ORACLE

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

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

Global Administrator, Cloud Application Administrator, Application Administrator

Secret token generated from

client ID

client secret

OCI Domain URL

https://<domainURL>/admin/v1

Sign-On URL

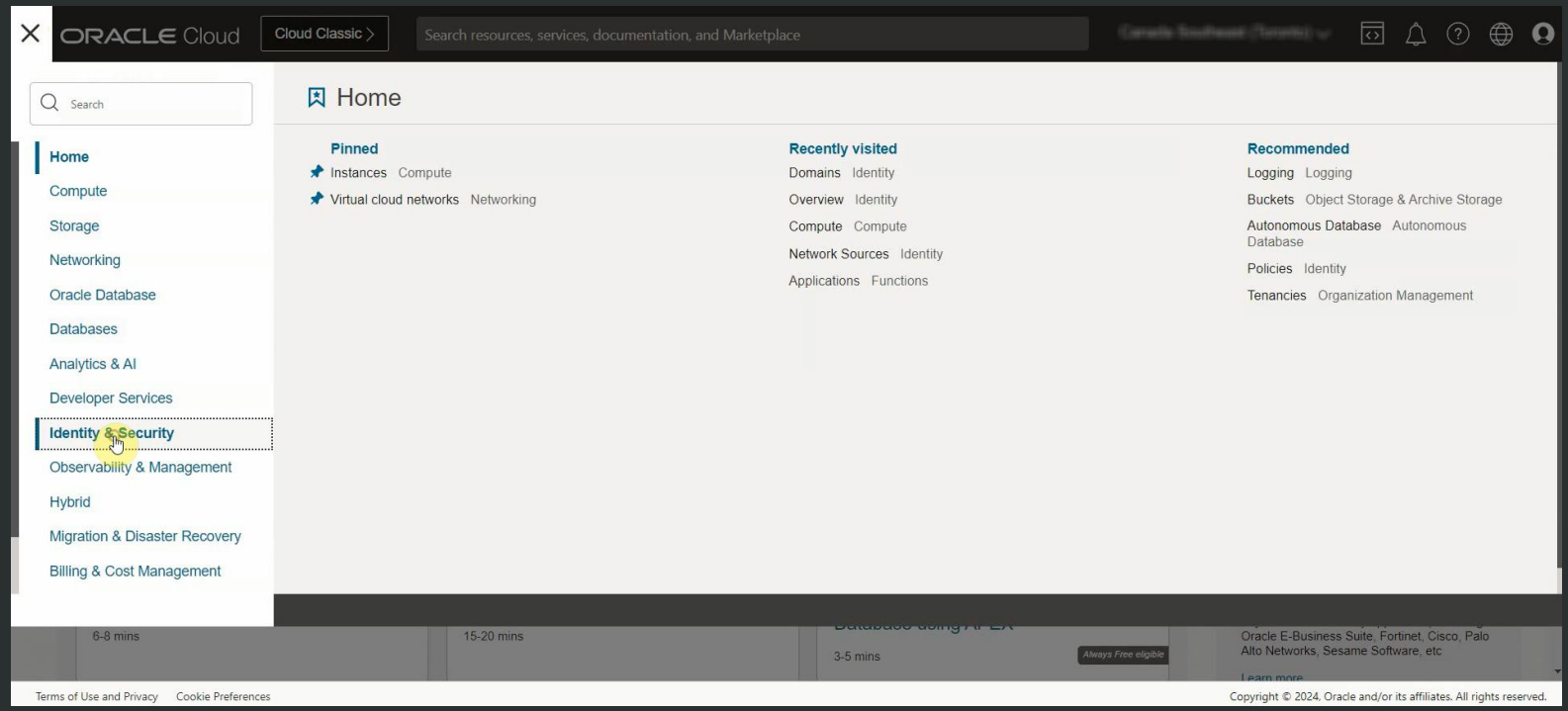
https://console.[REGION].oraclecloud.com/

Pushing user accounts from Entra ID to OCI IAM

Pushing user accounts from Entra ID to OCI IAM

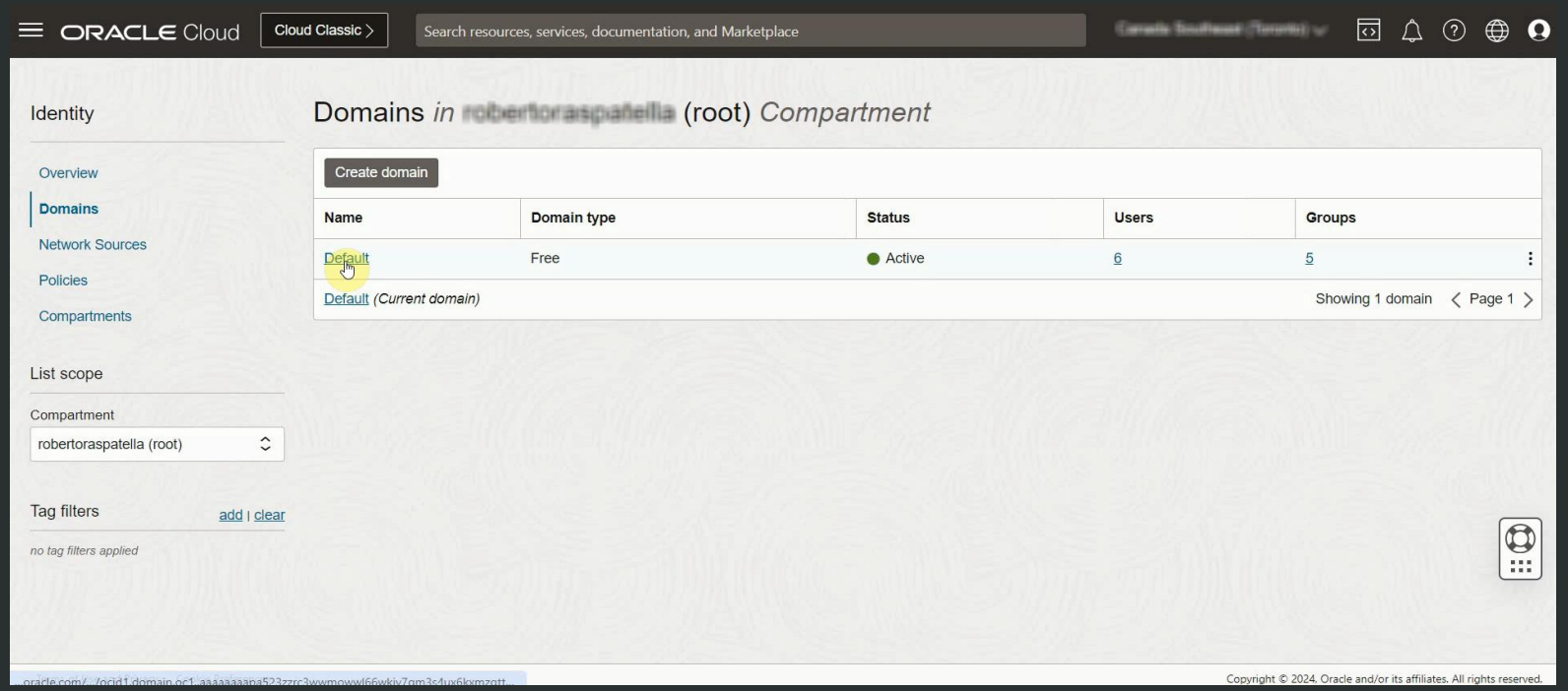
At first, it is needed to configure Entra ID to act as the identity manager so that user accounts are synchronized from Entra ID to OCI IAM.

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

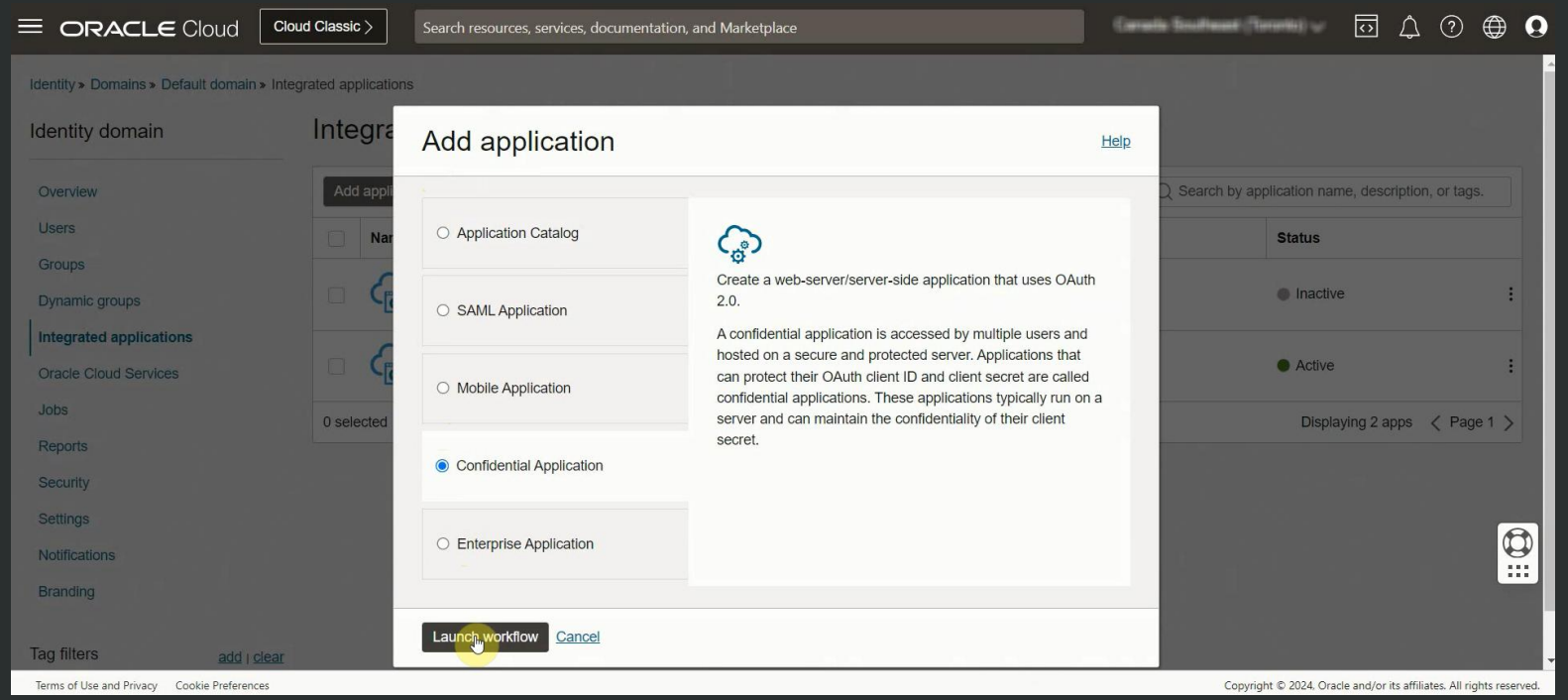


Pushing user accounts from Entra ID to OCI IAM

In the identity domain, select *Applications*

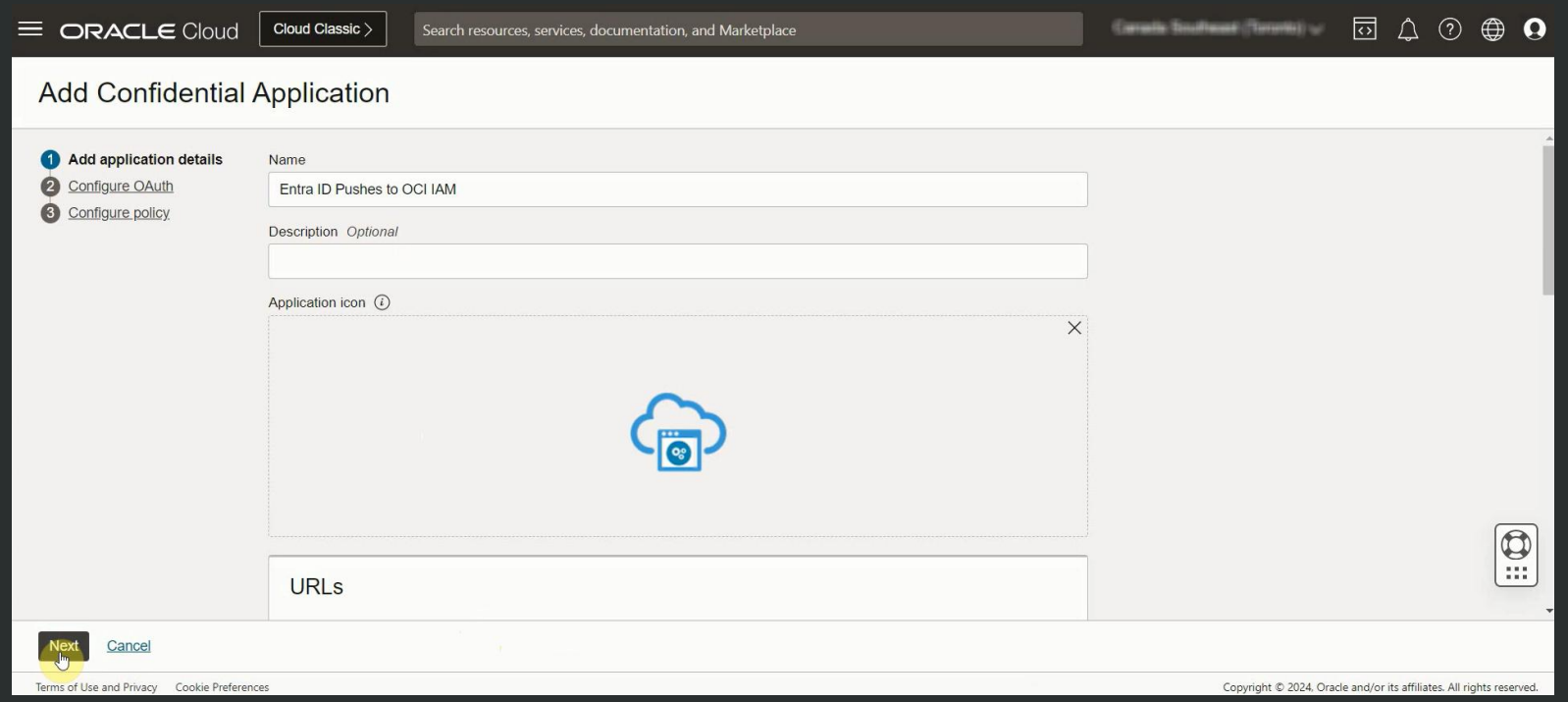
Select *Add Application* and choose *Confidential Application*

