Oracle® Banking Enterprise Default Management

User Provisioning Guide

Release 2.11.0.0.0

F36758-01

December 2020

ORACLE®

Oracle Banking Enterprise Default Management User Provisioning Guide, Release 2.11.0.0.0

F36758-01

Contents

List of Tables

List of Figures

Preface

This document covers the functional flow and detailed configuration required for provisioning users in Collections using OIM or DB based configuration. OIM Reconciliation and Schedule jobs are not in scope.

This preface contains the following topics:

Audience

This document is intended for the following:

- IT Deployment Team
- Consulting Staff
- Administrators

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at

http://www.oracle.com/us/corporate/accessibility/index.html

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support.

For information, visit http://www.oracle.com/us/corporate/accessibility/support/index.html#info or visit http://www.oracle.com/us/corporate/accessibility/support/index.html#trs if you are hearing impaired.

Organization of the Guide

This document contains:

Chapter 1 About this Guide

This chapter provides details about the applicability of this guide.

Chapter 2 Introduction

This chapter presents an overview of user provisioning.

Chapter 3 Configuration

This chapter provides information on configuring OIM and DB for user provisioning.

Chapter 4 User Fields and Constraints

This chapter provides information on the user provisioning fields and related constraints.

Chapter 5 Create, Modify, Delete Users using OIM

This chapter provides information on user provisioning activities using OIM.

Chapter 6 Create, Modify, Delete Users using DB Based Configurations

This chapter provides information on user provisioning activities using DB based configurations.

Chapter 7 Verification

This chapter provides information on verification of OIM configuration performed.

Related Documents

For more information, see the following documentation:

- For information on the configuration that should be performed on day zero, see the Oracle Banking Enterprise Default Management Day Zero Setup Guide.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 About this Guide

This guide is applicable for the following products:

- Oracle Banking Platform (Oracle Banking Collections and Oracle Banking Recovery)
- Oracle Banking Enterprise Default Management (Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery)

References to Oracle Banking Platform or OBP in this guide apply to all the above mentioned products.

2 Introduction

In Oracle Banking Platform (OBP), users are maintained in a centralized repository, either in Oracle Internet Directory (OID) or in DB based repository. This repository is used for authentication and authorization purpose.

Oracle Banking Enterprise Collections module has its own authentication and authorization process. Users configured in the OBP require access to some of the services of Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery. To access those services, user must be present in the Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery database. Hence, the user provisioned in OBP is required to be provisioned in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery module as soon as it is created in OBP. A typical Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery request flow from online OBP user is authenticated and authorized by the OBP framework and is forwarded to the Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery module. Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery uses the user detail to create context to fetch underline service to serve the request.

Users are provisioned in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery when they are created in OBP.

3 Configuration

This chapter details the configuration required for Oracle Identity Manager (OIM) and DB.

3.1 Prerequisites for OIM Configuration

Following is the list of prerequisites for configuring OIM:

1. You must install the following software:
   - Weblogic Server 12.2.1.4.0
   - SOA Suite 12.2.1.4.0
   - IAM Suite 12.2.1.4
   - RCU 12.2.1.4
2. You must have administrative access to the following:
   - Oracle Identity System Administration http://<Host>:<Port>/sysadmin/
   - Oracle Identity Self Service http://<Host>:<Port>/identity/
   - Oracle Directory Services Manager (ODSM). For more information, see Chapter 7.1 Verification of OIM Configuration.
3. URL of OID to which OIM is synchronized is known. Also, must have administrative access to ODSM to connect OID.
4. Check following artifacts are available as part of Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery release bundle:
   - collections_oim_export.xml

3.2 Create System User

The following configuration is to create Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery System User for OIM. System User is required to authenticate OIM Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery user provisioning request at OBP server.

Note

It is assumed OBP default User and Role (Application Role Enterprise Role) configuration is already seeded in OID.

1. Create user with User ID **OIMOBPCOLL** using ODSM. Provide necessary User attributes.
2. Assign enterprise Role **Administrators** to User.
3. Create same user in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery using native Collections Admin Application UI. Assign **CLNHOSTUSER** Group to User, to provide minimum access of native admin screen. For more information, see Section 7.3 Create Users in Collections Admin Application

3.3 OIM Configuration

This section provides information on OIM Configuration.

3.3.1 Import Configuration

Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery connector configuration for User Provisioning must be imported. Below is the list of artifacts developed for Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Provisioning.

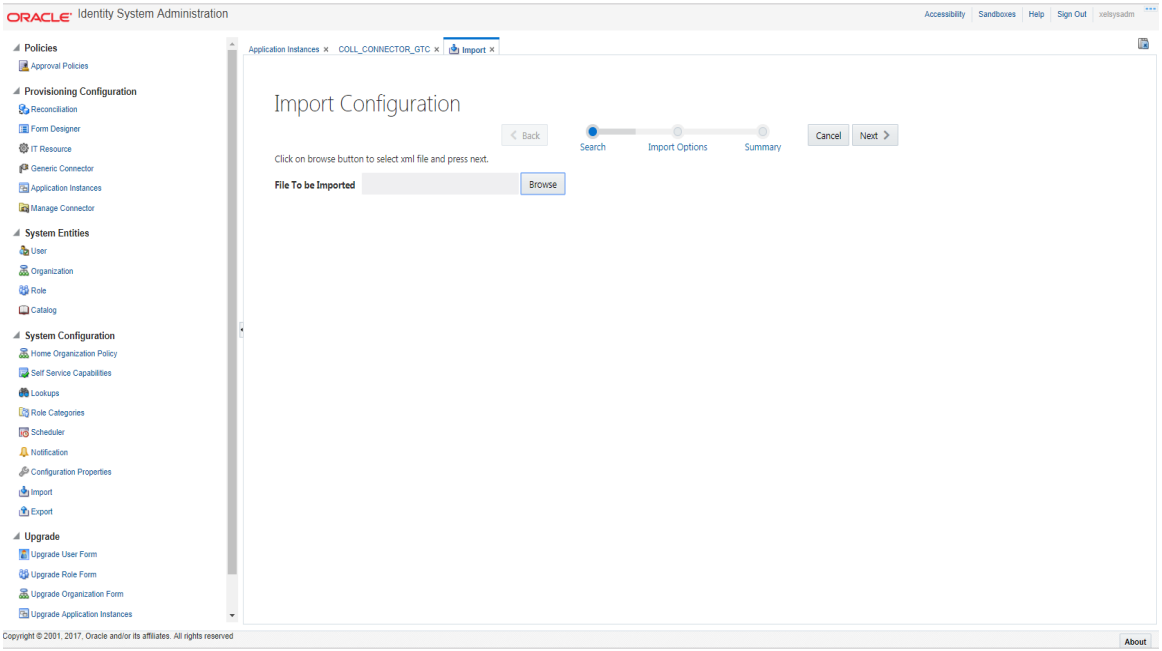
Table 3–1 Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Provisioning Artifacts

Artifact	Artifact Type	Description
COLL_CONNECTTOR_GTC	IT Resource Definition	It stores definition of connection parameters to connect Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery system.
Xellerate Users	Organization	
adpCOLL_CONNECTOR_GTC_AUTOC	Event Handler	
adpCOLL_CONNECTOR_GTC	Event Handler	
UD_ORMBCONN	Form	
UD_ORMUSERG	Form	
COLL_CONNECTOR	Generic Connector	

Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery configuration can be imported in OIM by using Oracle Identity System Administration.

1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Import**.

Figure 3–1 Oracle Identity System Administration - Import Configuration Screen



3. Click **Browse** to import the configuration xml file and click **Next**.

Figure 3–2 Browse the file to be imported

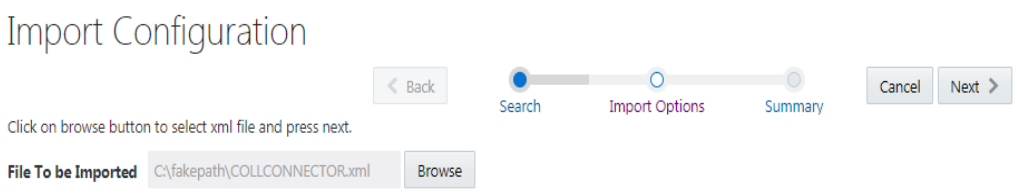
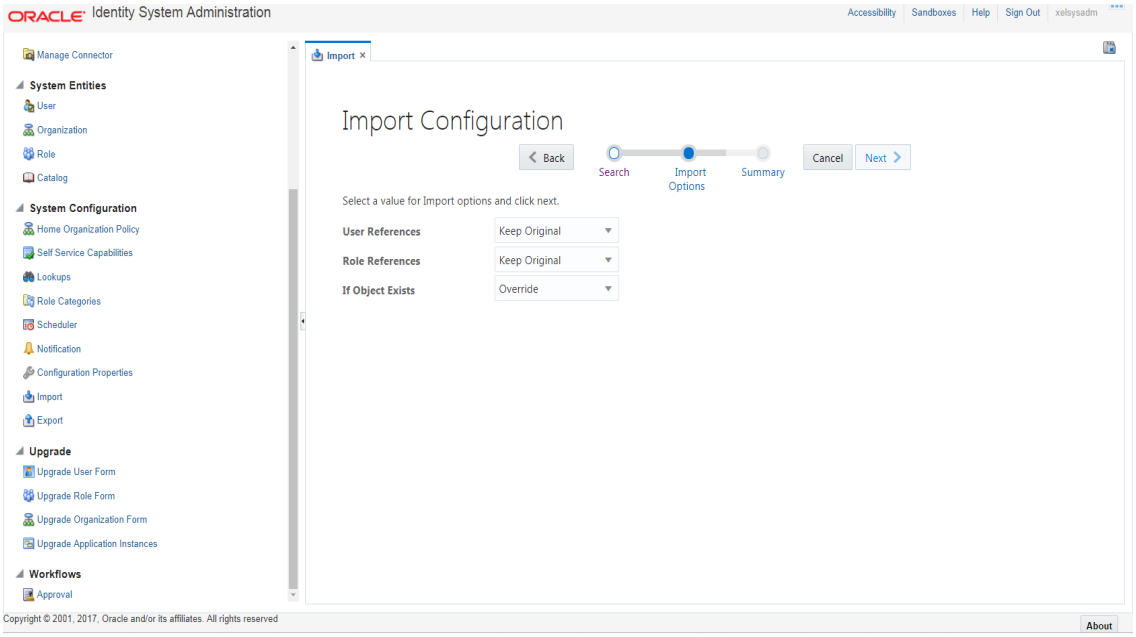
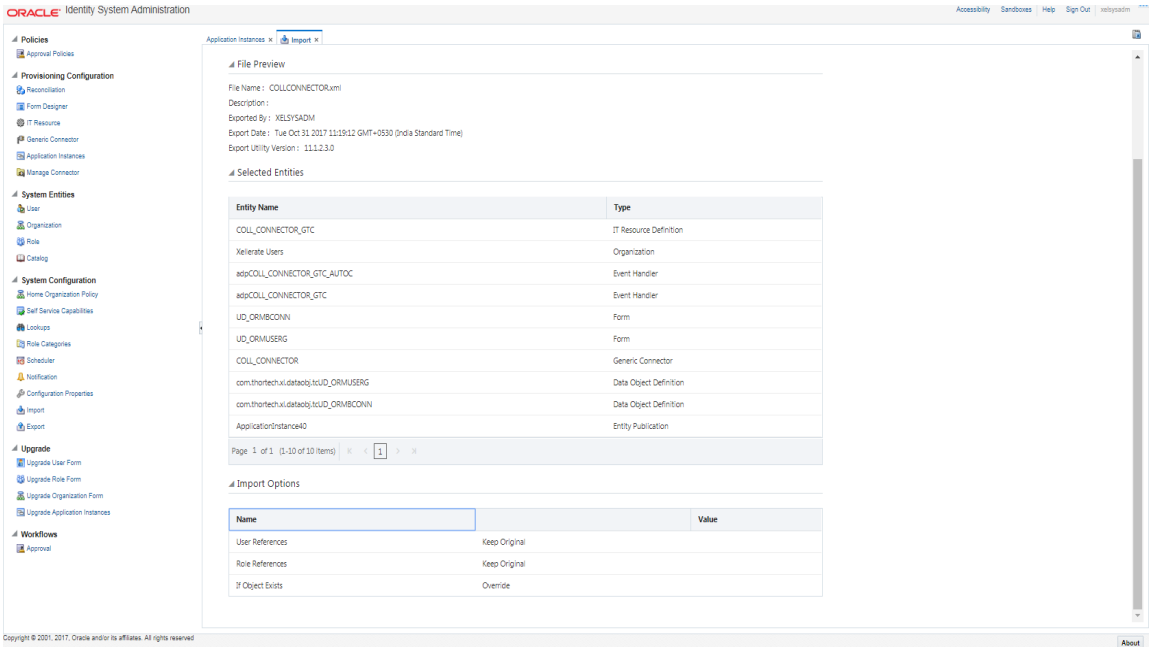


Figure 3–3 Import Options



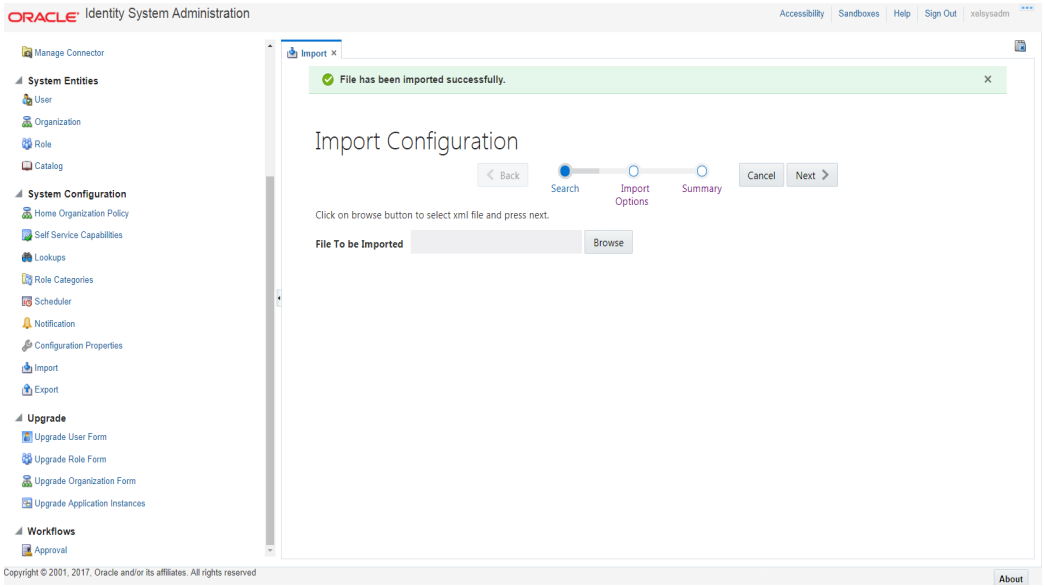
4. Click **Next**.

Figure 3–4 Summary of the import



5. Click **Import**.
6. On successful import of data,**File has been imported successfully** message will be displayed.

Figure 3–5 Successful Import Message

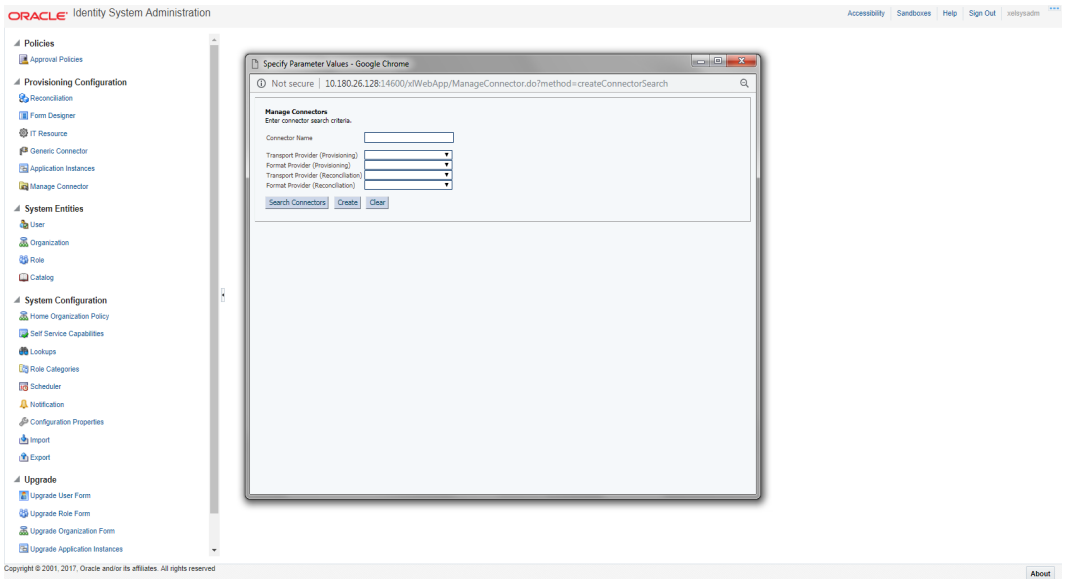


3.3.2 Manage Generic Technology Connector

Following Run-Time Parameters need to be set.

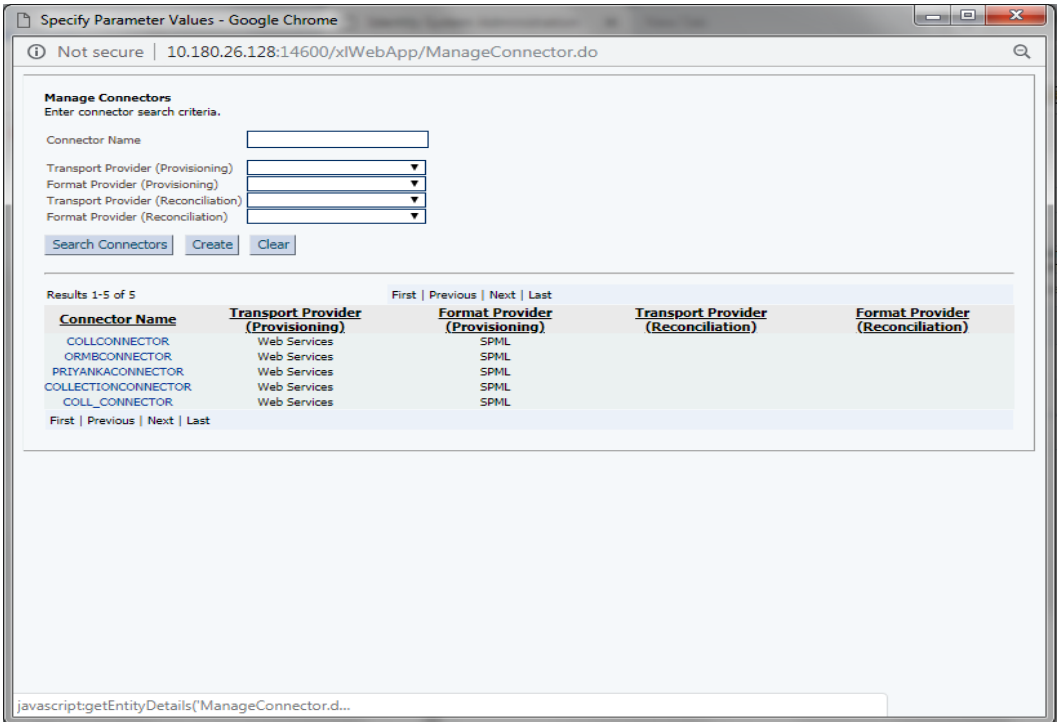
1. In the left pane, click **Generic Connector**. Following window appears.

Figure 3–6 Generic Connector



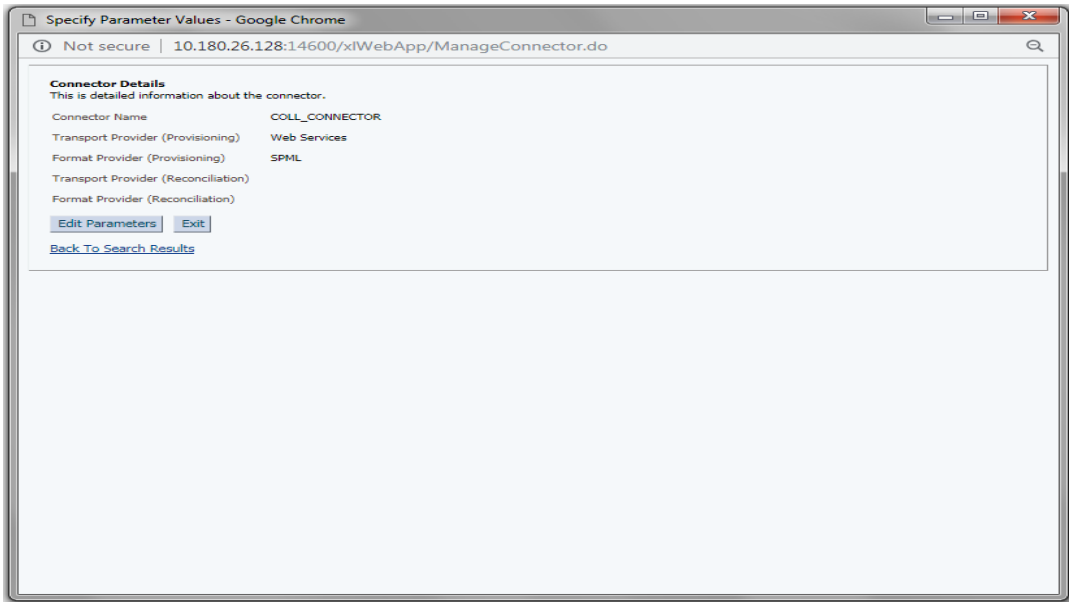
2. Click **Search Connectors** and click **COLL_CONNECTOR**.

Figure 3–7 Search Connectors



3. Click **Edit Parameters**.

Figure 3–8 Edit Connector Parameters

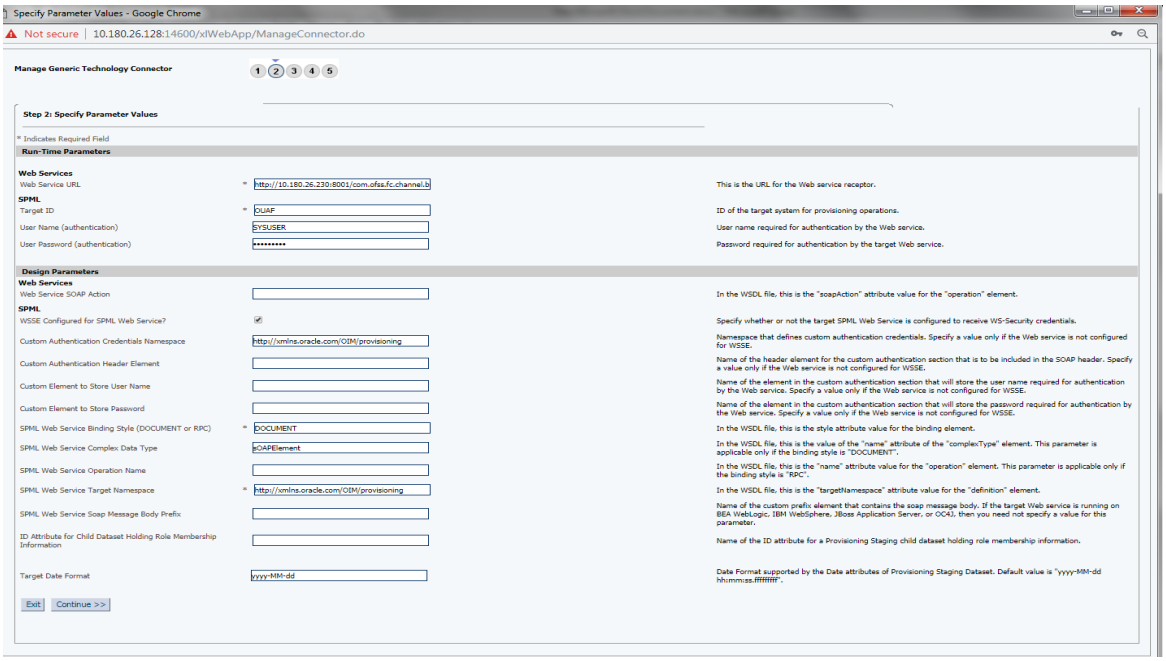


4. Specify parameter values as shown below:

Table 3–2 Run Time Connector Parameters

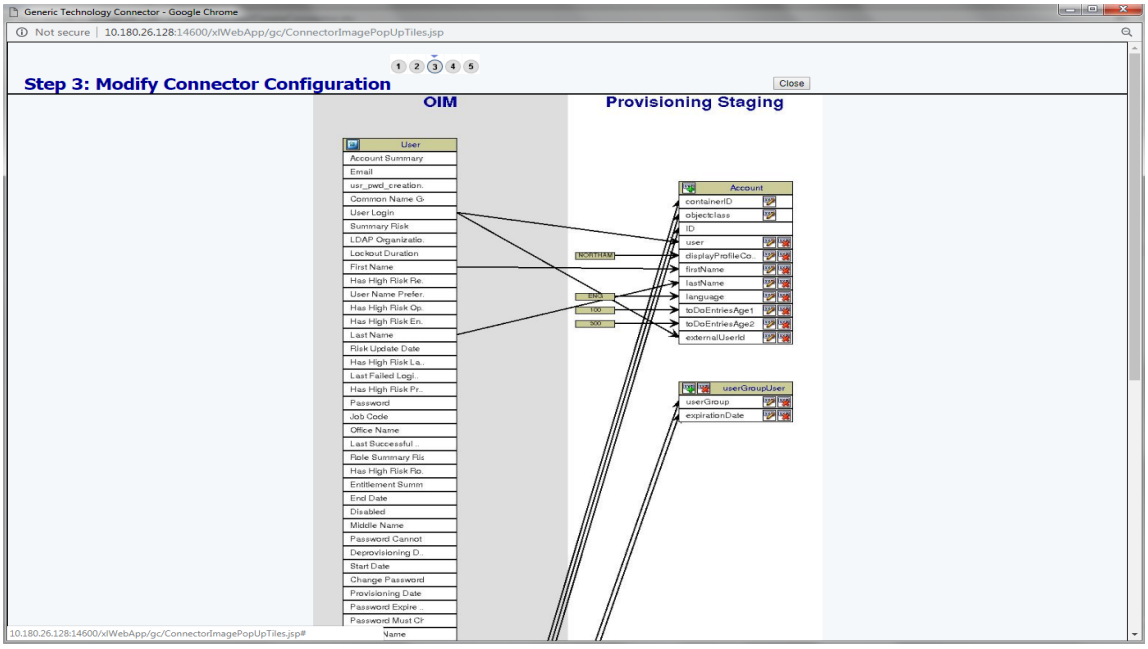
Parameter Name	Parameter Value	Description
Web Services		
Web Service URL	http://<Host>:<Port>/com.ofss.fc.channel.branch/spml2	This is the URL for the Web service receptor.
SPML		
Target ID	OUAF	ID of the target system for provisioning operations.
User Name (authentication)	SYSUSER	User name required for authentication by the Web service.
User Password (authentication)	sysuser00	Password required for authentication by the target Web service.

Figure 3–9 Specify parameter values



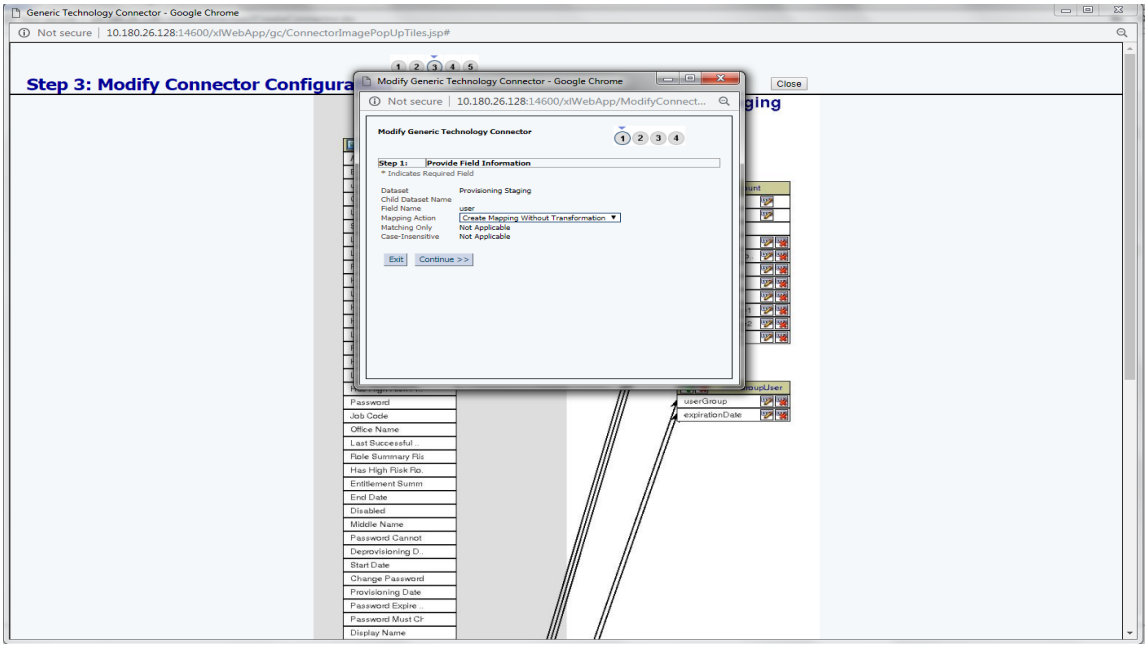
5. Click **Continue**. Modify Connector configuration screen appears.

Figure 3–10 Modify Connector Configuration (Mapping Information)



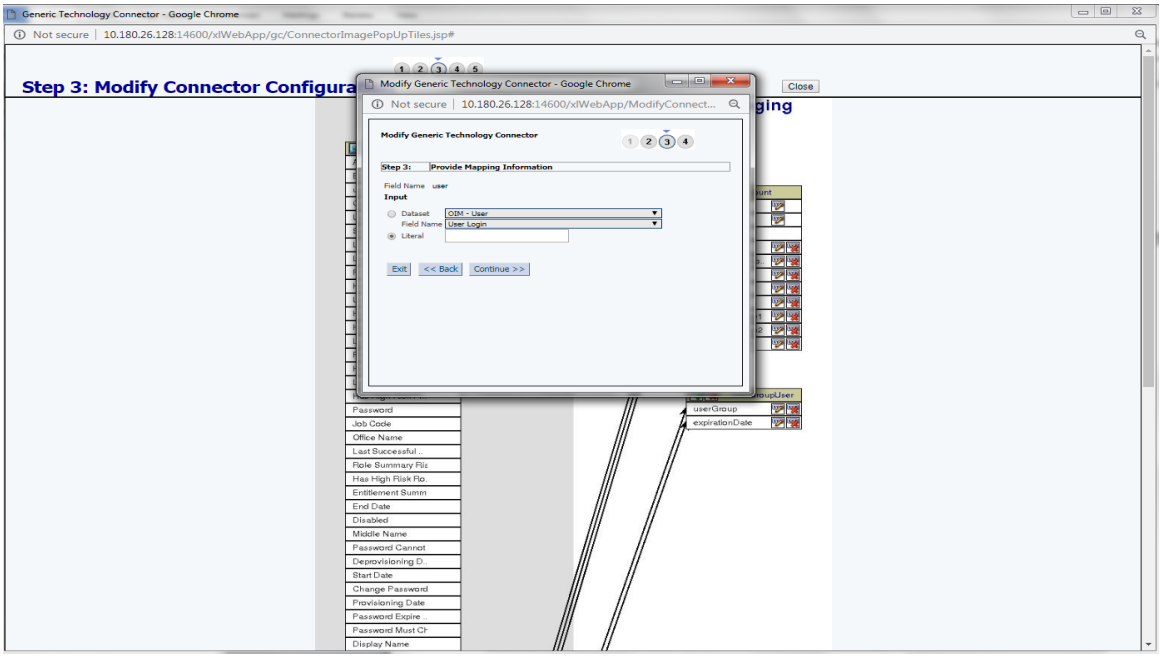
6. Click the **Edit** icon for User field name in the provisioning staging column.

