

Oracle® Banking Enterprise Default Management

User Provisioning Guide

Release 2.11.0.0.0

F36758-01

December 2020

Oracle Banking Enterprise Default Management User Provisioning Guide, Release 2.11.0.0.0

F36758-01

Copyright © 2017, 2020, Oracle and/or its affiliates.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface	10
Audience	10
Documentation Accessibility	10
Organization of the Guide	10
Related Documents	11
Conventions	11
1 About this Guide	13
2 Introduction	15
3 Configuration	17
3.1 Prerequisites for OIM Configuration	17
3.2 Create System User	17
3.3 OIM Configuration	18
3.3.1 Import Configuration	18
3.3.2 Manage Generic Technology Connector	21
3.3.3 Create and Activate Sandbox	26
3.3.3.1 Create Sandbox	27
3.3.3.2 Activate Sandbox	29
3.3.3.3 Deactivate Sandbox	29
3.3.3.4 Publish Sandbox	30
3.3.4 Create Form Associated with Application Instance	31
3.3.5 Create Access Policy and Role	38
3.3.5.1 Create Access Policy	38
3.3.5.2 Creating Roles	43
3.4 DB Based Configuration	49

3.4.1 DB Based Policy Configuration	49
3.4.2 Role Based Local Menu Configuration	54
3.4.3 Database Identity Store Provider (Both Middleware and UI server)	55
4 User Fields and Constraints	71
4.1 User Fields Provisioned From OIM	71
5 Create, Modify, Delete Users using OIM	73
5.1 Create and Provision Users	73
5.2 Feature Configurations	76
5.3 Modify Users	77
5.4 Delete Users	81
6 Create, Modify, Delete Users using DB Based Configurations	83
6.1 Create and Provision Users	83
7 Verification	87
7.1 Verification of OIM Configuration	87
7.2 Verify Users in Native Collections Admin Application	88
7.3 Create Users in Collections Admin Application	90

List of Tables

Table 3–1 Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Provisioning Artifacts	18
Table 3–2 Run Time Connector Parameters	23
Table 3–3 Create Sandbox Parameters	28
Table 4–1 User Fields	71
Table 5–1 OID schema attributes	87

List of Figures

Figure 3–1 Oracle Identity System Administration - Import Configuration Screen	19
Figure 3–2 Browse the file to be imported	19
Figure 3–3 Import Options	20
Figure 3–4 Summary of the import	20
Figure 3–5 Successful Import Message	21
Figure 3–6 Generic Connector	21
Figure 3–7 Search Connectors	22
Figure 3–8 Edit Connector Parameters	22
Figure 3–9 Specify parameter values	23
Figure 3–10 Modify Connector Configuration (Mapping Information)	24
Figure 3–11 Edit Mapping Information	24
Figure 3–12 Provide Mapping Information	25
Figure 3–13 Verify Connector Information	25
Figure 3–14 Successful Configuration Message	26
Figure 3–15 Oracle Identity System Administration - Sandbox tab	27
Figure 3–16 Create Sandbox Dialog Box and Parameters	27
Figure 3–17 Sandbox Creation Confirmation	28
Figure 3–18 Available Sandbox	29
Figure 3–19 Activated Sandbox	29
Figure 3–20 Deactivate Sandbox	30
Figure 3–21 Publish Sandbox	30
Figure 3–22 Published Sandbox	30
Figure 3–23 Create Form - Form Designer	31
Figure 3–24 Create Form - Resource Type	31

Figure 3–25 Create Form - Resource Type (COLL_CONNECTOR_GTC)	32
Figure 3–26 Create Form Resource Type - Available Form Fields	32
Figure 3–27 Search Form	33
Figure 3–28 Manage Collections User Form	33
Figure 3–29 Manage Form	34
Figure 3–30 Manage Child Objects form fields	34
Figure 3–31 Set default values for field- userGroup	35
Figure 3–32 Set default value for field- expirationDate	35
Figure 3–33 Search Application Instances and select COLL_CONNECTOR_GTC	36
Figure 3–34 Application Instance Attributes	37
Figure 3–35 Associate Form with Application instance	37
Figure 3–36 Success message	38
Figure 3–37 Identity Self Service – Manage tab	39
Figure 3–38 Access Policies	39
Figure 3–39 Create Access Policy	40
Figure 3–40 Access Policy details	40
Figure 3–41 Add application instance associated with access policy	41
Figure 3–42 Search Access Policy	41
Figure 3–43 Provisioned applications for the policy	42
Figure 3–44 Application Attributes	43
Figure 3–45 Oracle Identity Self Service- Roles Tab	44
Figure 3–46 Create Role	45
Figure 3–47 Create Role	46
Figure 3–48 Add Access Policy to the role	46
Figure 3–49 Add Access Policy to the role	47
Figure 3–50 Create Membership Rule	47

Figure 3–51 Build Membership Rule Expression	48
Figure 3–52 Build Membership Rule Expression	49
Figure 3–53 FLX_SM_LOCAL_USERS	50
Figure 3–54 FLX_SM_LOCAL_ENT_ROLE	50
Figure 3–55 FLX_SM_LOCAL_APP_ROLES	51
Figure 3–56 FLX_SM_LOCAL_ENT_APP_LNK	51
Figure 3–57 FLX_SM_LOCAL_USR_ENT_ROLES	52
Figure 3–58 FLX_SM_LOCAL_RESOURCES	52
Figure 3–59 FLX_SM_LOCAL_POLICY_ENTRY	53
Figure 3–60 FLX_SM_LOCAL_RES_POENT_LNK	53
Figure 3–61 Configuration for DB Menu	54
Figure 3–62 Configuration for Role Based Menu	55
Figure 3–63 Create Authentication Provider	56
Figure 3–64 Provider Specific Settings	56
Figure 3–65 Common Settings	58
Figure 3–66 Service Provider Configuration	61
Figure 3–67 Identifying Store Provider for Configuration	62
Figure 3–68 Adding Custom Property Virtualize with value True	62
Figure 3–69 Users and Groups	67
Figure 3–70 Selecting from Users	68
Figure 3–71 Selecting from Roles	68
Figure 3–72 Selecting from Groupmembers	69
Figure 4–1 Create User - Mandatory and Optional Attributes	72
Figure 4–2 Create User in Oracle Identity Self Service	73
Figure 4–3 Input User Attributes	74
Figure 4–4 Search and select the added User	75

Figure 4–5 Applications provisioned to User	76
Figure 4–6 Feature Configuration	77
Figure 4–7 Searching User	77
Figure 4–8 Detailed Information about the User	78
Figure 4–9 Modify User Confirmation	79
Figure 4–10 Viewing Modified and Provisioned User Details	79
Figure 4–11 Modify Detail Information	80
Figure 4–12 Edit Detail Information	80
Figure 4–13 Viewing Changes	81
Figure 4–14 Searching Users To Delete	82
Figure 4–15 View User Details	82
Figure 4–16 Define Application Role (Fast Path: SM002)	83
Figure 4–17 Define Enterprise Role (Fast Path: SM003)	84
Figure 4–18 Manage User Creation (Fast Path: SM004)	84
Figure 4–19 Policy Management (Fast Path: SM502)	85
Figure 5–1 Viewing IT Resource Details and Parameters	87
Figure 5–2 Login screen	88
Figure 5–3 User Screen - User Navigation	88
Figure 5–4 User Screen - Main Tab	89
Figure 5–5 Searching Particular User	89
Figure 5–6 Search Result in User screen	90
Figure 5–7 Login screen	90
Figure 5–8 User Navigation	91
Figure 5–9 User Screen - Main Tab	91
Figure 5–10 User Screen	92

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
- Documentation Accessibility
- Organization of the Guide
- Related Documents
- Conventions

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.
<i>italic</i>	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.

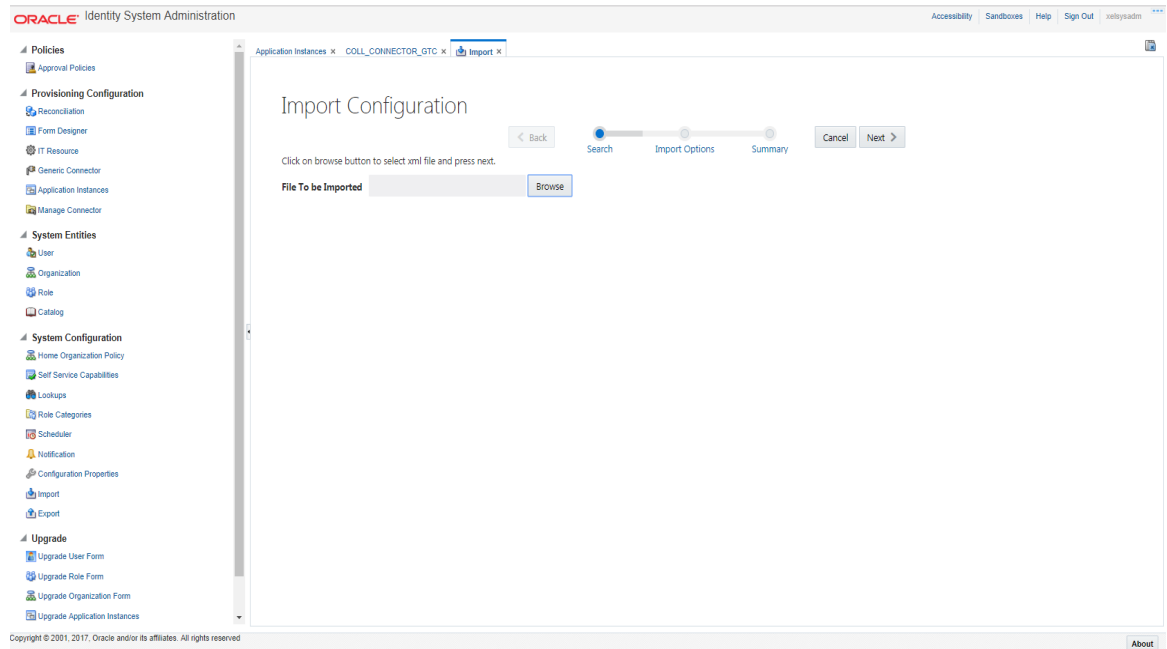
Table 3–1 Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery User Provisioning Artifacts

Artifact	Artifact Type	Description
COLL_CONNECTOR_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

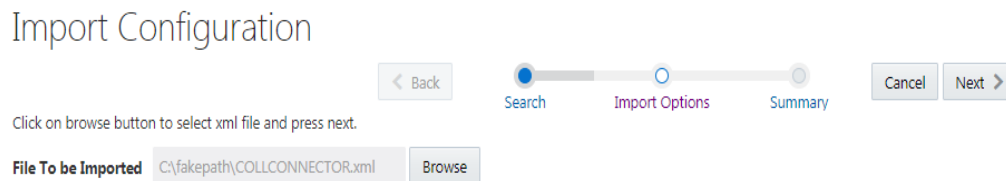
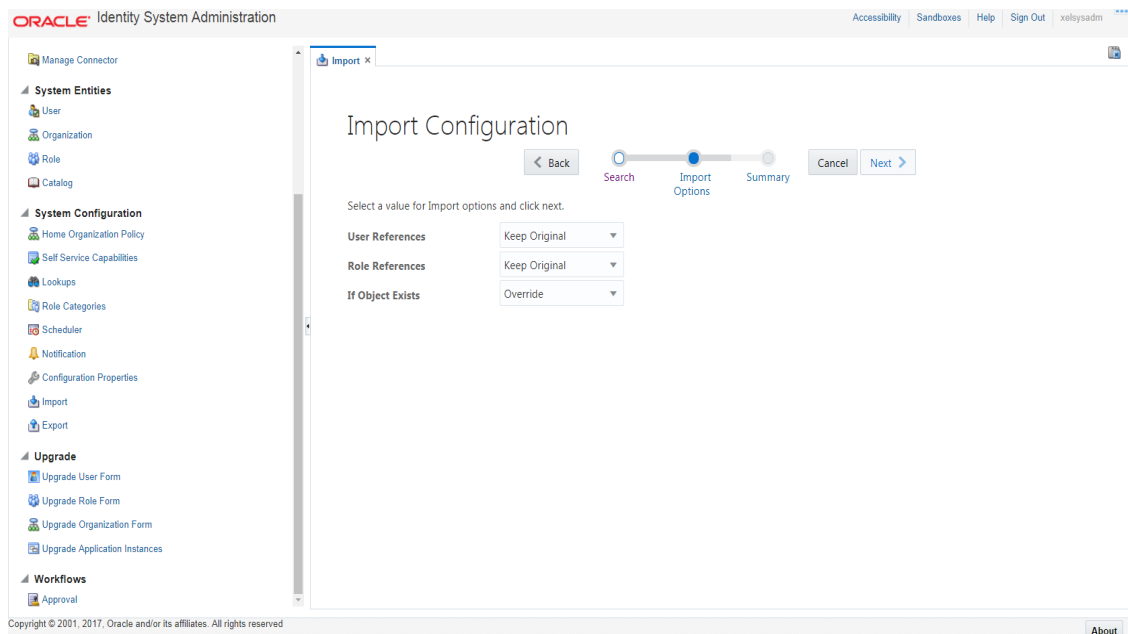
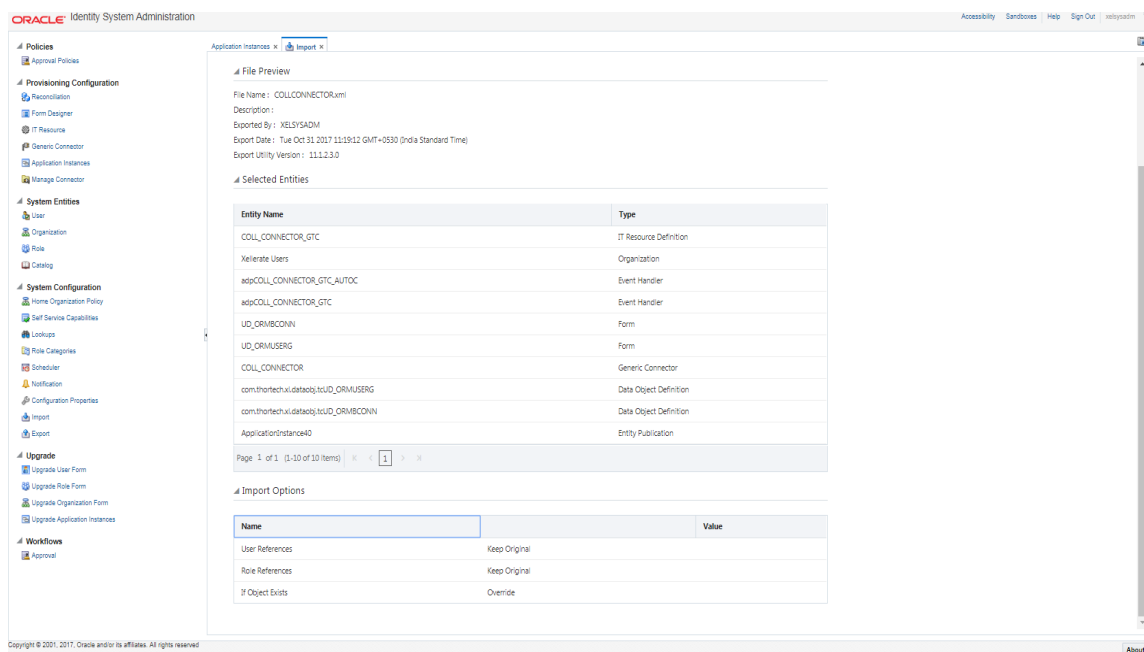


Figure 3–3 Import Options



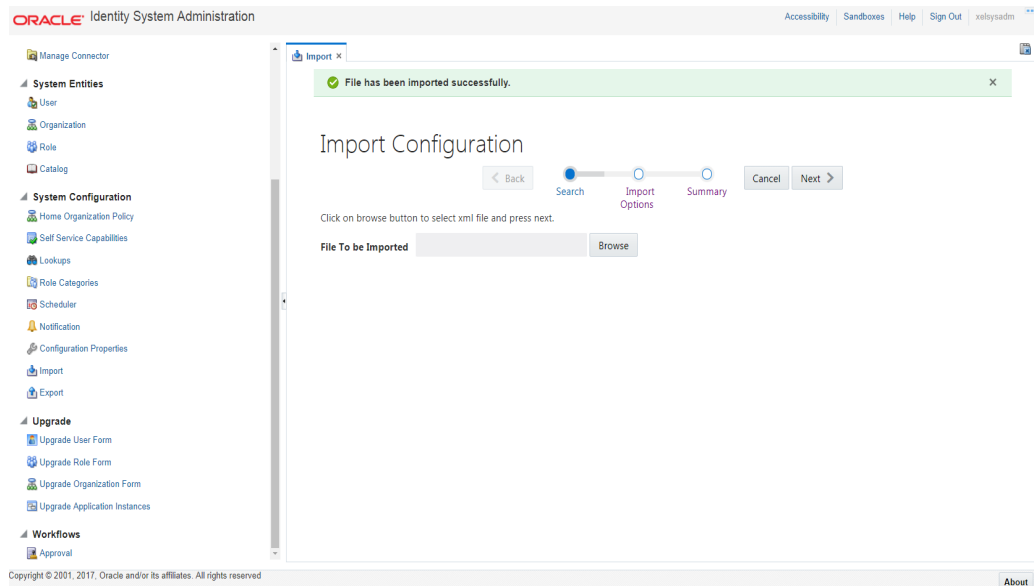
4. Click **Next**.

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

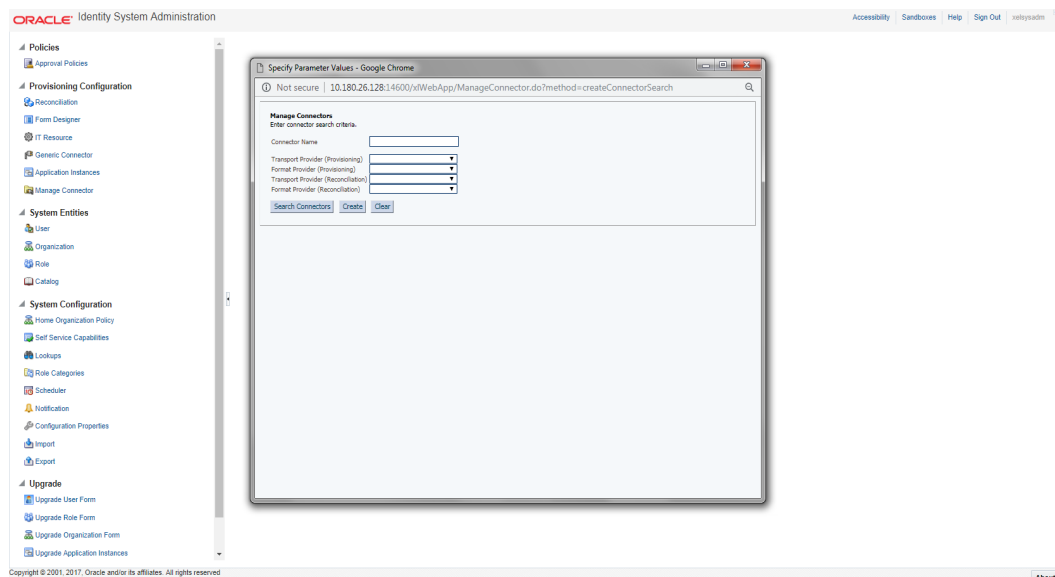


3.3.2 Manage Generic Technology Connector

Following Run-Time Parameters need to be set.

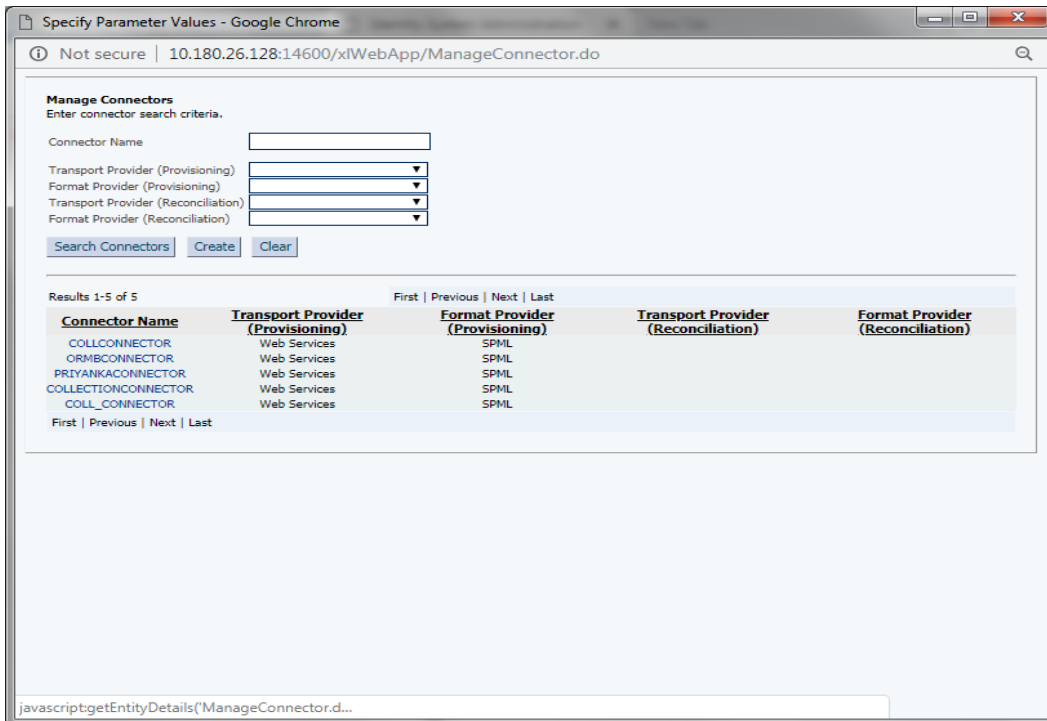
1. In the left pane, click **Generic Connector**. Following window appears.

Figure 3–6 Generic Connector



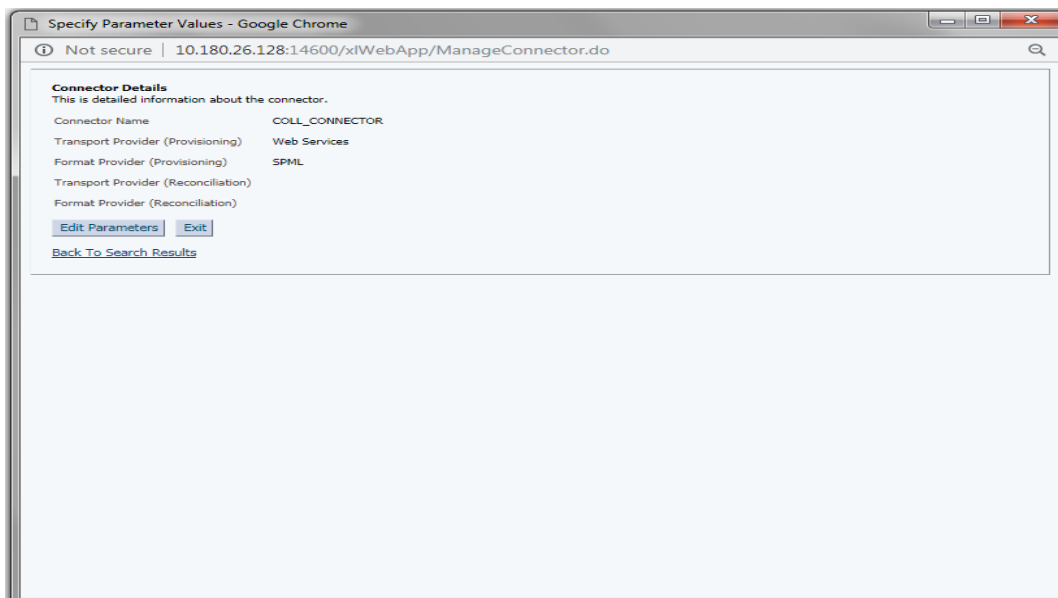
2. Click **Search Connectors** and click **COLL_CONNECTOR**.