Then select *Launch workflow*



Pushing user accounts from Entra ID to OCI IAM

Enter a name for the application and select *Next*

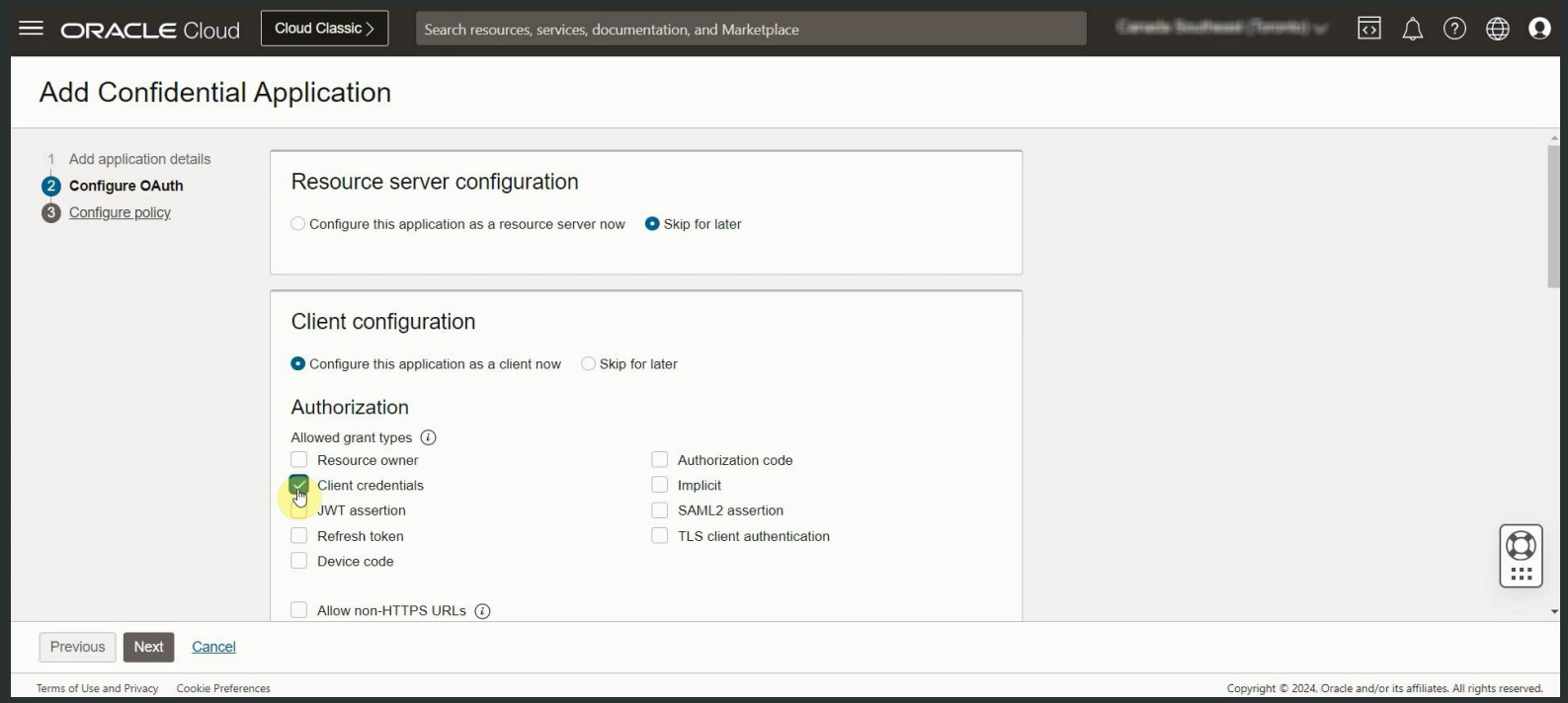


Pushing user accounts from Entra ID to OCI IAM

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

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

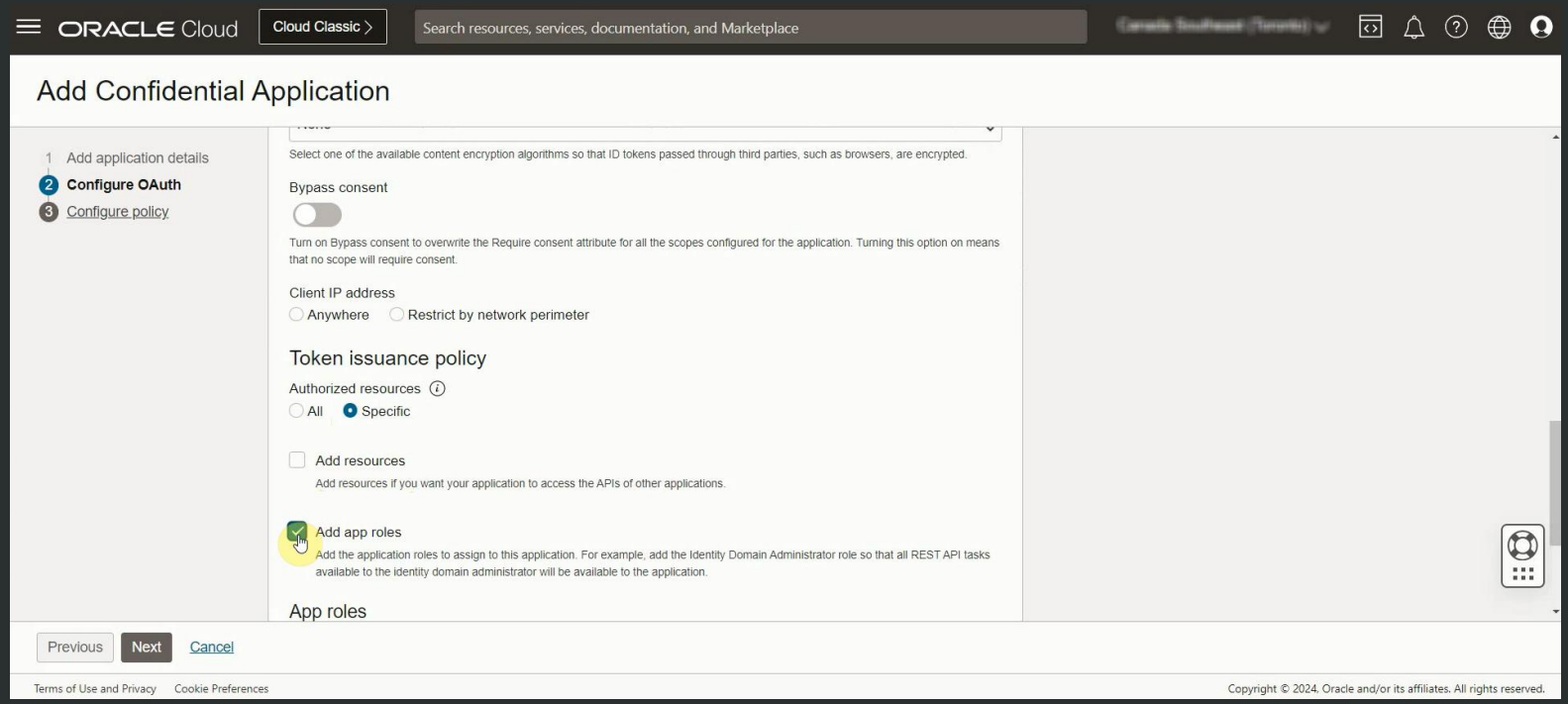
Scroll Down the page.



Pushing user accounts from Entra ID to OCI IAM

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

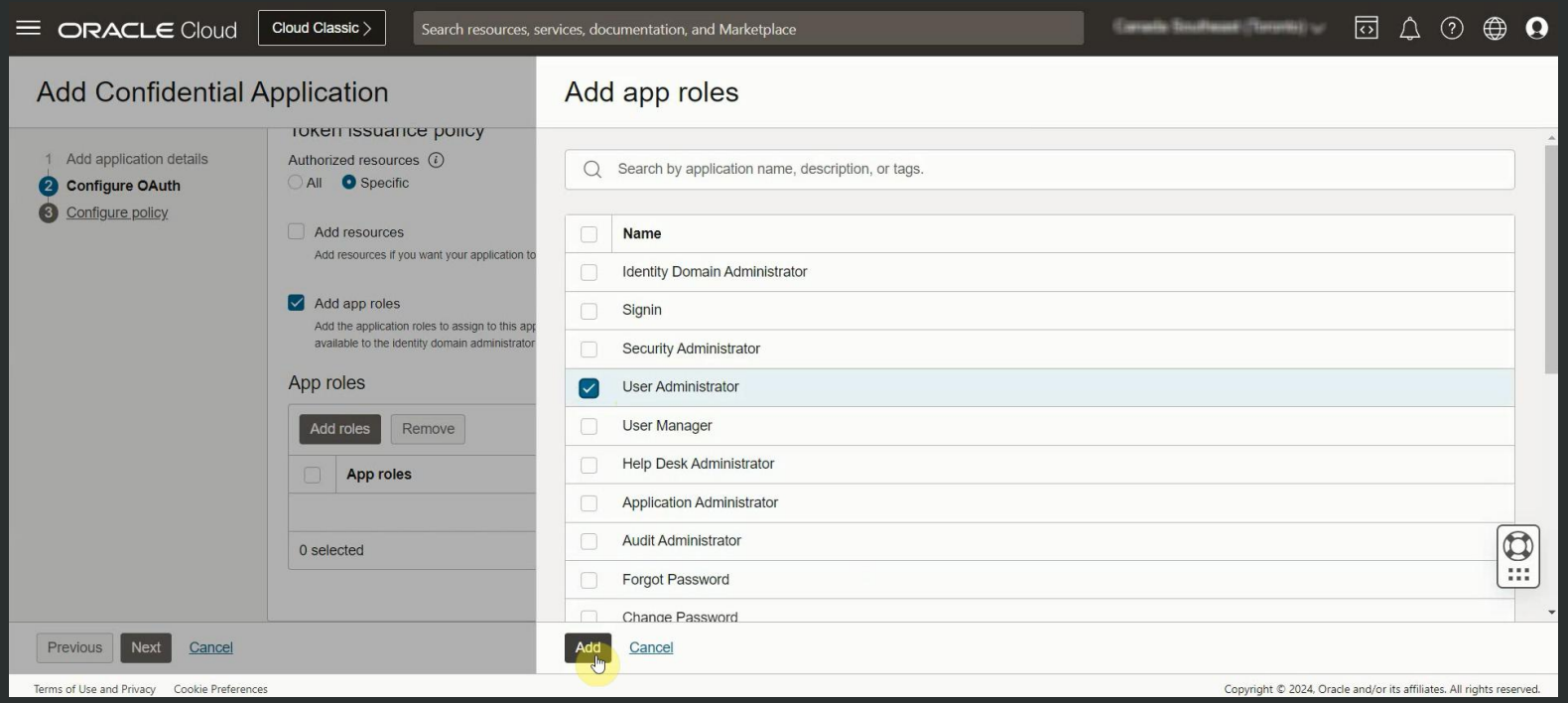
Select then *Add app roles*



Pushing user accounts from Entra ID to OCI IAM

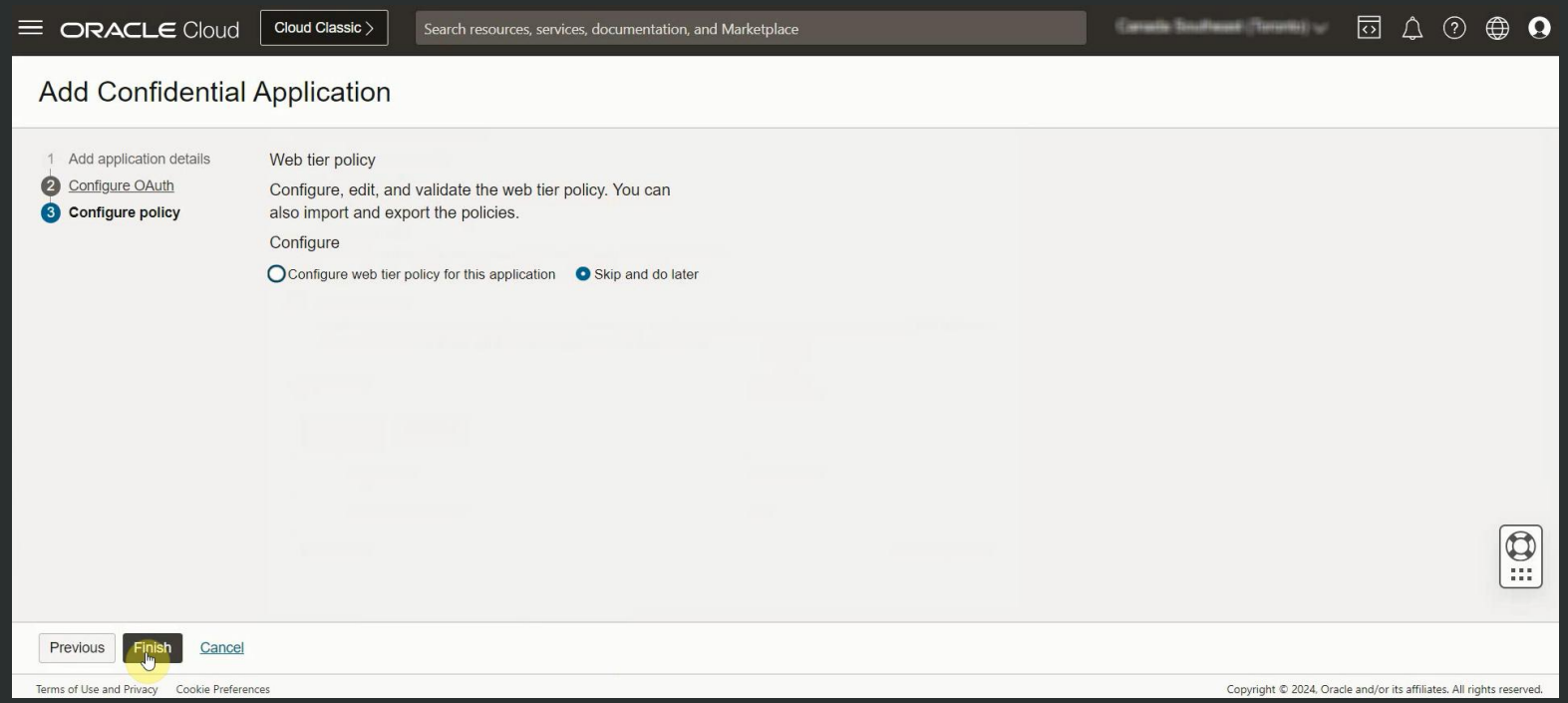
In the *App Roles* section, select *Add roles*, and in the *Add app roles* page select *User Administrator,* then select *Add*

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



Pushing user accounts from Entra ID to OCI IAM

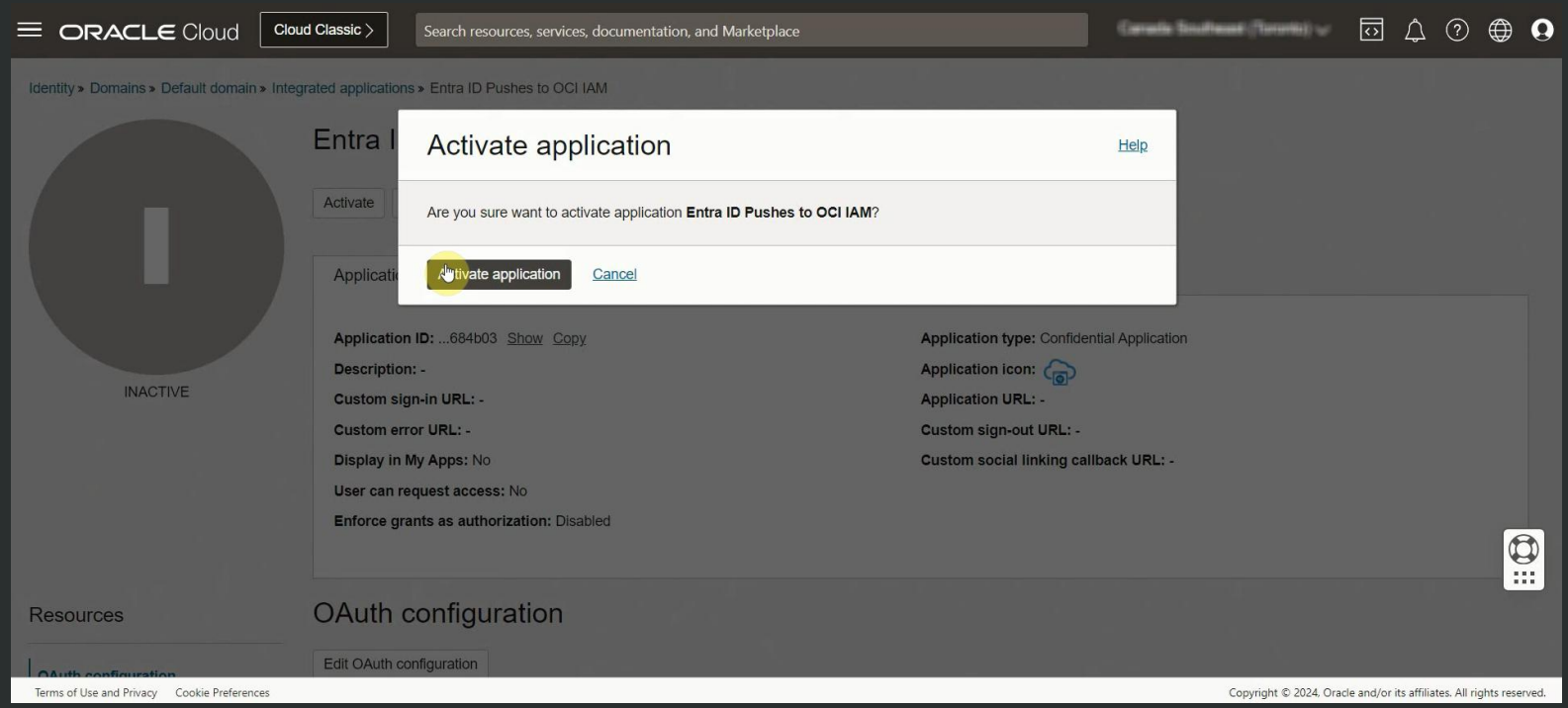
Select *Next* and then select *Finish*



Pushing user accounts from Entra ID to OCI IAM

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

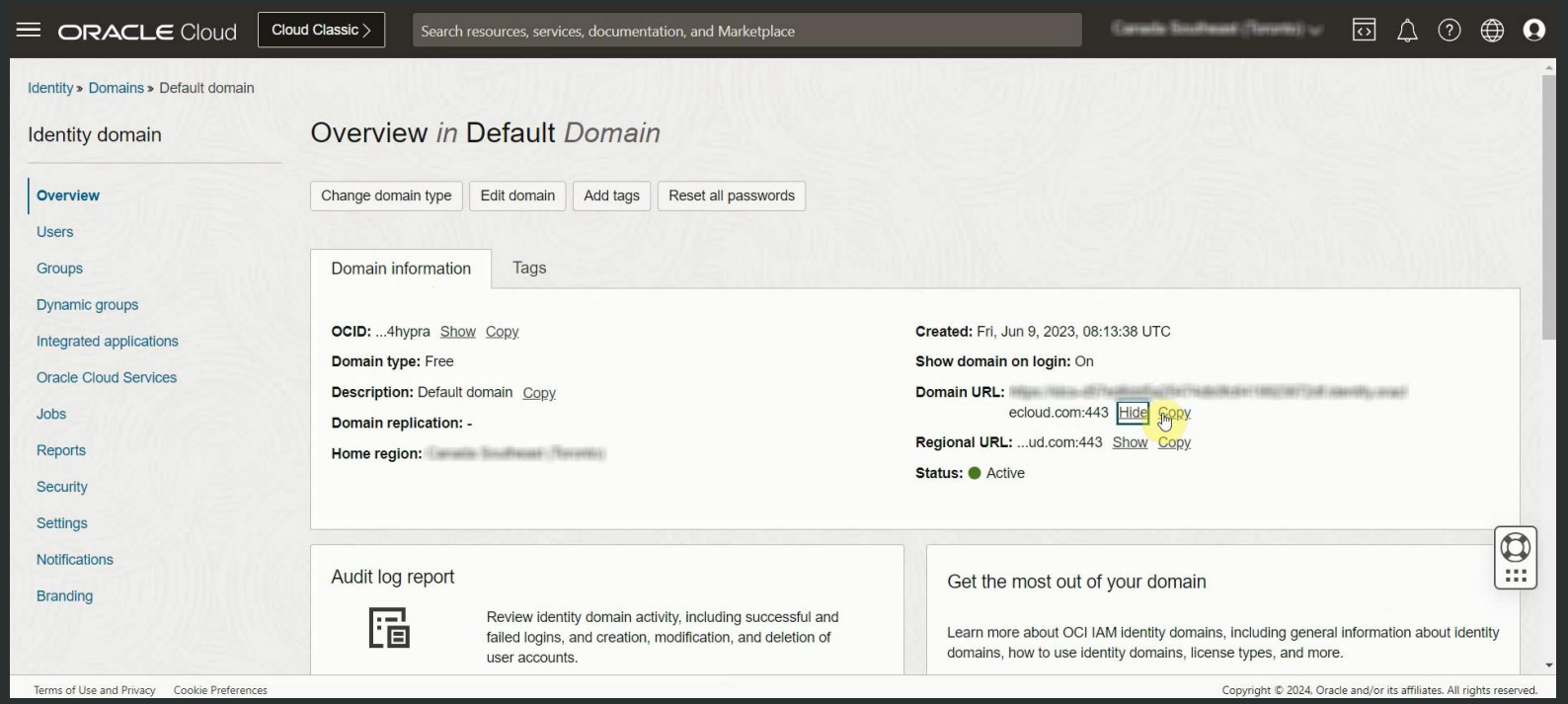
The confidential application is now activated.



