Setting up Oracle Fusion Analytics Warehouse and Single Sign-On

**Authors:**

**Krithika Raghavan,  Director, Oracle Analytics**
**Ravi Guddanti, Principal Member of Technical Staff, Oracle Analytics**
**Veera Raghavendra Koka, Consulting Member of Technical Staff, Oracle Analytics**

## Background:

This blog post walks through the Oracle Fusion Analytics Warehouse (FAW) provisioning process following a FAW order activation. For more details on FAW order activation, please refer to the documentation.

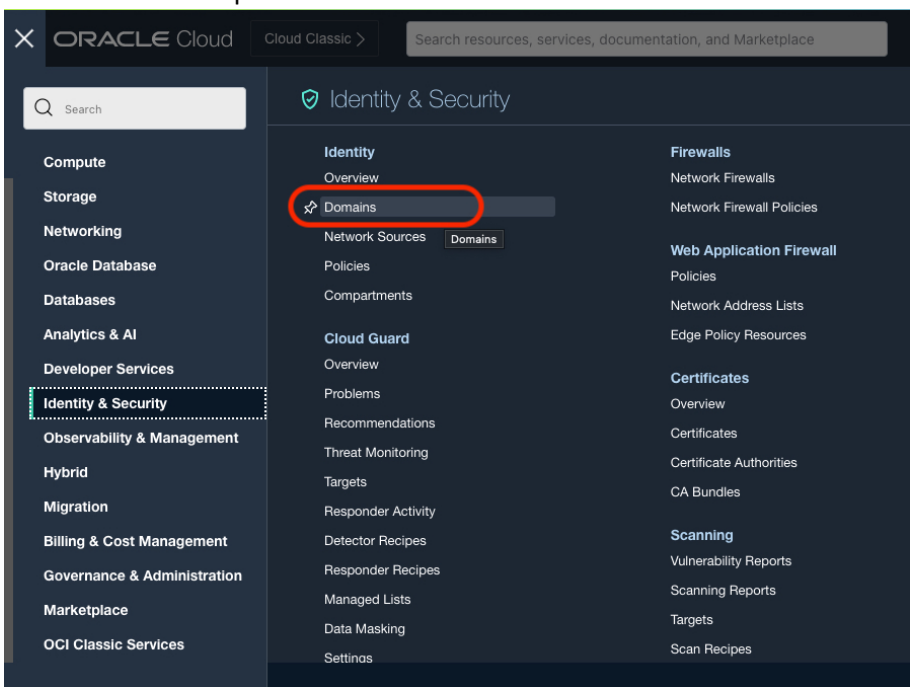
Oracle is merging IDCS with OCI IAM. We're standardizing on the OCI branding. Hence, the updated service is called OCI IAM. It's a native OCI service available in all regions and integrated with other OCI services.

The steps to enable single sign-on, so that users from Oracle Applications Cloud can access Oracle Fusion Analytics Warehouse (FAW), vary depending on the scenarios identified in the Support Matrix section.

You must set up single sign-on before you create your FAW instance.

Prior to setting up single sign-on, verify if your Oracle Cloud account offers Identity Domains (post migration to OCI IAM) or not?

- Log into your Oracle Cloud account.
- From the Oracle Cloud Infrastructure left navigation menu, click **Identity & Security** and verify that the **Domains** option is available.



## Support Matrix:

Depending on when you created the Oracle Cloud account for Oracle Applications Cloud and in which Oracle Cloud account you activated Oracle Fusion Analytics Warehouse (FAW), the steps to sync users may vary.

Listed below are various scenarios.

| | FAW activated in the same Oracle Cloud account as Oracle Applications Cloud | FAW activated in a different pre-existing Oracle Cloud account (pre-migration to OCI IAM) | FAW activated in a different new Oracle Cloud account (brand new post migration to OCI IAM) |
|---|---|---|---|
| Existing Oracle Applications Cloud (prior to migration to OCI IAM) | Scenario #1 | Scenario #3 | Scenario #5 |
| New Oracle Applications Cloud (post migration to OCI IAM) | Scenario #2 (Recommended Approach) | Scenario #4 | Scenario #6 |

**Steps to Complete:**

**Scenario #1**
Existing Oracle Applications Cloud (prior to migration to OCI IAM)
FAW activated in the same Oracle Cloud account as Oracle Applications Cloud

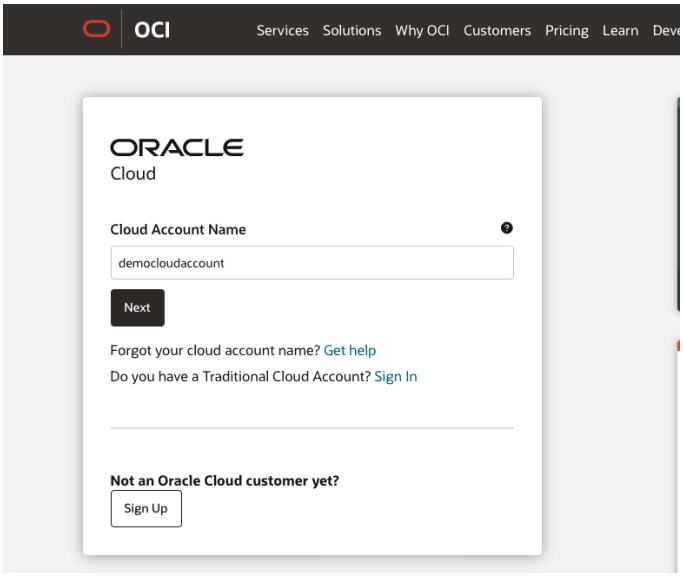
Steps:

Perform the steps outlined in
https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement
The Oracle Cloud account mentioned in steps #3 and #4 are one and the same.

