Oracle® Banking Platform Collections and Recovery

User Provisioning Guide

Release 2.12.0.0.0

F43567-01

June 2021

ORACLE®

Oracle Banking Platform Collections and Recovery User Provisioning Guide, Release 2.12.0.0.0

F43567-01

Copyright © 2011, 2021, 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
4 User Fields and Constraints **51**

4.1 User Fields Provisioned From OIM 51
5 Create, Modify, Delete Users using OIM 53
5.1 Create and Provision Users 53
5.2 Feature Configurations 56
5.3 Modify Users 57
5.4 Delete Users 61
6 Verification 63
6.1 Verification of OIM Configuration 63
6.2 Verify Users in Native Collections Admin Application 64
6.3 Create Users in Collections Admin Application 66

List of Tables

Table 3–1 Oracle Banking Collections and Oracle Banking 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 51

Table 5–1 OID schema attributes 63

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 4–1 Create User - Mandatory and Optional Attributes 52
Figure 4–2 Create User in Oracle Identity Self Service 53
Figure 4–3 Input User Attributes 54
Figure 4–4 Search and select the added User 55
Figure 4–5 Applications provisioned to User 56
Figure 4–6 Feature Configuration 57
Figure 4–7 Searching User 57
Figure 4–8 Detailed Information about the User 58
Figure 4–9 Modify User Confirmation 59
Figure 4–10 Viewing Modified and Provisioned User Details 59
Figure 4–11 Modify Detail Information 60
Figure 4–12 Edit Detail Information 60
Figure 4–13 Viewing Changes 61
Figure 4–14 Searching Users To Delete 62
Figure 4–15 View User Details 62
Figure 5–1 Viewing IT Resource Details and Parameters 63
Figure 5–2 Login screen 64
Figure 5–3 User Screen - User Navigation 64
Figure 5–4 User Screen - Main Tab 65
Figure 5–5 Searching Particular User 65
Figure 5–6 Search Result in User screen 66
Figure 5–7 Login screen 66
Figure 5–8 User Navigation 67
Figure 5–9 User Screen - Main Tab 67

Figure 5–10 User Screen 68

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/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=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 1 Create, Modify, Delete Users (DB Based)

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

Chapter 6 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 Platform Collections and Recovery 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 centralized repository, Oracle Internet Directory (OID). This repository is used for authentication and authorization purpose.

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

Users are provisioned in Oracle Banking Collections and Oracle Banking 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 6.1 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 Collections and Oracle Banking Recovery release bundle:
   - collections_oim_export.xml

3.2 Create System User

The following configuration is to create Oracle Banking Collections and Oracle Banking Recovery System User for OIM. System User is required to authenticate OIM Oracle Banking Collections and Oracle Banking 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 Collections and Oracle Banking 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 6.3 Create Users in Collections Admin Application

3.3 OIM Configuration

This section provides information on OIM Configuration.

3.3.1 Import Configuration

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

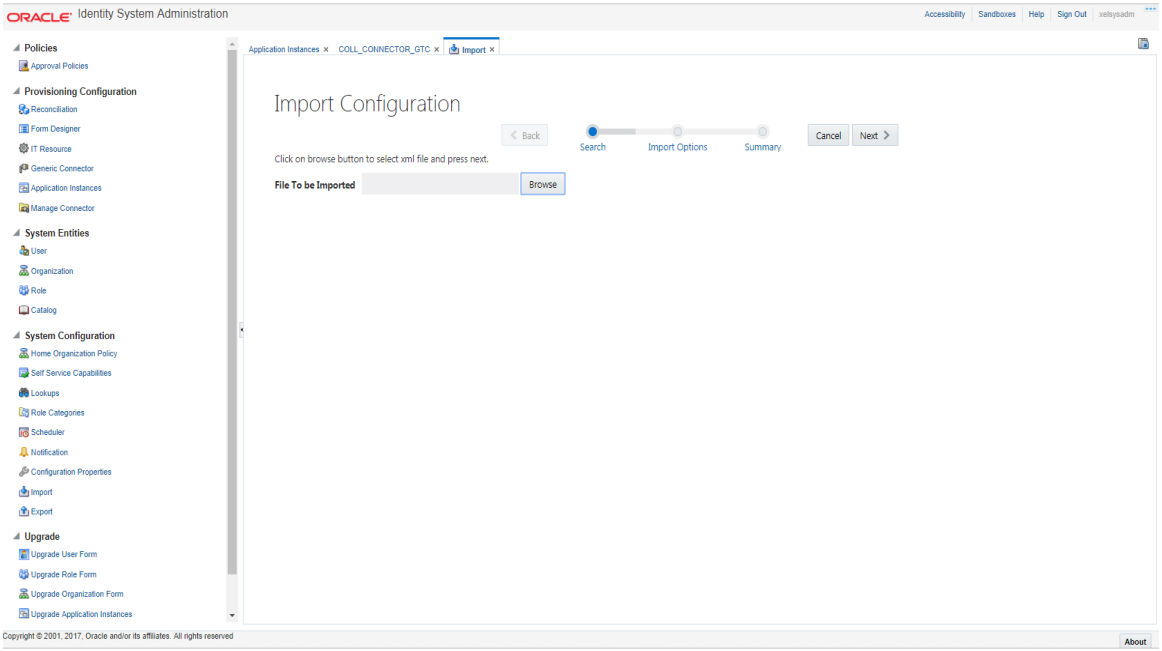
Table 3–1 Oracle Banking Collections and Oracle Banking Recovery User Provisioning Artifacts

Artifact	Artifact Type	Description
COLL_CONNECTTOR_GTC	IT Resource Definition	It stores definition of connection parameters to connect Oracle Banking Collections and Oracle Banking 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 Collections and Oracle Banking 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

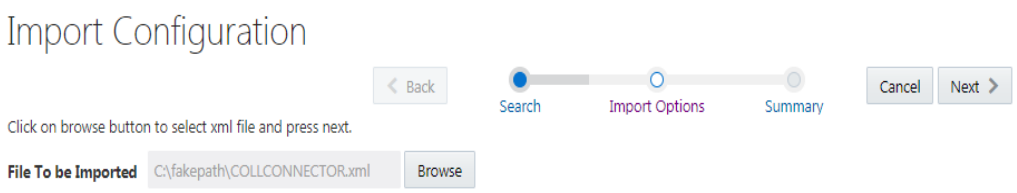
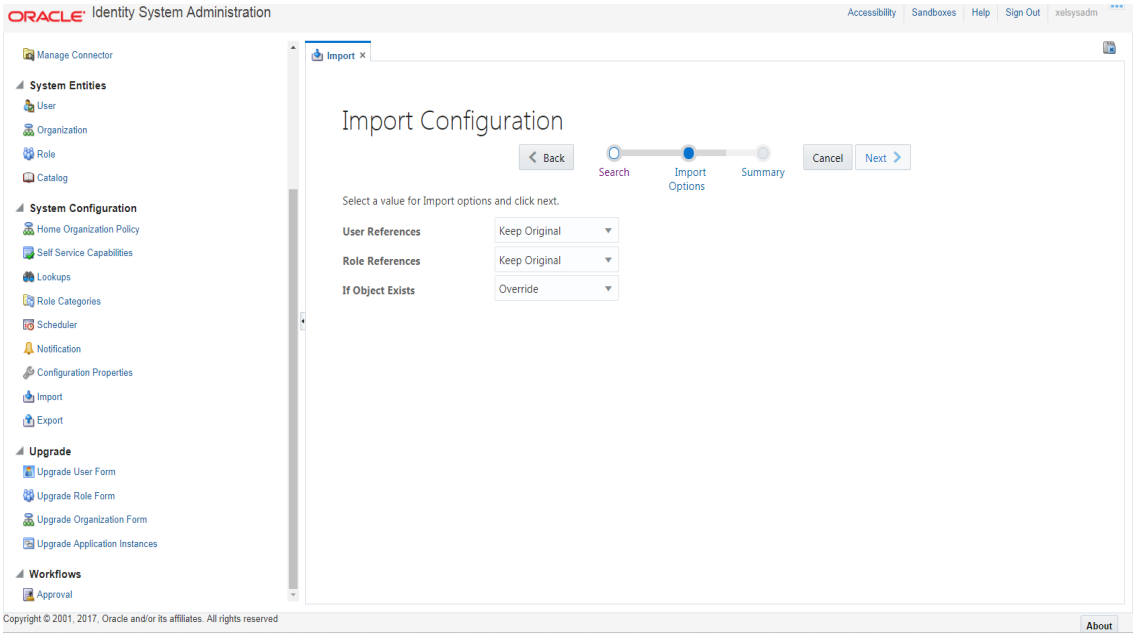
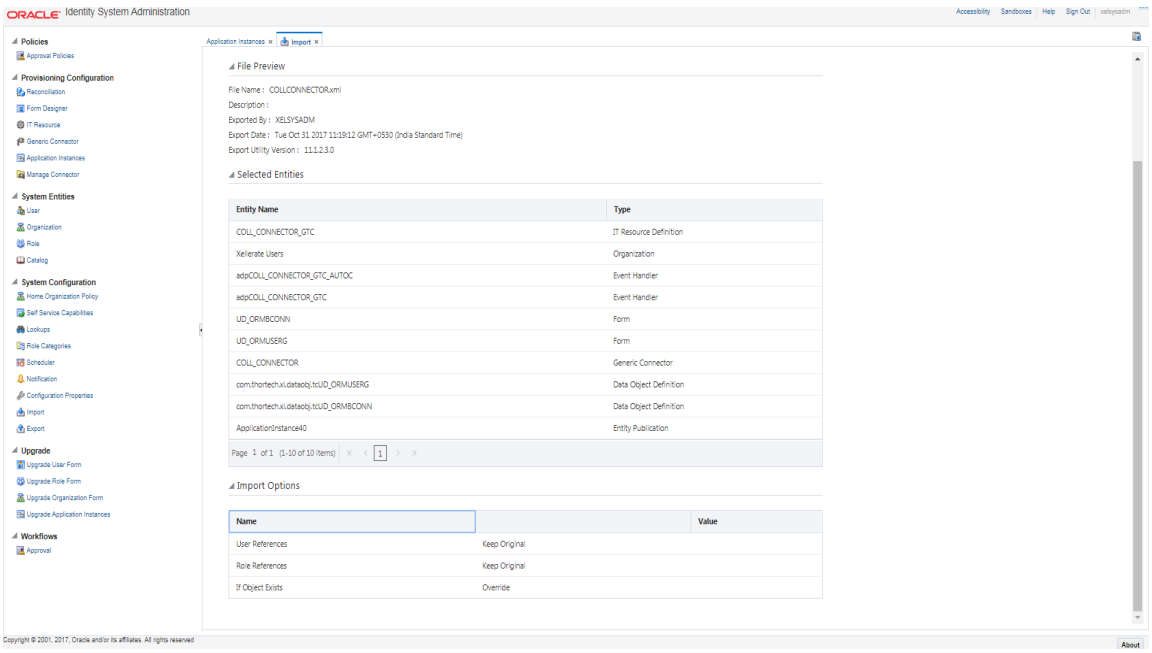


Figure 3–3 Import Options



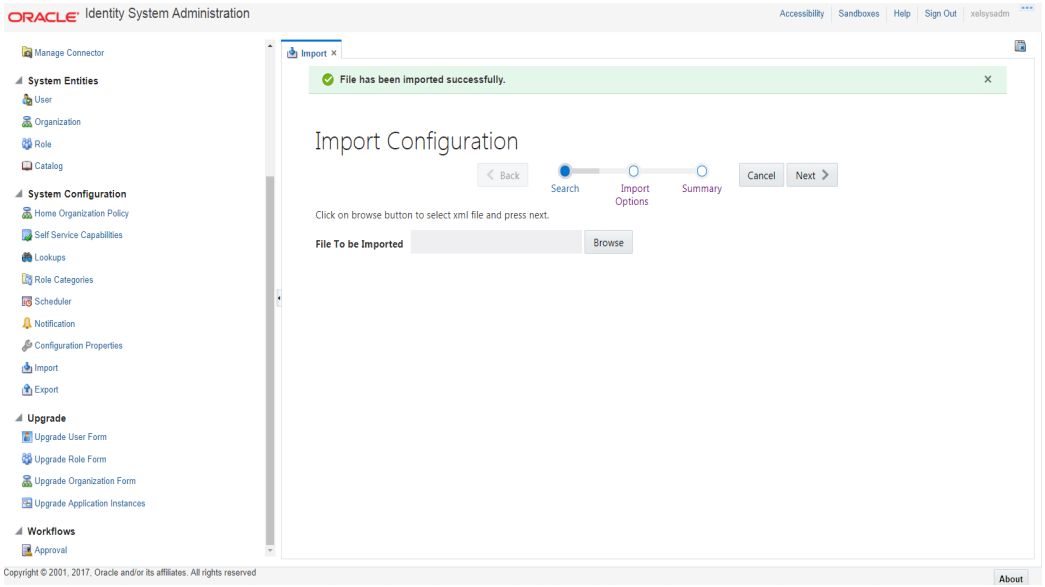
4. Click **Next**.

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

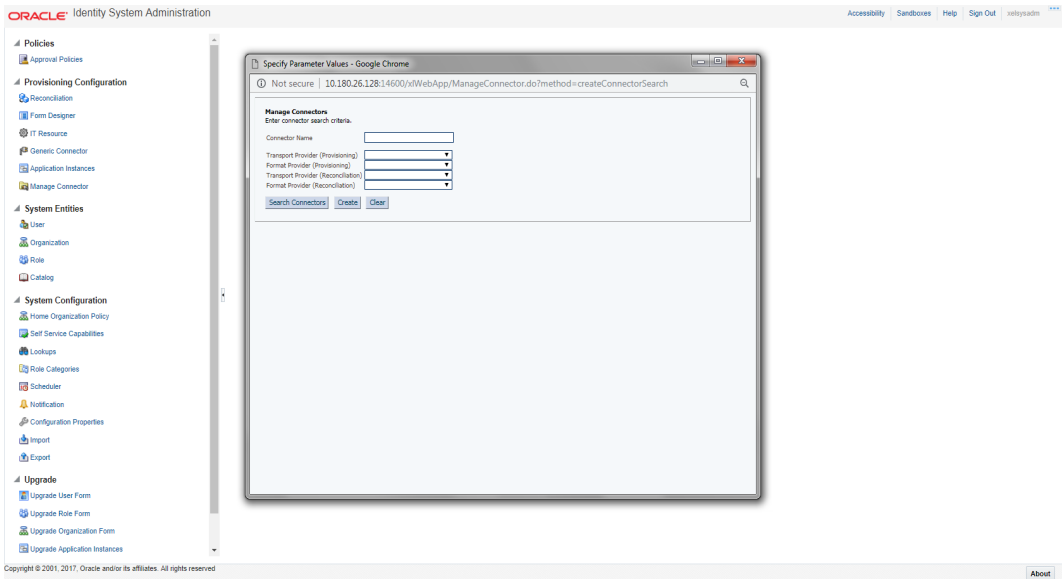


3.3.2 Manage Generic Technology Connector

Following Run-Time Parameters need to be set.

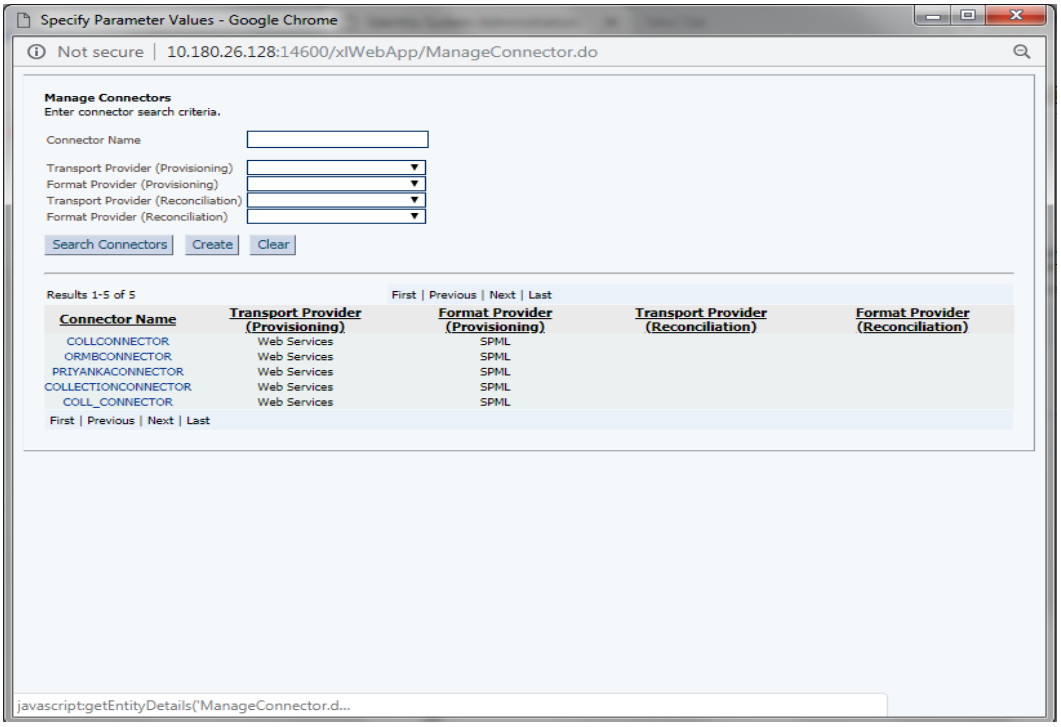
1. In the left pane, click **Generic Connector**. Following window appears.

Figure 3–6 Generic Connector



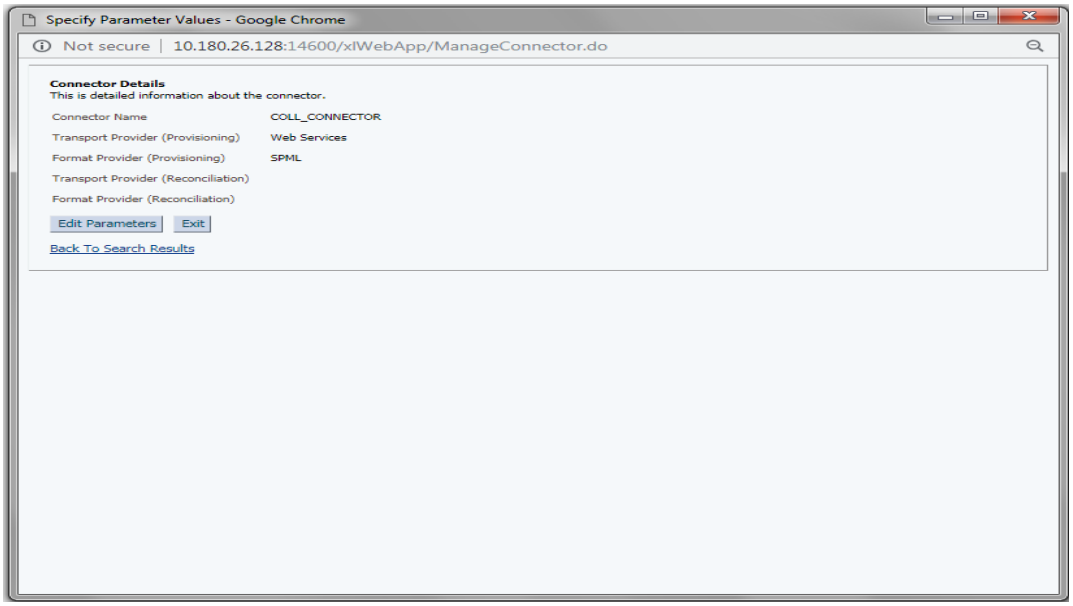
2. Click **Search Connectors** and click **COLL_CONNECTOR**.