Figure 3–11 Edit Mapping Information



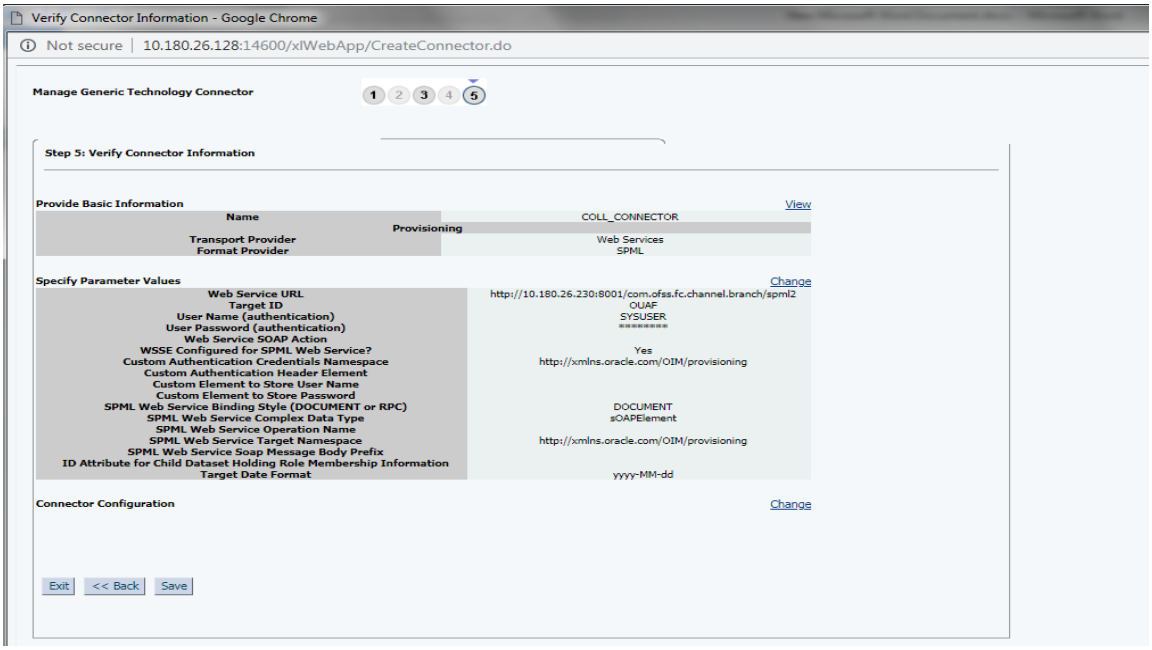
7. Click **Continue** to provide mapping information for the User field name. Select the **Literal** radio button and keep the input blank.

Figure 3–12 Provide Mapping Information



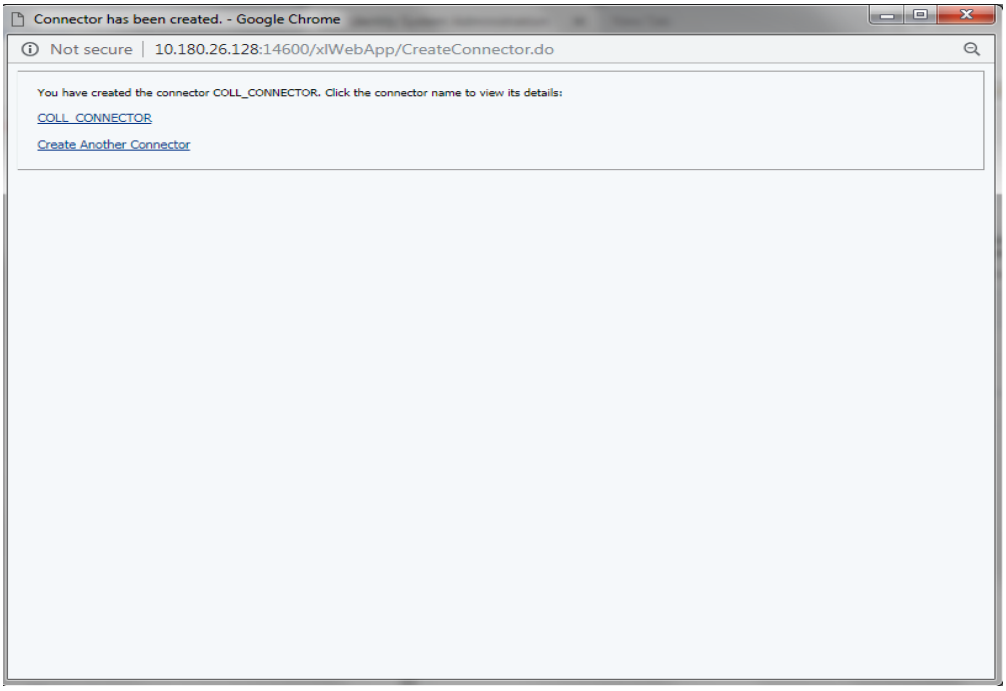
8. Click **Continue** and then **Close**. Following window appears where Connector Information can be verified.

Figure 3–13 Verify Connector Information



9. Click **Save**.
Following message window appears on successful configuration of run time parameters.

Figure 3–14 Successful Configuration Message

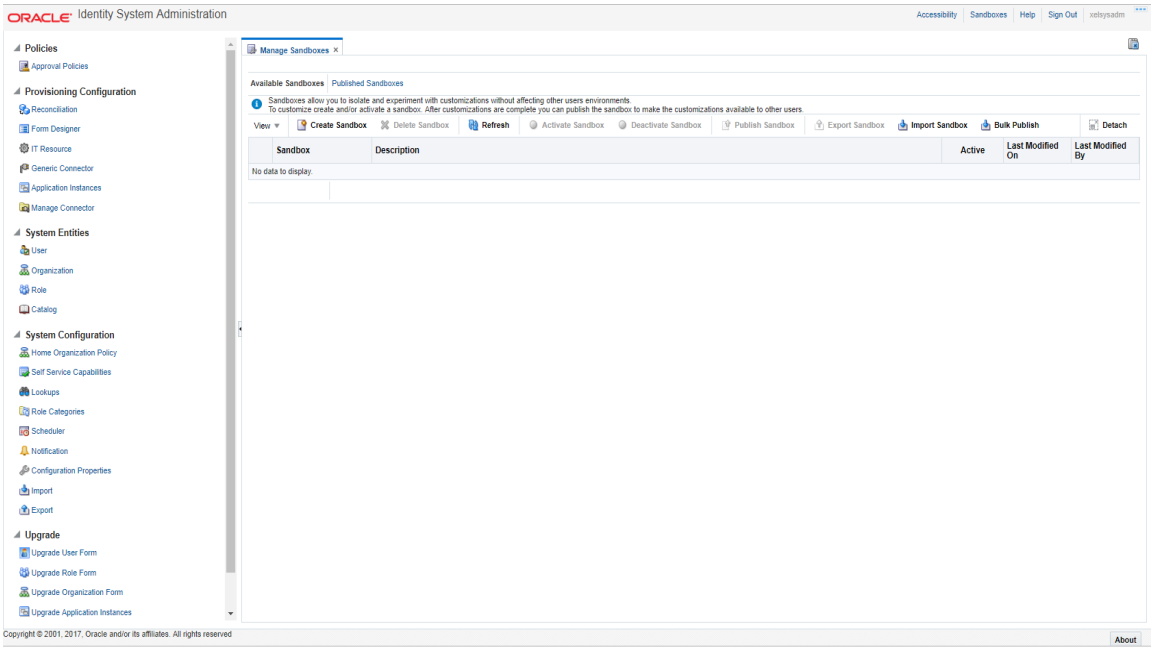


3.3.3 Create and Activate Sandbox

Following is the configuration to create, activate, deactivate, and publish sandbox.

1. Click **Sandboxes**.
   Manage Sandboxes page is displayed.

Figure 3–15 Oracle Identity System Administration - Sandbox tab

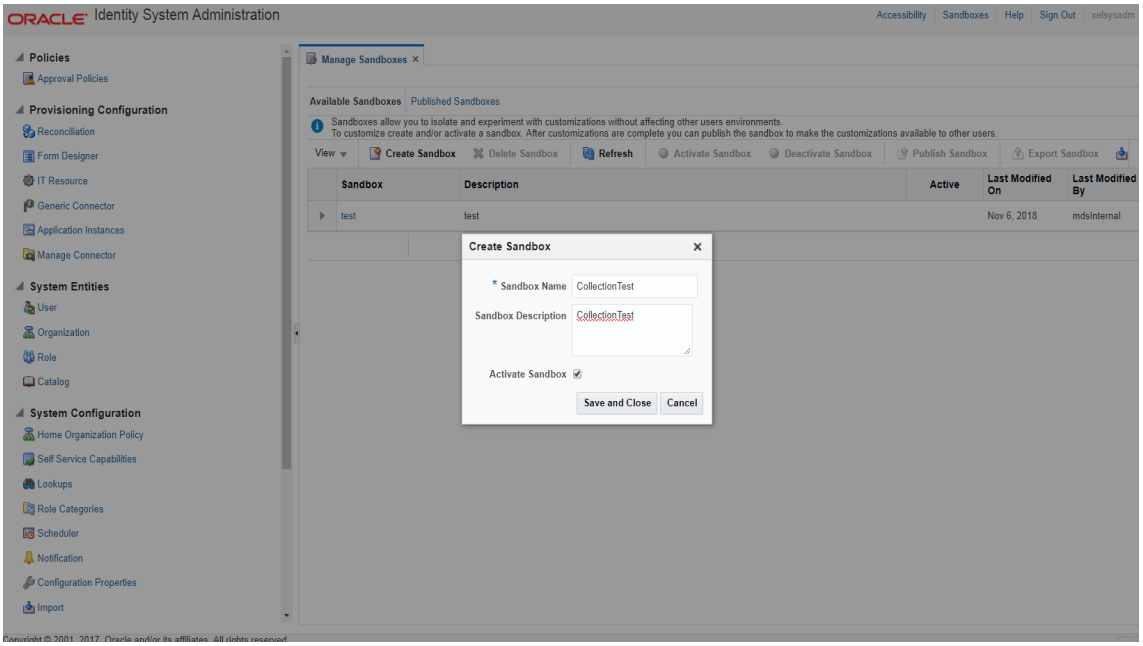


3.3.3.1 Create Sandbox

To create a Sandbox, perform the following steps:

1. Click **Create Sandbox**.
   Create Sandbox dialog box is displayed.

Figure 3–16 Create Sandbox Dialog Box and Parameters



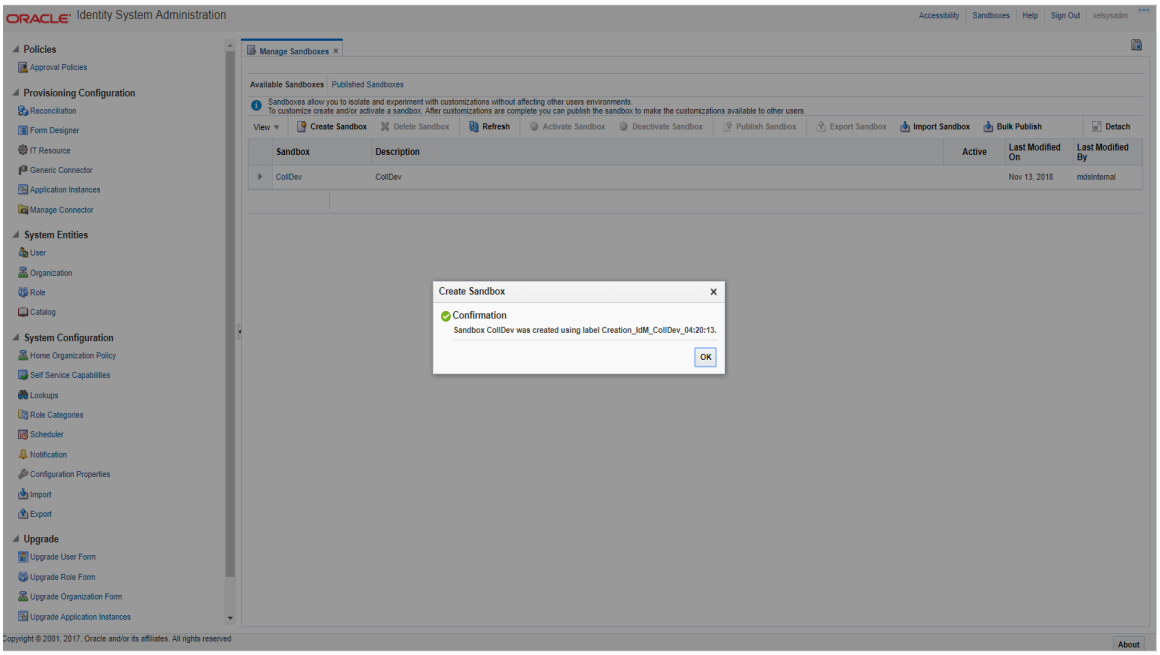
2. Specify the following values:

Table 3–3 Create Sandbox Parameters

Sandbox Fields	Values
Sandbox Name	CollectionsDev
Sandbox Description	Collections Development
Activate Sandbox	Check check box

3. Click **Save** and **Close**.
The Confirmation dialog box appears.

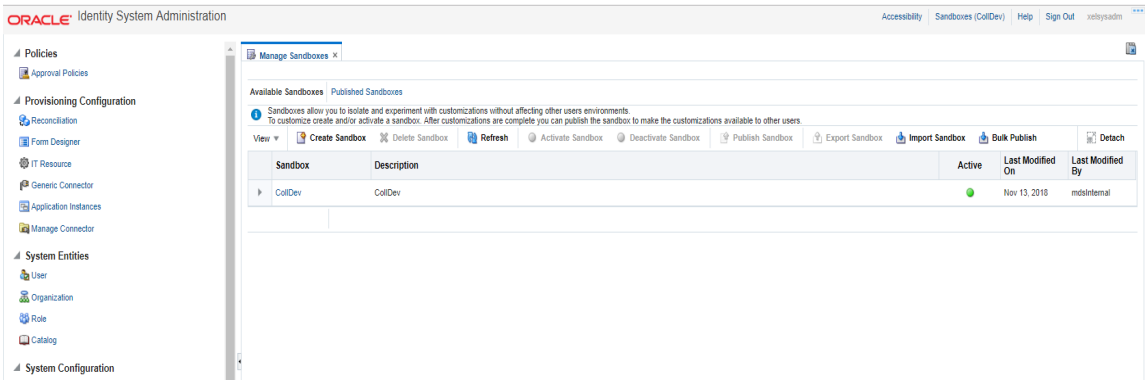
Figure 3–17 Sandbox Creation Confirmation



4. CollectionsDev sandbox is created and it is activated.

> **Note**
>
> After you activate the sandbox, any changes to metadata objects are stored in the sandbox only. There can be only one active sandbox at a time. The information about the active sandbox is stored in the session. Therefore, a sandbox must be activated to continue with customization after every login to Oracle Identity Manager.

Figure 3–18 Available Sandbox

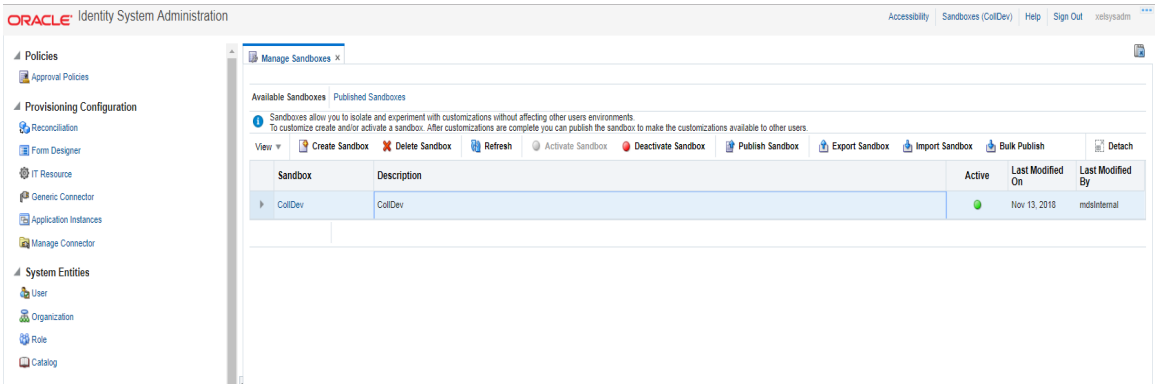


3.3.3.2 Activate Sandbox

To activate a Sandbox, perform the following steps:

1. Select **CollectionsDev** sandbox and then click **Activate Sandbox** to activate sandbox.

Figure 3–19 Activated Sandbox



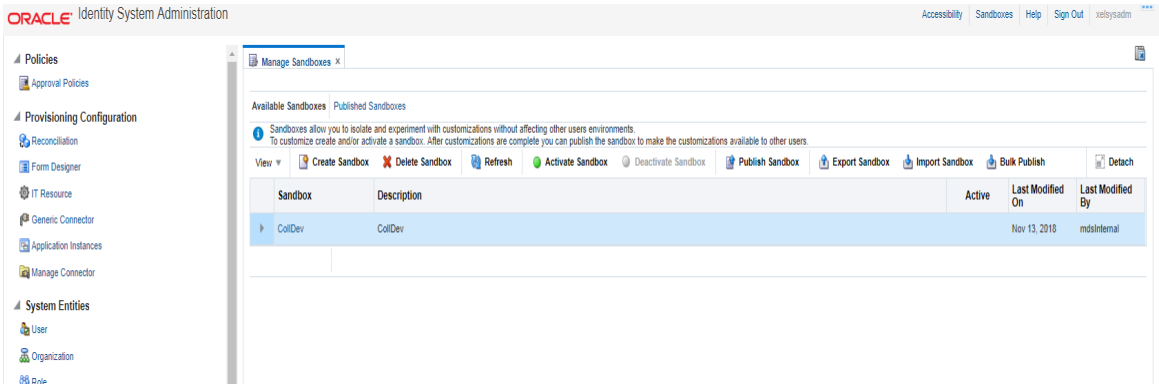
2. Sandbox is active now. It will be highlighted with green dot.

3.3.3.3 Deactivate Sandbox

To deactivate a Sandbox, perform the following steps:

1. Select **CollectionsDev** sandbox.
2. Click **Deactivate Sandbox** to deactivate sandbox.
   Sandbox is deactivated now.

Figure 3–20 Deactivate Sandbox

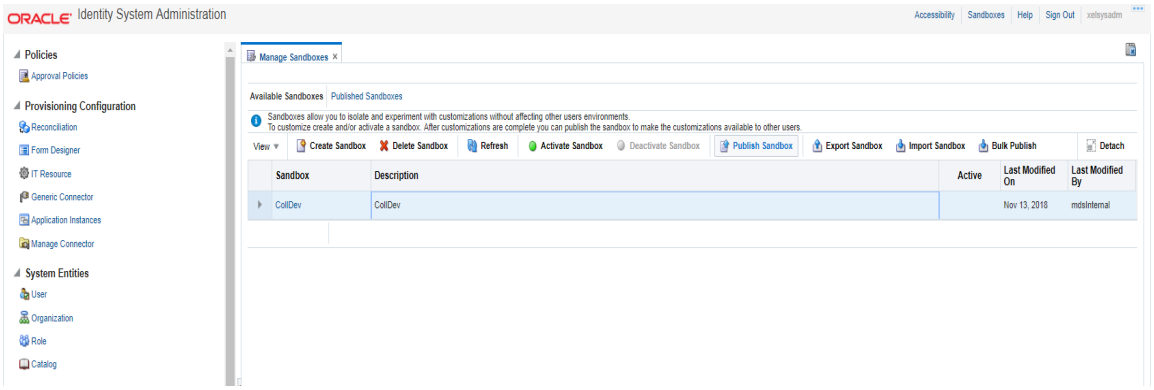


3.3.3.4 Publish Sandbox

To publish a Sandbox, perform the following steps:

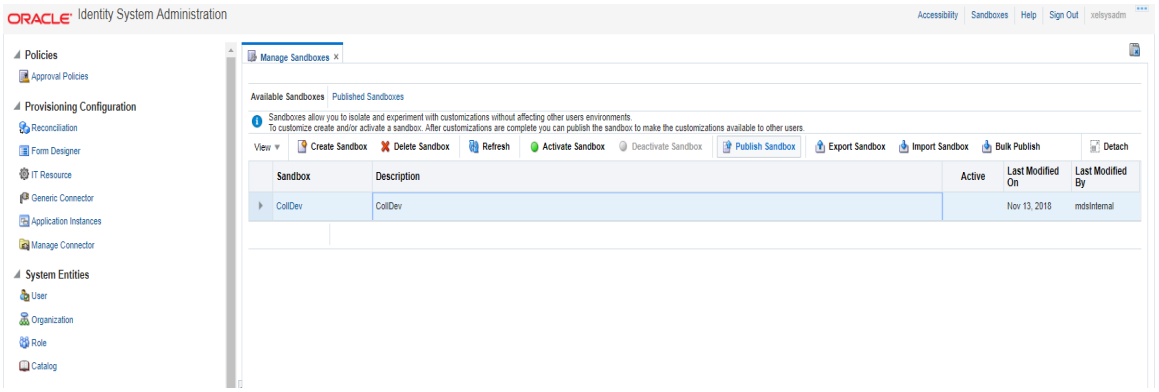
1. Select **CollectionsDev** sandbox and then click **Publish Sandbox** to publish sandbox.

Figure 3–21 Publish Sandbox



2. Sandbox is published now. It will be removed from sandbox list.
   Once Sandbox is published, all changes will be visible to all the users.

Figure 3–22 Published Sandbox

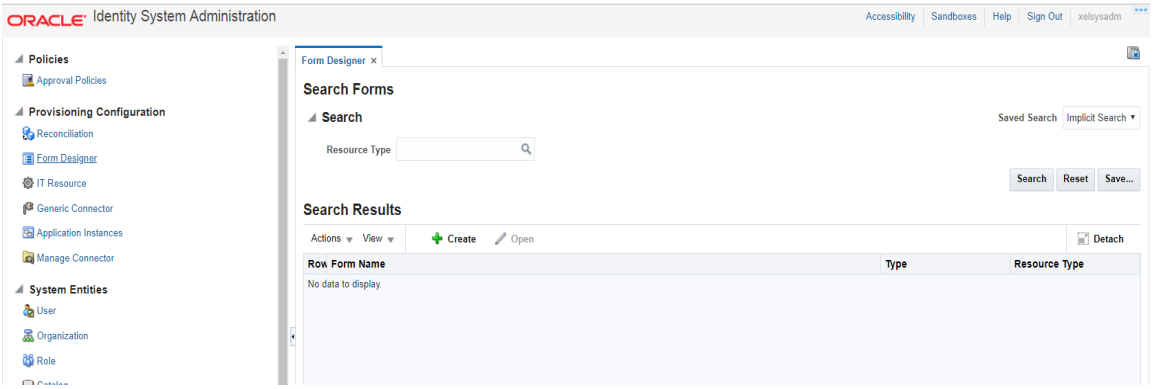


3.3.4 Create Form Associated with Application Instance

To create forms associated with the resource objects, and subsequently with the application instances, follow the below steps:

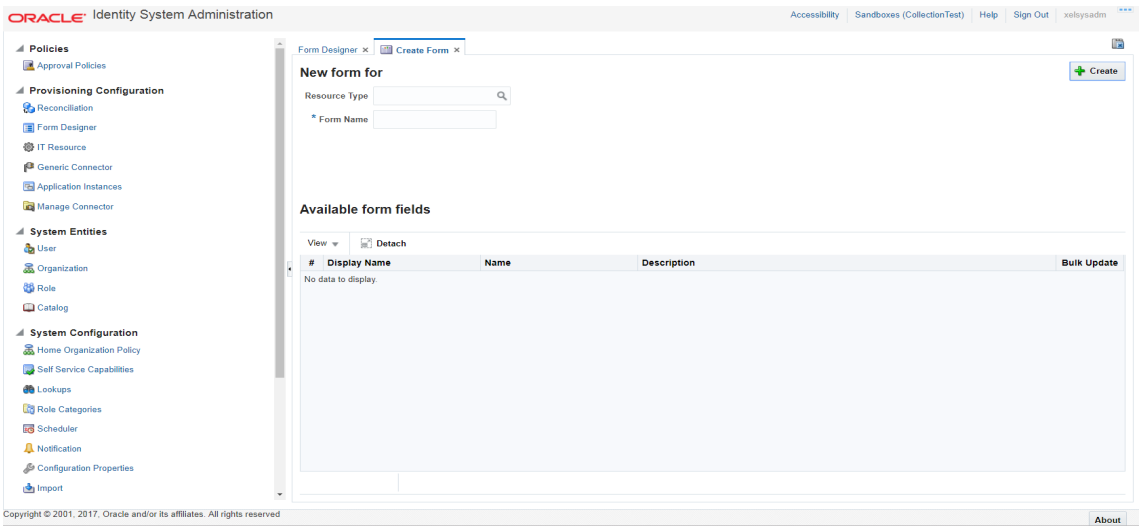
1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Chapter 1.3.3 Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery Sandbox.
3. In the left pane, under Configuration, click **Form Designer**. The **Form Designer** page is displayed.

Figure 3–23 Create Form - Form Designer



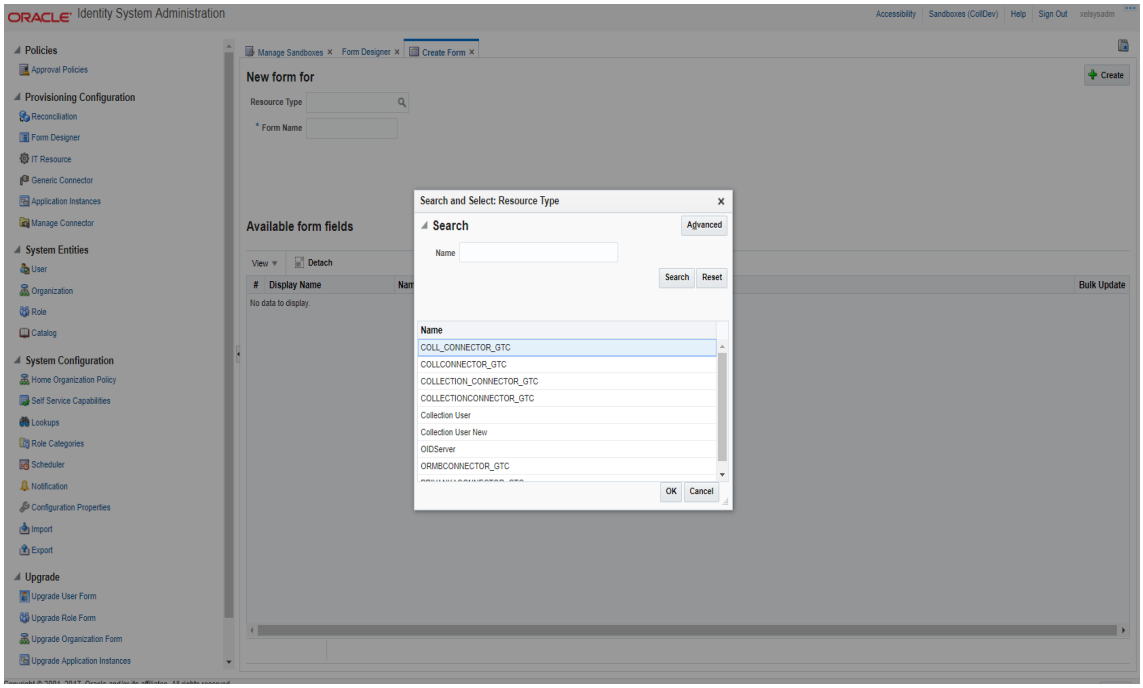
4. Click **Create** on the toolbar. The **Create Form** page is displayed.
5. In the **Resource Type** field, verify the name of the resource object with which the form is associated is displayed. To change the resource object name, click the Search icon next to the **Resource Type** field, and search and select a name from the **Search and Select: Resource Type** dialog box.

Figure 3–24 Create Form - Resource Type



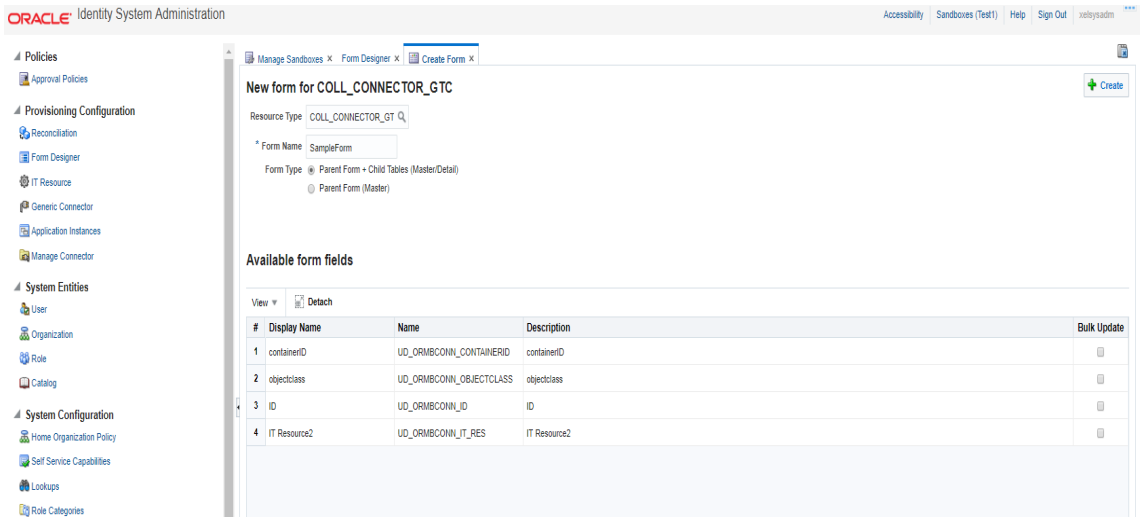
6. Select **Resource Type** as **COLL_CONNECTOR_GTC** and provide a name for the form (for example, SampleForm).

Figure 3–25 Create Form - Resource Type (COLL_CONNECTOR_GTC)



7. **Available Form Fields** will be displayed in the below section of the page.

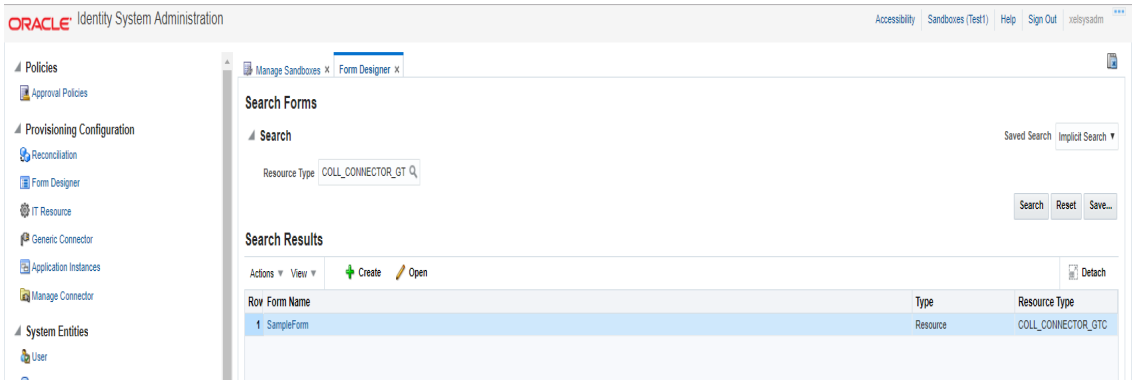
Figure 3–26 Create Form Resource Type - Available Form Fields



8. Click **Create**.
A message is displayed stating that the form is created.

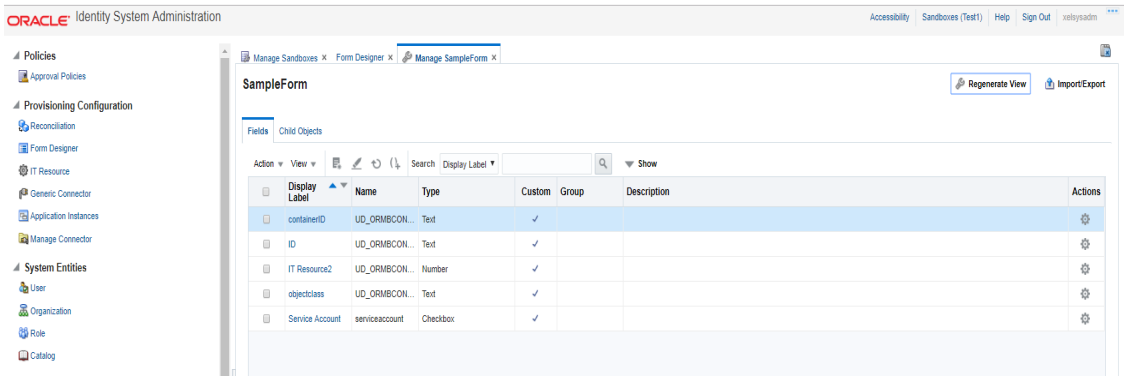
9. Refresh the **Search Results** in **Form Designer** page for resource type : COLL_CONNECTOR_GTC.
10. Select the **SampleForm** from the results.