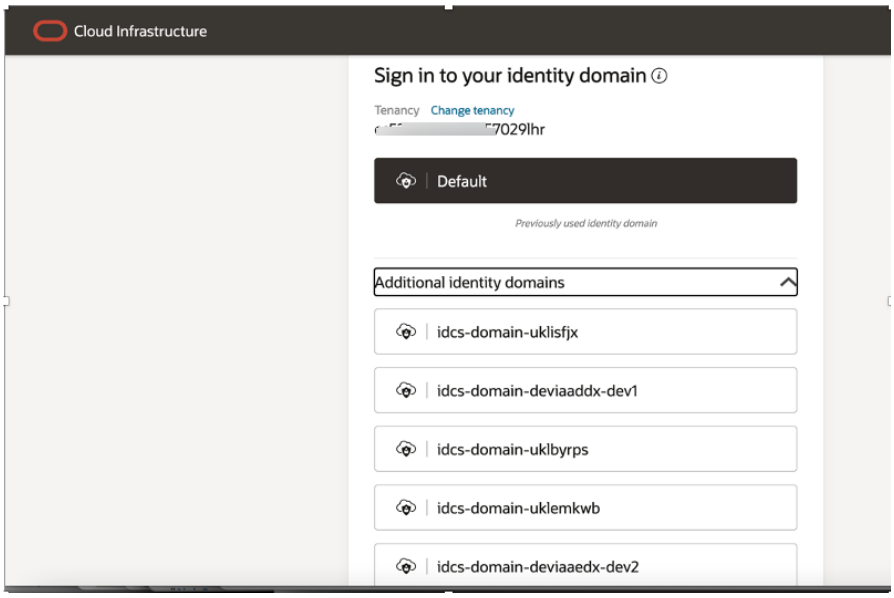
**Scenario #2**
New Oracle Applications Cloud (post migration to OCI IAM)
Fusion Analytics Warehouse activated in the same Oracle Cloud account as Oracle Applications Cloud

Steps:

1. Identify the pod that will serve as the source Oracle Applications Cloud for the Fusion Analytics Warehouse instance.
2. As the Oracle Cloud account administrator, sign into the Oracle Cloud account where both Oracle Applications Cloud and Fusion Analytics Warehouse services have been activated.




3. Choose the domain that's corresponding to the underlying Oracle Applications Cloud source.




4. Create the following OCI policy to enable a specific group of users to create and manage the FAW instances on the tenancy:
   Example:

Allow group '<DomainName>'/'<GroupName>' to manage analytics-warehouses in tenancy
Allow group '<DomainName>'/'<GroupName>' to manage analytics-instances in tenancy
Allow group '<DomainName>'/'<GroupName>' to manage autonomous-database-family in tenancy

5. Follow Steps to create Fusion Analytics Warehouse Instance by referencing Step 5 on the blog https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement

**Scenario #3**
**Existing Oracle Applications Cloud (prior to migration to OCI IAM)**
**FAW activated in a different pre-existing Oracle Cloud account (pre-migration to OCI IAM)**

Steps:

Perform all the steps outlined in
https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement

**Scenario #4**
**New Oracle Applications Cloud (post migration to OCI IAM)**
**FAW activated in a different pre-existing Oracle Cloud account (pre-migration to OCI IAM)**

Steps:

Perform steps outlined in the following blog
https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement

You can skip Steps 1 and 2 from the blog assuming the synchronization has been preconfigured.

If the synchronization is not pre-configured, then go through the following steps to enable it:

1. Sign into the Oracle Cloud account where Oracle Applications Cloud is hosted.
2. Navigate to the Identity Domain home page of the corresponding Fusion environment. (OCI Console -> Identity & Security -> Domains -> Click on the Domain for the Fusion environment being used for FAW provisioning.)
3. Click on Oracle Cloud Services on the left menu options.
4. Click on the application "Oracle Applications Cloud (Fusion)"
5. Go to Provisioning -> Enable Provisioning
6. Select Authoritative Sync check box, also Enable Synchronization
7. Save and Import.

For Step 3 in the blog, when adding the Identity Provider to the OCI tenancy where FAW is activated, use the Domain URL associated with the Oracle Applications Cloud.

**Scenario #5**
**Existing Oracle Applications Cloud (prior to migration to OCI IAM)**
**FAW in a different new Oracle Cloud account (Brand new post migration to OCI IAM)**

The steps needed to support this include:

- Synchronizing Users and Groups from Oracle Applications Cloud IDCS instance to Identity Domain on new Oracle Cloud account using GenericScim – Client Credential template from App Catalog.
- Source IDCS Instance: Fusion Applications IDCS
- Destination Identity Domain: FAW Tenancy's IDCS Domain

Steps:

1. Synchronization of Oracle Applications Cloud users and roles with the IDCS instance. Refer to steps 1 and 2 from the following blog https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement
2. Create an identity domain in your FAW Oracle Cloud account and login to the OCI Console as the default domain user – see Appendix A.
3. Configure the GenericSCIM template on the new identity domain – see Appendix B.
4. Configure single sign-on between Oracle Applications Cloud and FAW – see Appendix C.
5. Create an OCI policy that authorizes identity domain users to create FAW instances – see Appendix D.
6. Create FAW instance – Step # 5 from https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement
7. Create an identity provider policy for single sign-on – see Appendix E.

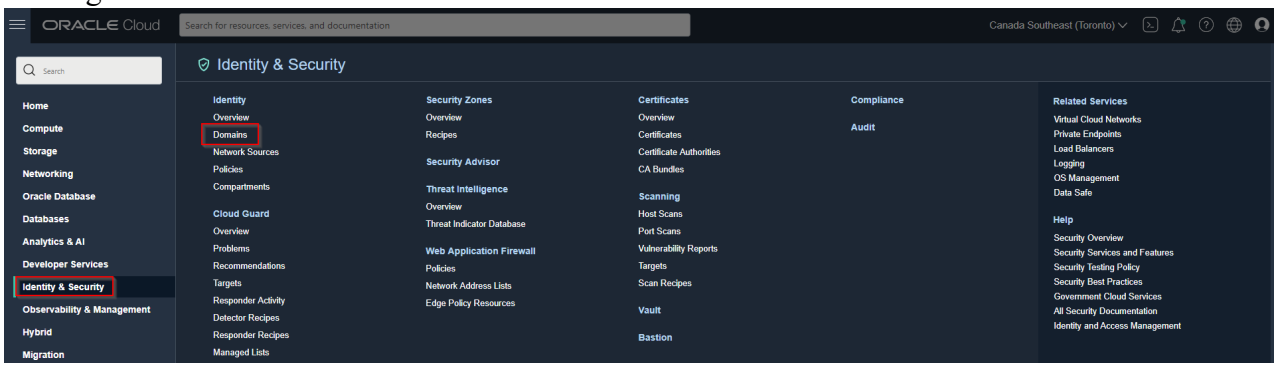
**Scenario #6**
**New Oracle Applications Cloud (post migration to OCI IAM)**
**FAW in a different new Oracle Cloud account (Brand new post migration to OCI IAM)**