Figure 3–7 Search Connectors



3. Click **Edit Parameters**.

Figure 3–8 Edit Connector Parameters

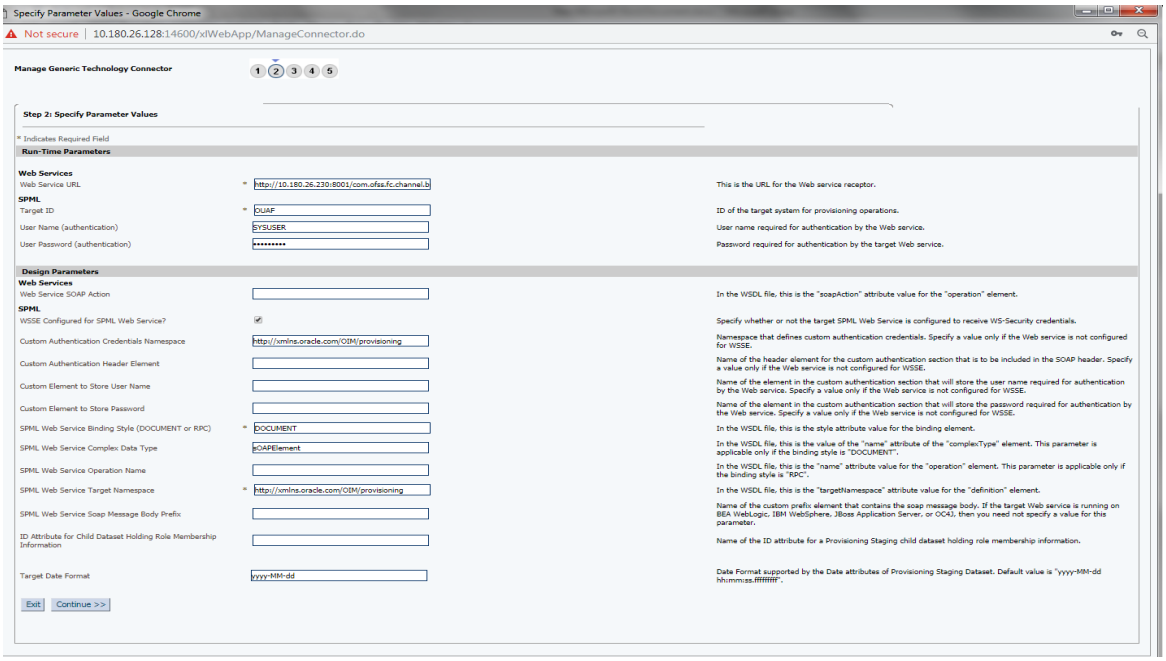


4. Specify parameter values as shown below:

Table 3–2 Run Time Connector Parameters

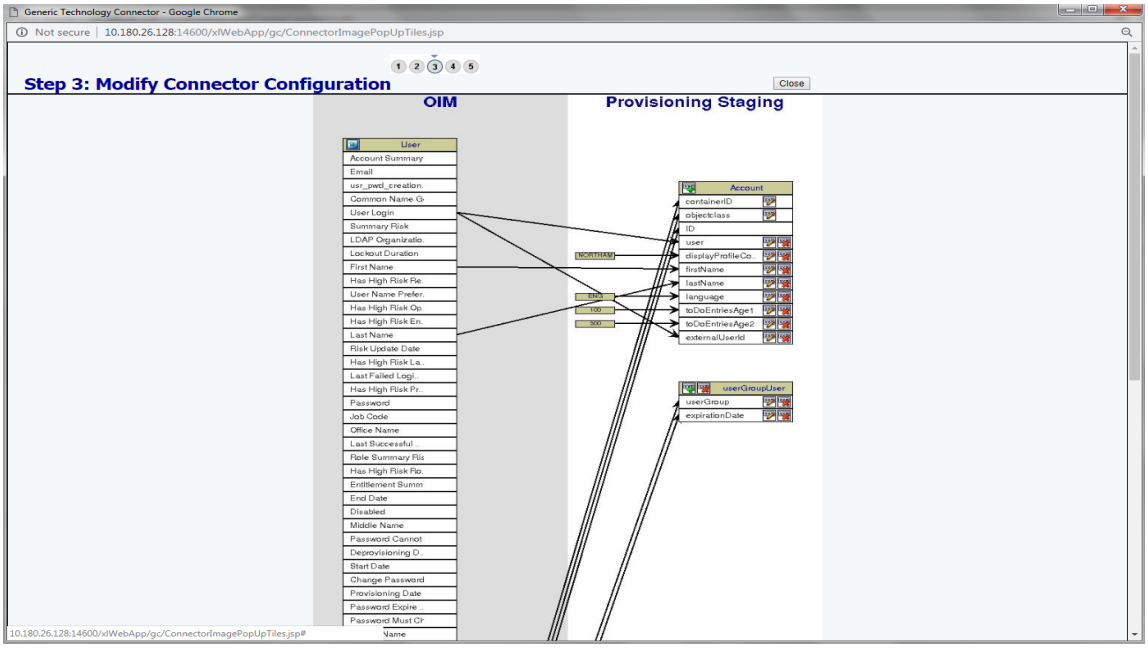
Parameter Name	Parameter Value	Description
Web Services		
Web Service URL	http://<Host>:<Port>/com.ofss.fc.channel.branch/spml2	This is the URL for the Web service receptor.
SPML		
Target ID	OUAF	ID of the target system for provisioning operations.
User Name (authentication)	SYSUSER	User name required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



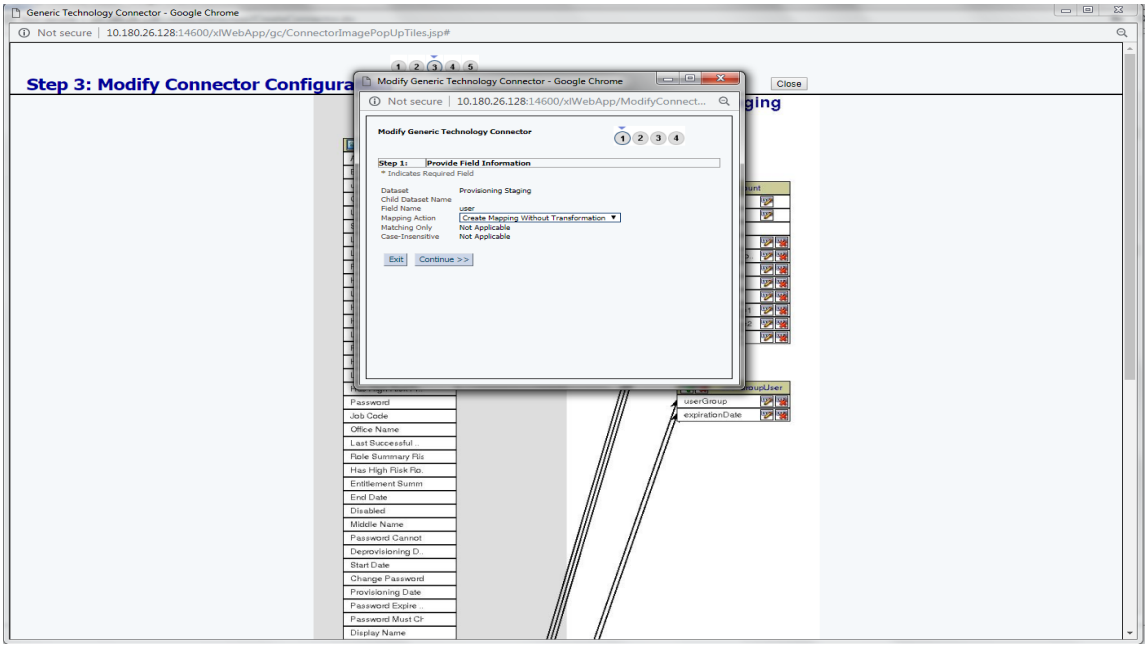
5. Click **Continue**. Modify Connector configuration screen appears.

Figure 3–10 Modify Connector Configuration (Mapping Information)



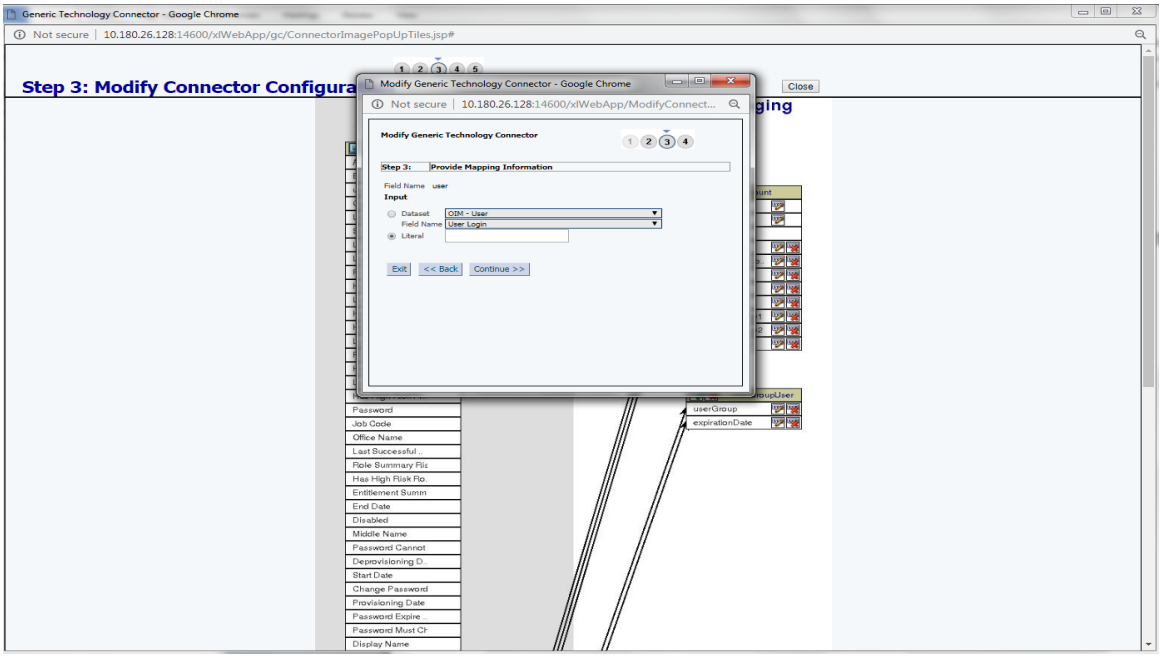
6. Click the **Edit** icon for User field name in the provisioning staging column.

Figure 3–11 Edit Mapping Information



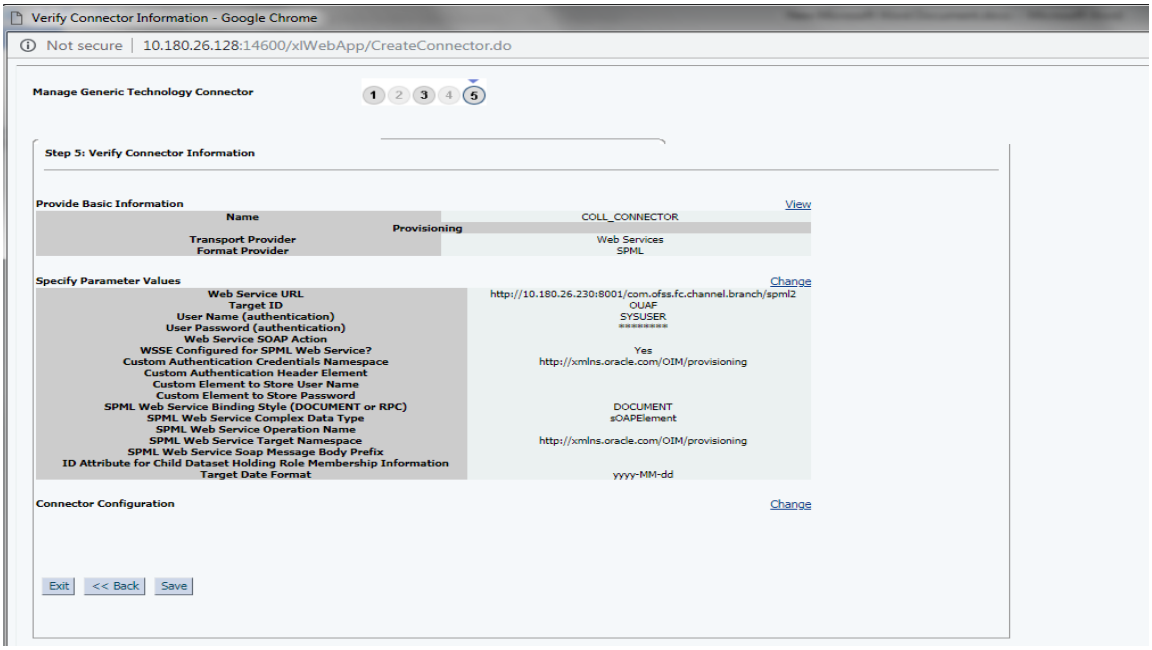
7. Click **Continue** to provide mapping information for the User field name. Select the **Literal** radio button and keep the input blank.

Figure 3–12 Provide Mapping Information



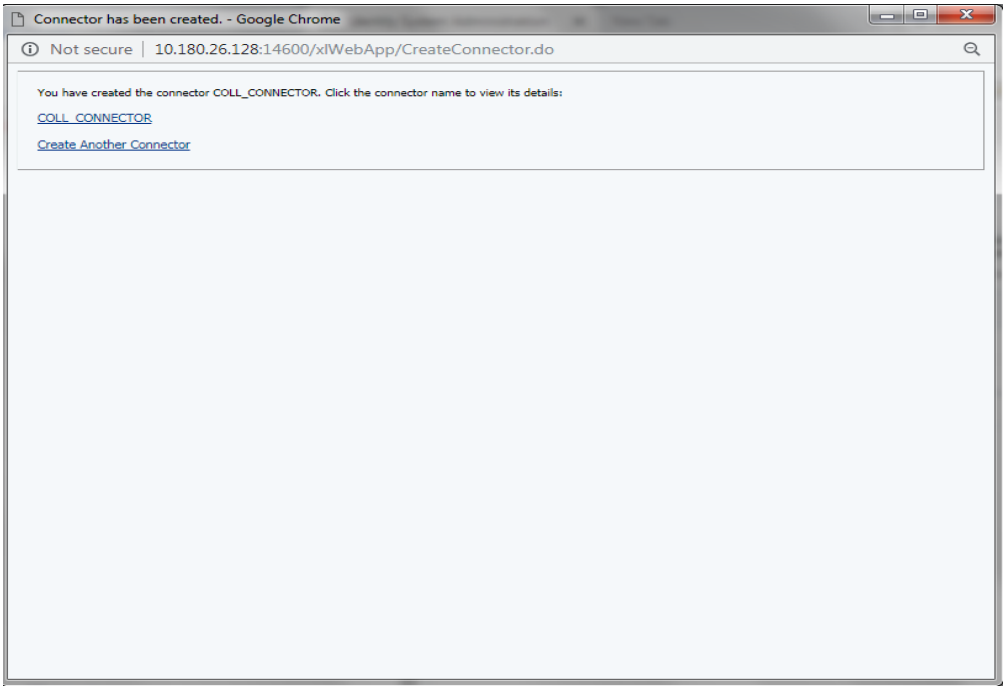
8. Click **Continue** and then **Close**. Following window appears where Connector Information can be verified.

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

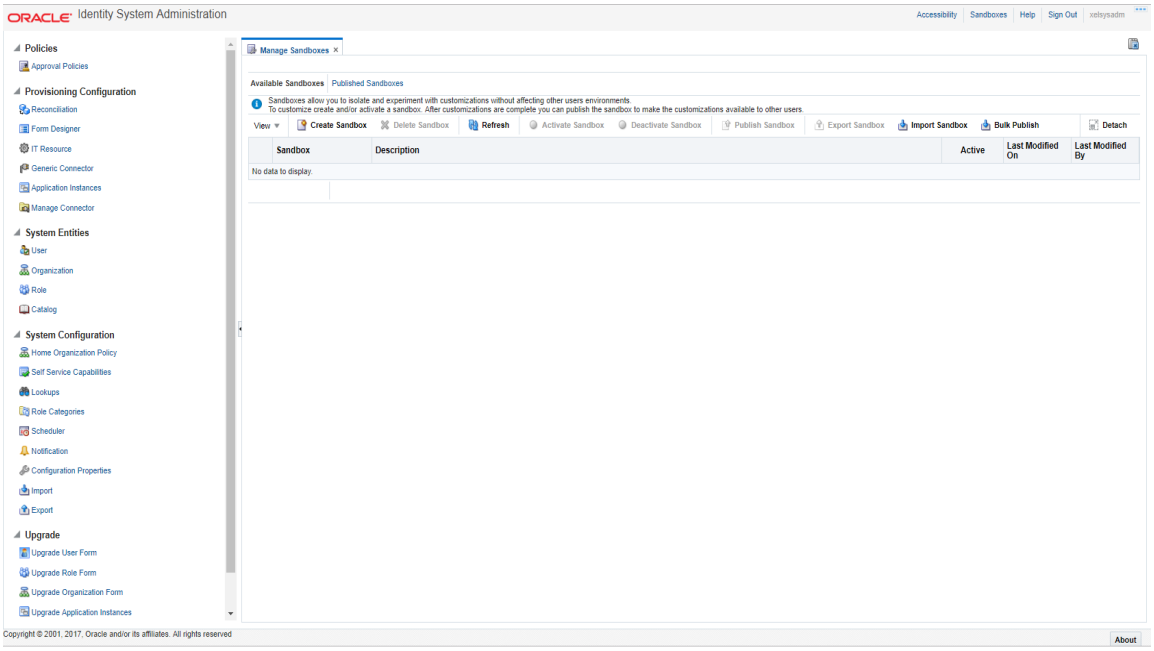


3.3.3 Create and Activate Sandbox

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

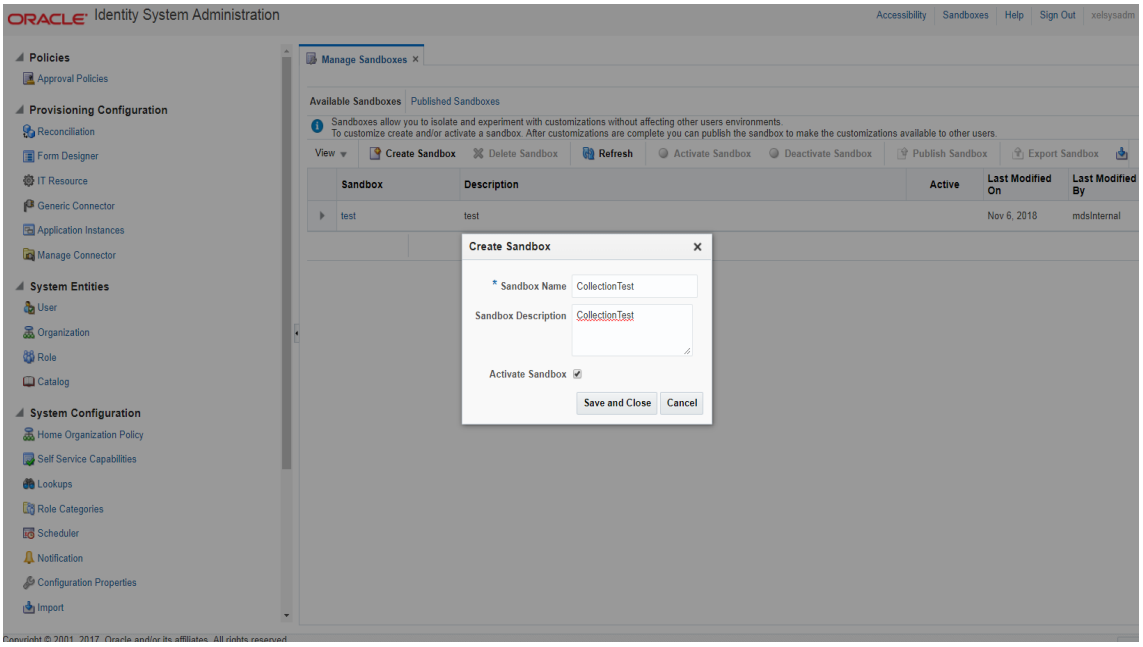


3.3.3.1 Create Sandbox

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



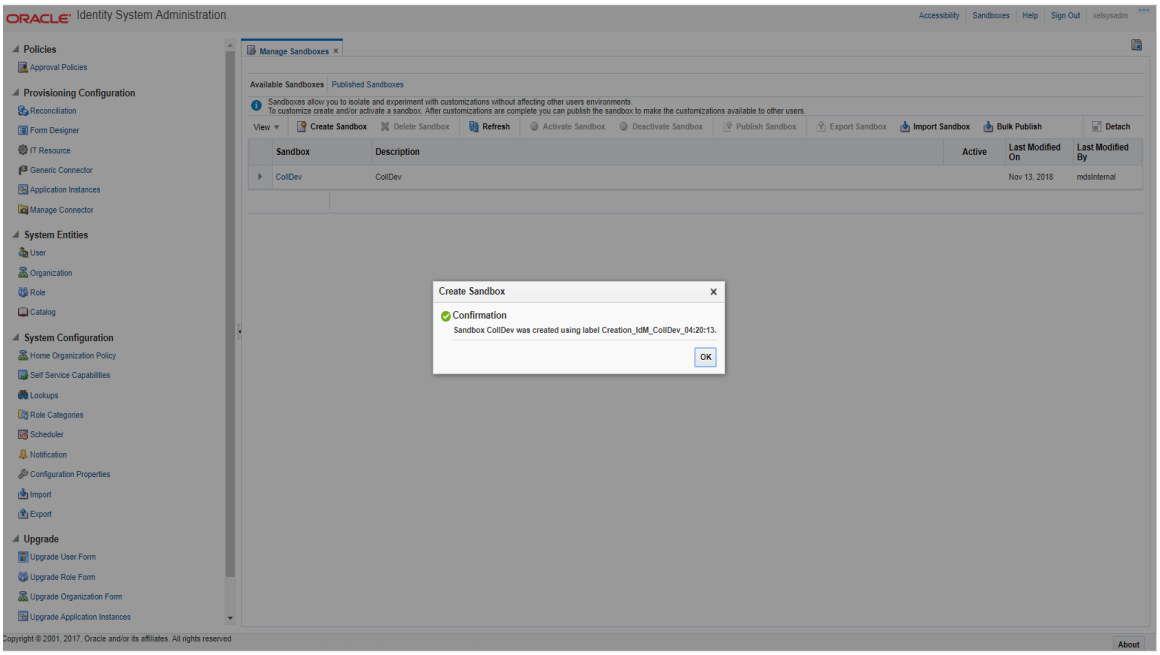
2. Specify the following values:

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.