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	OOUAF	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

Specify Parameter Values - Google Chrome
 Not secure | 10.180.26.128:14600/xWebApp/ManageConnector.do

Manage Generic Technology Connector

Step 2: Specify Parameter Values

* Indicates Required Field

Run-Time Parameters

Web Services

Web Service URL This is the URL for the Web service receptor.

SPML

Target ID ID of the target system for provisioning operations.

User Name (authentication) User name required for authentication by the Web service.

User Password (authentication) Password required for authentication by the target Web service.

Design Parameters

Web Services

Web Service SOAP Action In the WSDL file, this is the "soapAction" attribute value for the "operation" element.

SPML

WSSSE Configured for SPML Web Service? Specify whether or not the target SPML Web Service is configured to receive WS-Security credentials.

Custom Authentication Credentials Namespace Namespace that defines custom authentication credentials. Specify a value only if the Web service is not configured for WSSSE.

Custom Authentication Header Element Name of the header element for the custom authentication section that is to be included in the SOAP header. Specify a value only if the Web service is not configured for WSSSE.

Custom Element to Store User Name Name of the element in the custom authentication section that will store the user name required for authentication by the Web service. Specify a value only if the Web service is not configured for WSSSE.

Custom Element to Store Password Name of the element in the custom authentication section that will store the password required for authentication by the Web service. Specify a value only if the Web service is not configured for WSSSE.

SPML Web Service Binding Style (DOCUMENT or RPC) In the WSDL file, this is the style attribute value for the binding element.

SPML Web Service Complex Data Type In the WSDL file, this is the value of the "name" attribute of the "complexType" element. This parameter is applicable only if the binding style is "DOCUMENT".

SPML Web Service Operation Name In the WSDL file, this is the "name" attribute value for the "operation" element. This parameter is applicable only if the binding style is "RPC".

SPML Web Service Target Namespace In the WSDL file, this is the "targetNamespace" attribute value for the "definition" element.

SPML Web Service Soap Message Body Prefix Name of the custom prefix element that contains the soap message body. If the target Web service is running on BBA WebLogic, IBM WebSphere, JBoss Application Server, or OC4J, then you need not specify a value for this parameter.

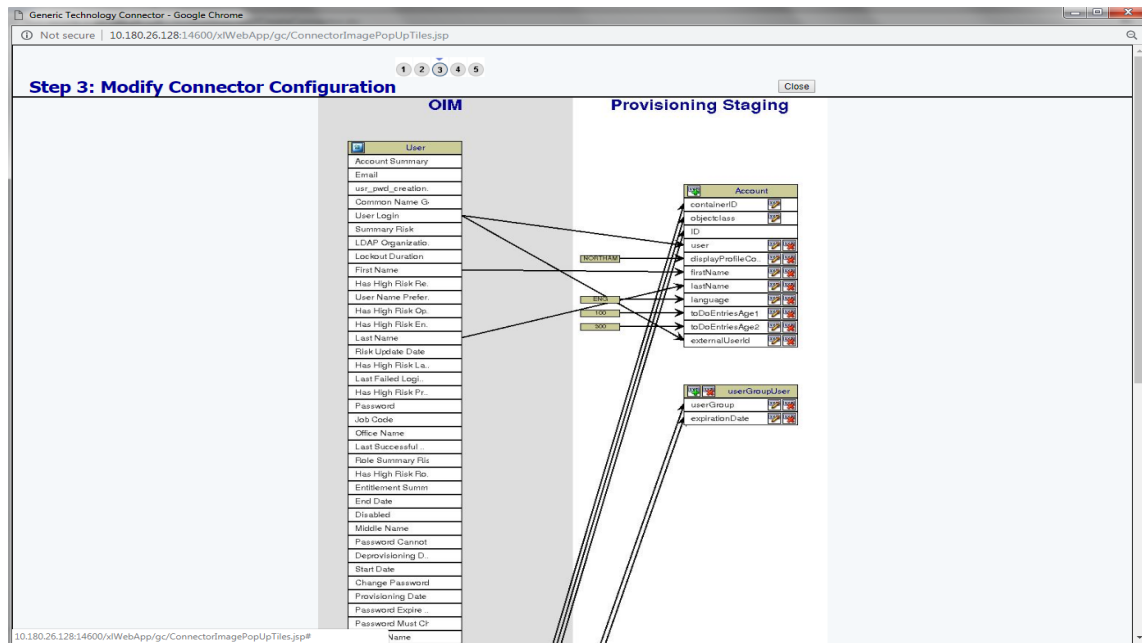
ID Attribute for Child Dataset Holding Role Membership Information Name of the ID attribute for a Provisioning Staging child dataset holding role membership information.

Target Date Format Date Format supported by the Date attributes of Provisioning Staging Dataset. Default value is 'yyyy-MM-dd hh:mm:ss.#####'.

Exit Continue >>

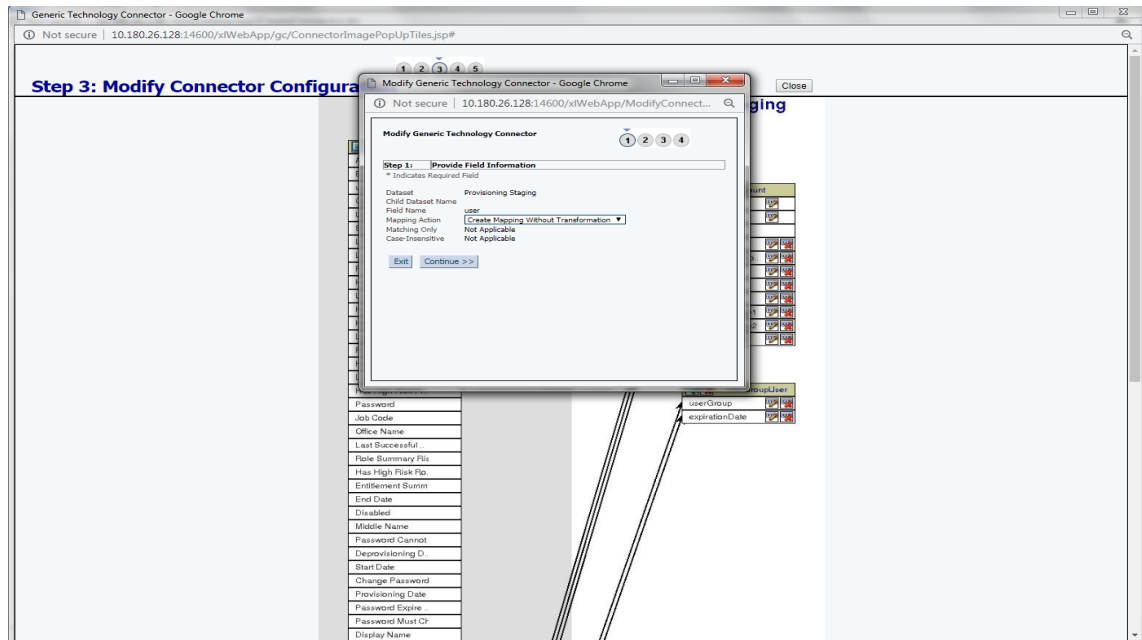
- Click **Continue**. Modify Connector configuration screen appears.

Figure 3–10 Modify Connector Configuration (Mapping Information)



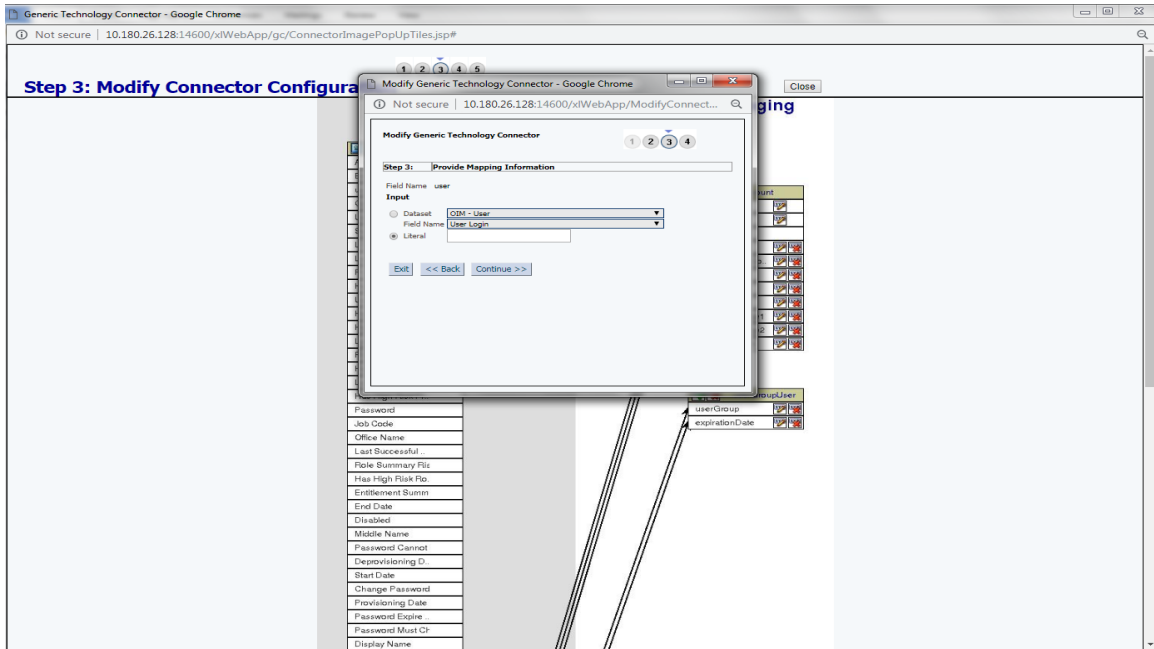
- Click the **Edit** icon for User field name in the provisioning staging column.

Figure 3–11 Edit Mapping Information



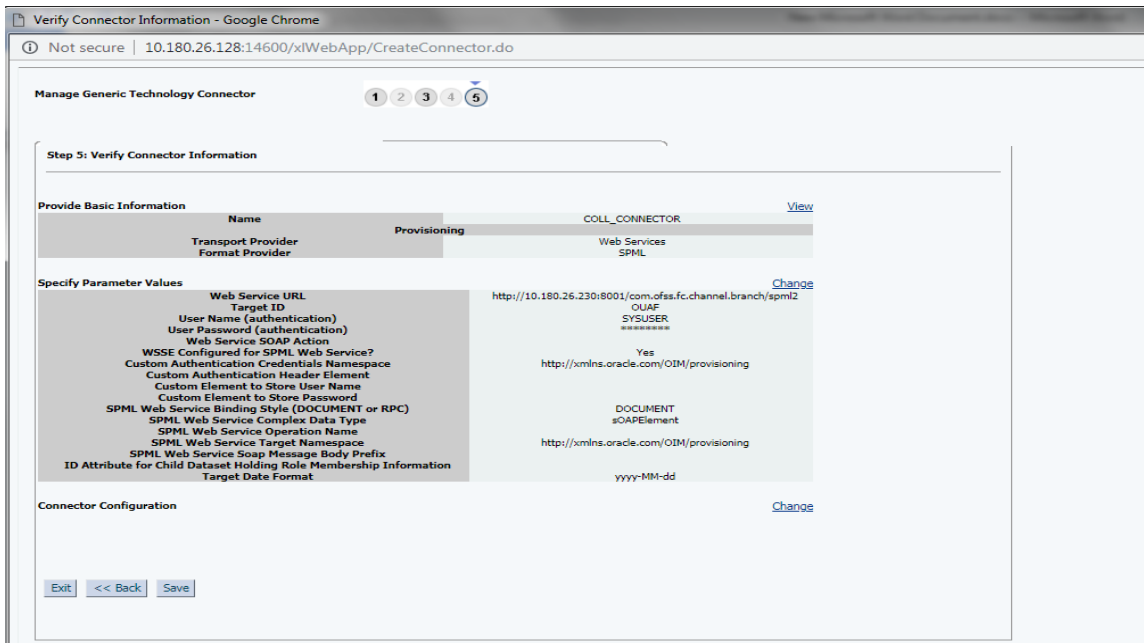
- Click **Continue** to provide mapping information for the User field name. Select the **Literal** radio button and keep the input blank.

Figure 3–12 Provide Mapping Information



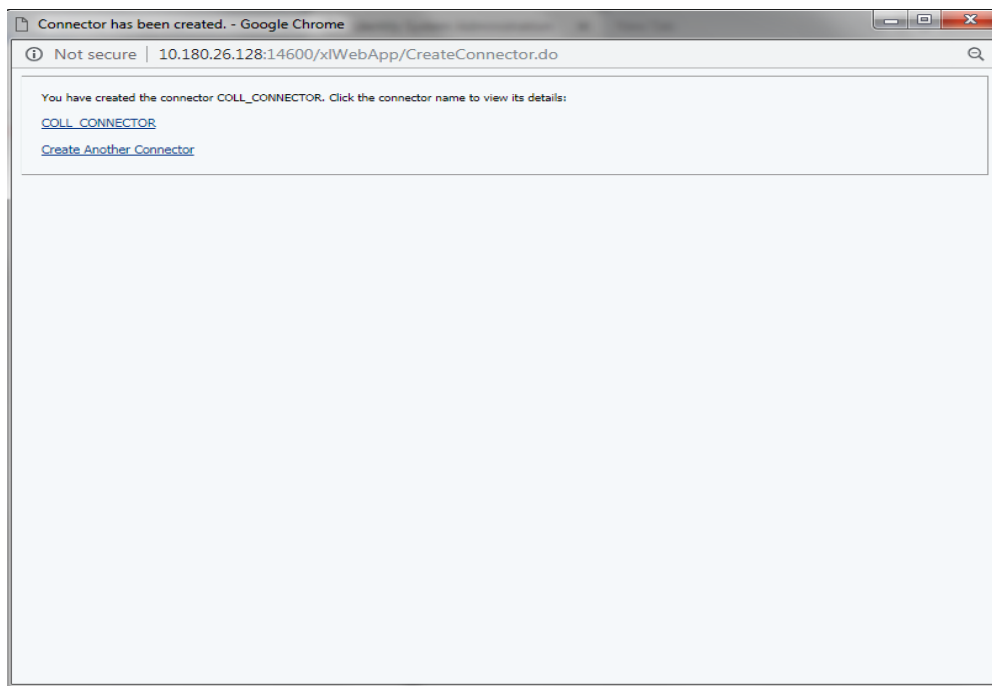
- Click **Continue** and then **Close**. Following window appears where Connector Information can be verified.

Figure 3–13 Verify Connector Information



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

Figure 3–14 Successful Configuration Message

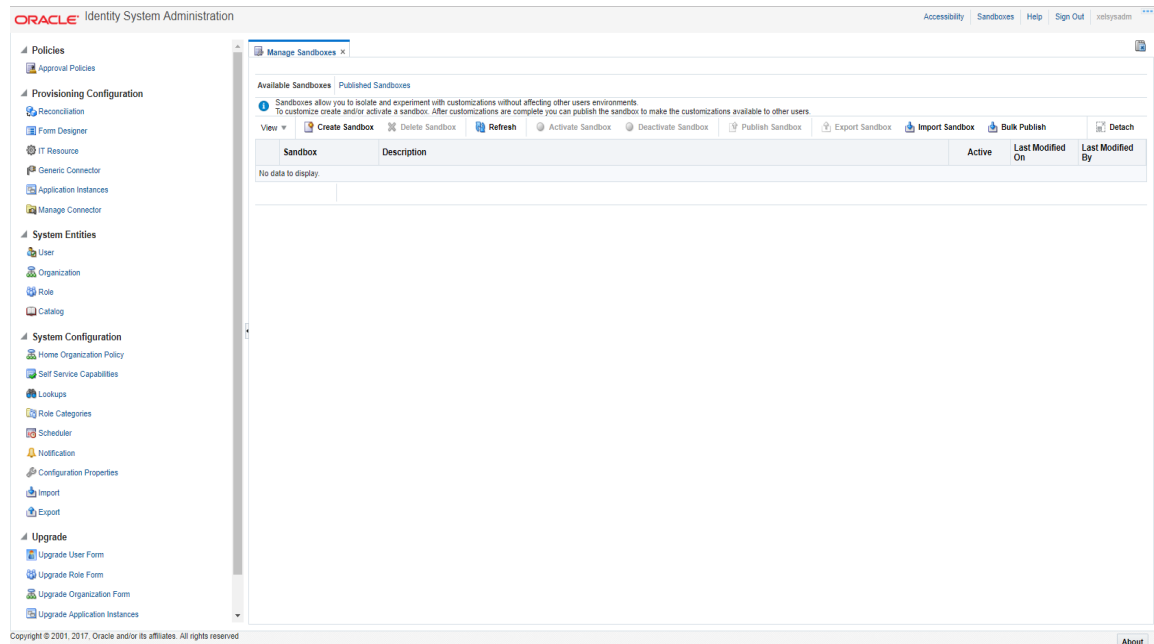


3.3.3 Create and Activate Sandbox

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

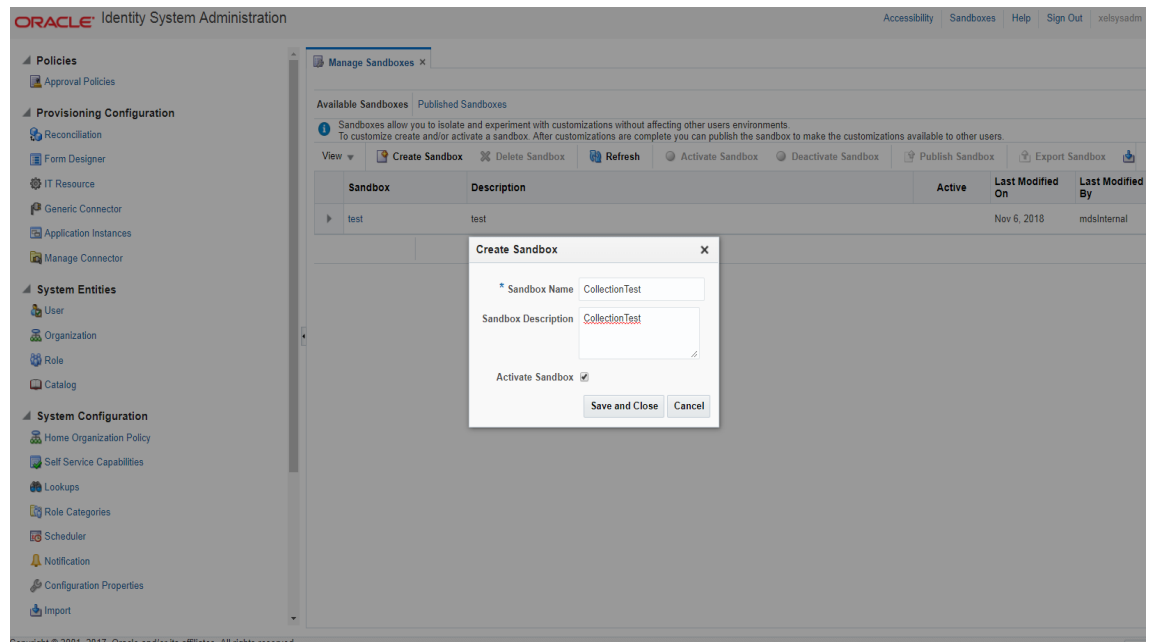


3.3.3.1 Create Sandbox

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



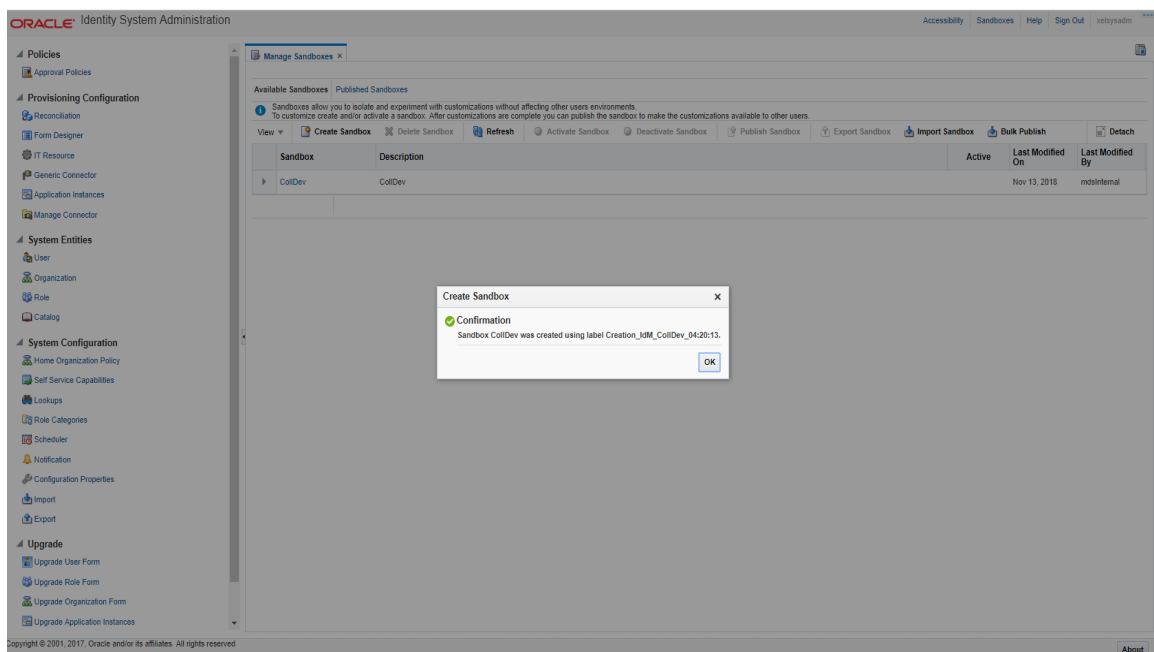
- Specify the following values:

Table 3–3 Create Sandbox Parameters

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

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

Figure 3–17 Sandbox Creation Confirmation

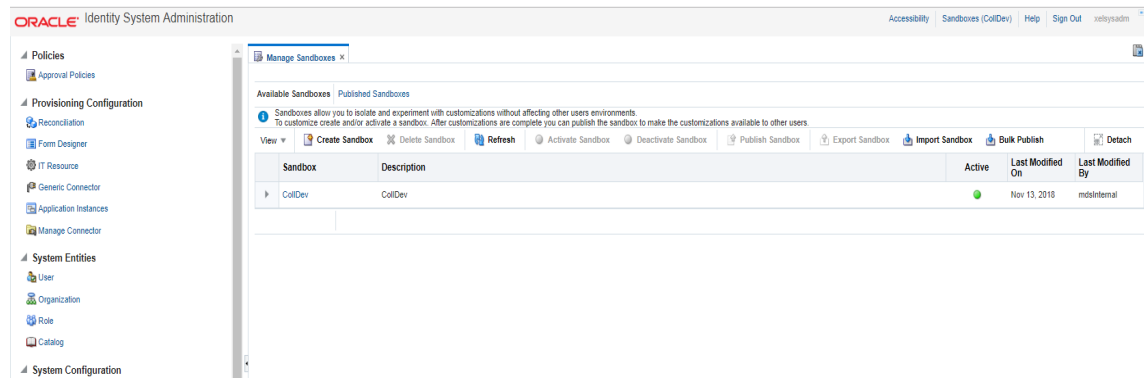


- CollectionsDev sandbox is created and it is activated.