1. Identify the pod that will serve as the source Oracle Applications Cloud for Fusion Analytics Warehouse instance.
2. Create an identity domain in your FAW Oracle Cloud account and login to the OCI Console as the default domain user – see Appendix A.
3. Configure the GenericSCIM template on the new identity domain –see Appendix B.
4. Configure single sign-on between Oracle Applications Cloud and FAW – see Appendix C.
5. Create an OCI policy that authorizes identity domain users to create FAW instances – see Appendix D.
6. Create FAW instance – Step # 5 from https://blogs.oracle.com/analytics/post/fusion-analytics-warehouse-idcs-sync-and-sso-enablement
7. Create an identity provider policy for single sign-on – see Appendix E.

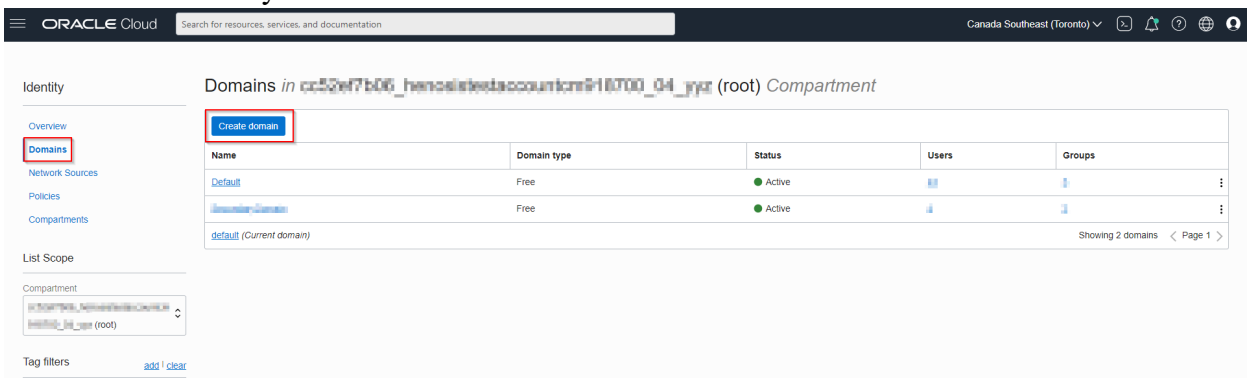
Appendix

## Appendix A: Create an Identity Domain in Your FAW Oracle Cloud Account and Login to the OCI Console as the Default Domain User

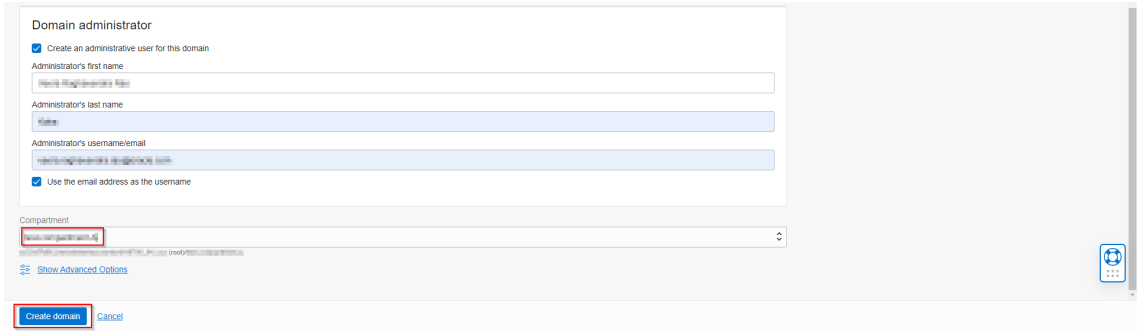
1. Login to OCI Console as the default domain user.




2. Create an identity domain.




3. Choose Domain Type – Free.
   (Note: The limits mentioned for Free domain type do not apply for FAW, please ignore)

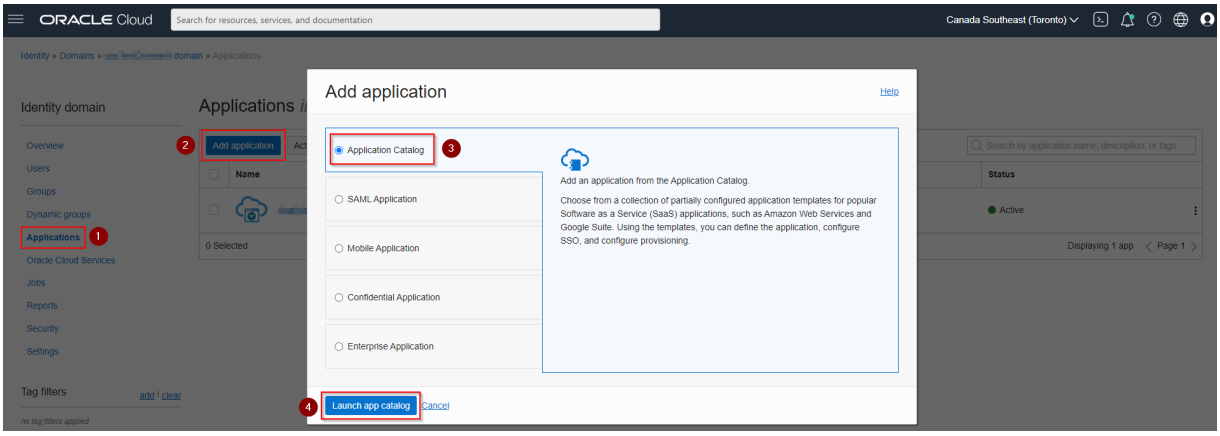



4. Enter the administrative user details for the new identity domain and select the compartment in which you want to create the Domain.
5. Click Create Domain.