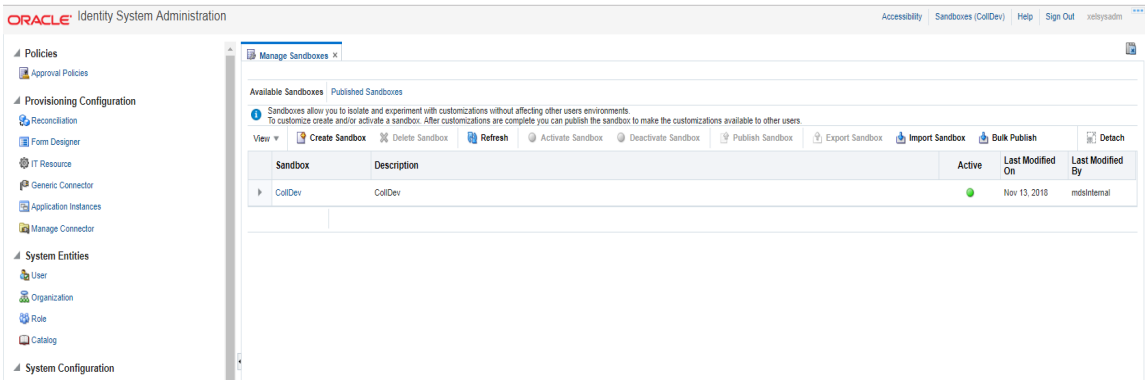
Figure 3–17 Sandbox Creation Confirmation



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

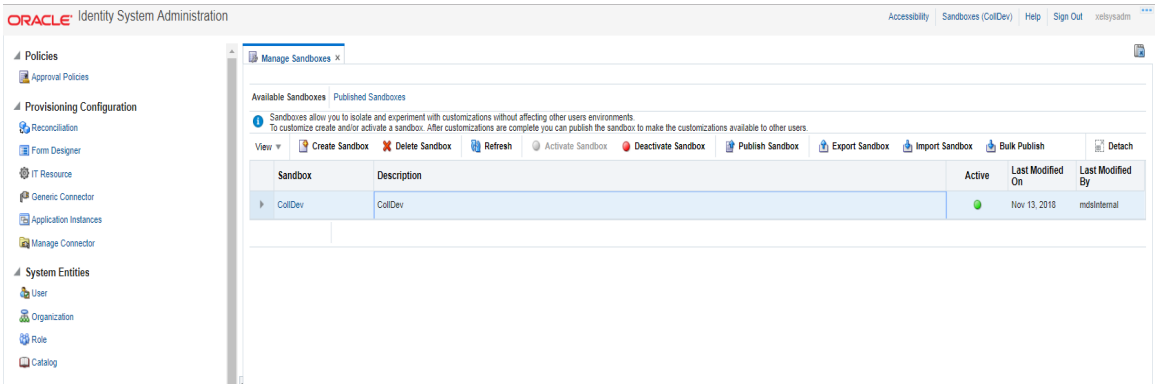


3.3.3.2 Activate Sandbox

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



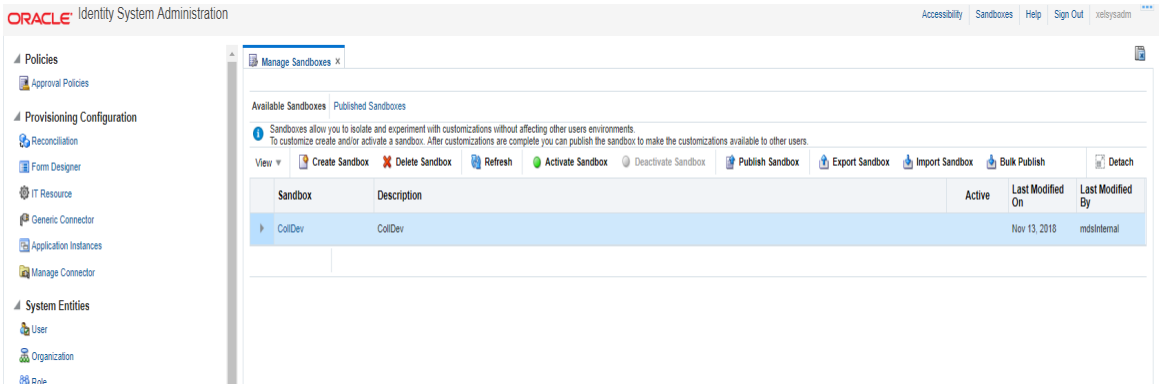
2. Sandbox is active now. It will be highlighted with green dot.

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

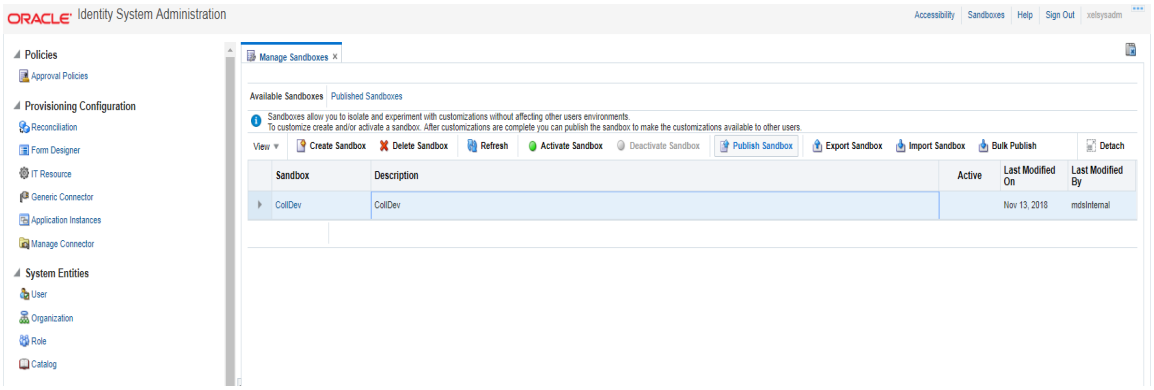


3.3.3.4 Publish Sandbox

To publish a Sandbox, perform the following steps:

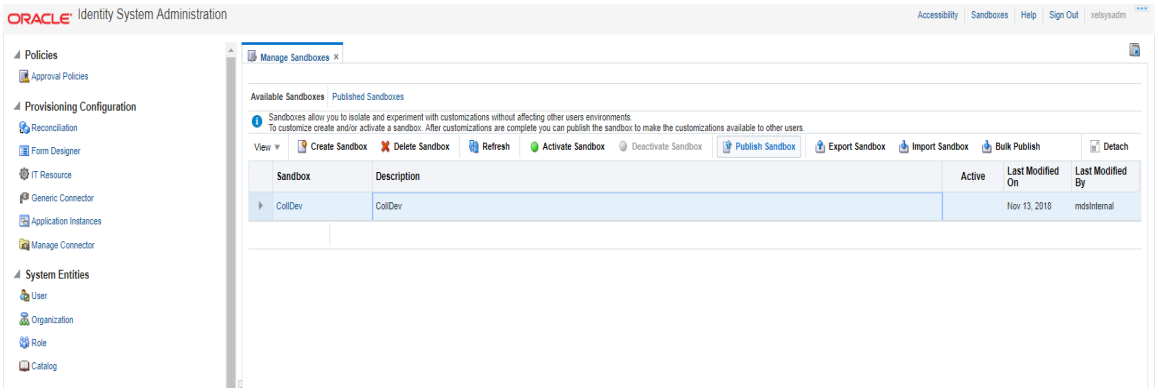
1. Select **CollectionsDev** sandbox and then click **Publish Sandbox** to publish sandbox.

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

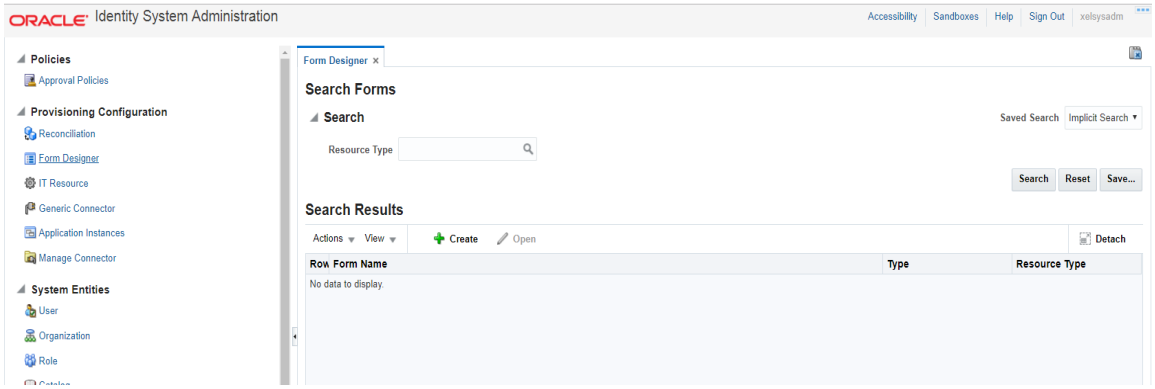


3.3.4 Create Form Associated with Application Instance

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

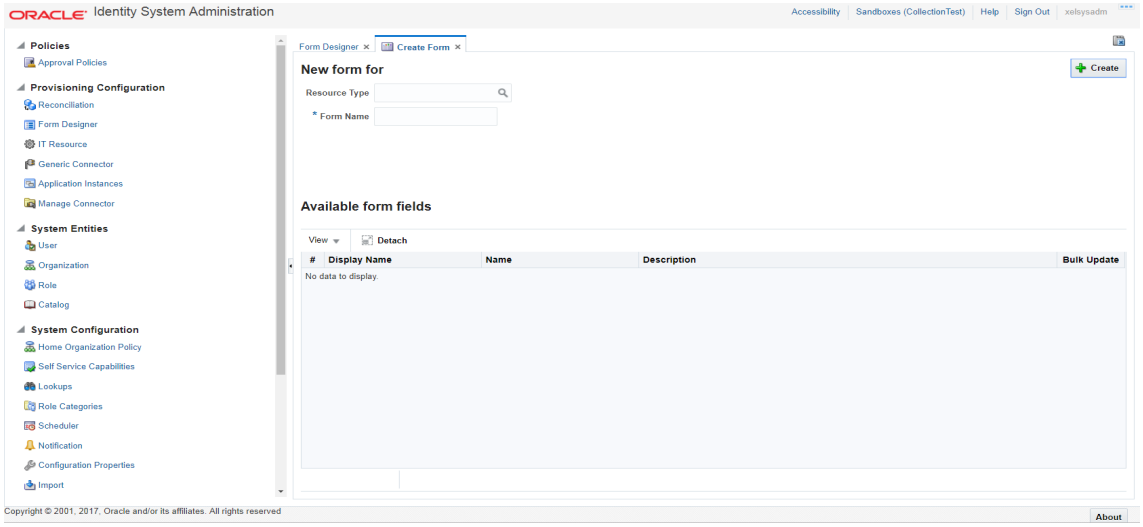
1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Chapter 1.3.3 Oracle Banking Collections and Oracle Banking Recovery Sandbox.
3. In the left pane, under Configuration, click **Form Designer**. The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

Figure 3–23 Create Form - Form Designer



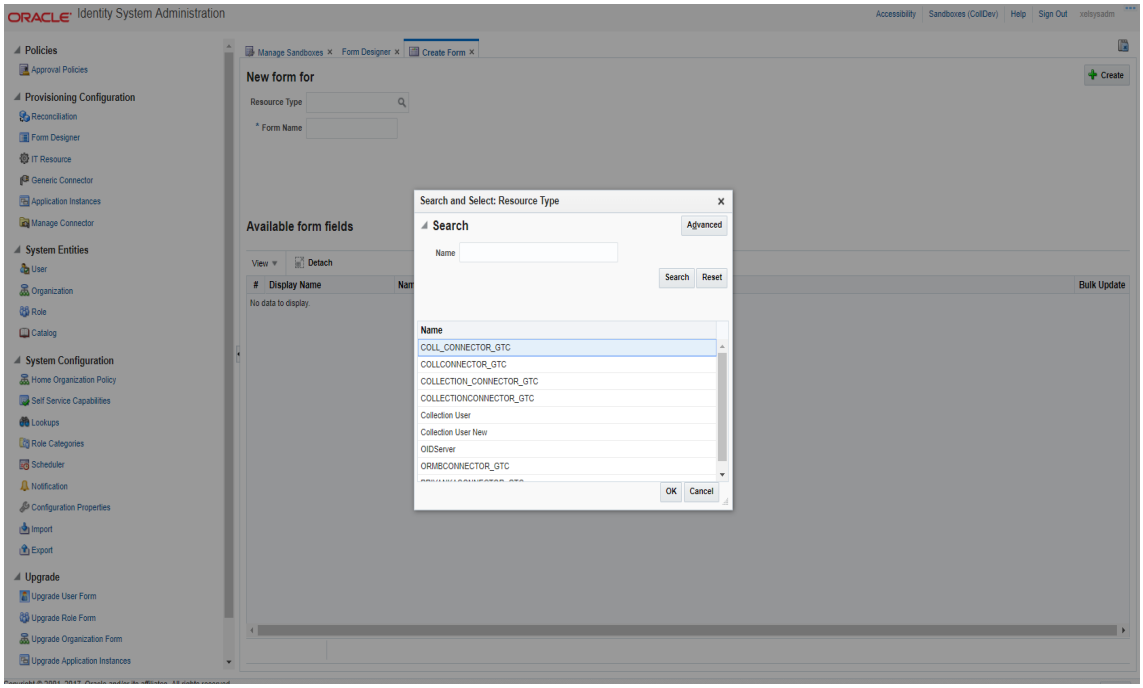
4. Click **Create** on the toolbar. The **Create Form** page is displayed.
5. In the **Resource Type** field, verify the name of the resource object with which the form is associated is displayed. To change the resource object name, click the Search icon next to the **Resource Type** field, and search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

Figure 3–24 Create Form - Resource Type



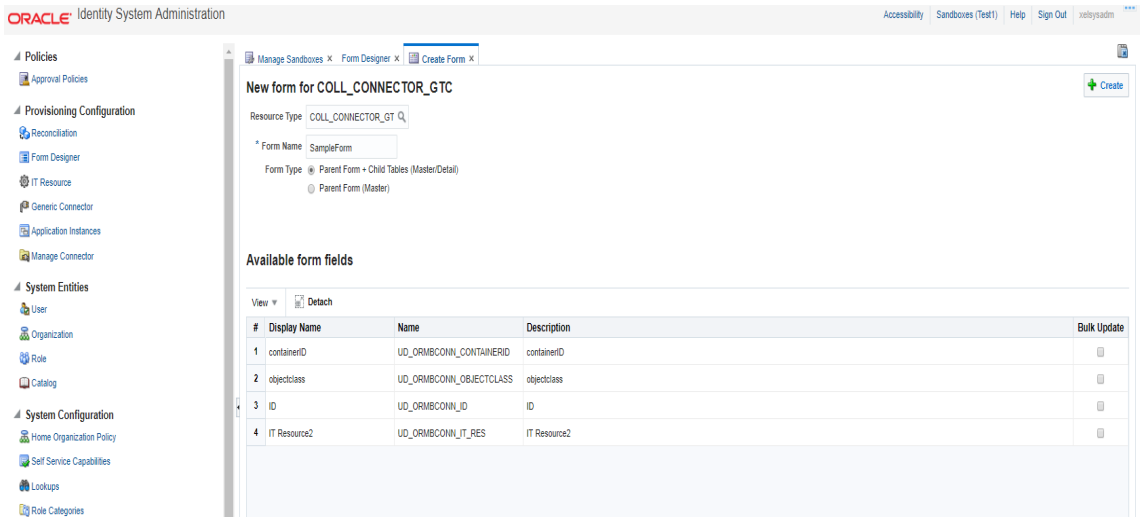
6. Select **Resource Type** as **COLL_CONNECTOR_GTC** and provide a name for the form (for example, SampleForm).

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



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

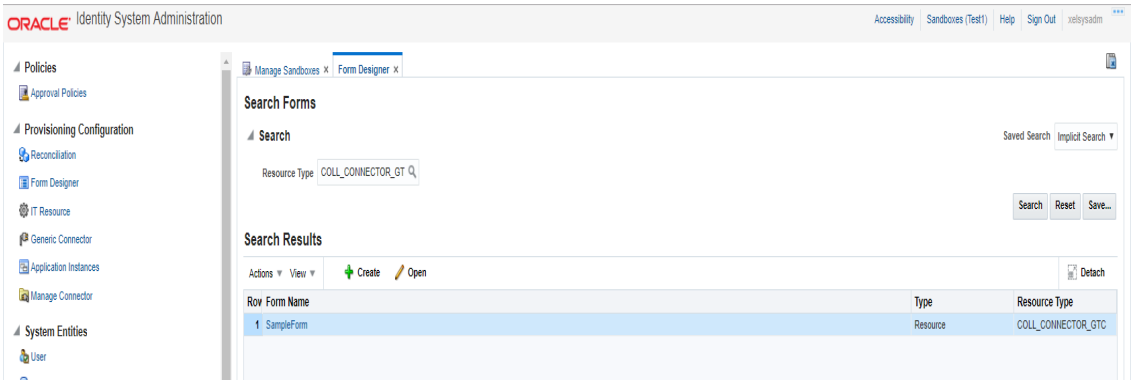
Figure 3–26 Create Form Resource Type - Available Form Fields



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

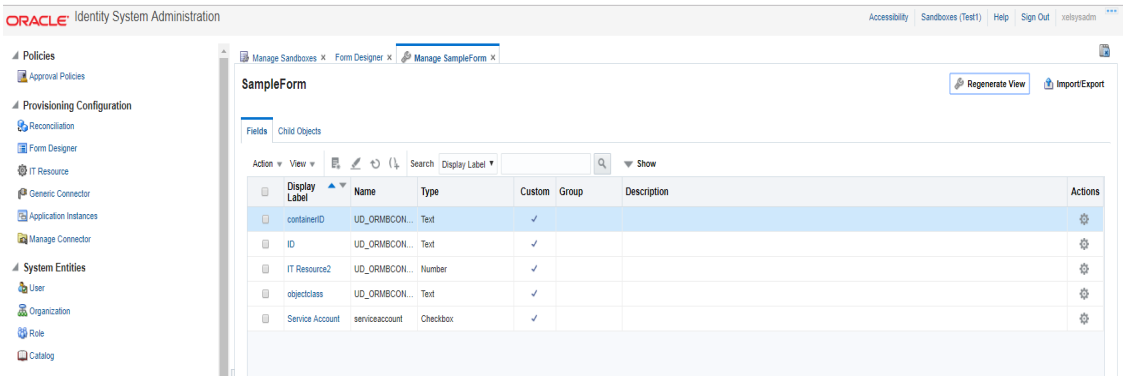
9. Refresh the **Search Results** in **Form Designer** page for resource type : COLL_CONNECTOR_GTC.
10. Select the **SampleForm** from the results.

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

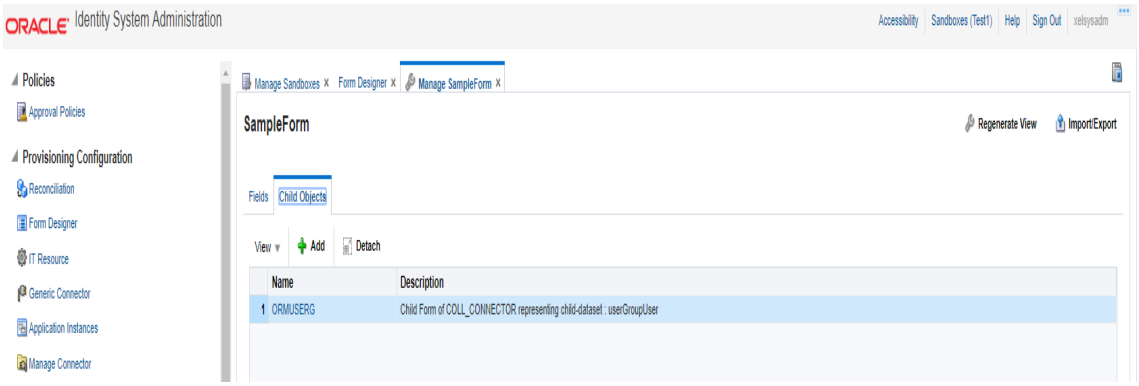
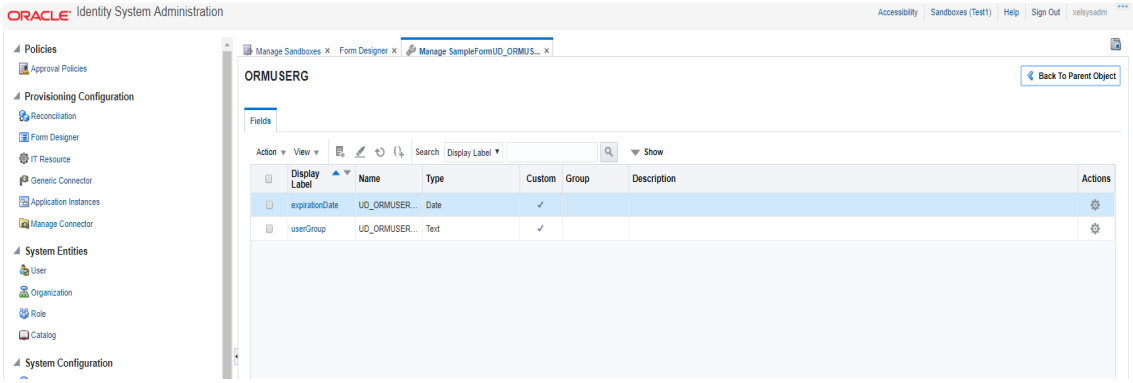
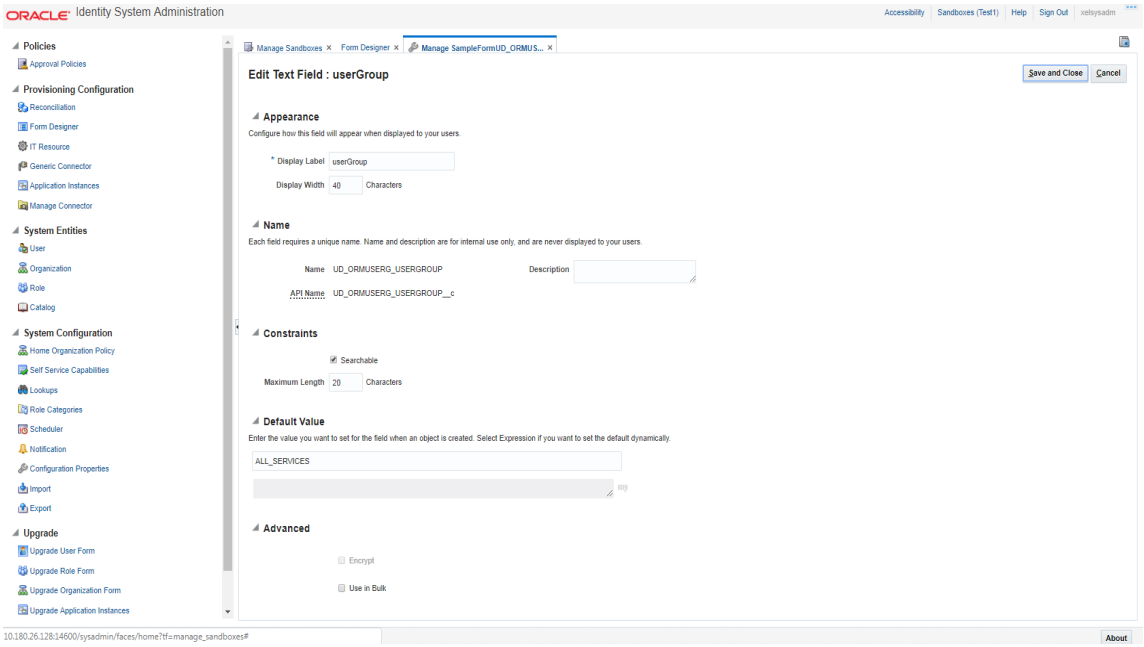


