|  |
| --- |
|  |
|  |
| **OAuth Configuration Manual** |
|  |
| Version 1.0 |
| February 2024  Copyright © 2025, Oracle and/or its affiliates  Confidential – Oracle Internal |

Table of Contents

[1.1 Document Control 3](#_Toc189962742)

[1.2 Glossary 3](#_Toc189962743)

[1.3 Introduction of OAuth2.0 Client Credentials Policy 4](#_Toc189962744)

[1.4 Pre-Requisites 4](#_Toc189962745)

[1.5 Navigating the Process IN Gen 3 IAM 4](#_Toc189962746)

[1.6 Important Info To Be Shared By Admin To Caller 11](#_Toc189962748)

Document Control

| Date | Author | Version | Change reference |
| --- | --- | --- | --- |
| 08-Feb-2023 | Suhas Nagendra | 1.0 |  |

Glossary

| Abbreviation | Definitions |
| --- | --- |
| OIC | Oracle Integration Cloud |
| PaaS | Platform as a Service |
| REST | Representational State Transfer |
| API | Application Programming Interface |
| WS | Web Service |

Introduction of OAuth2.0 Client Credentials Policy

It's recommended to use OAuth 2.0 to avoid issues like password management, expirations, and policy changes. This single setup streamlines user roles and aligns with Oracle's new security standards.

In essence, using OCI Cloud Console and IDCS/IAM Access aligns strategically with Oracle's advancements. This, coupled with OAuth 2.0's effectiveness, promotes modern security practices and smooth transitions between releases, ensuring continuous and efficient monitoring functions.

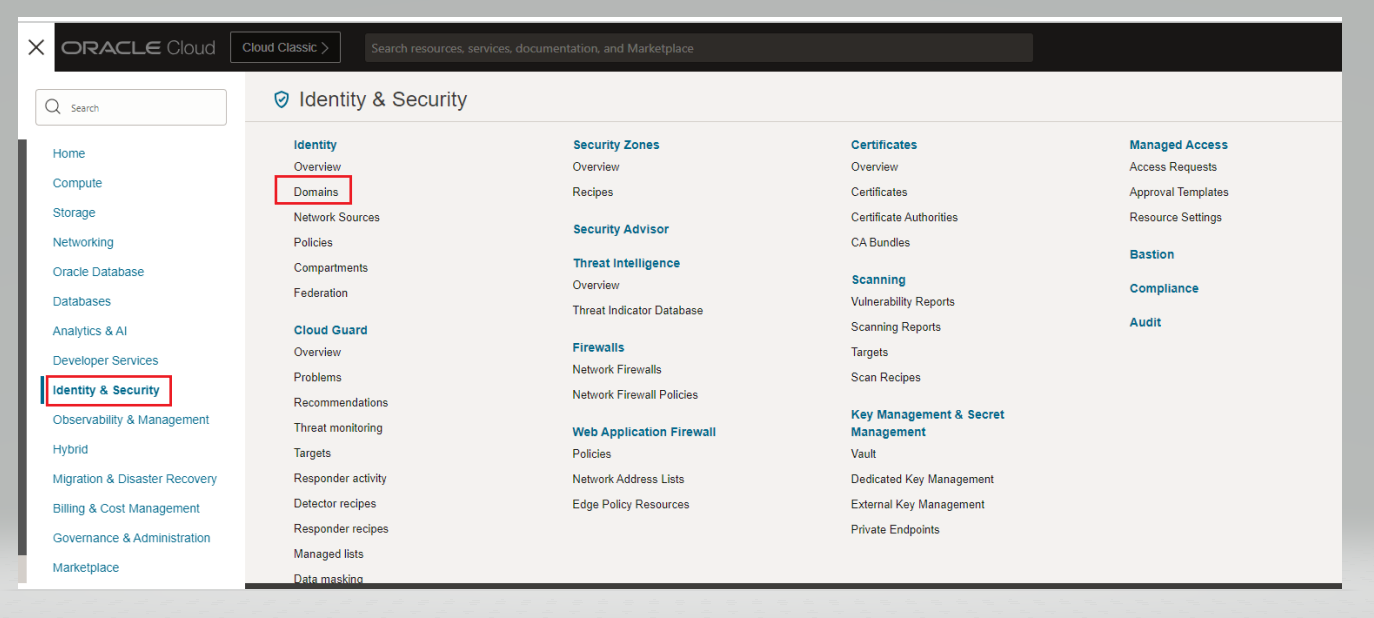
Clients commence by registering through a confidential app creation in Oracle IDCS/IAM. This app becomes the gateway for clients to seek access tokens from Oracle IDCS/IAM. Subsequently, the access token from this app is acquired, granting them access to safeguarded resources within various requesting applications.