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



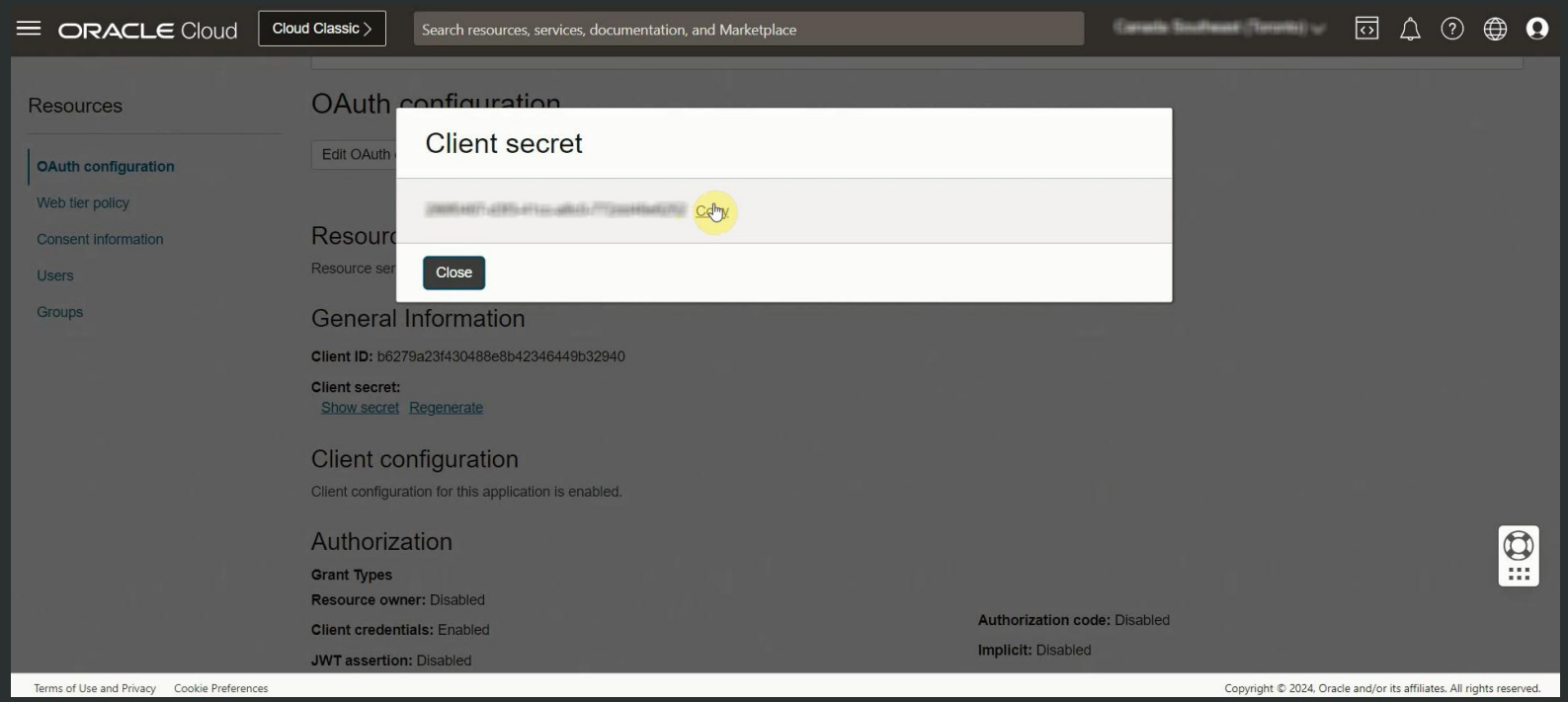
Pushing user accounts from Entra ID to OCI IAM

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

In Linux, use

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

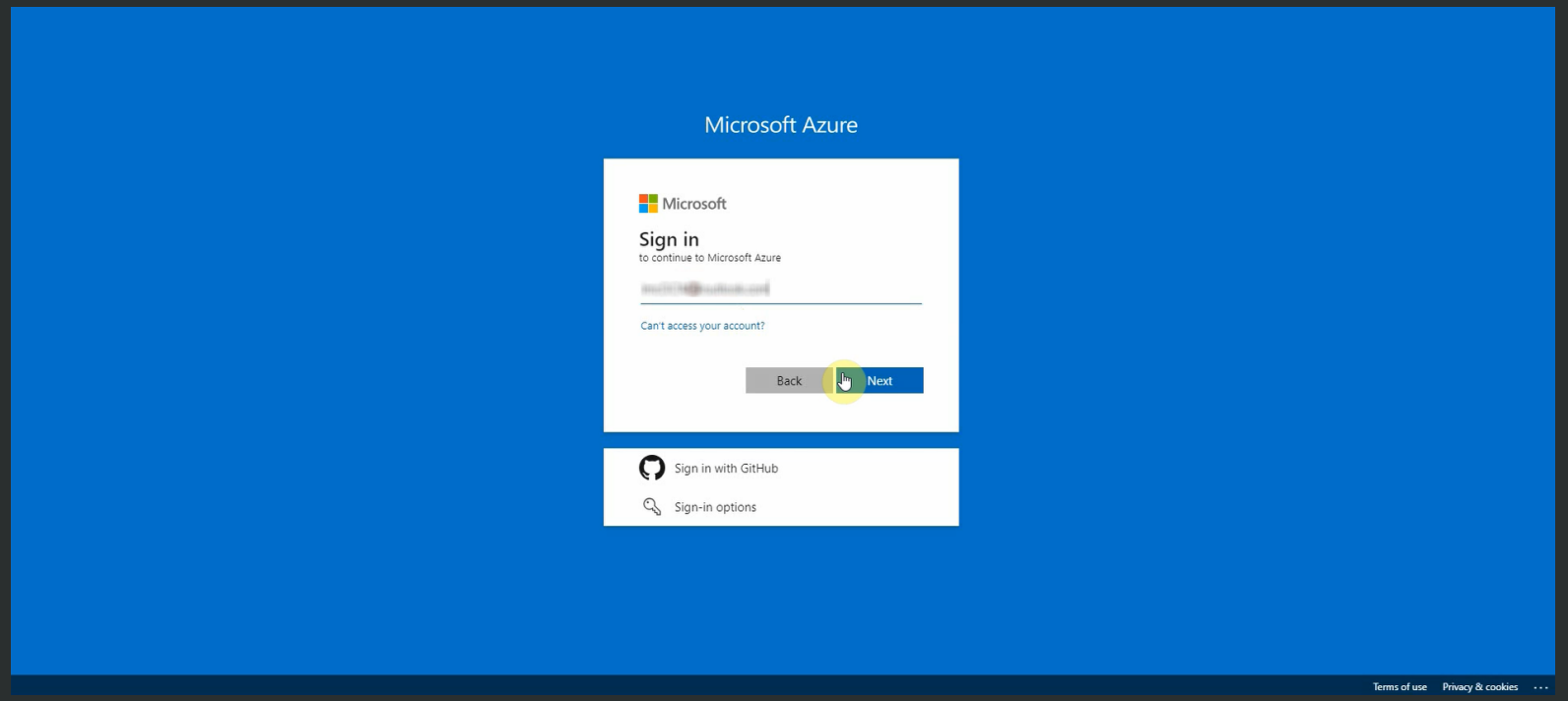
In MacOS, use

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

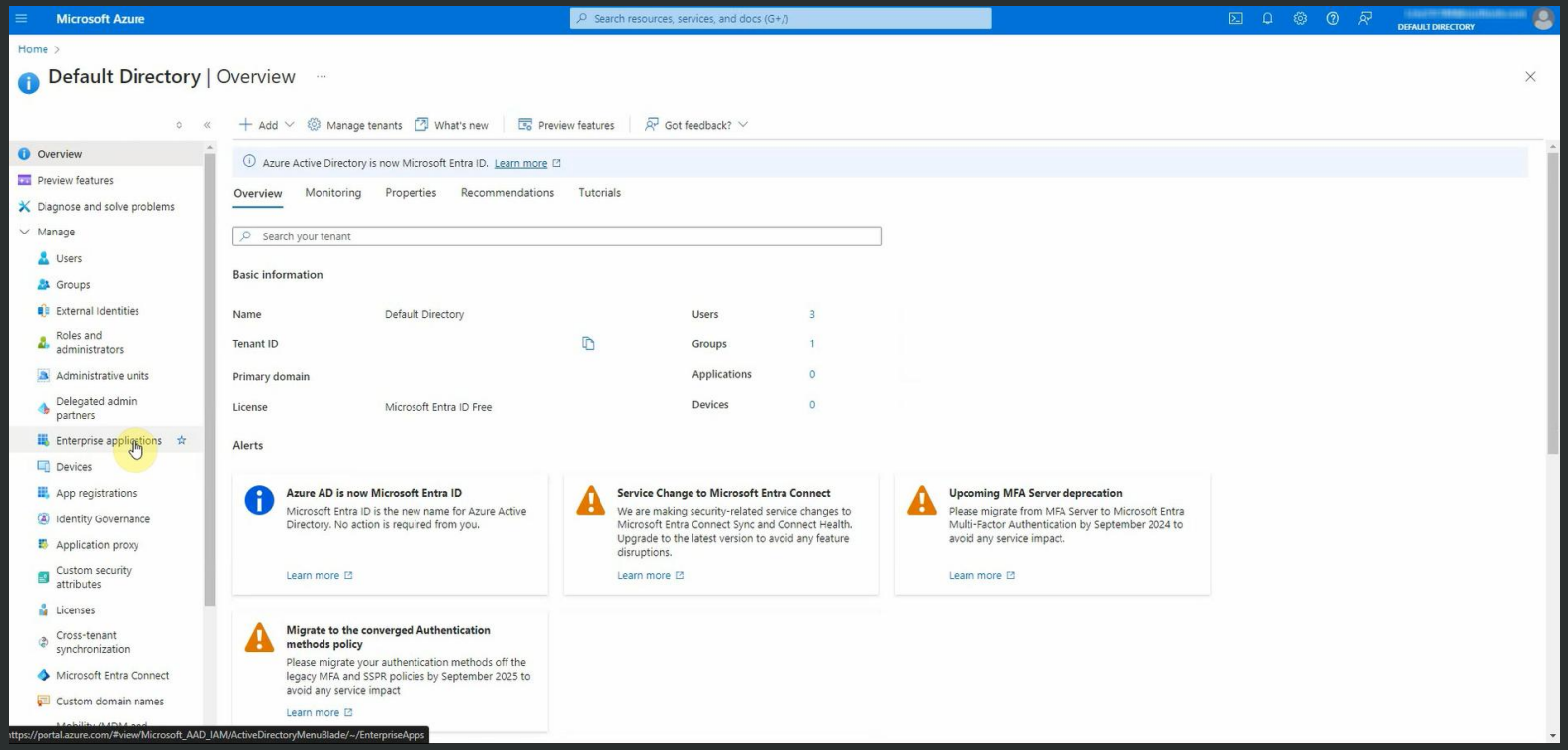
In the browser, sign in to Microsoft Entra ID using username and password on the URL: https://portal.azure.com



Pushing user accounts from Entra ID to OCI IAM

Select *Identity* then *Applications*

Select *Enterprise applications*

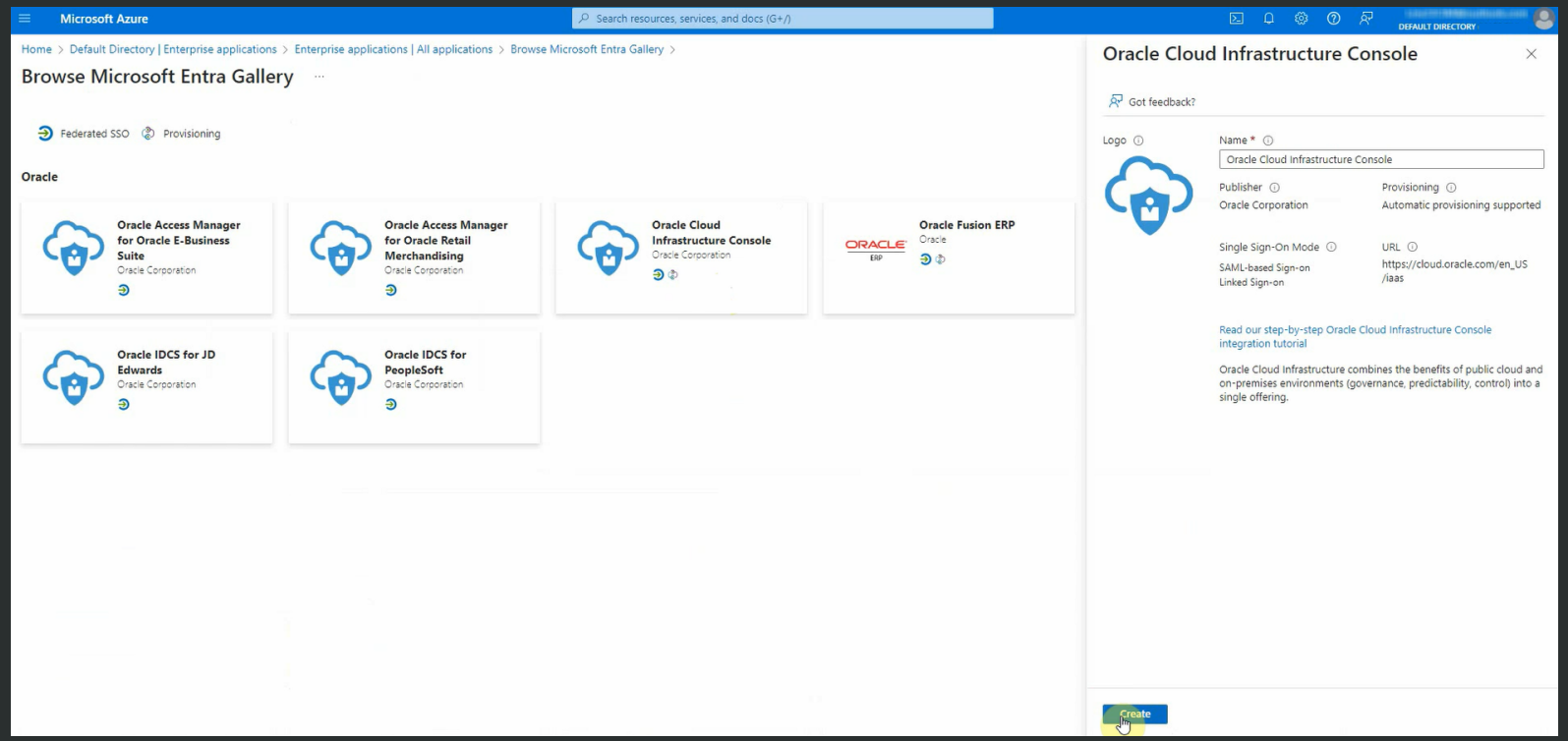


Pushing user accounts from Entra ID to OCI IAM

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

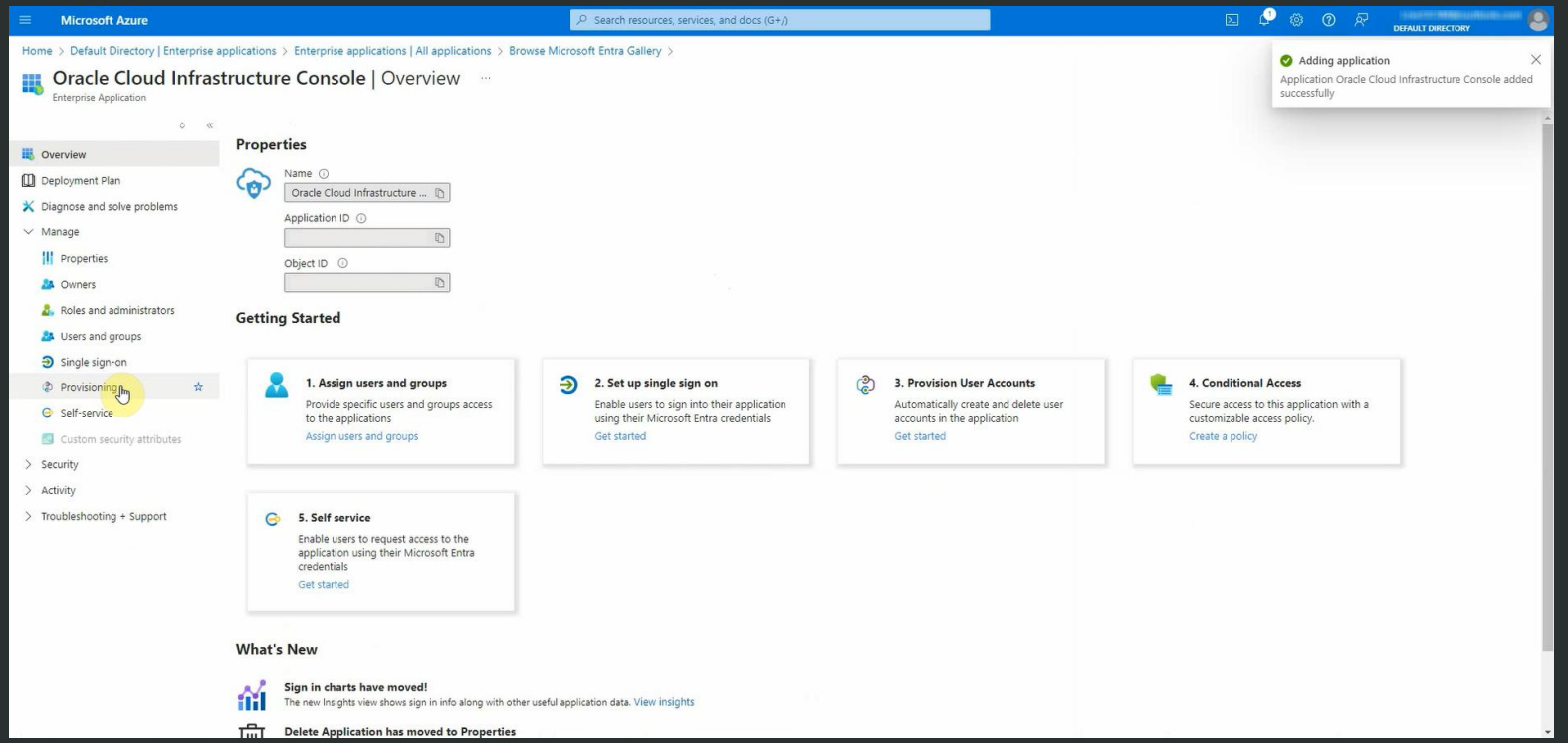
Choose Oracle Cloud Infrastructure Console and enter a name or accept the default one of *Oracle Cloud Infrastructure Console*

