
By creating an app in OCI IAM to act like identity provider for Entra ID, and by enabling synchronization, users, groups and group membership from Entra ID will be populated in OCI IAM as well



In OCI, select *Identity & Security* from the top left menu.

# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Then select the domain of the users that is intended to synchronize



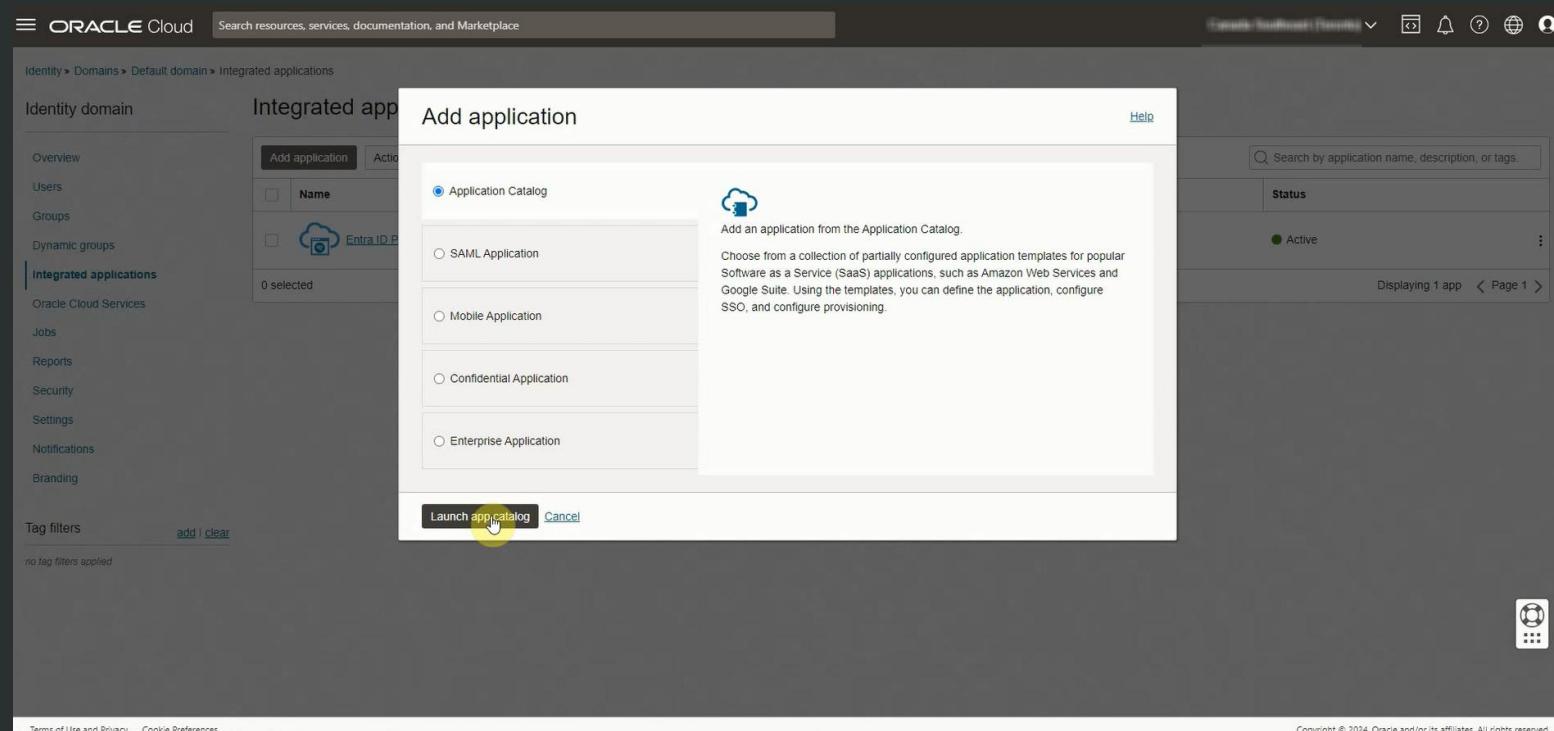
The screenshot shows the Oracle Cloud Identity Domains page. The left sidebar has 'Identity' selected, with options for Overview, Domains (which is active), Network Sources, Policies, and Compartments. The main area displays a table titled 'Domains in robertoraspapella (root) Compartment'. The table has columns for Name, Domain type, Status, Users, and Groups. A single row is shown: 'Default' (highlighted with a yellow box and a cursor icon) is of type 'Free', status is 'Active', there are 6 users and 5 groups. Below the table, it says 'Showing 1 domain < Page 1 >'. At the bottom right of the page is a small circular icon with a grid pattern.

Name	Domain type	Status	Users	Groups
Default (Current domain)	Free	Active	6	5

# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

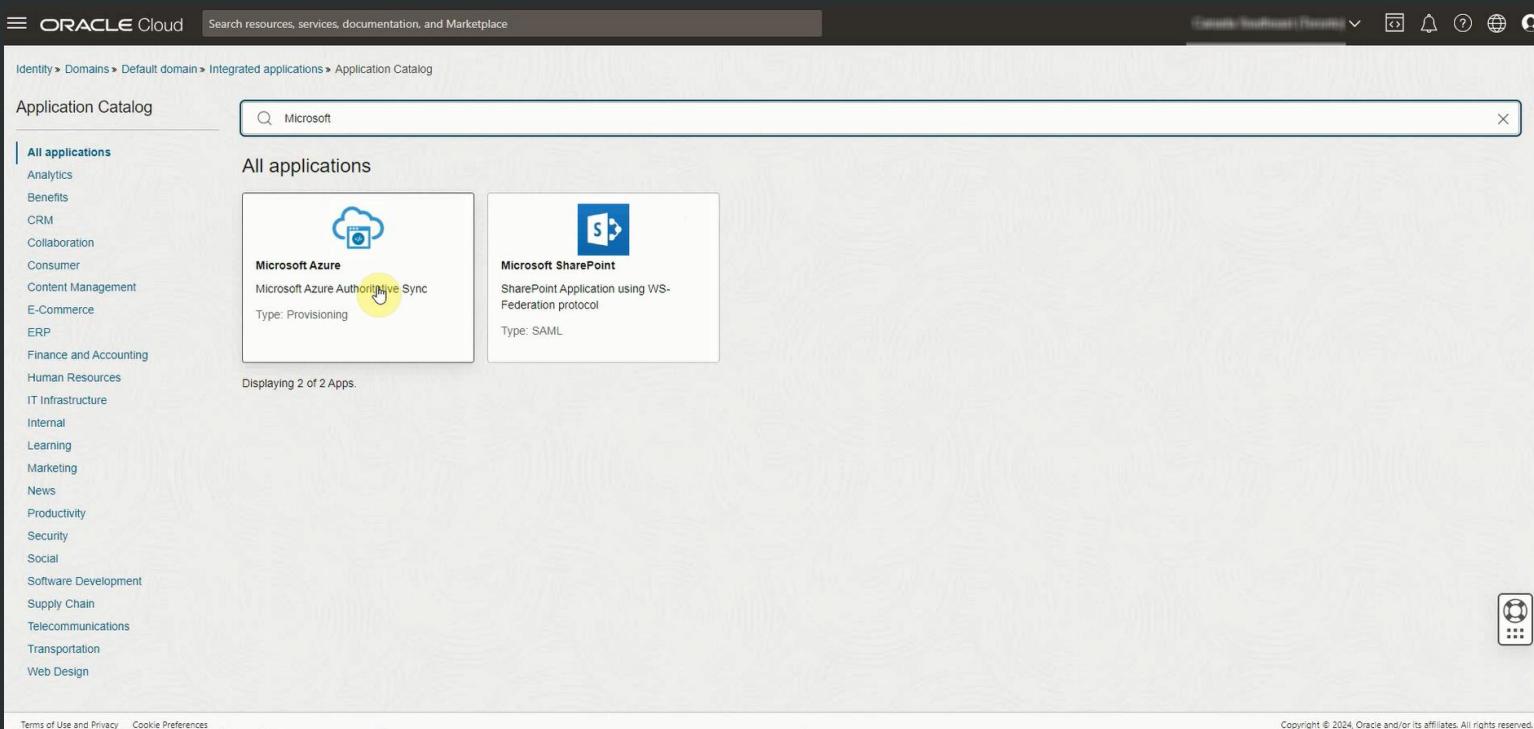
Under *Integrated application*, select Add application and then select Application Catalog