Pre-Requisites

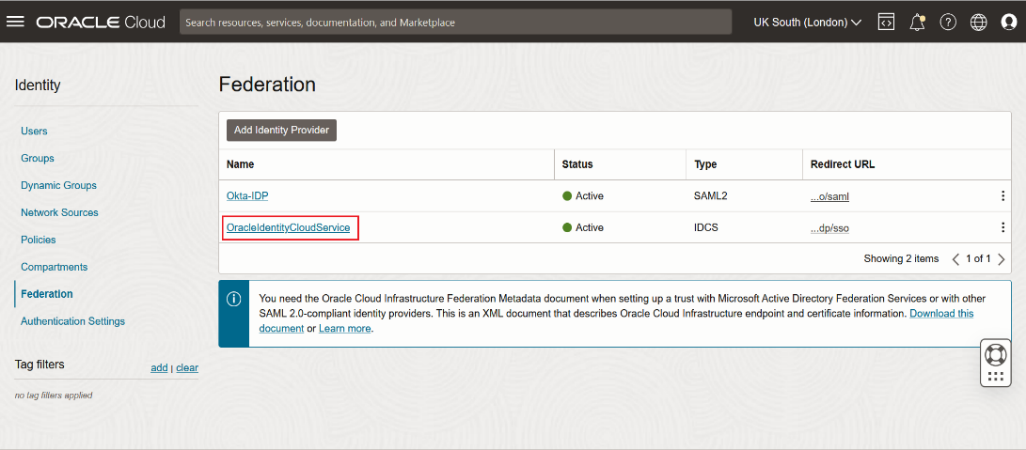
These steps are performed who primarily have admin access to navigate to Oracle IDCS/IAM Administrator.

Navigating the Process IN Gen 3 IAM

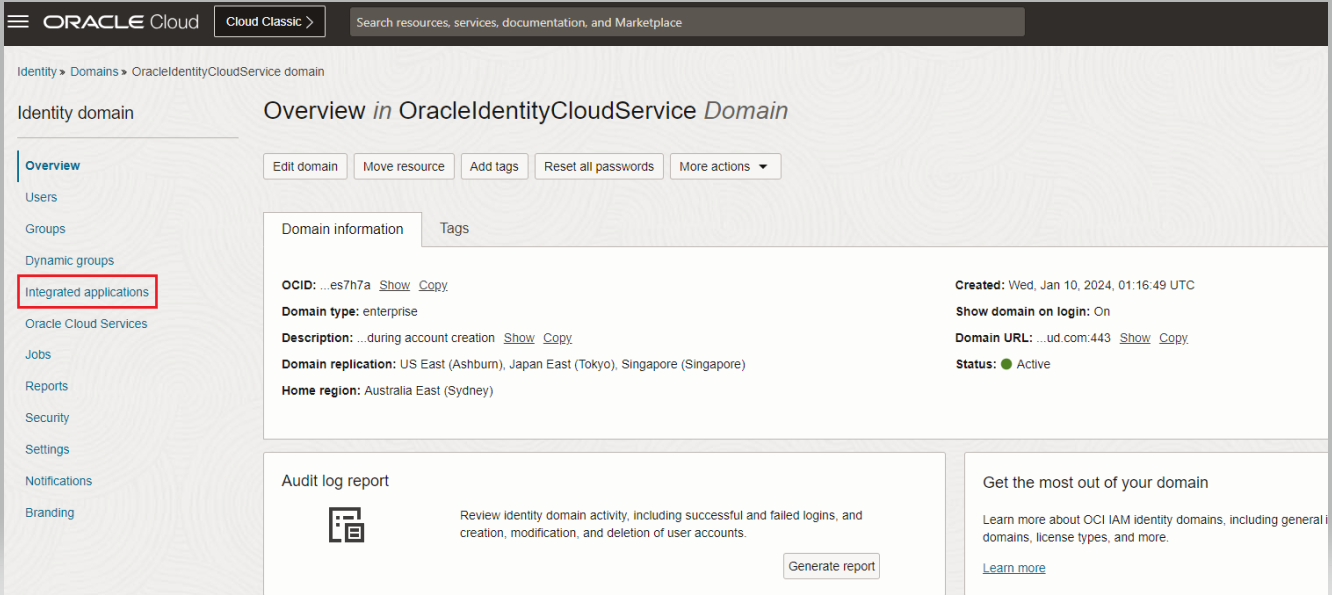
1. Navigate to **https://cloud.oracle.com** and inputting your tenancy name. Then, log in to the OCI platform after providing the credentials.
2. To access the Oracle IDCS console, proceed to **"Identity & Security"** and click on **"Domains."**