Select *Create*



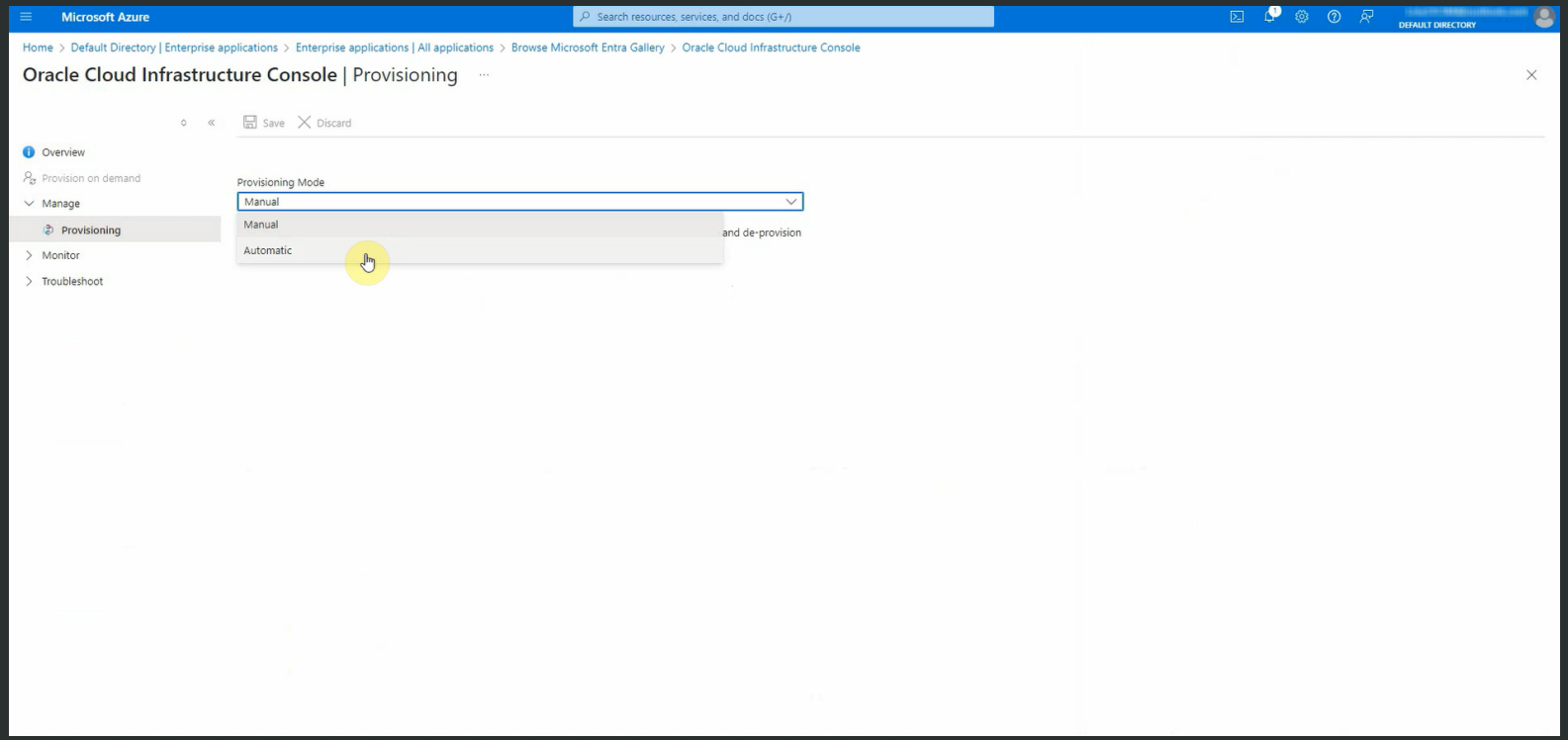
Pushing user accounts from Entra ID to OCI IAM

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



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

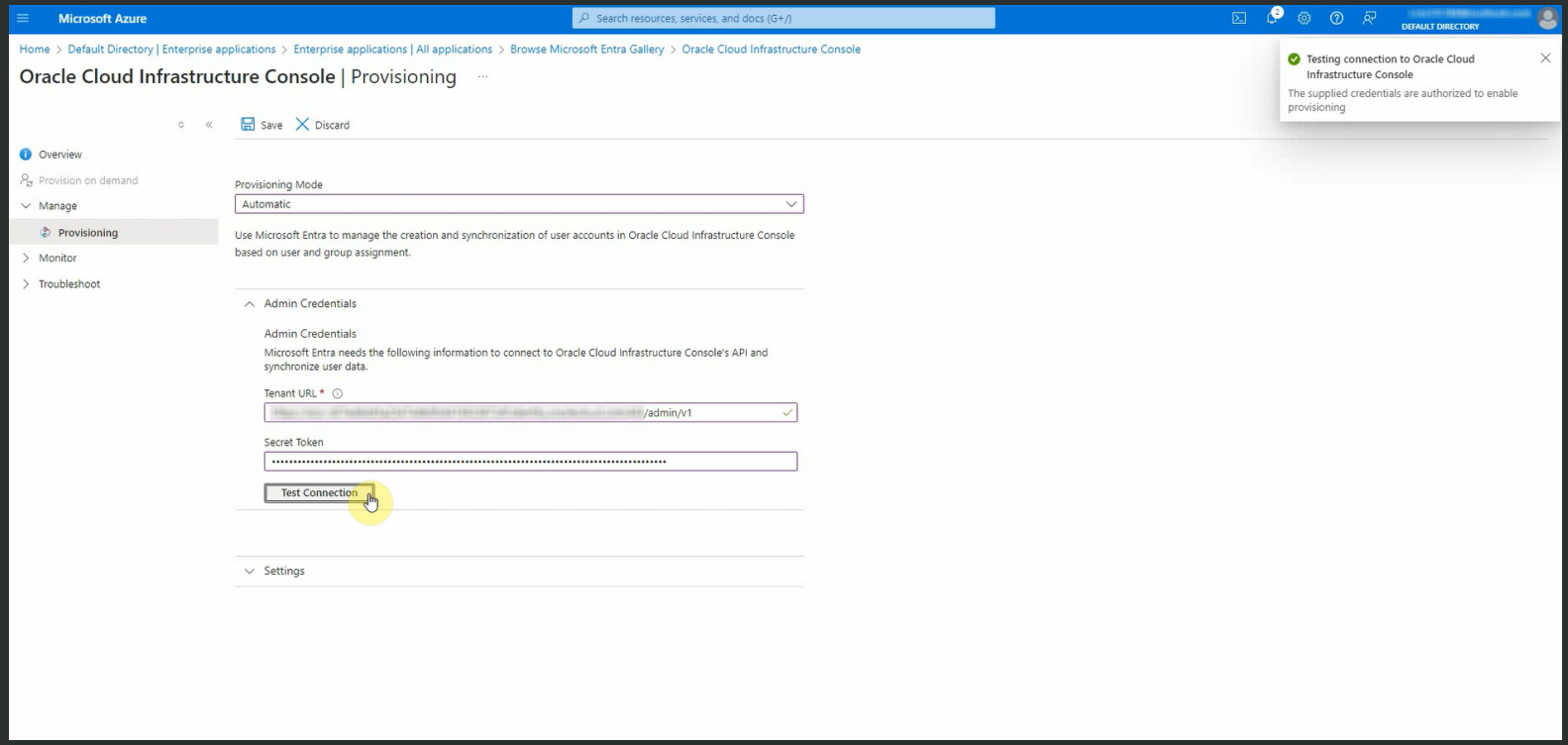
https://<domainURL>/admin/v1

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

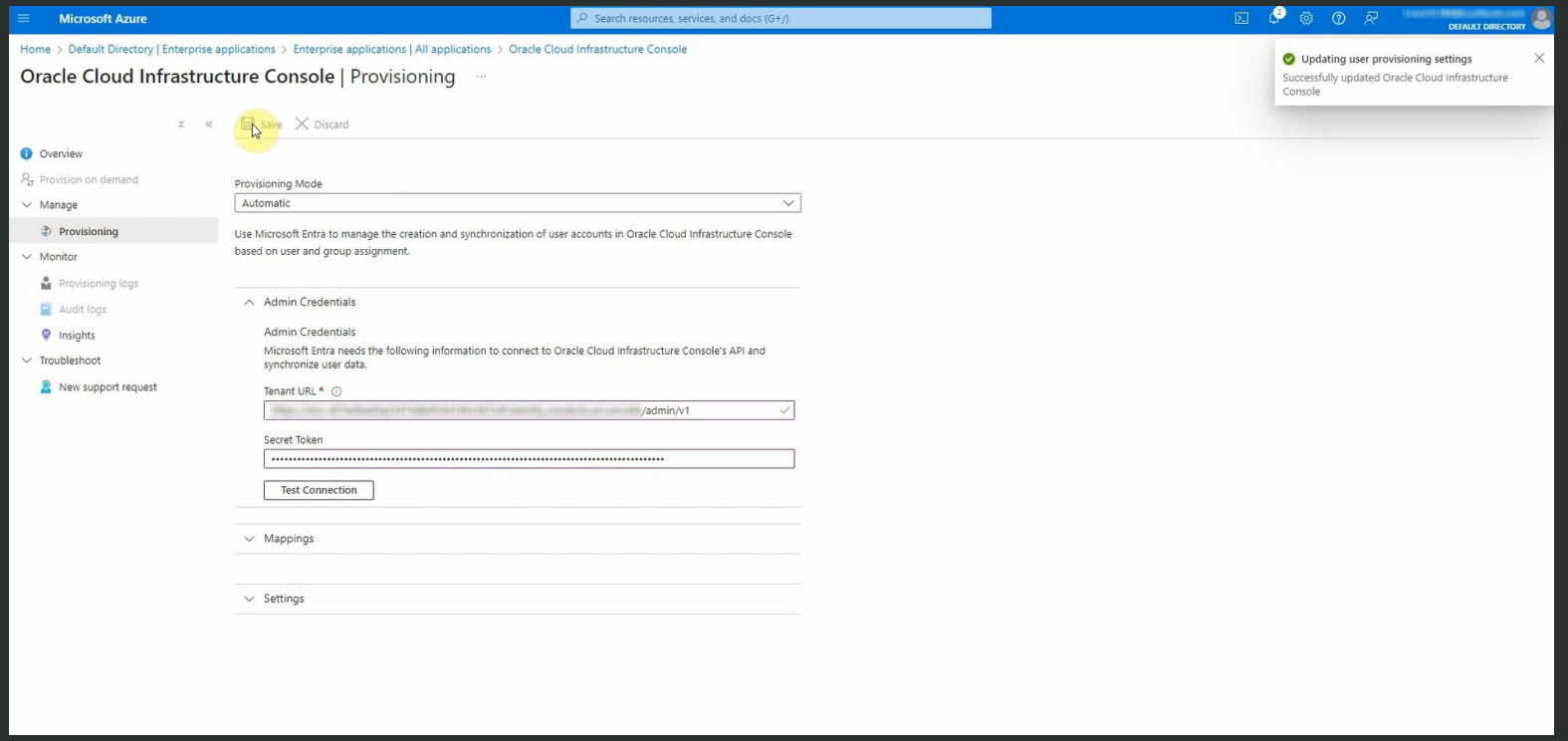


Pushing user accounts from Entra ID to OCI IAM

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

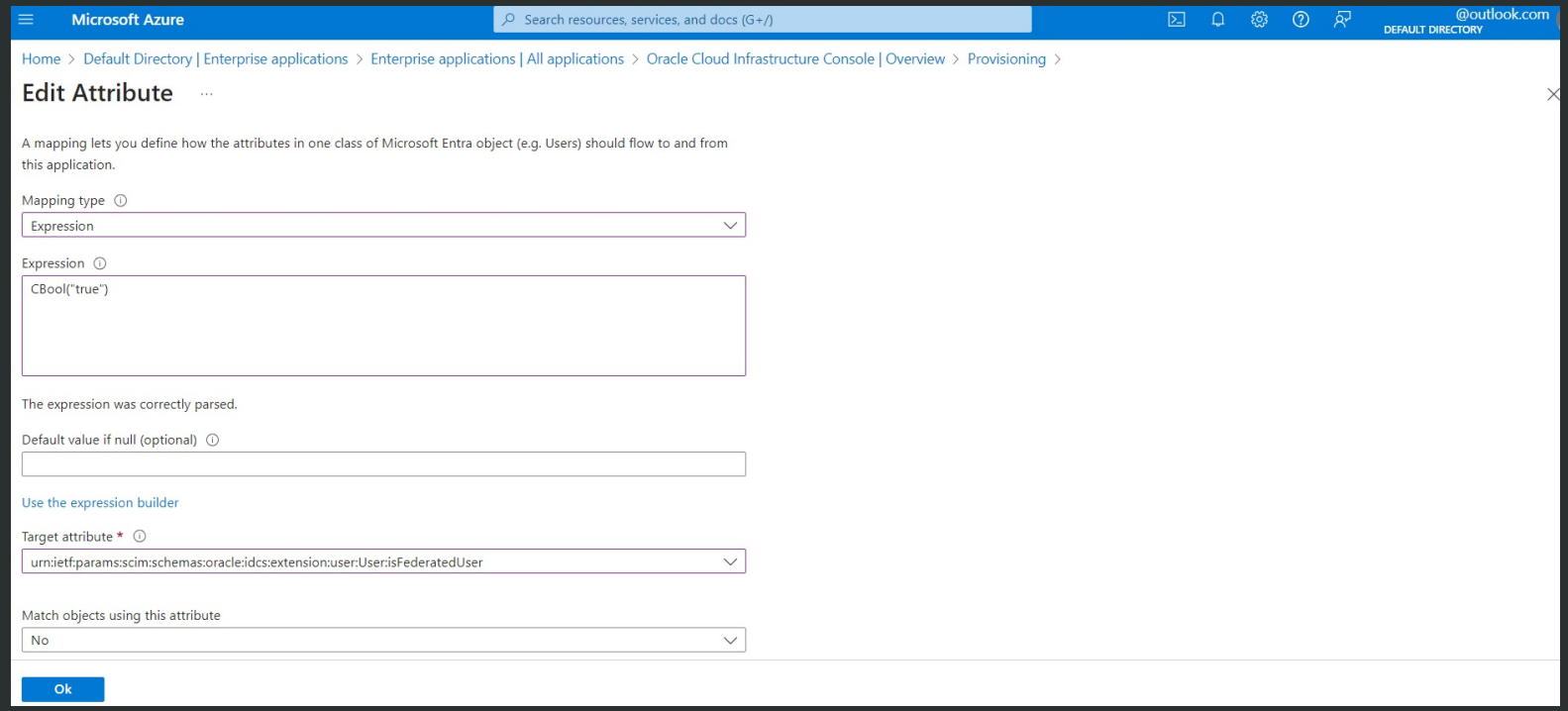
At this point, users don't have credentials to sign in directly to OCI. By setting the federated attribute to *TRUE*, they'll be able to use their federated accounts to sign in to OCI.

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*

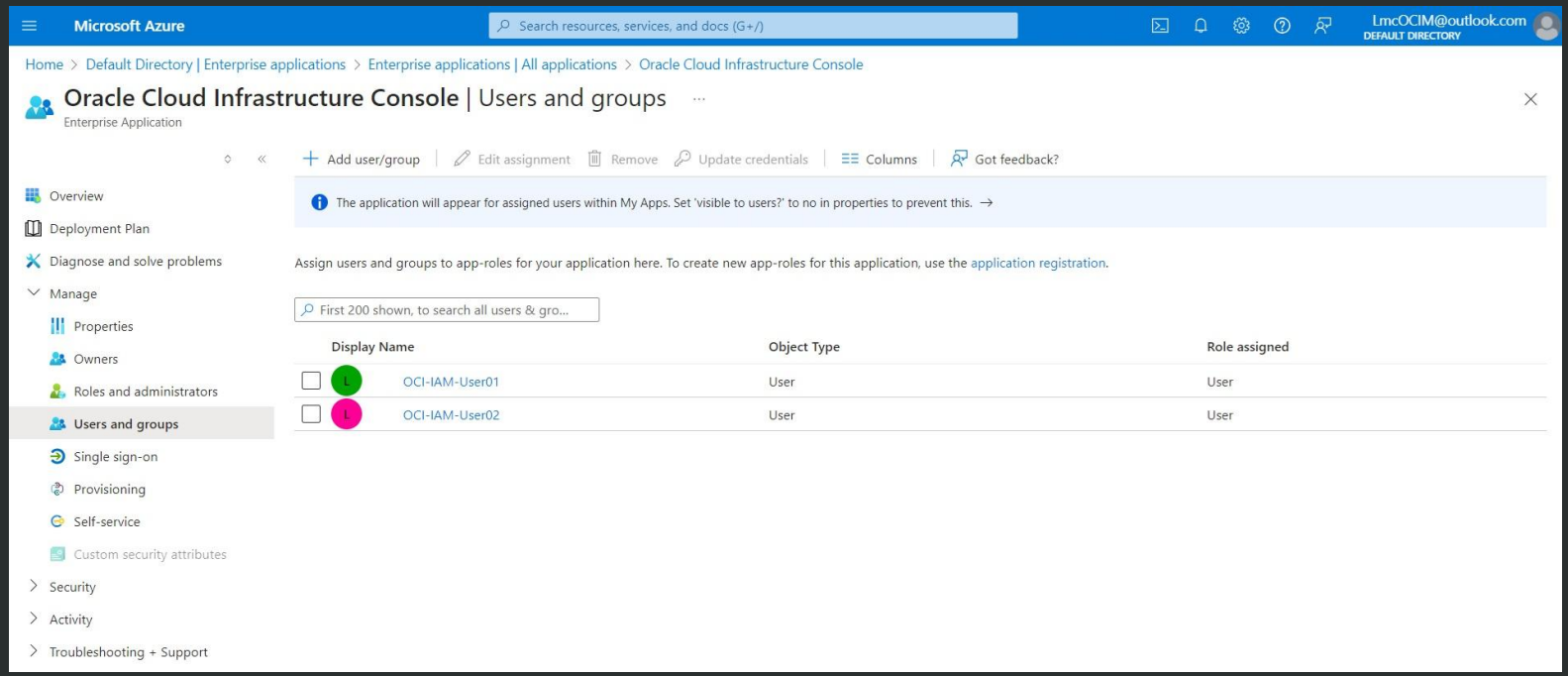
In the *Users and groups* page, select *Add user/group*