Select Launch workflow



# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Search for “Microsoft” and select *Microsoft Azure*



The screenshot shows the Oracle Cloud Application Catalog interface. At the top, there's a navigation bar with 'ORACLE Cloud' and a search bar. Below the navigation, the path is listed as 'Identity > Domains > Default domain > Integrated applications > Application Catalog'. A search bar on the right contains the text 'Microsoft'. The main area is titled 'Application Catalog' and 'All applications'. It displays two items: 'Microsoft Azure' and 'Microsoft SharePoint'. The 'Microsoft Azure' item is highlighted with a yellow circle around its icon and name, indicating it is selected. The 'Microsoft SharePoint' item is also visible with its icon and details. The left sidebar lists various application categories such as Analytics, Benefits, CRM, Collaboration, Consumer, Content Management, E-Commerce, ERP, Finance and Accounting, Human Resources, IT Infrastructure, Internal, Learning, Marketing, News, Productivity, Security, Social, Software Development, Supply Chain, Telecommunications, Transportation, and Web Design.

# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Enter the name of the application to be used

The screenshot shows the Oracle Cloud interface for adding a new application. The title bar says "Add Microsoft Azure". The main form has two tabs: "Add application details" (selected) and "Configure provisioning".

**Add application details:**

- Name:** Entra ID Pulls from OCI IAM
- Description (Optional):** Microsoft Azure Authoritative Sync
- Application icon:** A placeholder box containing a blue cloud icon with a person icon inside.

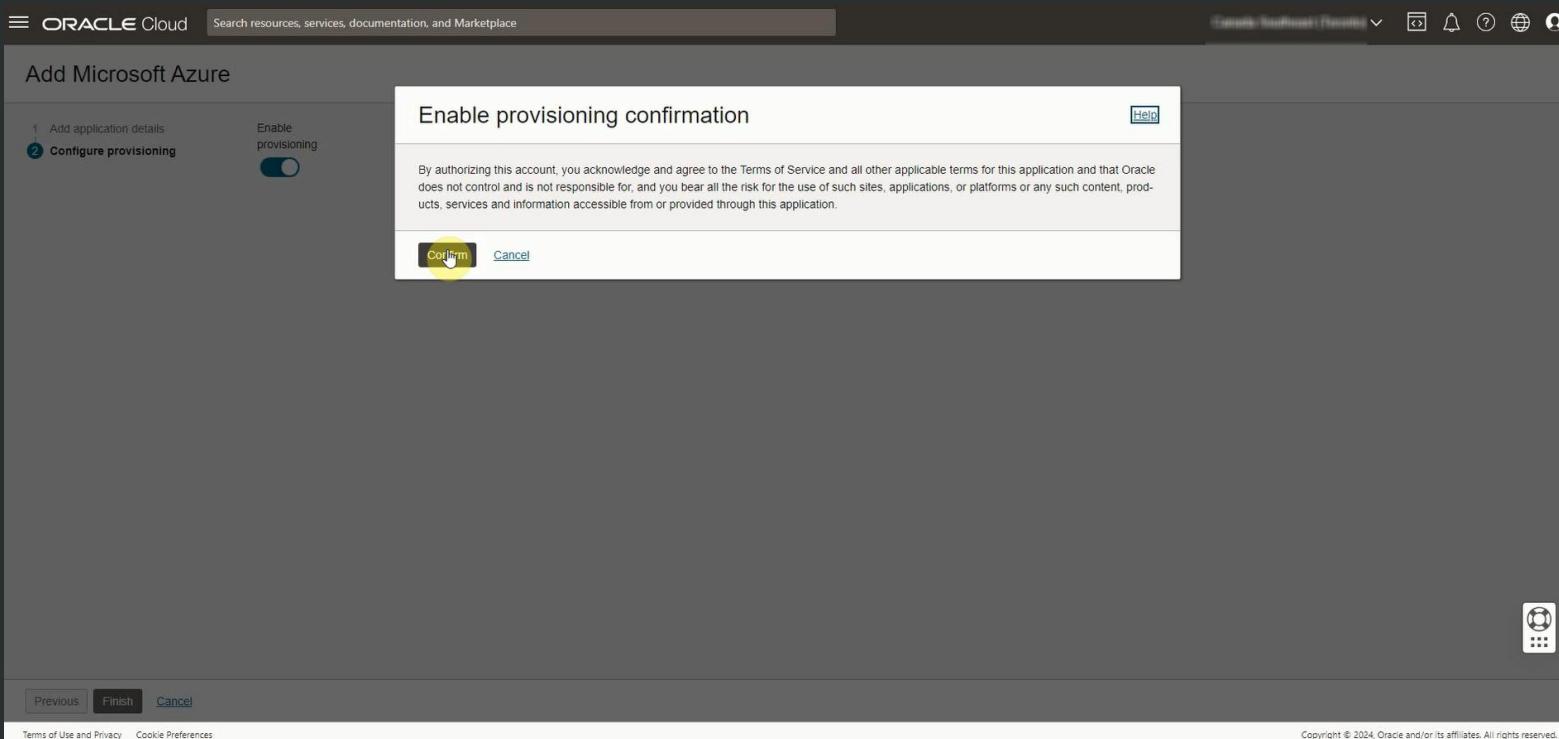
**URLs:**

- Custom sign-in URL (Optional):** An empty input field with a note: "Enter the URL where the user is redirected to sign in. Leave this field blank if you're using a default sign-in page provided by Oracle."
- Custom sign-out URL (Optional):** An empty input field with a note: "Enter the URL where the user is directed after the sign-out process. Leave this field blank if you're using a default sign-in page provided by Oracle."
- Custom error URL (Optional):** An empty input field.