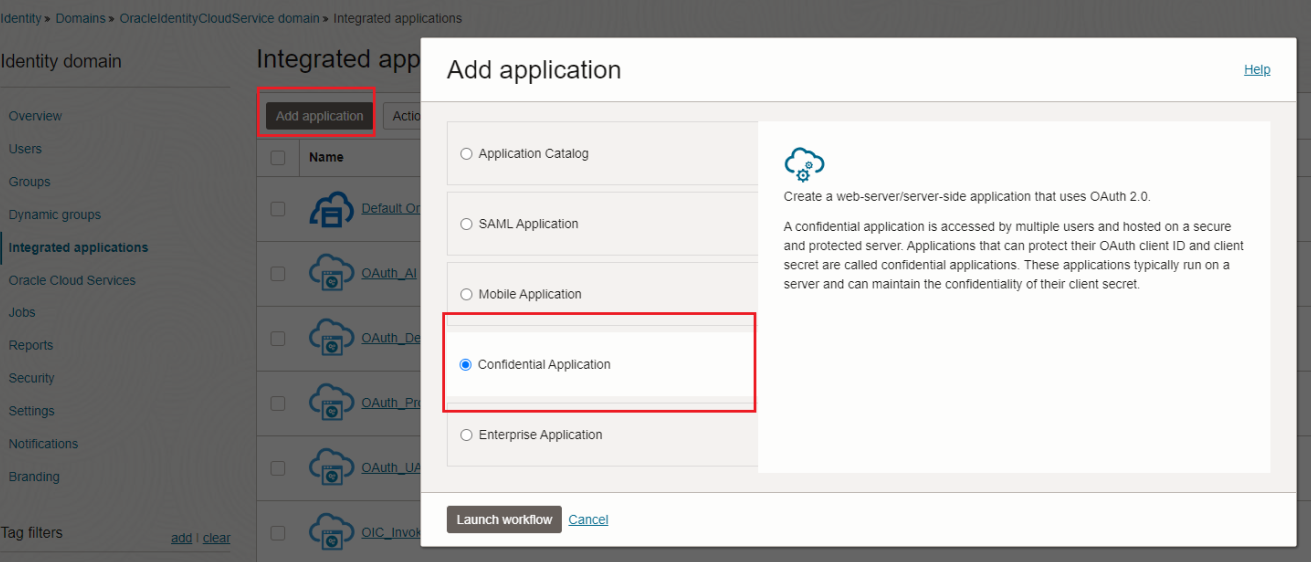
1. Open **"OracleIdentityCloudService"**