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*

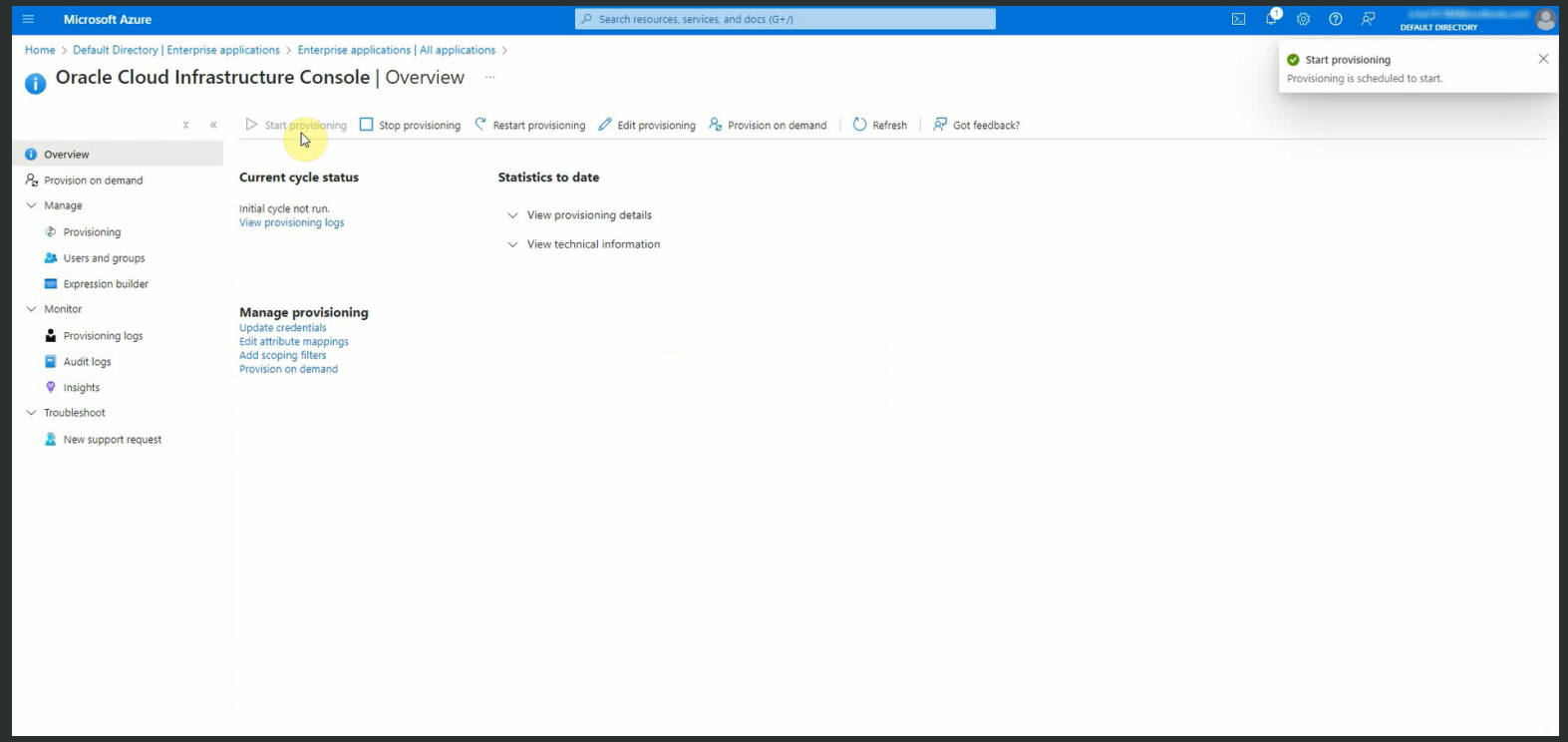
The Users and groups page now shows the chosen users and groups



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



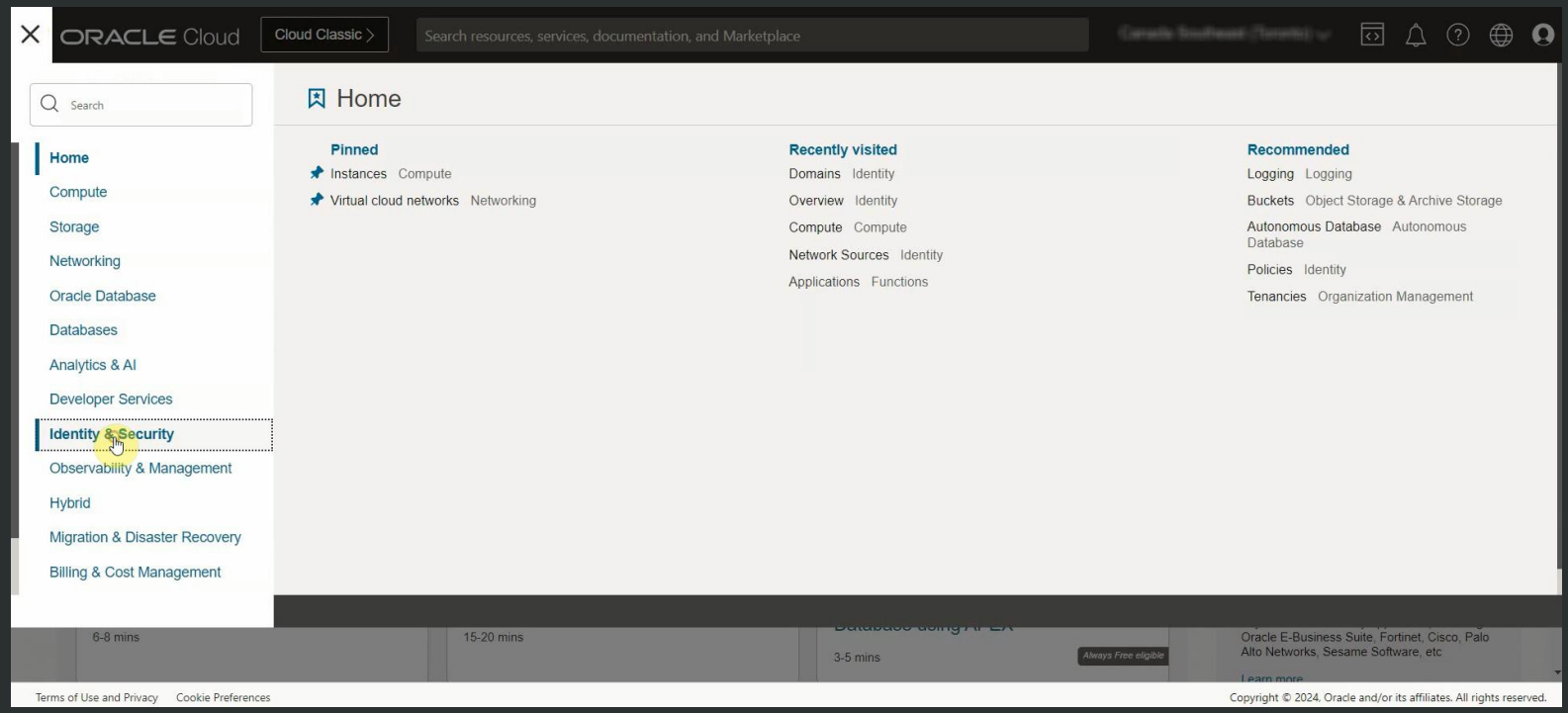
Pulling user accounts, groups and group membership from Entra ID to OCI IAM

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

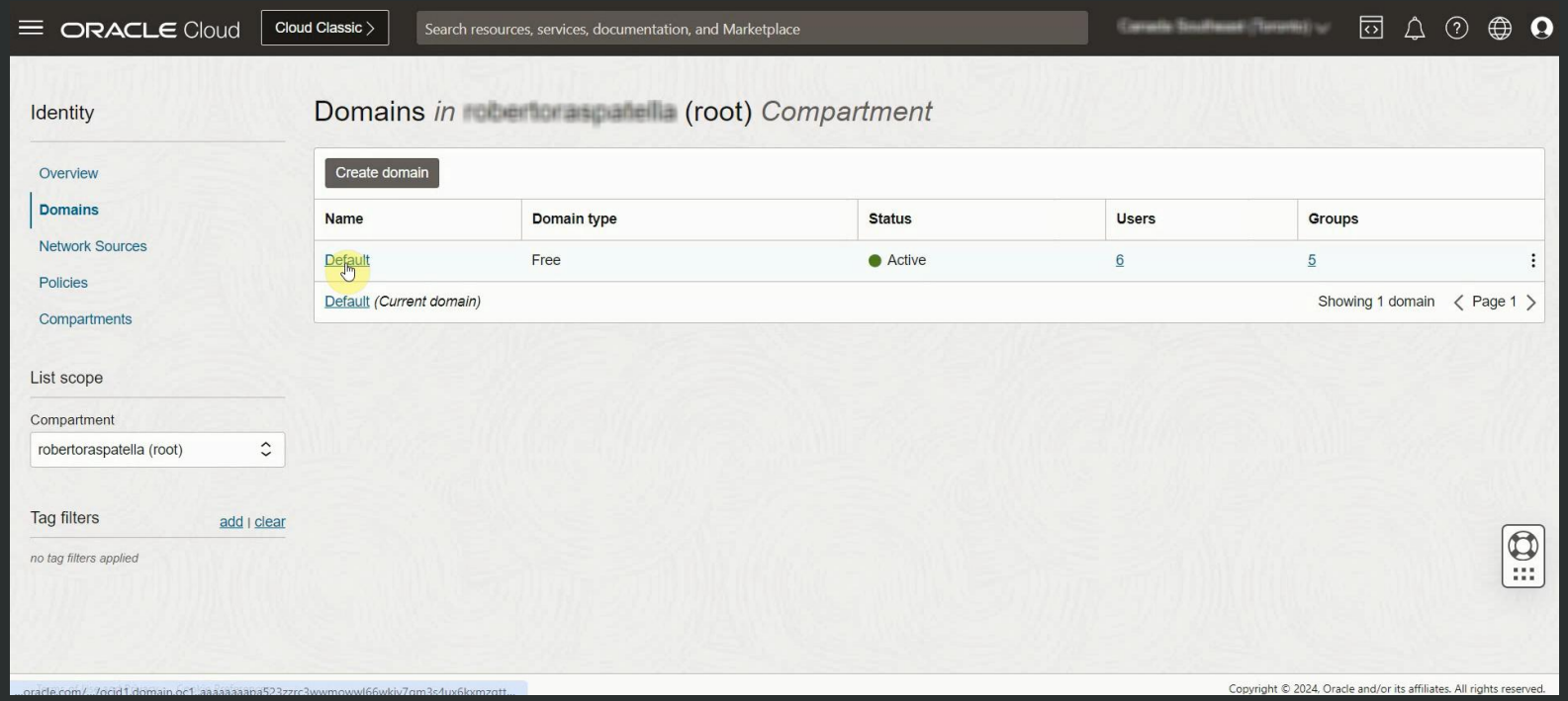
By creating an app in OCI IAM to act like identity provider for Entra ID, and by enabling synchronization, users, groups and group membership from Entra ID will be populated in OCI IAM as well

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



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

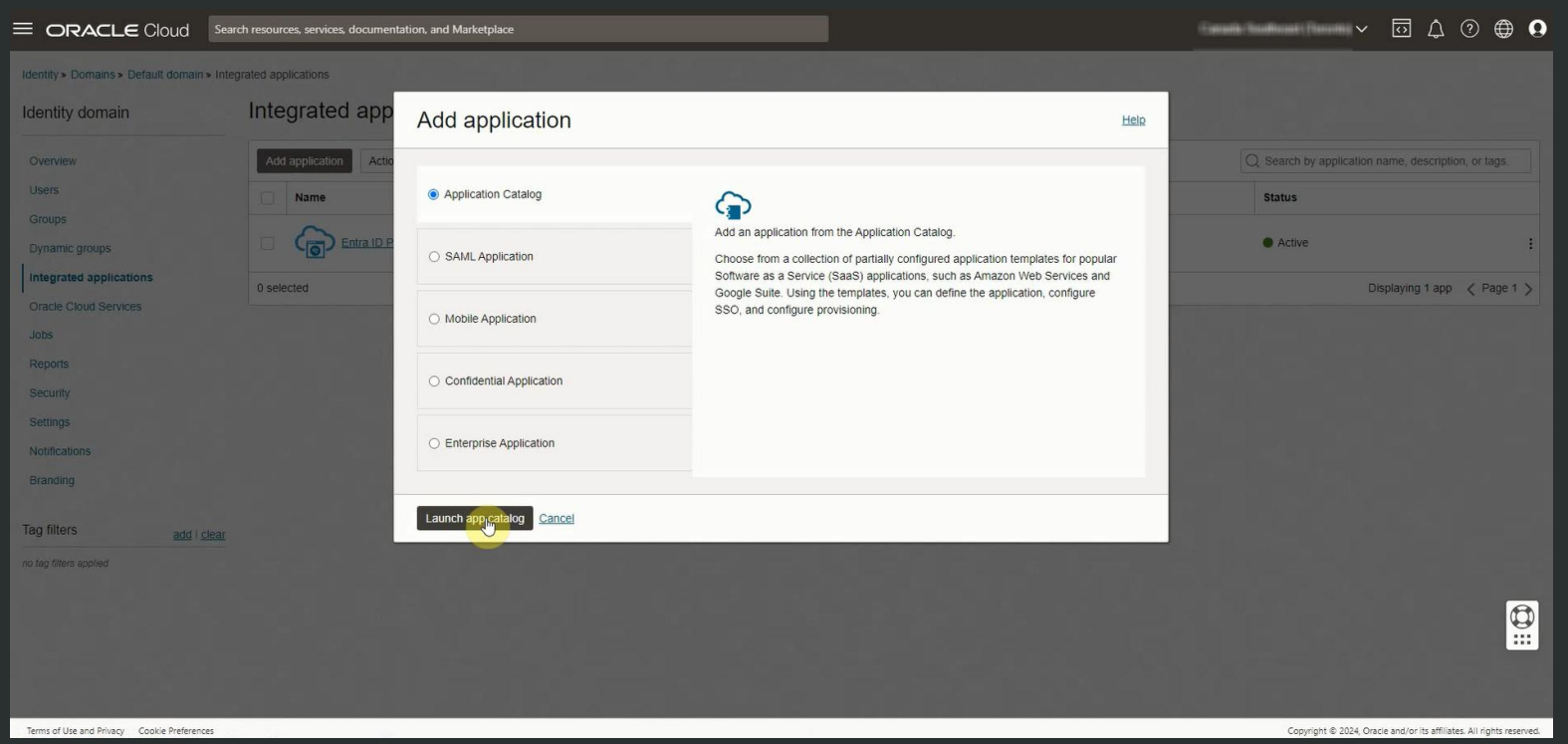
Then select the domain of the users that is intended to synchronize



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

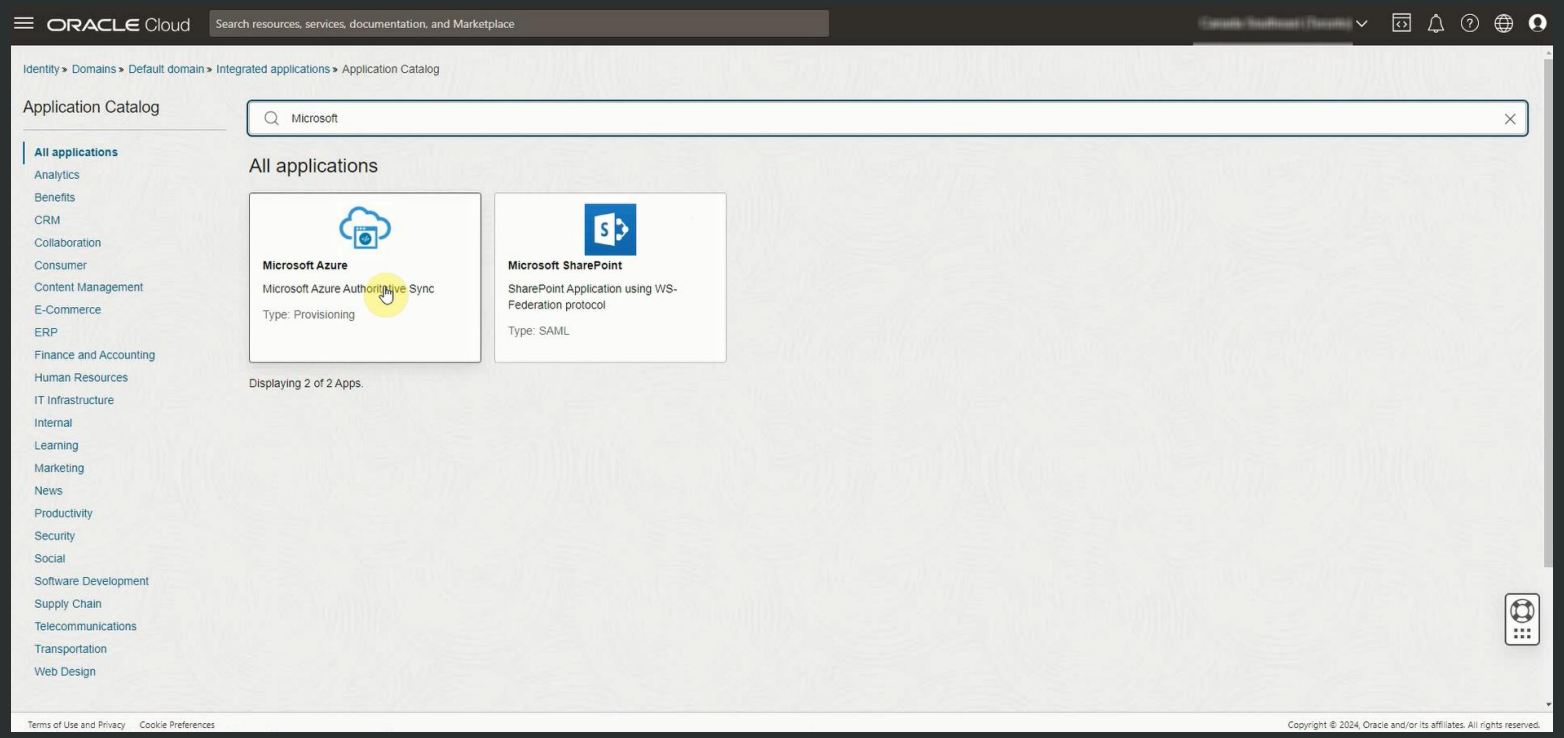
Under *Integrated application*, select Add application and then select Application Catalog