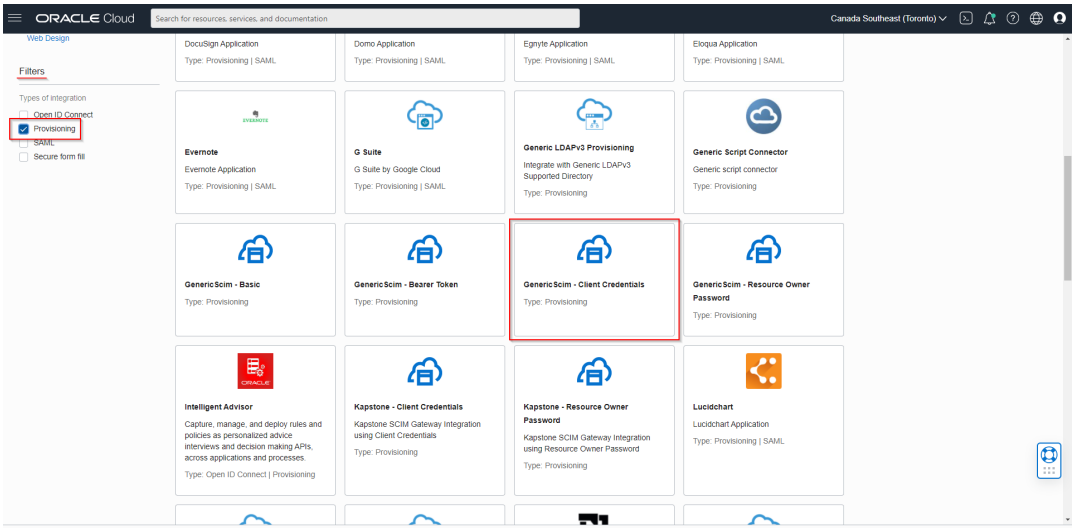
## Appendix B: Configure the GenericSCIM Template on the New Identity Domain

Configure a GenericSCIM Template on destination identity domain created as part of step 2 above, for enabling synchronization of users, roles, role mappings from the source instance.

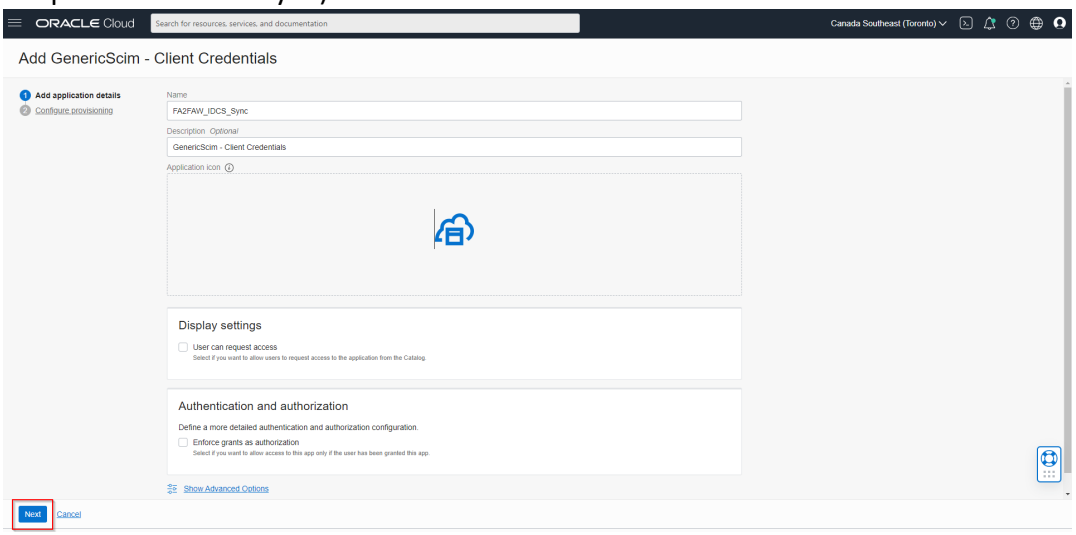
1. Sign in to the OCI Console using the new identity domain.
2. From the left navigation menu go to Identity & Security -> Domains. Click on the Domain that was created as part of Step 2.
3. Click on Applications -> Add Application -> Launch Application Catalog.