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

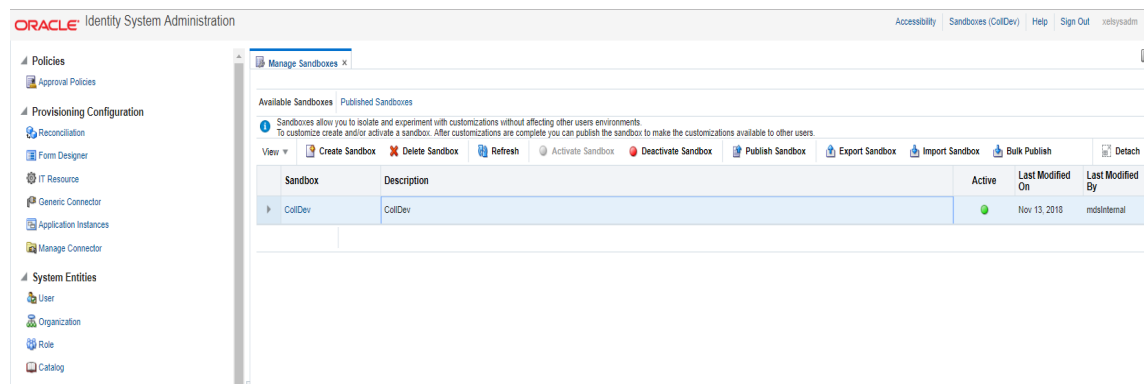


3.3.3.2 Activate Sandbox

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

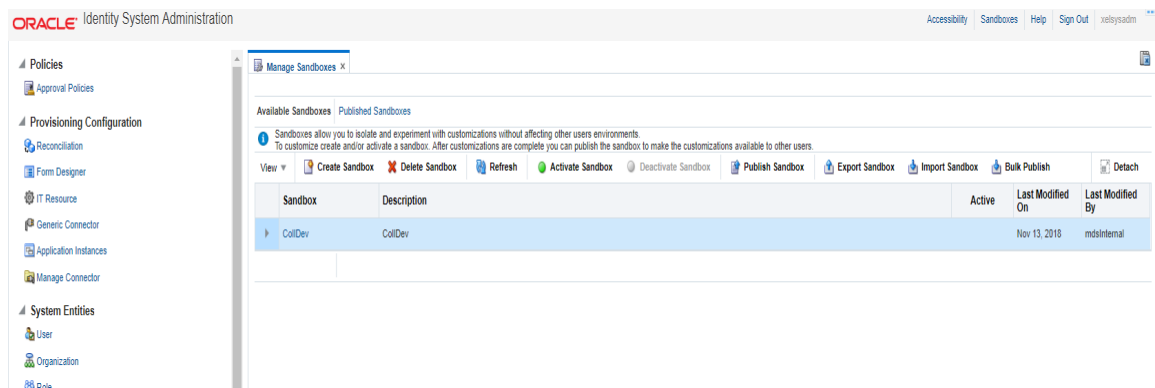


2. Sandbox is active now. It will be highlighted with green dot.

3.3.3.3 Deactivate Sandbox

To deactivate a Sandbox, perform the following steps:

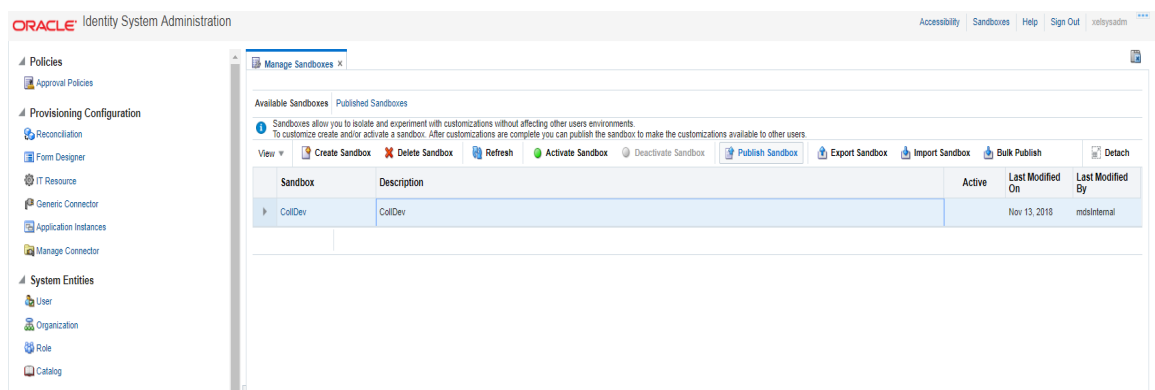
1. Select **CollectionsDev** sandbox.
2. Click **Deactivate Sandbox** to deactivate sandbox.
Sandbox is deactivated now.

Figure 3–20 Deactivate Sandbox

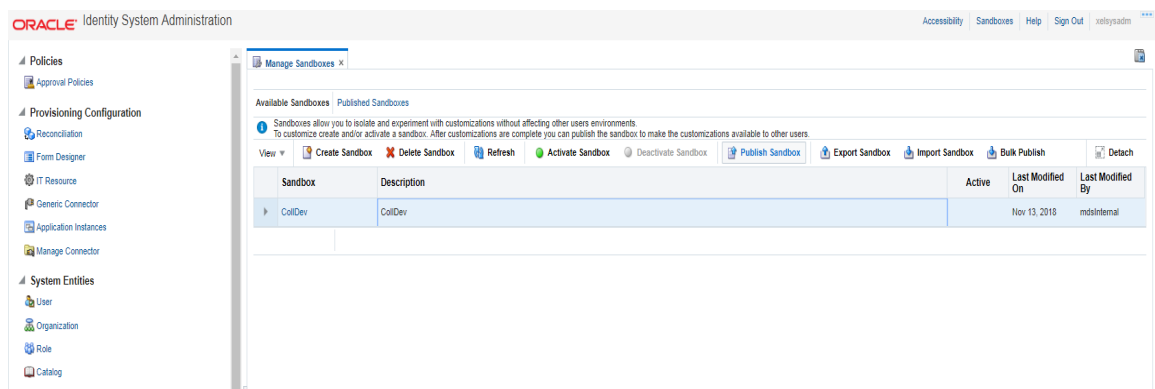
3.3.3.4 Publish Sandbox

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.

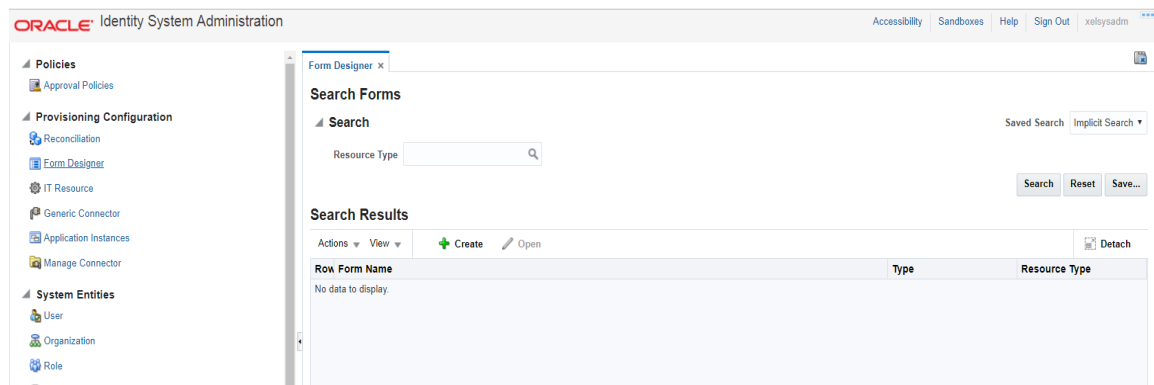
Figure 3–22 Published Sandbox

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:

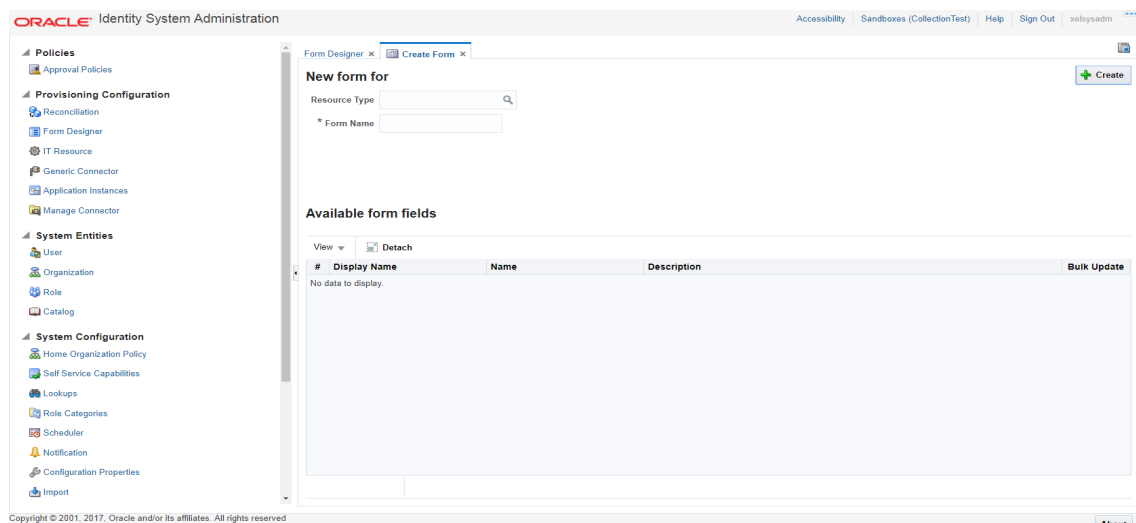
1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see [Chapter 1.3.3 Oracle Banking Enterprise Collections and Oracle Banking Enterprise Recovery Sandbox](#).
3. In the left pane, under Configuration,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

Figure 3–23 Create Form - Form Designer



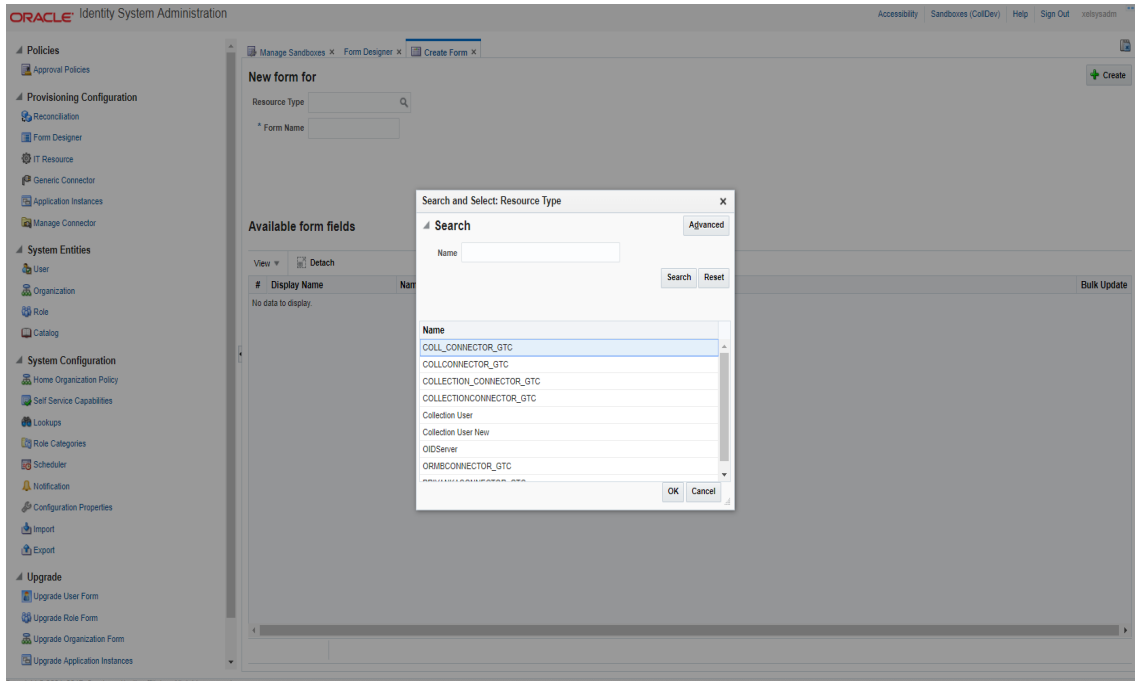
4. Click **Create** on the toolbar. The **Create Form** page is displayed.
5. In the **Resource Type** field, verify the name of the resource object with which the form is associated is displayed. To change the resource object name, click the Search icon next to the **Resource Type** field, and search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

Figure 3–24 Create Form - Resource Type



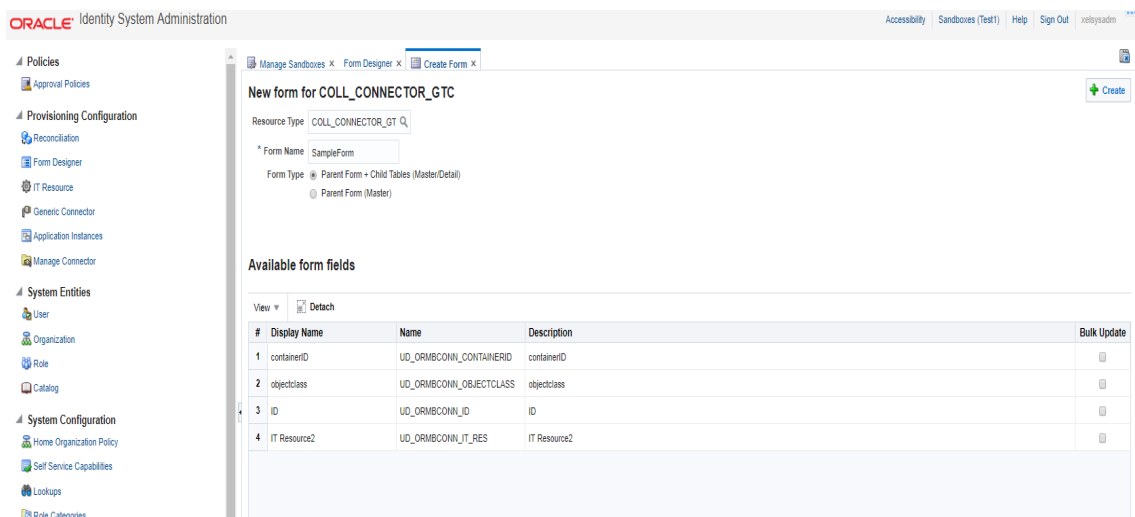
6. Select **Resource Type** as **COLL_CONNECTOR_GTC** and provide a name for the form (for example, SampleForm).

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



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

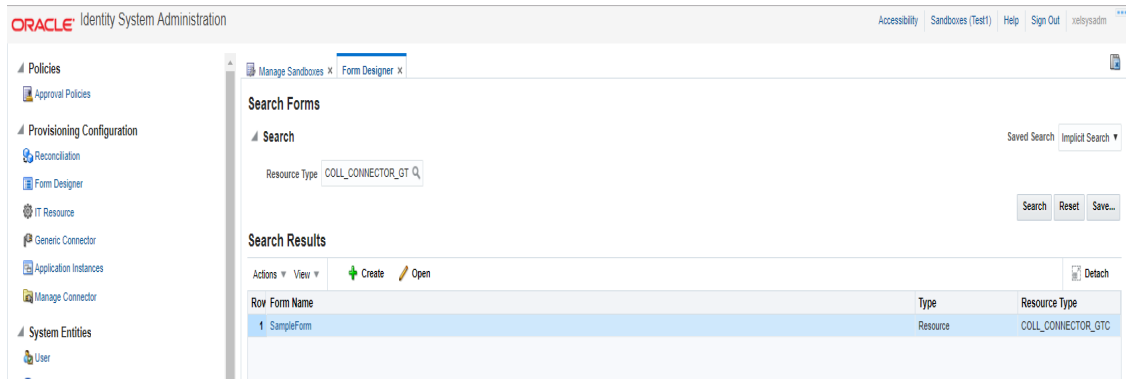
Figure 3–26 Create Form Resource Type - Available Form Fields



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

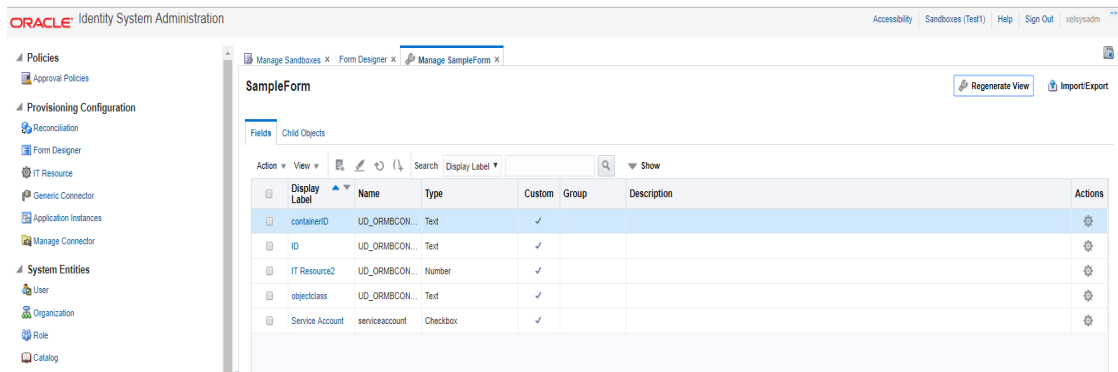
9. Refresh the **Search Results** in **Form Designer** page for resource type : `COLL_CONNECTOR_GTC`.
10. Select the **SampleForm** from the results.

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

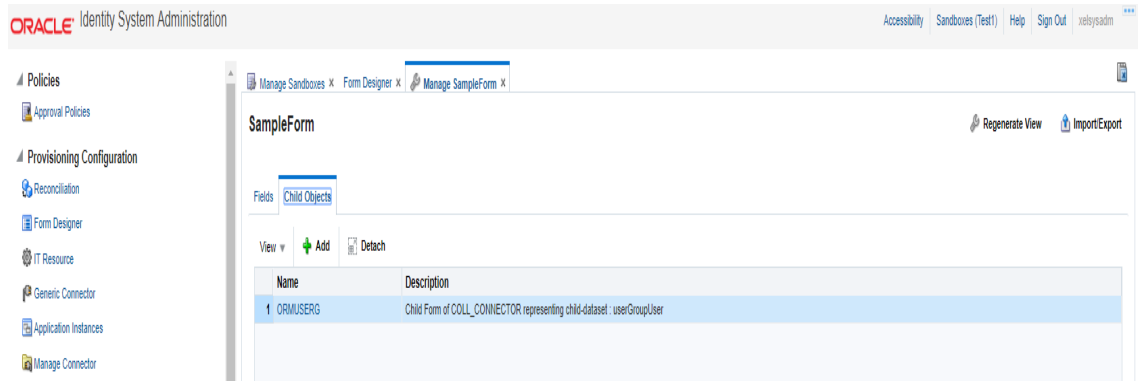
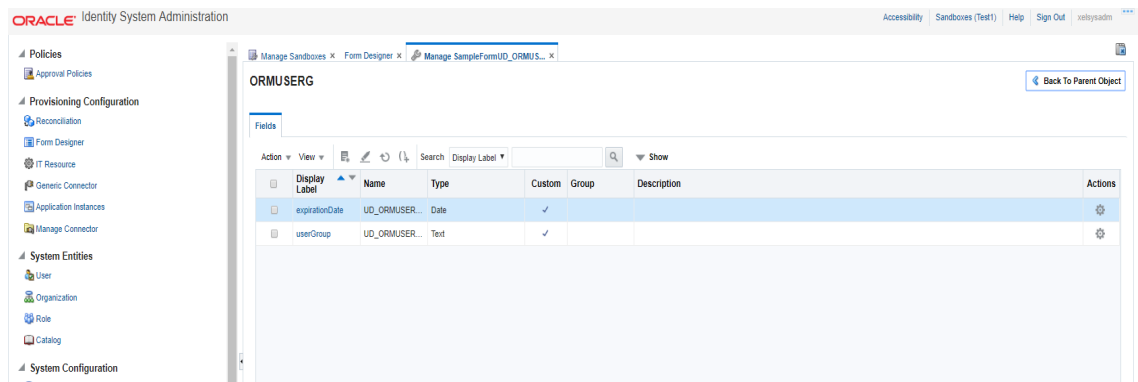


Figure 3–30 Manage Child Objects form fields



- Click the userGroup and give default value as ALL_SERVICES.

Figure 3–31 Set default values for field- userGroup

The screenshot shows the Oracle Identity System Administration interface. The left sidebar contains a navigation menu with categories like Policies, Provisioning Configuration, System Entities, System Configuration, and Upgrade. The main content area is titled "Edit Text Field : userGroup". It has several sections:

- Appearance:** "Display Label" is set to "userGroup" and "Display Width" is 40 characters.
- Name:** "Name" is "UD_ORMUSERG_USERGROUP" and "API Name" is "UD_ORMUSERG_USERGROUP__c".
- Constraints:** "Searchable" is checked and "Maximum Length" is 20 characters.
- Default Value:** The value is set to "ALL_SERVICES".
- Advanced:** "Encrypt" and "Use in Bulk" are unchecked.

 Buttons for "Save and Close" and "Cancel" are in the top right. The browser address bar shows "10.180.26.128:14600/sysadmin/faces/home?_af=manage_sandboxes#".

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

Figure 3–32 Set default value for field- expirationDate

The screenshot shows the Oracle Identity System Administration interface. The left sidebar is the same as in Figure 3-31. The main content area is titled "Edit Date Field : expirationDate". It has several sections:

- Appearance:** "Display Label" is set to "expirationDate".
- Name:** "Name" is "UD_ORMUSERG_EXPIRATIONDATE" and "API Name" is "UD_ORMUSERG_EXPIRATIONDATE__c".
- Constraints:** "Searchable" is checked.
- Default Value:** The value is set to "2023-11-29".
- Advanced:** "Use in Bulk" is unchecked.