Select Launch workflow



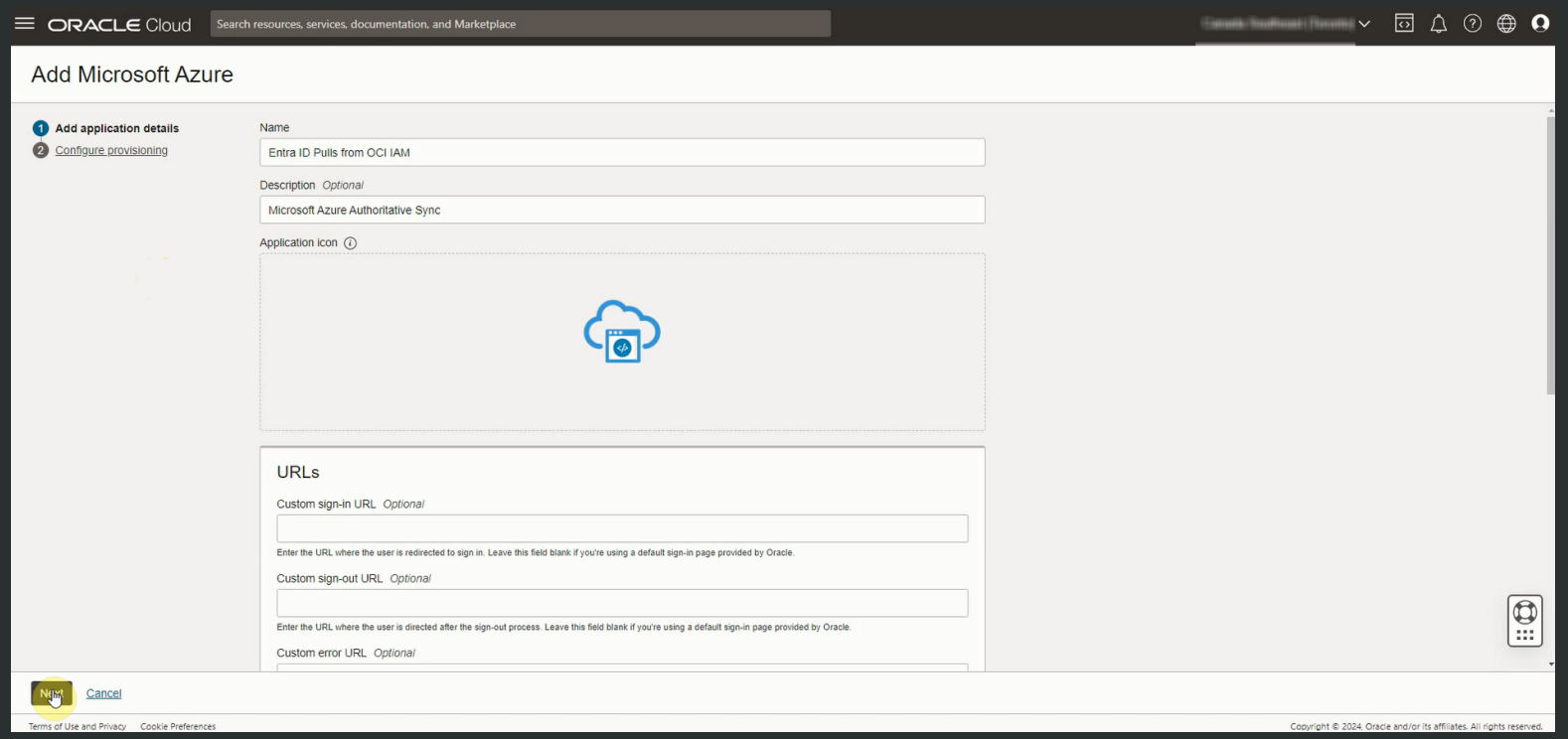
Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Search for “Microsoft” and select *Microsoft Azure*



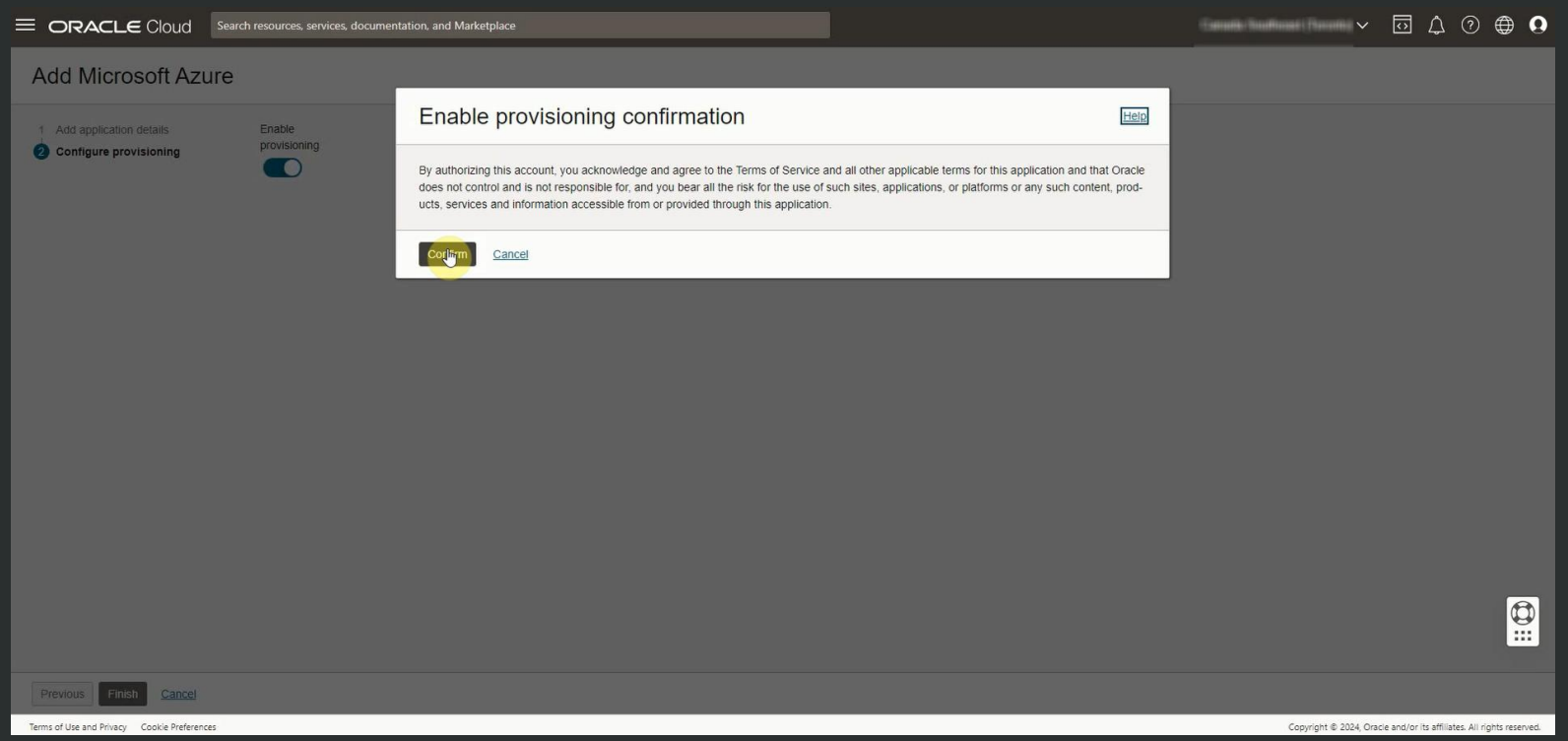
Pulling user accounts, groups and group membership from Entra ID to OCI IAM

Enter the name of the application to be used



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

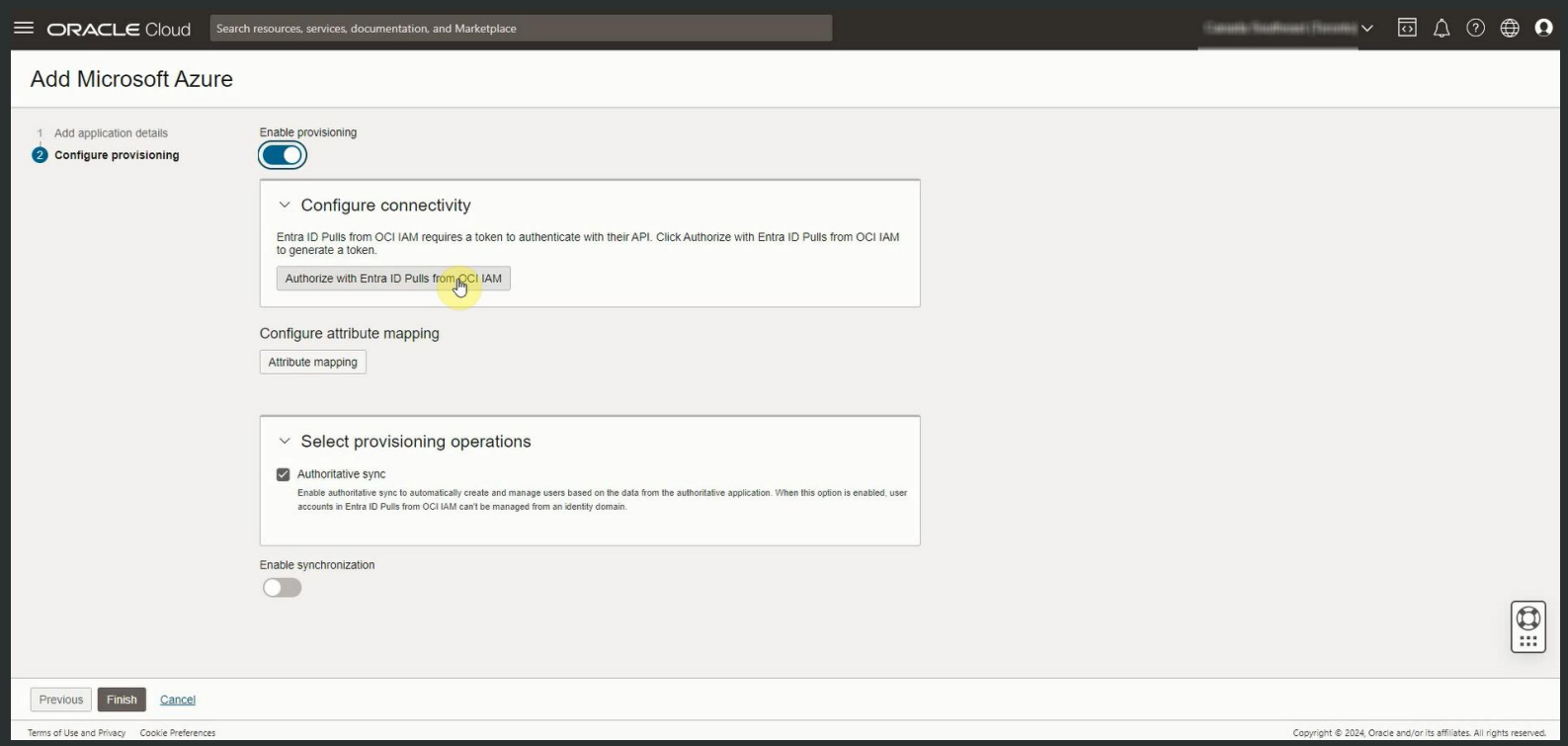
On the *Configure provisioning* page, select *Confirm* to enable provisioning



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

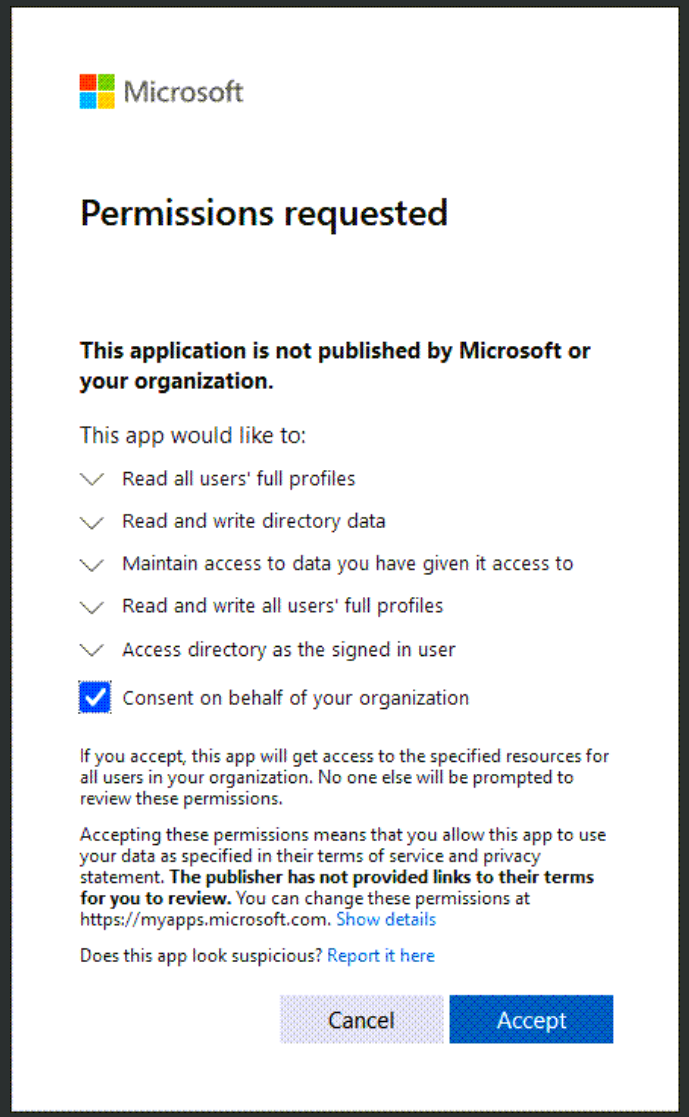
Microsoft will open a new browser window, sign in using Microsoft Entra ID credentials, in the Permissions requested dialog select *Accept*



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

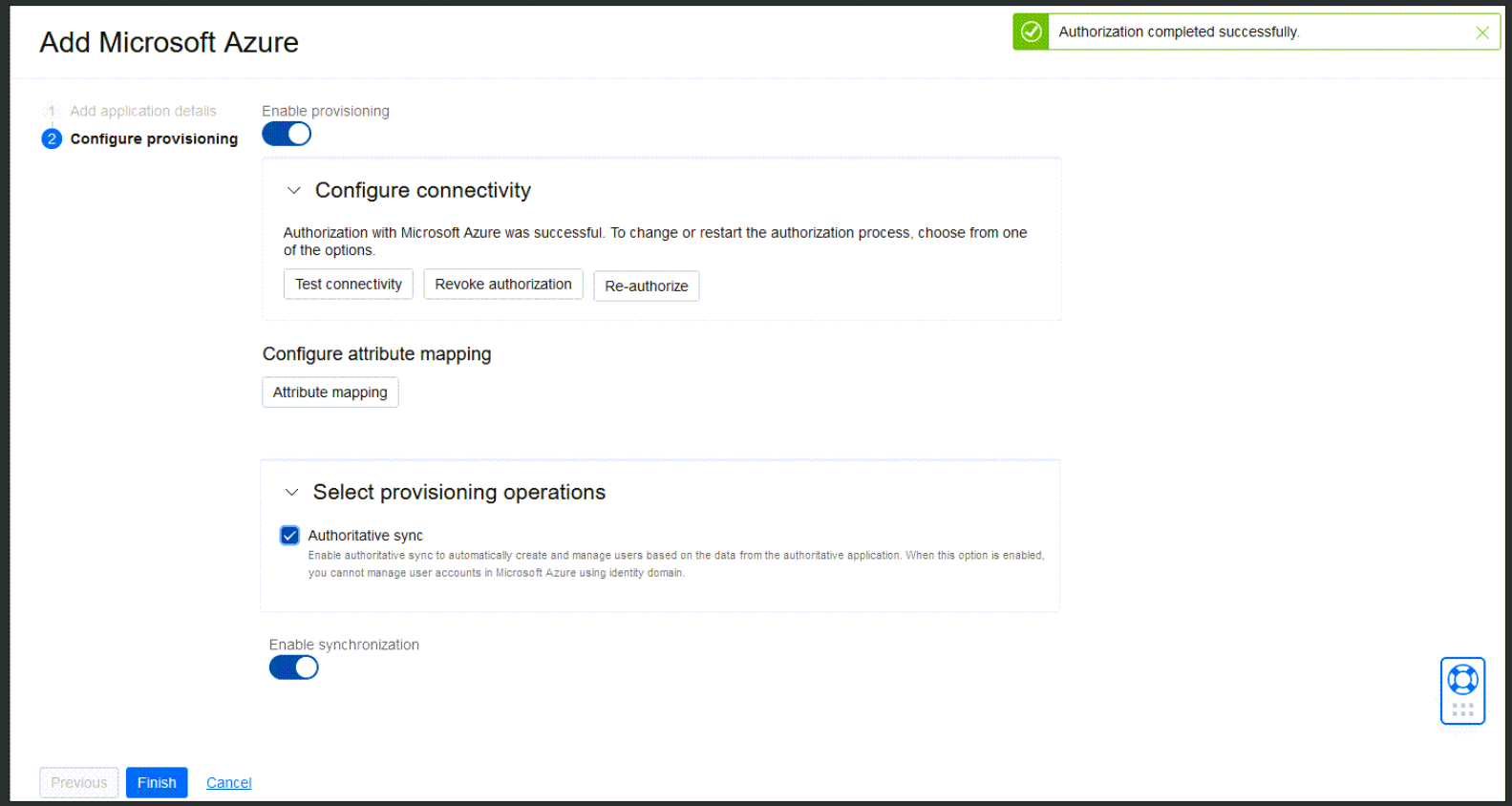


Pulling user accounts, groups and group membership from Entra ID to OCI IAM

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

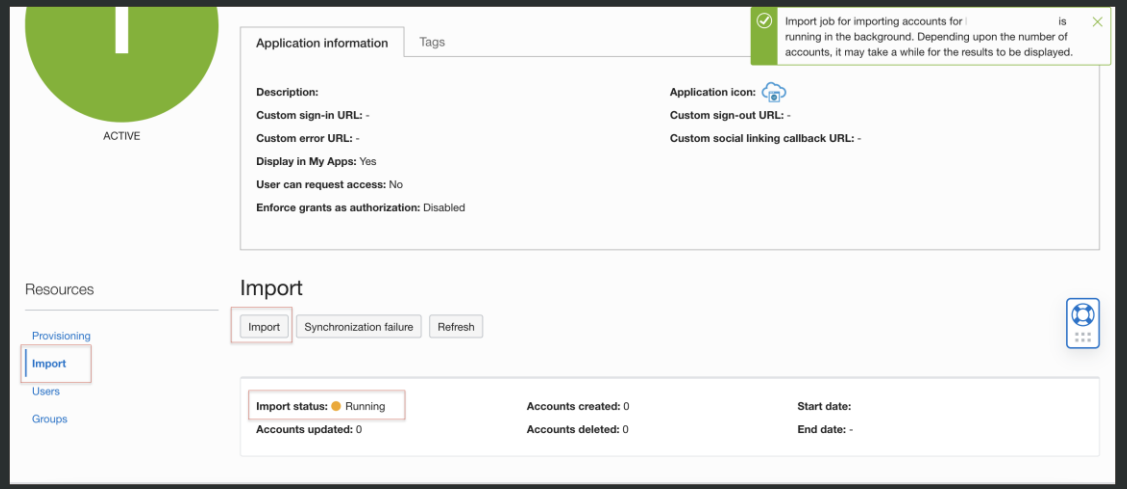


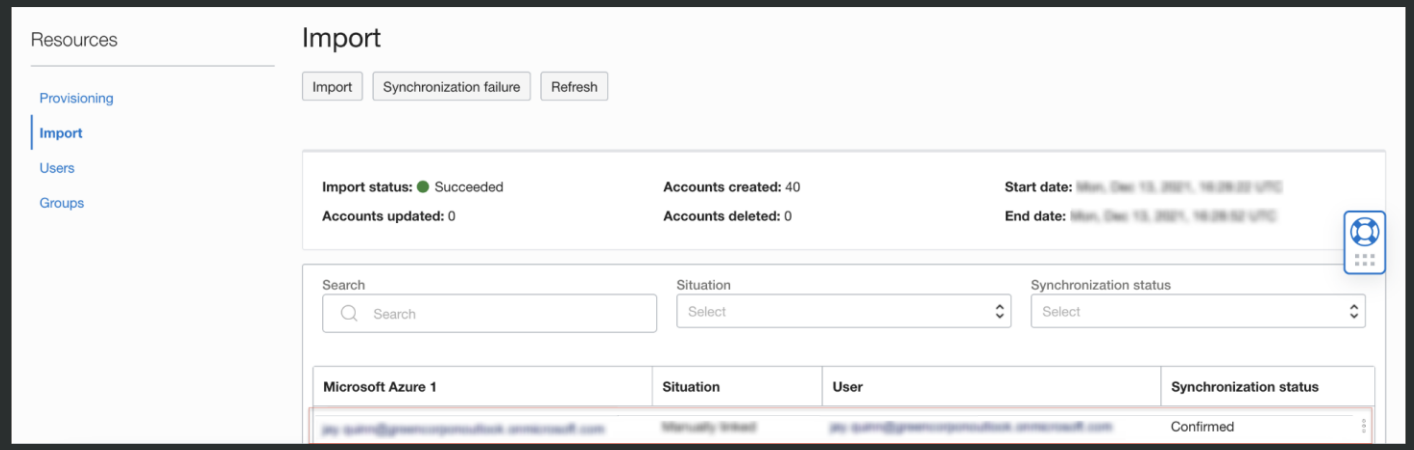
Pulling user accounts, groups and group membership from Entra ID to OCI IAM