At the bottom left are "Next" and "Cancel" buttons. At the bottom center are "Terms of Use and Privacy" and "Cookie Preferences" links. On the far right, there is a copyright notice: "Copyright © 2024, Oracle and/or its affiliates. All rights reserved."

# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

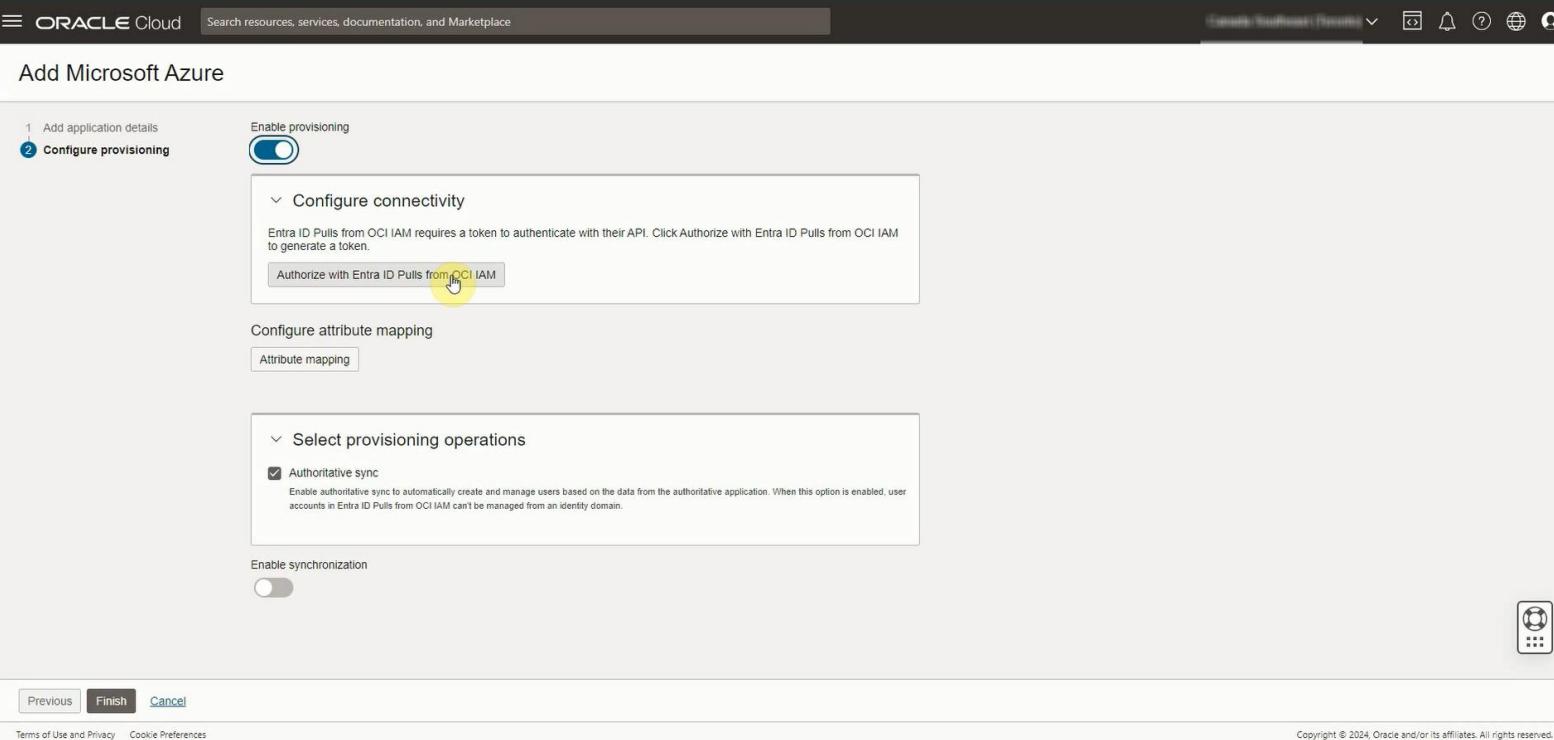
On the *Configure provisioning* page, select *Confirm* to enable provisioning



# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

By selecting *Authorize with Entra ID Pulls from OCI IAM*, administrators will be redirected to Entra ID for the token generation that will ensure the authentication with respective API

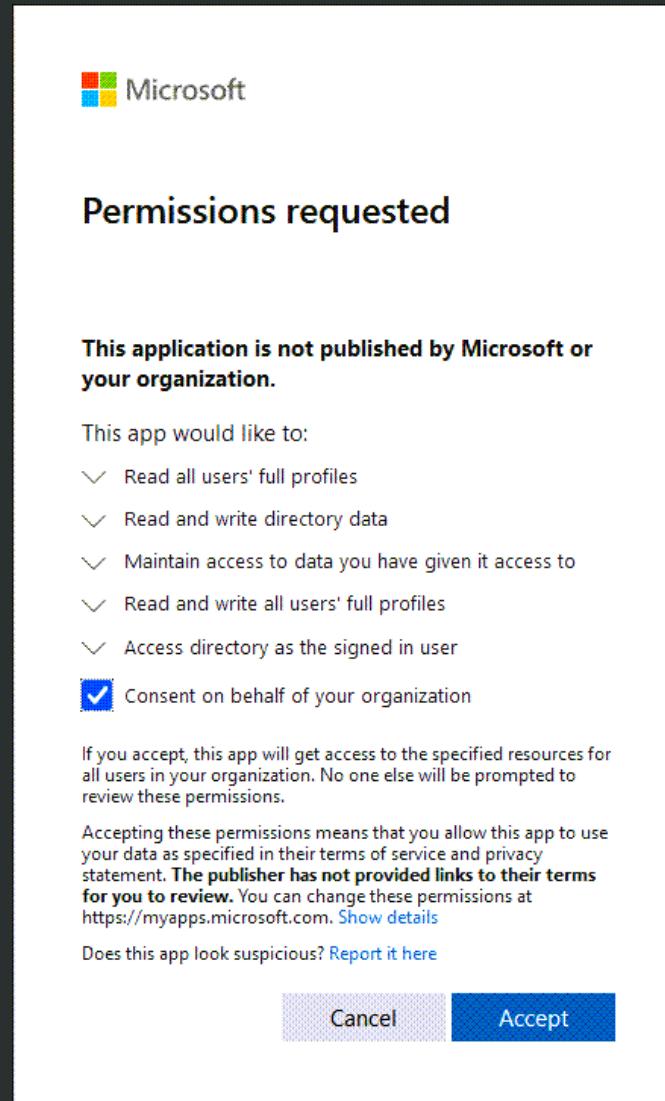
Microsoft will open a new browser window, sign in using Microsoft Entra ID credentials, in the Permissions requested dialog select *Accept*



# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Microsoft will open a new browser window, sign in using Microsoft Entra ID credentials, in the Permissions requested dialog select *Accept*