 Buttons for "Save and Close" and "Cancel" are in the top right. The browser address bar shows "10.180.26.128:14600/sysadmin/faces/home?_af=manage_sandboxes#".

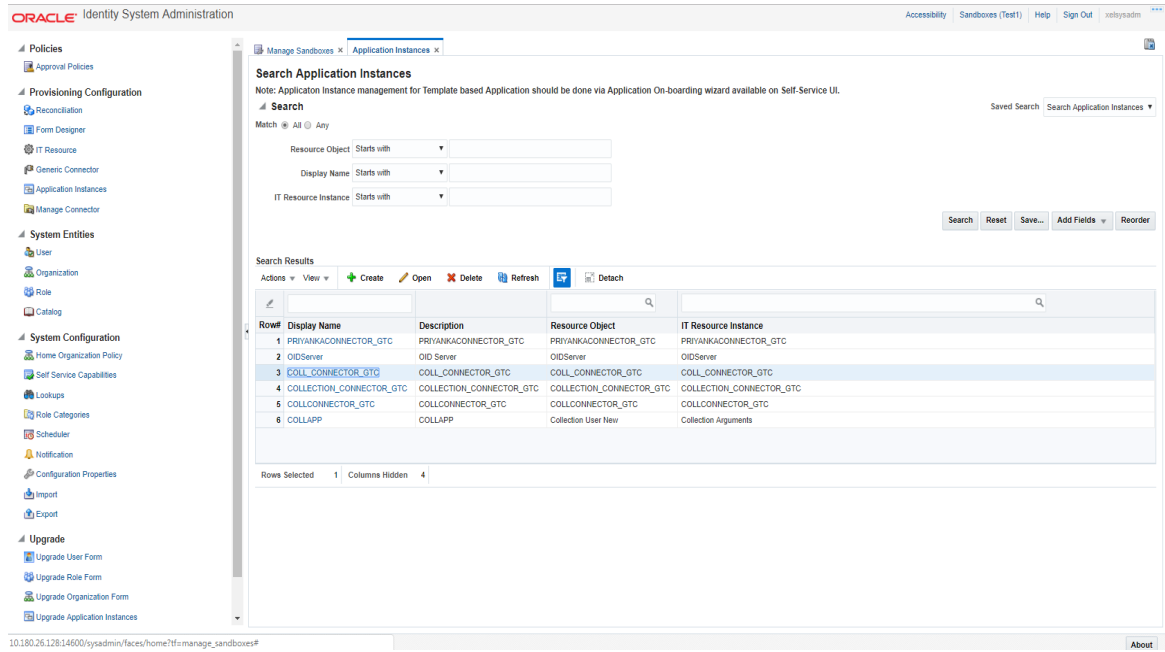
- Click **Save and Close**.
- Click the **Back to Parent Object** Link.

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

The screenshot shows the Oracle Identity System Administration interface. The left sidebar contains a navigation menu with categories like Policies, Provisioning Configuration, System Entities, System Configuration, and Upgrade. The main content area is titled 'Application Instance: COLL_CONNECTOR_GTC' and has three tabs: 'Attributes', 'Organizations', and 'Entitlements'. The 'Attributes' tab is active. Below the tabs, there are several input fields: 'Name' (COLL_CONNECTOR_GTC), '* Display Name' (COLL_CONNECTOR_GTC), 'Description' (COLL_CONNECTOR_GTC), 'Resource Object' (COLL_CONNECTOR_GTC), 'IT Resource Instance' (COLL_CONNECTOR_GTC), 'Form' (a dropdown menu with 'SampleForm' selected), and 'Parent Appliance' (empty). There are 'Apply' and 'Revert' buttons at the top right. The bottom of the page shows a URL and an 'About' button.

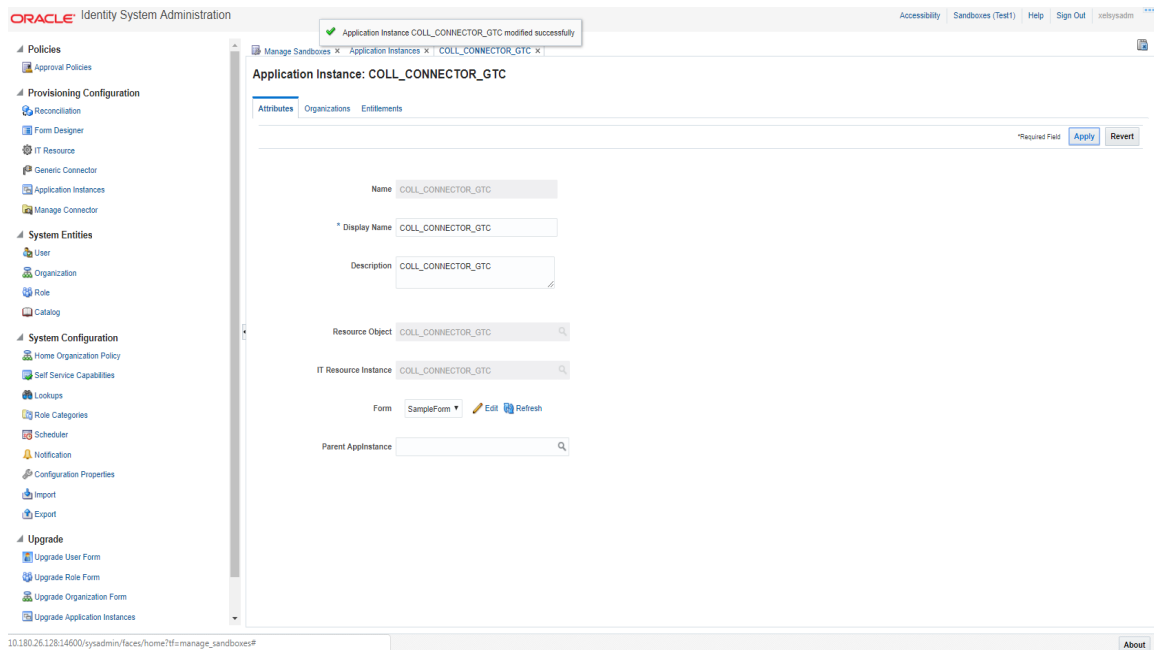
3. In Form list, select above created form and click **Apply**.

Figure 3–35 Associate Form with Application instance

This screenshot is identical to Figure 3-34, showing the 'Application Instance: COLL_CONNECTOR_GTC' configuration page. The 'Form' dropdown menu is now populated with a list of forms, and 'SampleForm' is selected. The 'Apply' button is visible at the top right. The rest of the interface, including the sidebar and other configuration fields, remains the same.

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

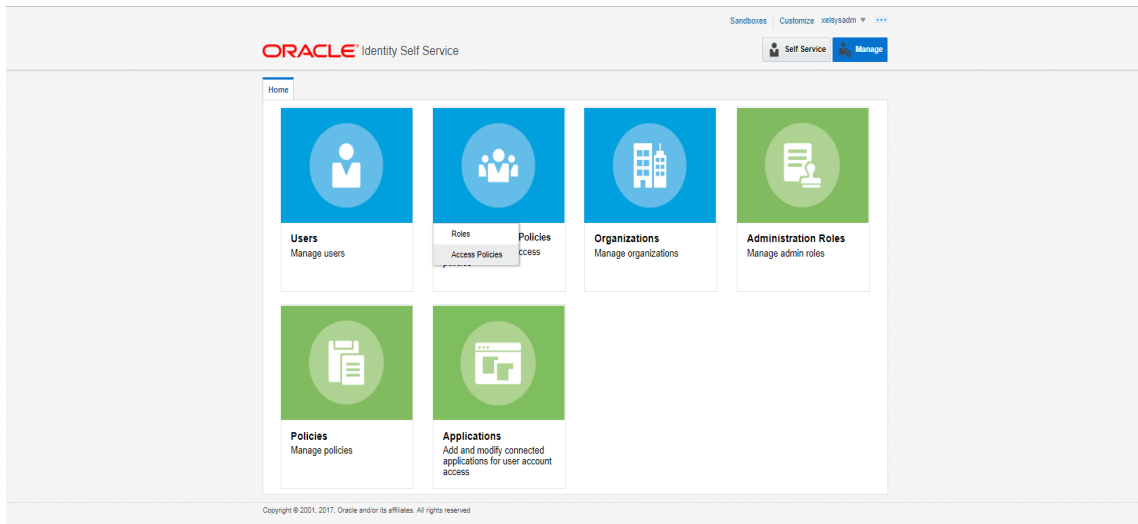
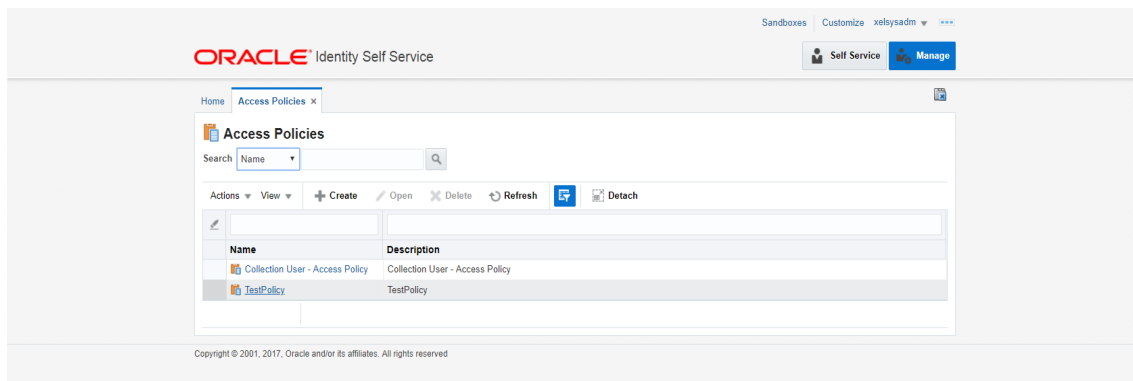


Figure 3–38 Access Policies



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

Figure 3–39 Create Access Policy

The screenshot shows the Oracle Identity Self Service interface. At the top, there's a navigation bar with 'Sandboxes', 'Customize', and 'xelsysadm'. Below that, a breadcrumb trail shows 'Home', 'Access Policies', and 'Create Access Policy'. The main content area is titled 'Create Access Policy' and features a progress bar with two steps: 'Attributes' (active) and 'Applications'. Below the progress bar, the 'General Attributes' section includes the following fields:

- * Name:
- * Description:
- * Owner: User (with a search icon)
- Retrofit:
- * Priority Level:

Buttons for 'Back', 'Cancel', and 'Next' are visible at the top of the form area.

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

Figure 3–40 Access Policy details

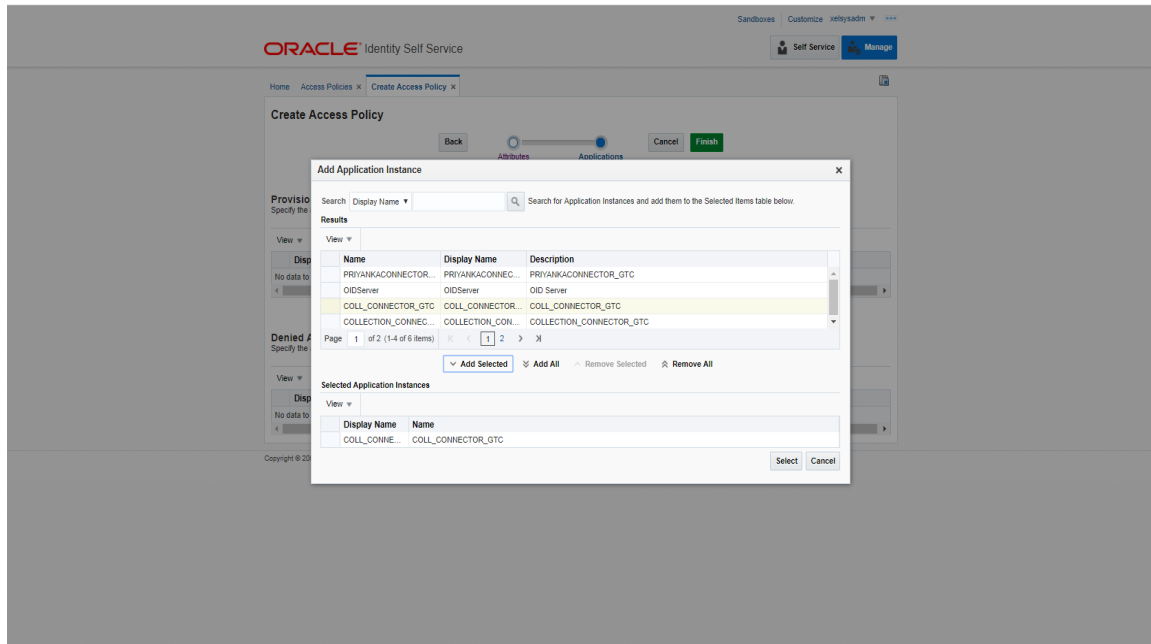
This screenshot shows the same 'Create Access Policy' page as Figure 3-39, but with the following example data entered:

- * Name: Coll_AccessPolicy
- * Description: Coll_AccessPolicy
- * Owner: User (with a search icon)
- Retrofit:
- * Priority Level:

The progress bar now shows 'Applications' as the active step, and the 'Next' button is highlighted.

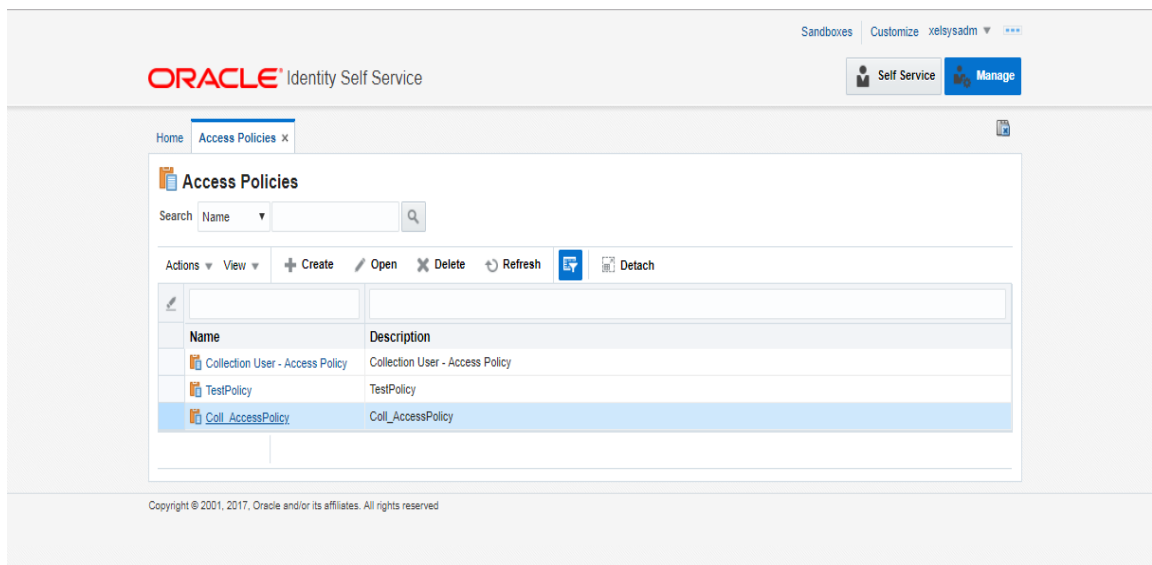
- To specify the application instances provisioned by this access policy, click **Add** and select **COLL_CONNECTOR_GTC** Application Instance. Click **Select**.

Figure 3–41 Add application instance associated with access policy



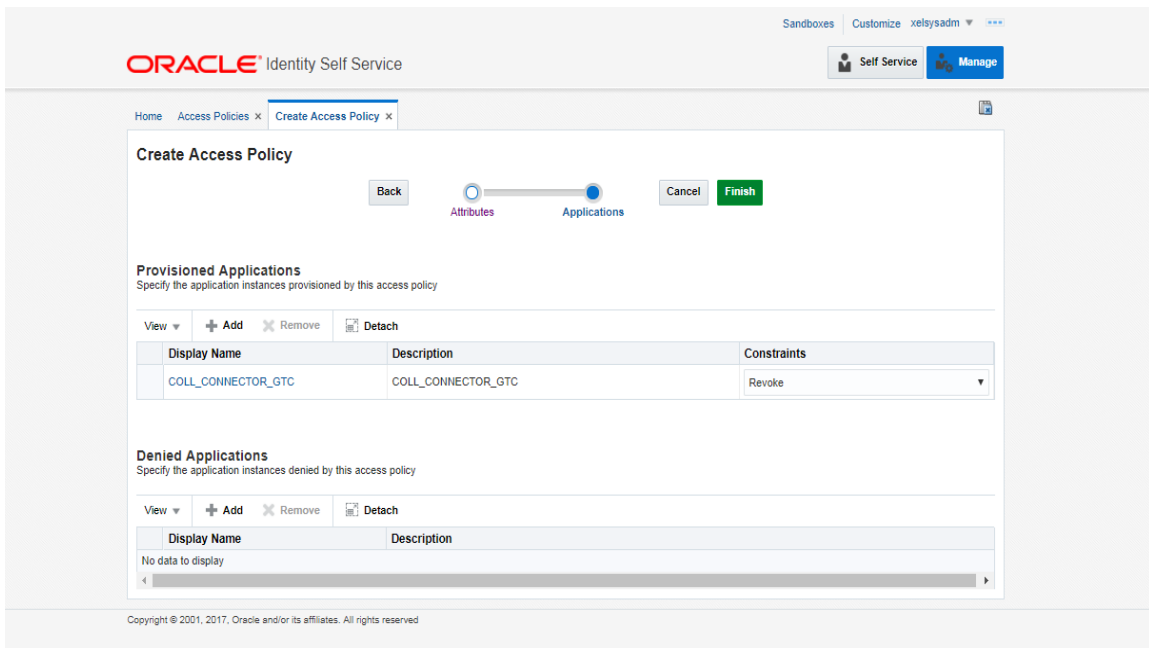
7. Click **Finish**.
8. In the Search Access Policies Page, select the above created policy and click the **Applications** tab.

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

ORACLE Identity Self Service

Home Access Policies x Access Policy - Coll_Acce... x

Attributes Applications Roles

Save Cancel

General Attributes

containerID ID

objectclass User IT Resource2 122

Child Form of COLL_CONNECTOR representing child-dataset : userGroupUser

Select Search

View + Add X Delete X Delete All Detach

	userGroup ^ v	expirationDate ^ v	Pending Action ^ v
1	ALL_SERVICES	11/30/2021	Add

Copyright © 2001, 2017, Oracle and/or its affiliates. All rights reserved.

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

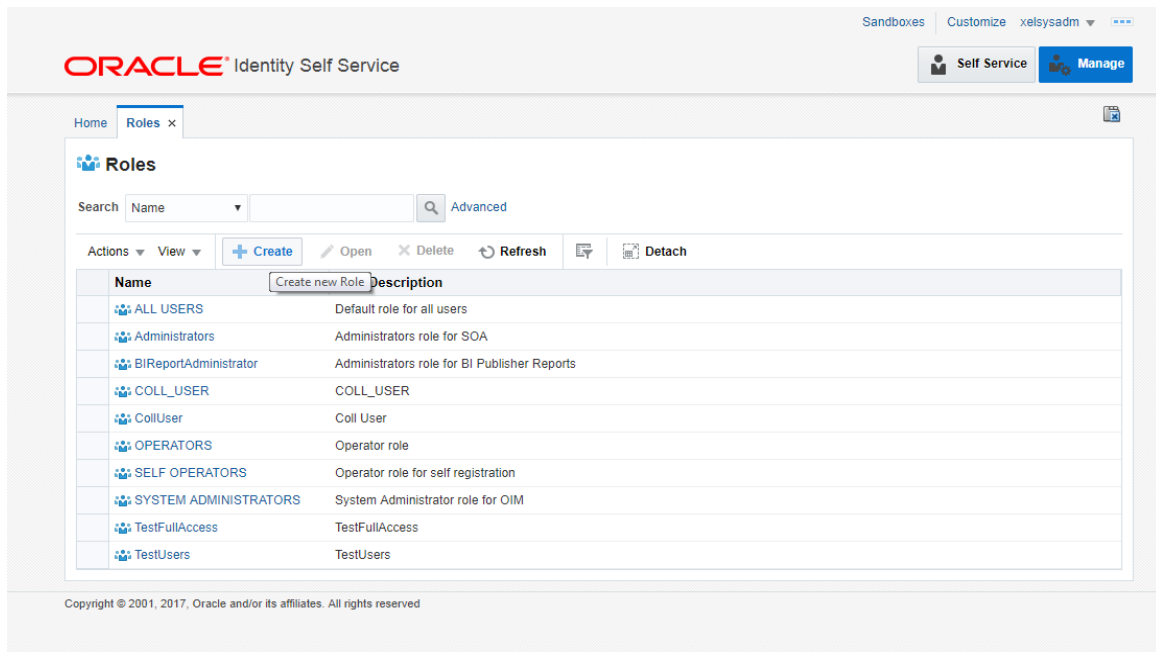
3.3.5.2 Creating Roles

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

ORACLE Identity Self Service

Sandboxes Customize xelsysadm

Self Service Manage

Home Roles x Create Role x

Create Role
This wizard walks you through the steps to create a Role.

Back Attributes Hierarchy Access Policy Members Organizations Summary Cancel Next

General Role Information

* Name

* Display Name

Role E-mail

Role Description

* Owned By

▾ Catalog Attributes

* Category

Audit Objective

Risk Level

User Defined Tags

Approver User

Approver Role

Certifier User

Certifier Role

Fulfillment User

Fulfillment Role

Certifiable

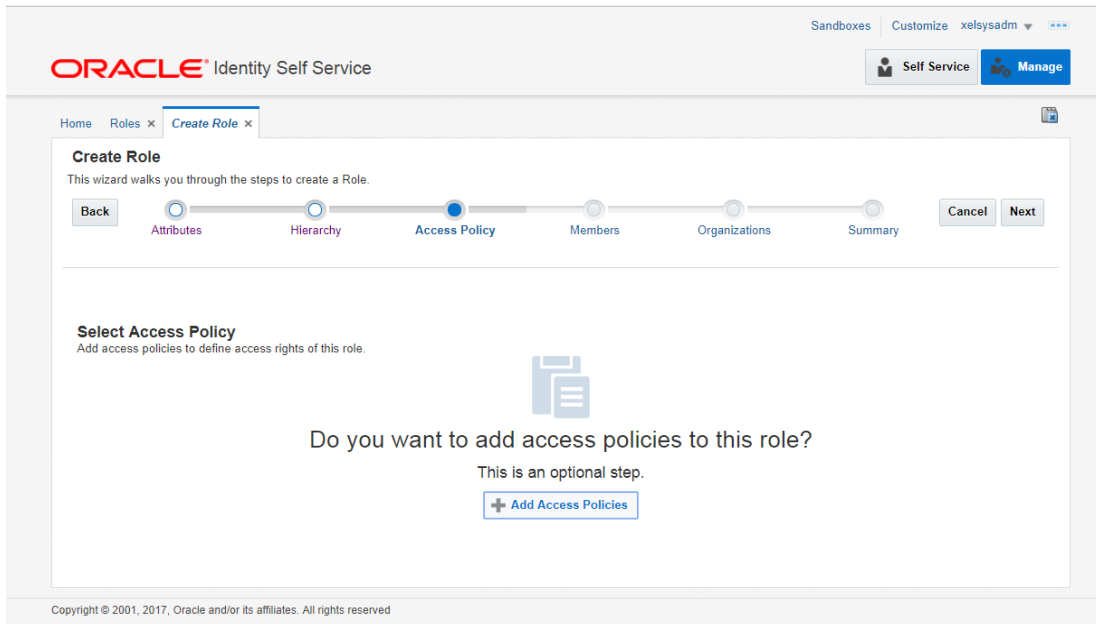
Auditable

Requestable

Copyright © 2001, 2017, Oracle and/or its affiliates. All rights reserved.