Figure 3–27 Search Form



11. **Manage SampleForm** page is displayed.

Figure 3–28 Manage Collections User Form



12. In the Fields tab click the **objectClass**.
    Edit Text Field page appears.
13. Enter Default Value as **User**. Click **Save** and **Close**.
14. In the Child Objects tab, click **ORMUSERG** (child form).
    expirationDate and userGroup fields are displayed.

Figure 3–29 Manage Form

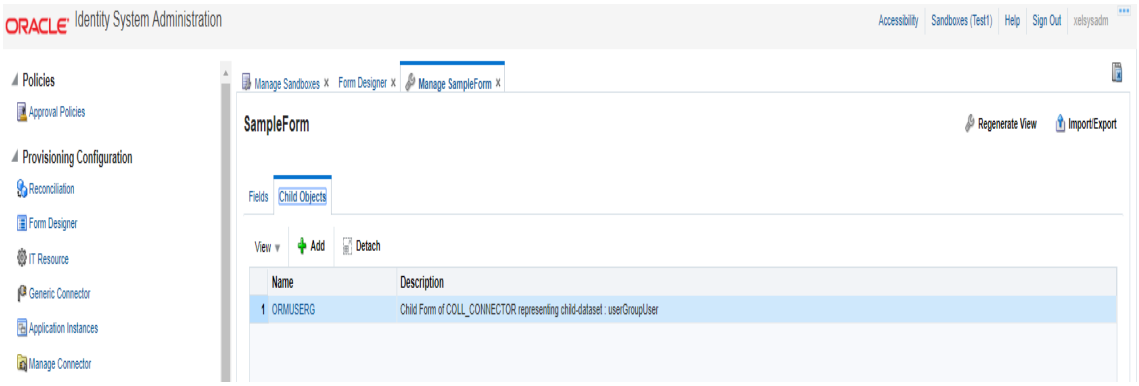
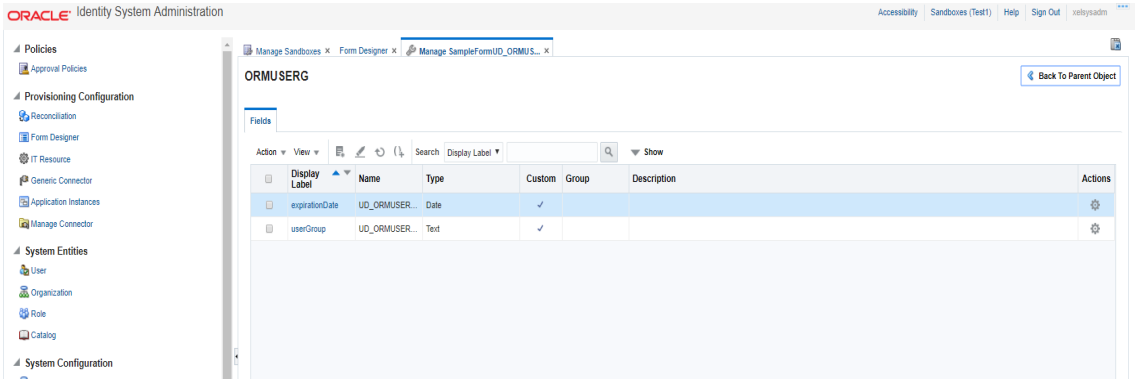
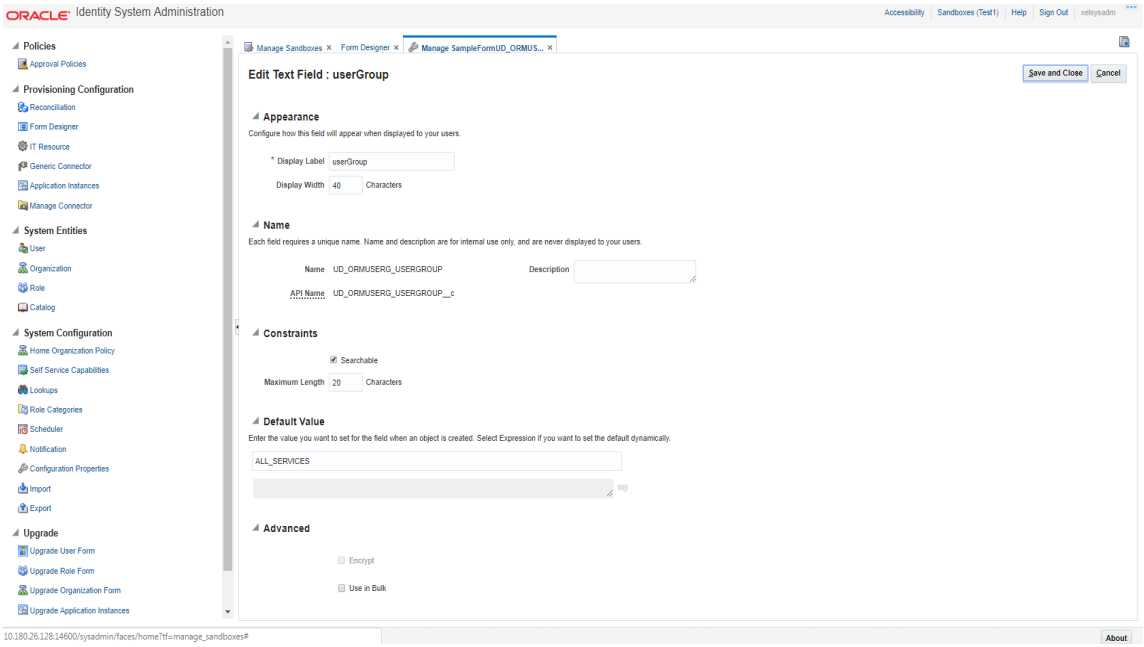


Figure 3–30 Manage Child Objects form fields



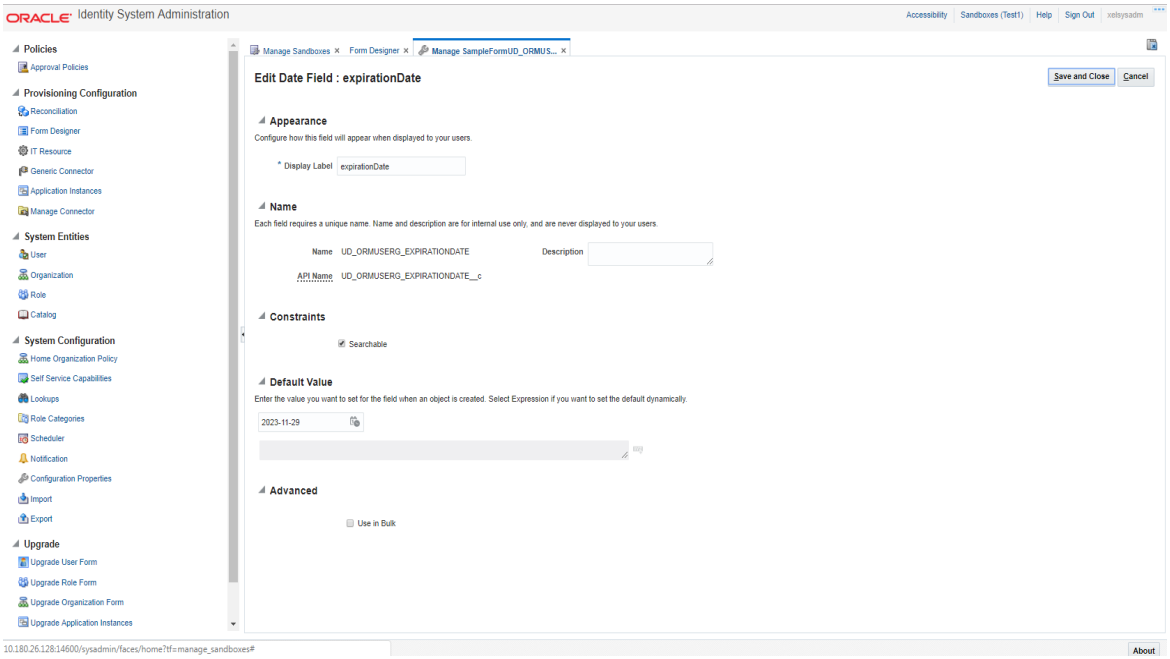
15. Click the userGroup and give default value as ALL_SERVICES.

Figure 3–31 Set default values for field- userGroup



16. Click **expirationDate** and give default value as 2100-01-01.

Figure 3–32 Set default value for field- expirationDate



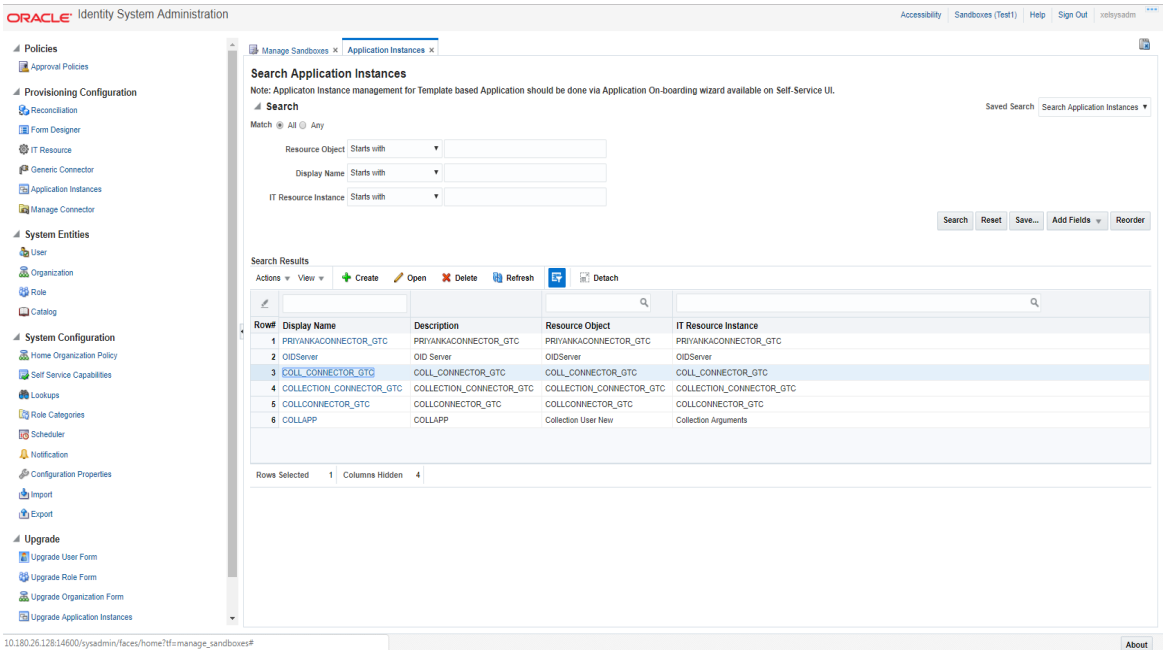
17. Click **Save** and **Close**.
18. Click the **Back to Parent Object** Link.

19. Close **Manage SampleForm** tab.

Steps to associate the form with the application instance:

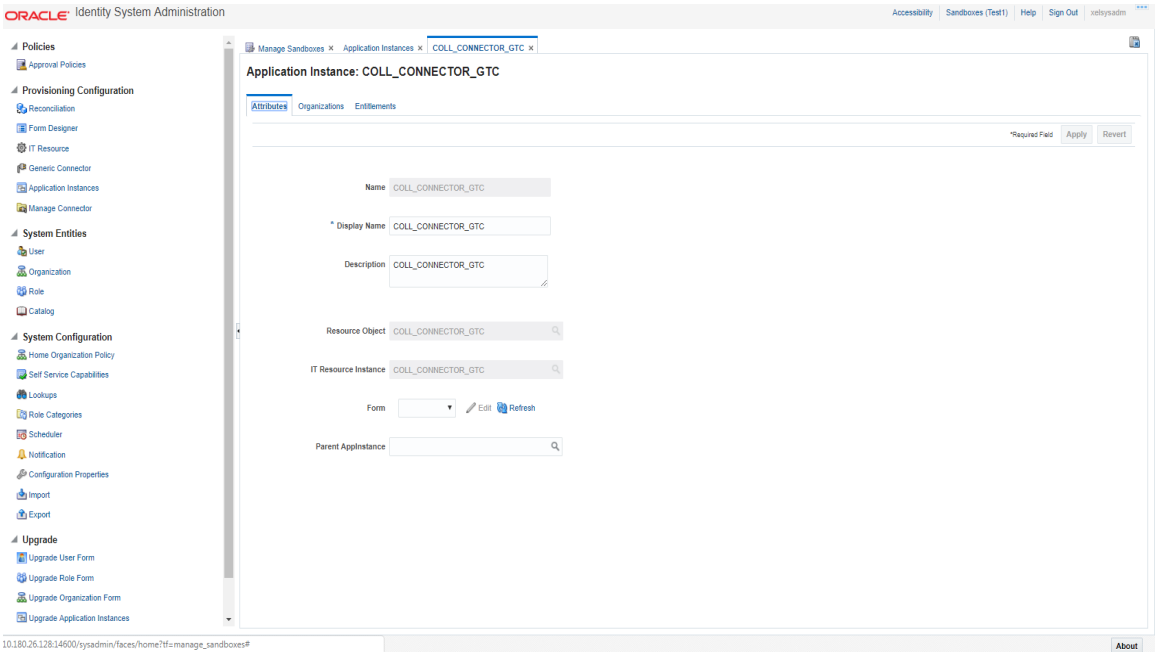
1. Click the **Application Instances** Menu. Click **Search** and select COLL_CONNECTOR_GTC.

Figure 3–33 Search Application Instances and select COLL_CONNECTOR_GTC



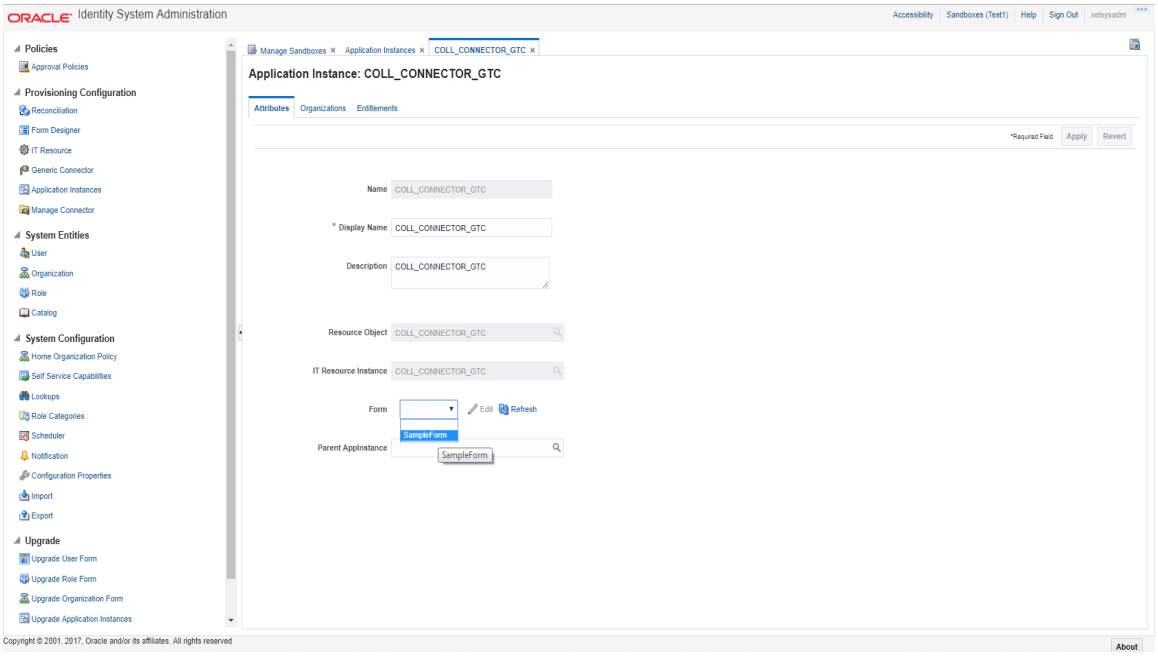
2. Click the **Attributes** tab.

Figure 3–34 Application Instance Attributes



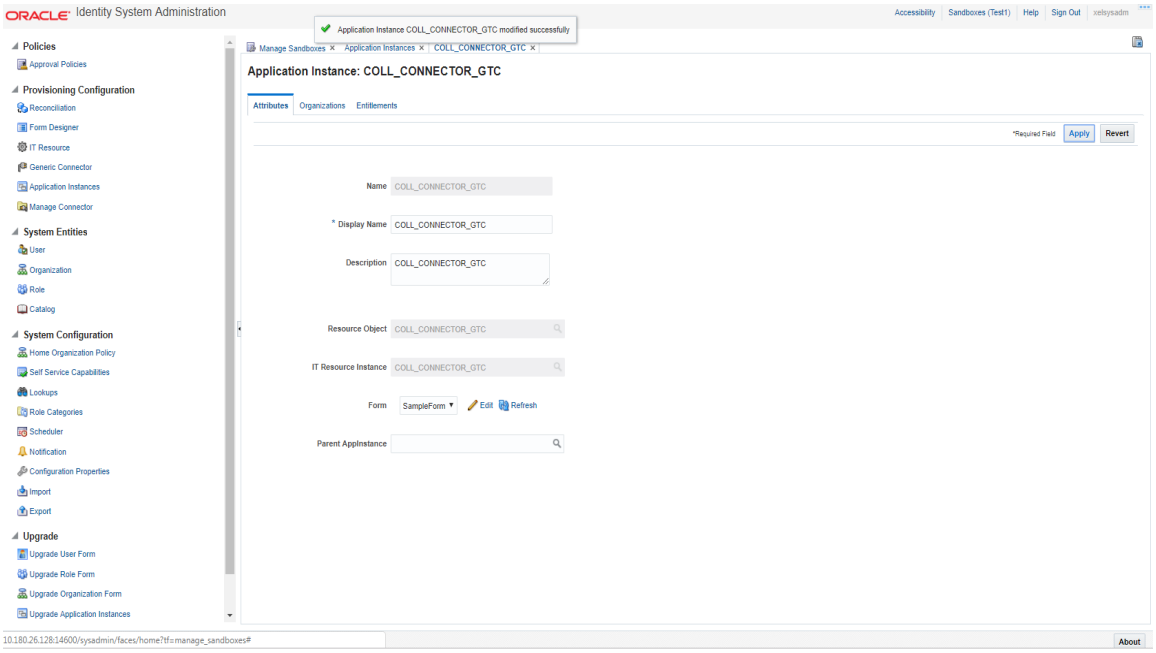
3. In Form list, select above created form and click **Apply**.

Figure 3–35 Associate Form with Application instance



4. Message ‘Application instance modified successfully’ is displayed.

Figure 3–36 Success message



5. If required, you can export the sandbox to store all the changes made in your sandbox.
6. Publish the sandbox.

3.3.5 Create Access Policy and Role

3.3.5.1 Create Access Policy

Policy based provisioning is being used, that is, whenever policy is applied, the user is directly provisioned to resource.

This policy is applied whenever a user is made part of specified role For example: Collection_Users. Also, Collection_Users is applied to user through membership rule. Thus, policy will be applied to user and the user would be provisioned to resource Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User.

> **Note**
>
> Here, we have used Collection_Users Role, but it can be changed as required. See Section 3.3.5.2 Creating Roles for Role Creation.

1. Log in to the Identity Self Service.
2. Click **Manage** and then click **Roles and Access Policies**.

3. Select the **Access Policies**. The Search Access Policies page is displayed.

Figure 3–37 Identity Self Service – Manage tab

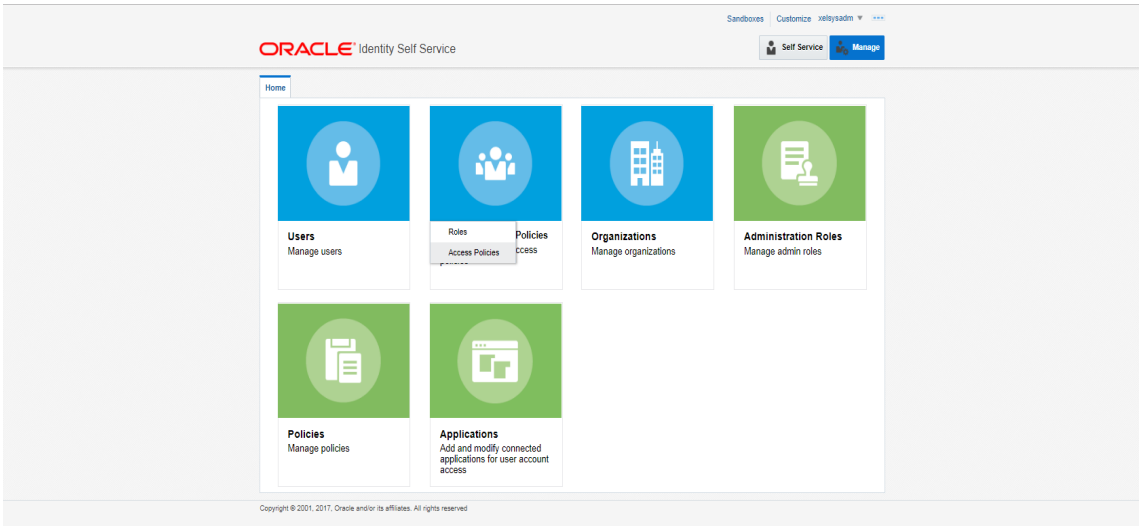
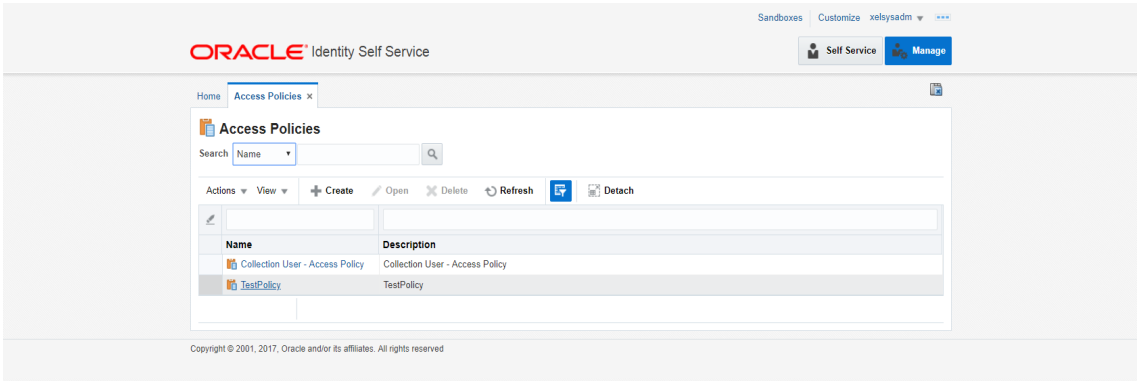
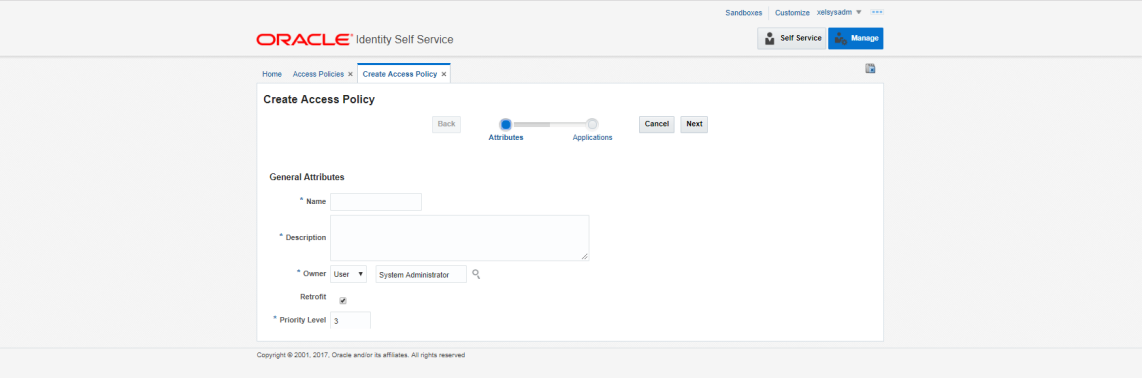


Figure 3–38 Access Policies



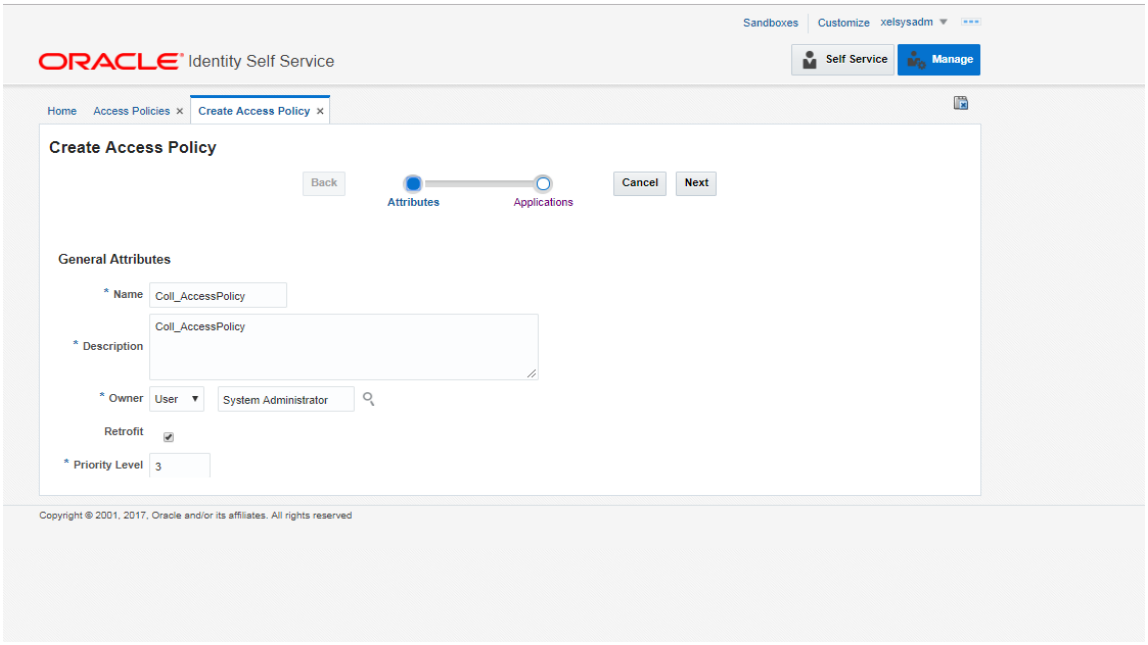
4. Click **Create**. Create Access Policy Page is displayed.

Figure 3–39 Create Access Policy



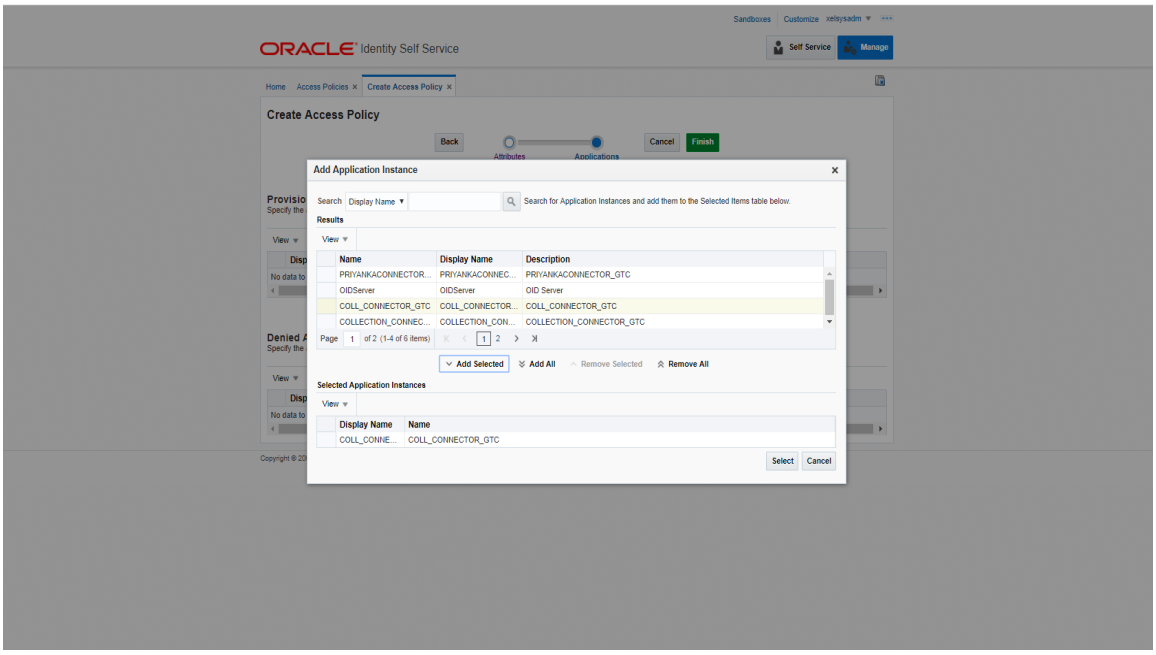
5. Enter following details (for example) and click **Next**.
   - **Name**: Coll_AccessPolicy
   - **Description**: Coll_AccessPolicy

Figure 3–40 Access Policy details



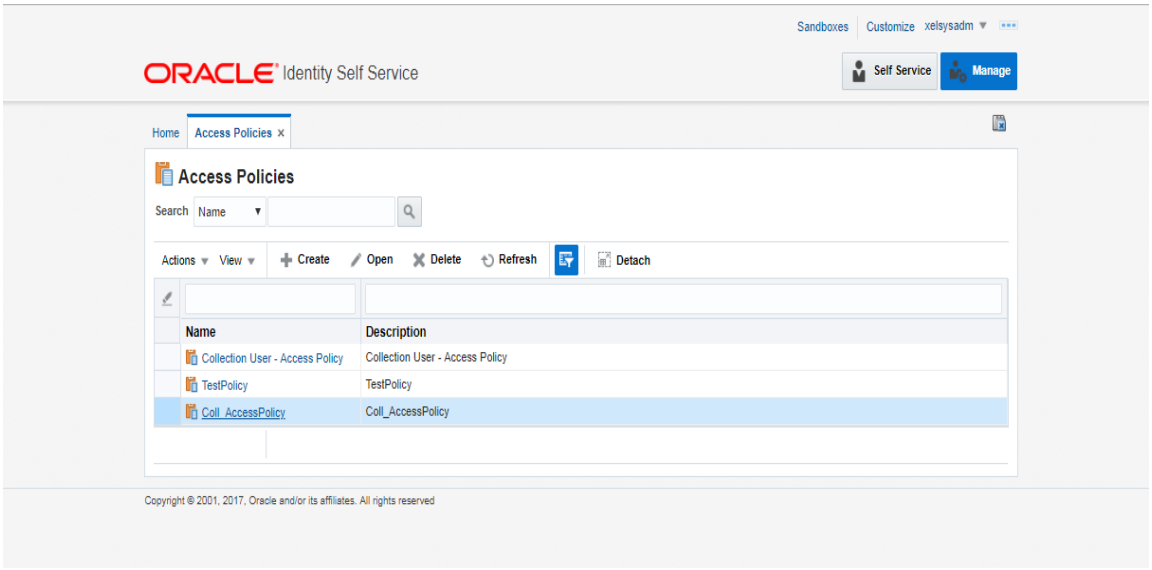
6. To specify the application instances provisioned by this access policy, click **Add** and select **COLL_CONNECTOR_GTC** Application Instance. Click **Select**.