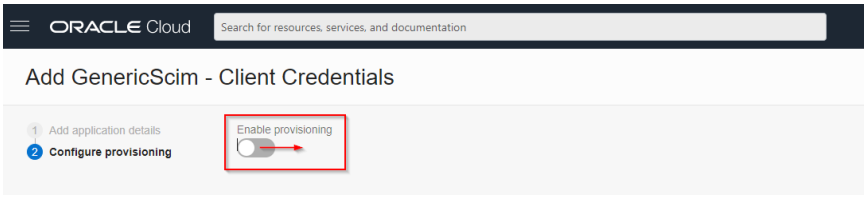

4. In the App Catalog page, search for GenericScim, and then click Add for the GenericScim - Client Credentials.

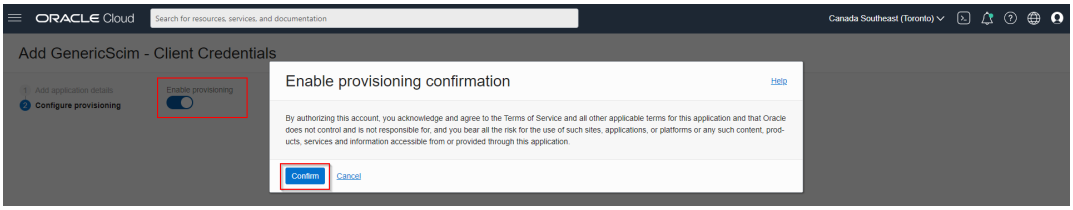


5. In the Add GenericScim - Client Credentials page, enter a name (example FA<podname>IDCS-Sync).

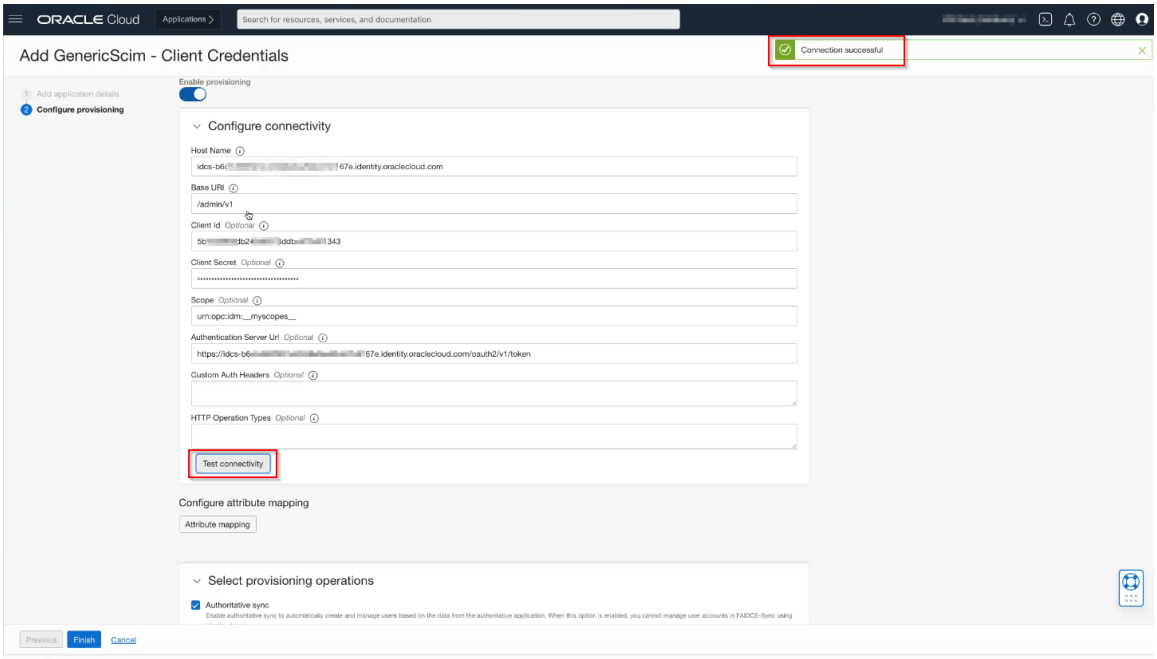



6. In the Provisioning pane, click Enable Provisioning, and then click Confirm in the Enable Provisioning confirmation window.

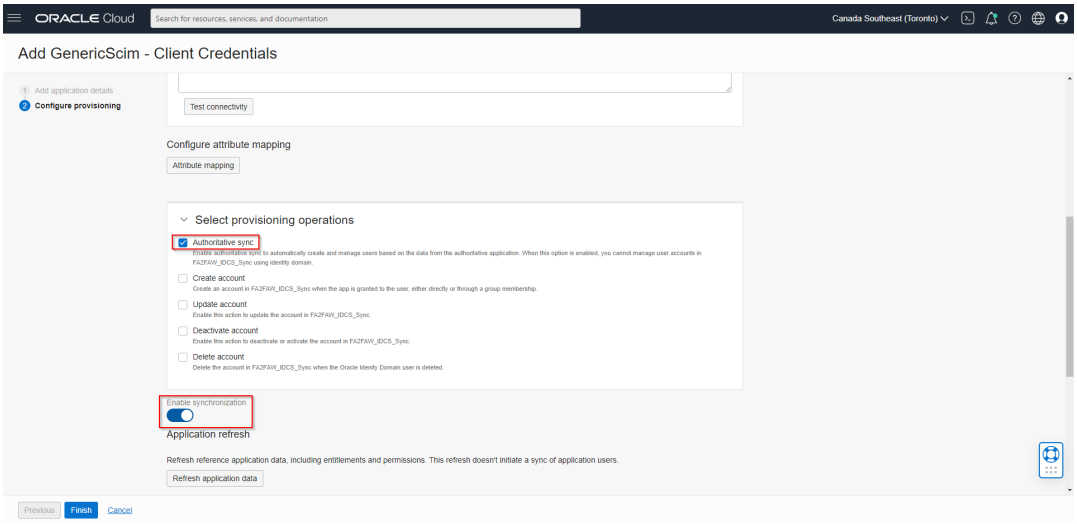



7. In the Configure Connectivity section, provide the following information (of source IDCS or Identity from where the Users are going to be synchronized):
    a. Host Name: For example, idcs-source.identity.oraclecloud.com
    b. Base URI: /admin/v1
    c. Client Id: Enter the Client ID you made note from the confidential application.
    d. Client Secret: Enter the Client Secret you made note from the confidential application.
    e. Scope: urn:opc:idm:__myscopes__
    f. Authentication Server Url: For example, https://idcs-source.identity.oraclecloud.com/oauth2/v1/token

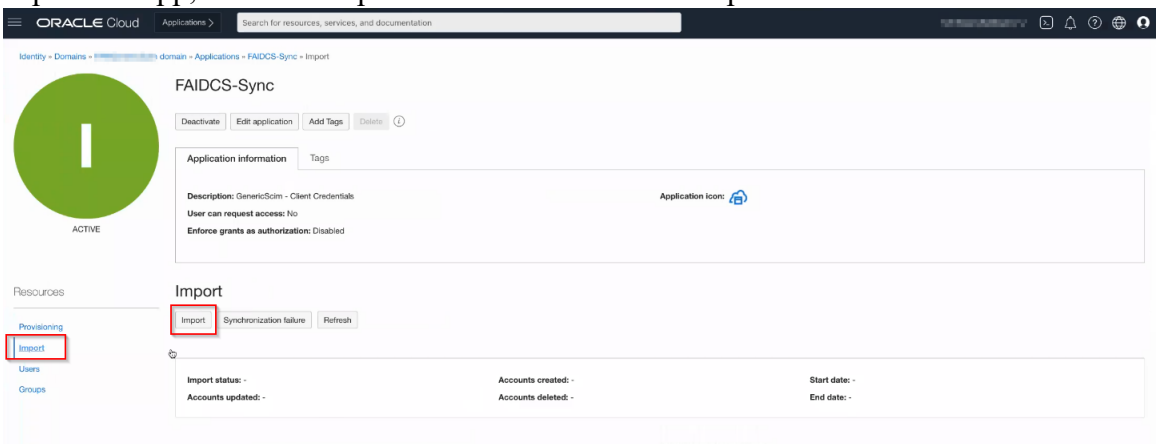



8. Click Test Connectivity to test the communication between the source and target identity instances. Verify the test connection is successful.
9. In Select Provisioning Operations section, click Authoritative Sync.