Figure 3–30 Manage Child Objects form fields



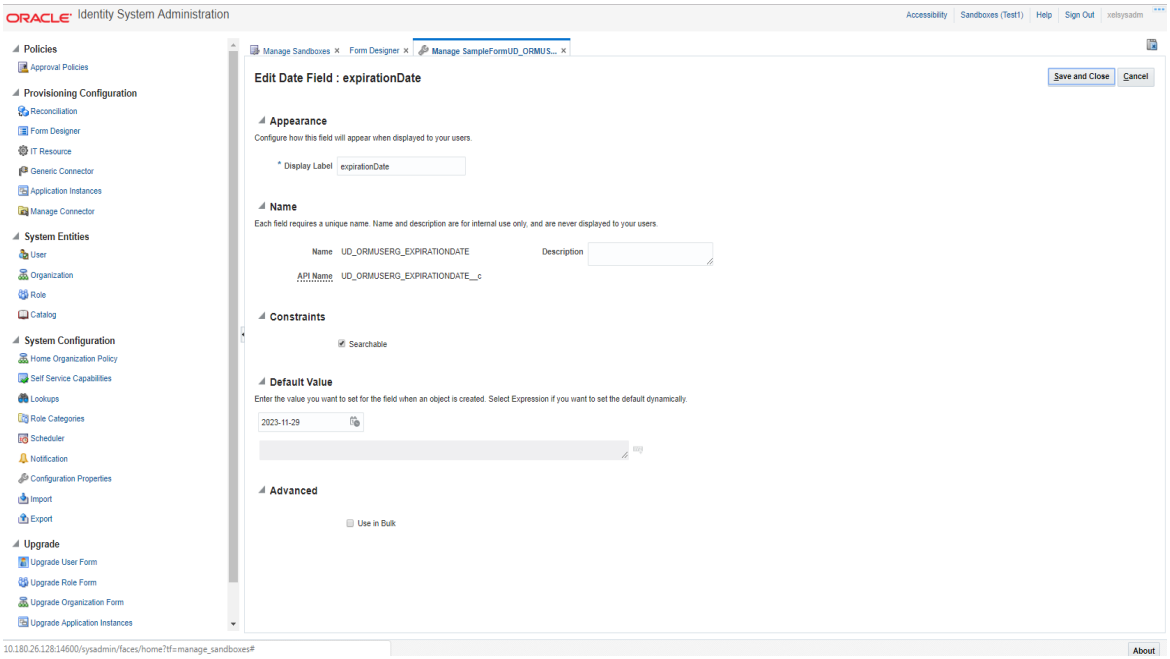
15. Click the userGroup and give default value as ALL_SERVICES.

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



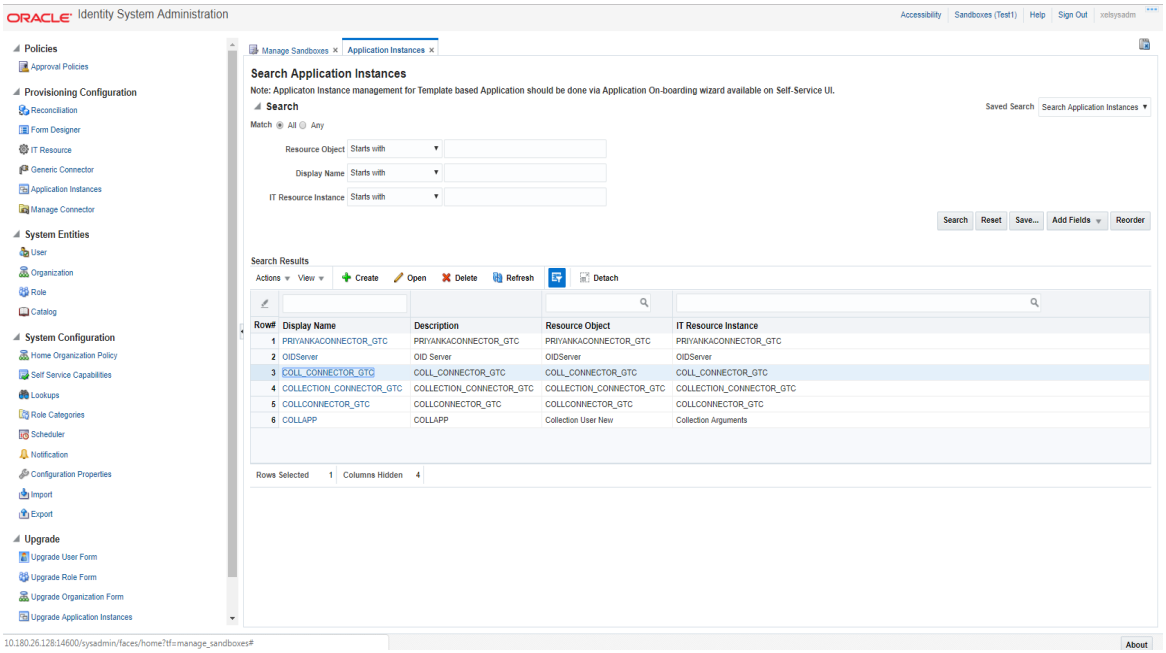
17. Click **Save** and **Close**.
18. Click the **Back to Parent Object** Link.

19. Close **Manage SampleForm** tab.

Steps to associate the form with the application instance:

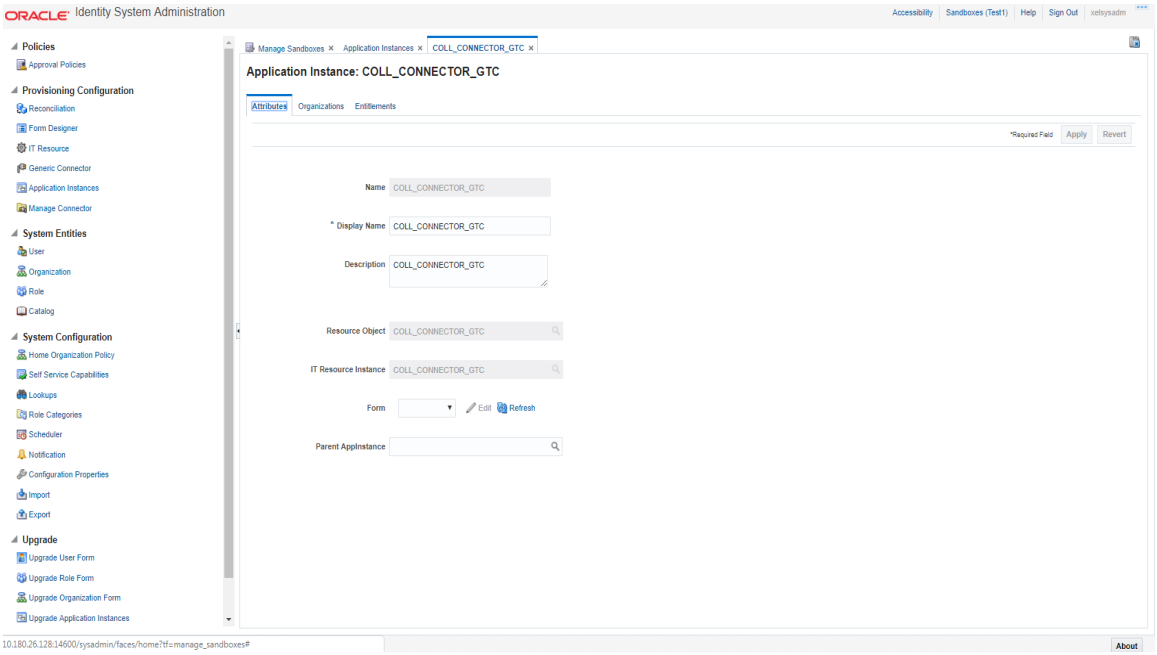
1. Click the **Application Instances** Menu. Click **Search** and select COLL_CONNECTOR_GTC.

Figure 3–33 Search Application Instances and select COLL_CONNECTOR_GTC



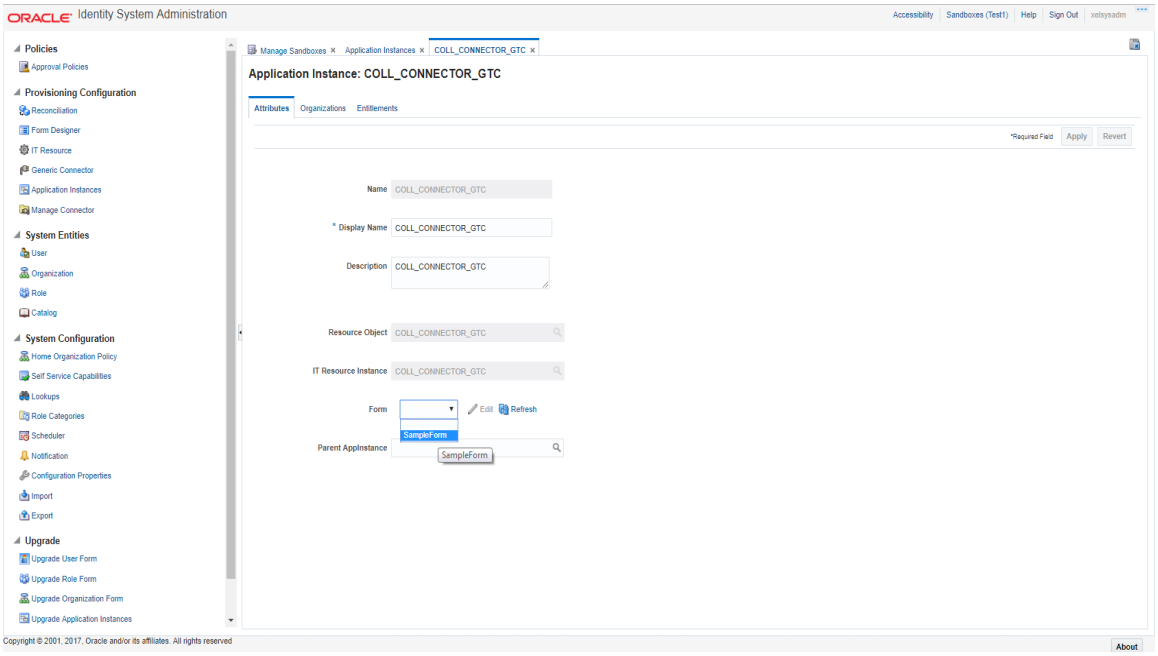
2. Click the **Attributes** tab.

Figure 3–34 Application Instance Attributes



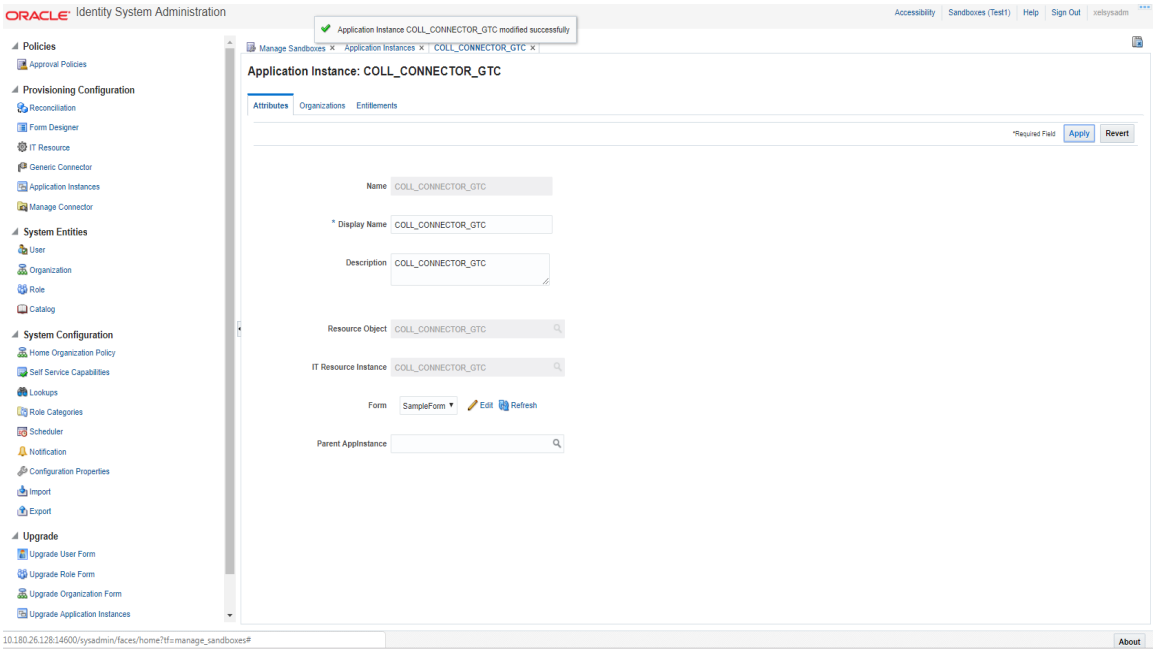
3. In Form list, select above created form and click **Apply**.

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 Collections and Oracle Banking 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

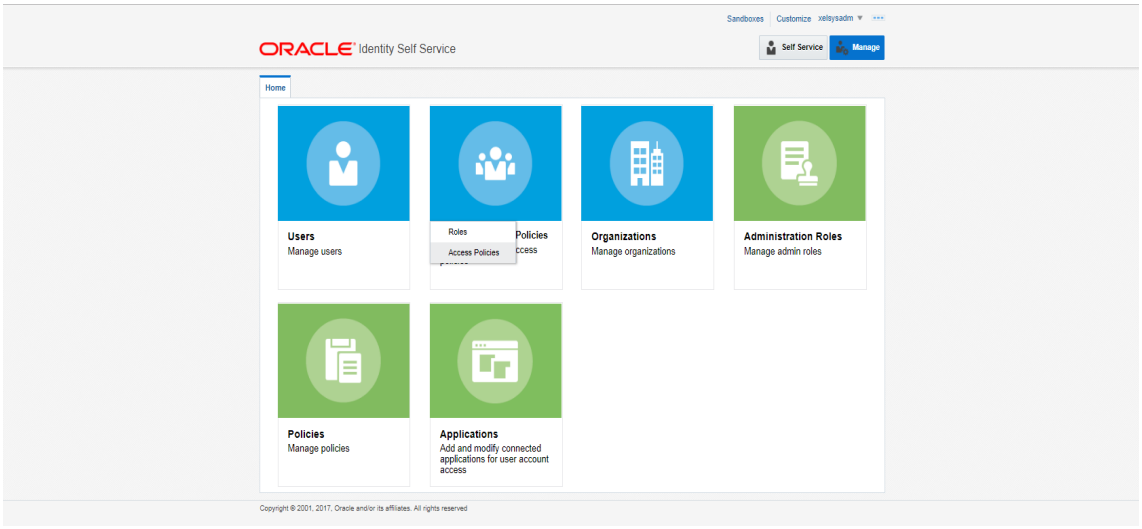
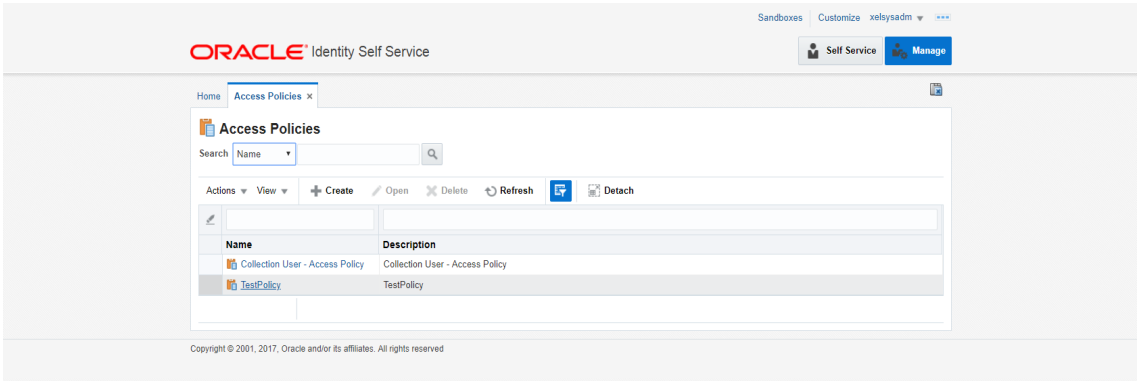
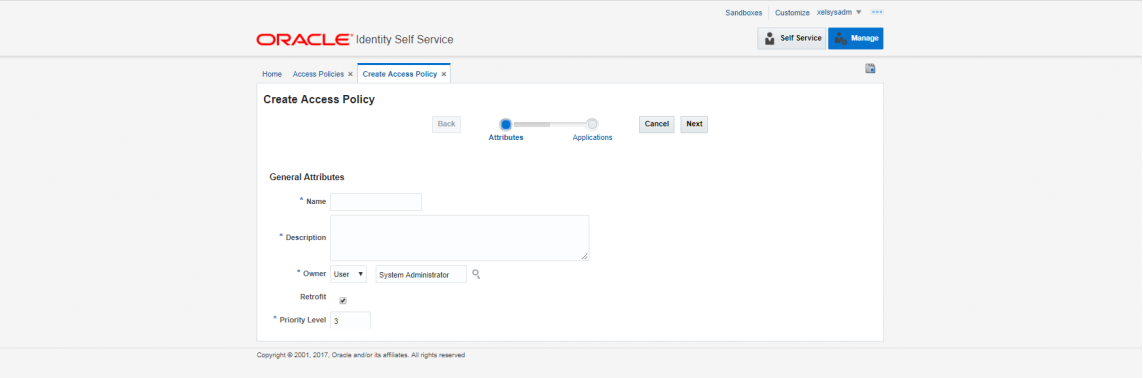


Figure 3–38 Access Policies



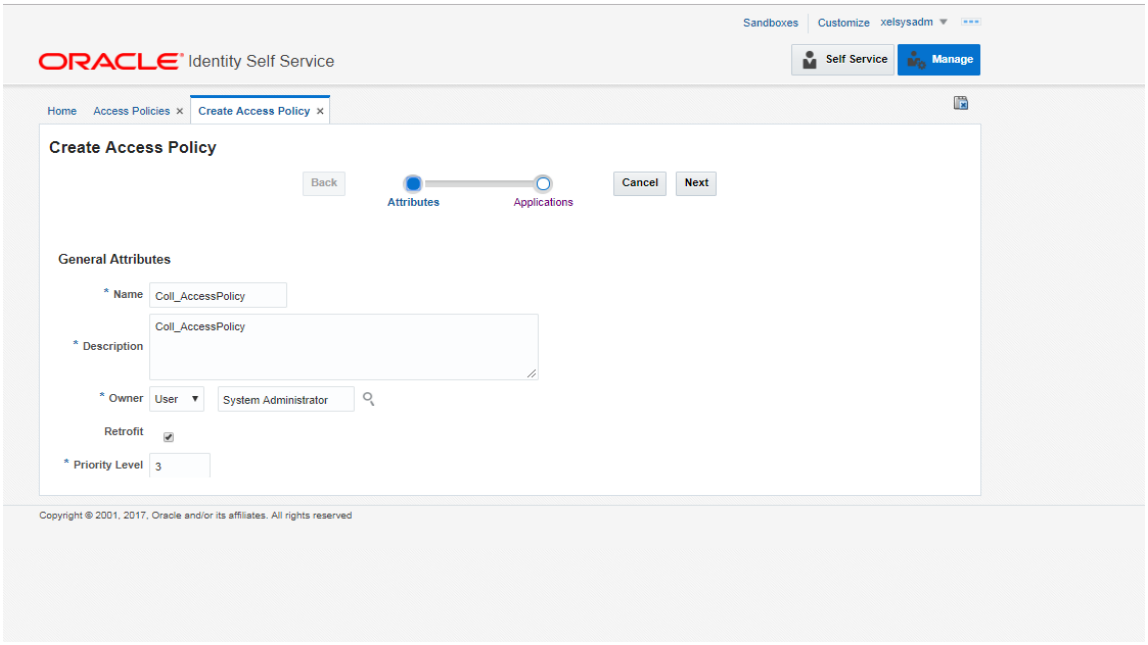
4. Click **Create**. Create Access Policy Page is displayed.