1. Click on Integrated Applications to create OAuth Confidential application.



1. Click on **“Add Application”** and **“Choose Confidential Application”** and click on Launch Workflow.

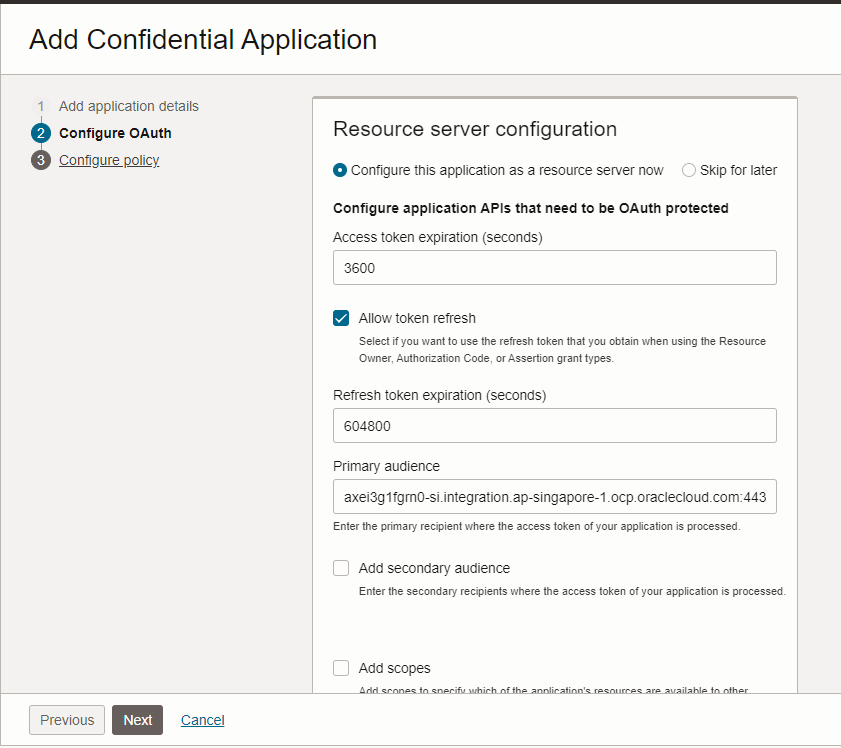


1. In Details tab enter name of application as Oracle<Your Env Name> and click **"Next"**.

## 

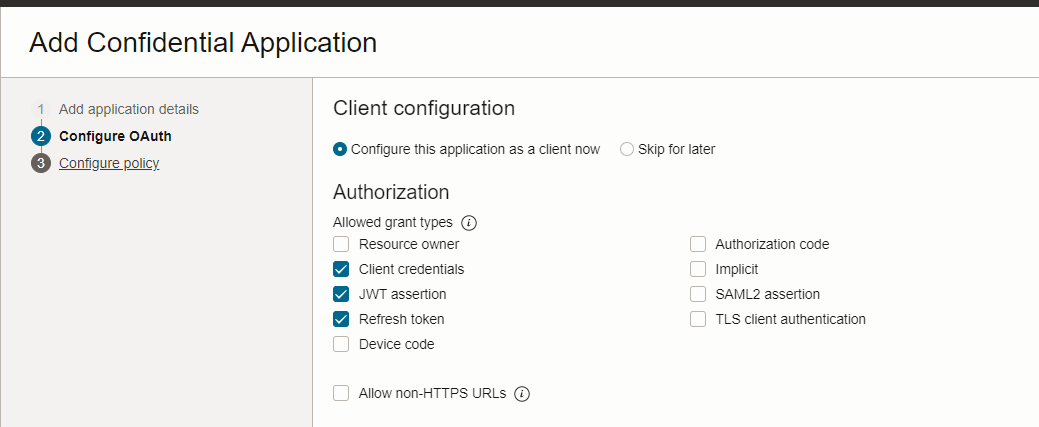
1. Next click on **Configure this applications as a resource server now** and select **“Access Token Expiration”** with default values and Select Allow Refresh Tokens.