Figure 3–41 Add application instance associated with access policy



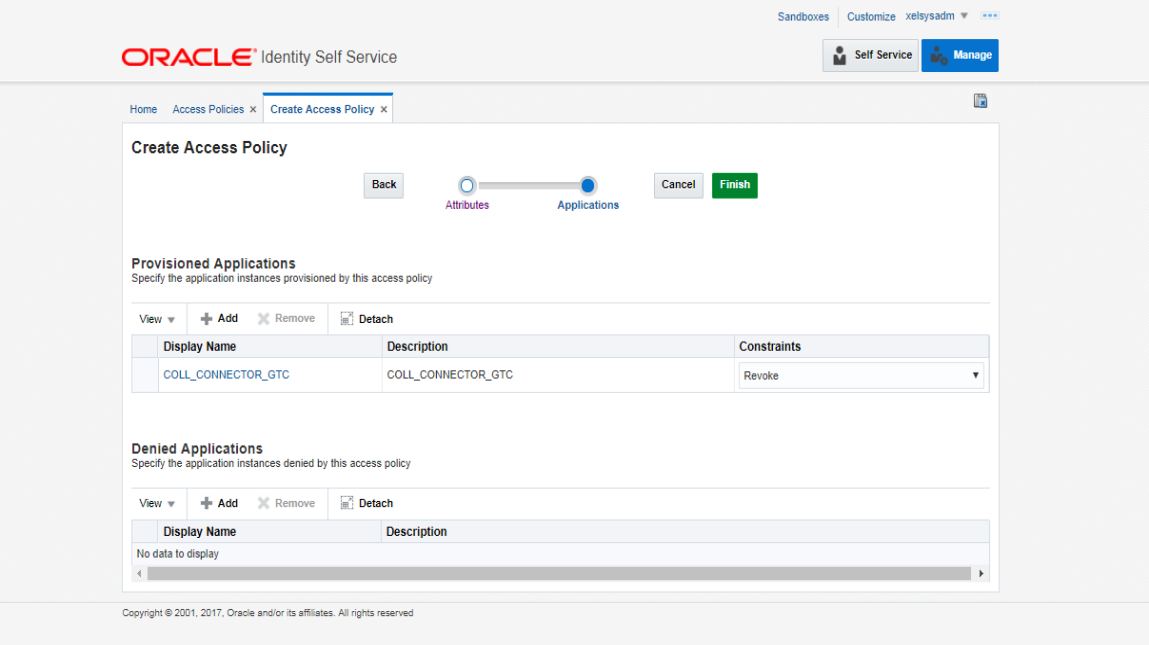
7. Click **Finish**.
8. In the Search Access Policies Page, select the above created policy and click the **Applications** tab.

Figure 3–42 Search Access Policy



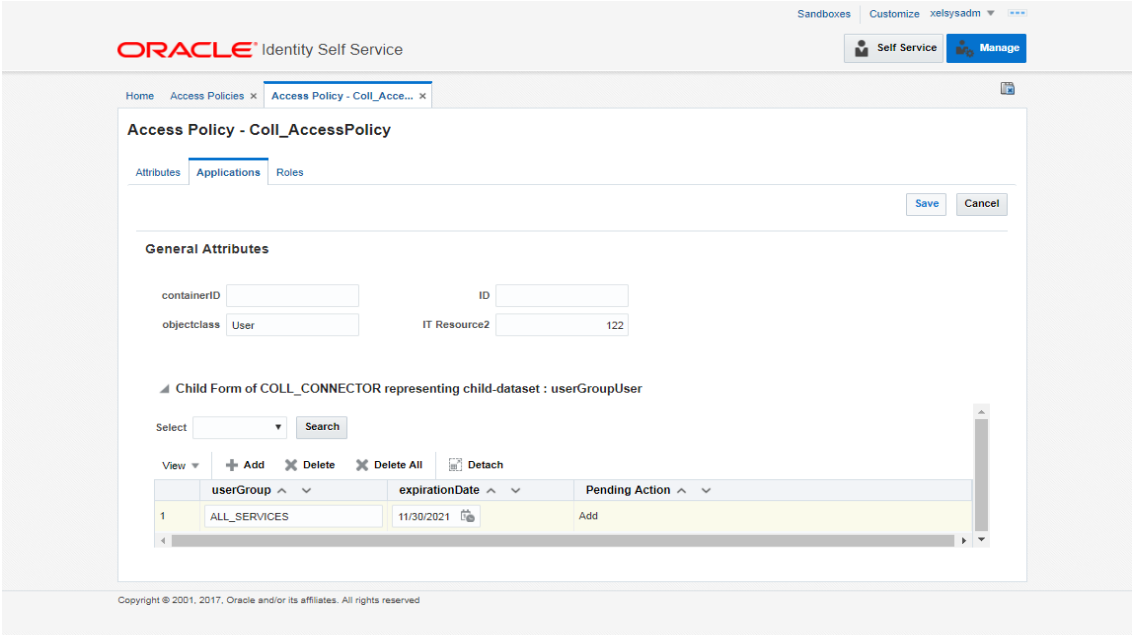
9. COLL_CONNECTOR_GTC application would be listed in the Provisioned Applications list.

Figure 3–43 Provisioned applications for the policy



10. Click the COLL_CONNECTOR_GTC application. Provide default values for the General Attributes and Child Form fields.
    - **objectClass: User**
    - **userGroup: ALL_SERVICES**
    - **expirationDate: 2100-01-01**

Figure 3–44 Application Attributes



11. Click **Save** and **Apply**.

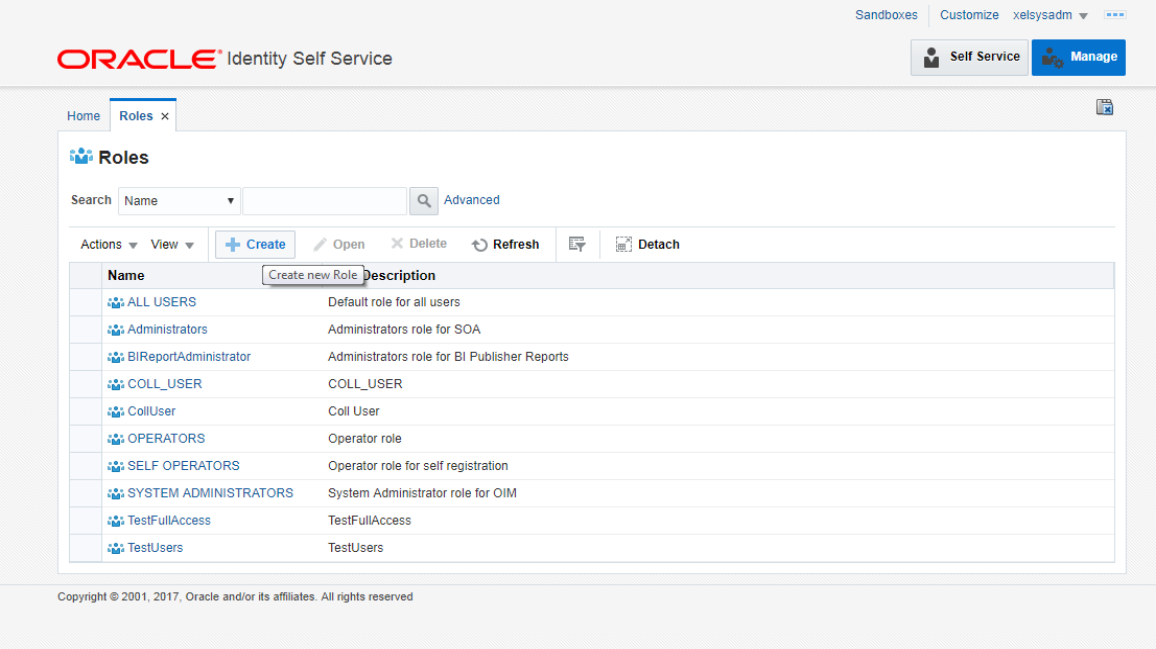
3.3.5.2 Creating Roles

This role is used to define access policy. Minimum access should be provided as it would be applied to every user eligible for Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User provisioning.

1. Log in to Identity Self Service.
2. Click **Manage** and then, click **Roles and Access Policies** .

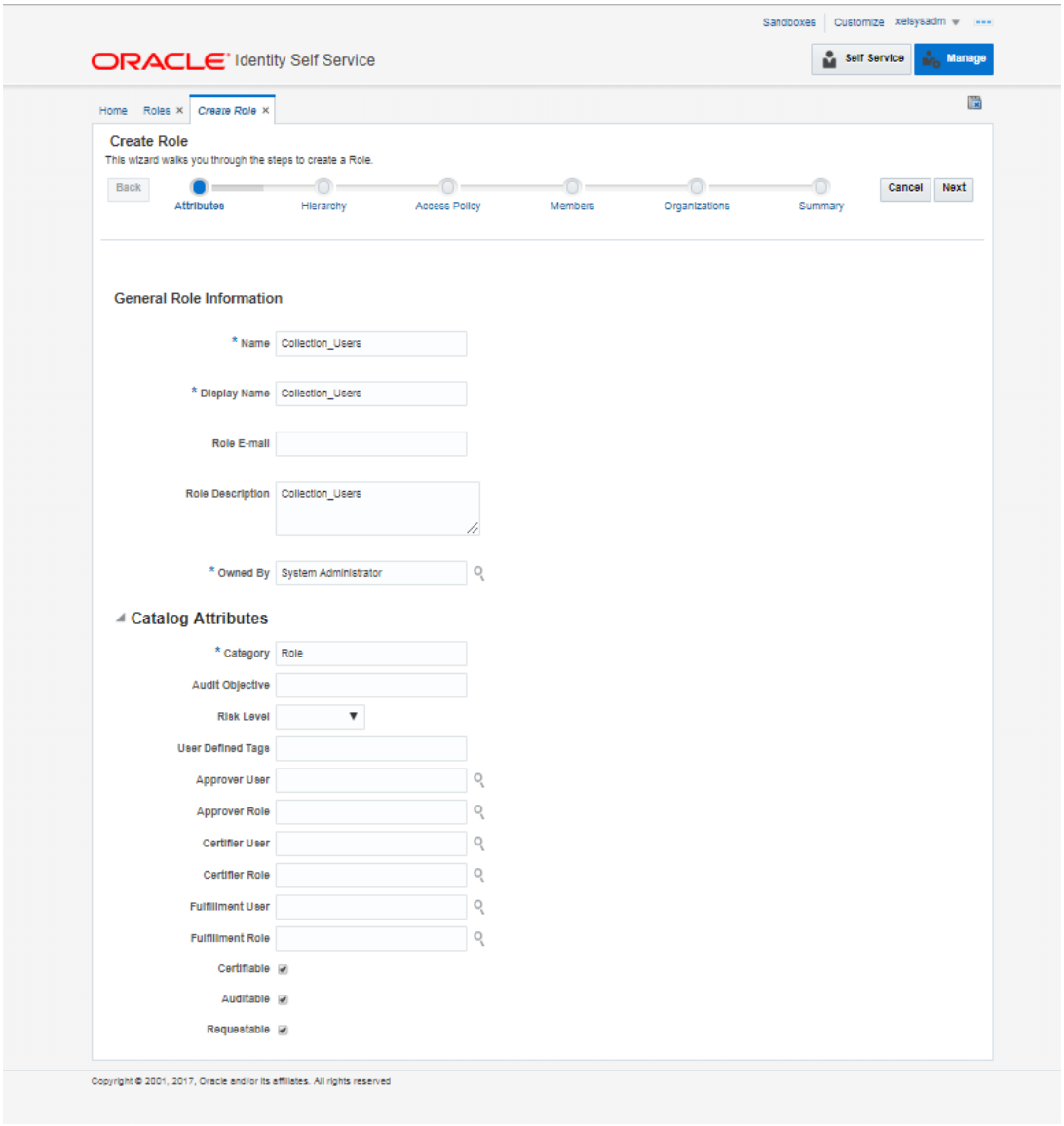
3. Select **Roles**. The Search Roles page is displayed.

Figure 3–45 Oracle Identity Self Service- Roles Tab



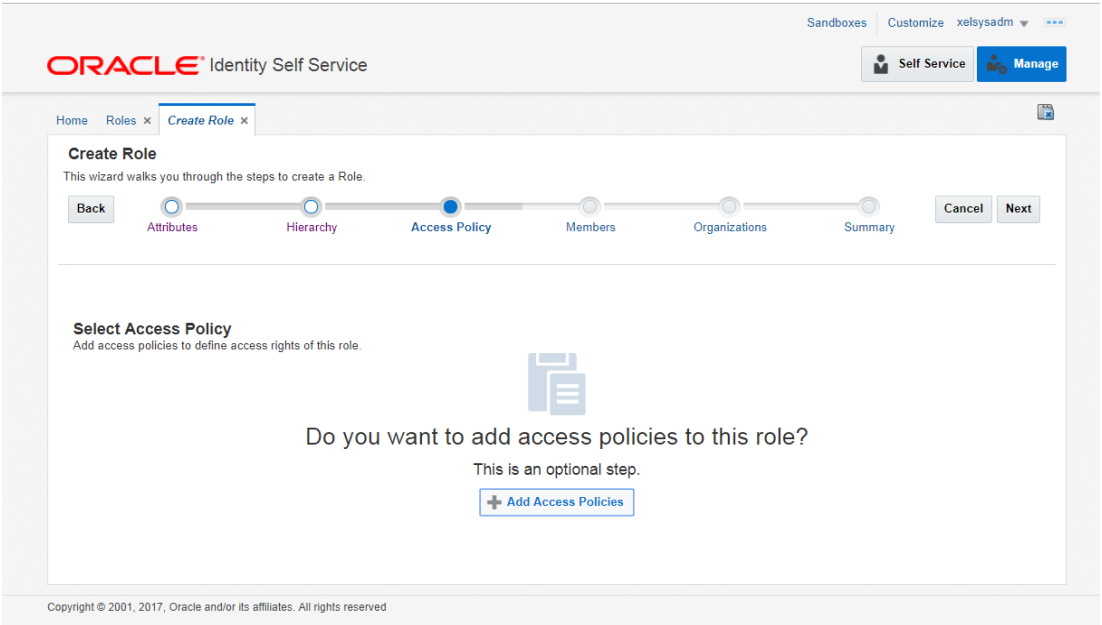
4. Click **Create** on the toolbar. The Create Role page is displayed.
5. Specify the following values and then click **Next**.
   - **Name**: Collection_Users
   - **Display Name**: Collection_Users
   - **Role Description**: Default Role for all Oracle Banking Enterprise Collections and Oracle Banking Enterprise RecoveryUser.
   - **Role Category**: Default

Figure 3–46 Create Role



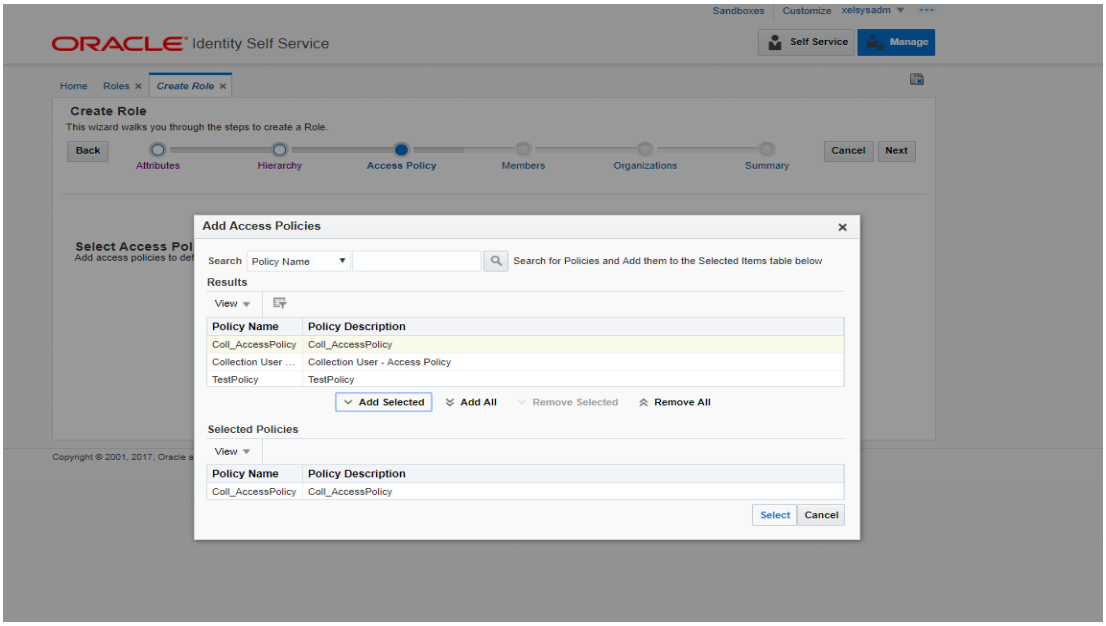
6. Click **Next** to go to the Access Policy step.

Figure 3–47 Create Role



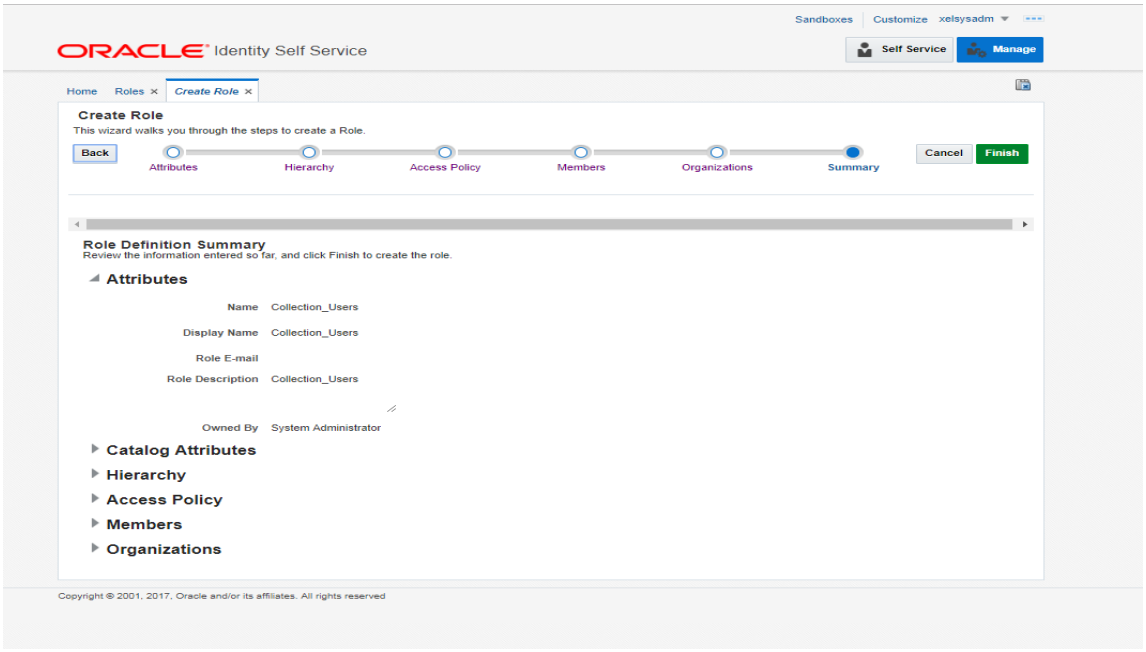
7. Click **Add Access Policies**. List of access policies is displayed on clicking the search icon.

Figure 3–48 Add Access Policy to the role



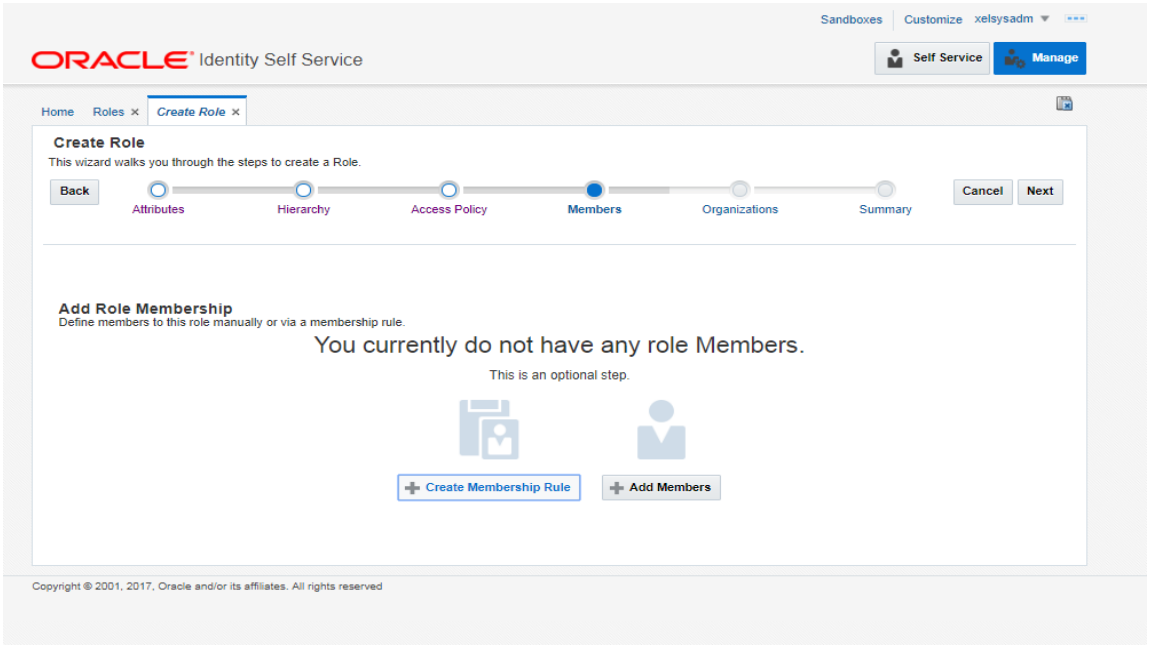
8. Select above created access policy (eg: Coll_AccessPolicy) and click **Next**.

Figure 3–49 Add Access Policy to the role



9. In the Members Step, click **Create Memebrship Rule**.

Figure 3–50 Create Membership Rule



10. Create rule such that Collection_Users role is assigned to a User that needs to be provisioned to Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery. Here we have defined Rule Based on Organization.
    Build the rule expression as follows:
    Select **Organization** attribute, operand: '=' and RHS operand value='Xellerate Users' (literal)

Figure 3–51 Build Membership Rule Expression

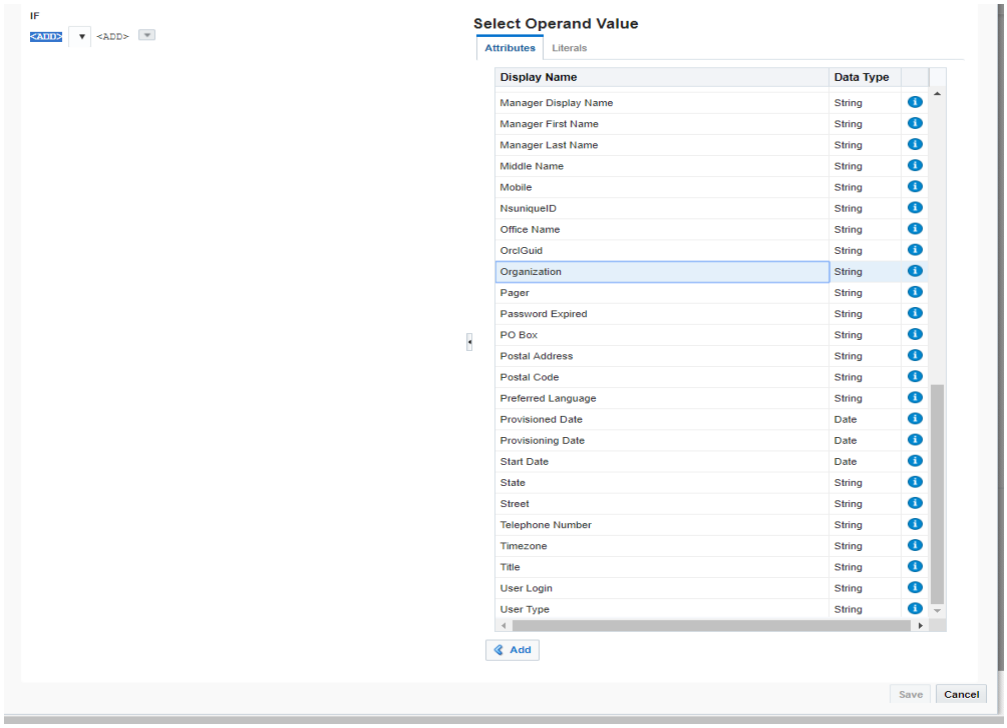
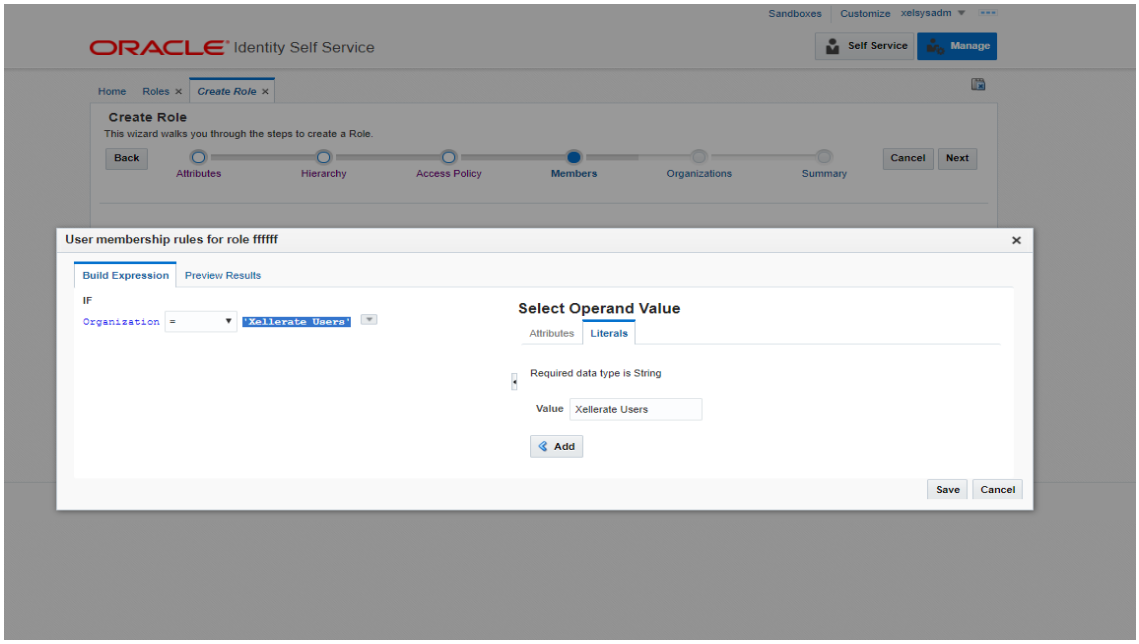


Figure 3–52 Build Membership Rule Expression



11. Click **Save**.

3.4 DB Based Configuration

This section provides the details required for provisioning users through DB based configurations.

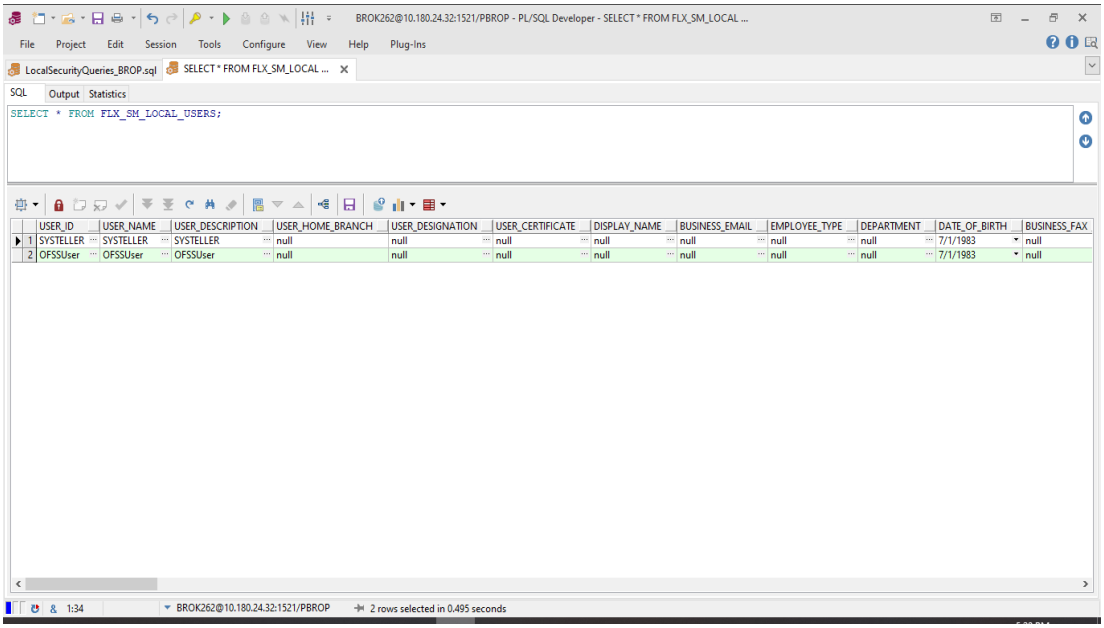
3.4.1 DB Based Policy Configuration

Policy configuration is performed by linking Users to Roles and then linking Roles to Service Policies with either grant or deny access.

Following are the tables related to Menu configuration:

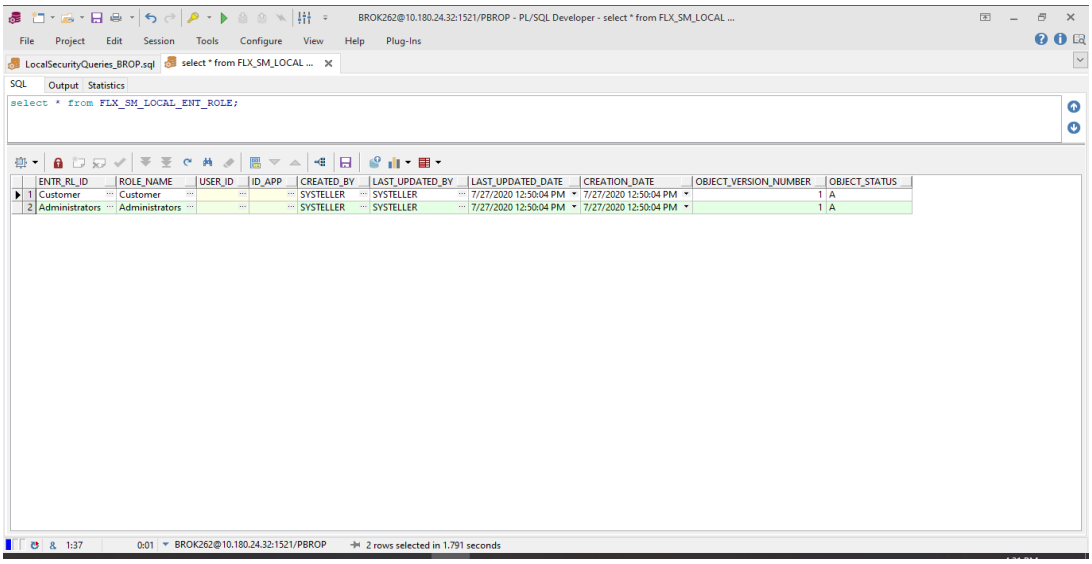
- **FLX_SM_LOCAL_USERS (Related view FLX_SM_LOCAL_USERS_V)**: This table defines the users in OBP for whom access policies are to be configured. All user IDs need to be in lowercase.

Figure 3–53 FLX_SM_LOCAL_USERS



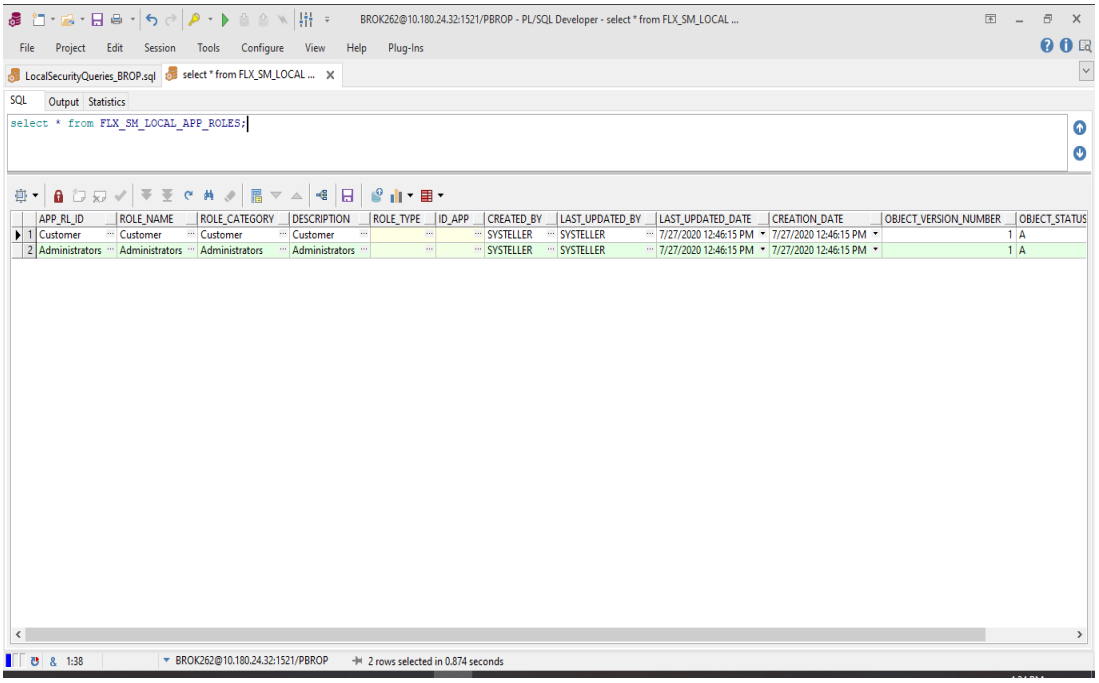
- **FLX_SM_LOCAL_ENT_ROLE (Related view FLX_SM_LOCAL_ENT_ROLE_V)**: This table defines the enterprise roles.