Figure 3–39 Create Access Policy



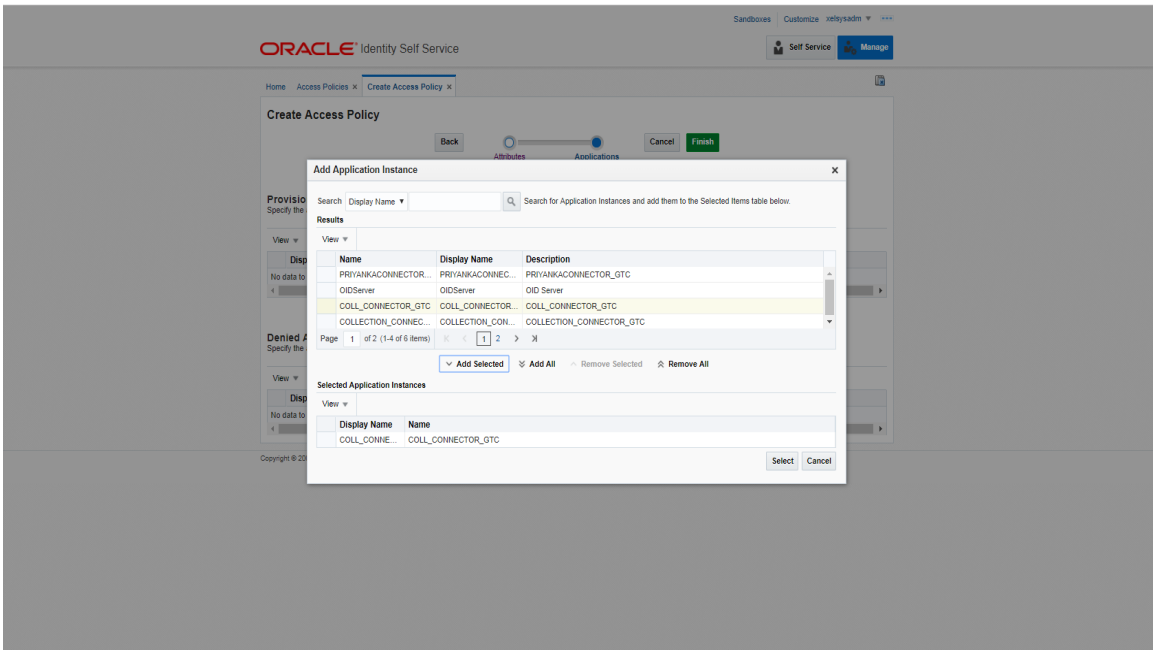
5. Enter following details (for example) and click **Next**.
   - **Name**: Coll_AccessPolicy
   - **Description**: Coll_AccessPolicy

Figure 3–40 Access Policy details



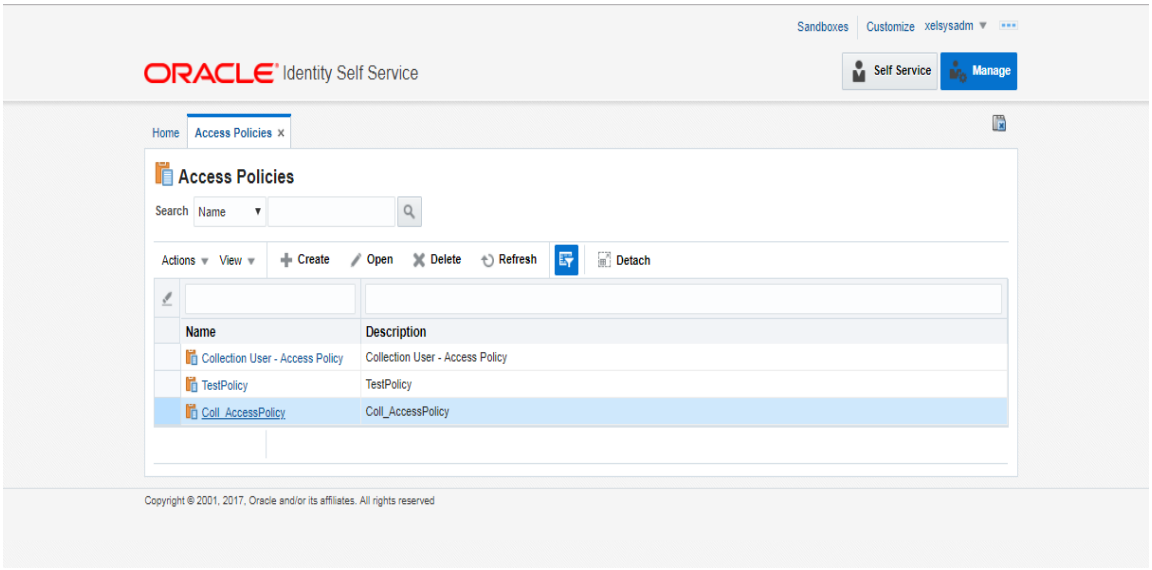
6. To specify the application instances provisioned by this access policy, click **Add** and select **COLL_CONNECTOR_GTC** Application Instance. Click **Select**.

Figure 3–41 Add application instance associated with access policy



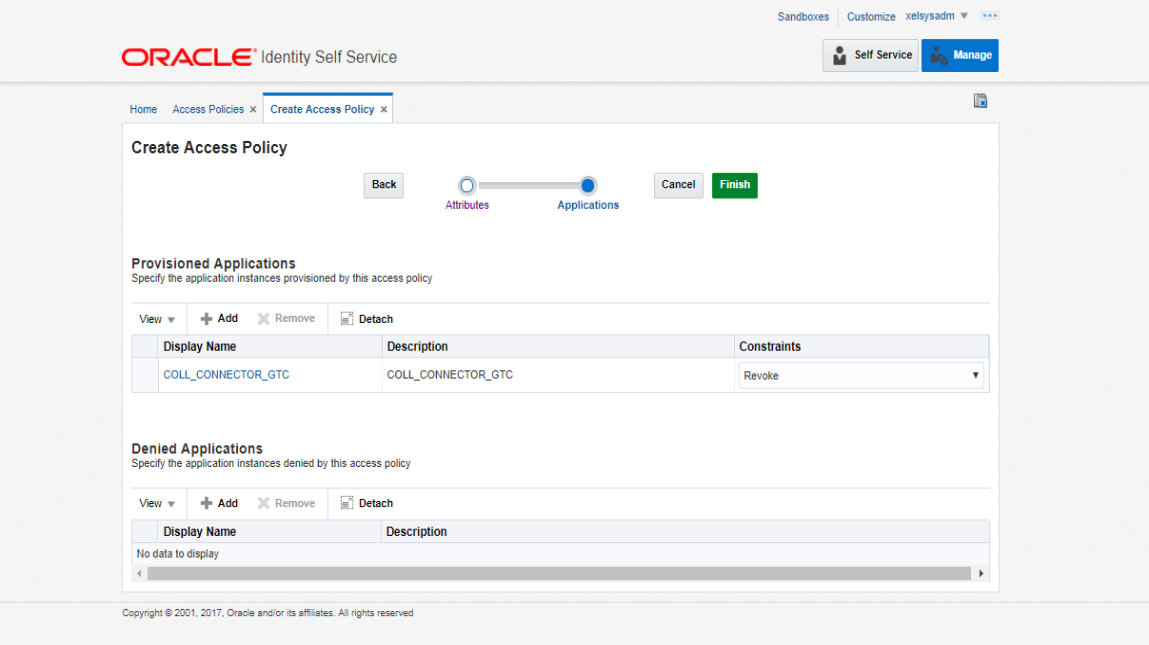
7. Click **Finish**.
8. In the Search Access Policies Page, select the above created policy and click the **Applications** tab.

Figure 3–42 Search Access Policy



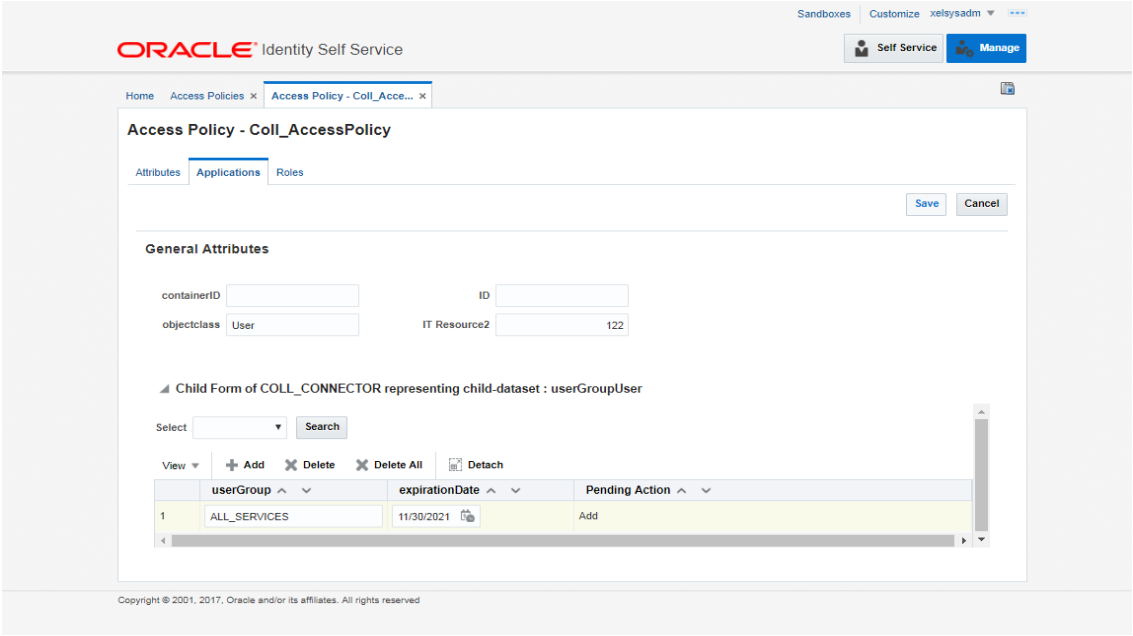
9. COLL_CONNECTOR_GTC application would be listed in the Provisioned Applications list.

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**.

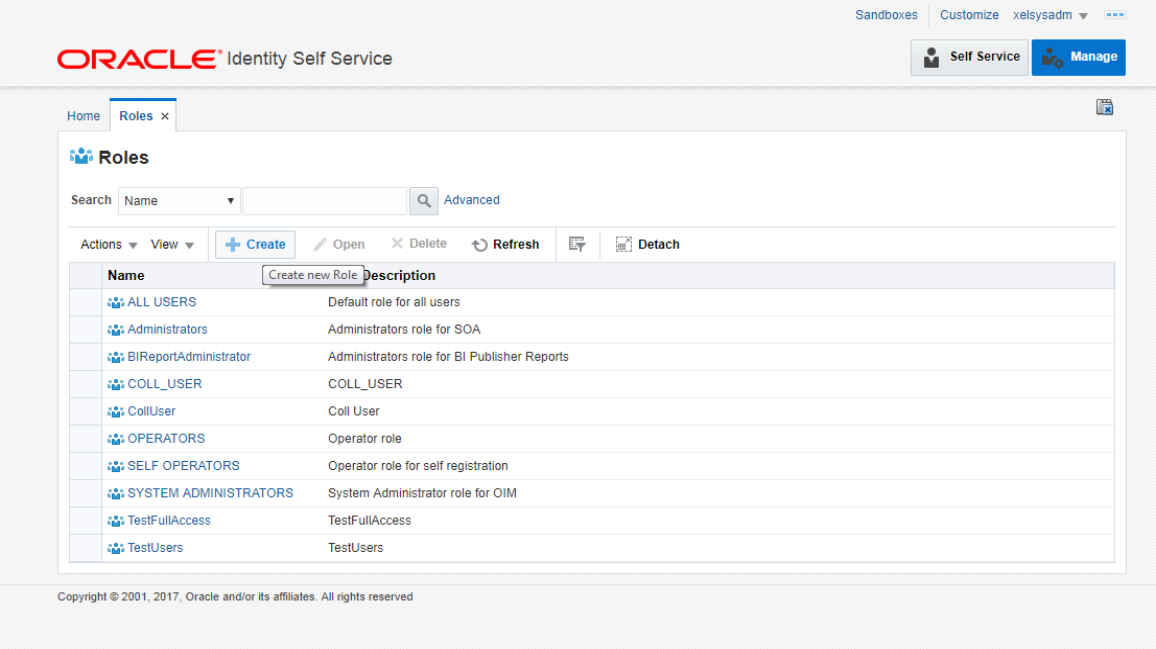
3.3.5.2 Creating Roles

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 Collections and Oracle Banking Recovery User provisioning.

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

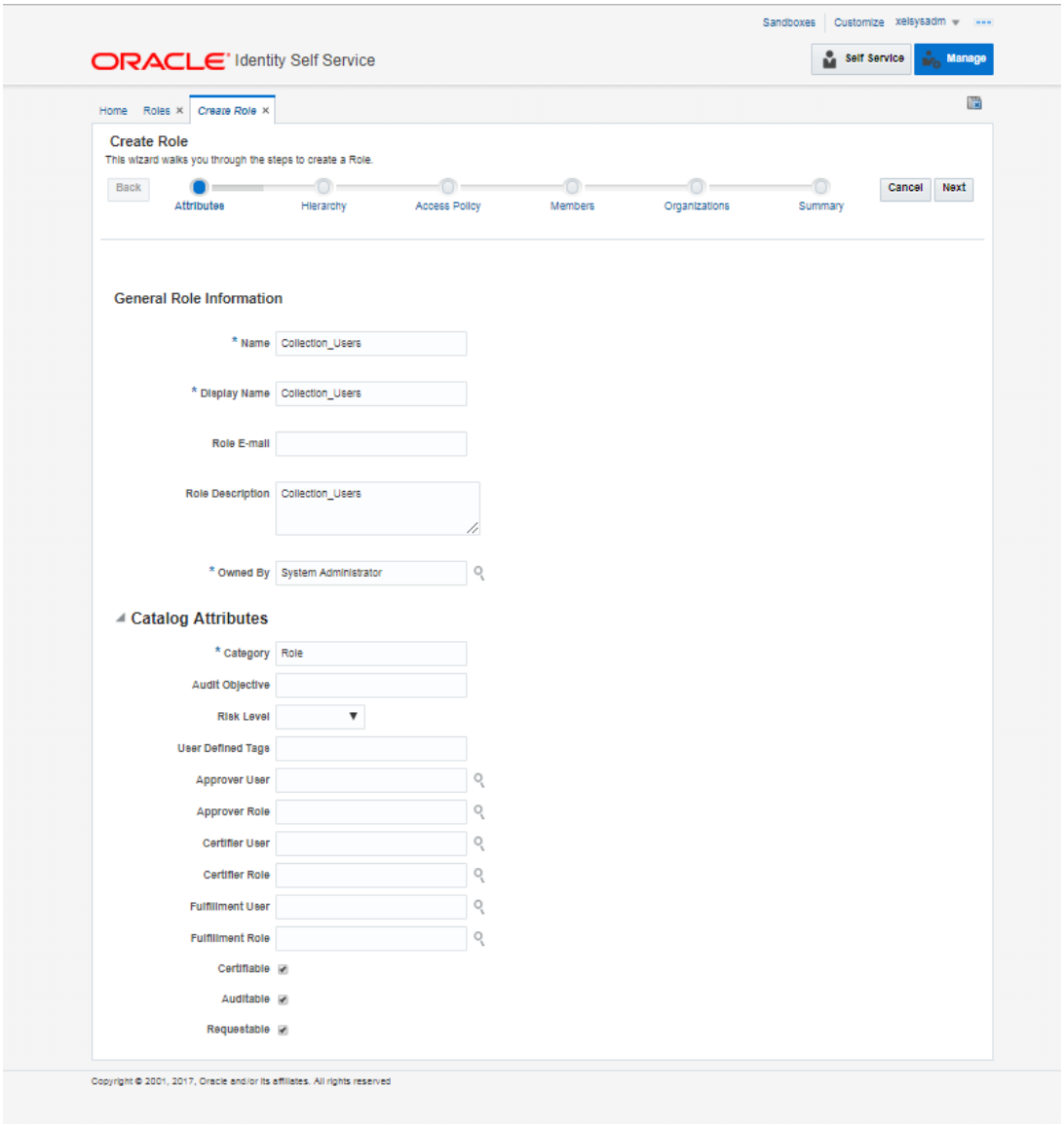
3. Select **Roles**. The Search Roles page is displayed.

Figure 3–45 Oracle Identity Self Service- Roles Tab



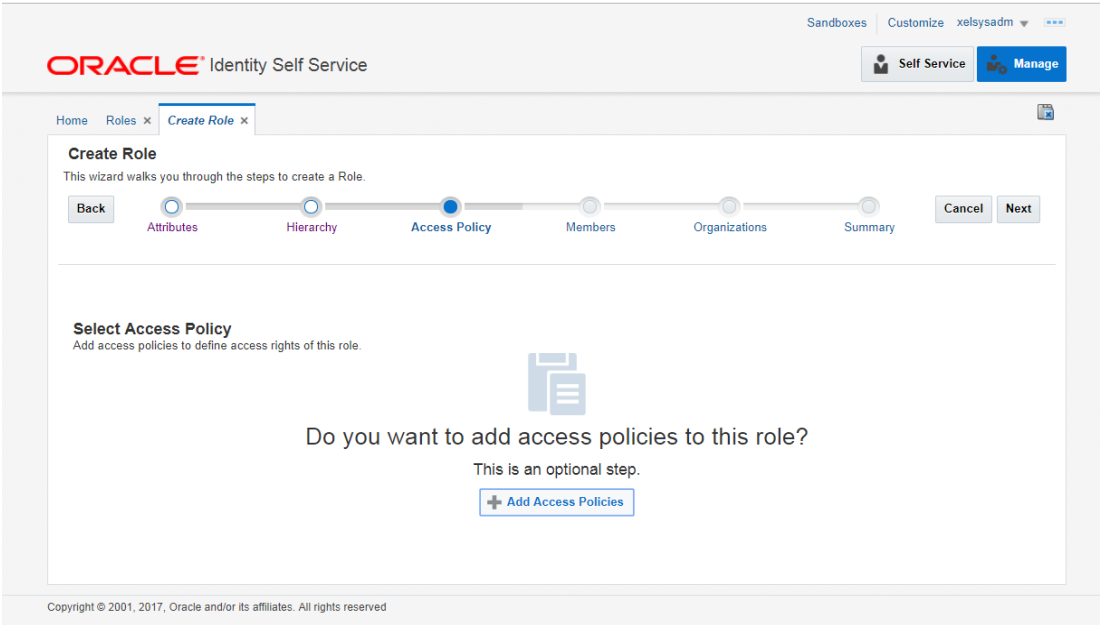
4. Click **Create** on the toolbar. The Create Role page is displayed.
5. Specify the following values and then click **Next**.
   - **Name**: Collection_Users
   - **Display Name**: Collection_Users
   - **Role Description**: Default Role for all Oracle Banking Collections and Oracle Banking RecoveryUser.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

Figure 3–46 Create Role



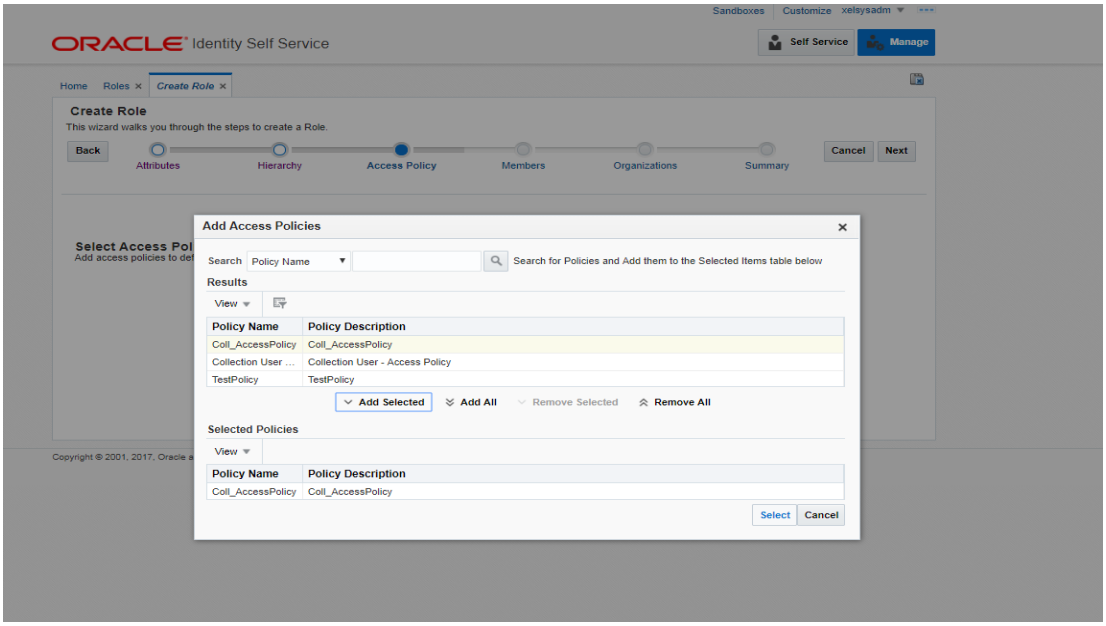
6. Click **Next** to go to the Access Policy step.