In the Primary Audience you need to add your respective OIC base URL without **“https://”**  
  
E.g. - **aoacsuatoic-axei3g1fgrn0-si.integration.ap-singapore-1.ocp.oraclecloud.com:443**

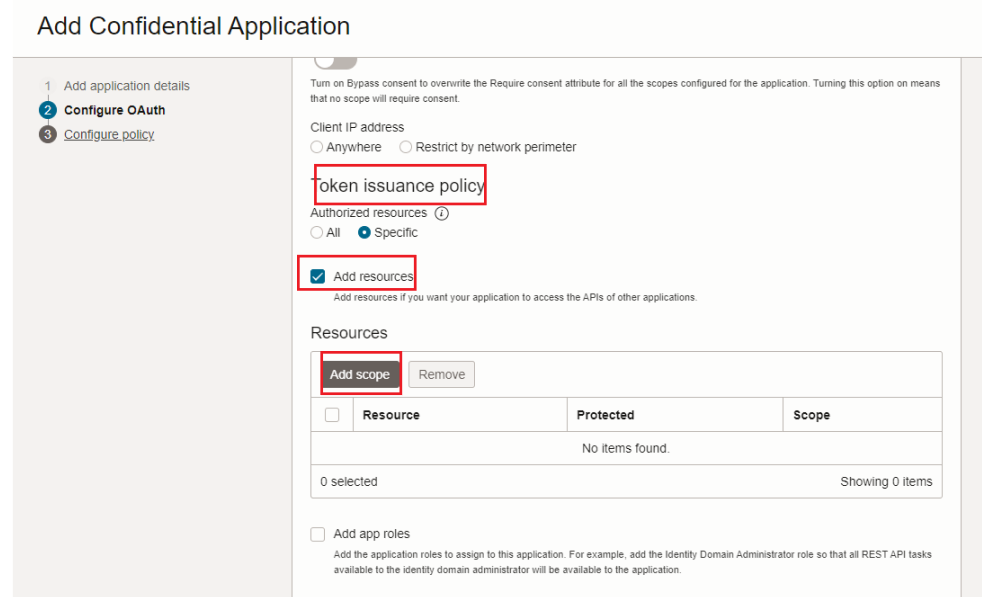


1. Next Choose **"Configure this application as a client now"** and make below selections in **Allowed Grant Types** section.

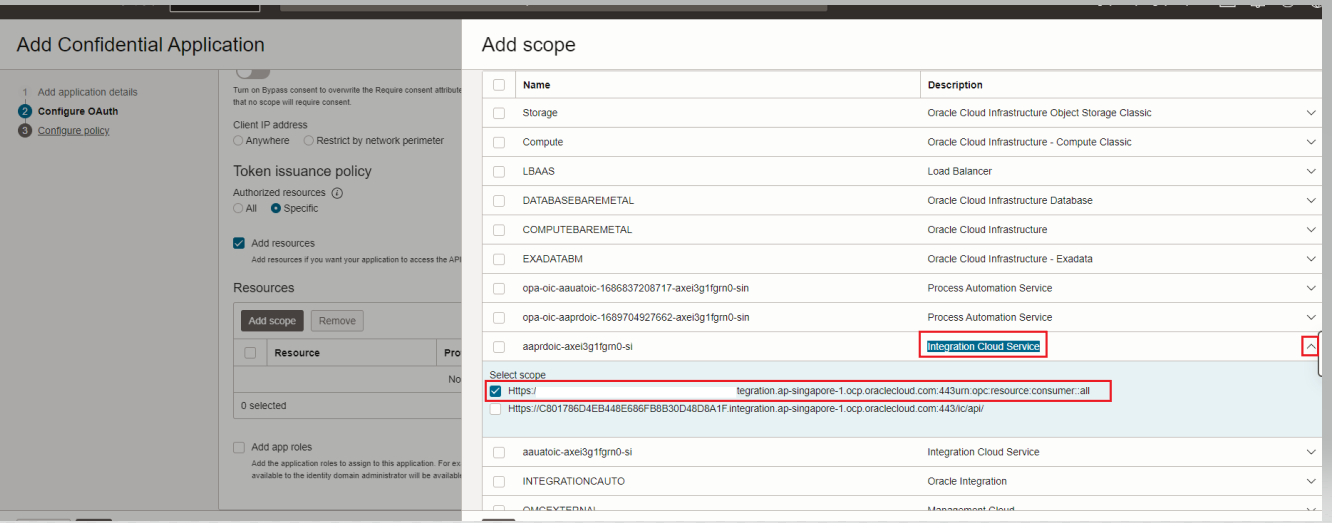
**Client Credentials”**   
**"JWT Assertion"**   
**“Refresh Tokens”**