The Console displays the message Authorization completed successfully

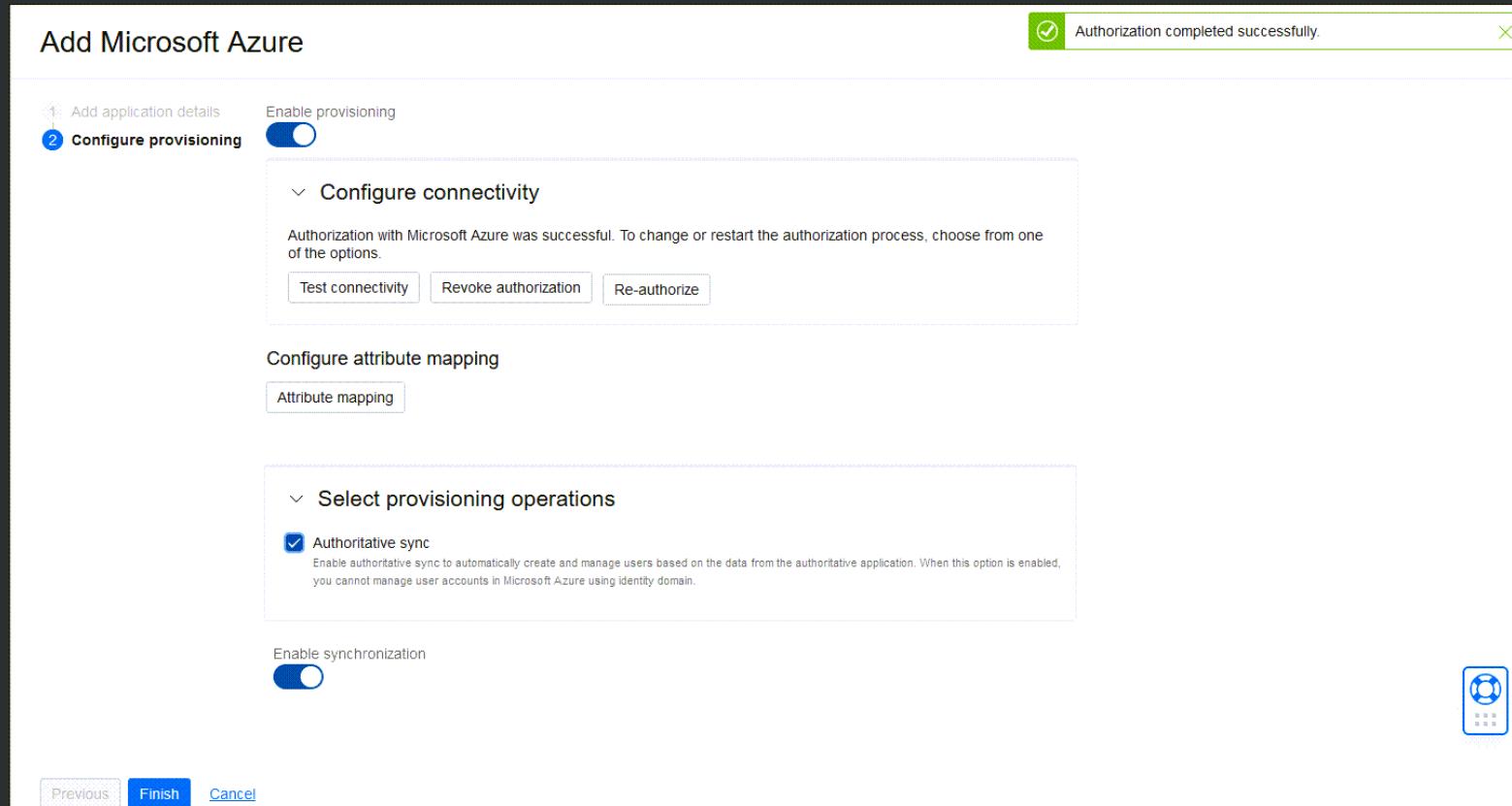


# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Choose *Enable synchronization* so that users are synchronized between OCI IAM and Microsoft Entra ID

Select *Finish*

On the application overview page, select *Activate* and confirm

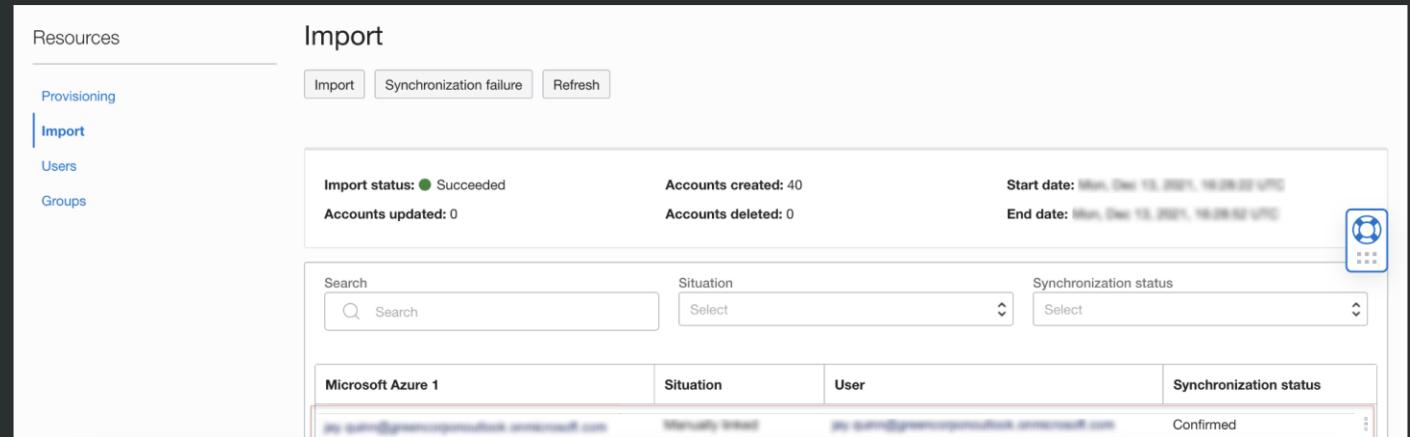
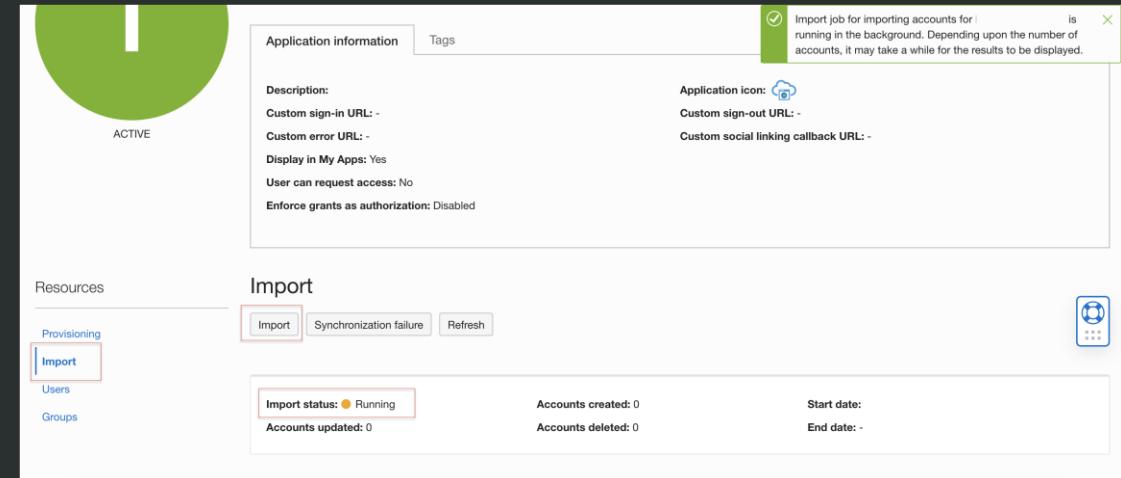