10. Click Enable Synchronization, and then click Save.
11. Pick a refresh schedule (Every Day or Every Hour).
12. Click Activate to activate the application.

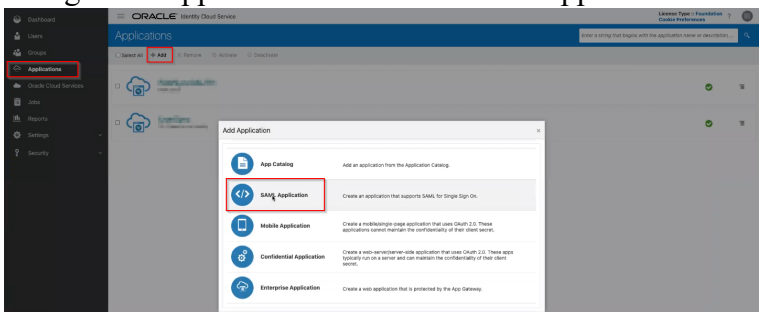
13. Open the App, click the Import tab and then click on Import button.

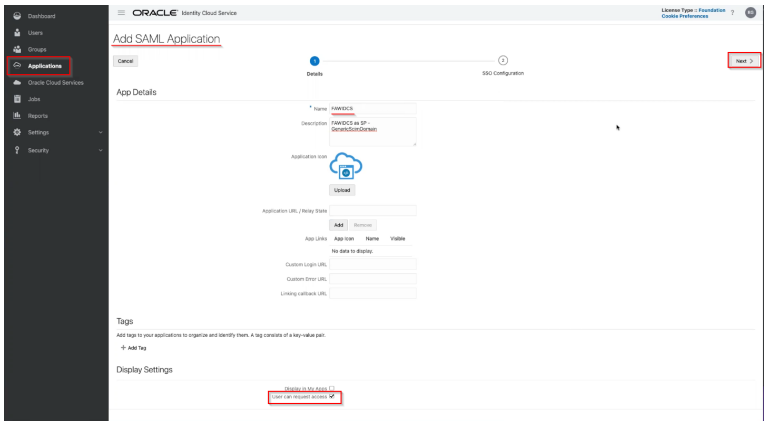



After the job finishes, the list of users and groups synchronized from the source identity appears.

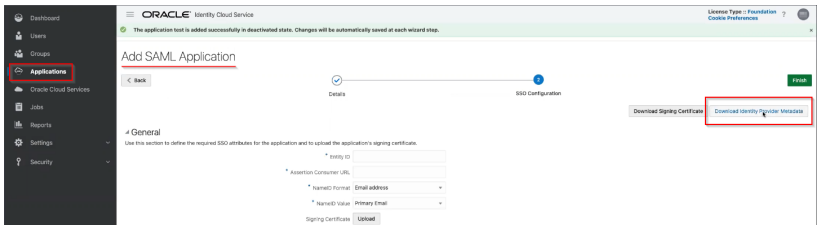
## Appendix C: Configure Single Sign-On between Oracle Applications Cloud and FAW

1. Login to FA's IDCS adminconsole if FA uses Oracle IDCS for identity management. If FA uses Identity Domains for identity management, then login to Oracle Cloud Infrastructure Console.
2. Navigate to Applications  Add  SAML Application.

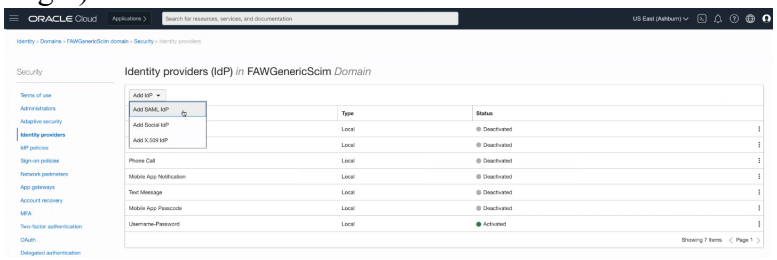


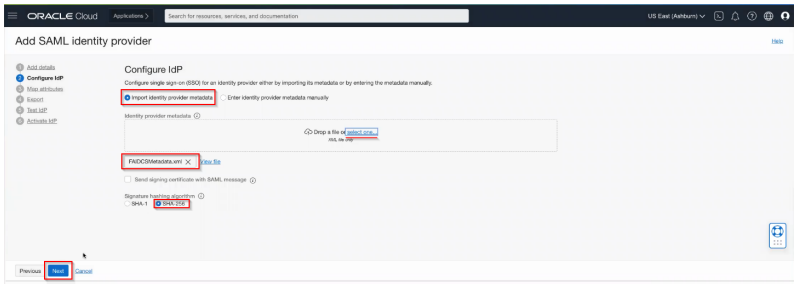

3. Check "User can request access" (Required so that the user need not be explicitly provisioned to the App).

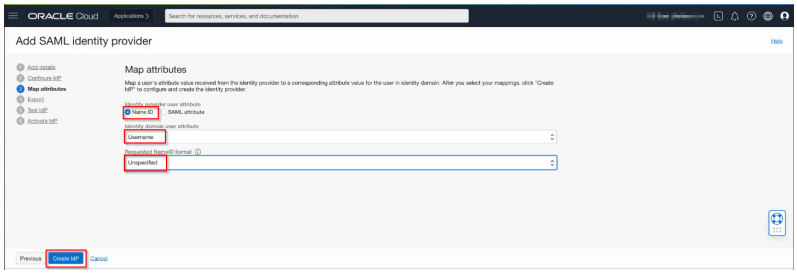



4. Download the FA's IDCS (IDP) Metadata XML file. Save to Local Machine.
5. Pause the configuration of this SAML App here and go to FAW Identity Domain (that was created as part of Appendix 1 above) for further configuration, we will resume this step after completing the following setup on FAW domain.
6. Login to FAW OCI Console.
7. Navigate to FAW Domain (Identity & Security -> Domains)  Security -> Identity Providers  Add IdP  Select "Add SAML IdP" -> Name (for example Fusion SSO Login).