Figure 3–47 Create Role



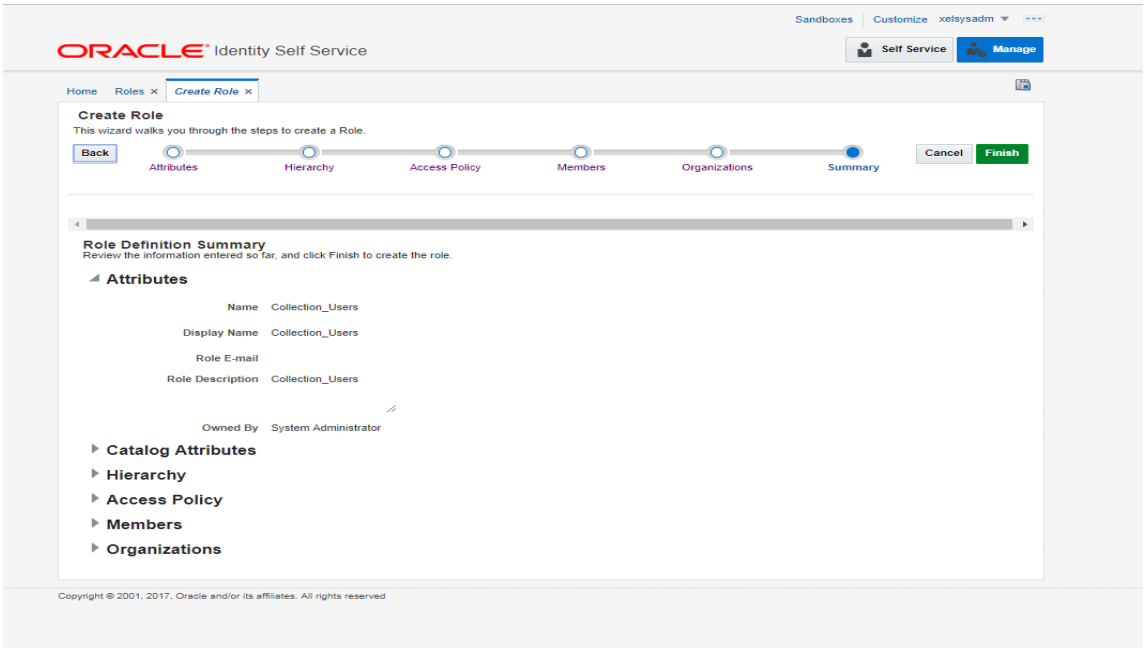
7. Click **Add Access Policies**. List of access policies is displayed on clicking the search icon.

Figure 3–48 Add Access Policy to the role



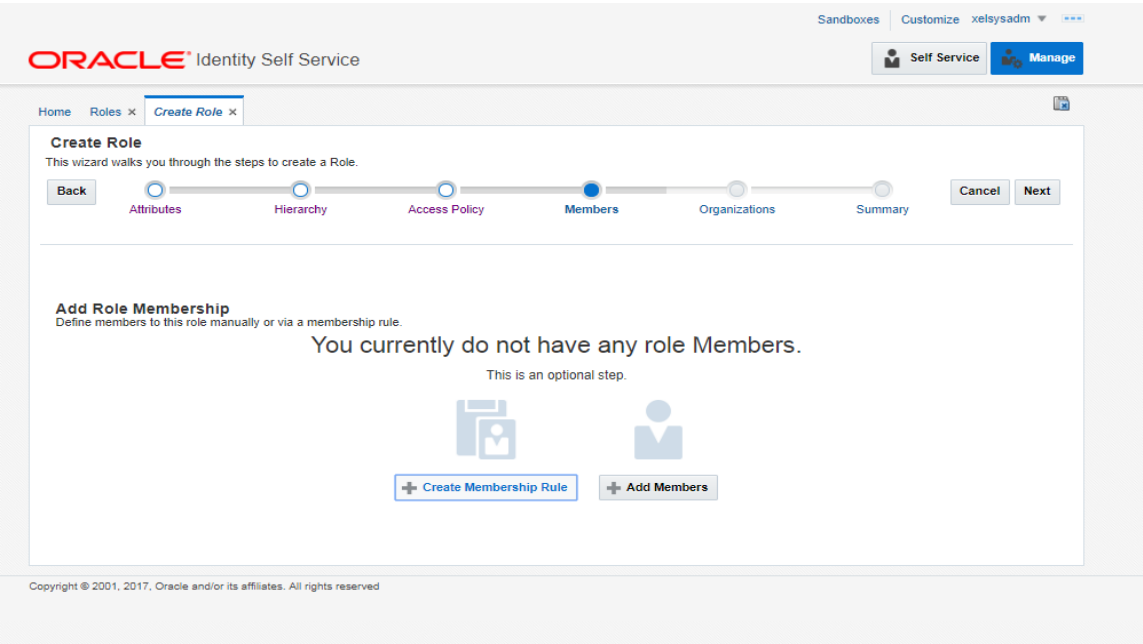
8. Select above created access policy (eg: Coll_AccessPolicy) and click **Next**.

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 Collections and Oracle Banking 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

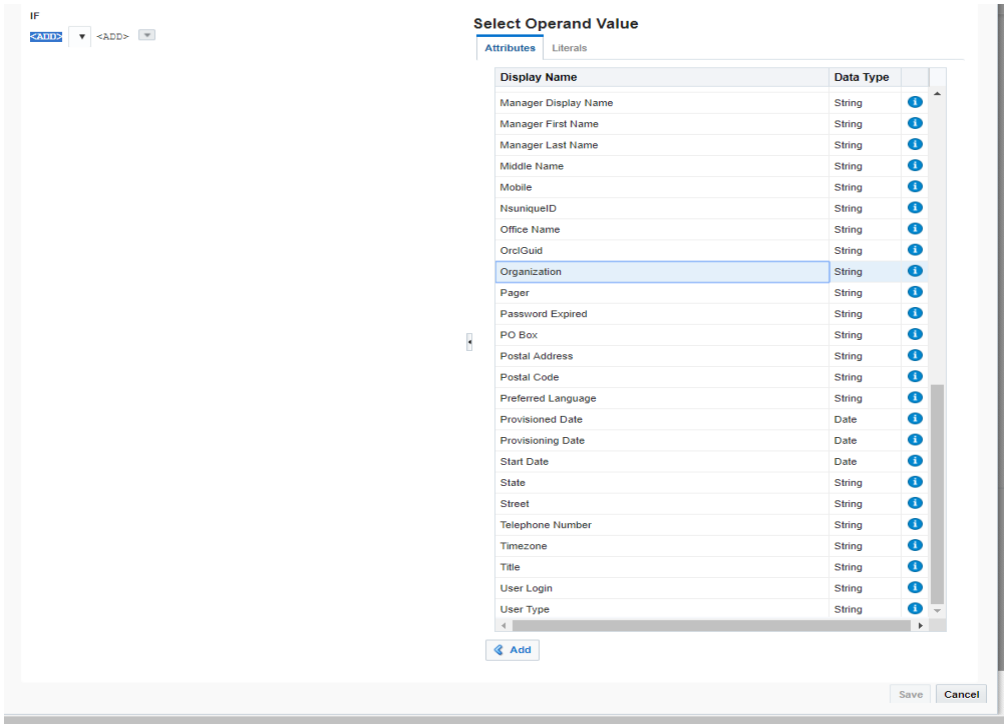
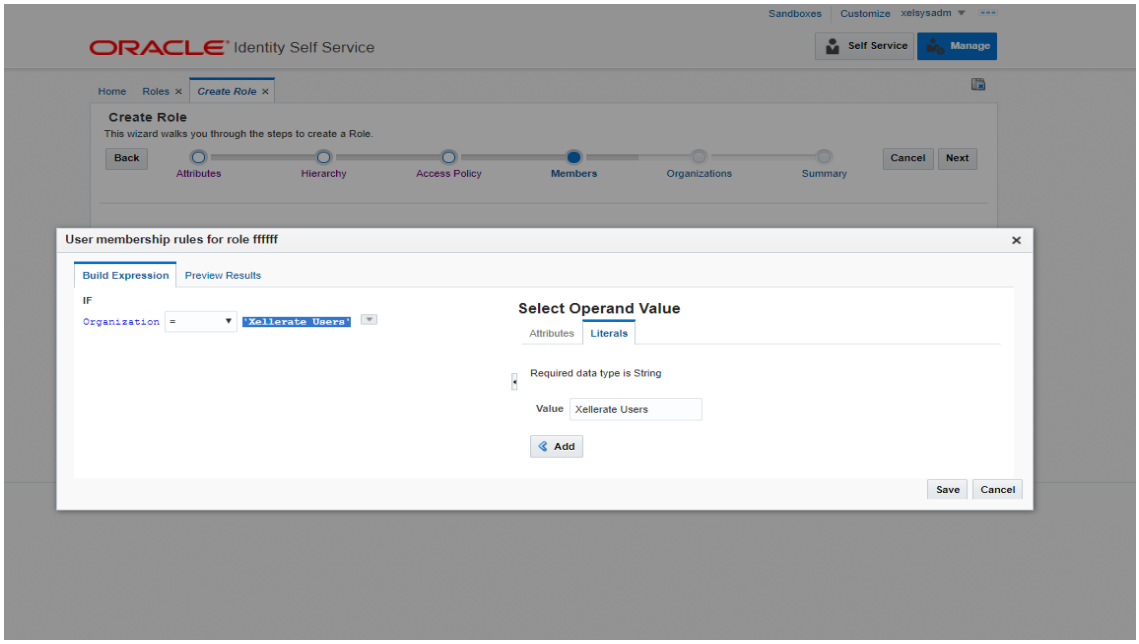


Figure 3–52 Build Membership Rule Expression



11. Click **Save**.

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 Collections and Oracle Banking 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 Collections and Oracle Banking 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 Collections and Oracle Banking Recovery. For every User, default User Group is populated in Oracle Banking Collections and Oracle Banking Recovery.
End Date	Date	N	Y	User's Log in expiry date.	

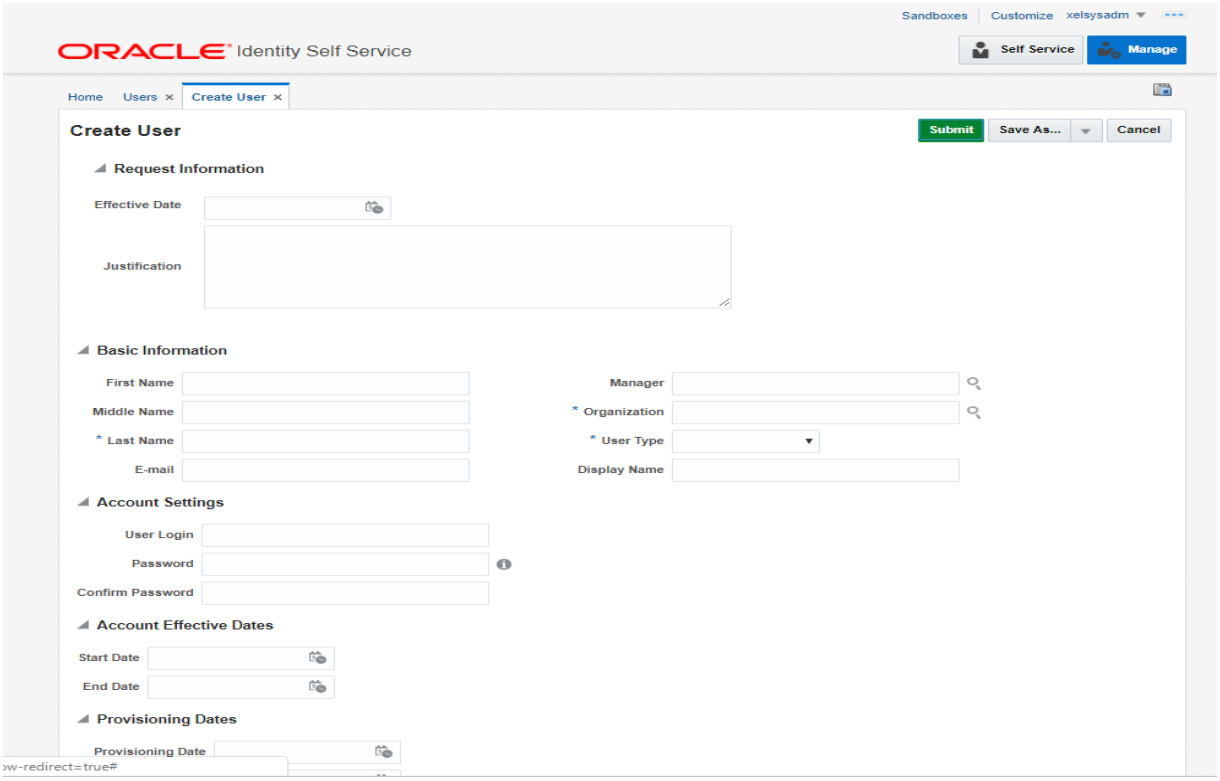
Note

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

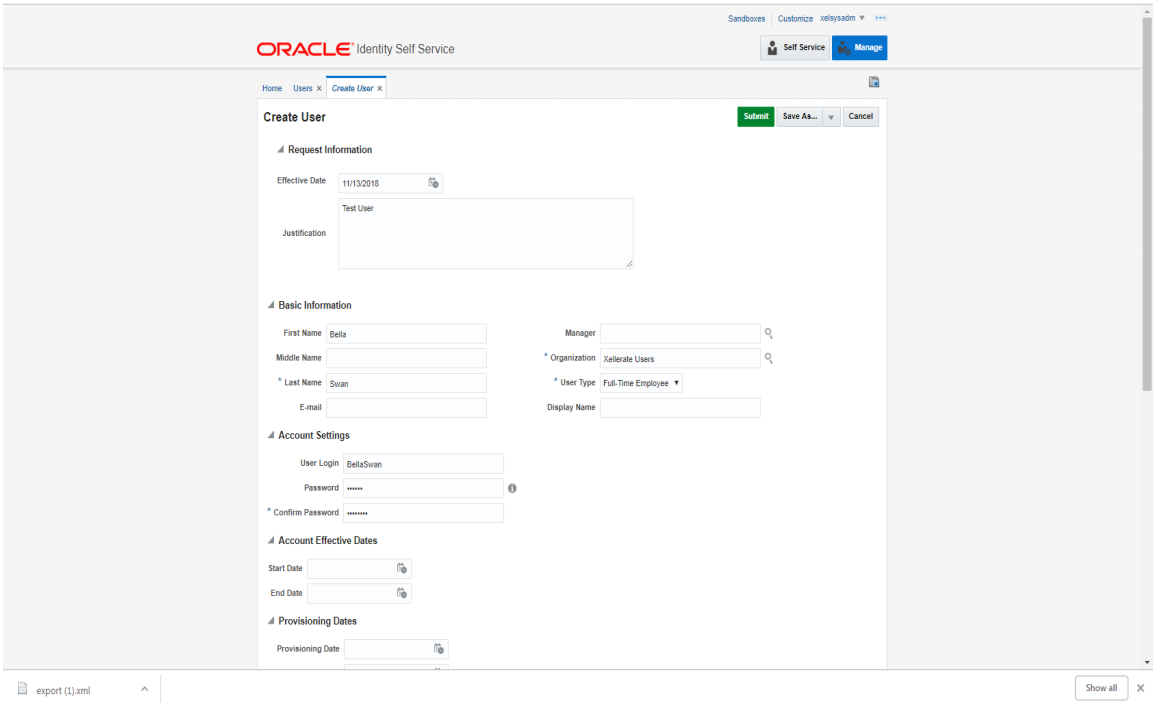
5 Create, Modify, Delete Users using OIM

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

5.1 Create and Provision Users

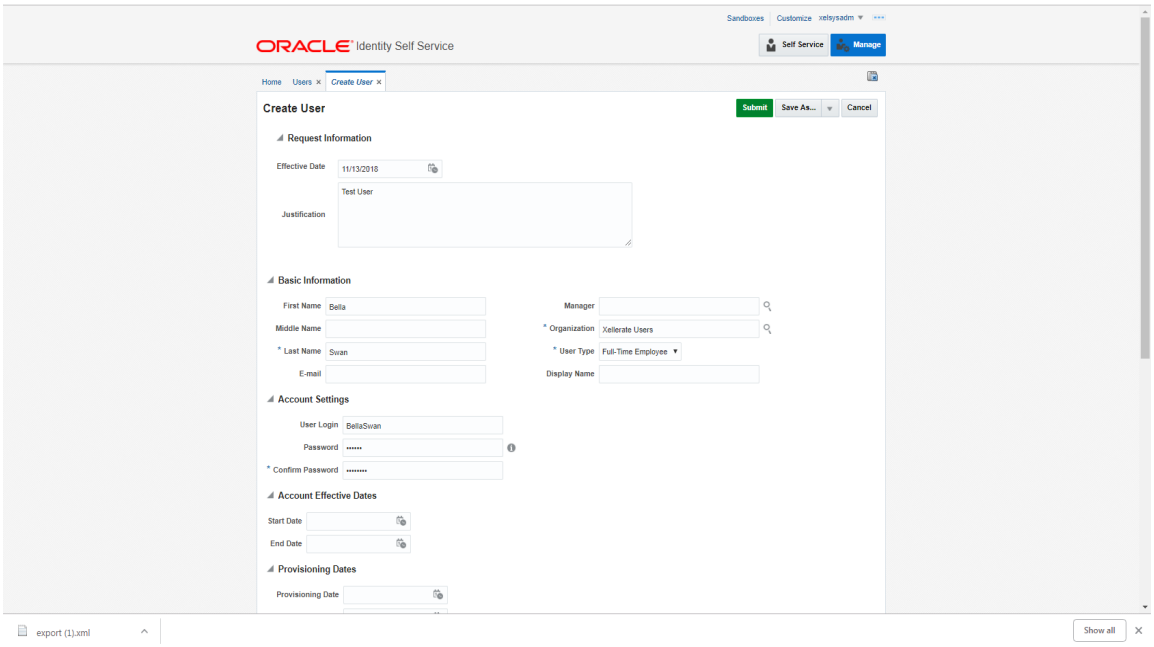
1. Log in OIM Identity Self Service.
2. Click **Users** and then click **Create**.
   The Create User tab opens.

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.

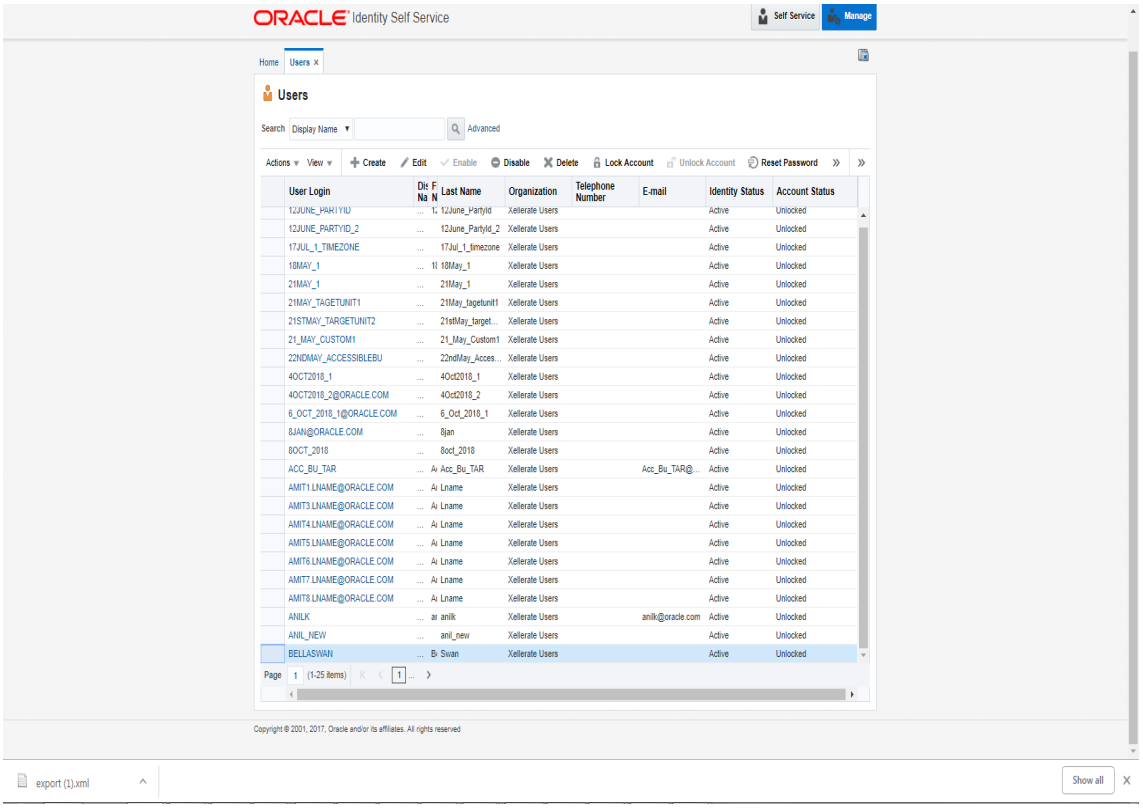
Figure 4–3 Input User Attributes



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

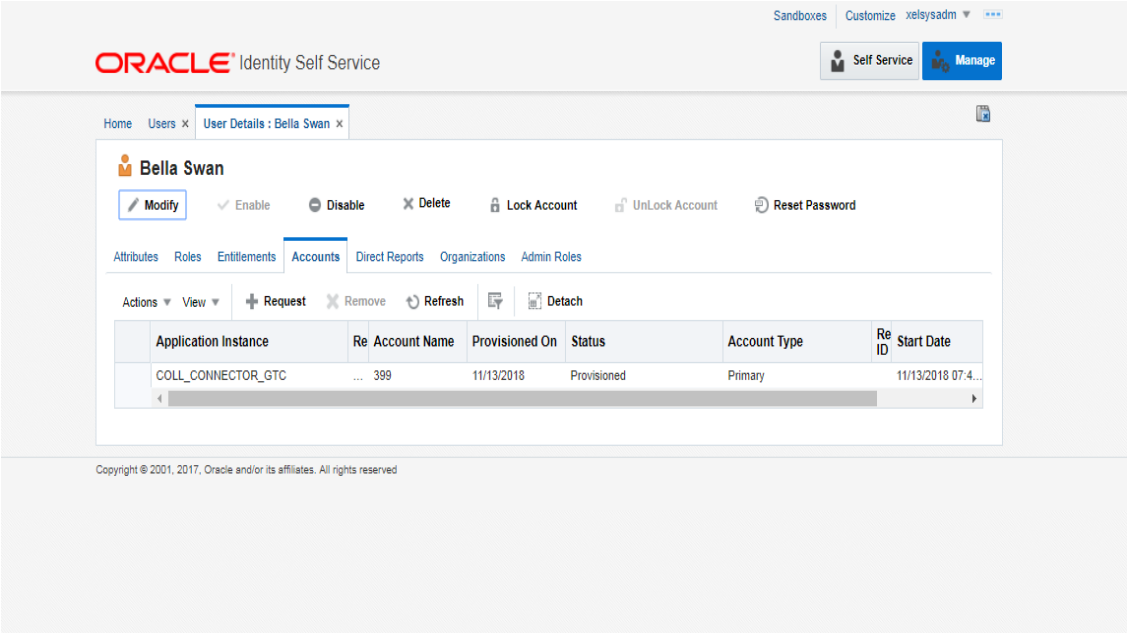
6. Click the above created user.