# Pulling user accounts, groups and group membership from Entra ID to OCI IAM

In the Microsoft Entra ID app in OCI IAM, select *Import* under *Resources*

Check the import status. When the status changes to *Succeeded*, a list of users is displayed

The Entra ID application in OCI IAM is created, to use it as an identity store, and users from Entra ID to OCI IAM are imported



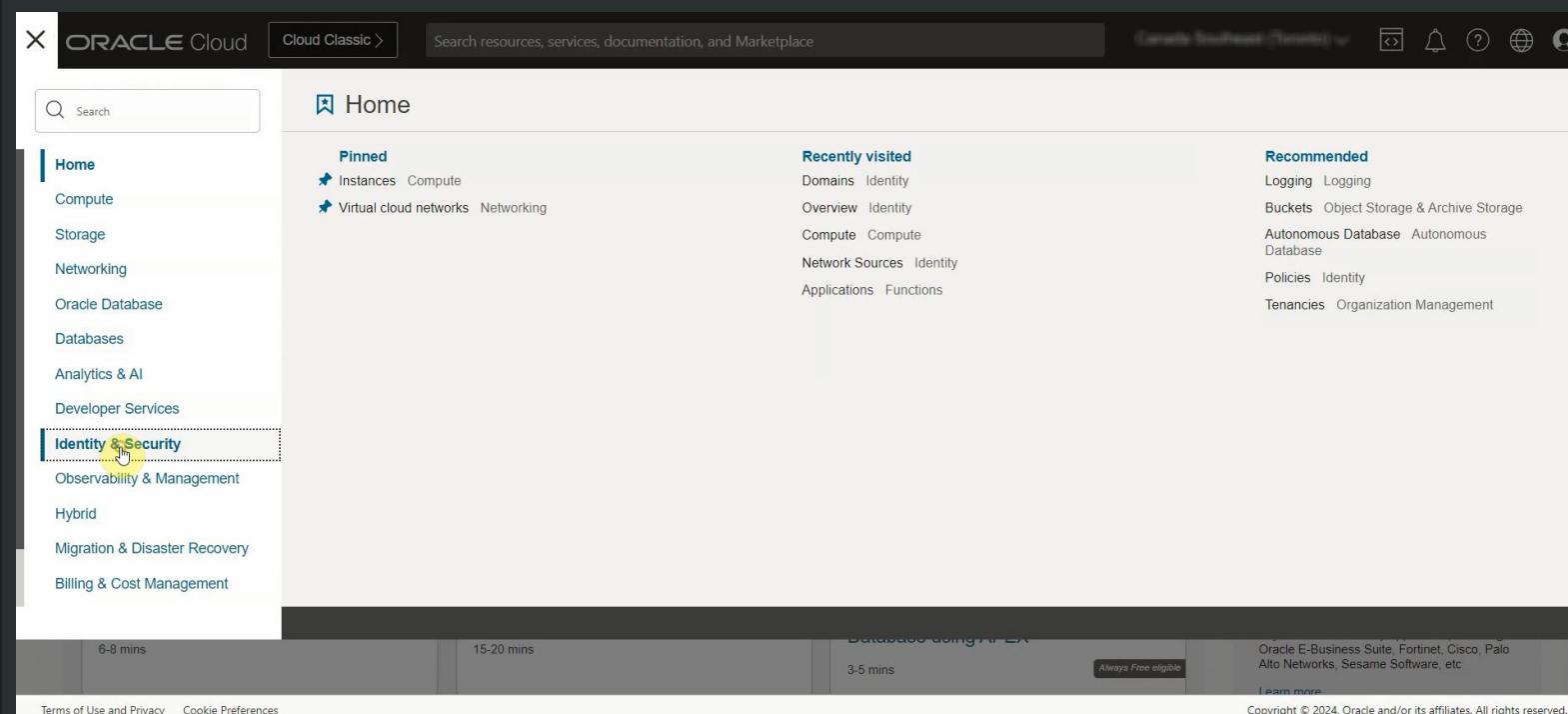
# **Pushing user accounts, groups and license from OCI IAM to Entra ID**

---

# Pushing user accounts, groups and license from OCI IAM to Entra ID

It is also possible to configure OCI IAM as identity store that pushes users, groups, and licenses to Entra ID