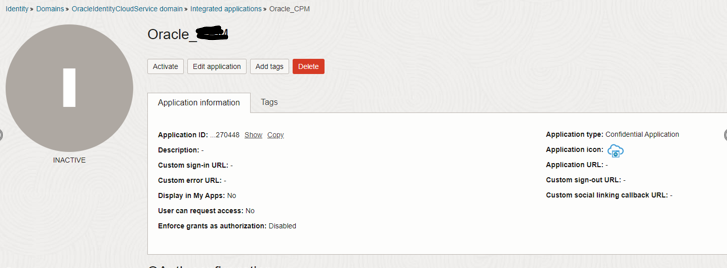
1. Then scroll down and in **Token Issuance Policy** and choose **"Specific"** Authorized Resources radio button then click on **"+Add Resource"** button and then click on **“Add Scope”** to add Prod OIC Service resource in scope.

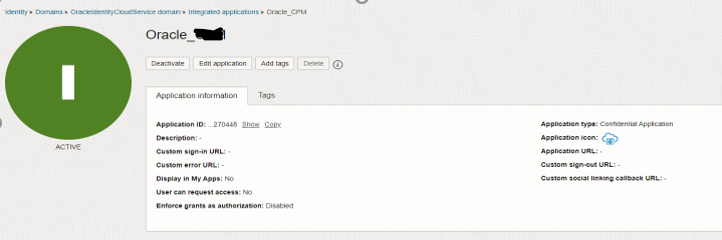


1. In Add Scope Section , Search for Description with Integration Cloud Service and choose the Production Instance. Click on the drop down on the right and choose **resource:consumer:all** URL resource .Click on **"Add"** button to complete the scope selection.

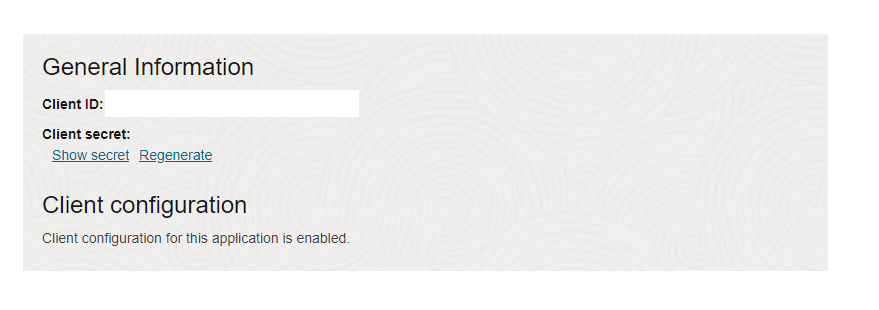


1. Next, Leave rest two tabs i.e. Web Tier Policy and Authorization tabs with default value and click on **"Finish"** button to complete the creation of the confidential application.
2. Activate confidential application by clicking on the **"Activate"** button on the top-right corner and click on the **"OK"** button on the alert shown. This will show the message in the green bar that the application has been activated.