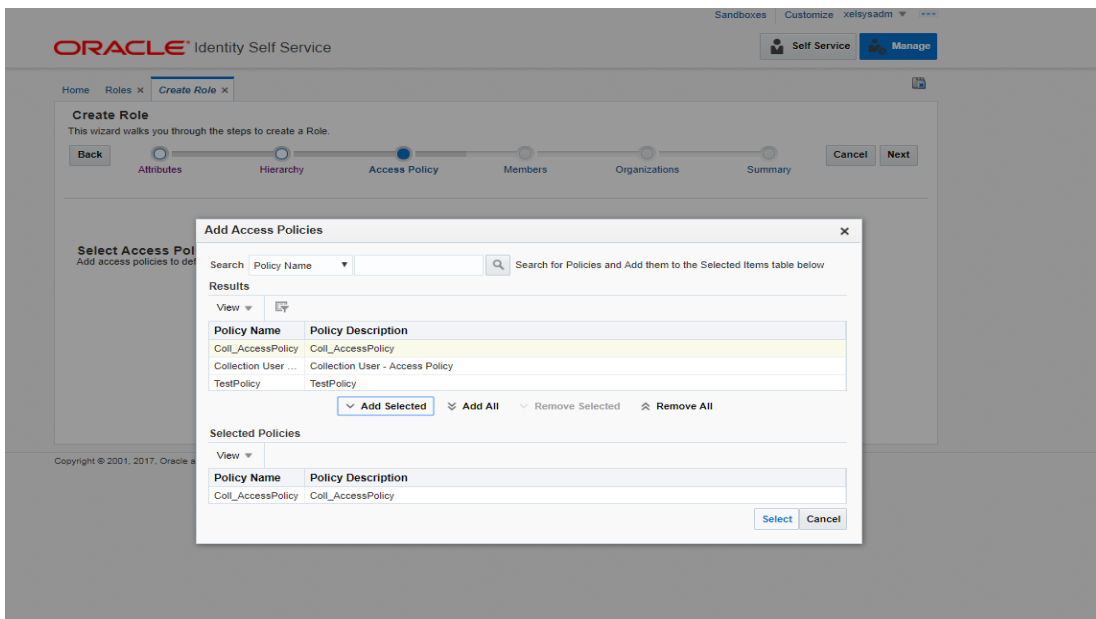
- Click **Next** to go to the Access Policy step.

Figure 3–47 Create Role



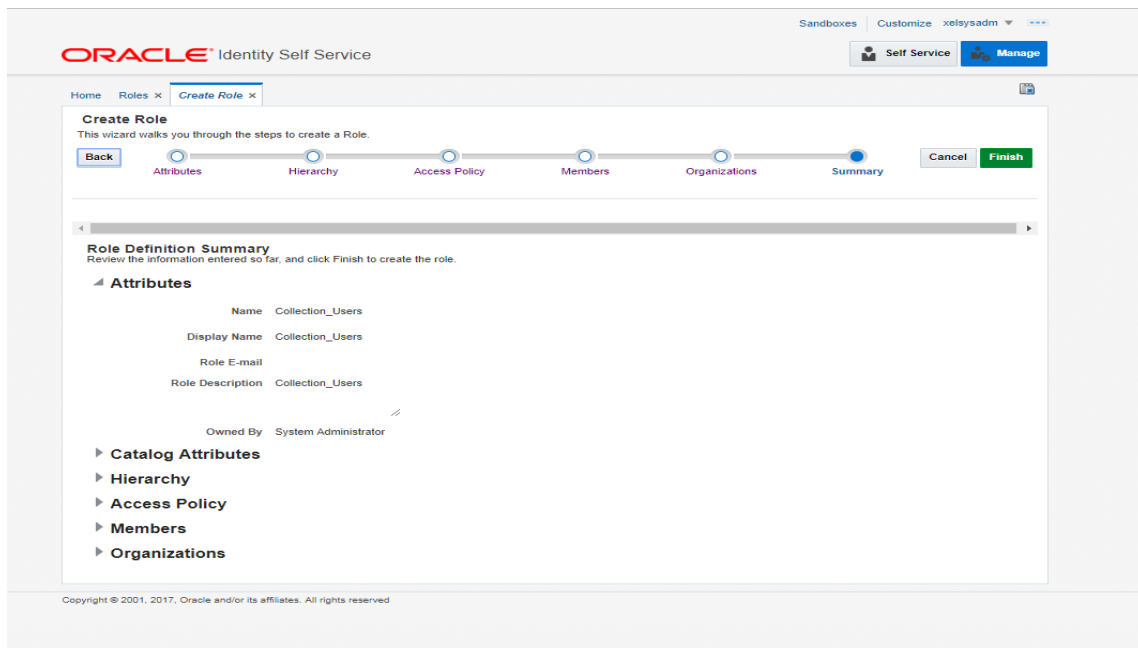
- Click **Add Access Policies**. List of access policies is displayed on clicking the search icon.

Figure 3–48 Add Access Policy to the role



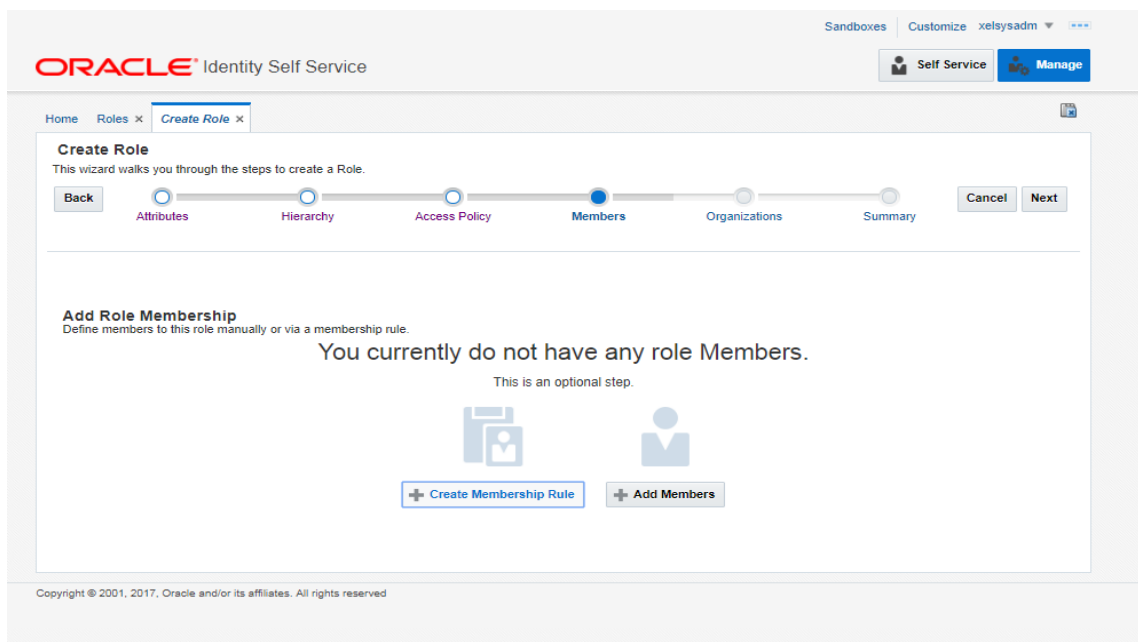
8. Select above created access policy (eg: Coll_AccessPolicy) and click **Next**.

Figure 3–49 Add Access Policy to the role



9. In the Members Step, click **Create Memembrship 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

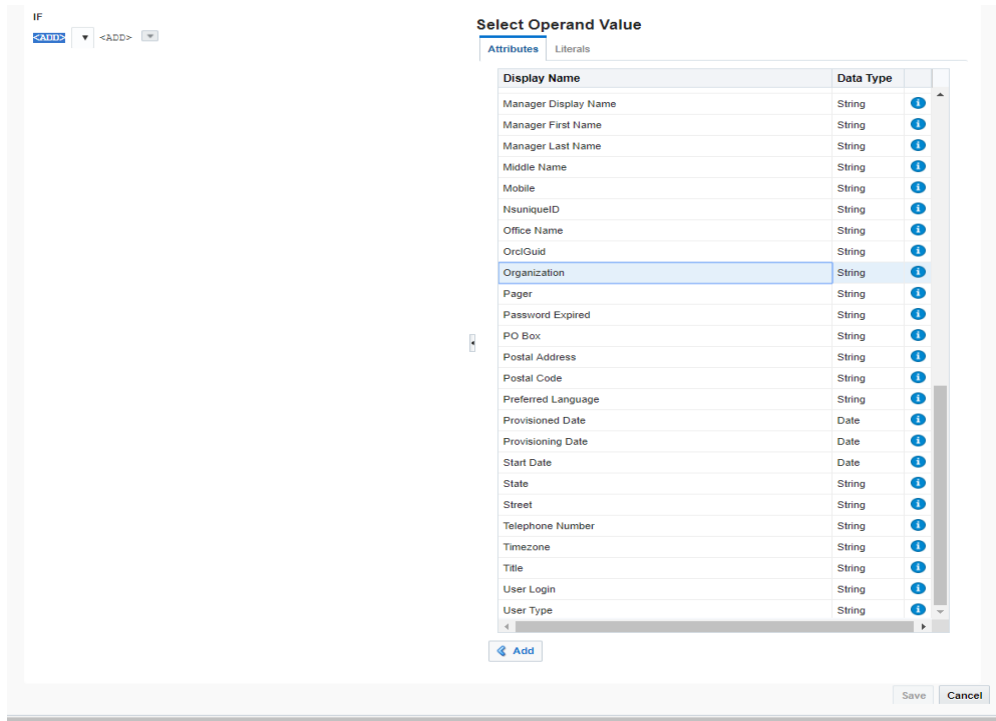
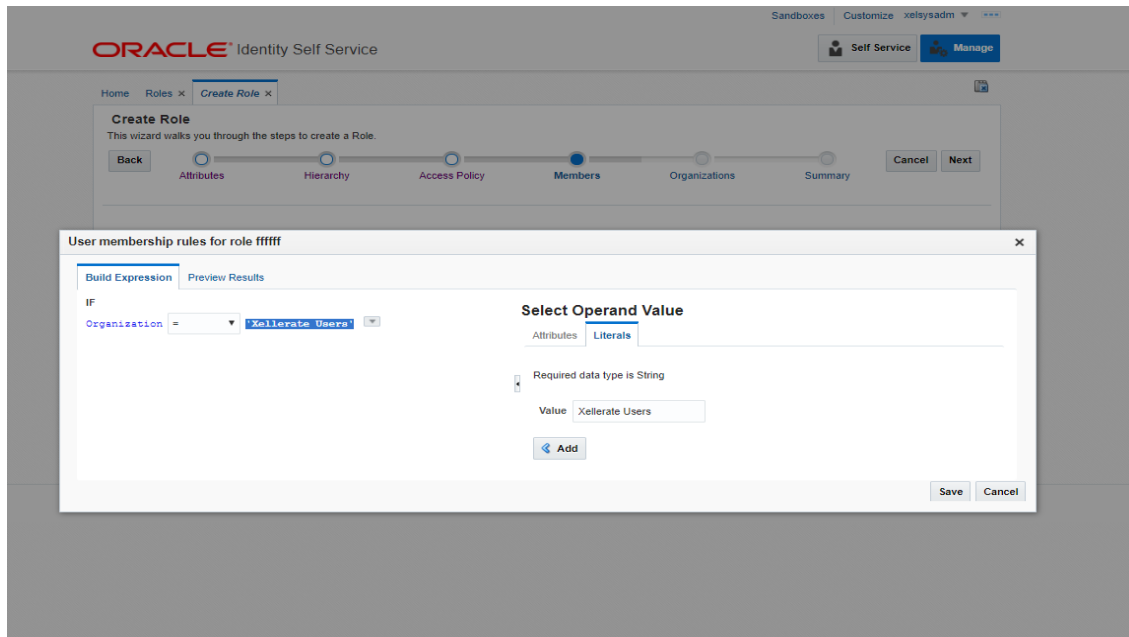


Figure 3–52 Build Membership Rule Expression



11. Click **Save**.

3.4 DB Based Configuration

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

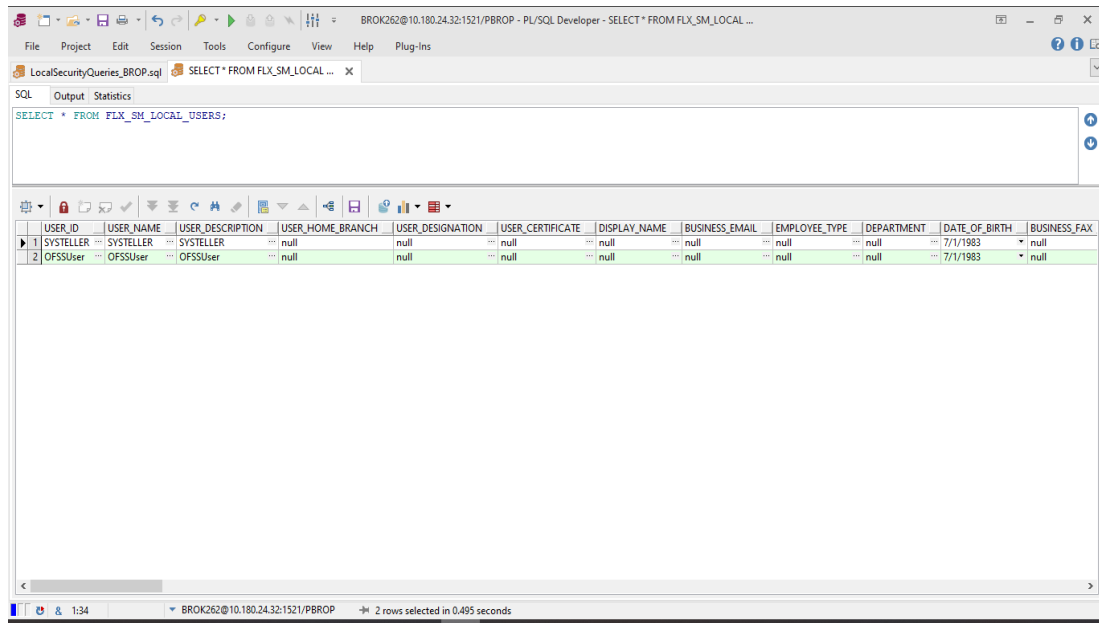
3.4.1 DB Based Policy Configuration

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:

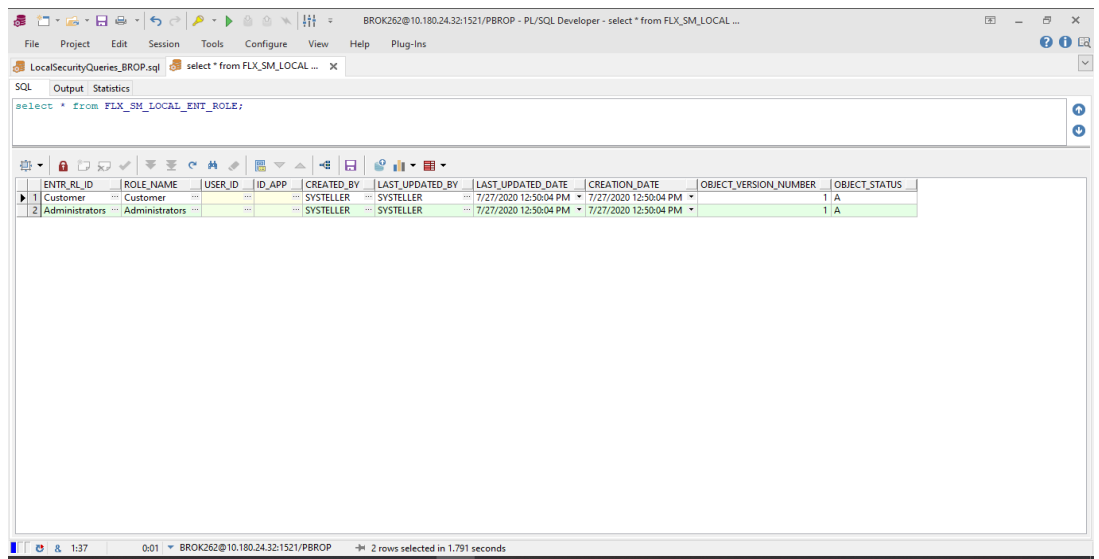
- **FLX_SM_LOCAL_USERS (Related view FLX_SM_LOCAL_USERS_V)**: This table defines the users in OBP for whom access policies are to be configured. All user IDs need to be in lowercase.

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

APP_RL_ID	ROLE_NAME	ROLE_CATEGORY	DESCRIPTION	ROLE_TYPE	ID_APP	CREATED_BY	LAST_UPDATED_BY	LAST_UPDATED_DATE	CREATION_DATE	OBJECT_VERSION_NUMBER	OBJECT_STATUS
1	Customer	Customer	Customer			SYSTELLER	SYSTELLER	7/27/2020 12:46:15 PM	7/27/2020 12:46:15 PM	1	A
2	Administrators	Administrators	Administrators			SYSTELLER	SYSTELLER	7/27/2020 12:46:15 PM	7/27/2020 12:46:15 PM	1	A

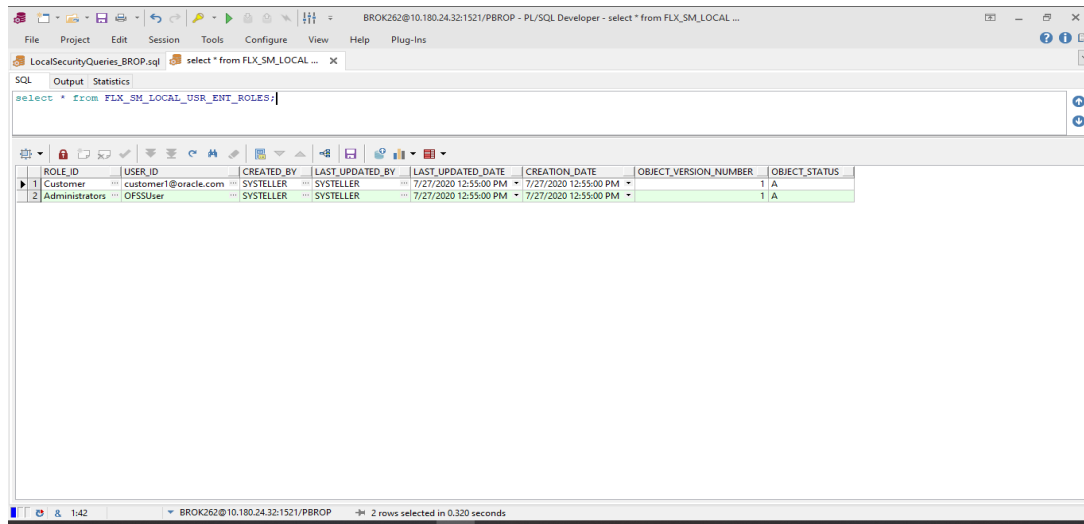
- **FLX_SM_LOCAL_ENT_APP_LNK (Related view FLX_SM_LOCAL_ENT_APP_LNK_V):** This table defines the mapping between Enterprise Roles and Application Roles.

Figure 3–56 FLX_SM_LOCAL_ENT_APP_LNK

ENTR_RL_ID	APP_RL_ID
1	Customer
2	Administrators

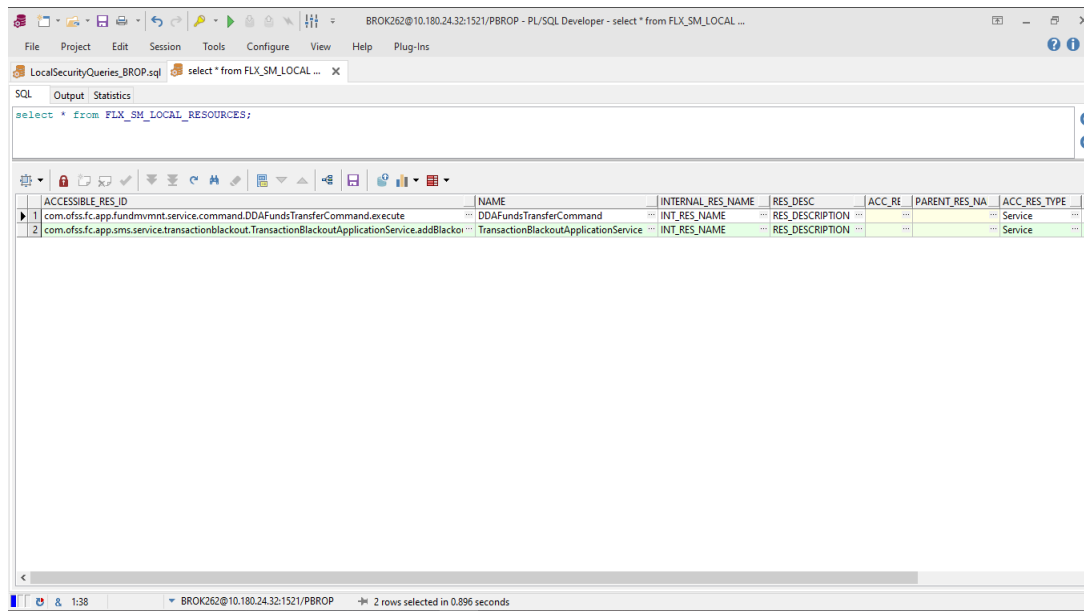
- **FLX_SM_LOCAL_USR_ENT_ROLES (Related view FLX_SM_LOCAL_USR_ENT_ROLES_V):** This table defines the user id to Application role mapping. All user IDs need to be in lowercase.