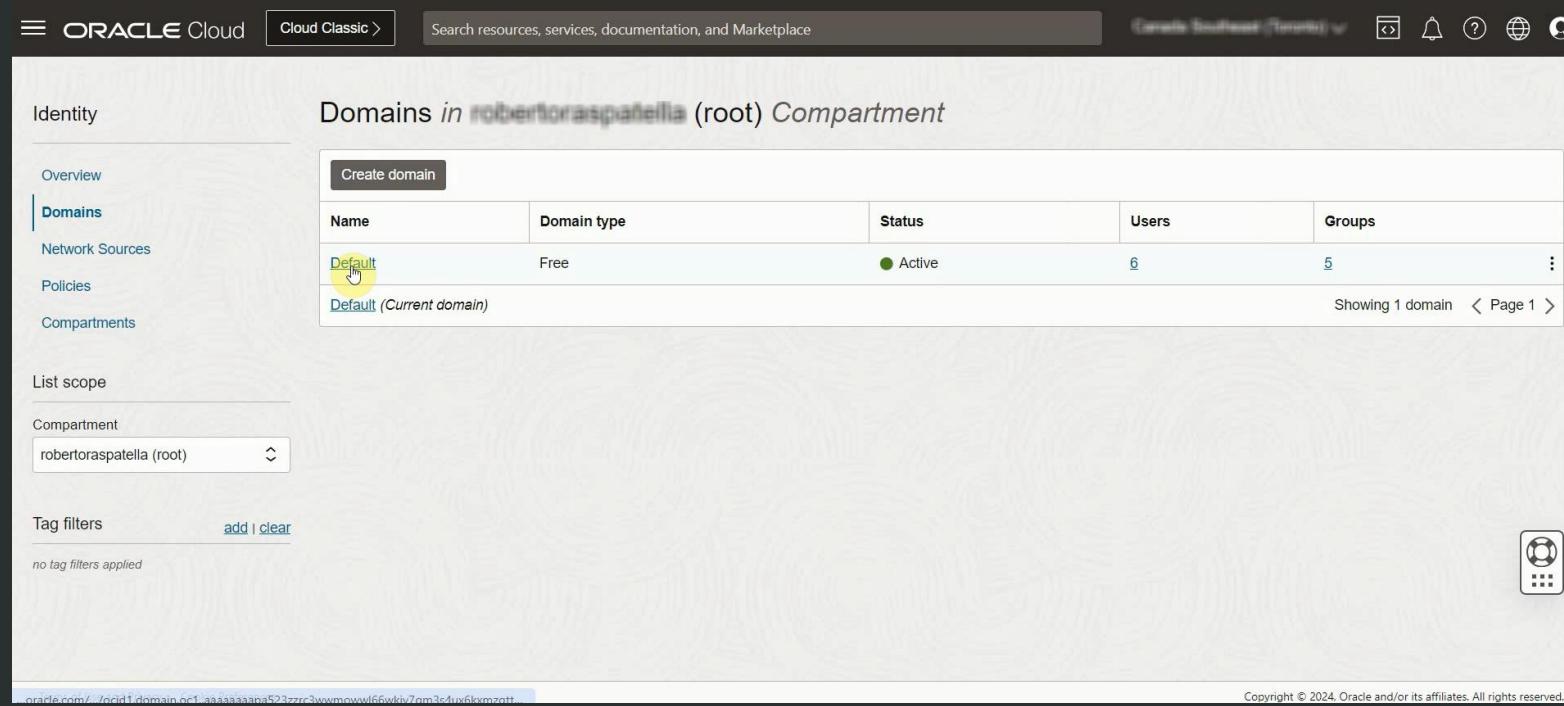
In OCI, select *Identity & Security* from the top left menu.



# Pushing user accounts, groups and license from OCI IAM to Entra ID

In this case, it is needed to configure OCI IAM to manage identities in Entra ID

Then select the domain of the users that is intended to synchronize



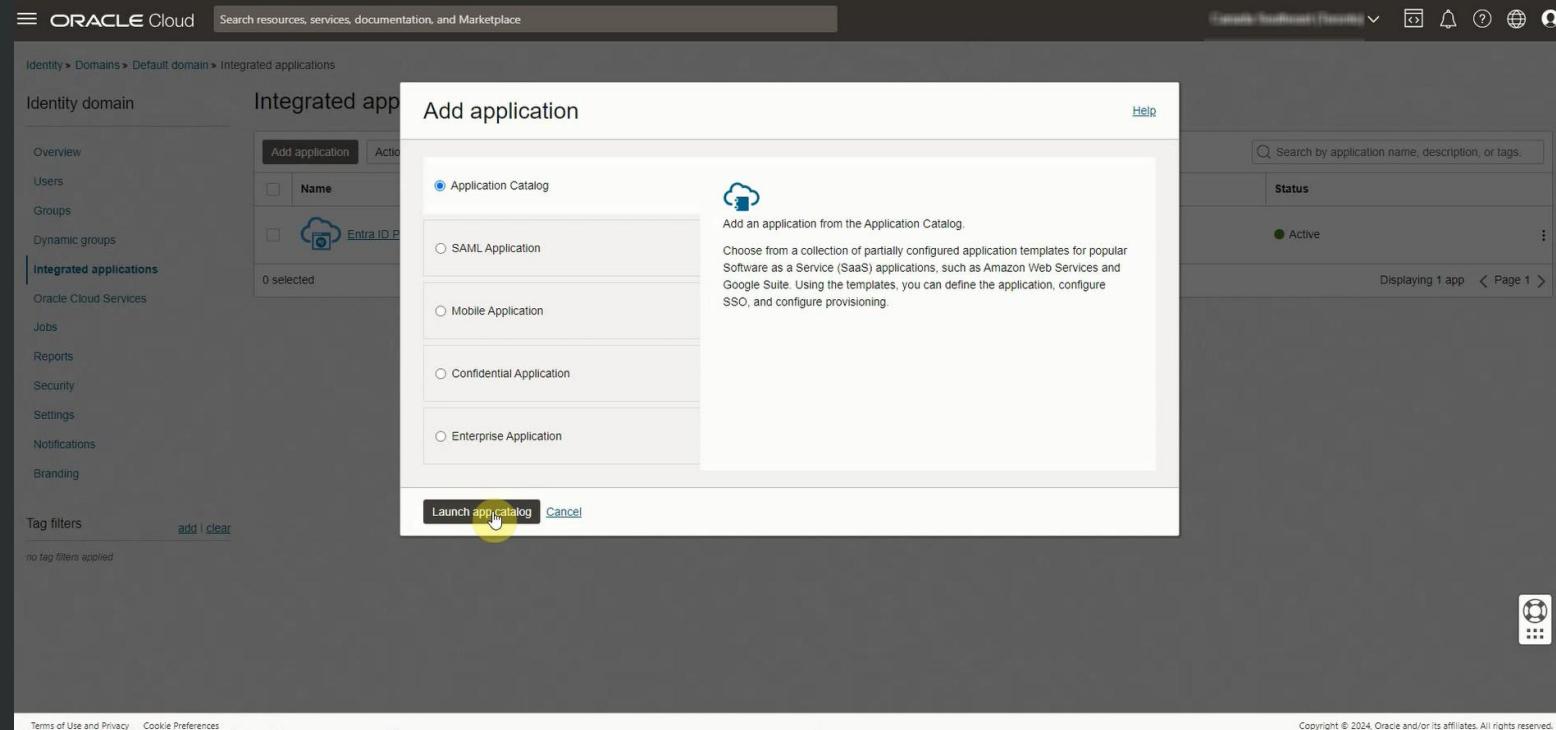
The screenshot shows the Oracle Cloud Identity interface. The left sidebar has 'Identity' selected, with options for Overview, Domains (which is highlighted), Network Sources, Policies, and Compartments. The main area displays a table titled 'Domains in robertoraspatarella (root) Compartment'. The table has columns for Name, Domain type, Status, Users, and Groups. One row is visible, labeled 'Default (Current domain)', which is highlighted with a yellow box and a cursor icon. The status is 'Active', there are 6 users, and 5 groups. At the bottom right of the table, it says 'Showing 1 domain < Page 1 >'. The URL at the bottom of the browser window is oracle.com/.../ocid1.domain.oc1..aaaaaaaapaa52zzrrcwwmnowwlf66wldv7am3c4ux6kvmz0tt.

# Pushing user accounts, groups and license from OCI IAM to Entra ID

A MS Office 365 application in OCI IAM will be created by using the Application Catalog

Under *Integrated application*, select Add application and then select Application Catalog

Select Launch workflow



# Pushing user accounts, groups and license from OCI IAM to Entra ID

Search for “MS Office 365” and select *MS Office 365*

The screenshot shows the Oracle Cloud Application Catalog interface. At the top, there is a navigation bar with the Oracle Cloud logo, a "Cloud Classic" button, a search bar containing "Search resources, services, documentation, and Marketplace", and a location dropdown set to "Canada Southeast (Toronto)". On the far right of the header are icons for notifications, help, and user profile.