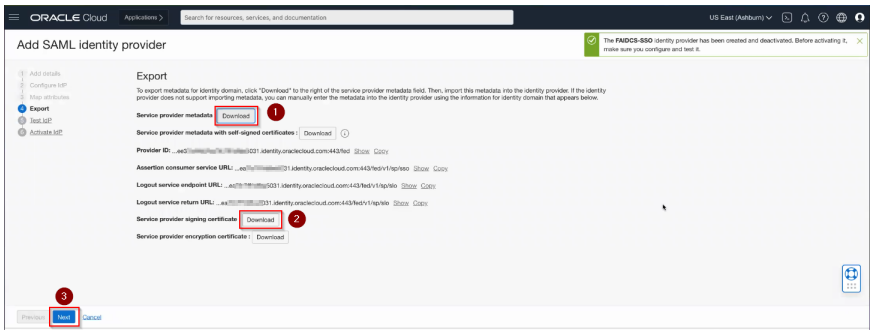

8. Import the FA's IDCS SAML IDP Metadata XML File which was download previously to the Local Machine.



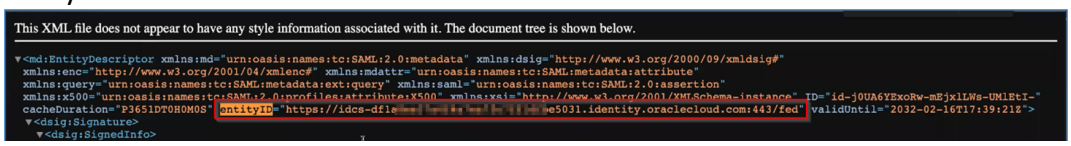




NOTE: Select Unspecified if FA IDCS Username can be email or short name. In case of FA IDCS username is email, select EmailAddress.

9. Download the FAW IDCS Domain SP Metadata XML file and its Signing Certificate.

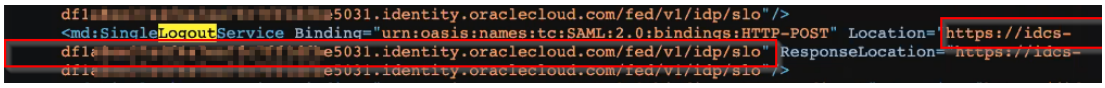



10. Open the SP-FAW-IDCS-Domain-Metadata.xml file saved in the above step in a text editor and capture below values:
entityID:

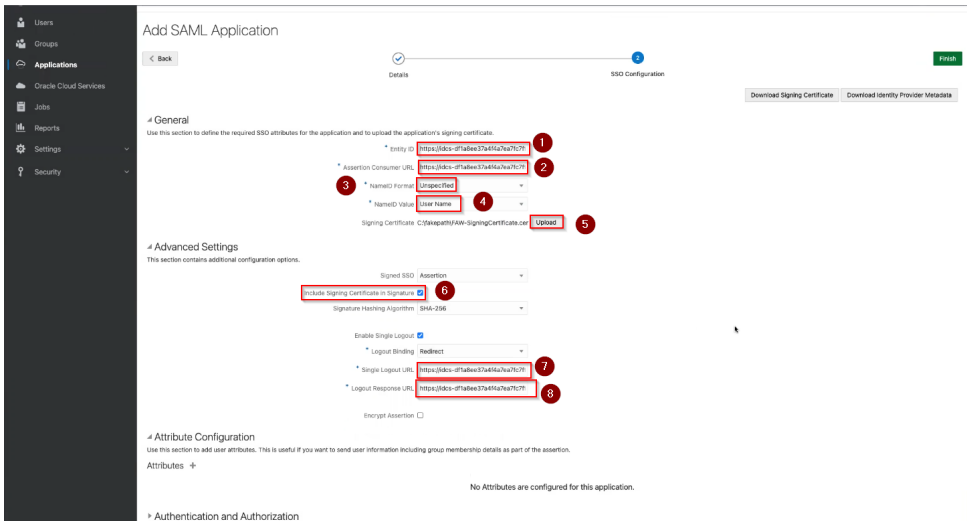



AssertionConsumerService:

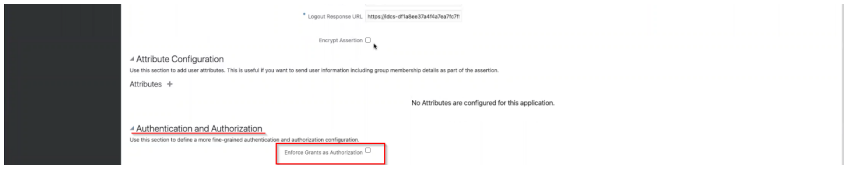

SingleLogoutService:



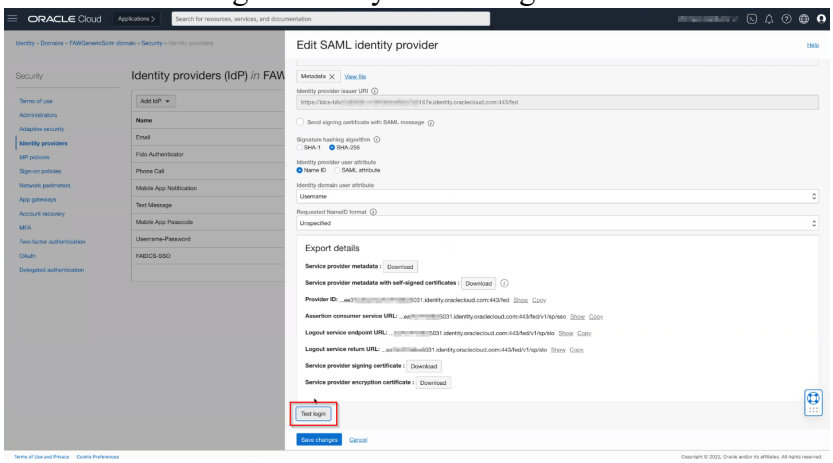

11. Continue configuring the SAML Application created in FA's IDCS adminconsole in previous steps (Resume step d. above).
Using the FAW IDCS Domain SP Metadata XML file and the Signing Certificate, fill in the details as shown in the screenshot below:



12. Expand the Authentication and Authorization section and make sure the "Enforce Grants as Authorization" Option unchecked.
13. Click "Finish" and Activate.