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



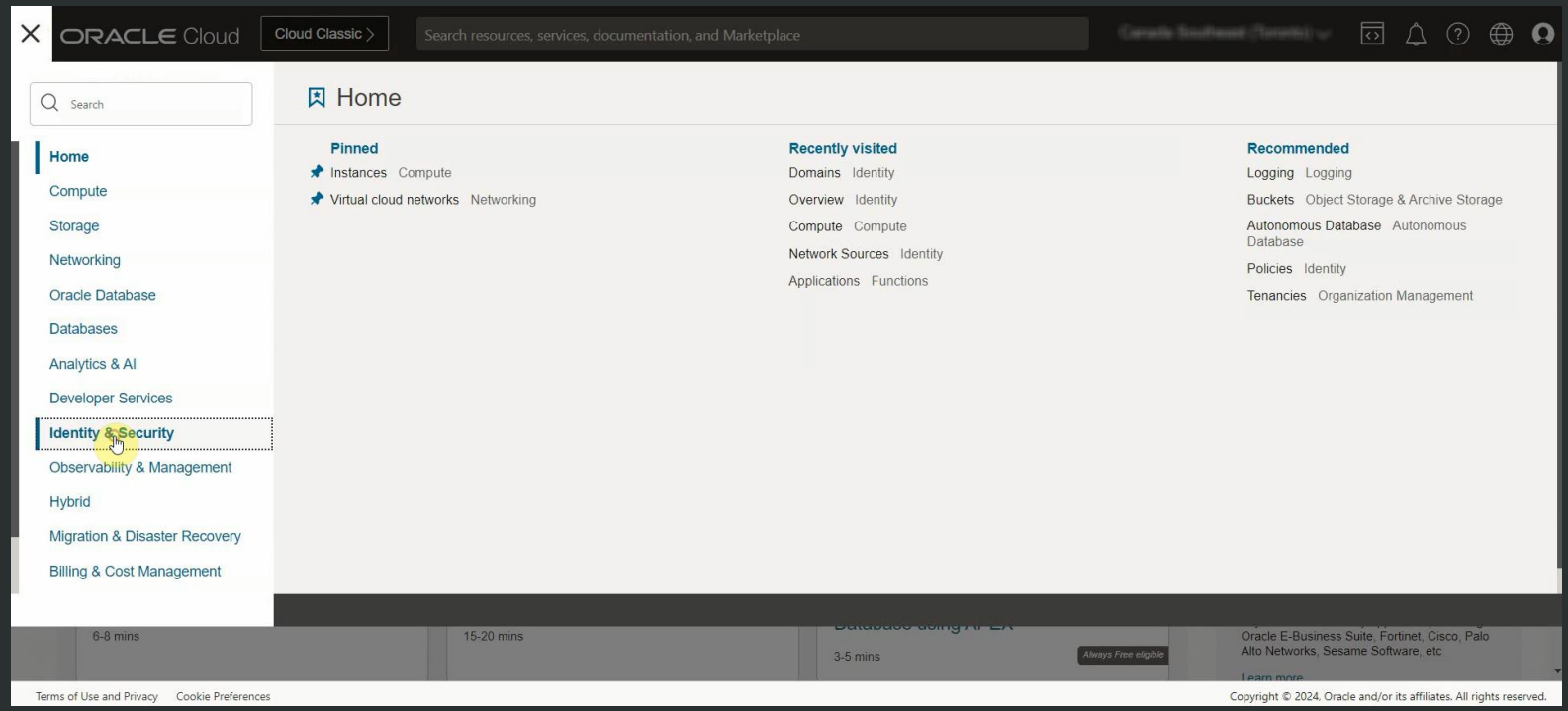


Pushing user accounts, groups and license from OCI IAM to Entra ID

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

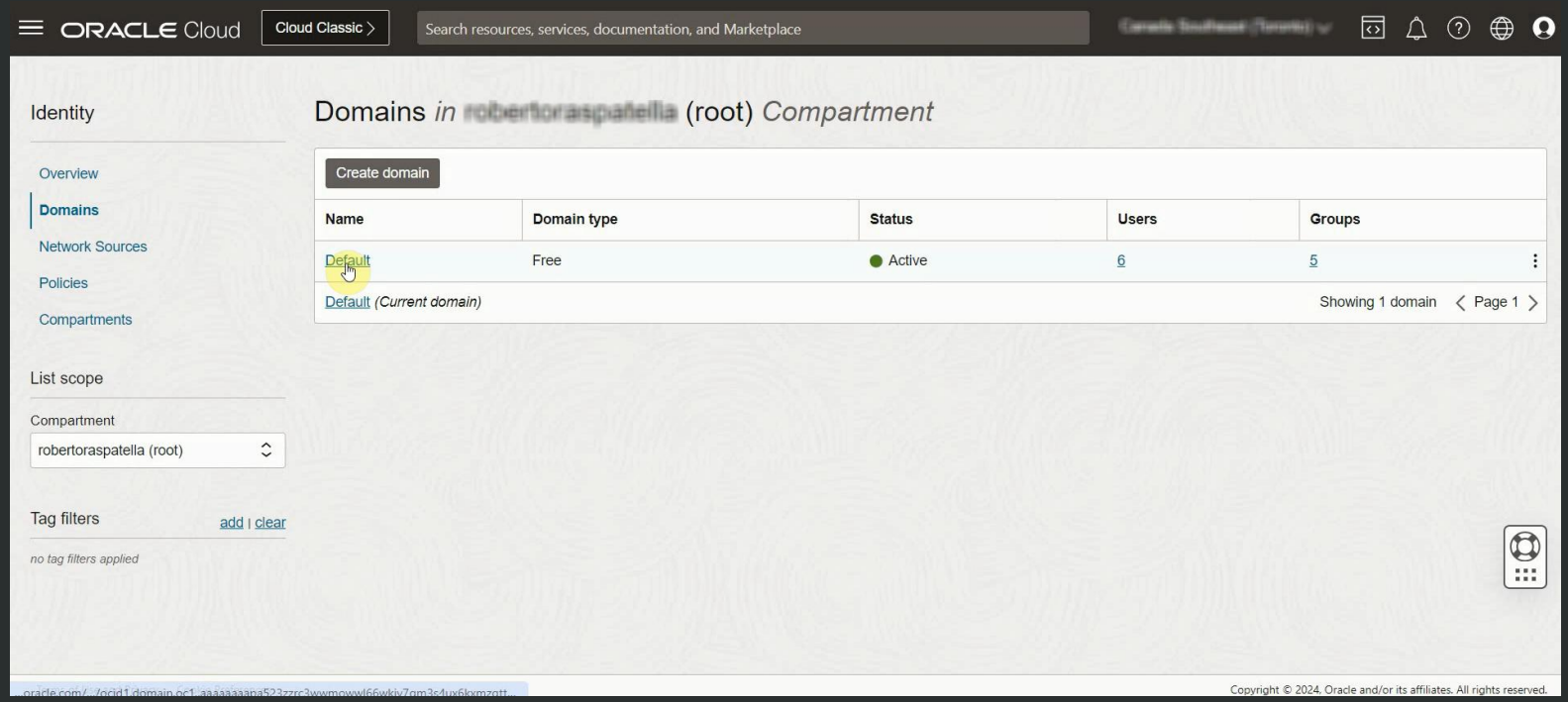
In OCI, select *Identity & Security* from the top left menu.



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

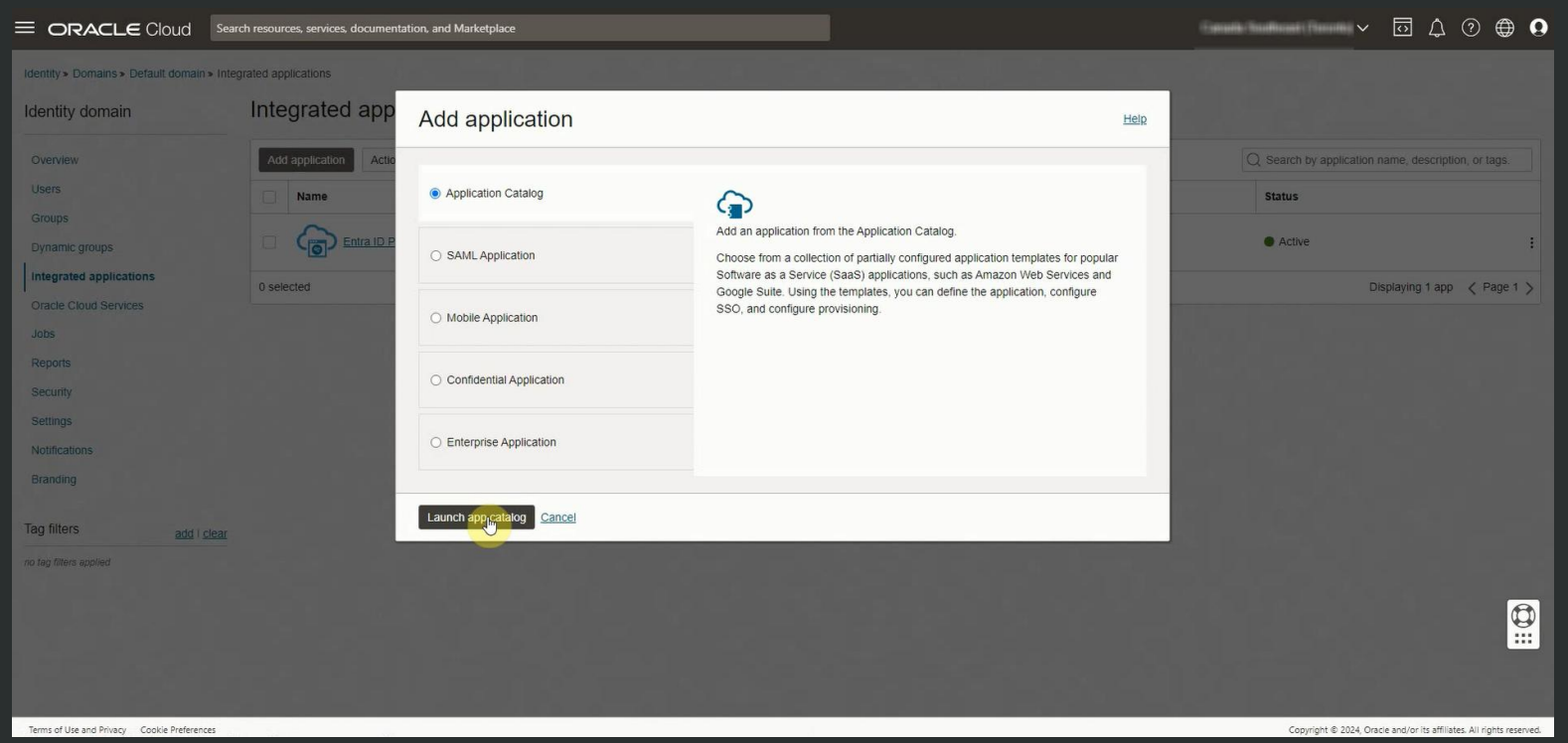


Pushing user accounts, groups and license from OCI IAM to Entra ID

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

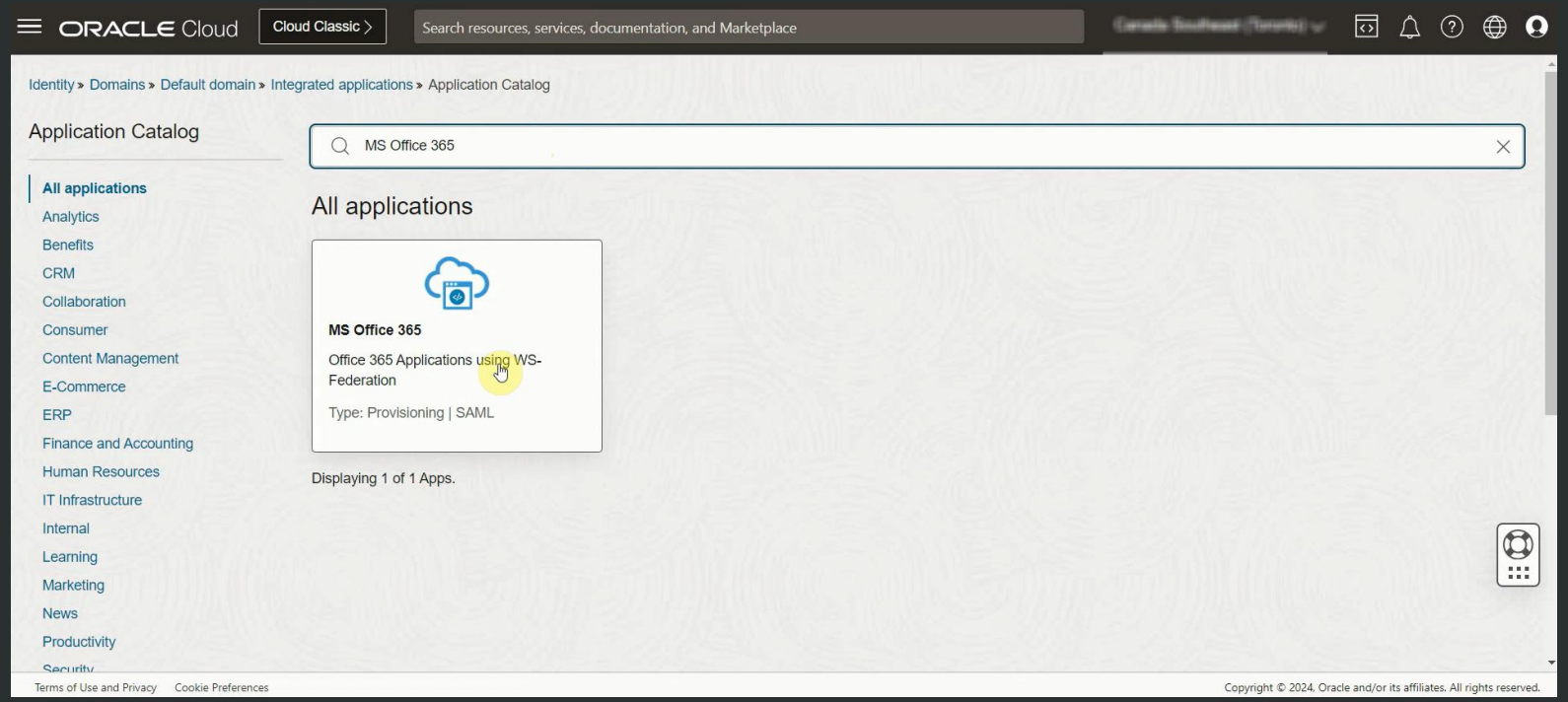
Under *Integrated application*, select Add application and then select Application Catalog

Select Launch workflow



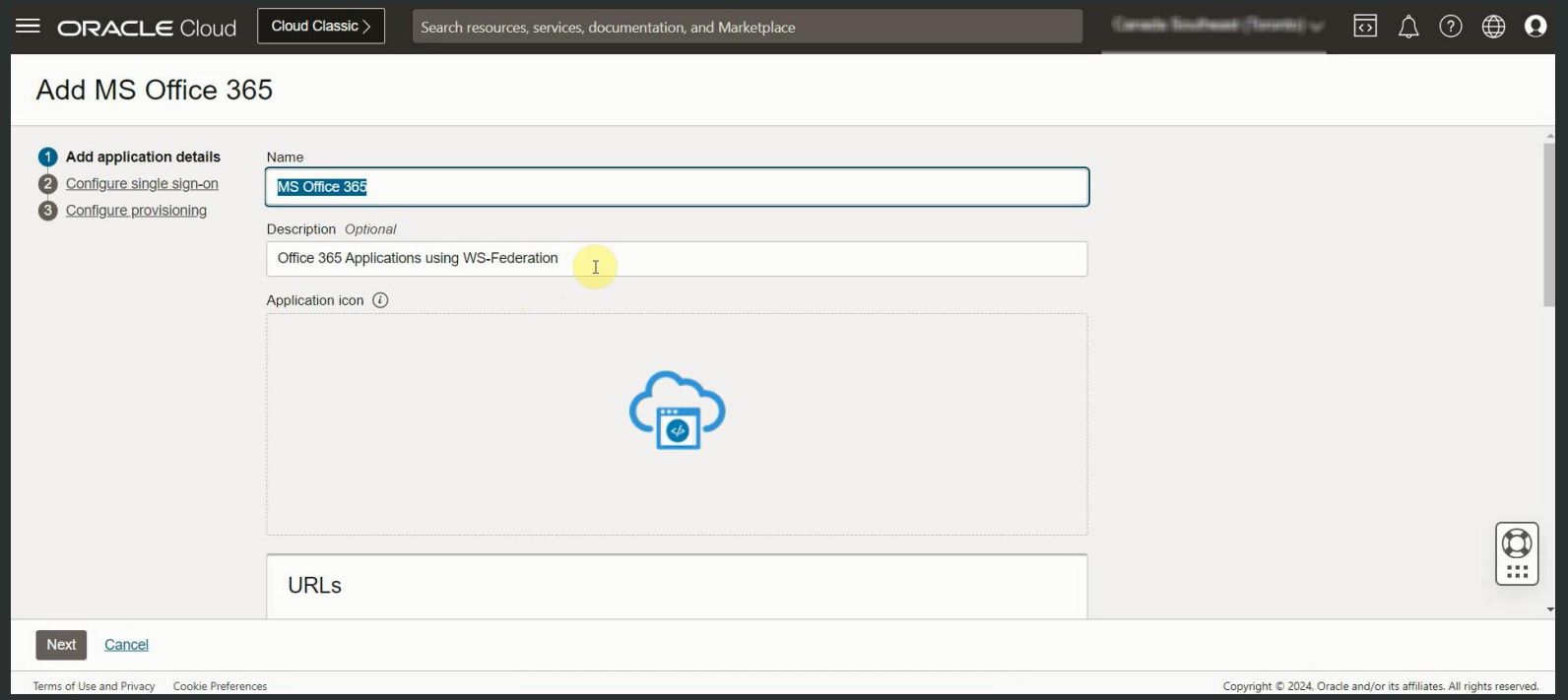
Pushing user accounts, groups and license from OCI IAM to Entra ID