The main content area is titled "Application Catalog". A search bar at the top right contains the text "MS Office 365". Below the search bar, a breadcrumb trail shows the path: Identity > Domains > Default domain > Integrated applications > Application Catalog.

A sidebar on the left lists various application categories under "All applications": Analytics, Benefits, CRM, Collaboration, Consumer, Content Management, E-Commerce, ERP, Finance and Accounting, Human Resources, IT Infrastructure, Internal, Learning, Marketing, News, Productivity, and Security. The "All applications" category is currently selected.

The main pane displays a single application entry for "MS Office 365". It features a thumbnail icon of a cloud with a document, the name "MS Office 365", a description "Office 365 Applications using WS-Federation", and a note "Type: Provisioning | SAML". A yellow circle with a cursor icon is overlaid on the "WS-Federation" text. Below the application entry, a message says "Displaying 1 of 1 Apps."

At the bottom of the page, there are links for "Terms of Use and Privacy" and "Cookie Preferences", and a copyright notice "Copyright © 2024, Oracle and/or its affiliates. All rights reserved." There is also a small red square icon in the bottom right corner.

# Pushing user accounts, groups and license from OCI IAM to Entra ID

Enter the name of the application to be used

≡ ORACLE Cloud Cloud Classic > Search resources, services, documentation, and Marketplace Canada Southeast (Toronto) ☰ 🔍 ⓘ ⓘ

## Add MS Office 365

① Add application details  
② Configure single sign-on  
③ Configure provisioning

Name: MS Office 365

Description (Optional): Office 365 Applications using WS-Federation

Application icon (i): 

URLs:

Next Cancel

Terms of Use and Privacy Cookie Preferences Copyright © 2024, Oracle and/or its affiliates. All rights reserved.

# Pushing user accounts, groups and license from OCI IAM to Entra ID

Select *Next* and then *Next* again

The screenshot shows the Oracle Cloud Identity interface for adding an application. The title bar says "Add MS Office 365". The navigation steps are listed as:

- 1 Add application details
- 2 Configure single sign-on
- 3 Configure provisioning

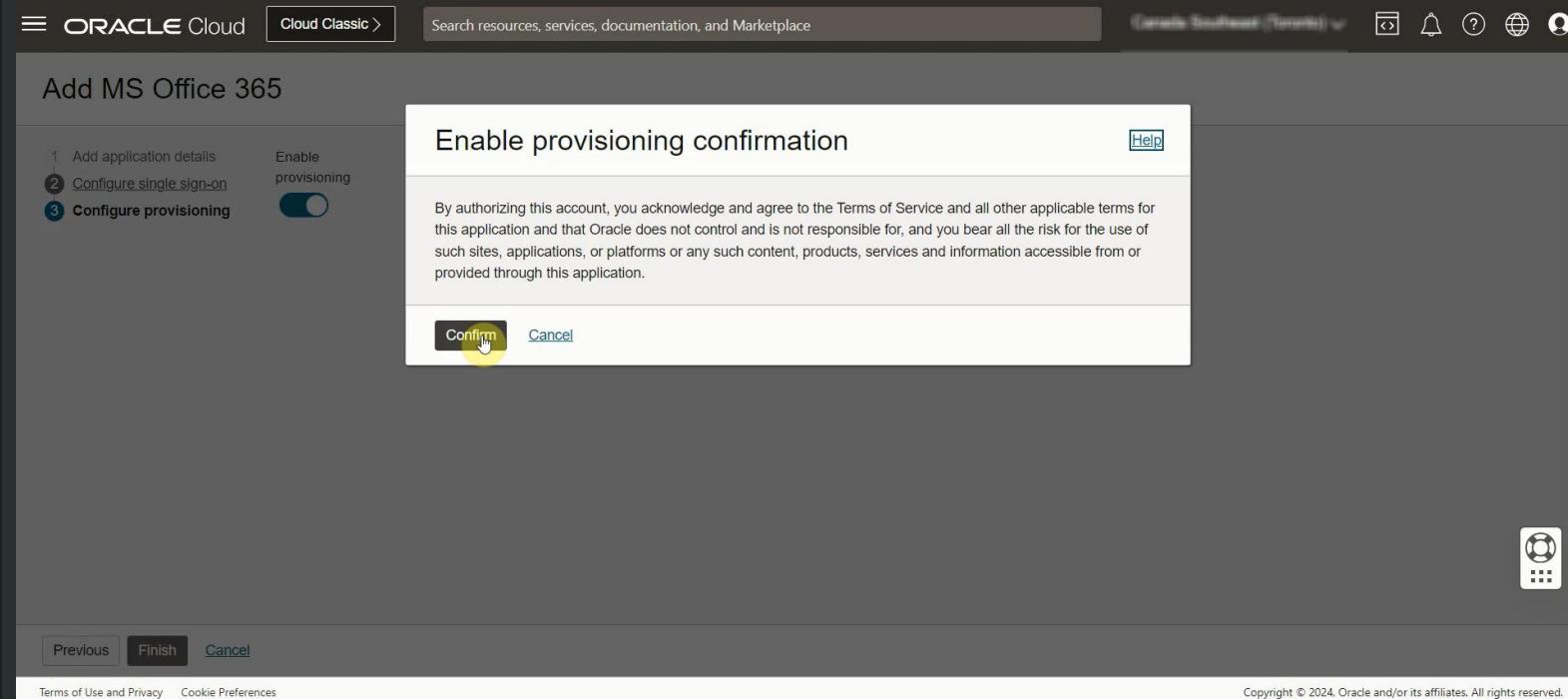
The "Configure single sign-on" step is currently selected. The "General" section contains the following fields:

- Name ID format: Unspecified
- Name ID value: Username

The "Attribute configuration" section is present but mostly empty. At the bottom, there are navigation buttons: "Previous", "Next" (which has a yellow box around it), and "Cancel".