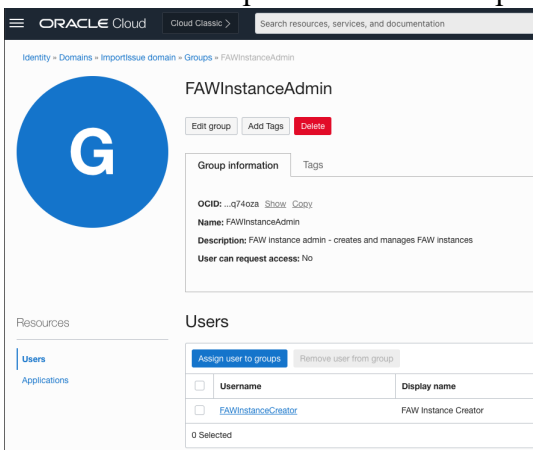



14. Switch back to FAW domain - edit the SAML IDP in the FAW Identity Domain and Click on "Test Login". Verify the test login is successful.

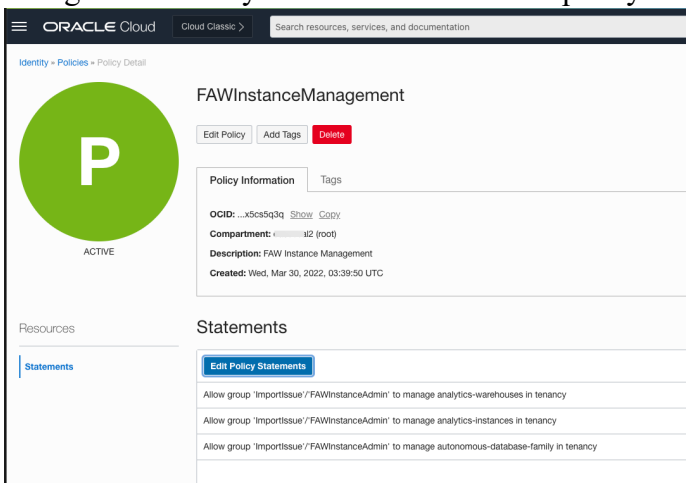



## Appendix D: Create an OCI Policy that Authorizes Identity Domain Users to Create FAW Instances

1. Sign into the Oracle Cloud account using Default identity domain as domain administrator
2. Navigate to Identity -> Domains -> click on the domain name where FAW instance will be created -> Groups -> Create a Group and assign user(s)



3. Navigate to Identity -> Policies -> Create a policy on the Group created above

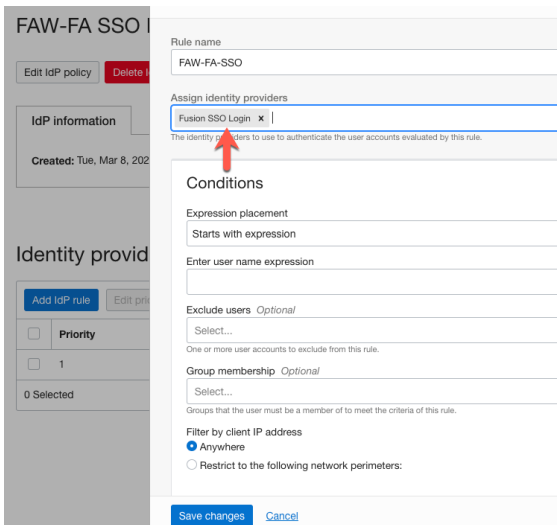



Allow group '<DomainName>'/'<GroupName>' to manage analytics-warehouses in tenancy
Allow group '<DomainName>'/'<GroupName>' to manage analytics-instances in tenancy
Allow group '<DomainName>'/'<GroupName>' to manage autonomous-database-family in tenancy

## Appendix E: Create an Identity Provider Policy for Single Sing-On

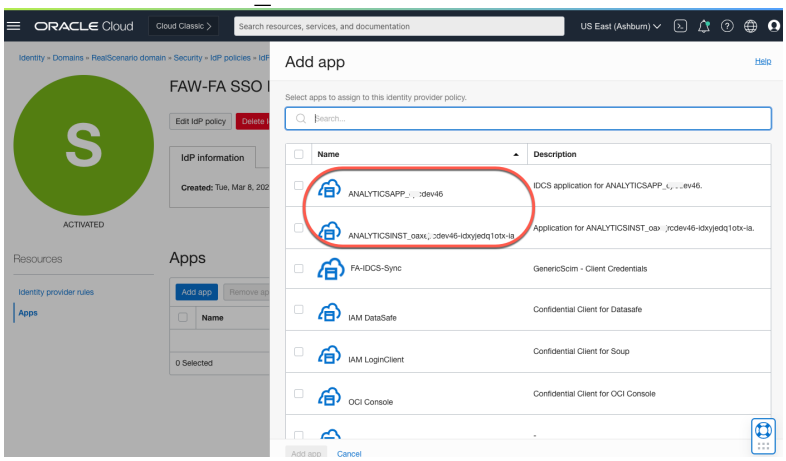
Following steps ensure that the FAW login page has an option to sign in with Oracle Applications Cloud (SSO).

1. OCI Console -> Navigate to FAW Domain -> Security -> IdP policies
2. Click on Create IdP Policy button to add a new policy
3. Add IdP rule – assign the SAML IDP created as part of Appendix C above "**Configure Single Sign-On between Oracle Applications Cloud and FAW**"




4. Add the Analytics apps that get created as part of FAW instance creation. ANALYTICSAPP_<faw-instance-name>

ANALYTICSINST_oax<faw-instance-name>-<id>




5. After this setup, you see an option to sign in with Fusion SSO on the FAW login page.