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

POLICY_ENTRY_ID	POLICY_NAME	POLICY_DESC	APP_ROLE_ID	EFFECT_TYPE	CREATED_BY	LAST_UPDATED_BY
1	PL_ENTRY_com.ofss.fc.app.fundmvmnt.service.command.DDAFundsTransferCommand.execute	Policy_For_DDAFundsTransferCommand	Customer	grant	OFSSUser	OFSS
2	PL_ENTRY_com.ofss.fc.app.sms.service.transactionblackout.TransactionBlackoutApplicationService.addBlackout	Policy_For_TransactionBlackoutApplicationService	Administrators	grant	OFSSUser	OFSS

- 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

ACCESSIBLE_RES_ID	POLICY_ENTRY_ID
com.ofss.fc.app.fundmvmnt.service.command.DDAFundsTransferCom	PL_ENTRY_com.ofss.fc.app.fundmvmnt.service.command.DDAFundsTra
com.ofss.fc.app.sms.service.transactionblackout.TransactionBlackoutAp	PL_ENTRY_com.ofss.fc.app.sms.service.transactionblackout.TransactionF

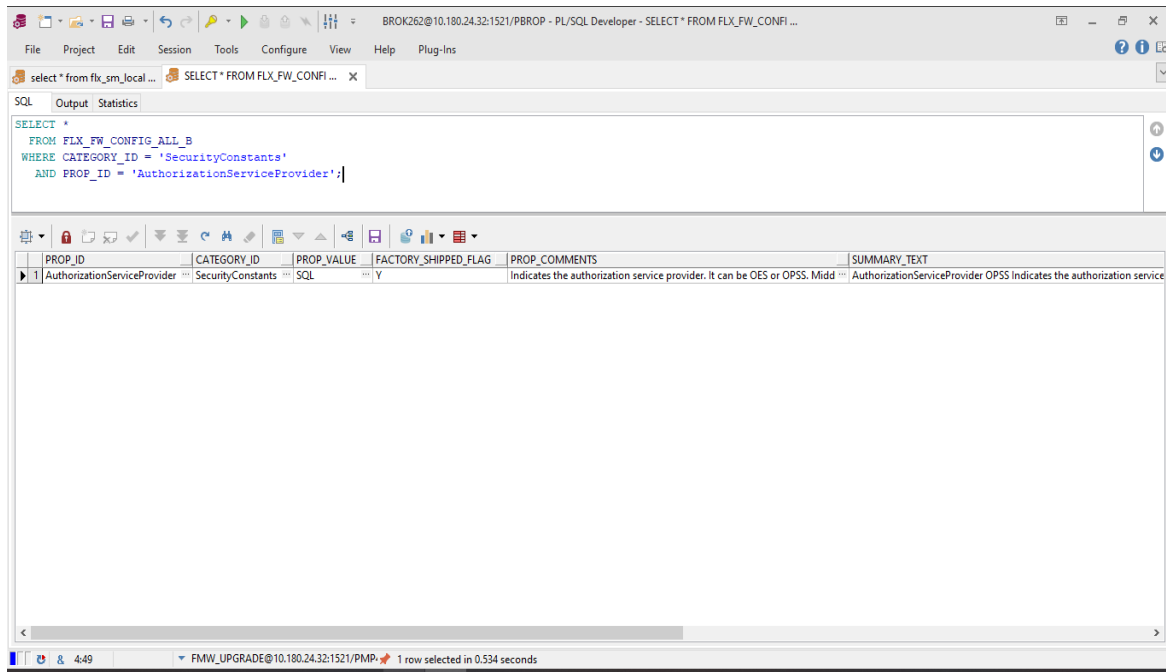
To enable DB based menu, following changes need to be made in the configuration (flw_fw_config_all_b):

```
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.

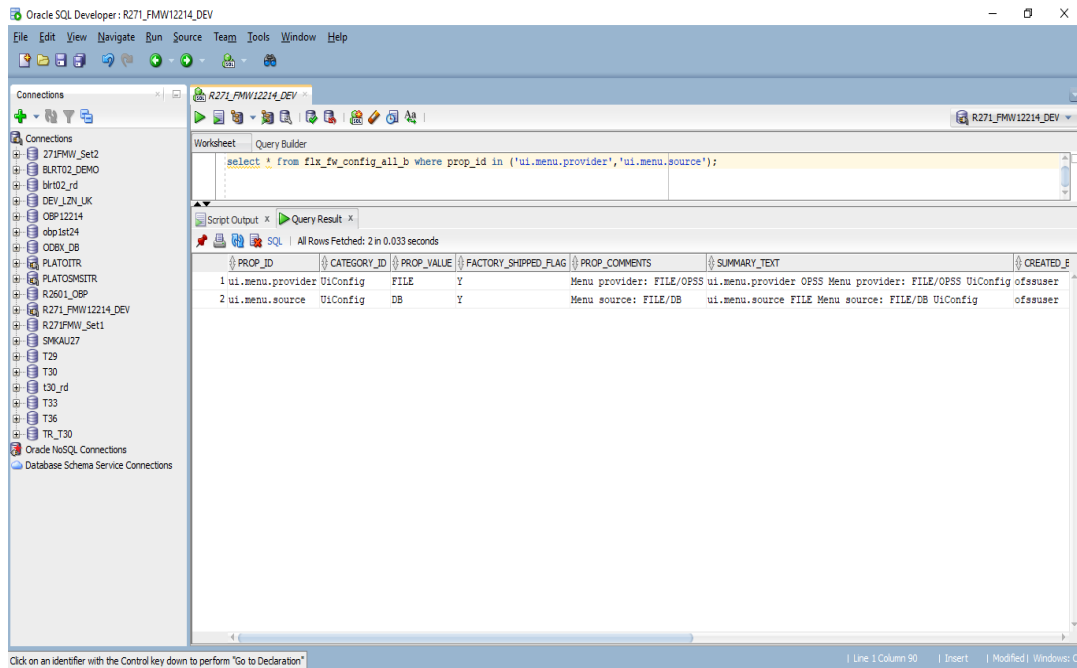
To enable or disable a certain menu element for a particular role:

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

Figure 3–62 Configuration for Role Based Menu



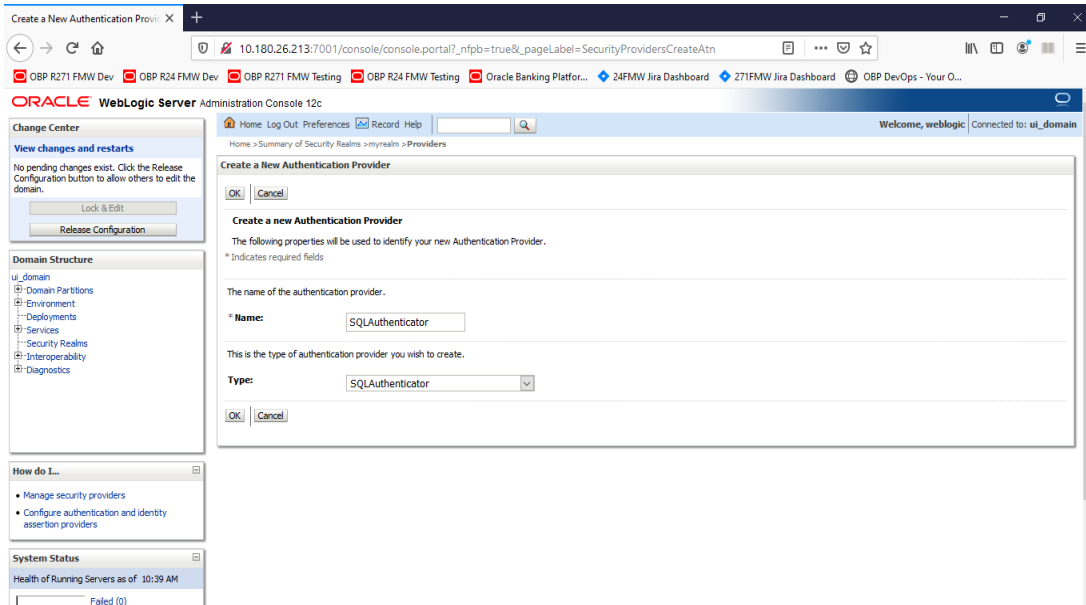
The UI Managed Server needs to be restarted. On login, the menu will be fetched using Menu files (from config) and policies as defined in database instead of OPSS.

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

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

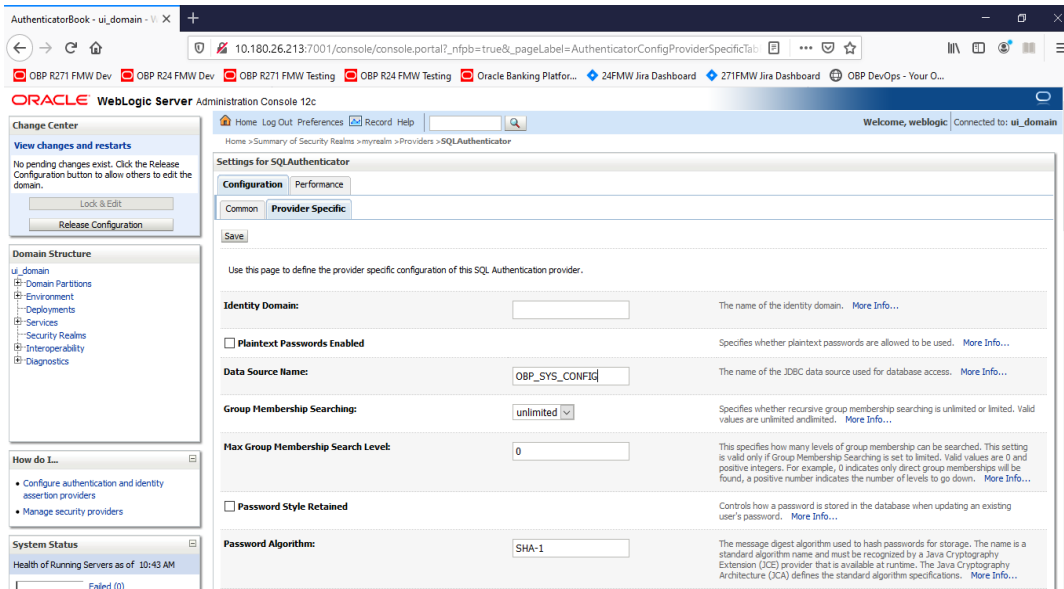
1. Navigate to Security Realms > myrealm > Providers
2. Create a new provider of Type **SQLAuthenticator**

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).

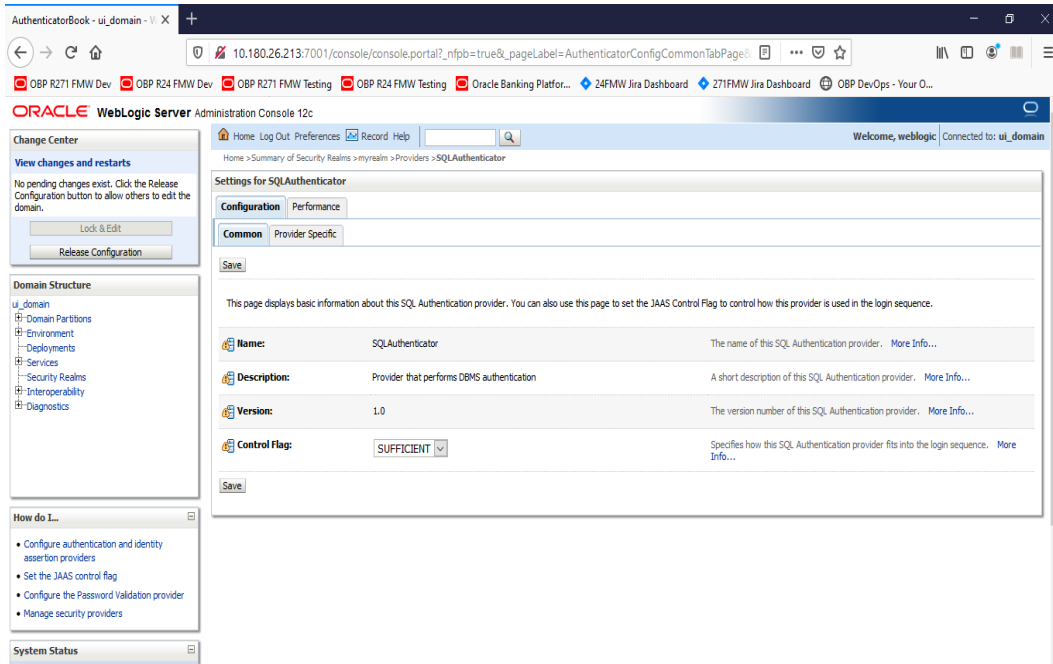
Figure 3–64 Provider Specific Settings



The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled 'Settings for SQLAuthenticator' and is divided into 'Configuration' and 'Performance' tabs. The 'Configuration' tab is active, and the 'Provider Specific' sub-tab is selected. The 'Password Algorithm' is set to 'SHA-512'. Other visible settings include 'Identity Domain', 'Plaintext Passwords Enabled', 'Data Source Name' (OBP_SYS_CONFIG), 'Group Membership Searching' (unlimited), and 'Max Group Membership Search Level' (0). The left sidebar contains navigation options like 'Change Center', 'Domain Structure', 'How do I...', and 'System Status'.

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,  
       PREFERRED_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 GROUPEMEMBERS

(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.

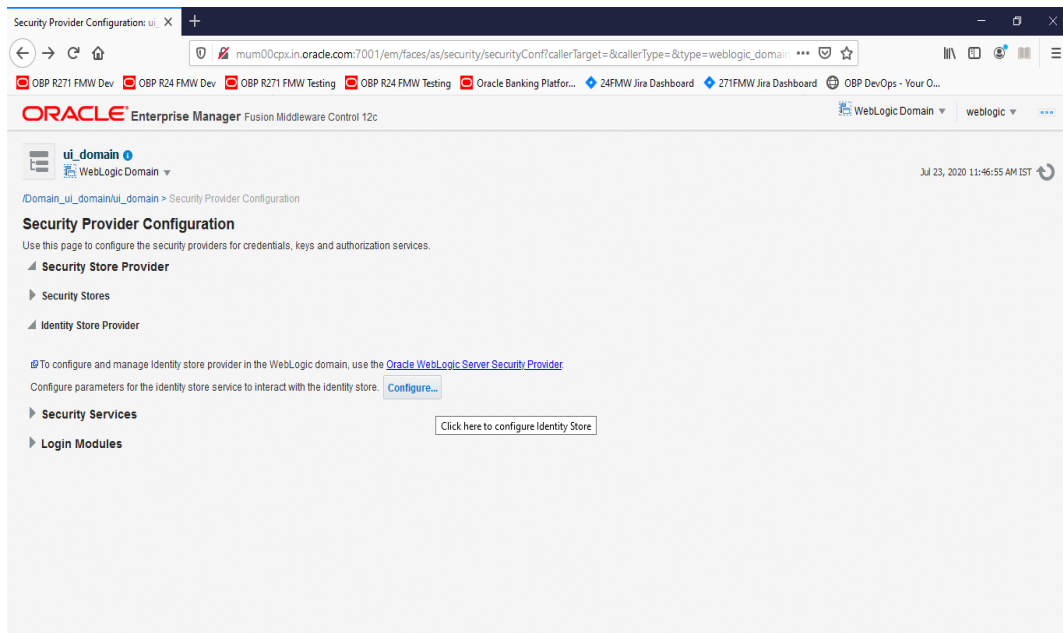
Figure 3–66 Service Provider Configuration

The screenshot shows the Oracle Enterprise Manager interface for a WebLogic Domain. The left navigation pane is expanded to 'Security' > 'Security Provider Configuration'. The main content area shows the configuration for the 'AdminServer' on host 'mum00cpx.in.oracle.com' at port 7001. Below this, a table displays the health and CPU usage of the servers in the domain.

Host	Machine	State	Health	Listen Port	CPU Usage (%)	Heap Usage (MB)
		Running	OK	7001	0.00	536.2
ui_cluster1	ui_machine1	Running	OK	8001	0.00	1,194.9

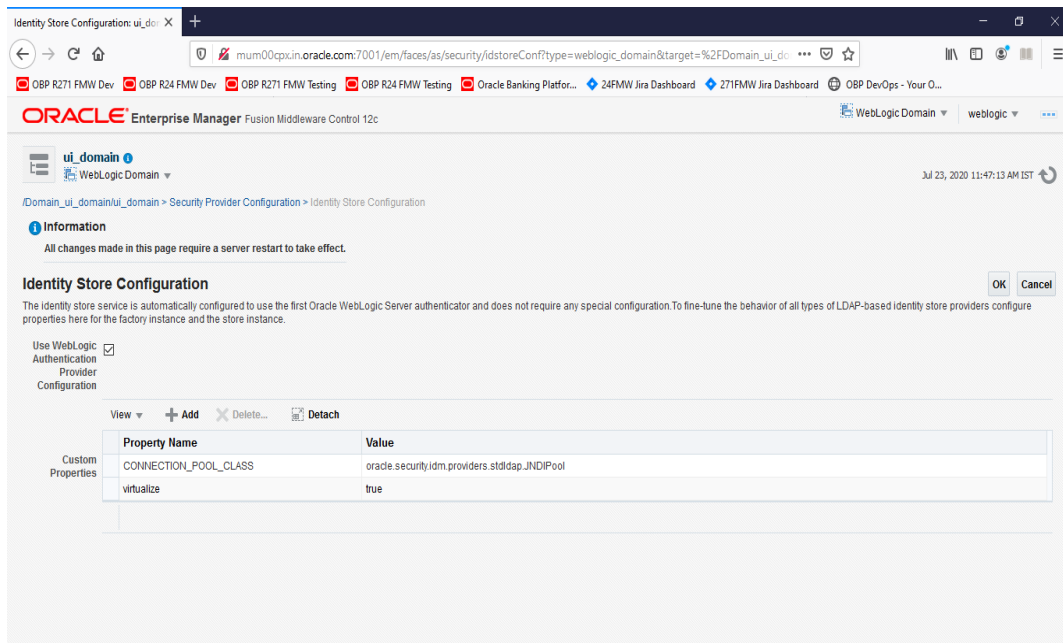
- Expand **Security Store Provider**, then **Identity Store Provider** and click on **Configure**.

Figure 3–67 Identifying Store Provider for Configuration



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

Figure 3–68 Adding Custom Property Virtualize with value True



- 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</ignoreObjectClassOnModify>
<includeInheritedObjectClasses>>true</includeInheritedObjectClasses>
<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</ignoreObjectClassOnModify>
<includeInheritedObjectClasses>>true</includeInheritedObjectClasses>
<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 adapter> -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

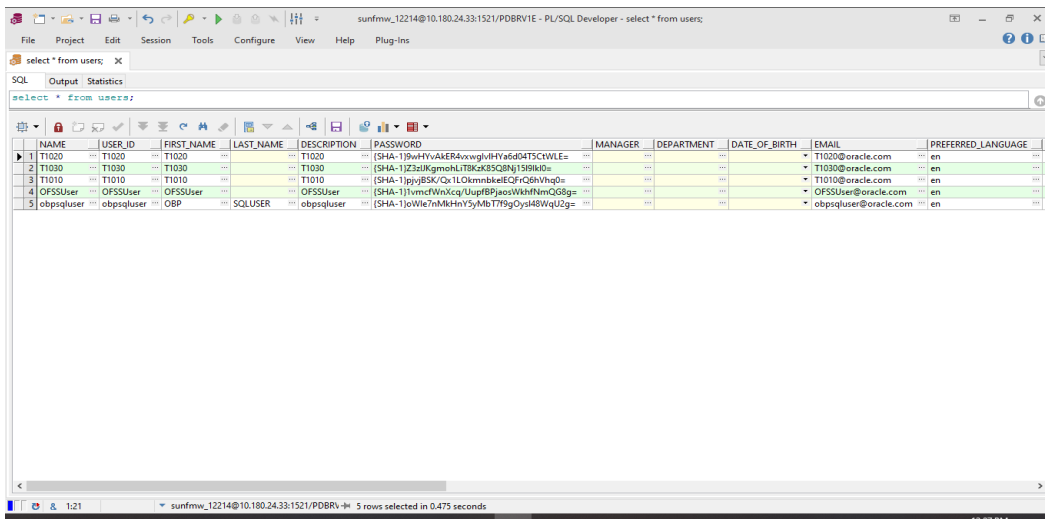
The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled 'Settings for myrealm' and is under the 'Users and Groups' tab. A table lists the configured users:

Name	Description	Provider
LCMUser	This is the default service account for WebLogic Server Lifecycle Manager configuration updates.	DefaultAuthenticator
obpsuser	obpsuser	SQLAuthenticator
OFSSUser	OFSSUser	SQLAuthenticator
OracleSystemUser	Oracle application software system user.	DefaultAuthenticator
T1010	T1010	SQLAuthenticator
T1020	T1020	SQLAuthenticator
T1030	T1030	SQLAuthenticator
weblogic	This user is the default administrator.	DefaultAuthenticator

Following are the data snapshot in the views created:

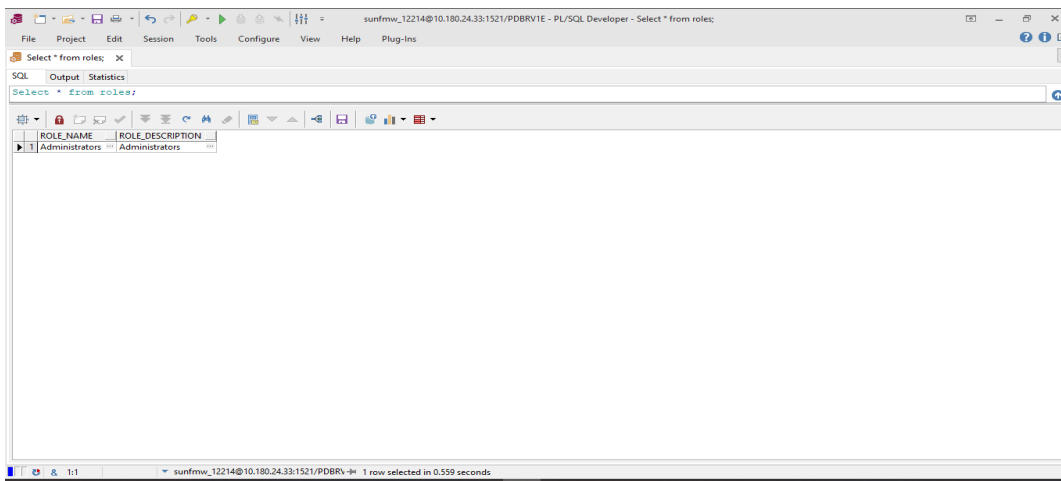
- Select * from users;

Figure 3–70 Selecting from Users



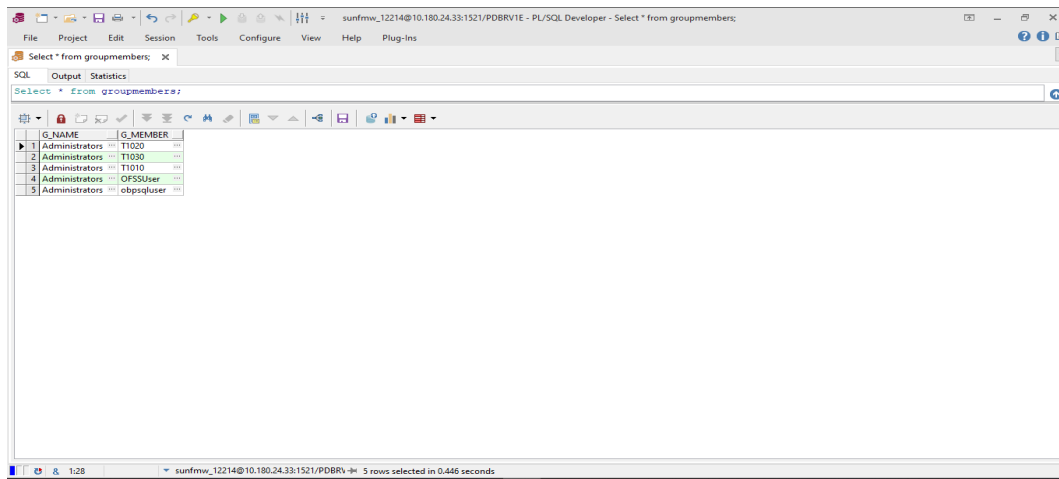
- Select * from roles;

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