Figure 3–54 FLX_SM_LOCAL_ENT_ROLE



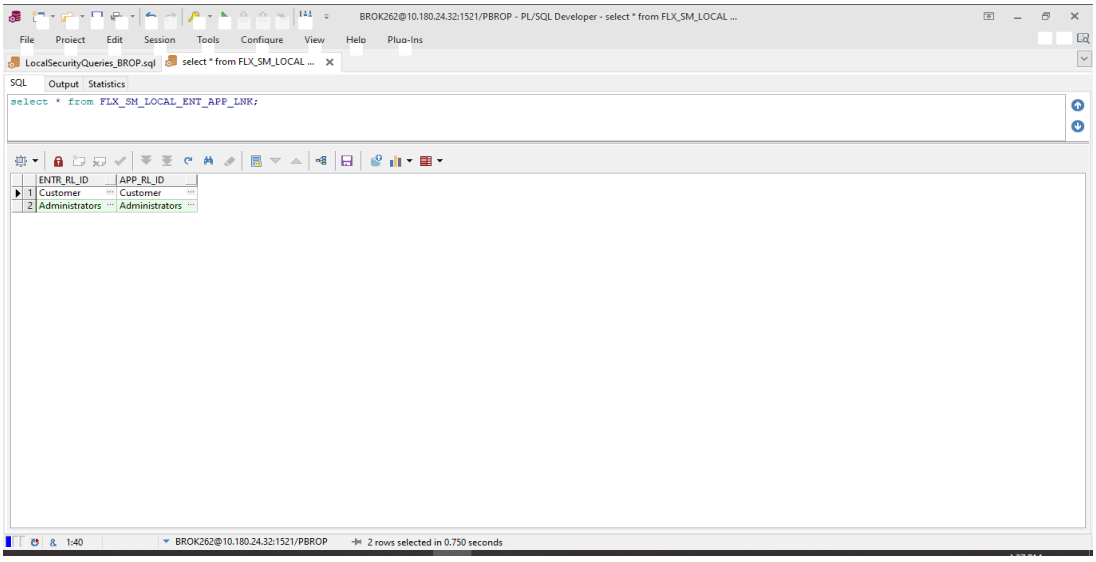
- **FLX_SM_LOCAL_APP_ROLES (Related view FLX_SM_LOCAL_APP_ROLES_V)**: This table defines the application roles, that is at OBP level.

Figure 3–55 FLX_SM_LOCAL_APP_ROLES



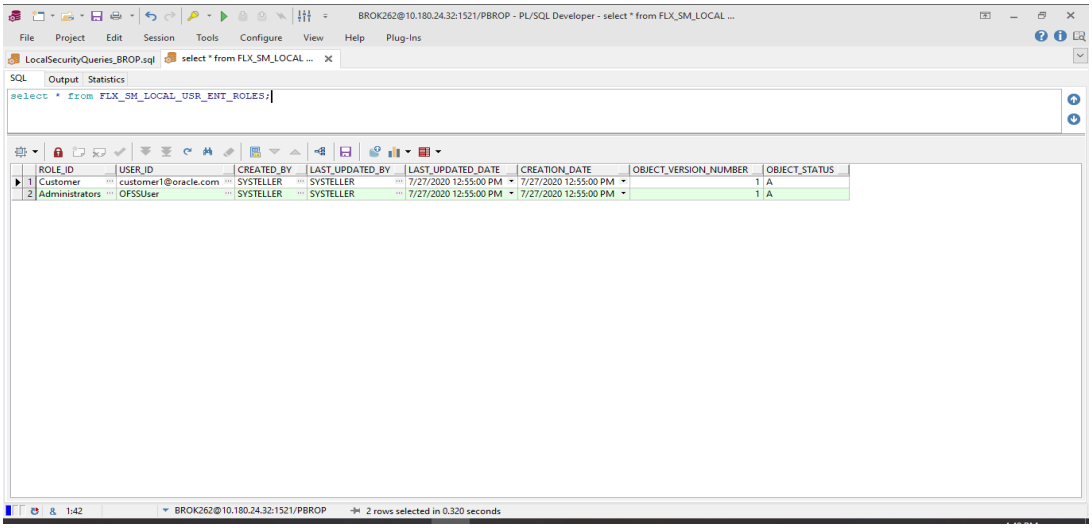
- **FLX_SM_LOCAL_ENT_APP_LNK (Related view FLX_SM_LOCAL_ENT_APP_LNK_V)**: This table defines the mapping between Enterprise Roles and Application Roles.

Figure 3–56 FLX_SM_LOCAL_ENT_APP_LNK



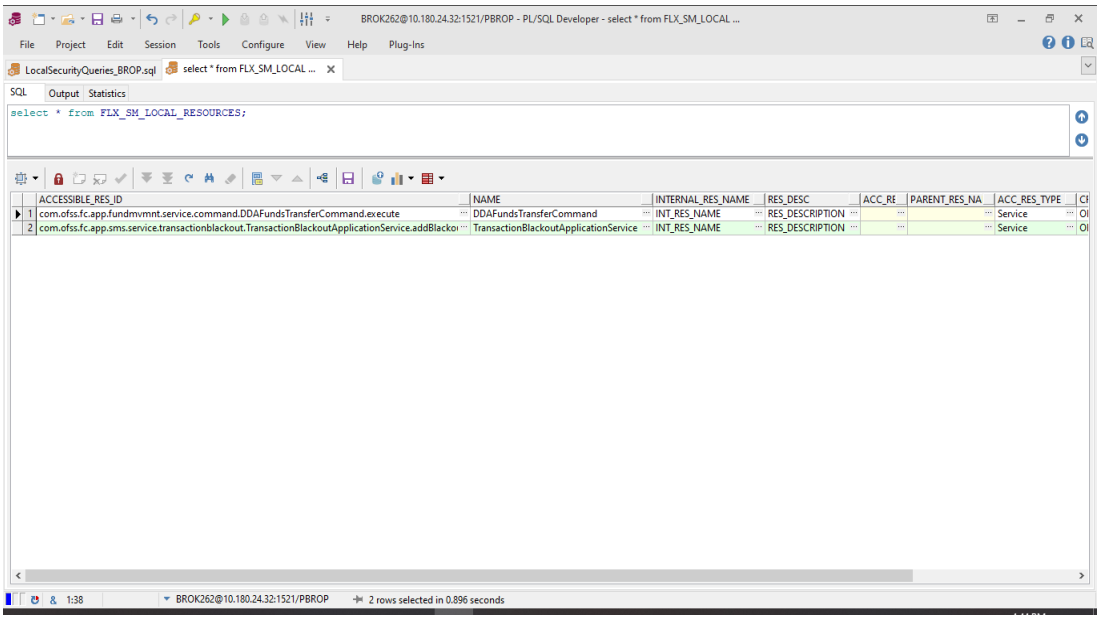
- **FLX_SM_LOCAL_USR_ENT_ROLES (Related view FLX_SM_LOCAL_USR_ENT_ROLES_V)**: This table defines the user id to Application role mapping. All user IDs need to be in lowercase.

Figure 3–57 FLX_SM_LOCAL_USR_ENT_ROLES



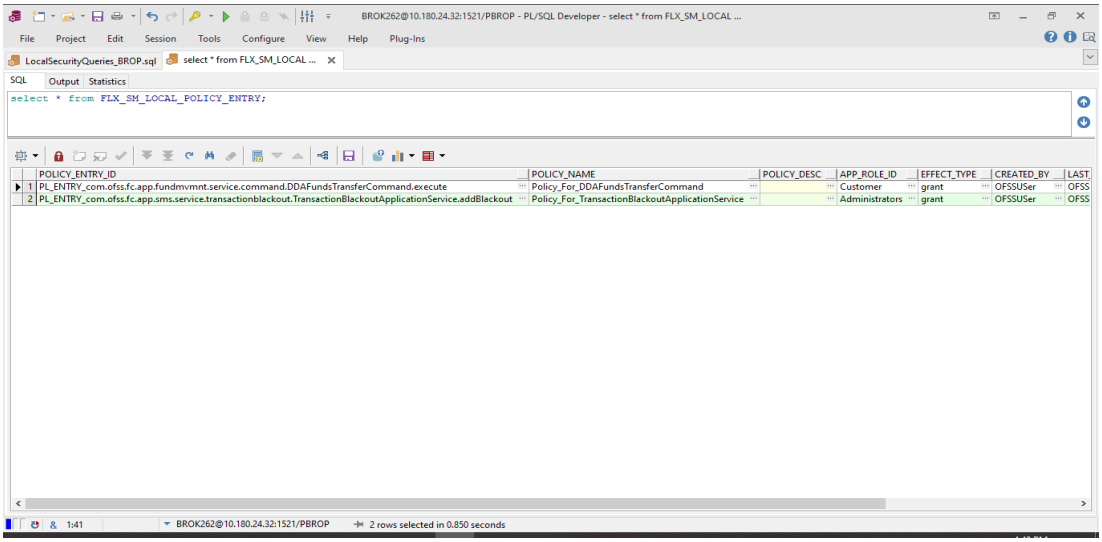
- **FLX_SM_LOCAL_RESOURCES (Related view FLX_SM_LOCAL_RESOURCES_V)**: This table defines the services (fully qualified method name) for which role based access is to be configured.

Figure 3–58 FLX_SM_LOCAL_RESOURCES



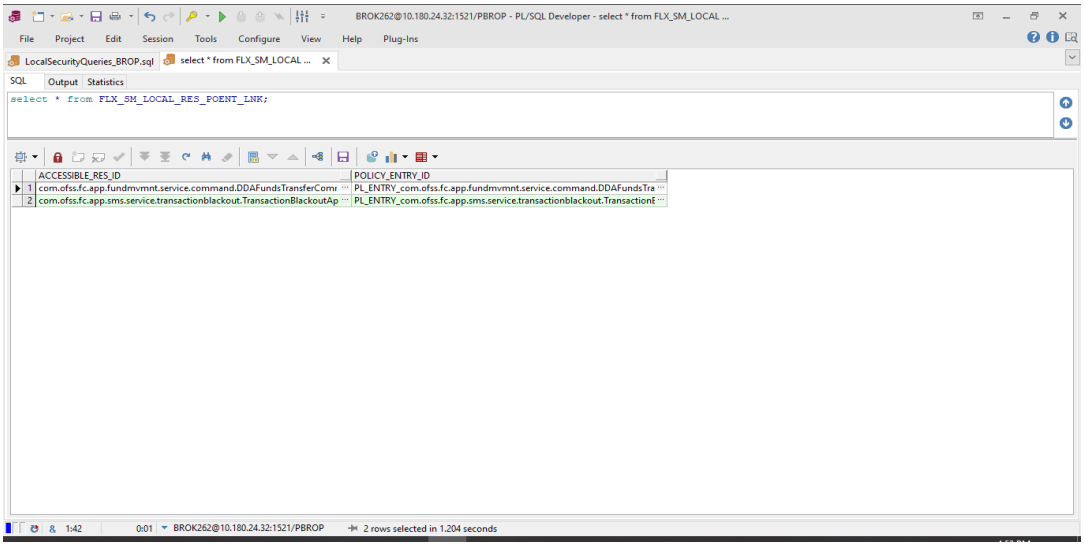
- **FLX_SM_LOCAL_POLICY_ENTRY (Related view FLX_SM_LOCAL_POLICY_ENTRY_V)**: This table defines the access policy based on application role and if access type is grant or deny.

Figure 3–59 FLX_SM_LOCAL_POLICY_ENTRY



- **FLX_SM_LOCAL_RES_POENT_LNK (Related view FLX_SM_LOCAL_RES_POENT_LNK_V)**: This table maps the service with the access policy, that is, ACCESSIBLE_RES_ID from FLX_SM_LOCAL_RESOURCES to POLICY_ENTRY_ID from FLX_SM_LOCAL_POLICY_ENTRY.

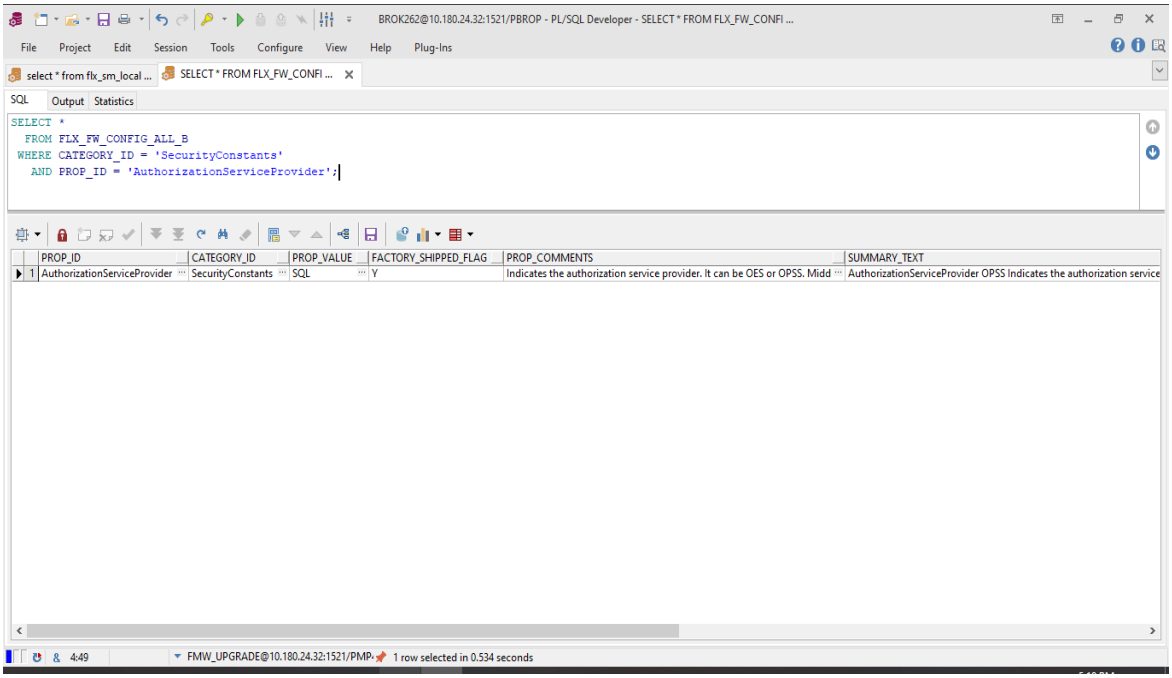
Figure 3–60 FLX_SM_LOCAL_RES_POENT_LNK



To enable DB based menu, following changes need to be made in the configuration (flw_fw_config_all_b):

```
UPDATE FLX_FW_CONFIG_ALL_B
SET PROP_VALUE = 'SQL'
WHERE CATEGORY_ID = 'SecurityConstants'
AND PROP_ID = 'AuthorizationServiceProvider';
```

Figure 3–61 Configuration for DB Menu



The Managed Server needs to be restarted. On restart, access policies from database will come in force, instead of access policies from OPSS.

3.4.2 Role Based Local Menu Configuration

Menu folders and elements will be created by reading the taskflowDefn_element, menu_elements and menu_ folders csv file from **config** folder based on the application and locale.

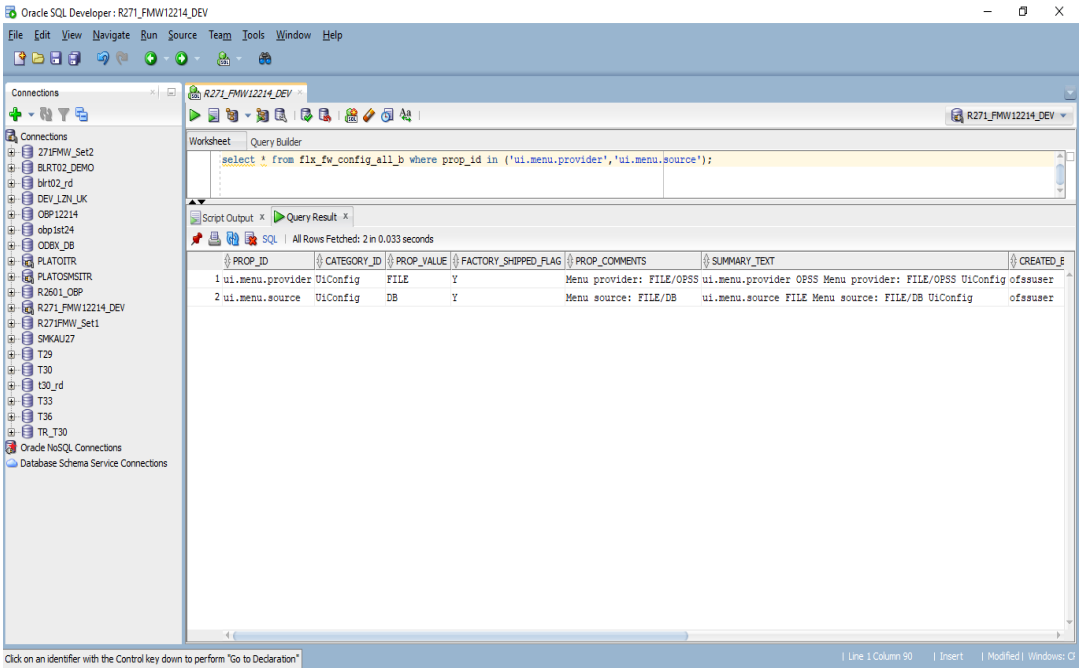
To enable or disable a certain menu element for a particular role:

- From Policy Management (Fast Path: SM502) page, modify the access policy for the pageDef entry for the particular screen to Grant/Deny as required for the particular role.
- The above menu element will be shown/hidden in the menu for users of that role as per access policy defined.
- In case all menu elements in a particular menu folder are denied access, the folder itself will not be seen in menu.

To enable the DB based menu, following changes needed to be made in configuration (flw_fw_config_all_b):

- UPDATE flx_fw_config_all_b SET prop_value = 'FILE' WHERE prop_id = 'ui.menu.provider';
- UPDATE flx_fw_config_all_b SET prop_value = 'DB' WHERE prop_id = 'ui.menu.source';
  Select * from flx_fw_config_all_b WHERE prop_id IN ('ui.menu.provider','ui.menu.source');

Figure 3–62 Configuration for Role Based Menu



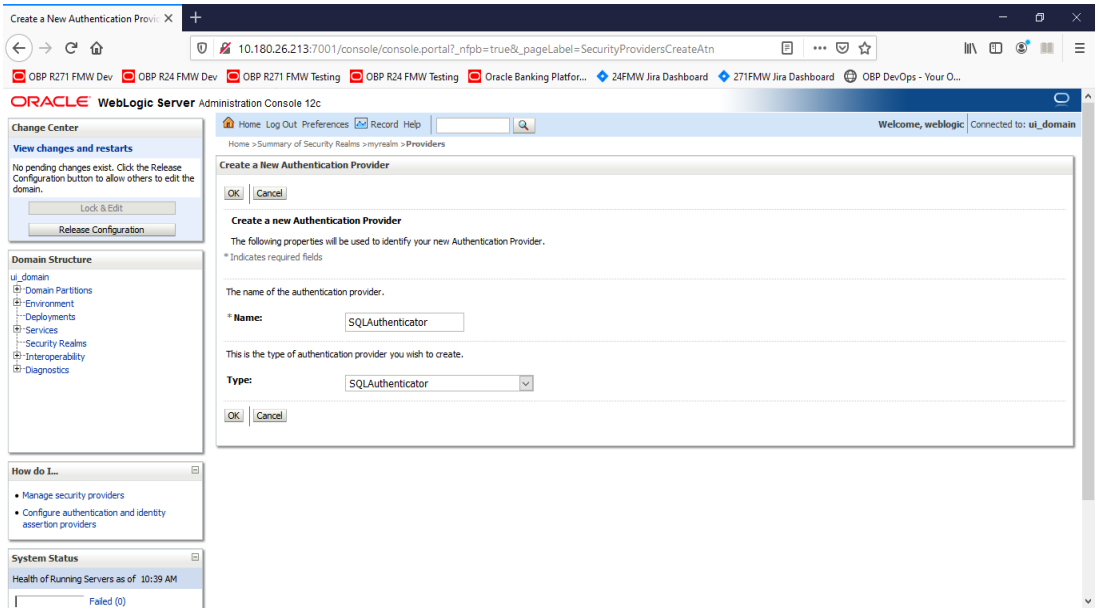
The UI Managed Server needs to be restarted. On login, the menu will be fetched using Menu files (from config) and policies as defined in database instead of OPSS.

3.4.3 Database Identity Store Provider (Both Middleware and UI server)

To create a new security provider in UI and Host WebLogic console:

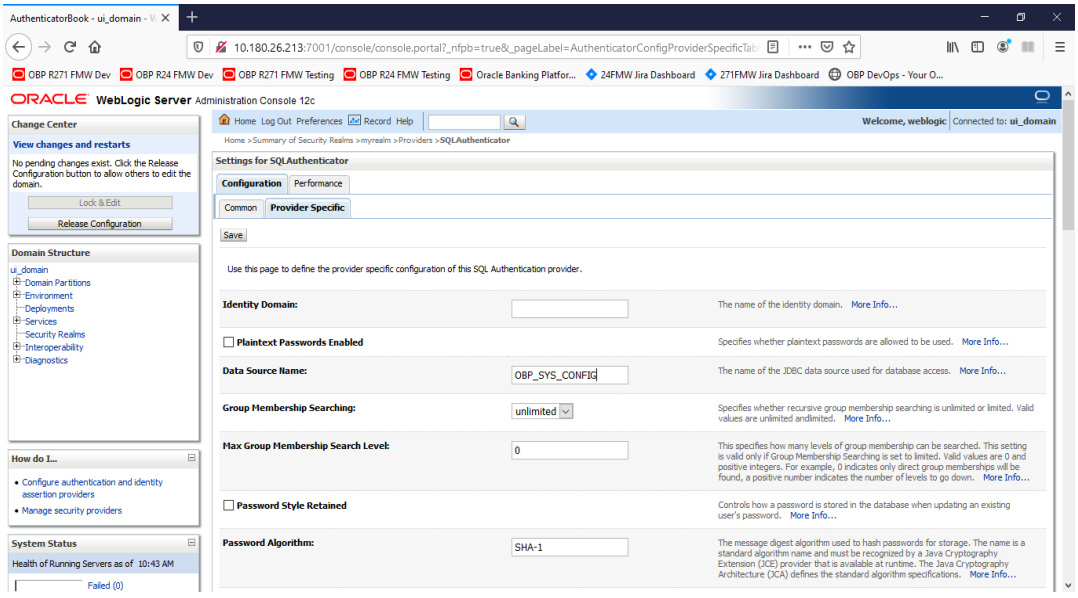
1. Navigate to Security Realms > myrealm > Providers
2. Create a new provider of Type **SQLAuthenticator**

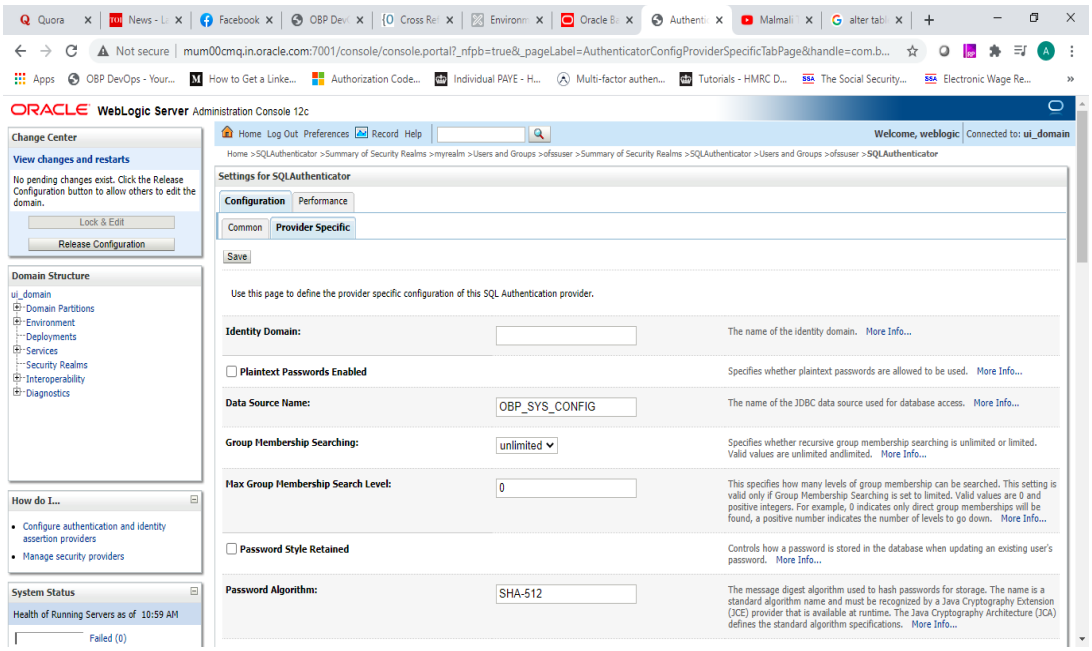
Figure 3–63 Create Authentication Provider



3. In the **Provider Specific** settings, set the Data Source Name e.g. OBP_SYS_CONFIG and set the Password Algorithm to either SHA-512 or SHA-256. (SHA-256 & SHA-512 are supported, product default is SHA-512).

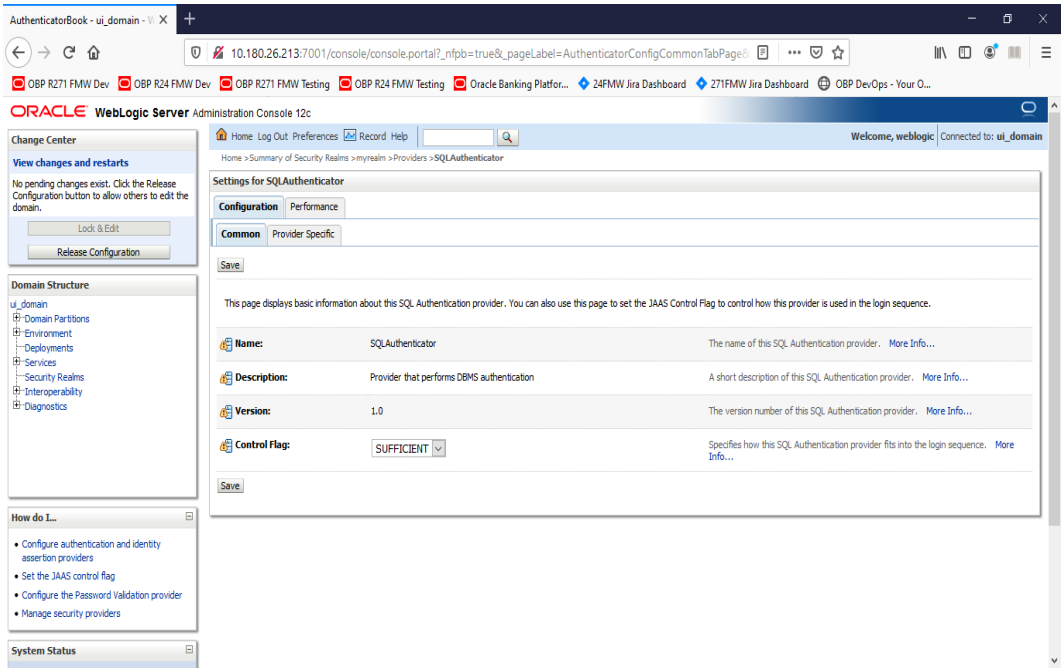
Figure 3–64 Provider Specific Settings





4. According to the Password Algorithm configured, update the **PASSWORD_HASH_ALGO** property value (Category SecurityConstants) in flx_fw_config_all_b table to the same value, that is SHA-512 or SHA-256 (SHA-256 & SHA-512 are supported, product default is SHA-512).
5. Property **HashedPasswordGenerator** in flx_fw_config_all_b table holds the fully qualified class name which will be used for generating hashed value of password. Product default class is com.ofss.fc.sms.local.service.password.SHASaltedHashedPasswordGenerator which supports hashed password generation using SHA-256 or SHA-512 algorithm. In case a different or custom algorithm is to be provided for hashing, respective class will have to be created for the same (which implements IUserHashedPasswordGenerator interface) and specified as value of HashedPasswordGenerator property.
6. In **Common** settings, set the Control Flag to **SUFFICIENT.**

Figure 3–65 Common Settings



Following are the changes to be done in the config.xml:

1. Navigate to **/scratch/app/product/fmw/user_projects/domains/ui_domain/config**
2. Edit config.xml and add the below entries, which are marked in **bold**.

```
<sec:authentication-provider xsi:type="wls:sql-
authenticatorType">
<sec:name>SQLAuthenticator</sec:name>
<sec:control-flag>SUFFICIENT</sec:control-flag>
<wls:data-source-name>OBP_SYS_CONFIG</wls:data-source-name>
<wls:plaintext-passwords-enabled>false</wls:plaintext-
passwords-enabled>
<wls:sql-get-users-password>SELECT PASSWORD FROM USERS WHERE
LOWER(USER_ID) = LOWER(?) AND IS_ACTIVE = 'Y'</wls:sql-get-
users-password>
<wls:sql-user-exists>SELECT USER_ID FROM USERS WHERE LOWER
(USER_ID) = LOWER(?) AND IS_ACTIVE = 'Y'</wls:sql-user-exists>
<wls:sql-list-member-groups>SELECT G_NAME FROM GROUPMEMBERS
WHERE LOWER(G_MEMBER) = LOWER(?)</wls:sql-list-member-groups>
<wls:sql-list-users>SELECT USER_ID FROM USERS WHERE LOWER
(USER_ID) LIKE LOWER(?) AND IS_ACTIVE = 'Y'</wls:sql-list-
users>
<wls:sql-get-user-description>SELECT NAME FROM USERS WHERE
LOWER(USER_ID) = LOWER(?) AND IS_ACTIVE = 'Y'</wls:sql-get-
user-description>
<wls:sql-list-groups>SELECT ROLE_NAME FROM ROLES WHERE ROLE_
NAME LIKE ?</wls:sql-list-groups>
```

```
<wls:sql-group-exists>SELECT ROLE_NAME FROM ROLES WHERE ROLE_
NAME = ?</wls:sql-group-exists>
<wls:sql-is-member>SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_
NAME = ? AND LOWER(G_MEMBER) = LOWER(?)</wls:sql-is-member>
<wls:sql-get-group-description>SELECT ROLE_DESCRIPTION FROM
ROLES WHERE ROLE_NAME = ?</wls:sql-get-group-description>
<wls:password-style-retained>false</wls:password-style-
retained>
<wls:sql-create-user>INSERT INTO USERS VALUES (?, ?, ?, ?, ?,
?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?,
?)</wls:sql-create-user>
<wls:sql-remove-user>DELETE FROM USERS WHERE LOWER(USER_ID) =
LOWER(?)</wls:sql-remove-user>
<wls:sql-remove-group-memberships>DELETE FROM GROUPMEMBERS
WHERE LOWER(G_MEMBER) = LOWER(?) OR G_NAME = ?</wls:sql-
remove-group-memberships>
<wls:sql-set-user-description>UPDATE USERS SET NAME = ? WHERE
LOWER(USER_ID) = LOWER(?)</wls:sql-set-user-description>
<wls:sql-set-user-password>UPDATE USERS SET PASSWORD = ? WHERE
LOWER(USER_ID) = LOWER(?)</wls:sql-set-user-password>
<wls:sql-create-group>INSERT INTO ROLES VALUES ( ? , ?
)</wls:sql-create-group>
<wls:sql-set-group-description>UPDATE ROLES SET ROLE_
DESCRIPTION = ? WHERE ROLE_NAME = ?</wls:sql-set-group-
description>
<wls:sql-remove-member-from-group>DELETE FROM GROUPMEMBERS
WHERE G_NAME = ? AND LOWER(G_MEMBER) = LOWER(?)</wls:sql-
remove-member-from-group>
<wls:sql-remove-group>DELETE FROM ROLES WHERE ROLE_NAME =
?</wls:sql-remove-group>
<wls:sql-list-group-members>SELECT G_MEMBER FROM GROUPMEMBERS
WHERE G_NAME = ? AND LOWER(G_MEMBER) LIKE LOWER(?)</wls:sql-
list-group-members>
</sec:authentication-provider>
```

Note

In **<wls:sql-create-user>INSERT INTO USERS VALUES (?, ?)</wls:sql-create-user>**, the number of '?' need to be same as the number of columns in the view Users.