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



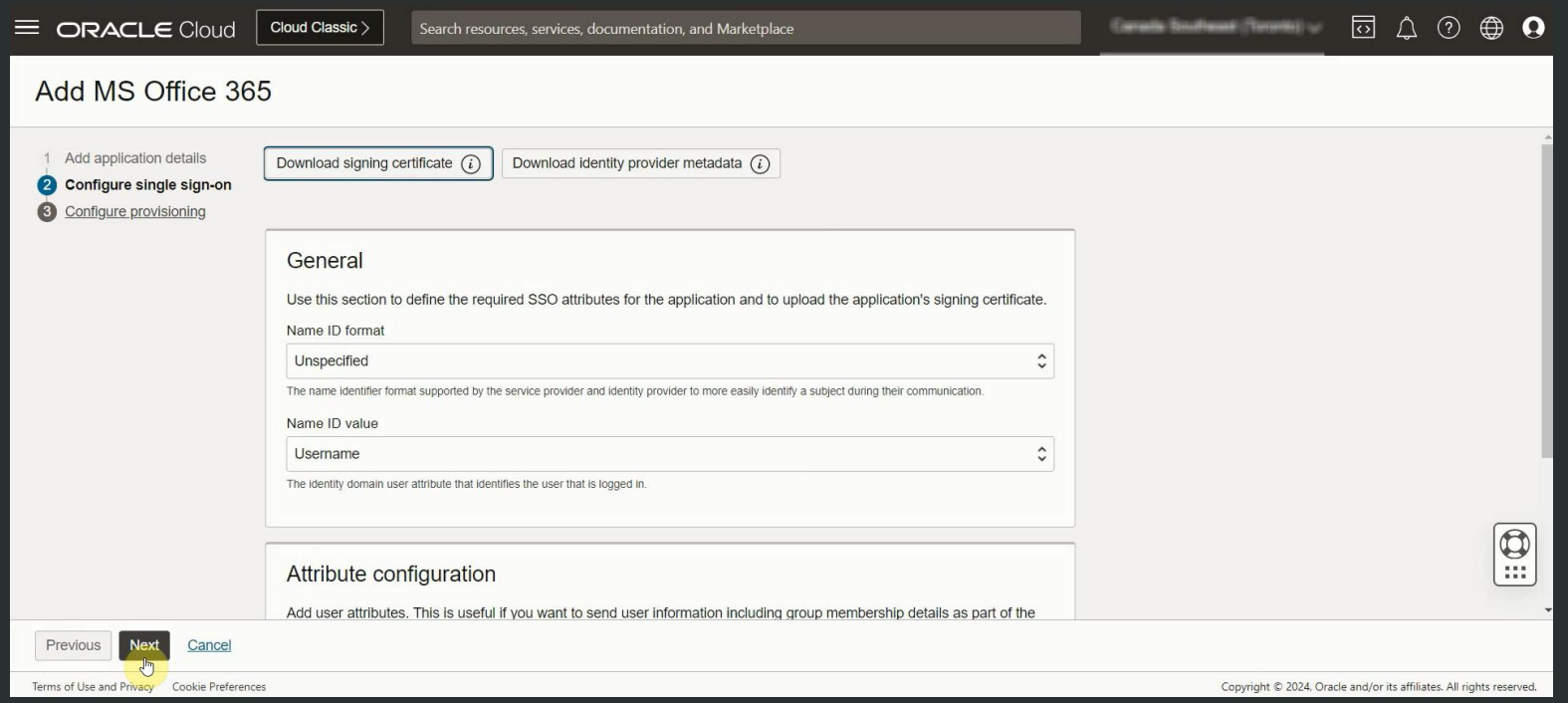
Pushing user accounts, groups and license from OCI IAM to Entra ID

Enter the name of the application to be used



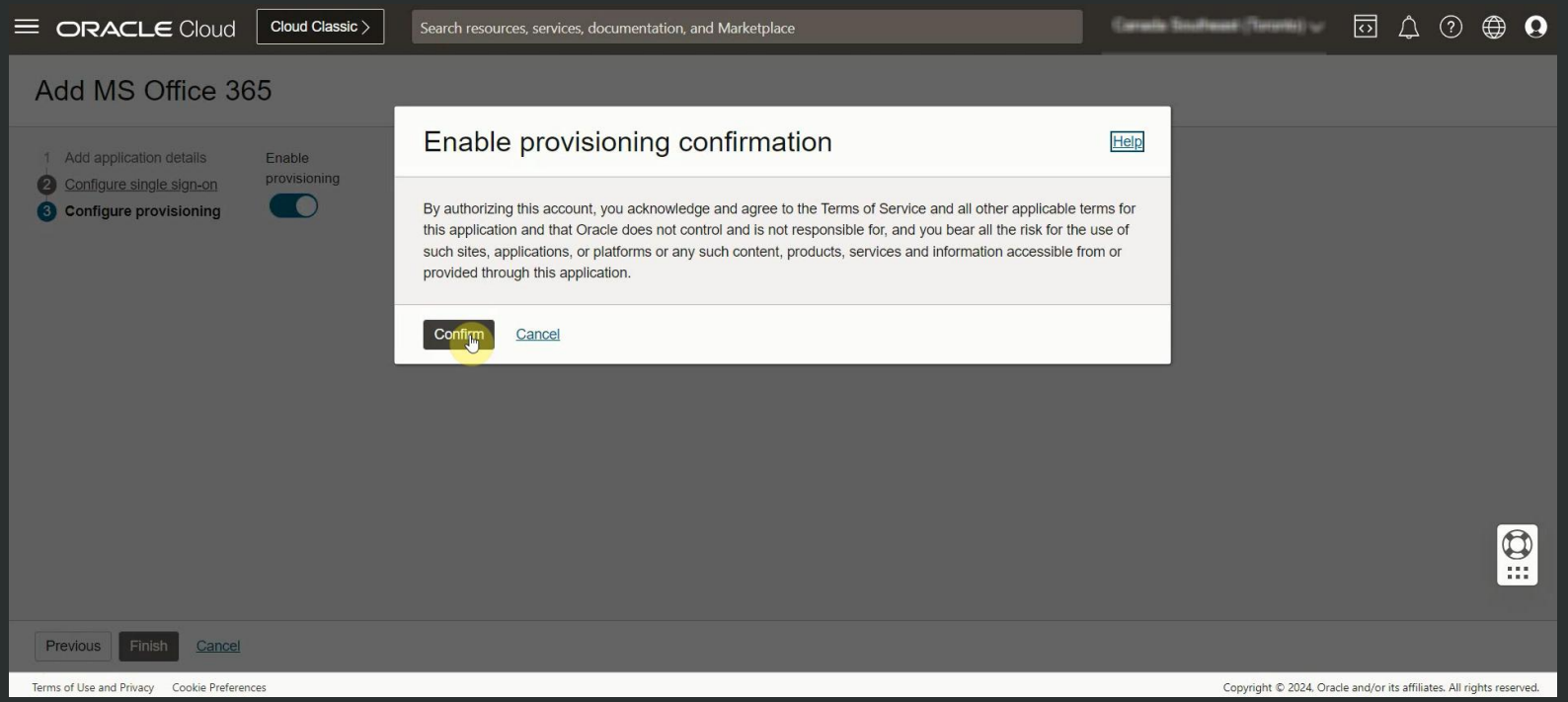
Pushing user accounts, groups and license from OCI IAM to Entra ID

Select *Next* and then *Next* again



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

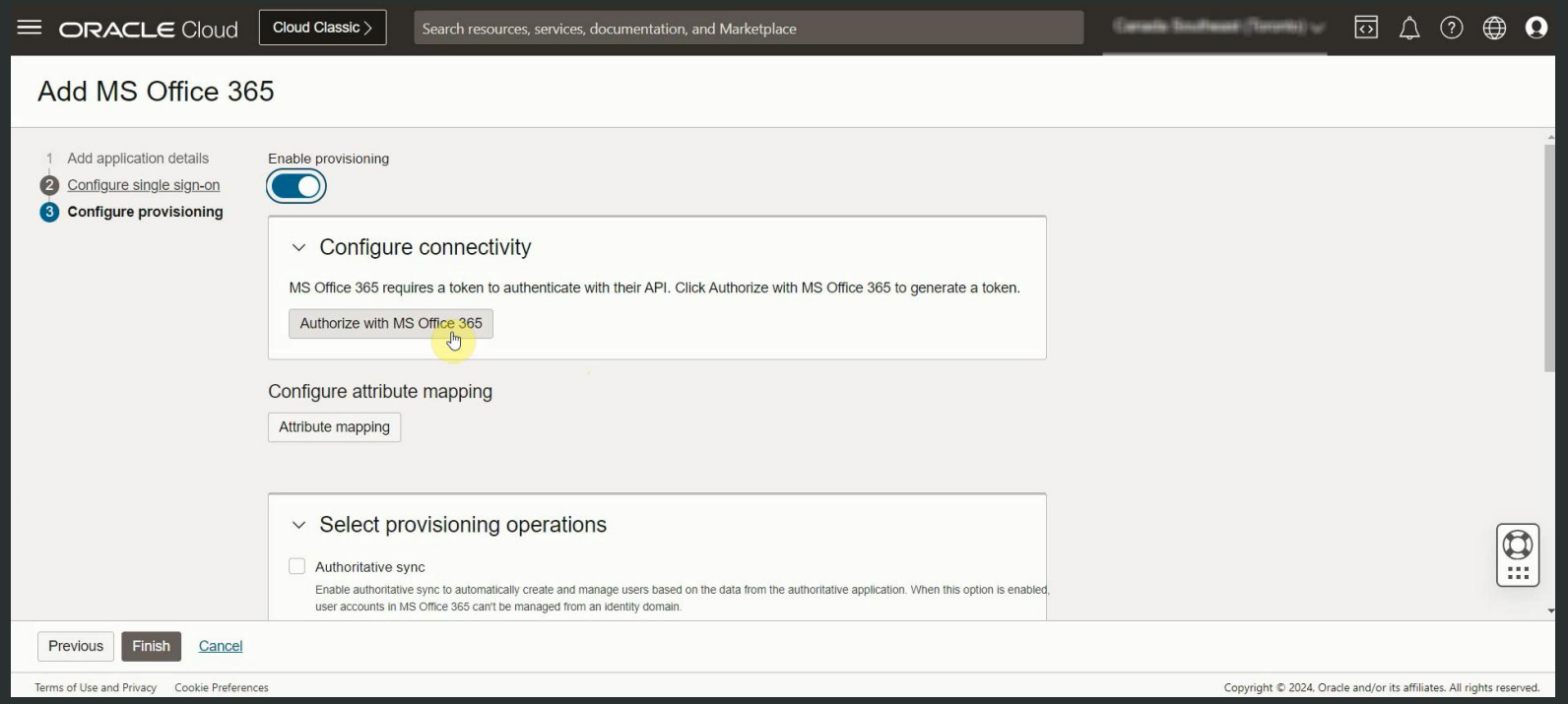
On the *Configure provisioning* page, select *Confirm* to enable provisioning



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

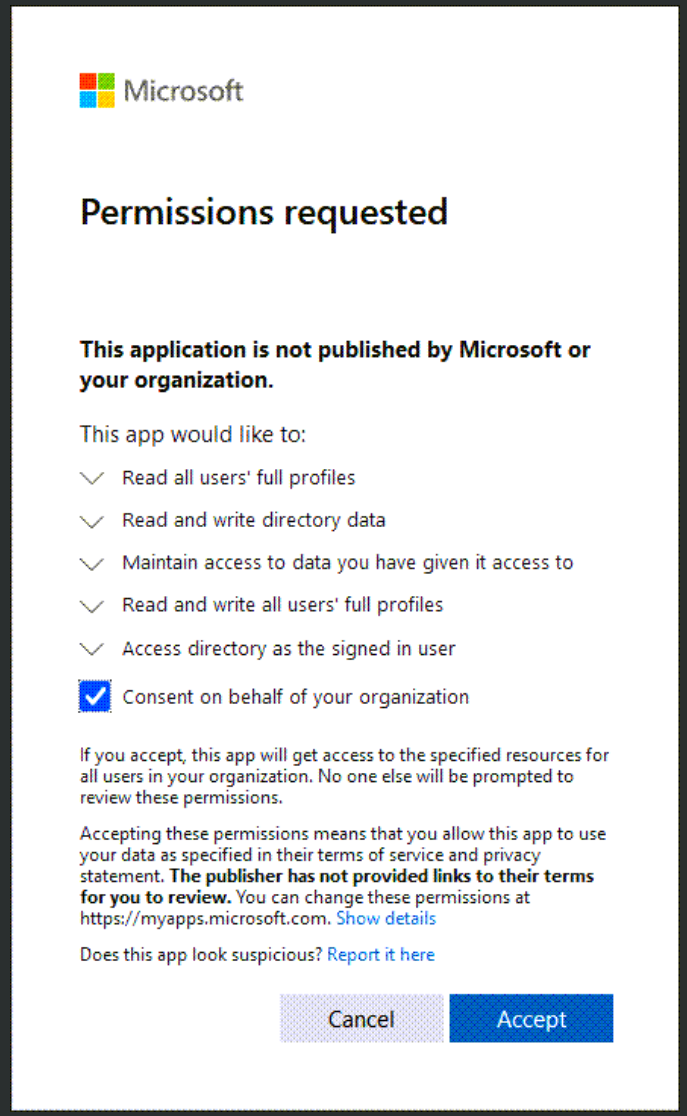
Log in using MS Office 365 credentials

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*

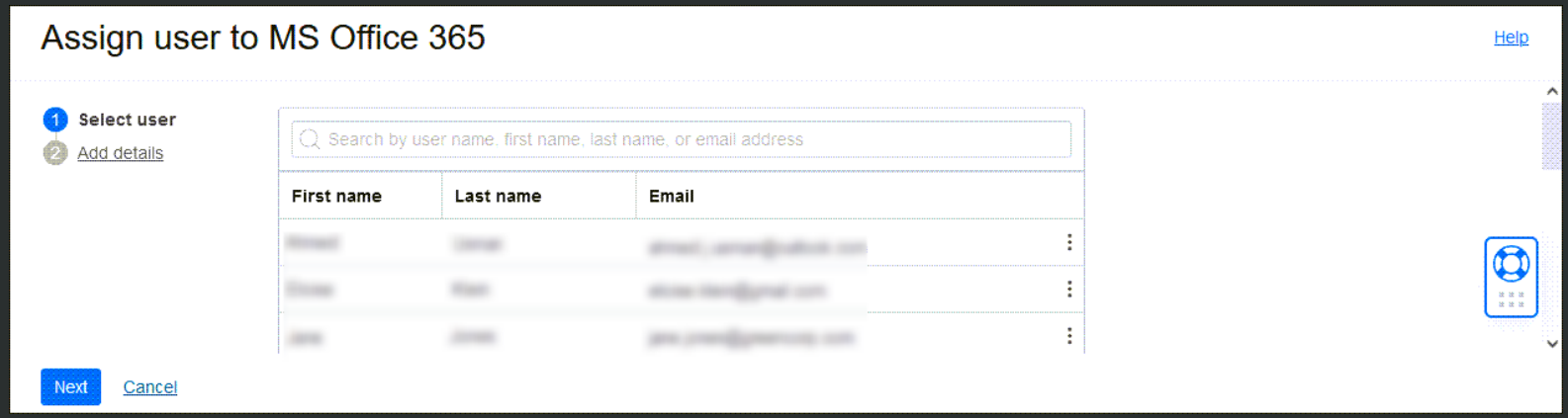
Search for the user to be assigned, then select the *Actions Menu* for that user and select *Assign.* Select *Next*

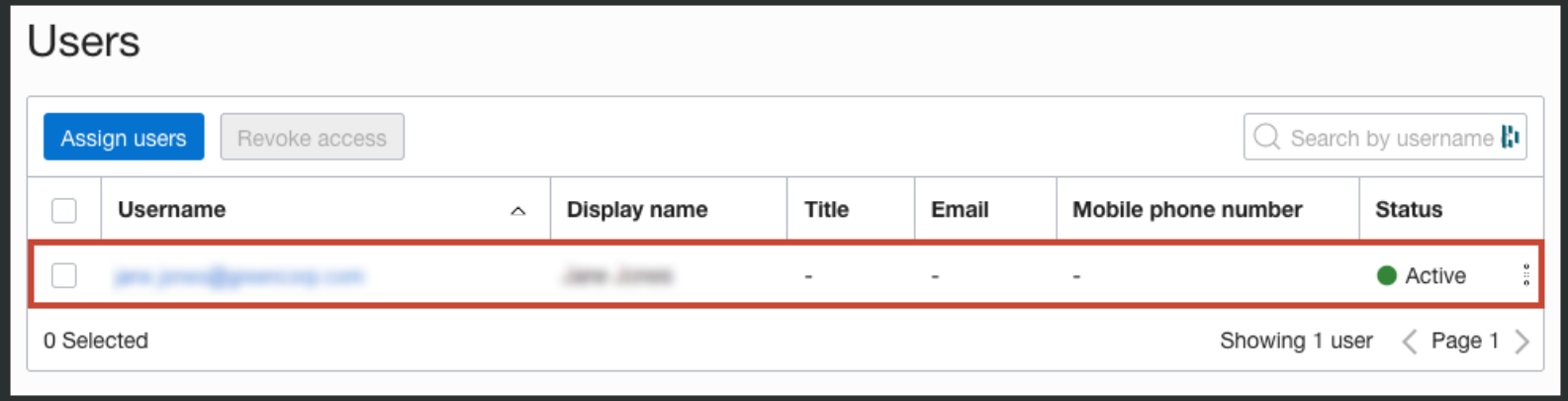
On the *Add Details page*, scroll down, and under *Licenses*, select *Add*

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*






ORACLE