The screenshot shows the Oracle Identity Self Service 'Create User' form. The form is titled 'Create User' and includes sections for Request Information, Basic Information, Account Settings, Account Effective Dates, and Provisioning Dates. Fields include Effective Date, Justification, First Name, Middle Name, Last Name, E-mail, Manager, Organization, User Type, Display Name, User Login, Password, Confirm Password, Start Date, End Date, and Provisioning Date. The form has 'Submit', 'Save As...', and 'Cancel' buttons at the top right.

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

The screenshot shows the Oracle Identity Self Service 'Create User' form. The form is titled 'Create User' and includes sections for Request Information, Basic Information, Account Settings, Account Effective Dates, and Provisioning Dates. The Request Information section has 'Effective Date' set to 11/13/2018 and 'Justification' set to 'Test User'. The Basic Information section includes fields for First Name (Beta), Middle Name, Last Name (Swan), Manager, Organization (Xellerate Users), User Type (Full-Time Employee), and Display Name. The Account Settings section includes User Login (BetaSwan), Password, and Confirm Password. The Account Effective Dates section includes Start Date and End Date. The Provisioning Dates section includes Provisioning Date. The form has 'Submit', 'Save As...', and 'Cancel' buttons at the top right.

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

- Click the above created user.

Figure 4–4 Search and select the added User

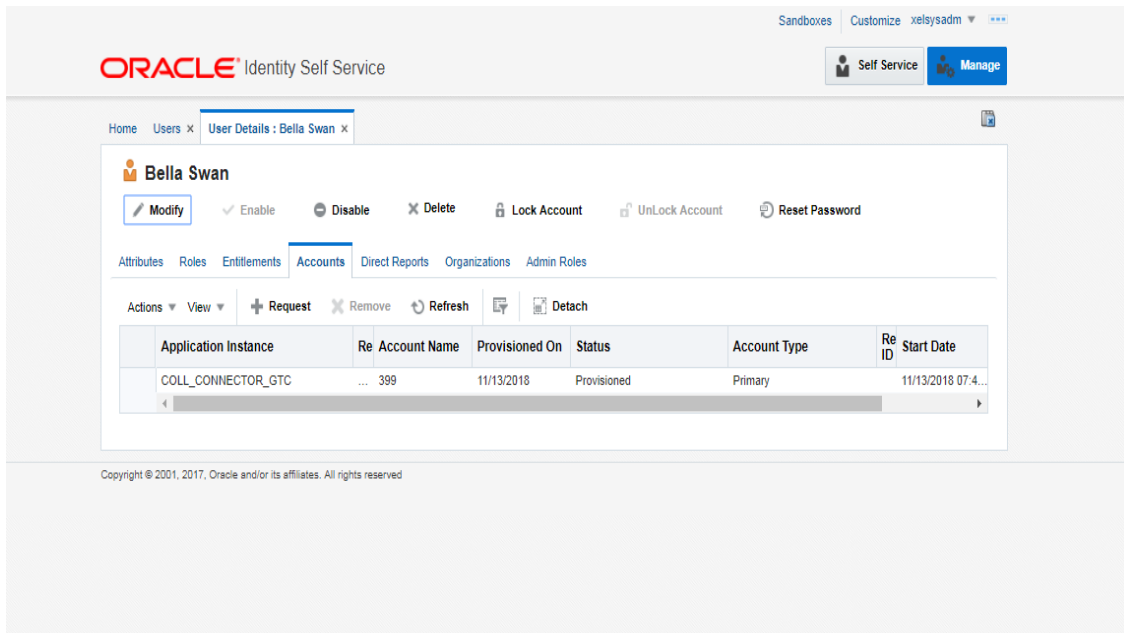
The screenshot displays the Oracle Identity Self Service interface for managing users. The main content area is a table listing various users. The user 'BELLASWAN' is selected, indicated by a blue highlight. The table columns include User Login, DN, First Name, Last Name, Organization, Telephone Number, E-mail, Identity Status, and Account Status. The user 'BELLASWAN' has a last name of 'Swan' and is currently active and unlocked.

User Login	DN	F Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account Status
12JUNE_PARTYID	...	12June_PartyId	Xellerate Users				Active	Unlocked
12JUNE_PARTYID_2	...	12June_PartyId_2	Xellerate Users				Active	Unlocked
17JUL_1_TIMEZONE	...	17Jul_1_timezone	Xellerate Users				Active	Unlocked
18MAY_1	...	18May_1	Xellerate Users				Active	Unlocked
21MAY_1	...	21May_1	Xellerate Users				Active	Unlocked
21MAY_TARGETUNIT1	...	21May_targetunit1	Xellerate Users				Active	Unlocked
21MAY_TARGETUNIT2	...	21May_target...	Xellerate Users				Active	Unlocked
21_MAY_CUSTOM1	...	21_May_Custom1	Xellerate Users				Active	Unlocked
22NDMAY_ACCESSIBLEBU	...	22ndMay_Acces...	Xellerate Users				Active	Unlocked
40CT2018_1	...	40c2018_1	Xellerate Users				Active	Unlocked
40CT2018_2@ORACLE.COM	...	40c2018_2	Xellerate Users				Active	Unlocked
6_OCT_2018_1@ORACLE.COM	...	6_Oct_2018_1	Xellerate Users				Active	Unlocked
8JAN@ORACLE.COM	...	8jan	Xellerate Users				Active	Unlocked
8OCT_2018	...	8oct_2018	Xellerate Users				Active	Unlocked
ACC_BU_TAR	...	Acc_Bu_TAR	Xellerate Users			Acc_Bu_TAR@...	Active	Unlocked
AMIT1.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT3.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT4.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT5.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT6.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT7.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
AMIT8.LNAME@ORACLE.COM	...	Ai Lname	Xellerate Users				Active	Unlocked
ANILK	...	anilk	Xellerate Users			anilk@oracle.com	Active	Unlocked
ANIL_NEW	...	anil_new	Xellerate Users				Active	Unlocked
BELLASWAN	...	B Swan	Xellerate Users				Active	Unlocked

Page 1 (125 items) | export (1).xml | Show all

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

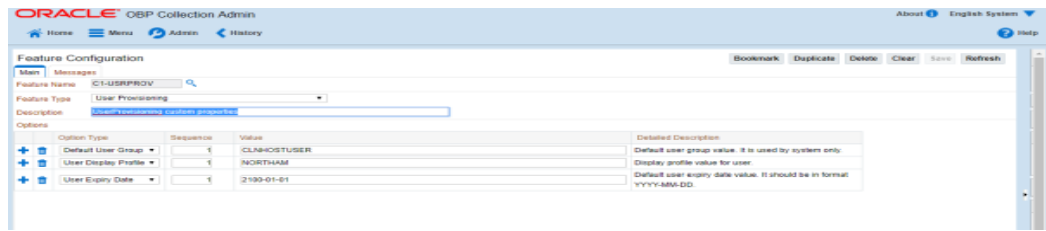
Collections Admin Application provides feature configuration C1-USRPROV to specify default values of the following:

- **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

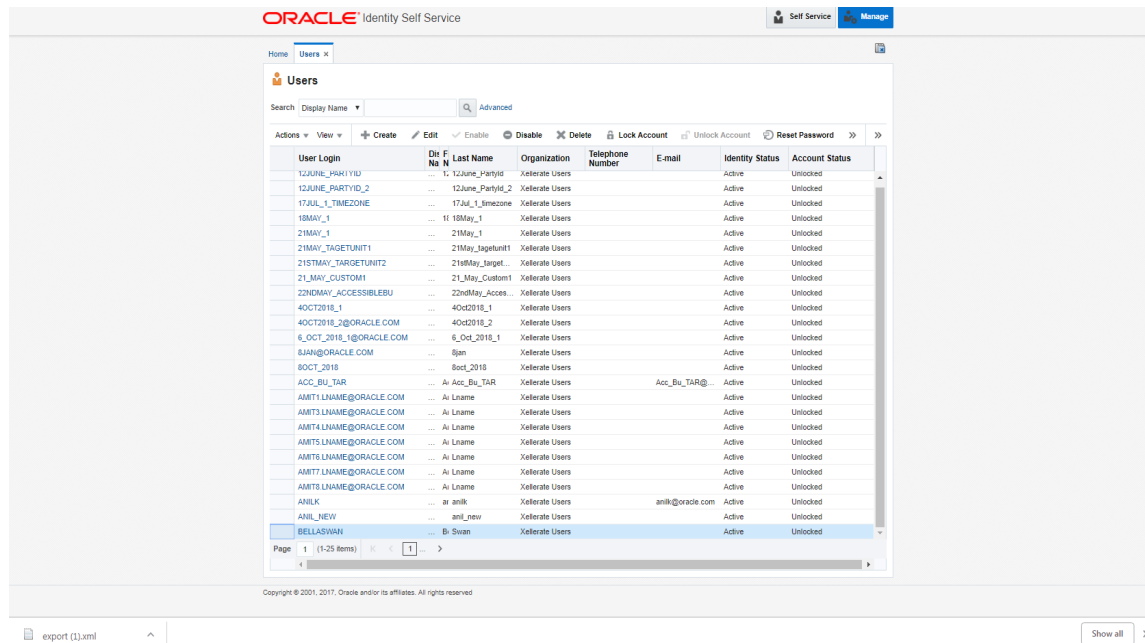


Figure 4–8 Detailed Information about the User

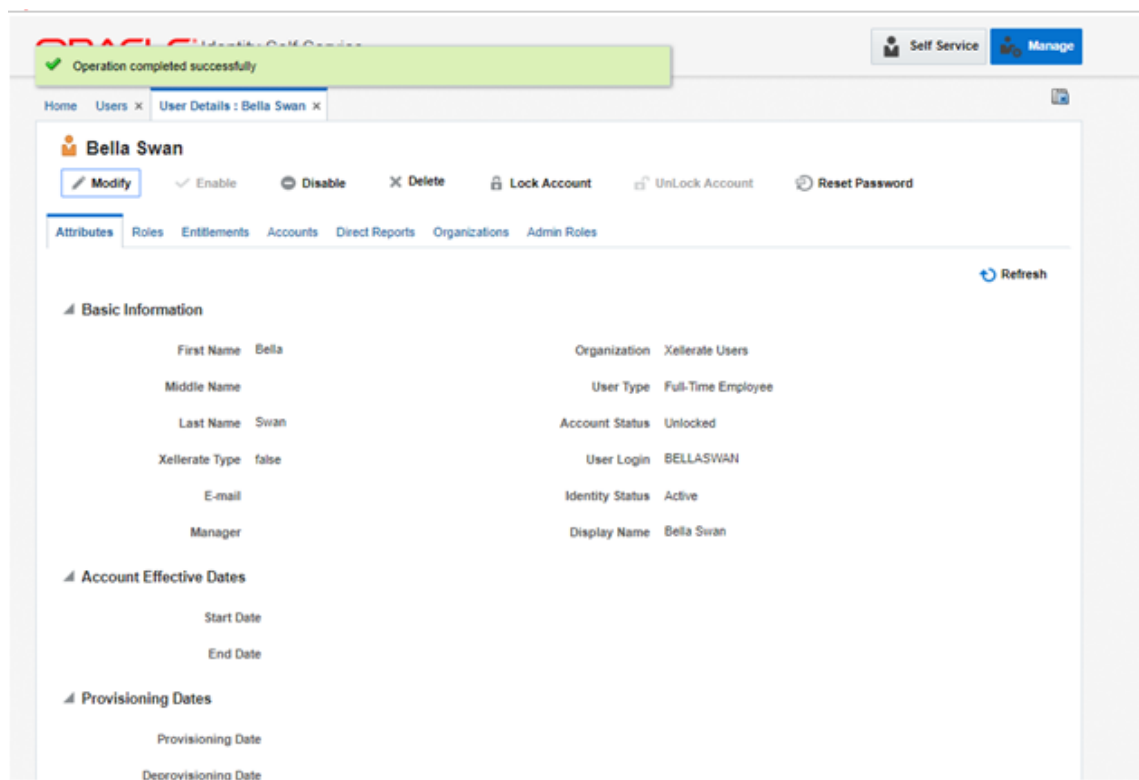
The screenshot displays the Oracle Identity Self Service interface for user management. The user profile for Bella Swan is shown with the following details:

Section	Attribute	Value
Basic Information	First Name	Bella
	Middle Name	
	Last Name	Swan
	Xellerate Type	false
	E-mail	
	Manager	
	Organization	Xellerate Users
	User Type	Full-Time Employee
Account Effective Dates	Start Date	
	End Date	
Provisioning Dates	Provisioning Date	
	Deprovisioning Date	
Contact Information	Telephone Number	
	Home Phone	
	Postal Address	
	PO Box	
	Account Status	Unlocked
	User Login	BELLASWAN
	Identity Status	Active
	Display Name	Bella Swan

To modify a user:

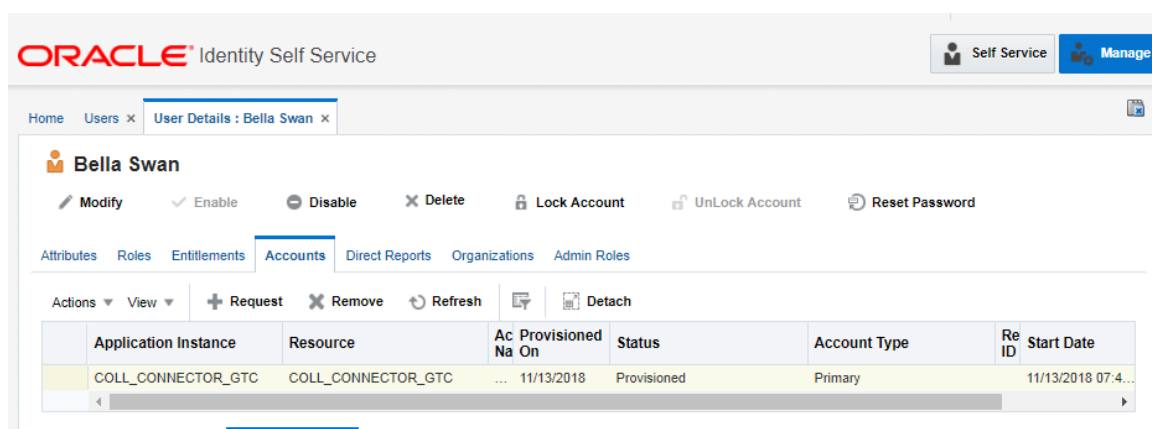
1. Click **Modify** to open Modify User page.
2. Modify the user details as per the requirement.
3. Click **Submit**. If the user details are valid (that is, if it does not violate any validation) then user details are modified. A message appears on successful completion of the modify operation. This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

Figure 4–9 Modify User Confirmation



- 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.
- If the data does not appear when the user is added, click **Refresh**.