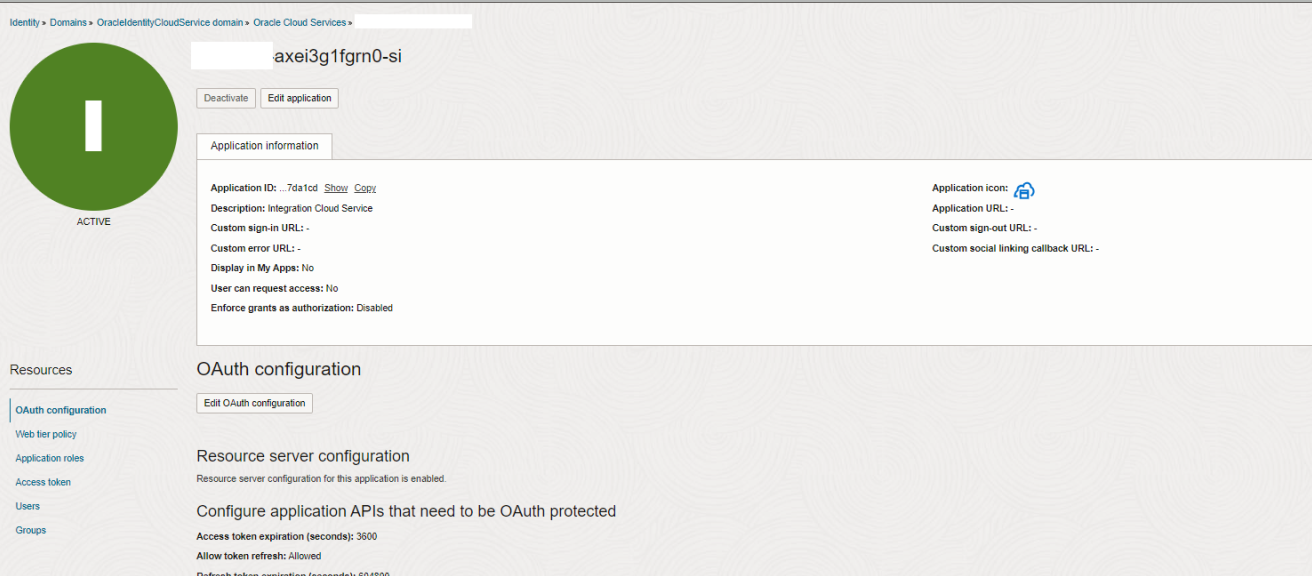




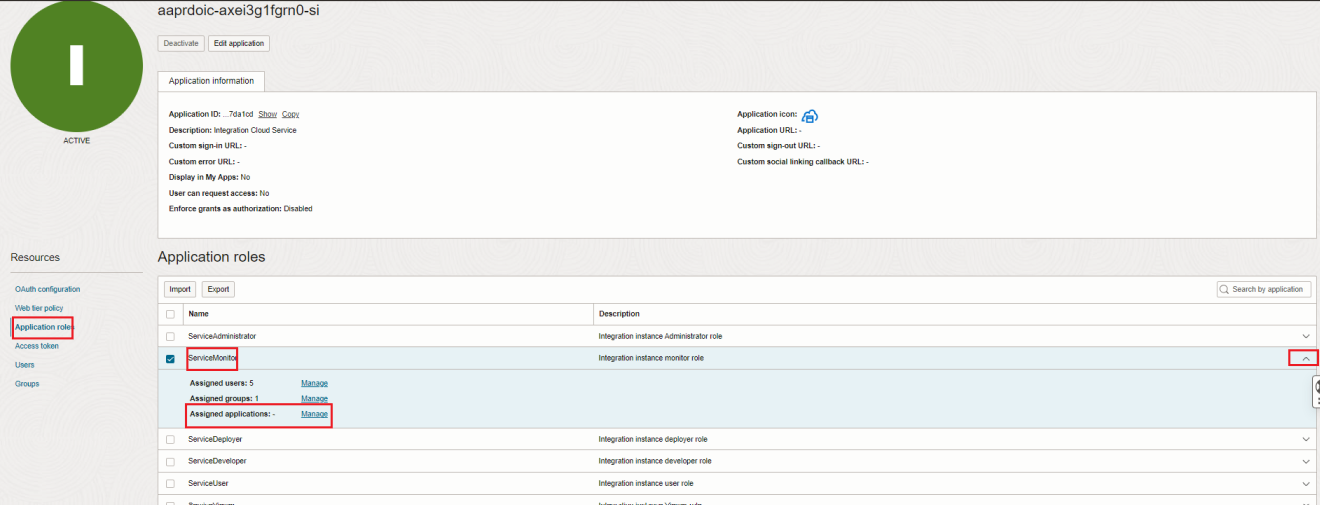
1. In **"General Information"** section **Client ID** is given. To show **Client Secret** click on **"Show Secret"** button. Note down these values which will be required to share at a later stage.