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.

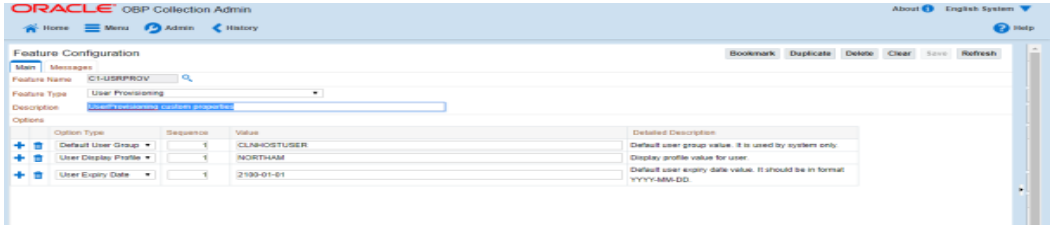
5.2 Feature Configurations

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

- **Default User Group**: Default Oracle Banking Collections and Oracle Banking 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 Collections and Oracle Banking 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

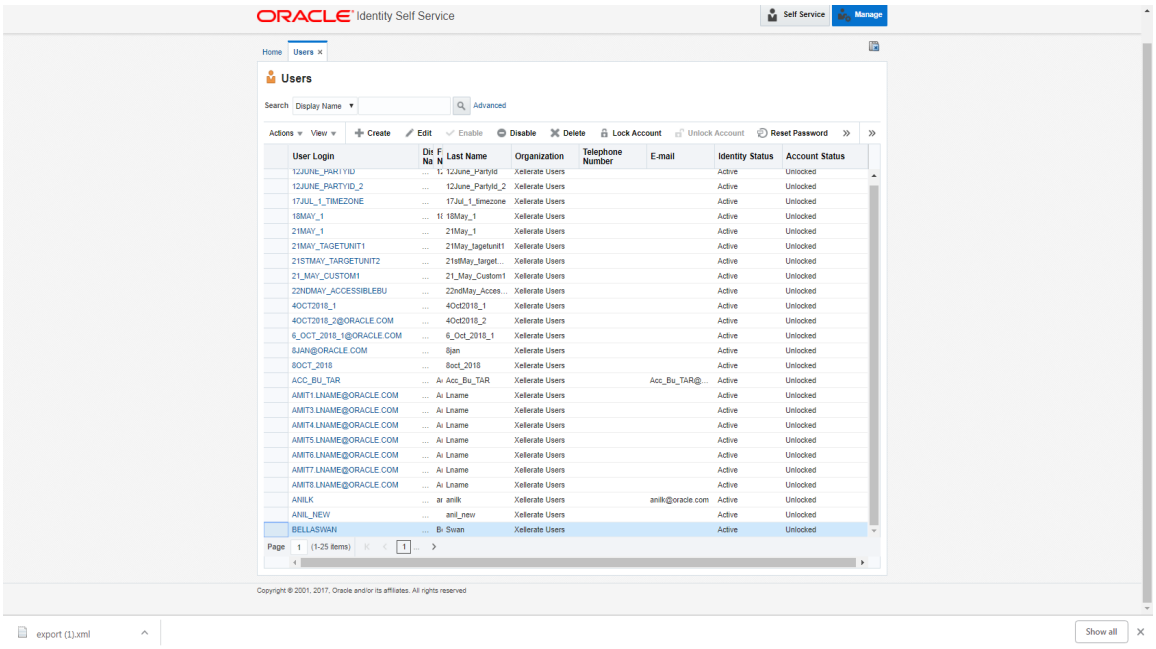
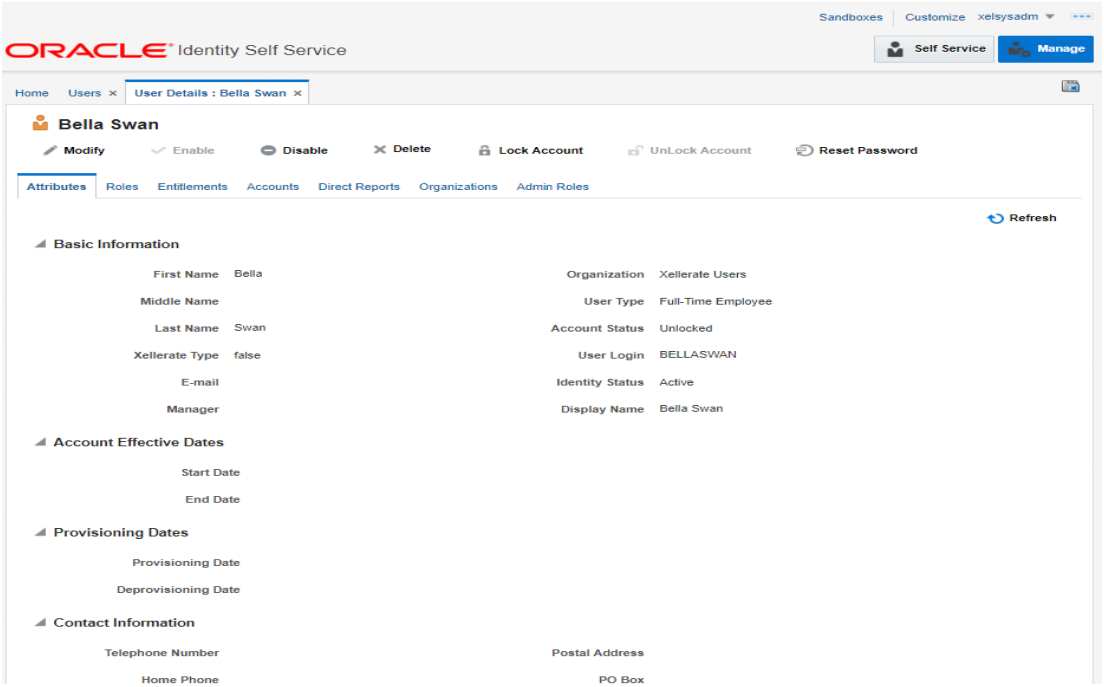


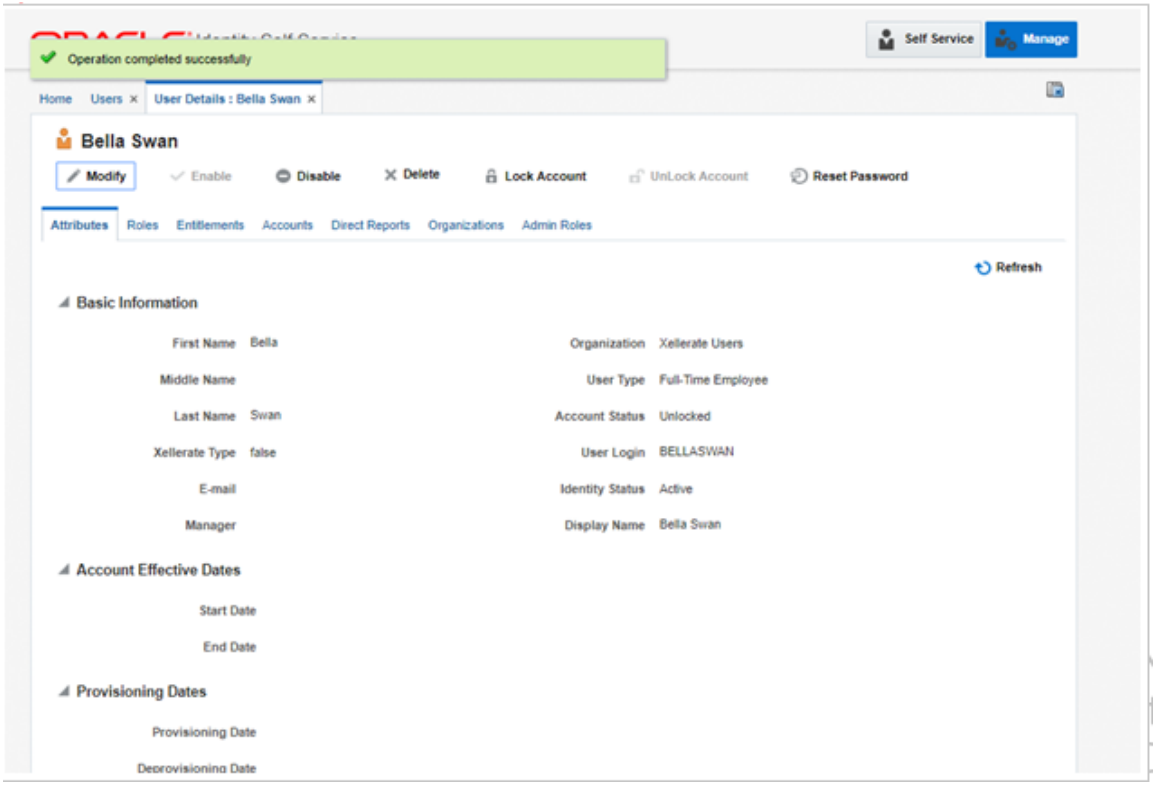
Figure 4–8 Detailed Information about the User



To modify a user:

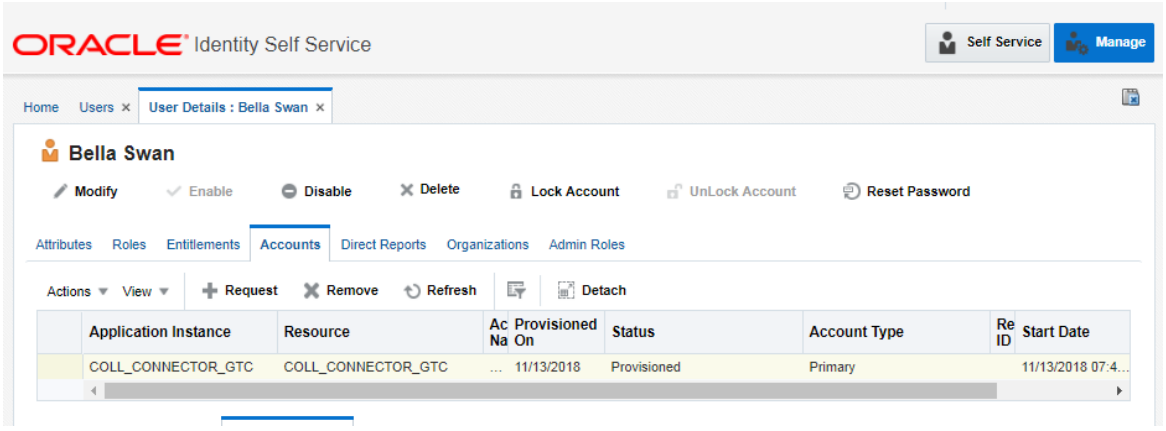
1. Click **Modify** to open Modify User page.
2. Modify the user details as per the requirement.
3. Click **Submit**. If the user details are valid (that is, if it does not violate any validation) then user details are modified. A message appears on successful completion of the modify operation. This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

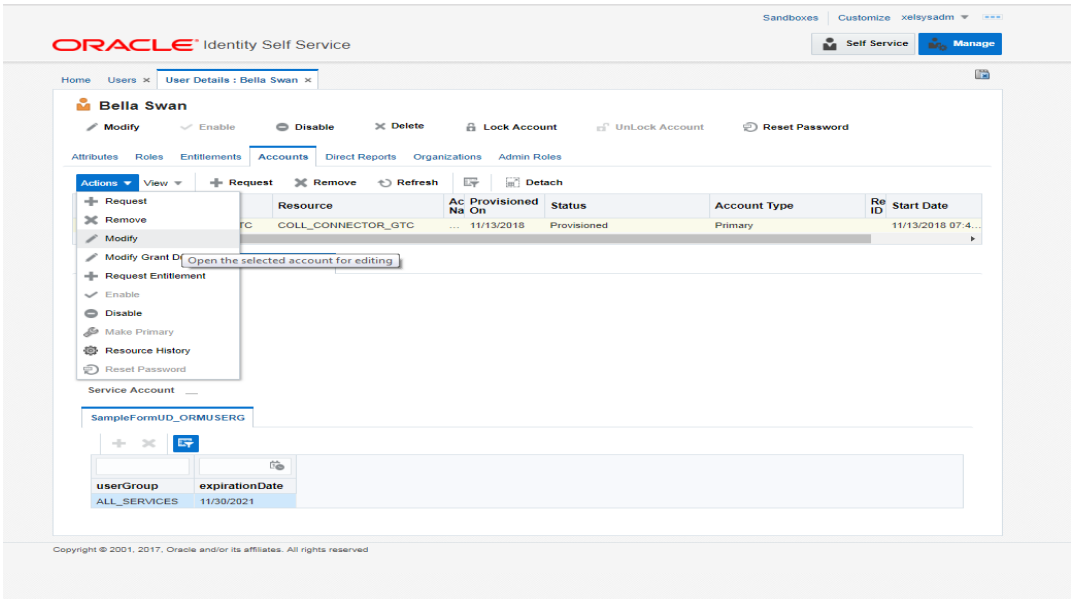
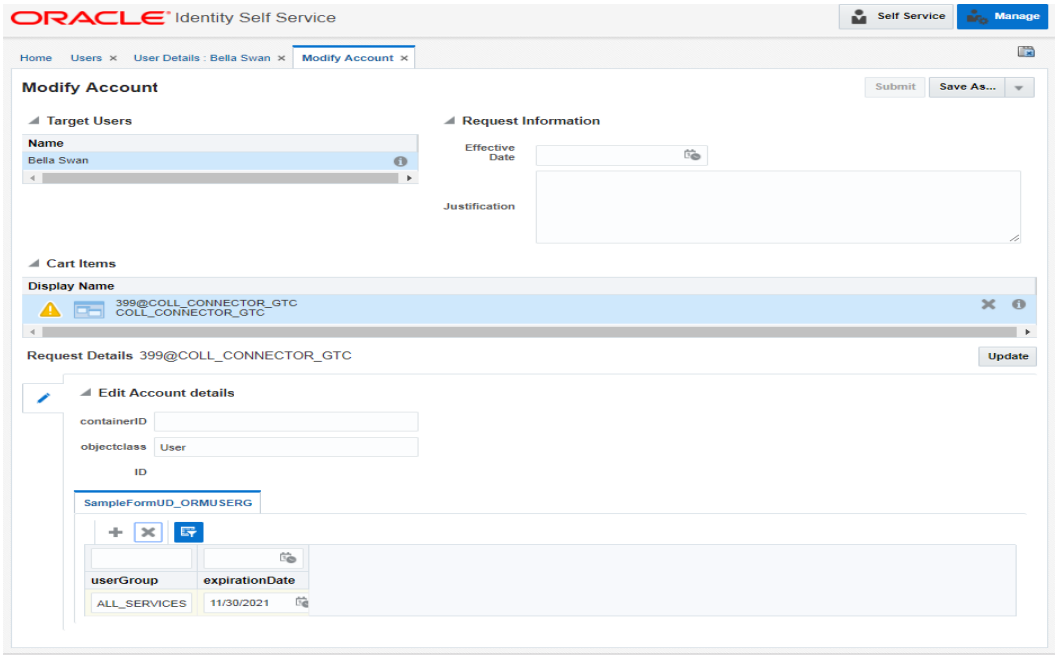


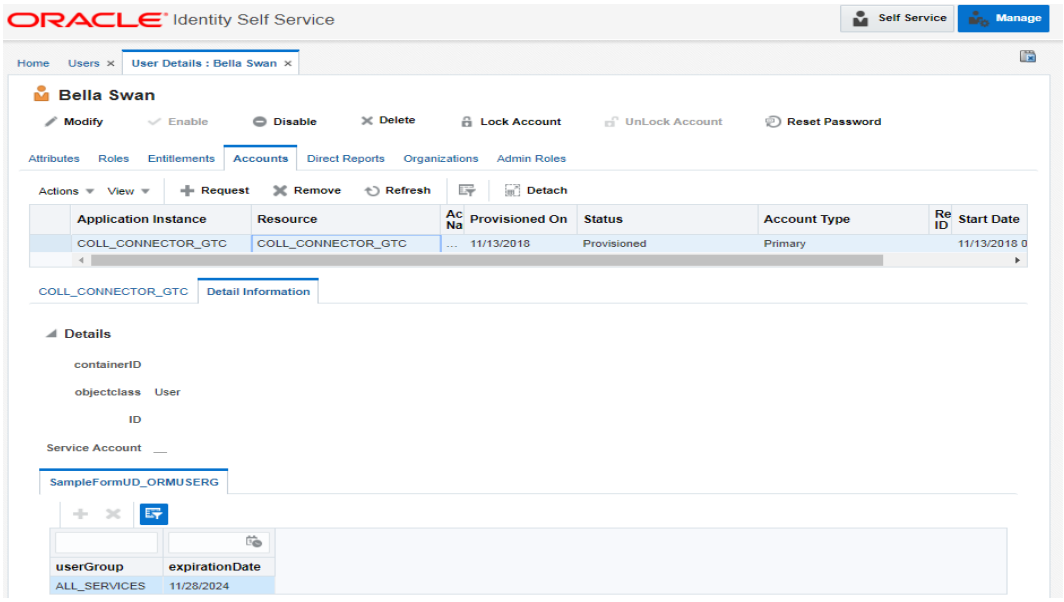
Figure 4–12 Edit Detail Information



    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 Collections and Oracle Banking Recovery supports soft delete, that is, it only expires User. User deletion request for Oracle Banking Collections and Oracle Banking 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