Figure 4–10 Viewing Modified and Provisioned User Details



- 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

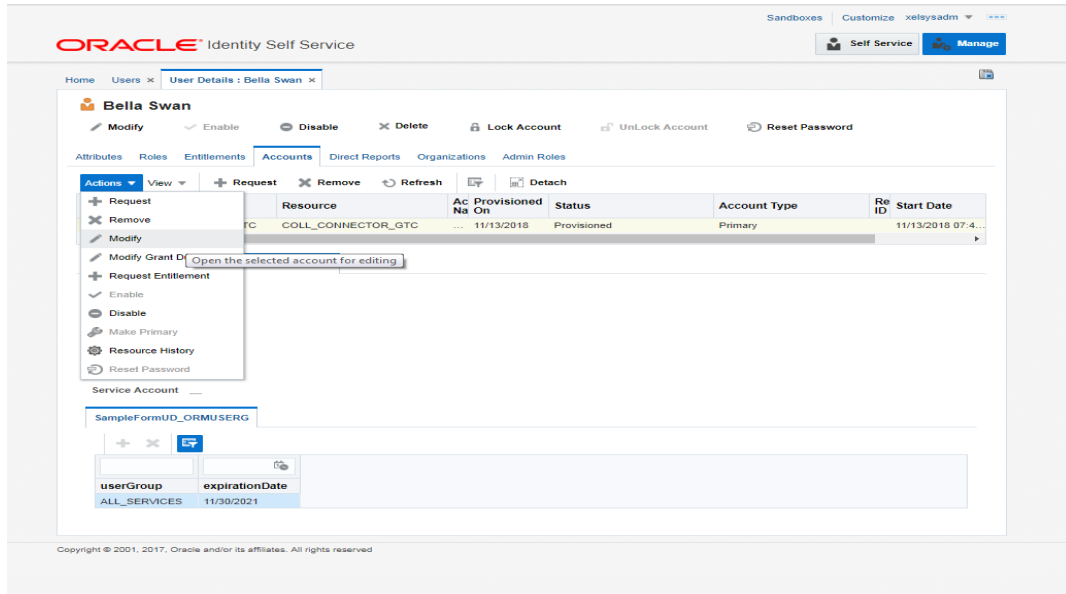
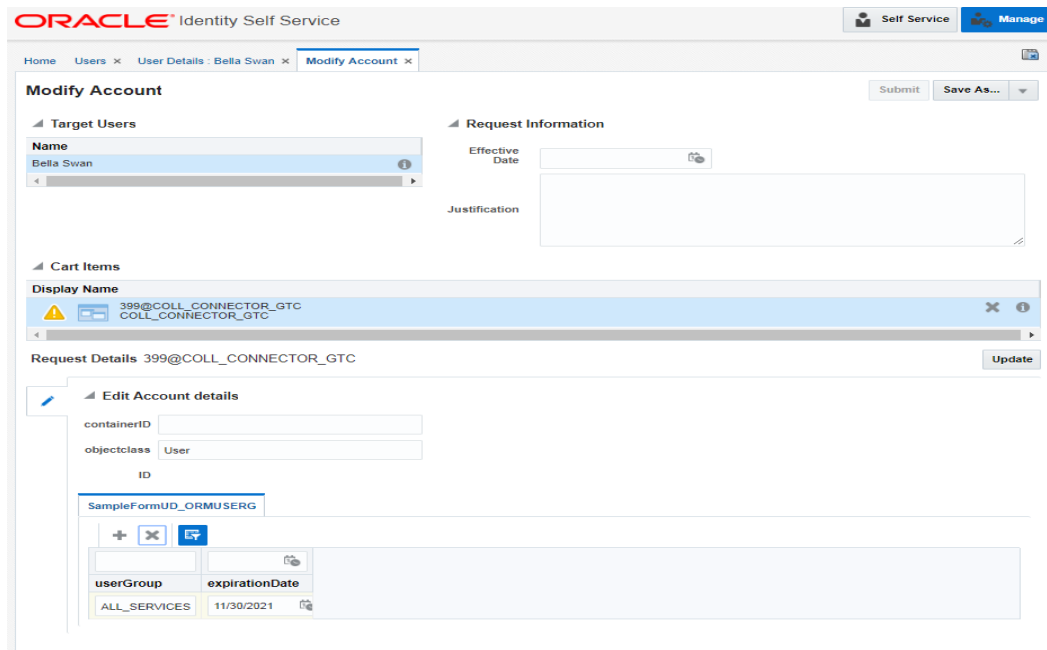


Figure 4–12 Edit Detail Information



- 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

The screenshot shows the Oracle Identity Self Service interface for user 'Bella Swan'. The 'Accounts' tab is selected, displaying a table of application instances. Below the table, the 'Detail Information' section is visible, showing details for the selected account 'SampleFormUD_ORMUSERG'.

Application Instance	Resource	Ac Na	Provisioned On	Status	Account Type	Re ID	Start Date
COLL_CONNECTOR_GTC	COLL_CONNECTOR_GTC	...	11/13/2018	Provisioned	Primary		11/13/2018 0

Below the table, the 'Detail Information' section shows the following details:

- containerID
- objectclass User
- ID
- Service Account —
- SampleFormUD_ORMUSERG

At the bottom, a table shows the user group and expiration date:

userGroup	expirationDate
ALL_SERVICES	11/28/2024

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.

5.4 Delete Users

Figure 4–14 Searching Users To Delete

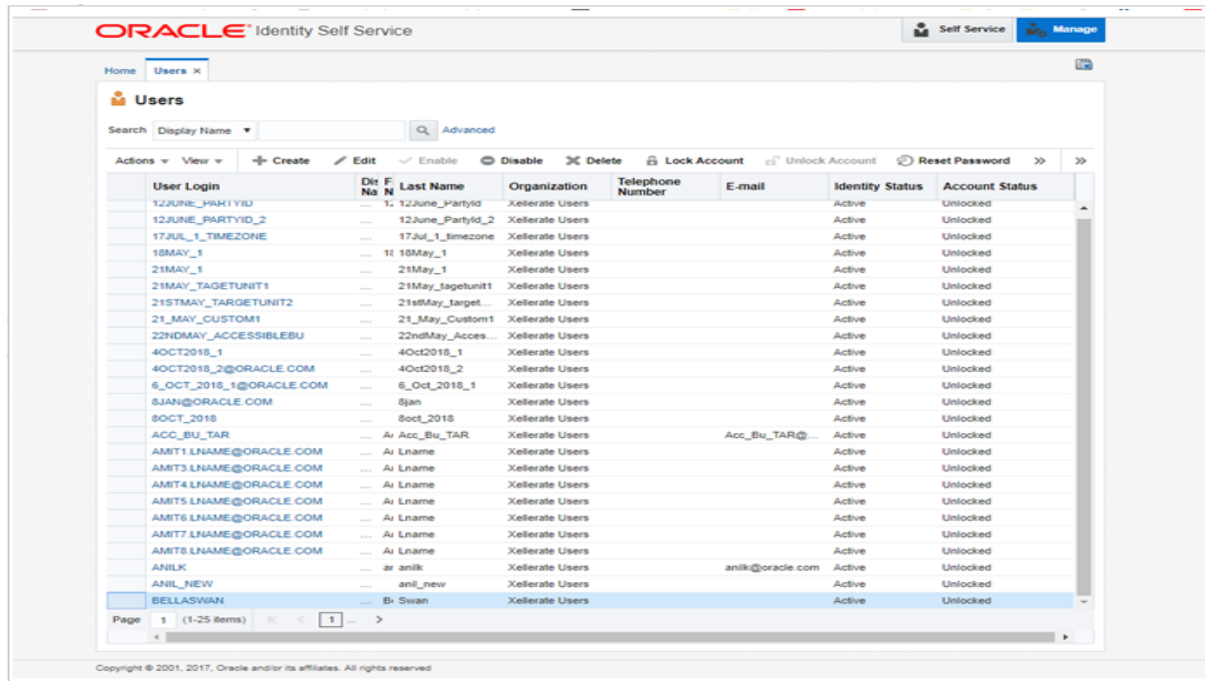
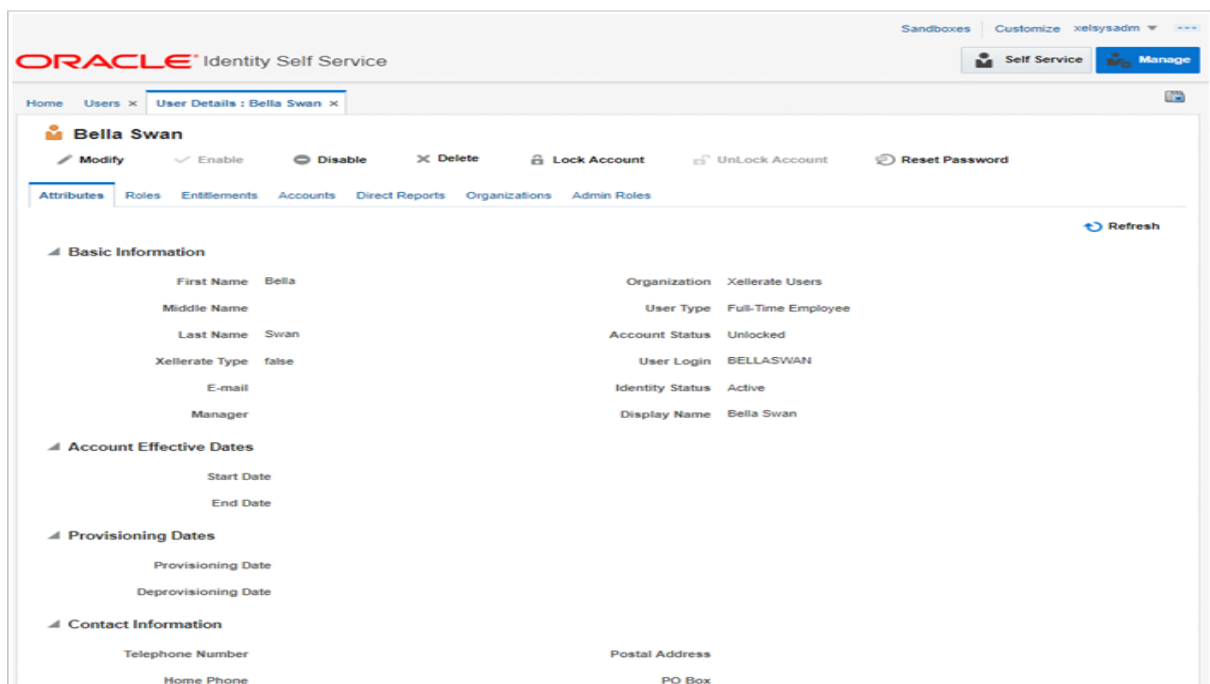


Figure 4–15 View User Details



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

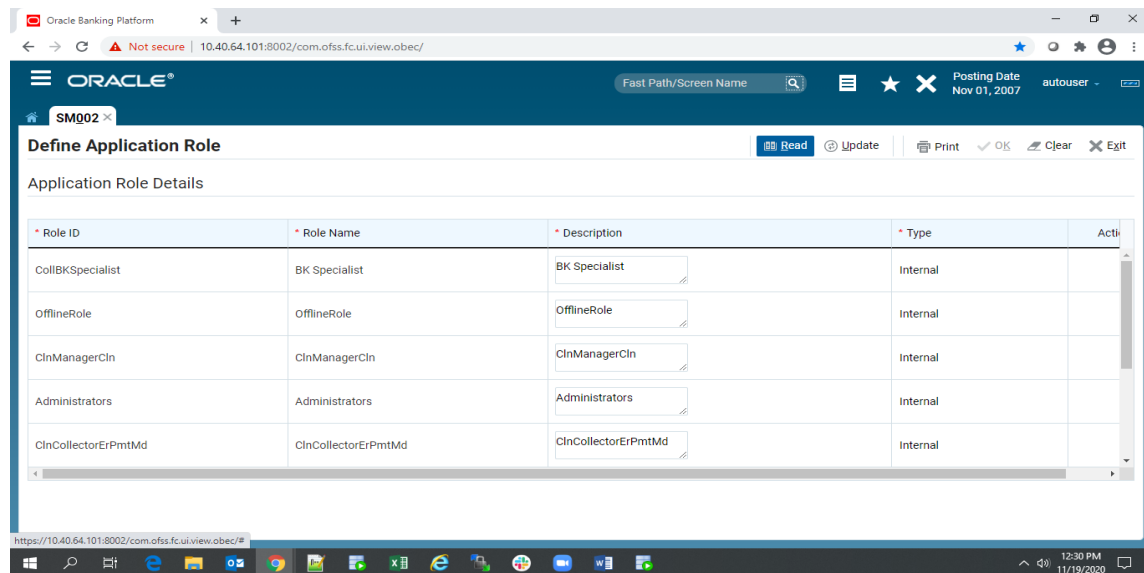
This chapter explains the process of creating and provisioning users using DB based configurations.

6.1 Create and Provision Users

To create users:

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

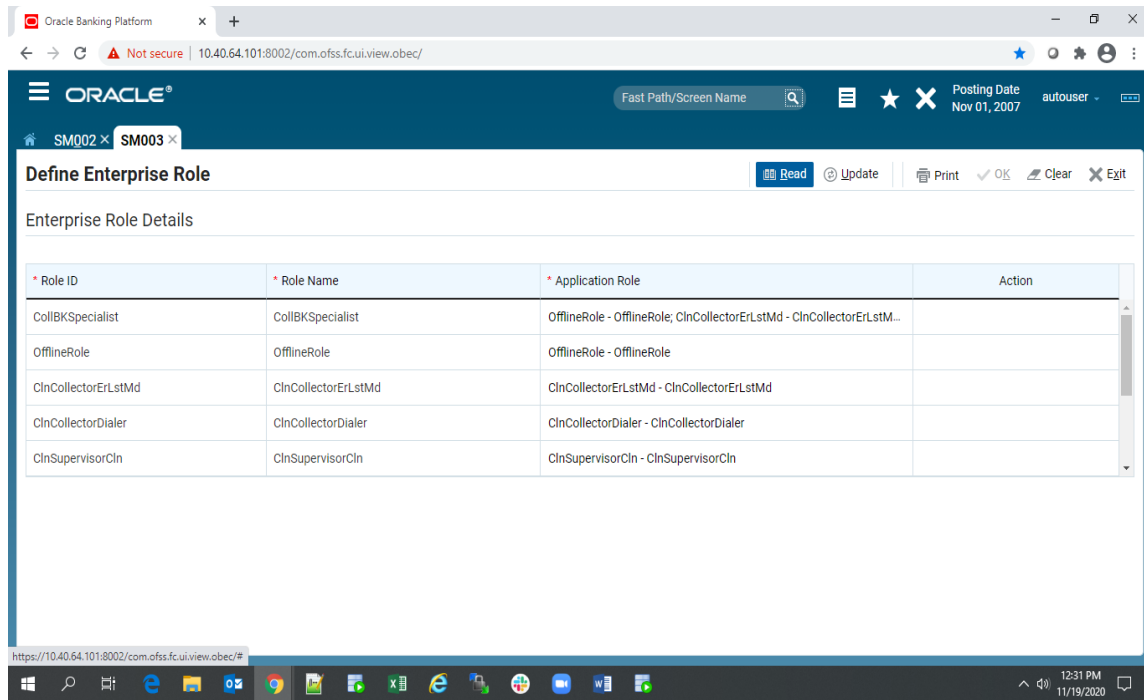
Figure 4–16 Define Application Role (Fast Path: SM002)



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.

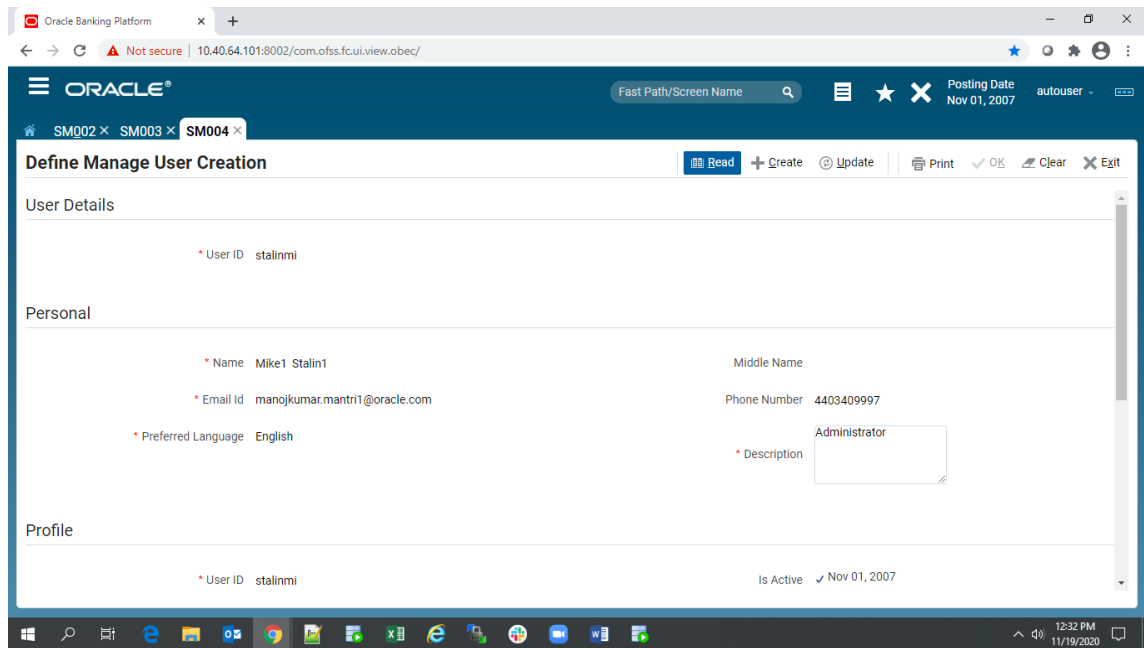
Figure 4–17 Define Enterprise Role (Fast Path: SM003)



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.

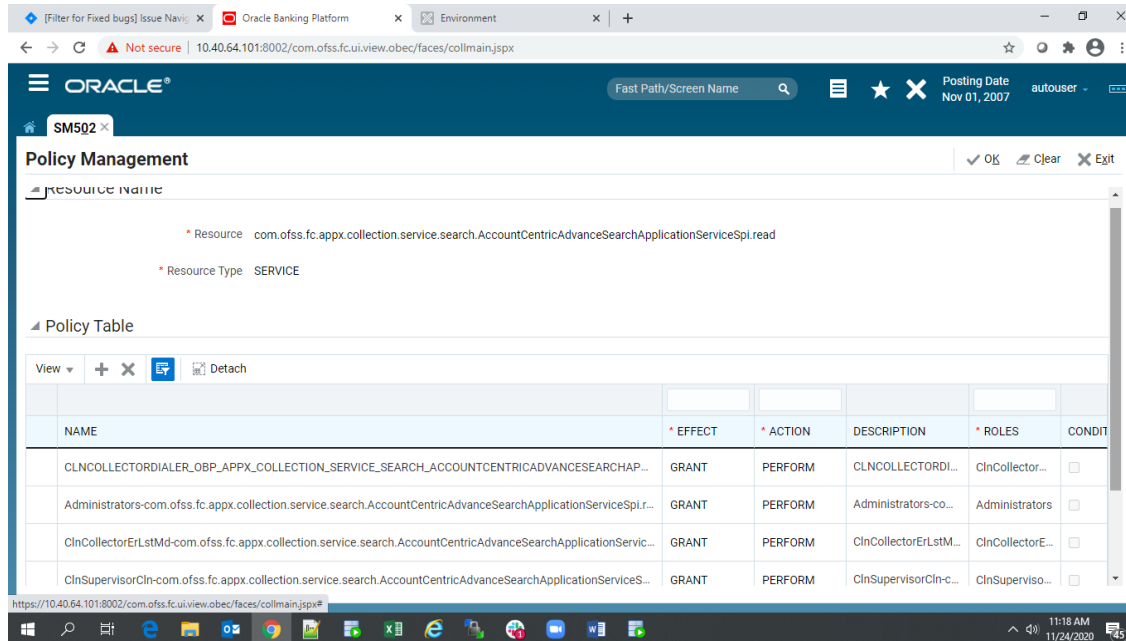
Figure 4–18 Manage User Creation (Fast Path: SM004)



Entries move in the FLX_SM_LOCAL_USERS and FLX_SM_LOCAL_USR_ENT_ROLES tables.

- 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

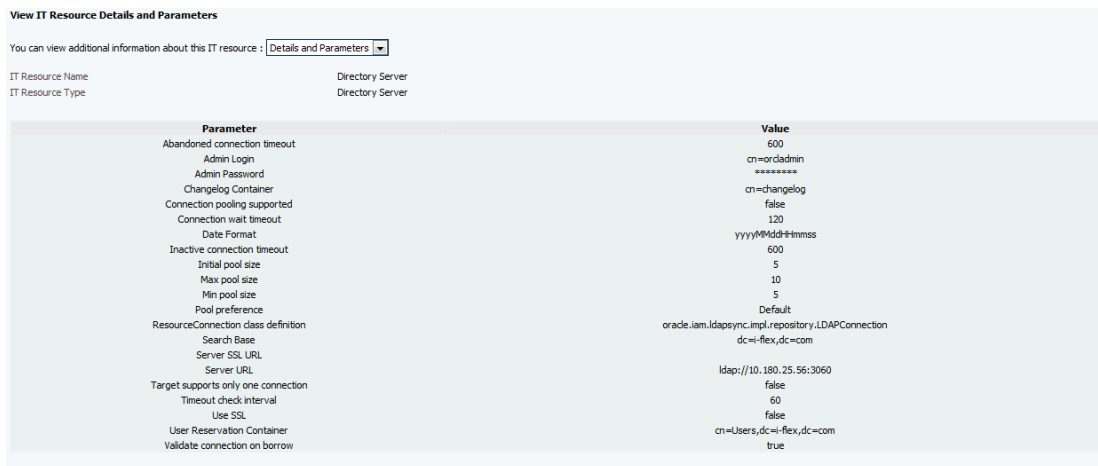
To verify OIM configuration, follow the steps:

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



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

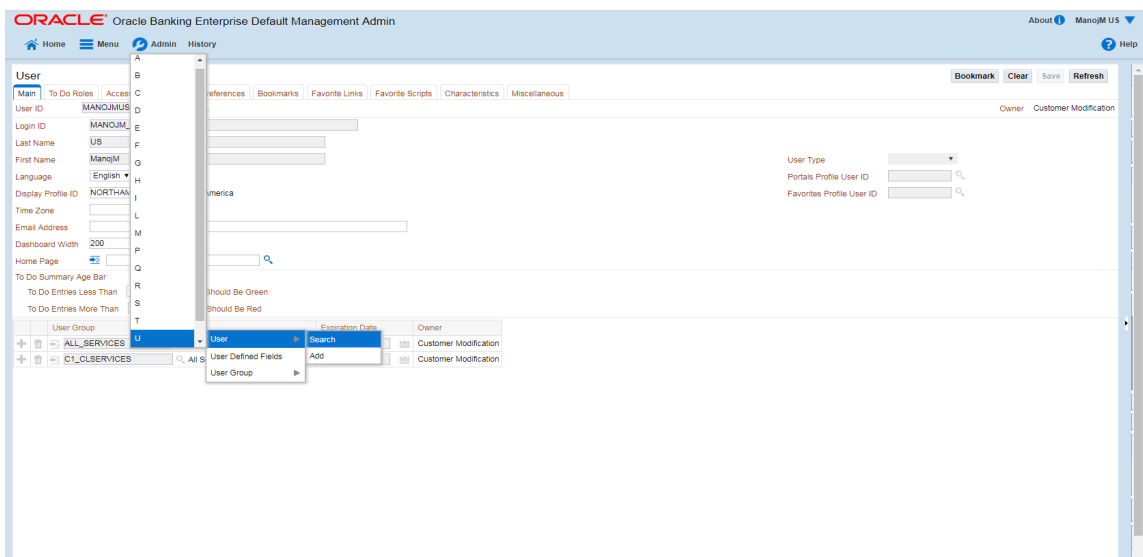


Figure 5–4 User Screen - Main Tab

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

The screenshot displays the Oracle Banking Enterprise Default Management Admin interface. The top navigation bar includes 'Home', 'Menu', 'Admin', and 'History'. The main content area is titled 'User' and shows search results for user ID 'BSWAN'. The user details include: Login ID 'BELLASWAN', Last Name 'Swan', First Name 'Bela', Language 'English', Display Profile ID 'NORTHAM', Time Zone, Email Address, Dashboard Width '200', and Home Page. A table below shows the user's group 'ALL_SERVICES', system user group, expiration date '11-30-2021', and owner 'Customer Modification'. The interface also features a 'To Do Summary Age Bar' with filters for 'Days Old Should Be Green' (100) and 'Days Old Should Be Red' (300).

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

The screenshot shows the Oracle Banking Enterprise Default Management Admin login screen. It features a large blue header with the 'ORACLE' logo. Below the header, there are two input fields for 'User ID' and 'Password', followed by a 'Login' button. At the bottom, there is a 'Language' dropdown menu set to 'English'. The footer contains the Oracle logo and copyright information: 'Oracle Banking Enterprise Default Management Admin V2.7.0.0.0 Copyright © 2000, 2015 Oracle. All rights reserved. The program (which includes both the software and documentation) contain proprietary information they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.'

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

Figure 5–8 User Navigation

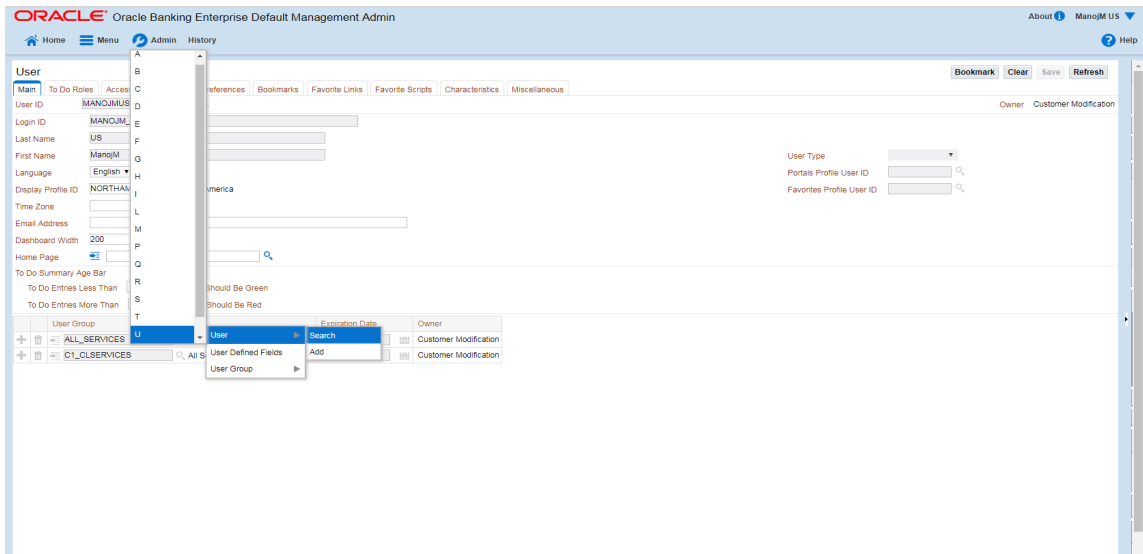
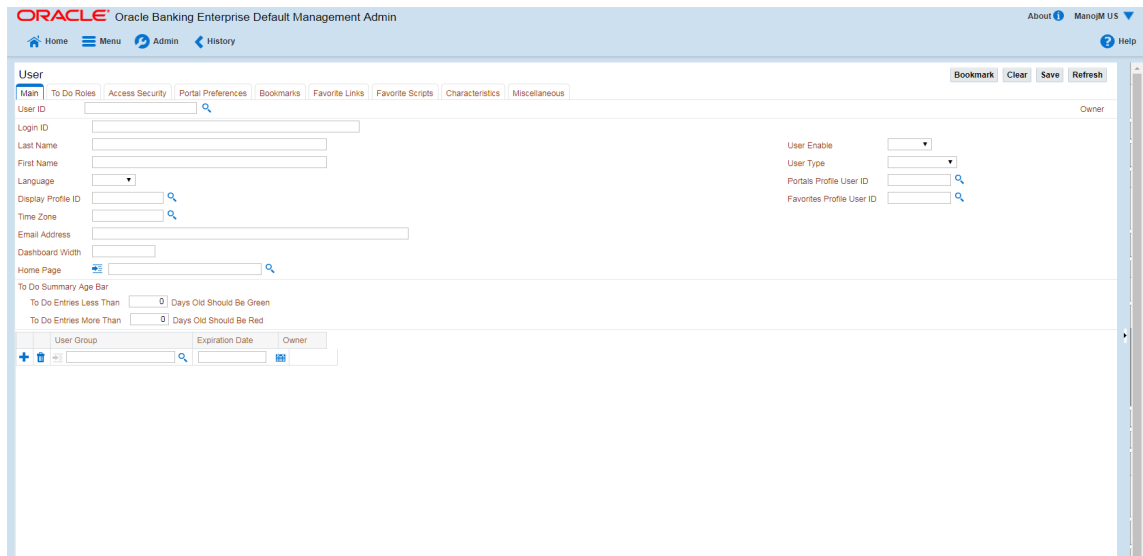


Figure 5–9 User Screen - Main Tab



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_ombhTabMenu
 - **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

The screenshot shows the Oracle Banking Enterprise Default Management Admin interface for creating a user. The user ID is 'OFSSUSER'. The configuration includes:

- Login ID:** OFSSUSER
- Last Name:** Ofssuser
- First Name:** Ofssuser
- Language:** English
- Display Profile ID:** NORTHAM (North America)
- Time Zone:** (empty)
- Email Address:** (empty)
- Dashboard Width:** 200
- Home Page:** (empty)
- To Do Summary Age Bar:**
 - To Do Entries Less Than: 50 Days Old Should Be Green
 - To Do Entries More Than: 100 Days Old Should Be Red
- User Group:** CLNHOSTUSER (All Services/C1- Collection Admin)
- Expiration Date:** 01-01-2100
- User Enable:** Enable
- User Type:** (empty)
- Portals Profile User ID:** (empty)
- Favorites Profile User ID:** (empty)

User Group	Expiration Date	Owner
ALL_SERVICES System User Group	01-01-2100	Customer Modification
C1_CLSERVICES All Services/C1- Collection Admin	01-01-2100	Customer Modification

5. OIMOBPCOLL User is successfully created.