# Pushing user accounts, groups and license from OCI IAM to Entra ID

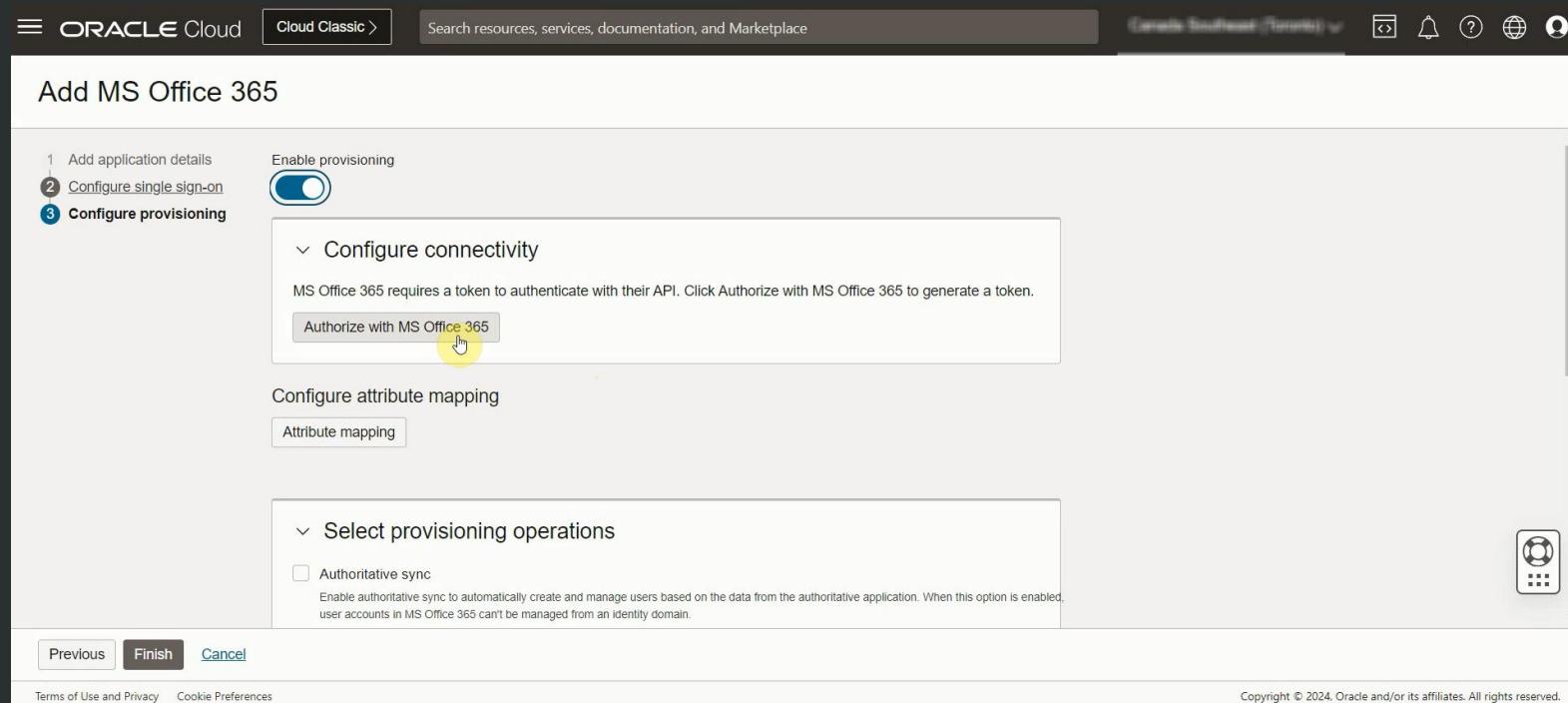
On the *Configure provisioning* page, select *Confirm* to enable provisioning



# Pushing user accounts, groups and license from OCI IAM to Entra ID

Configure connectivity by selecting *Authorize with MS Office 365*

Microsoft will open a new browser window



# Pushing user accounts, groups and license from OCI IAM to Entra ID

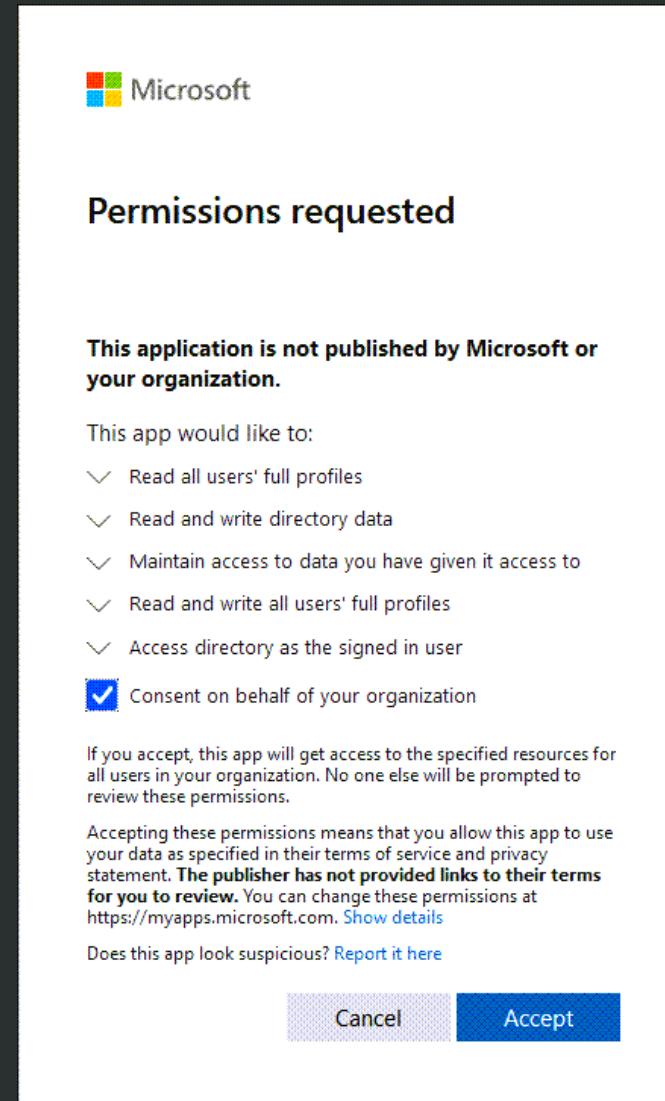
Log in using MS Office 365 credentials

On the *Permissions requested* dialog,  
Select *Consent on behalf of your organization*, and select *Accept*

A message pops up to say that the connection has been successful. Select *Finish*

Back to the application overview page, select *Activate*

The MS Office application is now active



# Pushing user accounts, groups and license from OCI IAM to Entra ID

In the MS Office 365 application, select *Users* on the left under *Resources*, then select *Assign users*

Search for the user to be assigned, then select the *Actions Menu* for that user and select *Assign*. Select *Next*

On the *Add Details page*, scroll down, and under *Licenses*, select *Add*

Assign the licences to the user to be provisioned with on MS Office 365

On the *Add Details page*, scroll down, and under *Roles*, select *Add* and assign the roles to the user to be provisioned with.

Under *Groups*, select *Add* and assign the groups of the user to be provisioned with. Select *Assign User*

The image shows two screenshots of the Microsoft Entra ID interface. The top screenshot is titled "Assign user to MS Office 365". It has a sidebar with steps: "1 Select user" (highlighted) and "2 Add details". Below is a search bar and a table with columns "First name", "Last name", and "Email". Several user entries are listed. At the bottom are "Next" and "Cancel" buttons. The bottom screenshot is titled "Users". It has tabs "Assign users" (highlighted) and "Revoke access". A search bar is at the top right. A table lists users with columns: "Username", "Display name", "Title", "Email", "Mobile phone number", and "Status". One user entry is highlighted with a red border. At the bottom are buttons for "0 Selected", "Showing 1 user", and "Page 1".

ORACLE