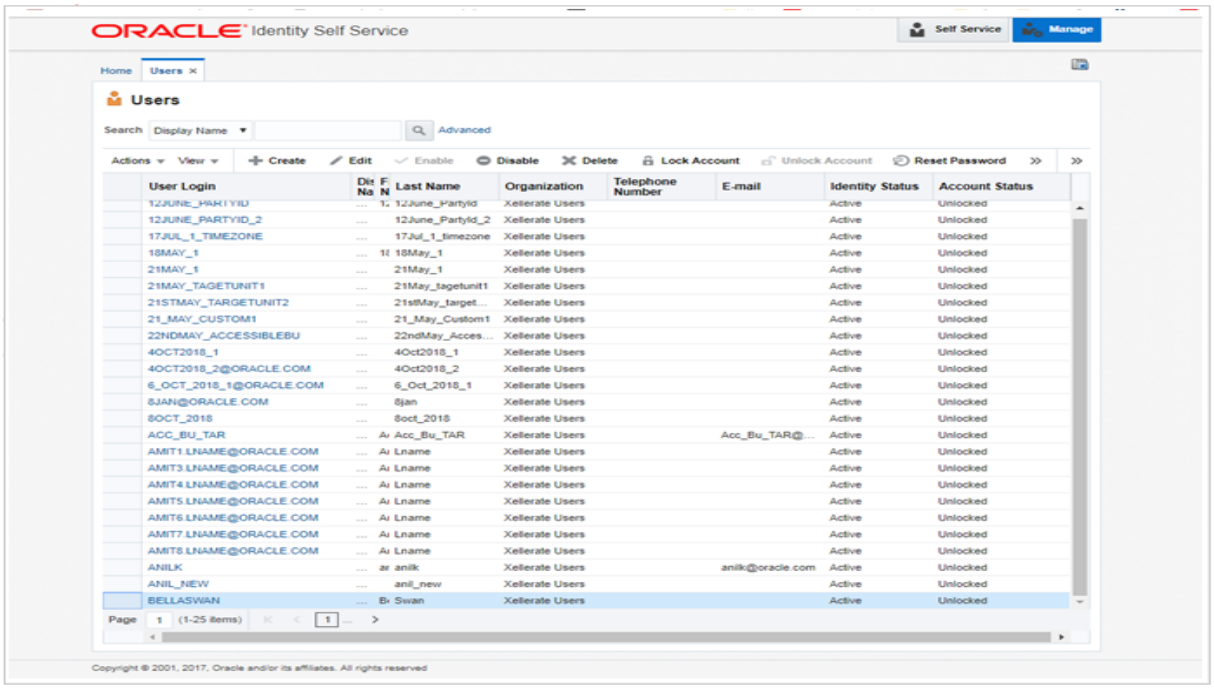
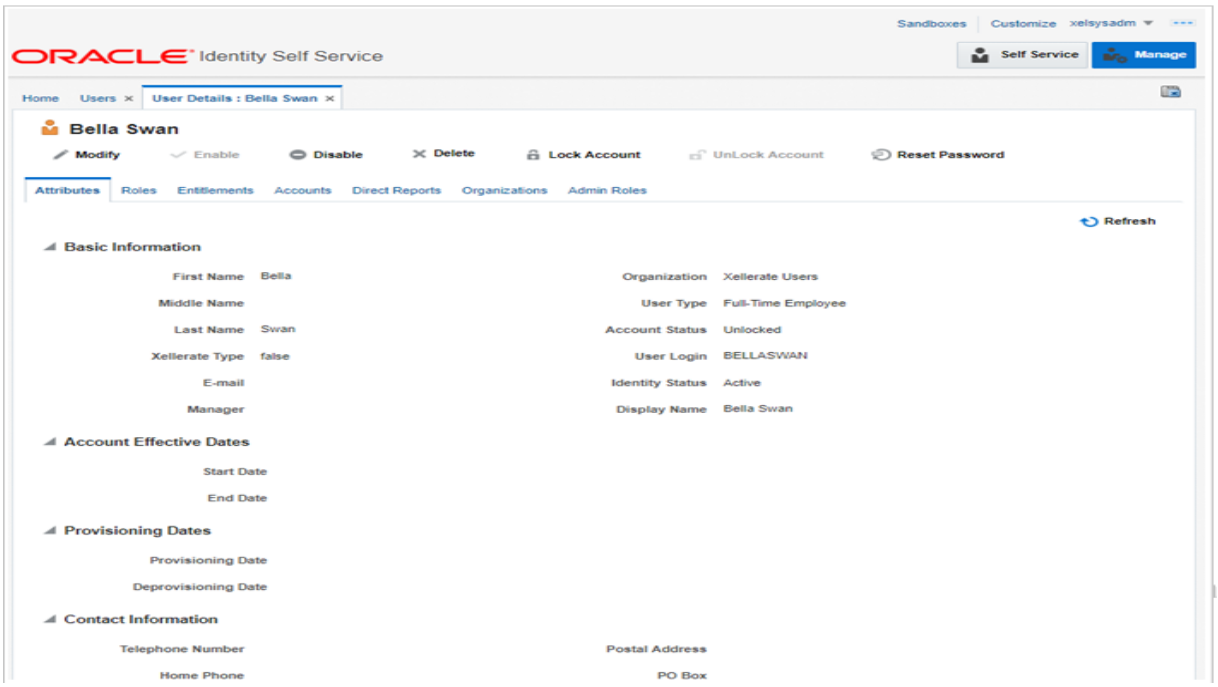


Figure 4–15 View User Details



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 Verification

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

6.1 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.

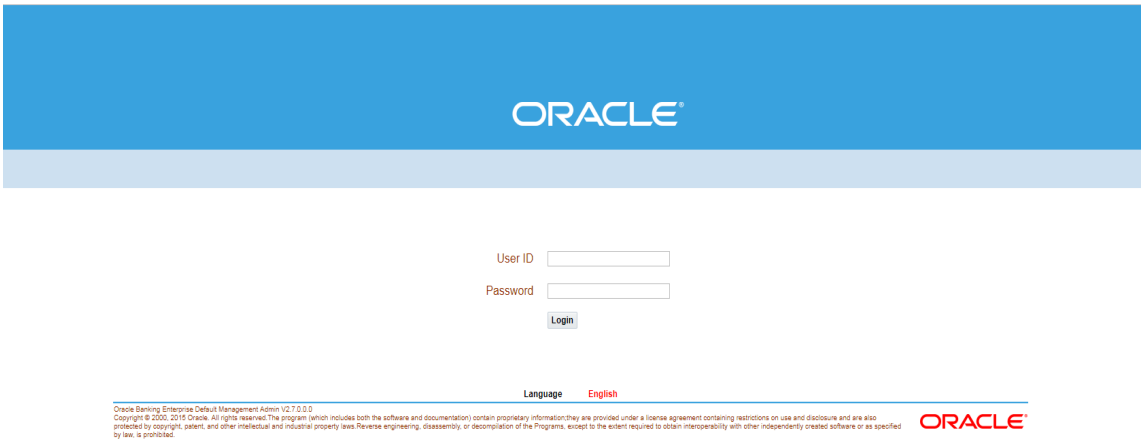
6.2 Verify Users in Native Collections Admin Application

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

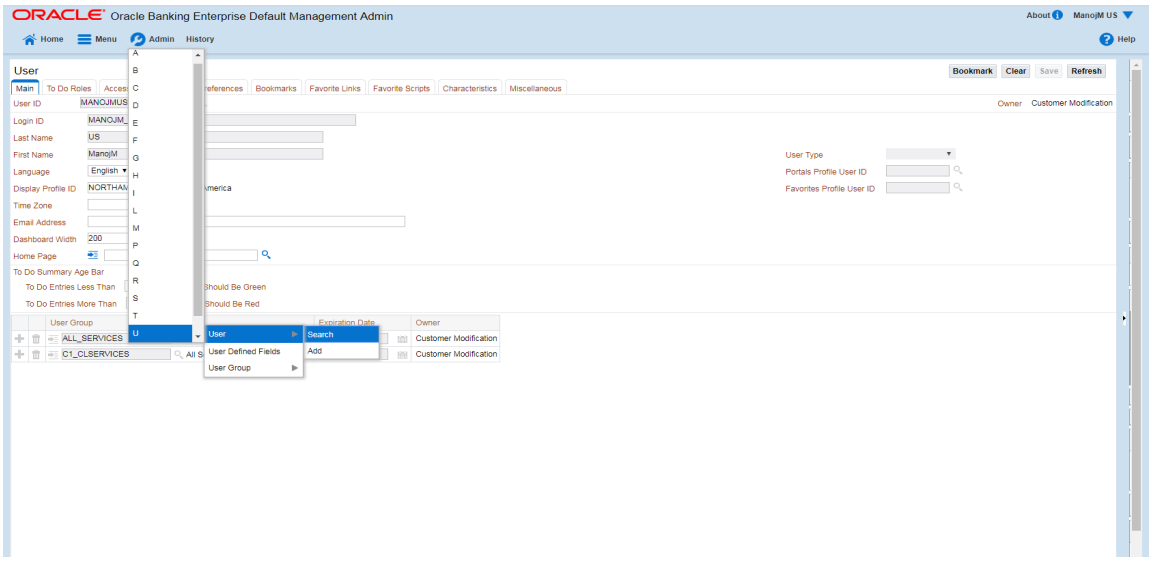
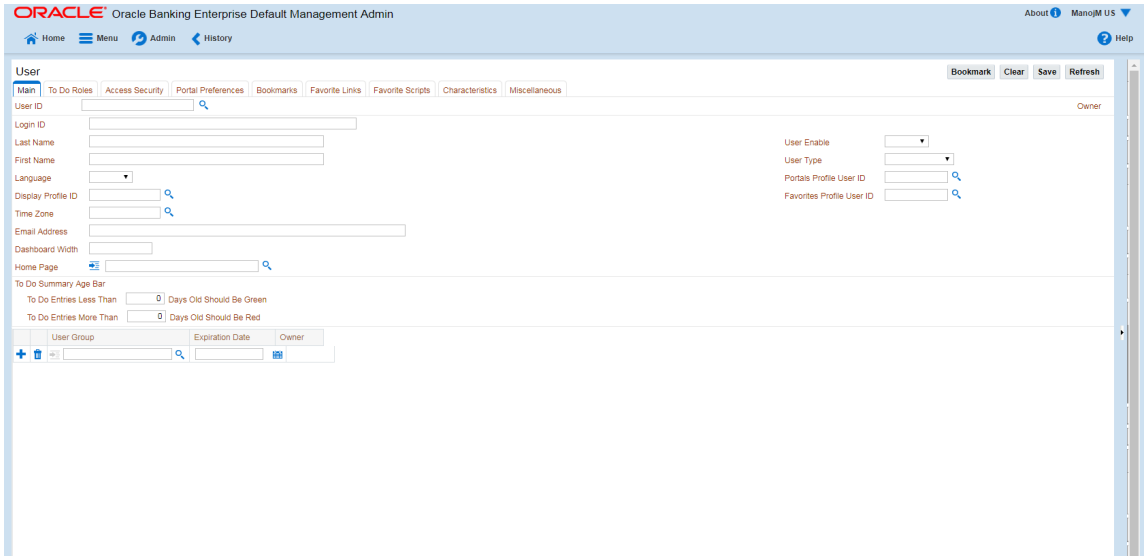


Figure 5–4 User Screen - Main Tab



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

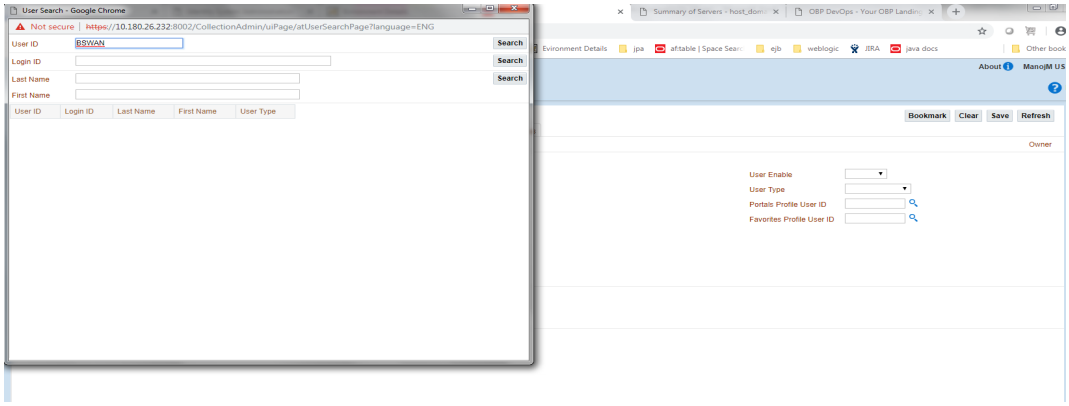
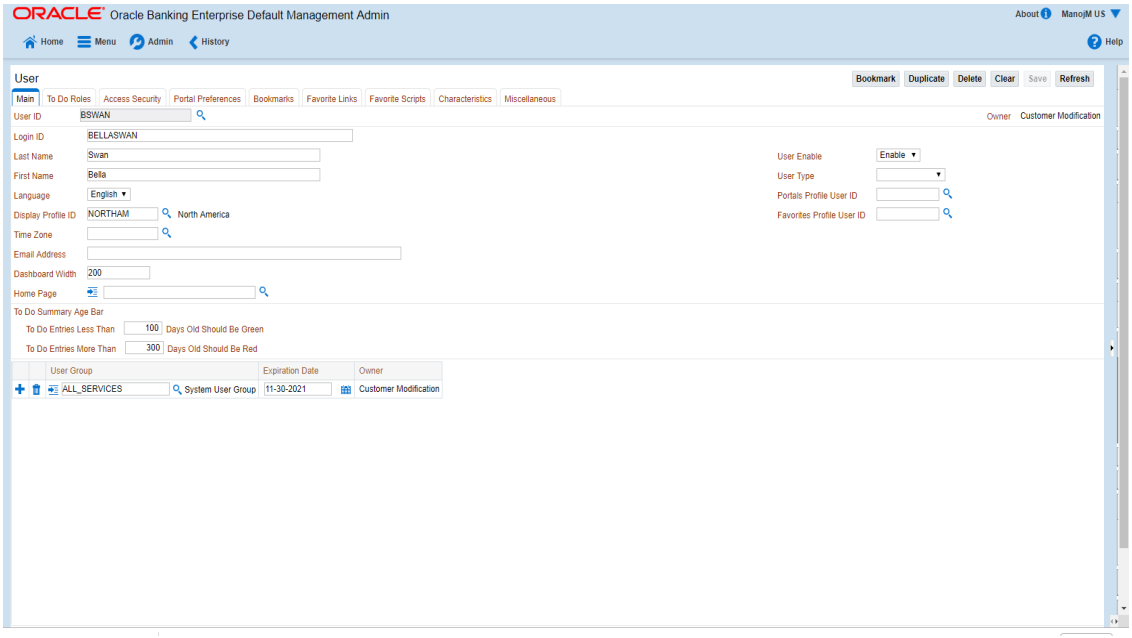


Figure 5–6 Search Result in User screen



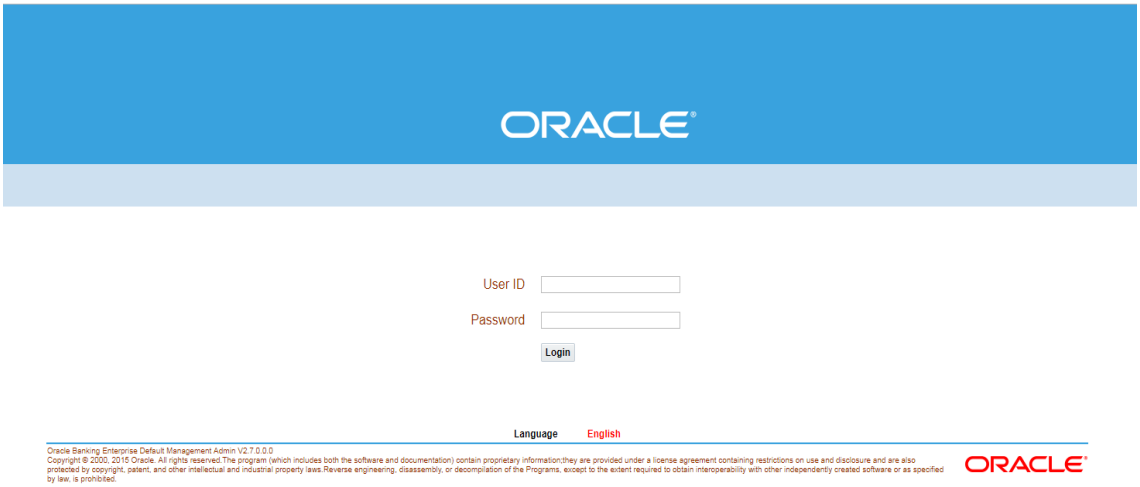
6.3 Create Users in Collections Admin Application

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

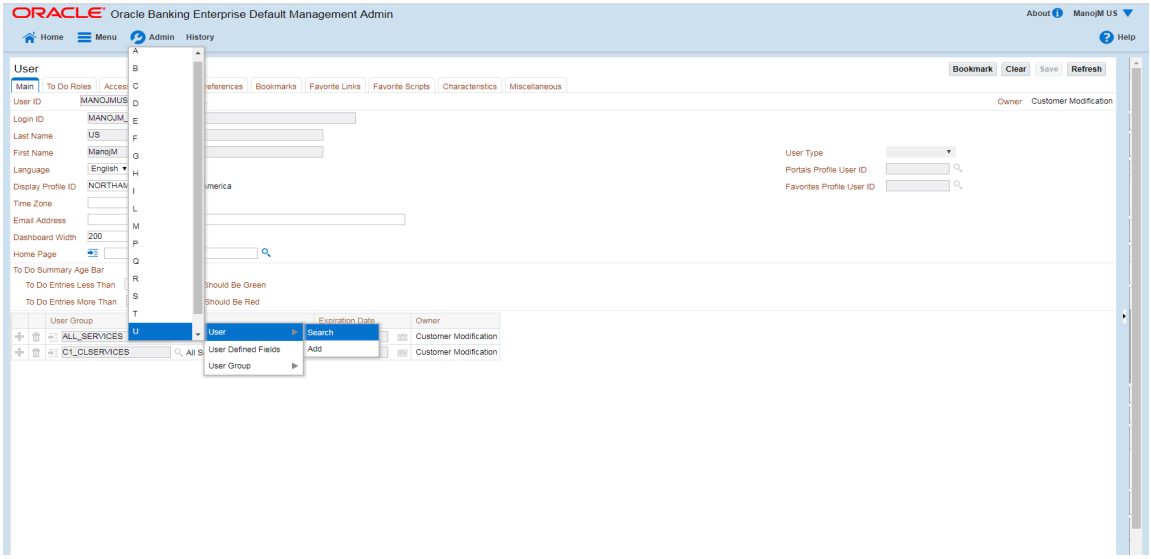
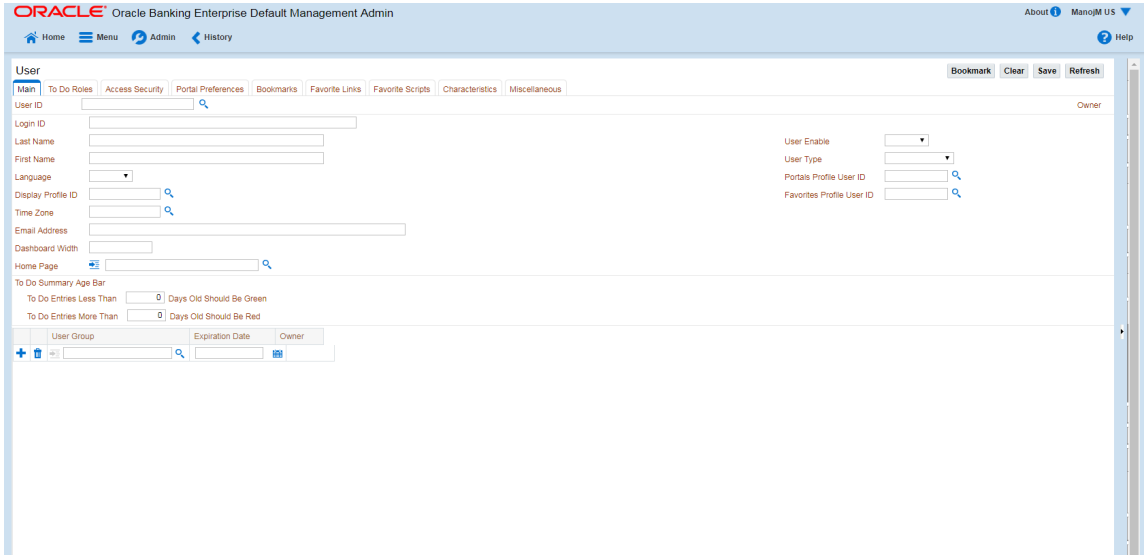


Figure 5–9 User Screen - Main Tab

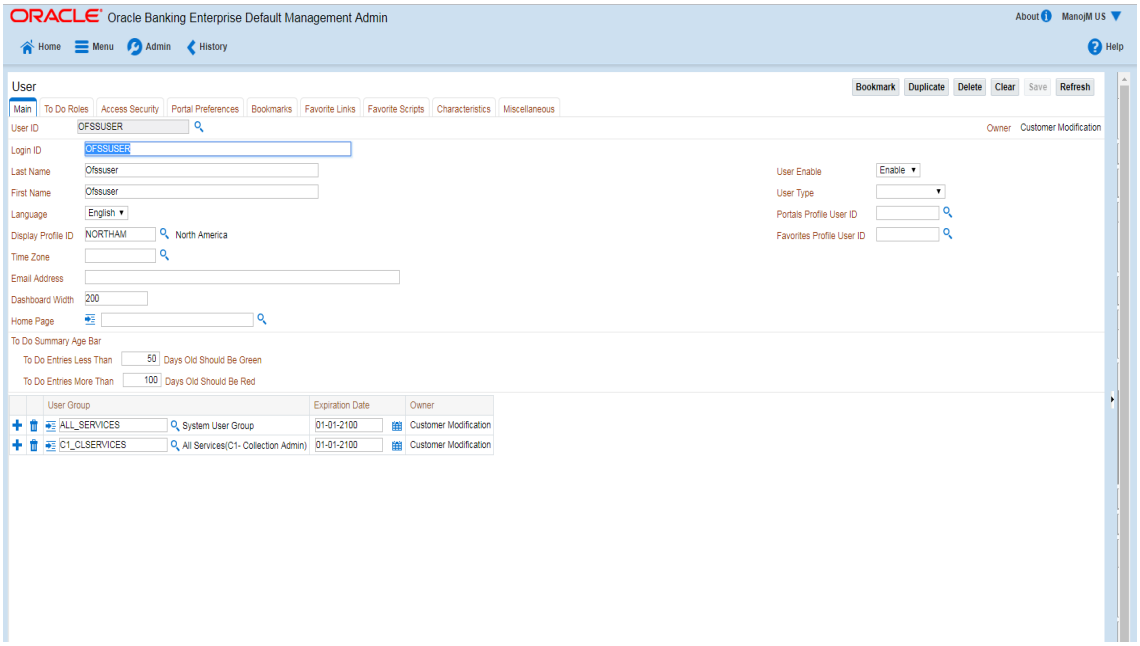


3. In the User page, enter the following details in the respective fields:
   - **User Id:** OIMOBPCO
   - **Login Id:** OIMOBPCOLL
   - **First Name:** OIMOBPCOLL
   - **Last Name:** OIMOBPCOLL
   - **Language:** English

- **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.