The database configuration are as follows:

- The tables already created as part of DB based Policy configuration:
  - Users Table: FLX_SM_LOCAL_USERS
  - Groups Table: FLX_SM_LOCAL_APP_ROLES

- Members to Group mapping Table: FLX_SM_LOCAL_USR_ENT_ROLES

- To view Creation scripts:

1. CREATE OR REPLACE VIEW USERS AS

   SELECT NAME,
   USER ID,
   FIRST_NAME,
   LAST_NAME,
   USER_DESCRIPTION,
   PASSWORD,
   MANAGER,
   DEPARTMENT,
   DATE_OF_BIRTH,
   BUSINESS_EMAIL,
   PREFFERED_LANGUAGE,
   USER_HOME_BRANCH,
   LAST_LOGIN_DATE,
   TWOFA_NONACTIVE_BEGIN_DATE,
   TWOFA_NONACTIVE_END_DATE,
   TWOFA_STATUS,
   BRAND,
   IS_ENROLLED_FOR_TWOFA,
   PARTY_ID,
   CORPORATE_PARTY_ID,
   FORUM_NICK_NAME,
   ACCREDITATION,
   TARGET_UNIT,
   ACCESSIBLE_TARGET_UNIT,
   IS_ACTIVE
   FROM FLX_SM_LOCAL_USERS;

2. CREATE OR REPLACE VIEW ROLES

   (role_name, role_description)

   AS

   SELECT app_rl_ID, DESCRIPTION FROM FLX_SM_LOCAL_APP_ROLES;

3. CREATE OR REPLACE VIEW GROUPMEMBERS

(g_name, g_member)

AS

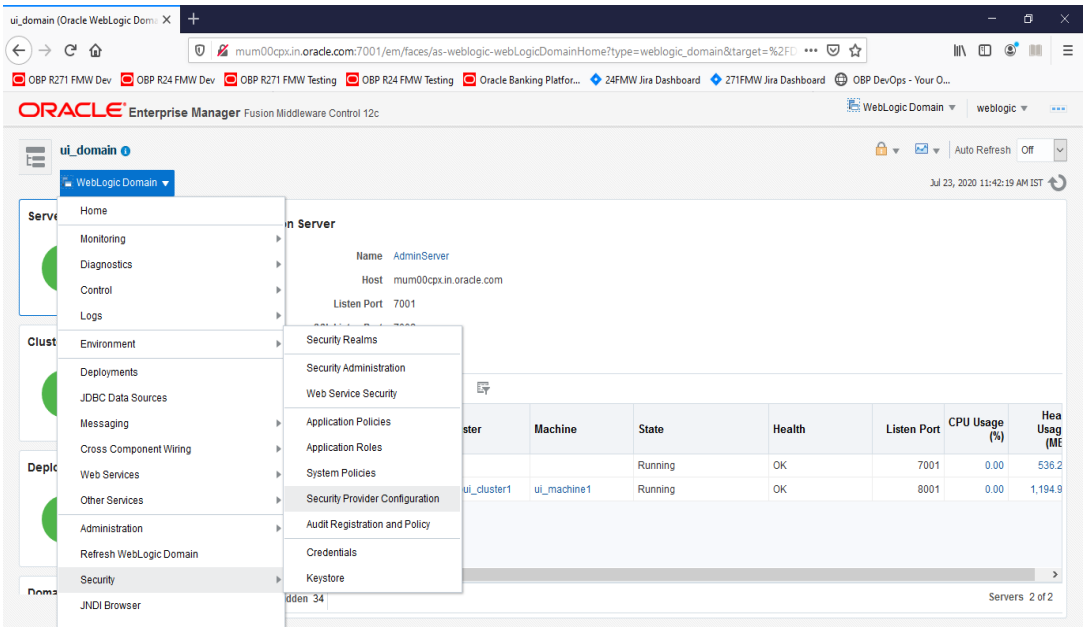
SELECT role_id, USER_ID FROM FLX_SM_LOCAL_USR_ENT_ROLES;

Note

The entries in SQLAuthenticator are as per these views.

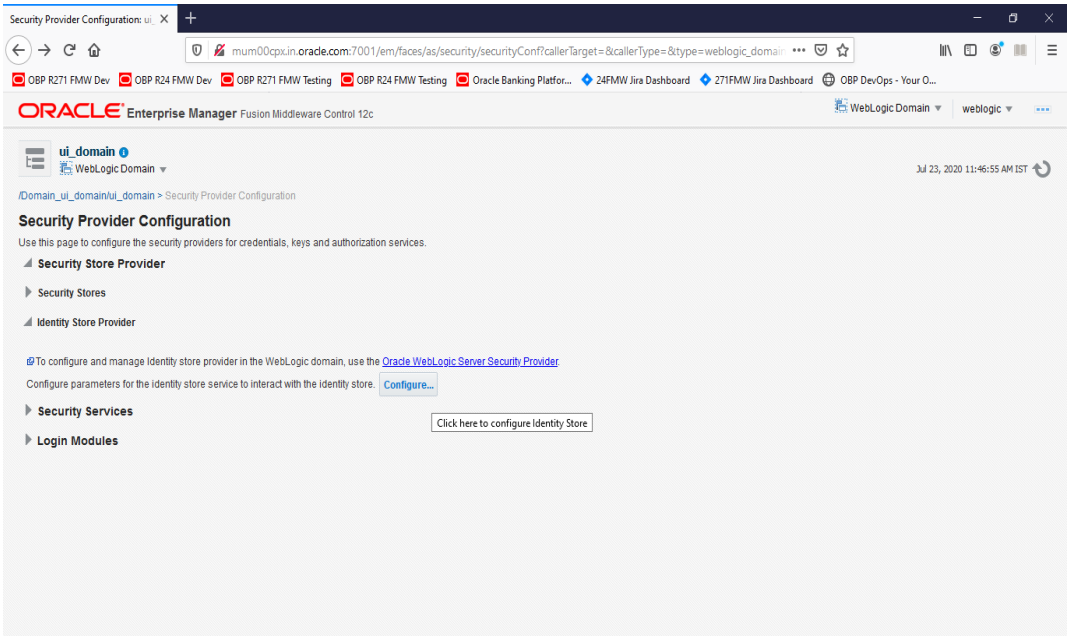
- To configure the Virtualized Identity Store Provider:
  1. In Enterprise Manager, click on WebLogic Domain (under ui_domain), select Security > Security Provider Configuration to display the Security Provider Configuration page.

Figure 3–66 Service Provider Configuration



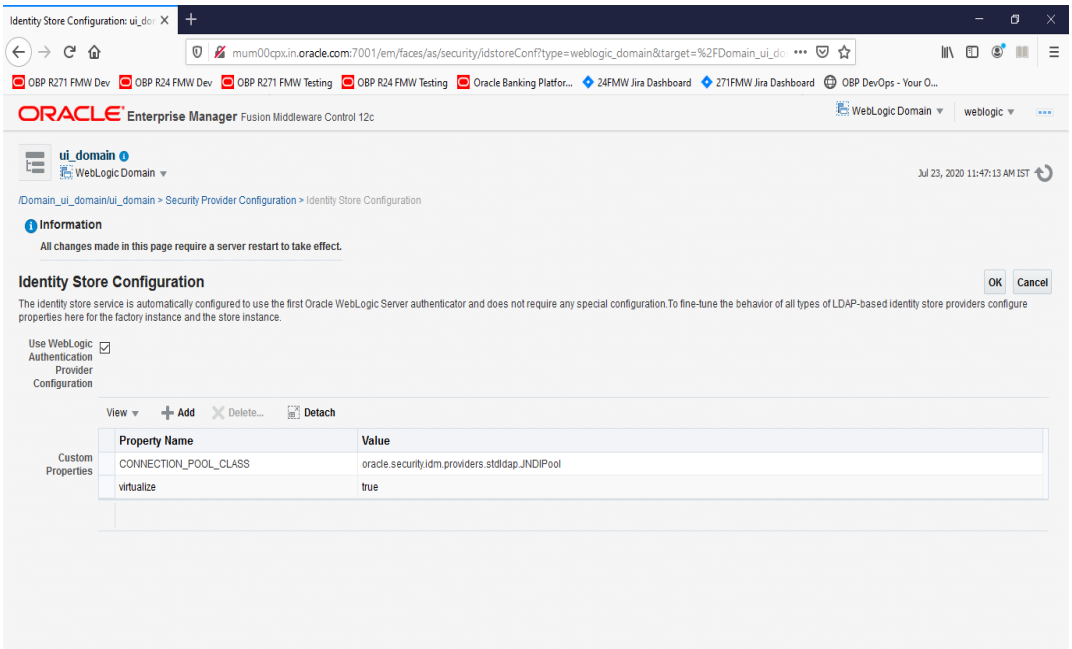
2. Expand **Security Store Provider**, then **Identity Store Provider** and click on **Configure.**

Figure 3–67 Identifying Store Provider for Configuration



3. Add a new Custom Property called **virtualize** with value **true.**

Figure 3–68 Adding Custom Property Virtualize with value True



4. Click **OK** to save the changes.

5. Restart the Admin Server and Managed Server(s).

- To create adapters for using tables as Identity Store:

1. Create a file named adapter_template_usergroup1.xml. This file is used to describe the mapping of the user table to a virtual LDAP store.

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<adapters schvers="303" version="1"
xmlns="http://www.octetstring.com/schemas/Adapters"
xmlns:adapters="http://www.w3.org/2001/XMLSchema-
instance">
<dataBase id="directoryType" version="0">
<root>%ROOT%</root>
<active>true</active>
<serverType>directoryType</serverType>
<routing>
<critical>true</critical>
<priority>50</priority>
<inclusionFilter/>
<exclusionFilter/>
<plugin/>
<retrieve/>
<store/>
<visible>Yes</visible>
<levels>-1</levels>
<bind>true</bind>
<bind-adapters/>
<views/>
<dnpattern/>
</routing>
<pluginChains
xmlns="http://xmlns.oracle.com/iam/management/ovd/config
/plugins">
<plugins>
<plugin>
<name>DBGUID</name>
<class>oracle.ods.virtualization.engine.chain.plugins.db
guid.DBGuidPlugin
</class>
<initParams>
<param name="guidAttribute" value="orclguid"/>
</initParams>
</plugin>
</plugins>
<default>
<plugin name="DBGUID"/>
</default>
```

```
<add/>
<bind/>
<delete/>
<get/>
<modify/>
<rename/>
</pluginChains>
<driver>oracle.jdbc.driver.OracleDriver</driver>
<url>%URL%</url>
<user>%USER%</user>
<password>%PASSWORD%</password>
<ignoreObjectClassOnModify>false</ignoreObjectClassOnMod
ify>
<includeInheritedObjectClasses>true</includeInheritedObj
ectClasses>
<maxConnections>10</maxConnections>
<mapping>
<joins/>
<objectClass name="person" rdn="cn">
<attribute ldap="cn" table="USERS" field="NAME" type=""/>
<attribute ldap="uid" table="USERS" field="USER_ID"
type=""/>
<attribute ldap="usernameattr" table="USERS" field="NAME"
type=""/>
<attribute ldap="loginid" table="USERS" field="USER_ID"
type=""/>
<attribute ldap="description" table="USERS" field="NAME"
type=""/>
<attribute ldap="orclguid" table="USERS" field="USER_ID"
type=""/>
</objectClass>
</mapping>
<useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
<connectionWaitTimeout>10</connectionWaitTimeout>
<oracleNetConnectTimeout>0</oracleNetConnectTimeout>
<validateConnection>false</validateConnection>
</dataBase>
</adapters>
```

2. Create a file named adapter_template_usergroup2.xml to describe the mapping of the group table to a virtual LDAP store.

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<adapters schvers="303" version="1"
xmlns="http://www.octetstring.com/schemas/Adapters"
xmlns:adapters="http://www.w3.org/2001/XMLSchema-
instance">
```

```
<dataBase id="directoryType" version="0">
<root>%ROOT%</root>
<active>true</active>
<serverType>directoryType</serverType>
<routing>
<critical>true</critical>
<priority>50</priority>
<inclusionFilter/>
<exclusionFilter/>
<plugin/>
<retrieve/>
<store/>
<visible>Yes</visible>
<levels>-1</levels>
<bind>true</bind>
<bind-adapters/>
<views/>
<dnpattern/>
</routing>
<pluginChains
xmlns="http://xmlns.oracle.com/iam/management/ovd/config
/plugins">
<plugins>
<plugin>
<name>VirtualAttribute</name>
<class>oracle.ods.virtualization.engine.chain.plugins.vi
rtualattr.VirtualAttributePlugin
</class>
<initParams>
<param name="ReplaceAttribute"
value="uniquemember=
{cn=%uniquemember%,cn=users,dc=in,dc=oracle,dc=com}"/>
</initParams>
</plugin>
</plugins>
<default>
<plugin name="VirtualAttribute"/>
</default>
<add/>
<bind/>
<delete/>
<get/>
<modify/>
<rename/>
</pluginChains>
<driver>oracle.jdbc.driver.OracleDriver</driver>
```

```
<url>%URL%</url>
<user>%USER%</user>
<password>%PASSWORD%</password>
<ignoreObjectClassOnModify>false</ignoreObjectClassOnMod
ify>
<includeInheritedObjectClasses>true</includeInheritedObj
ectClasses>
<maxConnections>10</maxConnections>
<mapping>
<joins/>
<objectClass name="groupofuniquenames" rdn="cn">
<attribute ldap="cn" table="GROUPMEMBERS" field="G_NAME"
type=""/>
<attribute ldap="description" table="GROUPMEMBERS"
field="G_NAME" type=""/>
<attribute ldap="uniquemember" table="GROUPMEMBERS"
field="G_MEMBER" type=""/>
</objectClass>
</mapping>
<useCaseInsensitiveSearch>true</useCaseInsensitiveSearch>
<connectionWaitTimeout>10</connectionWaitTimeout>
<oracleNetConnectTimeout>0</oracleNetConnectTimeout>
<validateConnection>false</validateConnection>
</dataBase>
</adapters>
```

3. Set below environment variables:
   - export MW_HOME=/scratch/app/product/fmw
   - export ORACLE_HOME=/scratch/app/product/fmw
   - export WL_HOME=/scratch/app/product/fmw/wlserver
   - export JAVA_HOME=/scratch/app/product/jdk1.8.0_231 (Modify as applicable)
4. Copy both the adapter files to <MW_HOME>/oracle_common/modules/oracle.ovd/templates
5. Open terminal window at <MW_HOME>/oracle_common/bin
6. Run the libovdadapterconfig script to create each of the two adapters from the template files above.
   libovdadapterconfig -adapterName <name of adapter> -adapterTemplate <name (NOT including path) of template file which defines adapater> -host localhost -port <Admin Server port> -userName <user id of account which has administrative privileges in the domain> -domainPath <path to the BI domain> -dataStore DB -root <nominal specification of a pseudo-LDAP query to treat as the “root” of this adapter – must match that specified in template for adapter 2 above> -contextName default -dataSourceJNDIName <JNDI name for DataSource which points at the database being mapped>

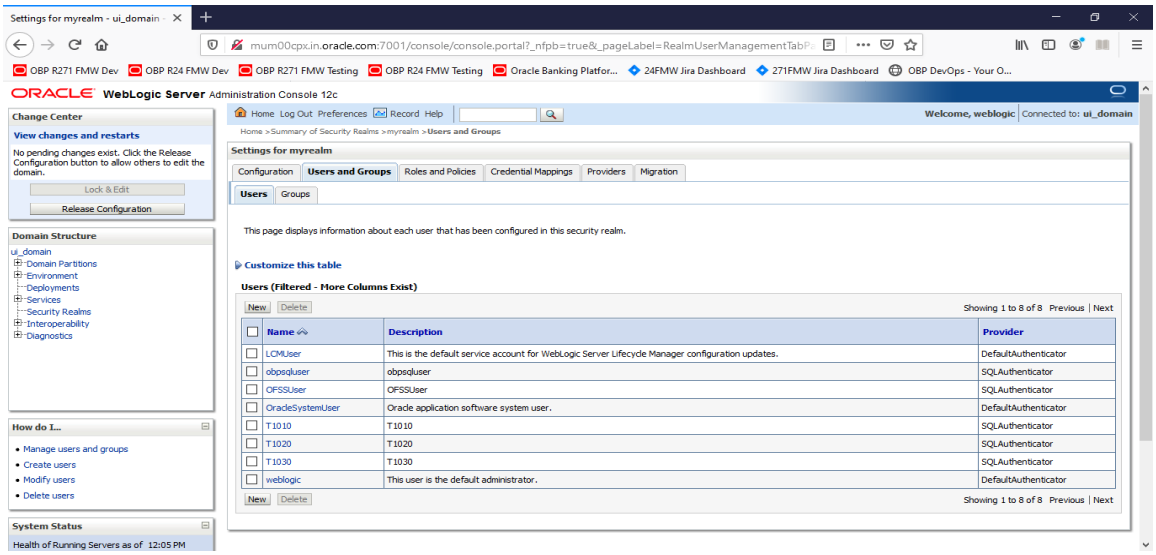
   For example:

./libovdadapterconfig.sh -adapterName userGroupAdapter1 -adapterTemplate adapter_template_usergroup1.xml -host 10.180.26.213 -port 7001 -userName weblogic -domainPath /scratch/app/product/fmw/user_projects/domains/ui_domain/ -dataStore DB -root cn=users,dc=in,dc=oracle,dc=com -contextName default -dataSourceJNDIName jdbc/FCBDataSourceConfig

./libovdadapterconfig.sh -adapterName userGroupAdapter2 -adapterTemplate adapter_template_usergroup2.xml -host 10.180.26.213 -port 7001 -userName weblogic -domainPath /scratch/app/product/fmw/user_projects/domains/ui_domain/ -dataStore DB -root cn=users,dc=in,dc=oracle,dc=com -contextName default -dataSourceJNDIName jdbc/FCBDataSourceConfig

The users created in database tables will be visible in WebLogic console under myrealm > Users and Groups.

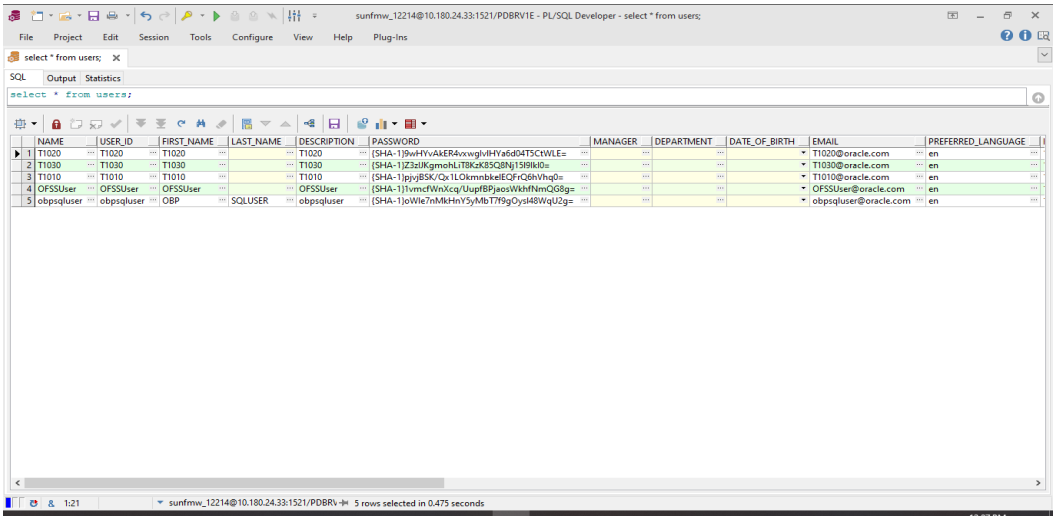
Figure 3–69 Users and Groups



Following are the data snapshot in the views created:

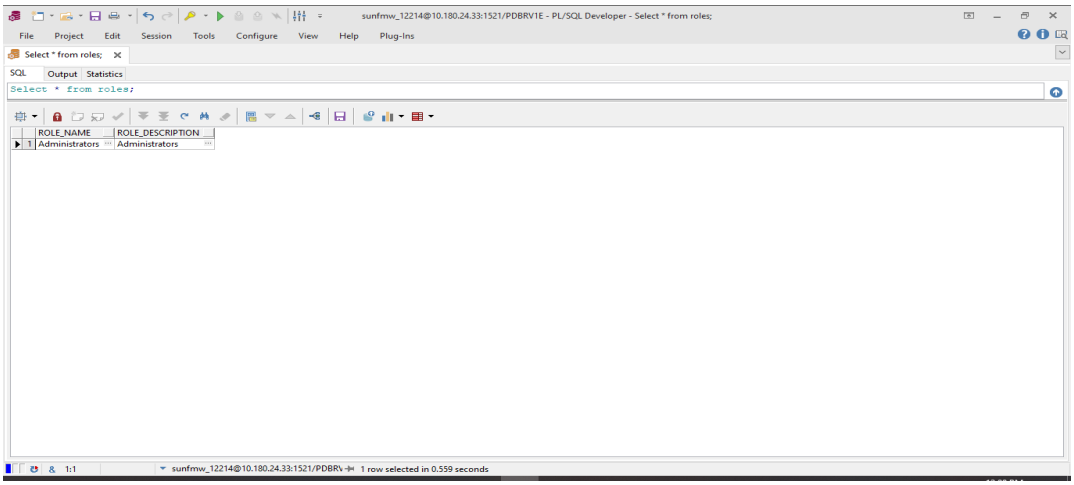
- Select * from users;

Figure 3–70 Selecting from Users



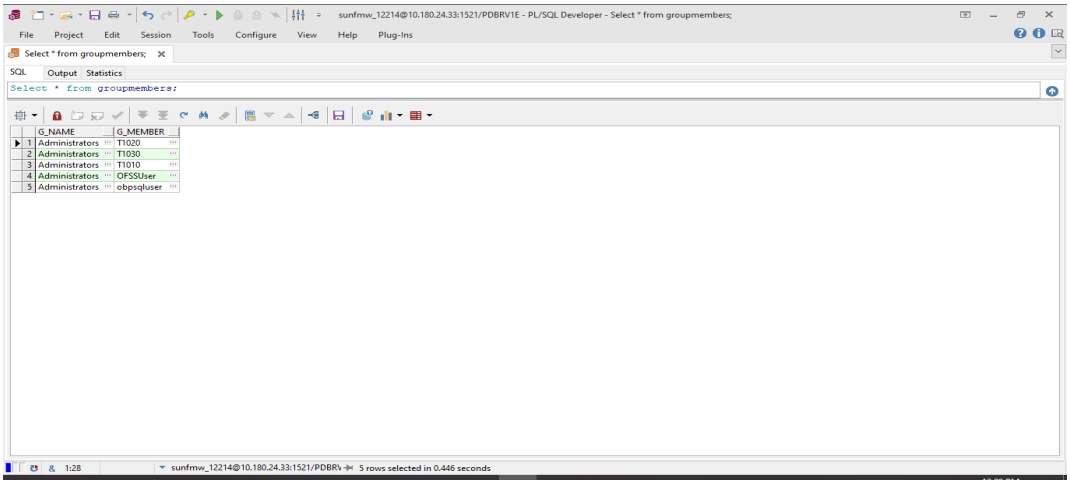
- Select * from roles;

Figure 3–71 Selecting from Roles



- Select * from groupmembers;

Figure 3–72 Selecting from Groupmembers



The user is now created in the database and can log in.

4 User Fields and Constraints

This chapter provides information on the user provisioning fields and related constraints.

4.1 User Fields Provisioned From OIM

You must follow the constraints (listed in the table below) to provision user to Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery irrespective of the constraints in OIM.

Irrespective of the field length allowed in OIM, you should restrict the field length to the specified values (in table below) for successful provisioning of user data. In case, if field length exceeds the specified limit, then data would be truncated and stored in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery.

The following table lists of user fields (provisioned from OIM) and its constraints.

Table 4–1 User Fields

Field Name in OIM	Field Name in Collections Admin Application	Length	Mandatory (Y/N)	Modifiable (Y/N)	Comments
User Login	User Id	255	Y	N	You can modify this field name.
First Name	First Name	50	Y	Y	Users First Name
Last Name	Last Name	50	Y	Y	Users Last Name
Email	Email Address	70	Y	Y	Users Email address
Collections User Group	User Group	20	N	Y	This User Group represents User Group in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery. For every User, default User Group is populated in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery.
End Date	Date	N	Y	User's Log in expiry date.	

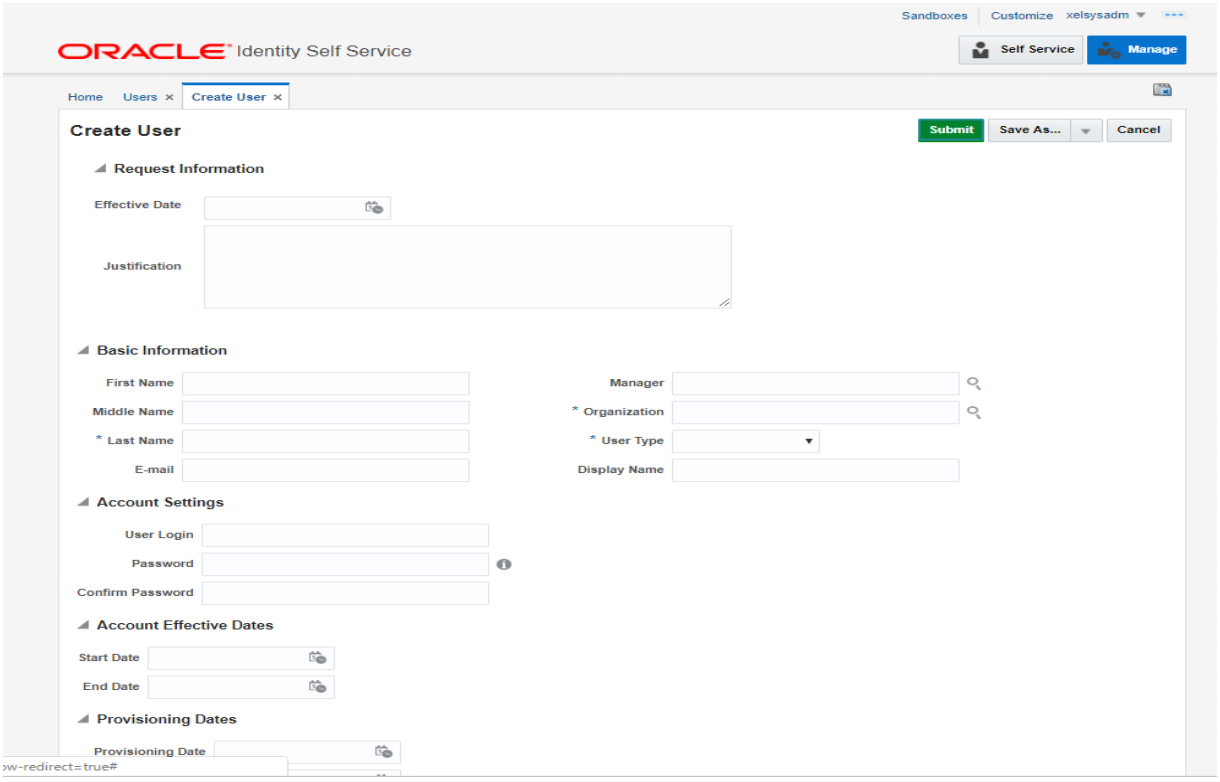
Note

User creation from Native Collections Admin Application is primarily discouraged. But in case of any failure in provisioning through OIM, you

can create or update the users through Native Collections Admin Application screen. Below are the constraints to be followed when user is to be created through Native Collections Admin Application:

- User login is not supported in lowercase. User login must be entered in uppercase only. (Same should be taken into account while creating user through OID or OIM.)
- Only system admin users will have access to create or modify users via Native Collections Admin screen.

Figure 4–1 Create User - Mandatory and Optional Attributes



Collections Mandatory Attributes:

1. First Name
2. Last Name
3. Email
4. User Login

Collections Optional Attribute:

1. End Date

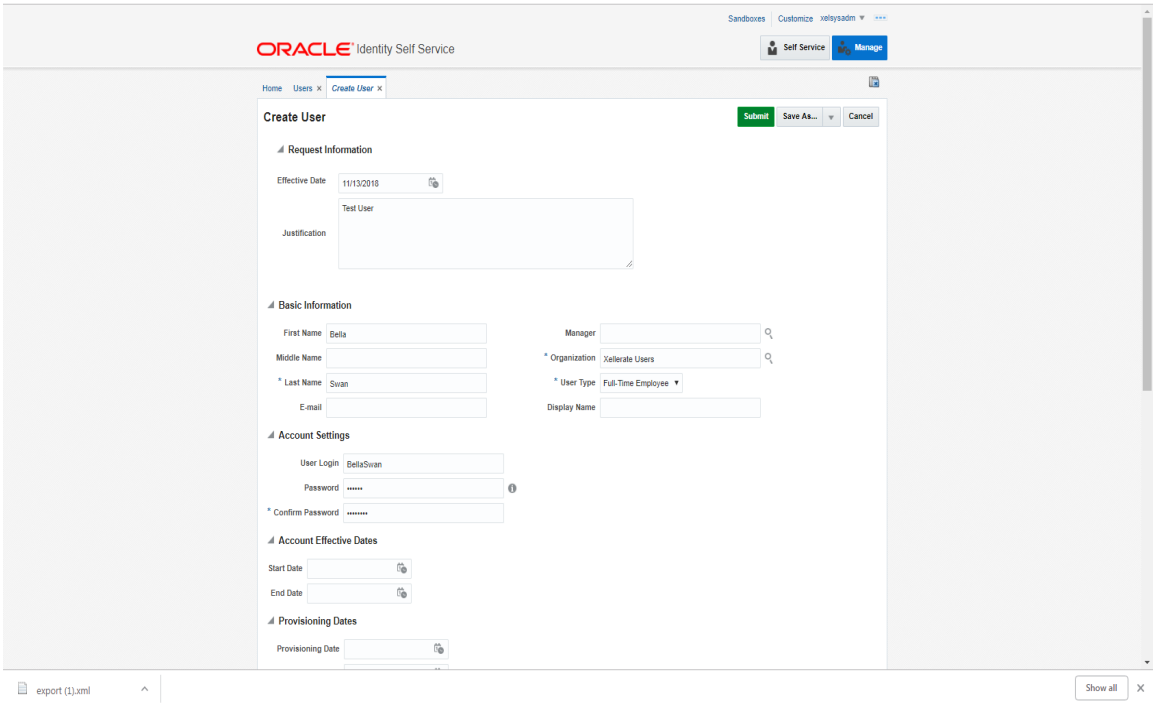
5 Create, Modify, Delete Users using OIM

This chapter explains the process of creating and provisioning users using OIM.

5.1 Create and Provision Users

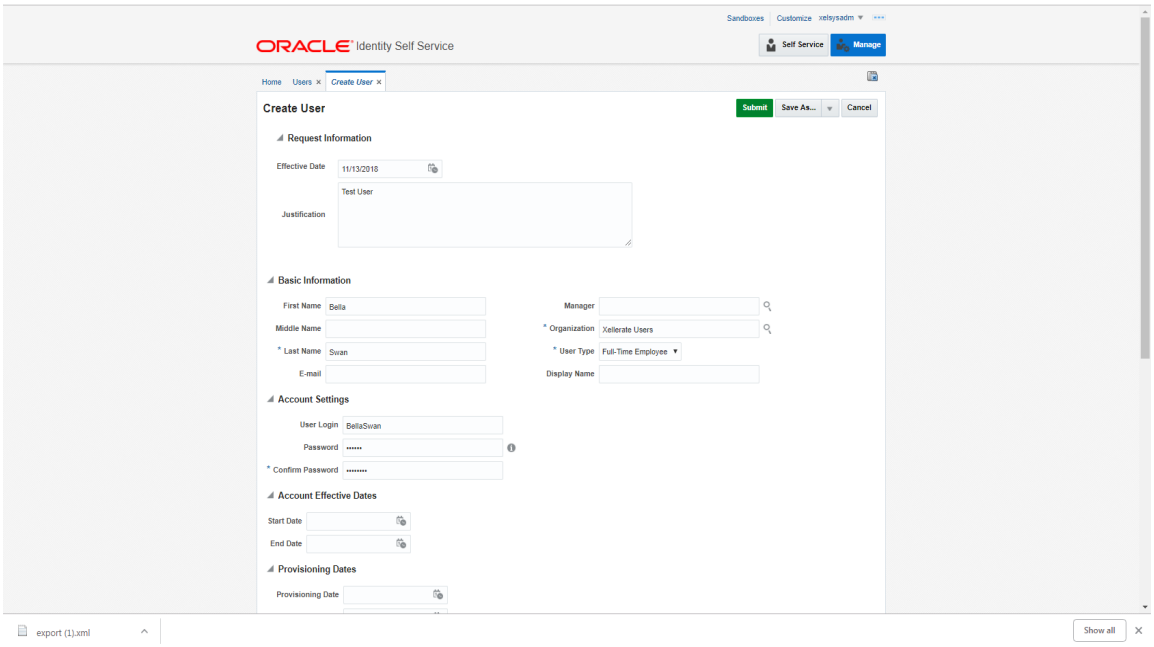
1. Log in OIM Identity Self Service.
2. Click **Users** and then click **Create**.
   The Create User tab opens.