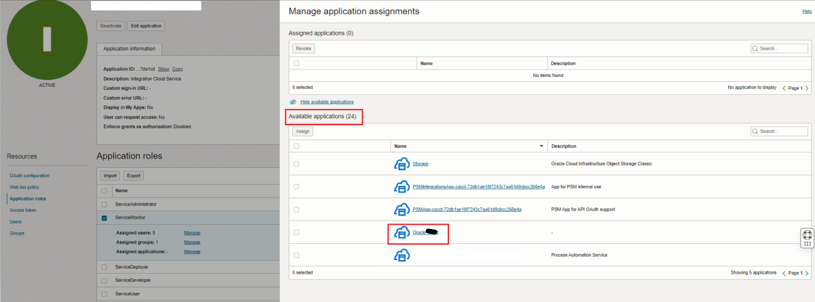
1. Next , Navigate to Overview and Click on **"Oracle Cloud Services"**  and select the Production OIC instance. Open OIC service by clicking on the production environment service name.



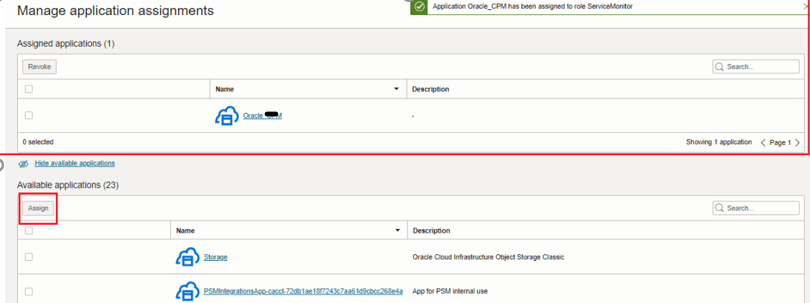
1. Go to **"Application Roles"** tab and click on menu icon on the right of **"ServiceMonitor"** and **"ServiceDeveloper"** role and choose option **"Assign Applications"** and **“Manage”**



1. In the Manage Application Window , Click on Show Available Applications and search for Oracle \_<Your Env Name> Application , select and click on Assign

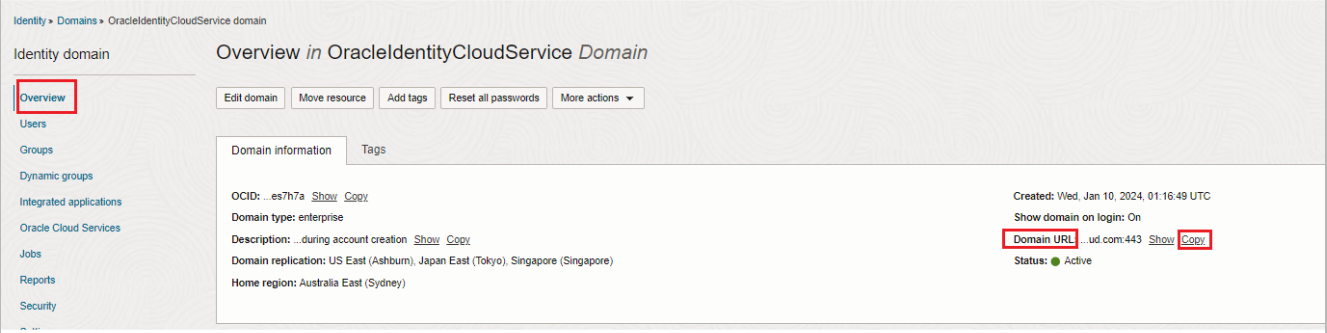


1. In "Assign Applications" window search confidential application created in previous steps, select the application and click on "OK".



We've **successfully** wrapped up the Oracle IAM configuration. We've generated a fresh confidential application for the client ,this application has been activated and is ready for action.

Important Info To Be Shared By Admin To Caller

1. Please Share the below information once all are configured to the caller.
2. Oracle identity Cloud Service URL **– Navigate to Overview Section and click on Copy on the Domain URL.  
     
   **

Get the below information by opening the confidential application that was created

1. Client ID
2. Client secret
3. Scope
4. Access Token URL – Please follow the below syntax.  
   https://**OracleIdentityCloudService Base URL**/oauth2/v1/token
5. Please note that Choose Client Authentication value should be Send as Basic Auth Header