Figure 4–2 Create User in Oracle Identity Self Service



3. Provide the user details such as FirstName, LastName, UserLogin, Password, Organization='Xellerate Users', UserType and so on.

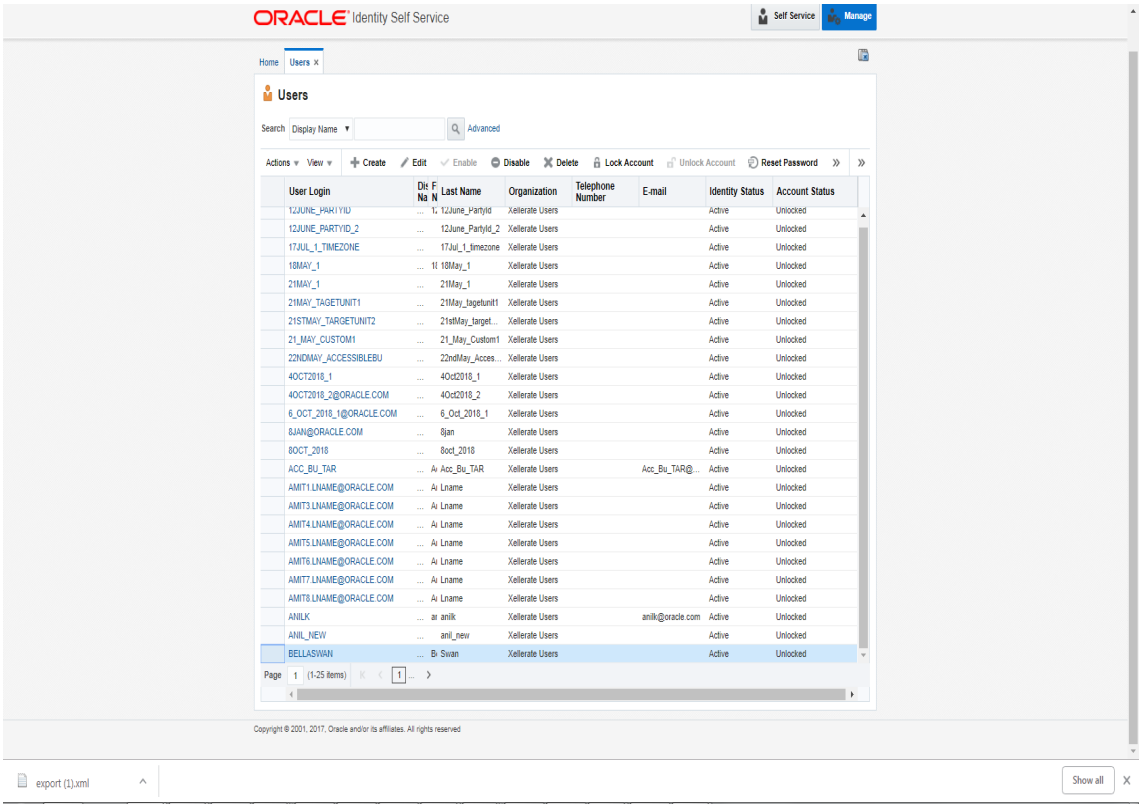
Figure 4–3 Input User Attributes



4. Click **Submit**.
5. In the Search Users page, click **Refresh**. The above created user is visible.

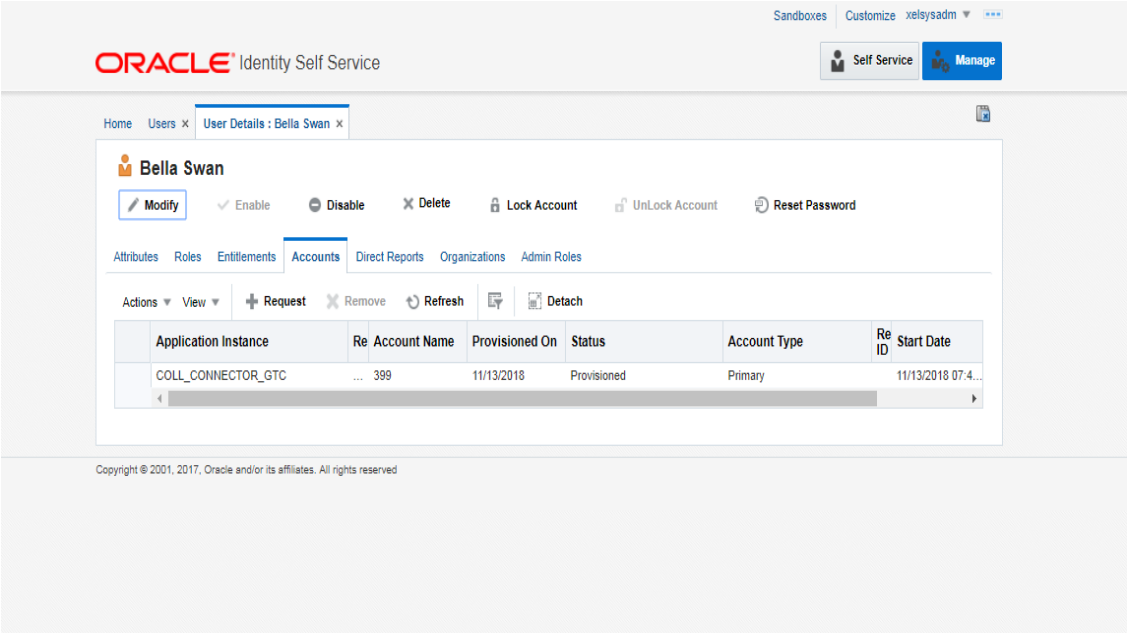
6. Click the above created user.

Figure 4–4 Search and select the added User



7. Go to the Accounts tab.

Figure 4–5 Applications provisioned to User



8. Verify the COLL_CONNECTOR_GTC application is in **Provisioned** status.

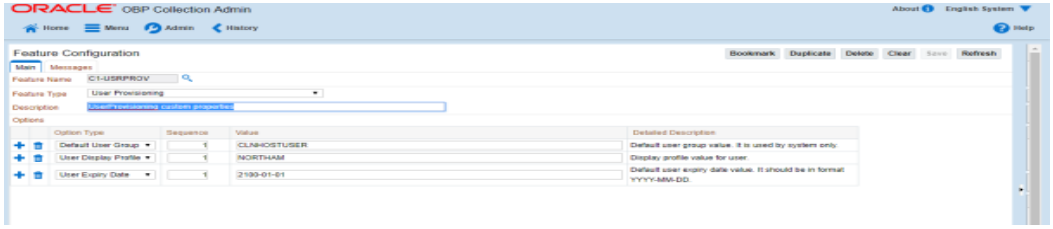
5.2 Feature Configurations

Collections Admin Application provides feature configuration C1-USRPROV to specify default values of the following:

- **Default User Group**: Default Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Group. It is used by system only. User should not add it manually. See the Day Zero Setup guide to get configured default user group.
- **User Display Profile**: Display profile value for Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User. Configure as per your environment.
  - **User Expiry Date**: Default value of User expiry date. If expiry date is not provided, this value is used. It should be in format YYYY-MM-dd.

> **Note**
>
> Feature Configuration can be updated using native Collections Admin Application screens.

Figure 4–6 Feature Configuration



5.3 Modify Users

Once user is added, it can be modified. Following are the modifiable fields:

- First Name
- Last Name
- Collections User Group
- Email
- End Date

You can search and modify the user. To search for user:

1. Log in to Oracle Identity Self Service.
2. In the Manage tab, you can search for the user from Users tab.
3. Click the searched user data to view its detail.

Figure 4–7 Searching User

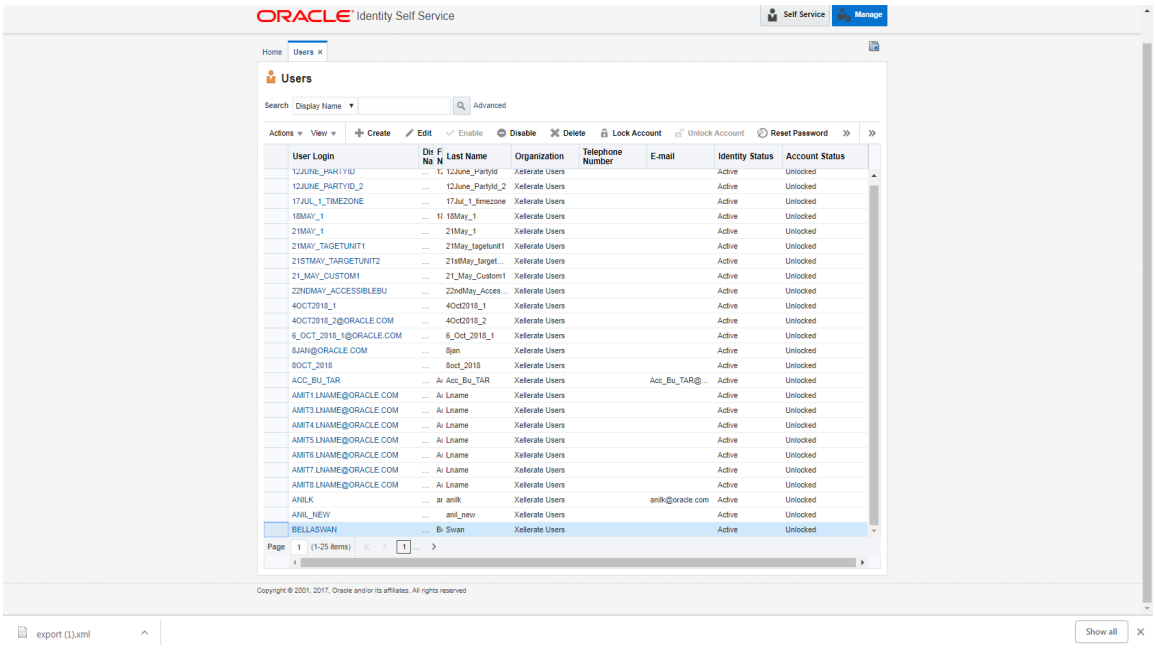
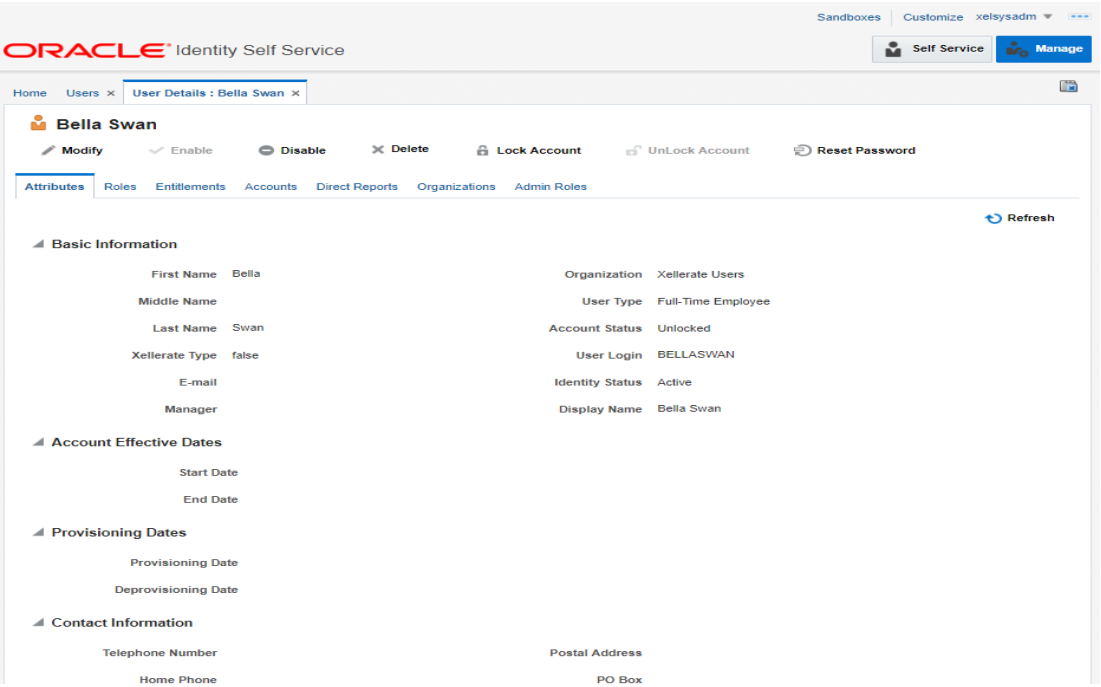


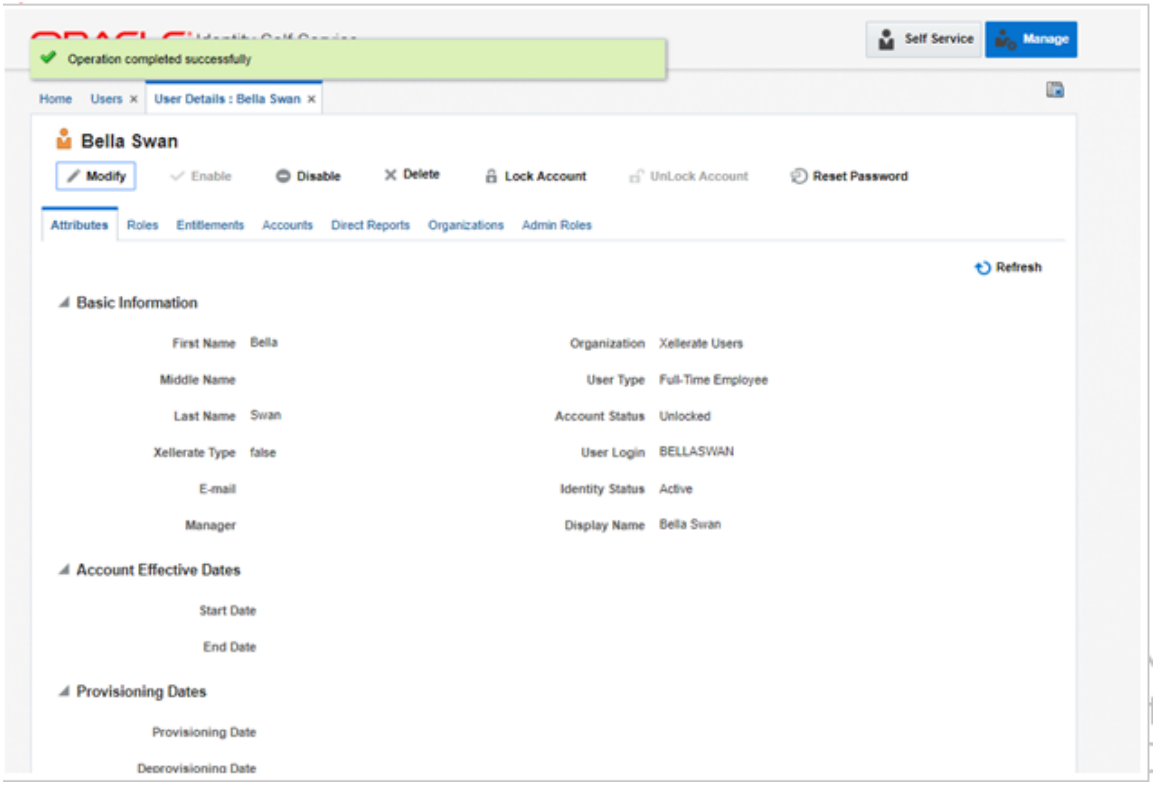
Figure 4–8 Detailed Information about the User



To modify a user:

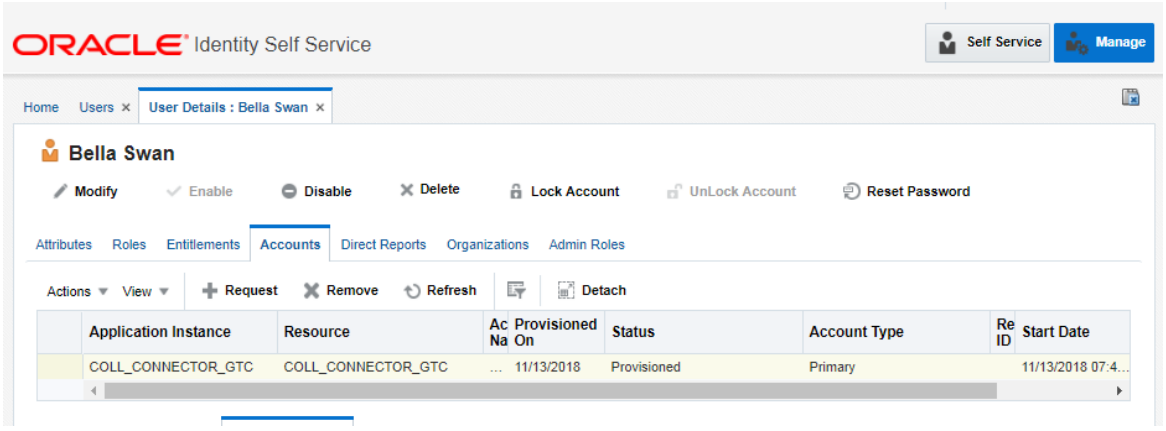
1. Click **Modify** to open Modify User page.
2. Modify the user details as per the requirement.
3. Click **Submit**. If the user details are valid (that is, if it does not violate any validation) then user details are modified. A message appears on successful completion of the modify operation. This does not guarantee successful modification of the user in Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery.

Figure 4–9 Modify User Confirmation



4. In User Details page, open the **Accounts** tab. If Resource Name is COLL_CONNECTOR_GTC Collection User and Status is **Provisioned**, then user details are successfully modified and provisioned to Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery.
5. If the data does not appear when the user is added, click **Refresh**.

Figure 4–10 Viewing Modified and Provisioned User Details



6. Select the account to view the modified values in **Detail Information** section.

7. To modify the Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Group, follow the below steps:
    a. In the **Accounts** tab, select the account that you want to modify.
    b. From the **Actions** menu, select **Modify**.

Figure 4–11 Modify Detail Information

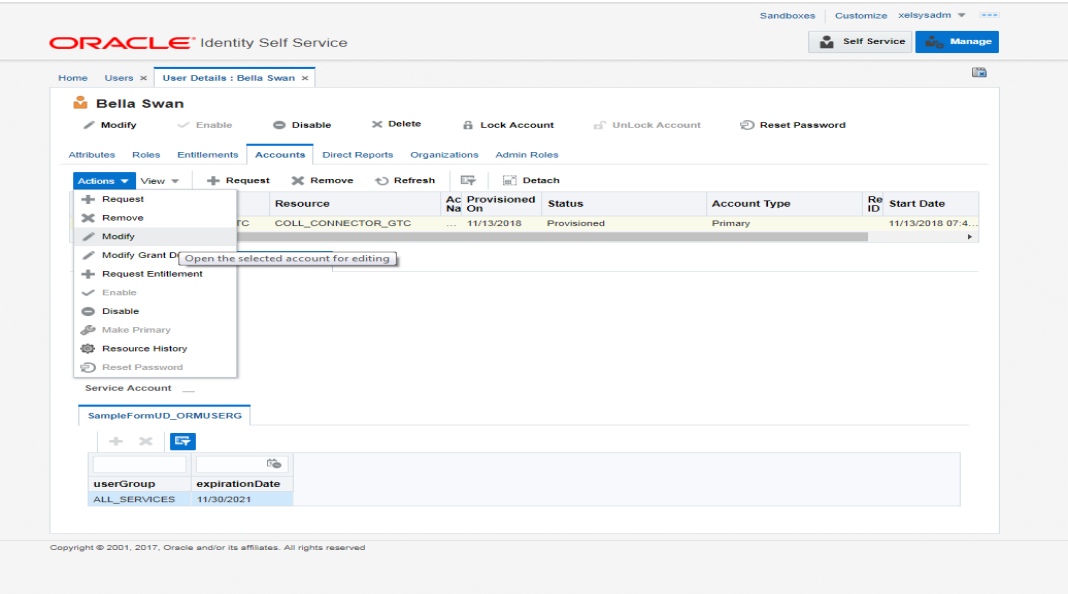
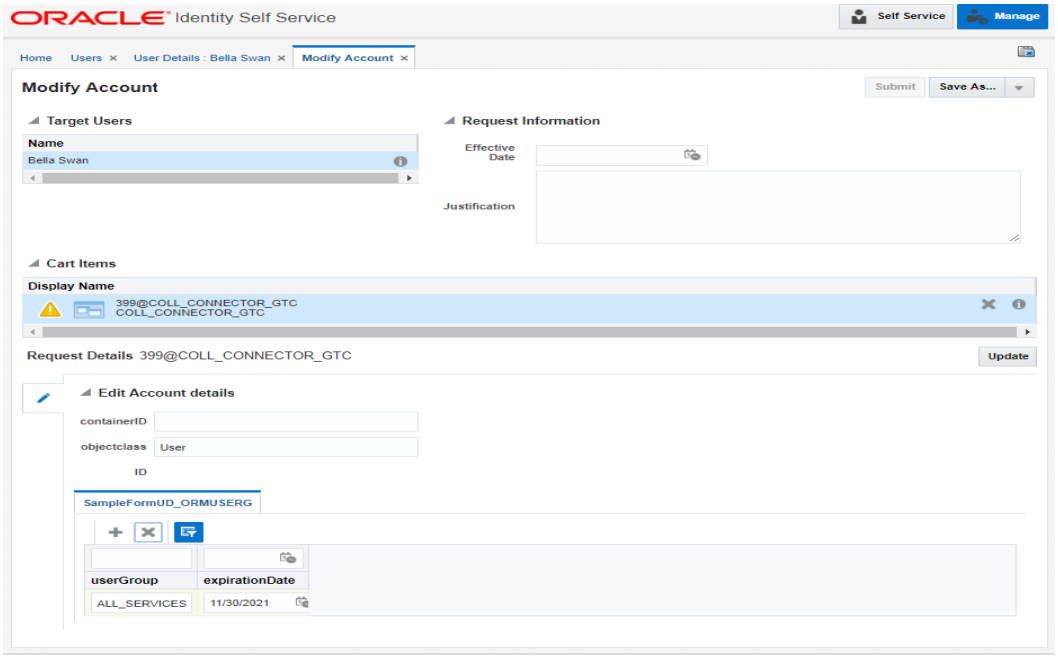


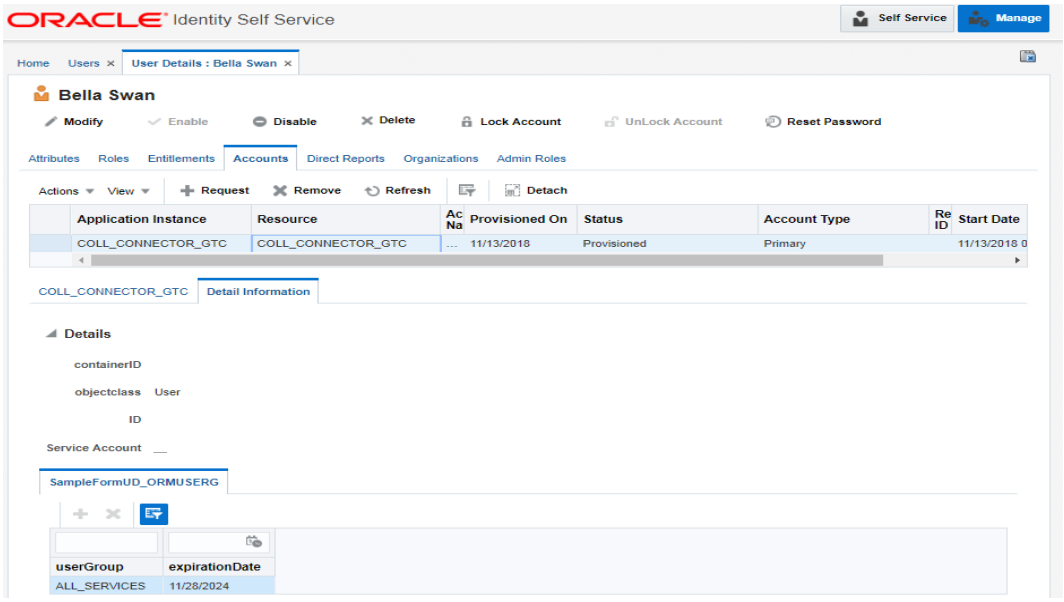
Figure 4–12 Edit Detail Information



    c. Click Update and then Submit.

d. To view the changes, go to the **Accounts** tab in **User Details** page and click **Refresh**. Select the account again to view the modified group in **Detail Information** section.

Figure 4–13 Viewing Changes



5.4 Delete Users

Once user is successfully provisioned, it can be deleted. Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery supports soft delete, that is, it only expires User. User deletion request for Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery will only trigger when **Create User provisioning** task is complete for that particular request, that is, it doesn't appear in open task list.

- If User provisioning request has failed then rectify the problem and complete **Create User provisioning** request, if required.
- If User is already provisioned then, mark **Create User provisioning** task as manually complete.

You can search and delete user. You can search for the user from **Search** panel and then click the searched user data to view its detail.

Figure 4–14 Searching Users To Delete

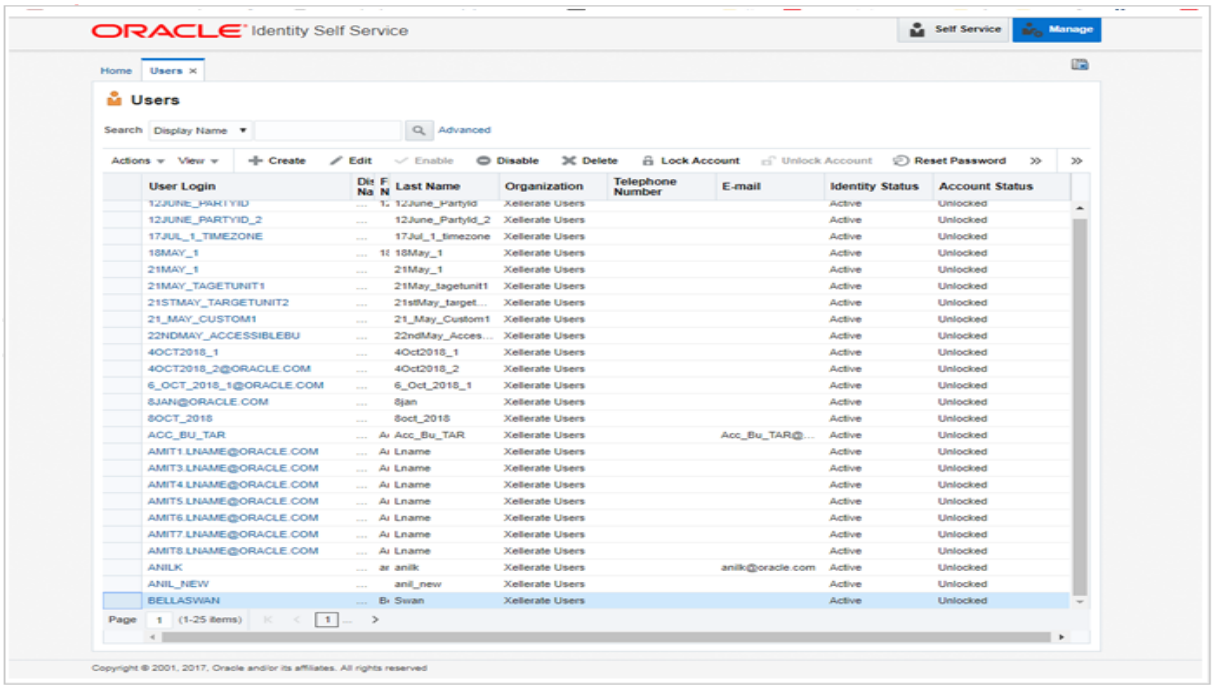
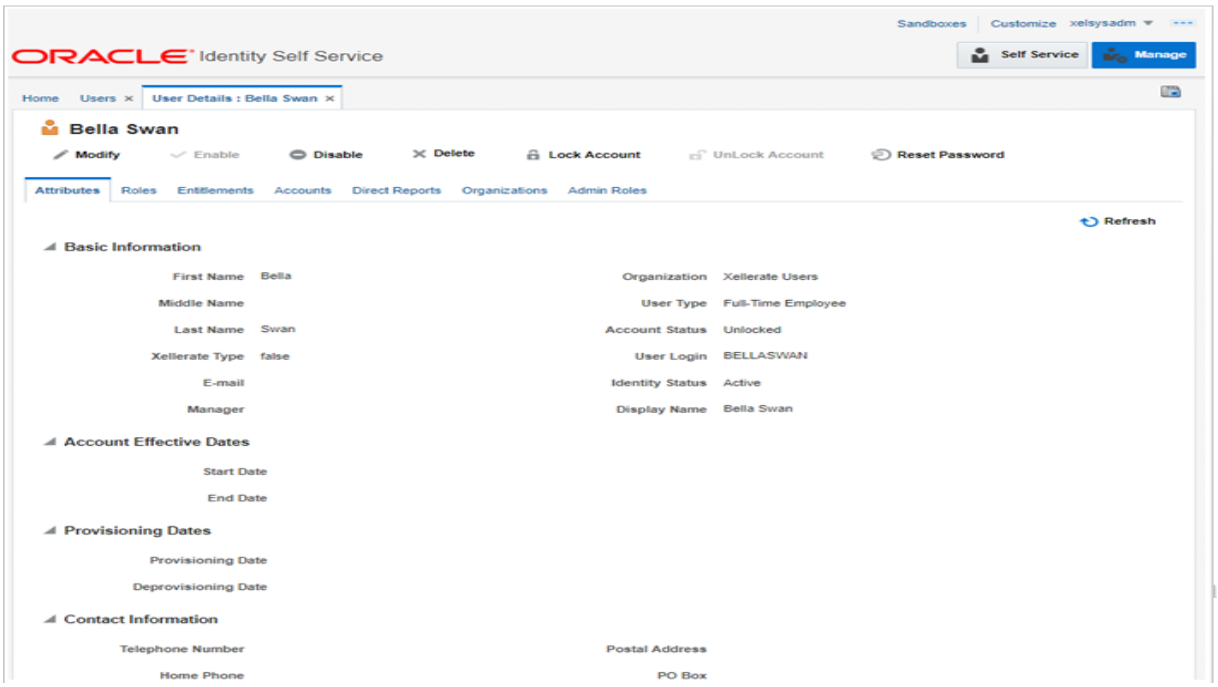


Figure 4–15 View User Details



1. Click Delete Icon to delete user.
   User authentication happens on data stored in OID. If user details are not available in OID then the user will no more be an authenticated user.

6 Create, Modify, Delete Users using DB Based Configurations

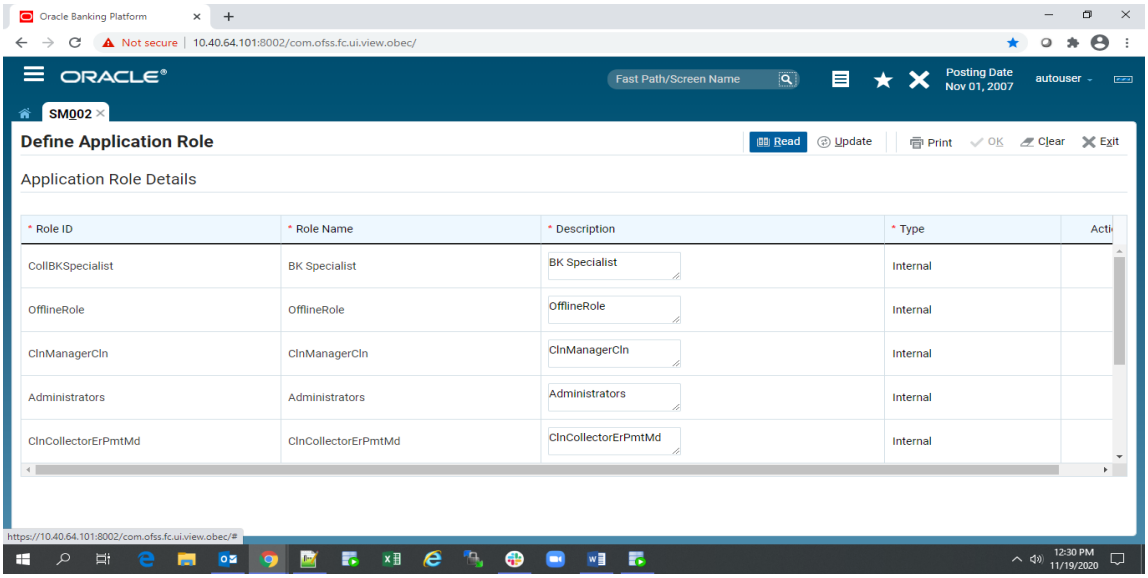
This chapter explains the process of creating and provisioning users using DB based configurations.

6.1 Create and Provision Users

To create users:

1. Create the application role from the Define Application Role (Fast Path: SM002) page.

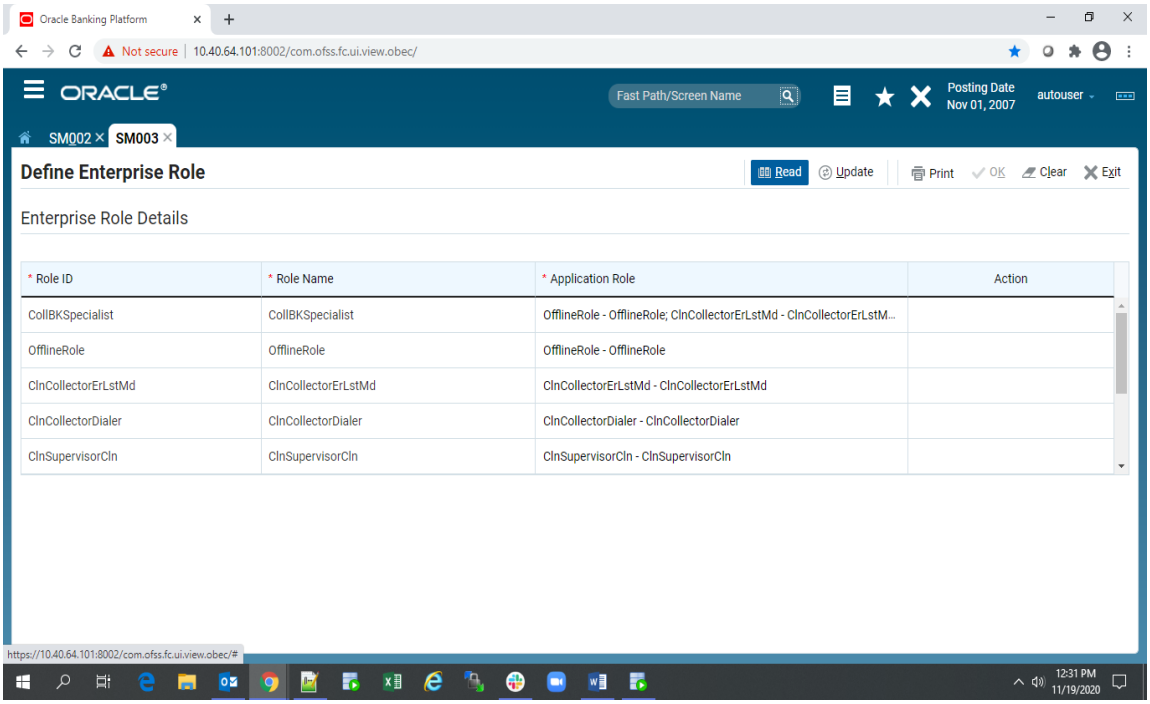
Figure 4–16 Define Application Role (Fast Path: SM002)



Entries move in the FLX_SM_LOCAL_APP_ROLES table.

2. Create the enterprise role and link application role to it from the Define Enterprise Role (Fast Path: SM003) page.

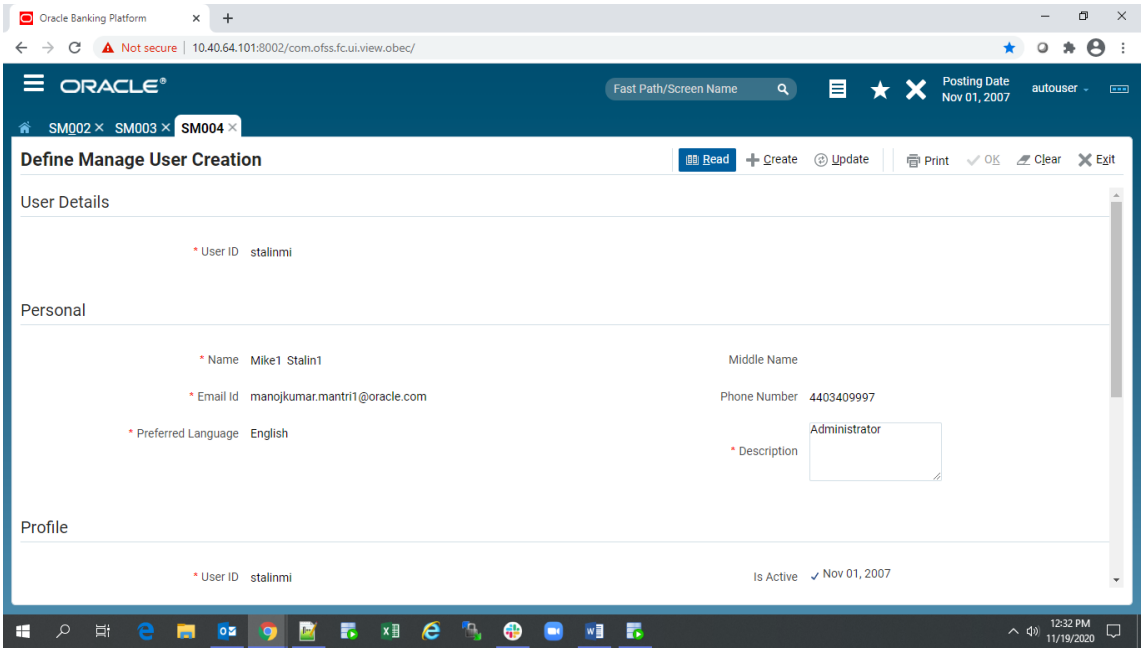
Figure 4–17 Define Enterprise Role (Fast Path: SM003)



Entries moves in the FLX_SM_LOCAL_ENT_ROLE and FLX_SM_LOCAL_ENT_APP_LNK tables.

3. Create user and link enterprise role to user from the Manage User Creation (Fast Path: SM004) page.

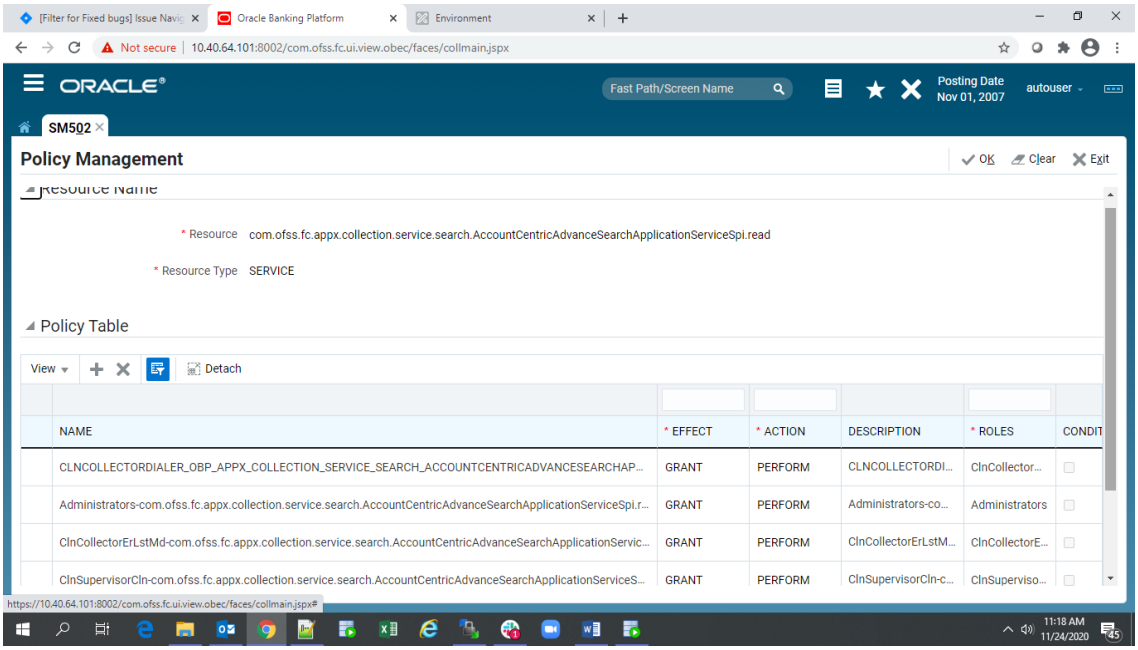
Figure 4–18 Manage User Creation (Fast Path: SM004)



Entries move in the FLX_SM_LOCAL_USERS and FLX_SM_LOCAL_USR_ENT_ROLES tables.

4. Policy for the services with respect to each role can be applied using the Policy Management (Fast Path: SM502) page. This helps in deriving which activities can be performed by which role. User can add or delete the role and grant access for the service.

Figure 4–19 Policy Management (Fast Path: SM502)



Note that seed will be applied of policy entries for product shipped roles.

Tables include FLX_SM_LOCAL_RESOURCES, FLX_SM_LOCAL_POLICY_ENTRY and FLX_SM_LOCAL_RES_POENT_LNK.

User Provisioning

User provisioning is achieved in two ways:

- **User Creation:** While administrator creates a user ID from Manage User Creation (Fast Path: SM004) page, system verifies the role linked to user created and compares in table flx_fw_config_all_b where prop_id='collection.roles'.
  - If role present in the table, an entry is created in Collections Admin (SC_USER and its respective tables) with pre-configured values as per feature configuration C1-USRPROV .
  - If role of new user created not present in flx_fw_config_all_b table, then no entry created for Oracle Banking Enterprise Collections as part of user provisioning.
- **User Access to Collections Service or Page:**
  - If Oracle Banking Enterprise Collections UI or service is called by user, that user is provisioned in Oracle Banking Enterprise Collections.
  - An entry is created in Collections Admin (SC_USER and its respective tables) with pre-configured values as per feature configuration C1-USRPROV.

Note

- The entry in FLX_FW_CONFIG_ALL_B with prop_ id=collection.roles is also used for showing the Collector Dashboard (Fast Path: COLL100) as the home page.
- If factory_shipped_flag is Y, then the dashboard of users linked to roles in prop_value will have COLL100 as default home page.
- But for user provisioning the factory_shipped_flag = Y or N check is not done, system picks the role mentioned in prop_ value by default.

7 Verification

This chapter details the verification of the configurations performed for OIM.

7.1 Verification of OIM Configuration

To verify OIM configuration, follow the steps:

1. Ensure that OID details are populated properly as per the environment used (under IT Resource details for Directory Server). Verify whether the server URL is in the following format:

   ldap ://< OID IP> :< OID PORT>.

   If **Connection pooling supported** flag is true, then update the parameter value to false. Current implementation is tested with Connection pooling supported flag to be false.

   Figure 5–1 Viewing IT Resource Details and Parameters


View IT Resource Details and Parameters

You can view additional information about this IT resource : Details and Parameters

IT Resource Name	Directory Server
IT Resource Type	Directory Server

Parameter	Value
Abandoned connection timeout	600
Admin Login	cn=orcladmin
Admin Password	********
Changelog Container	cn=changelog
Connection pooling supported	false
Connection wait timeout	120
Date Format	yyyyMMddHHmmss
Inactive connection timeout	600
Initial pool size	5
Max pool size	10
Min pool size	5
Pool preference	Default
ResourceConnection class definition	oracle.iam.ldapsync.impl.repository.LDAPConnection
Search Base	dc=i-flex,dc=com
Server SSL URL	
Server URL	ldap://10.180.25.56:3060
Target supports only one connection	false
Timeout check interval	60
Use SSL	false
User Reservation Container	cn=Users,dc=i-flex,dc=com
Validate connection on borrow	true

2. While creating User from OIM, an exception *Unable to find attributes in OID schema* may occur for following attributes. If such issue is faced, ensure the following attributes are present in OID Schema and are added to object class **orclIDXPerson** as optional attributes. (Required for OIM functioning).

   Table 5–1 OID schema attributes

Attribute Name	Syntax
Orclpwdexpirationdate	Generalized Time
Orclpwdchangerequired	Boolean
Orclaccountenabled	Boolean
Orclaccountlocked	Integer

> **Note**
>
> The above mentioned attributes are added only for OIM functioning.

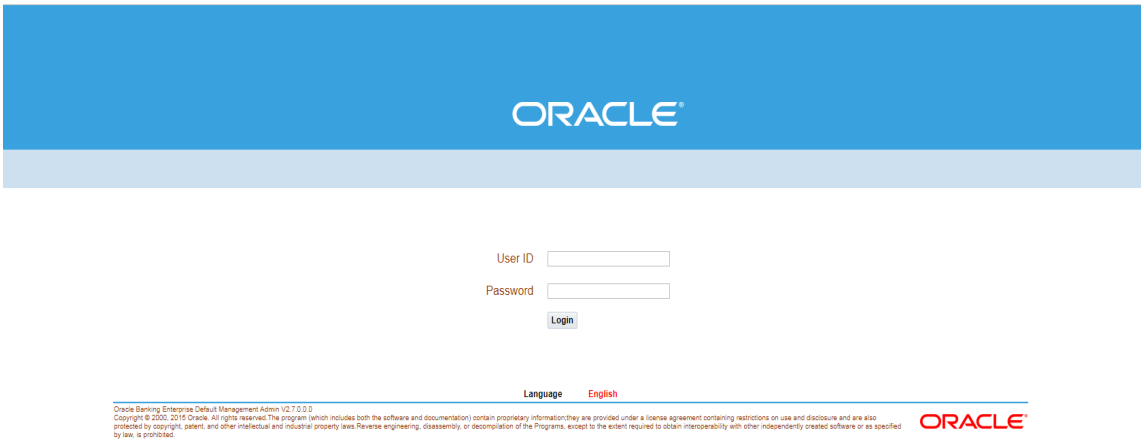
7.2 Verify Users in Native Collections Admin Application

Following steps are required to verify users in native Collections Admin Application after provisioning:

1. Log in to native Collections Admin Application UI using administrative credentials.

   http://<Host>:<Port>/CollectionAdmin/cis.jsp

   Figure 5–2 Login screen



2. Navigate to User screen from **Menu > Admin > U > User**.

   Figure 5–3 User Screen - User Navigation

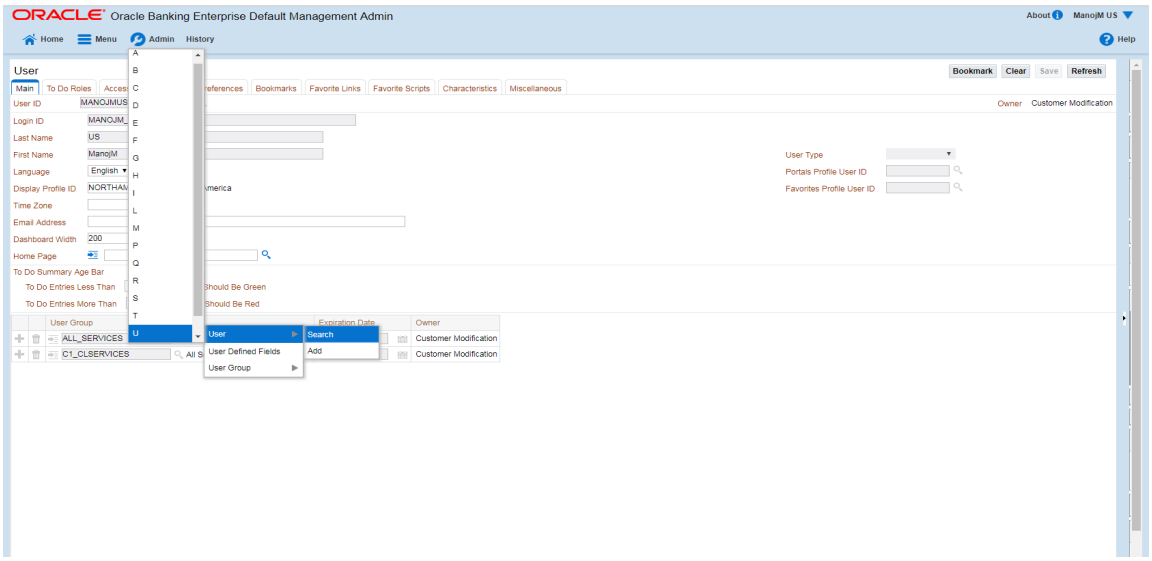
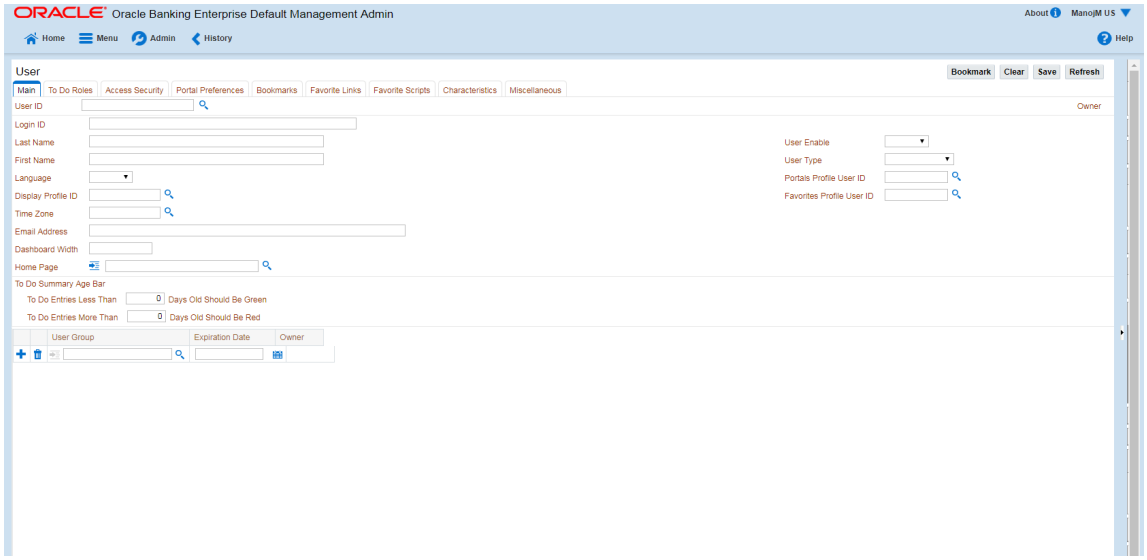


Figure 5–4 User Screen - Main Tab



3. Click **Search** icon. User Search dialog window is displayed. To search for a user, enter **User ID** and click **Search**.

Figure 5–5 Searching Particular User

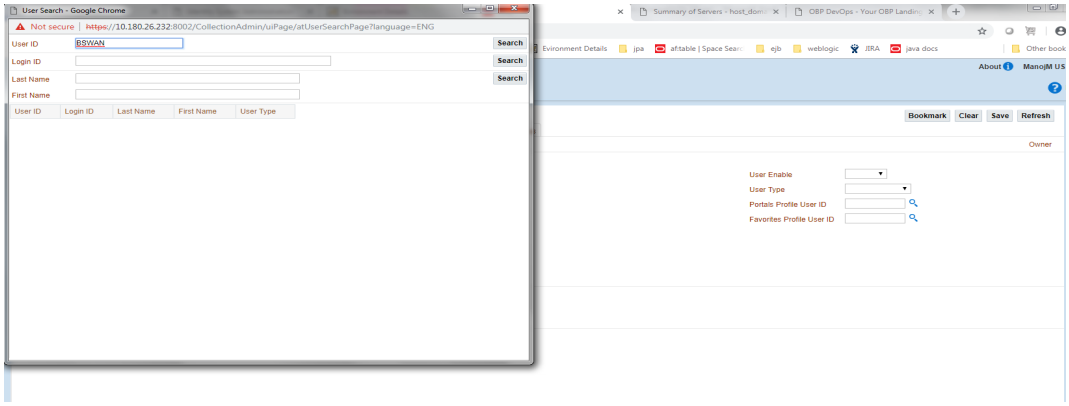
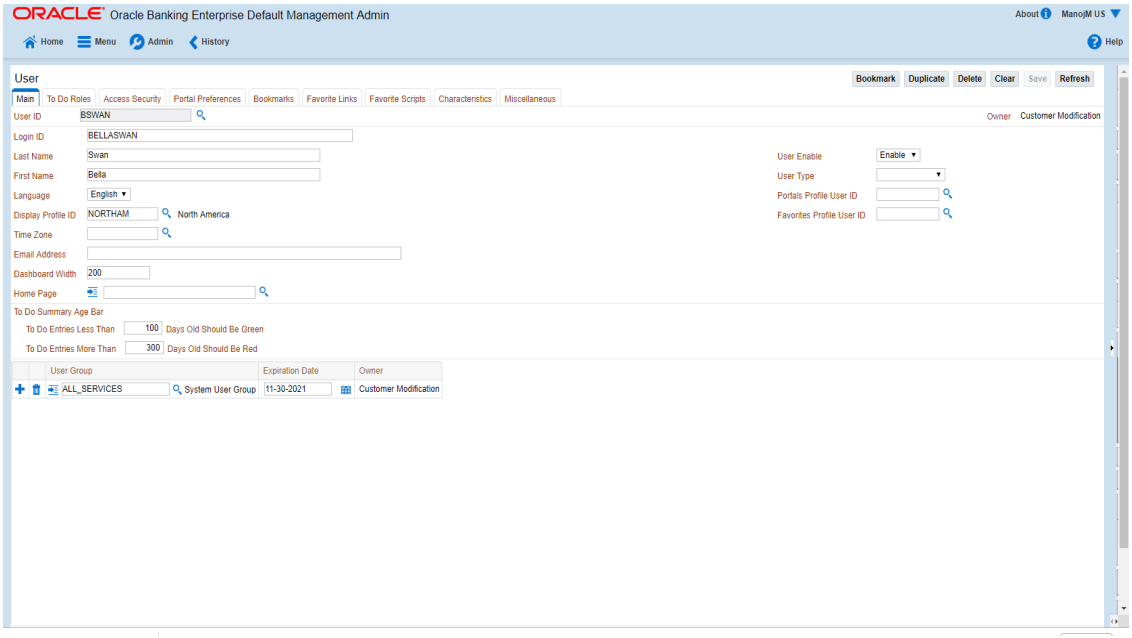


Figure 5–6 Search Result in User screen



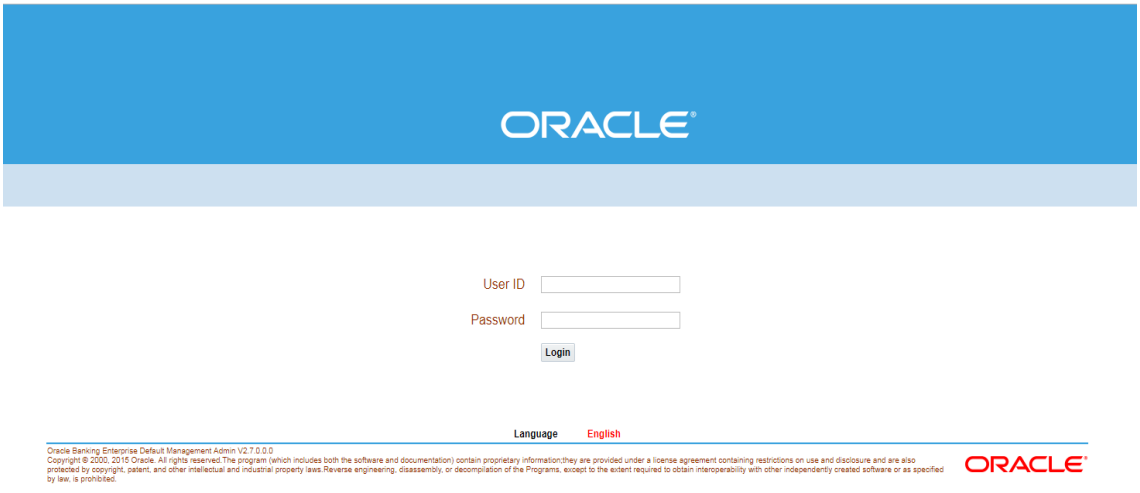
7.3 Create Users in Collections Admin Application

Follow below steps to create user in Collections Admin Application.

1. Log in to native Collections Admin Application UI using administrative credentials.

   http://<Host>:<Port>/CollectionAdmin/cis.jsp

Figure 5–7 Login screen



2. Navigate to User screen from **Menu > Admin > U > User**.

Figure 5–8 User Navigation

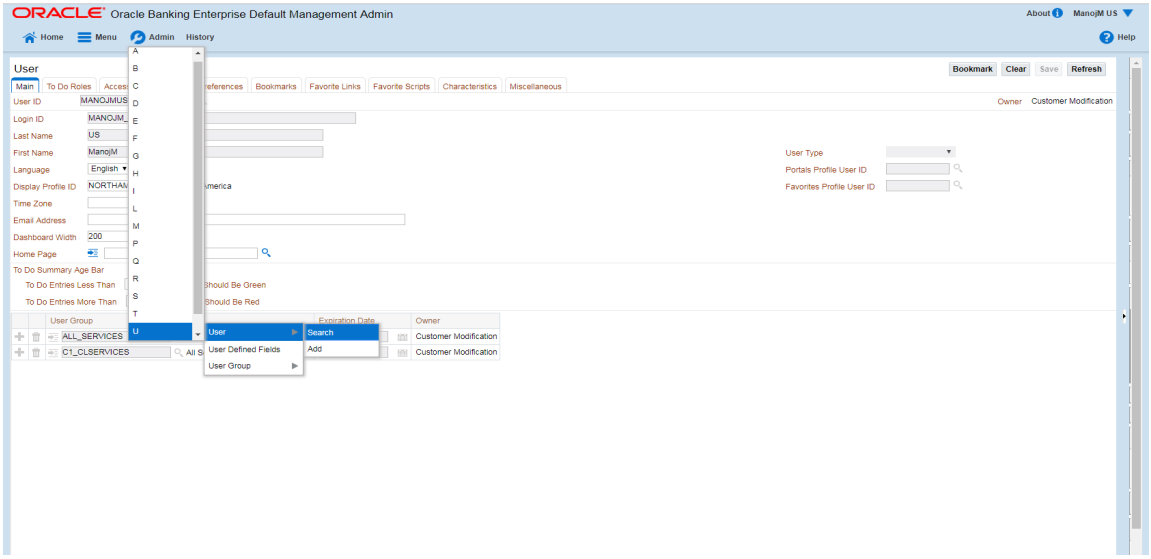
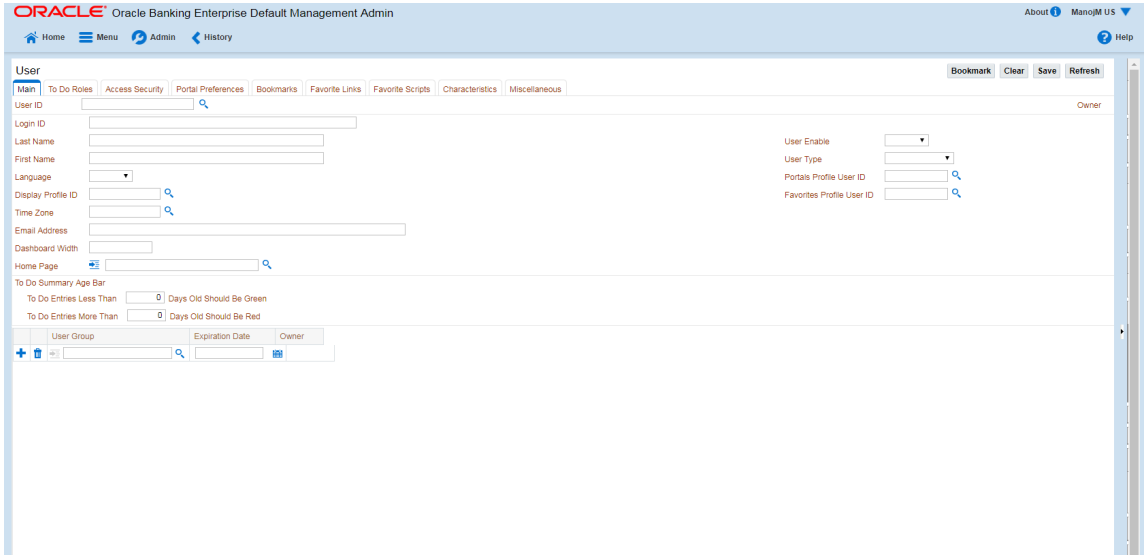


Figure 5–9 User Screen - Main Tab

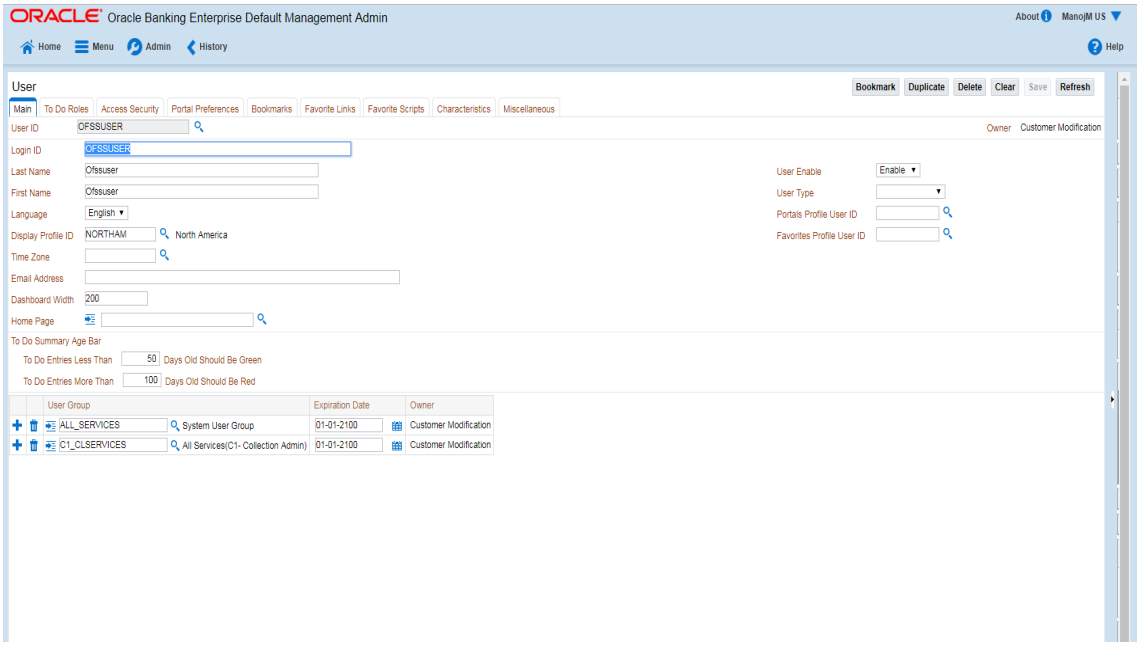


3. In the User page, enter the following details in the respective fields:
   - **User Id:** OIMOBPCO
   - **Login Id:** OIMOBPCOLL
   - **First Name:** OIMOBPCOLL
   - **Last Name:** OIMOBPCOLL
   - **Language:** English

- **Display Profile ID Tender Source:** NORTHAM
- **Email Address:** OIMOBPCOLL@oracle.com (This is a sample email address. Provide valid administrator email address)
- **Dashboard Width:** 200
- **Home Page:** c1_ormbhTabMenu
- **To Do Entries <:** 50
- **To Do Entries >:** 100
- **User Group:** CLNHOSTUSER with Expiration Date: 01-01-2100 (add expiration date as per requirement)
- **User Enable:** Select Enable

4. Click **Save.**

Figure 5–10 User Screen



5. OIMOBPCOLL User is successfully created.