

Oracle® Banking Platform Collections

User Provisioning Guide

Release 2.6.2.0.0

E95189-01

May 2018

Oracle Banking Platform Collections User Provisioning Guide, Release 2.6.2.0.0

E95189-01

Copyright © 2011, 2018, Oracle and/or its affiliates. All rights reserved.

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.

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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.

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

This software or hardware and documentation may provide access to or information on 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. 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.

Contents

Preface	12
Audience	12
Documentation Accessibility	12
Organization of the Guide	12
Related Documents	13
Conventions	13
1 About this Guide	15
2 Introduction	17
3 Configuration	19
3.1 Prerequisites	19
3.2 Create OBP Collections System User	21
3.3 OIM Configuration	21
3.3.1 Configure Collections Jar files	21
3.3.2 Configure Collections User Groups	22
3.3.3 Collection 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 Import Collections Configuration	31
3.3.5 Verify and Override Date Format Lookup	37
3.3.6 Add Process Trigger	39
3.3.7 Create Collections Role	43
3.3.8 Create Access Policy	48

3.3.9 Create Form Associated with Application Instance	61
3.3.10 Create Application Instance	65
3.3.11 Security Configuration	73
3.4 OBP-Collections Configuration	76
4 User Fields and Constraints	79
4.1 User Fields Provisioned From OIM	79
5 Functional Flow	81
5.1 Add Users in Collections	81
5.2 Modify Users in Collections	93
5.3 Delete Users in Collections	101
6 Verification	105
6.1 Verification of OIM Configuration	105
6.2 Verify Users in Native Collections	106
6.3 Create Users in Collections	108

List of Tables

Table 3–1 OBP Collection Connection Parameters	19
Table 3–2 Collection Jar files	21
Table 3–3 Create Sandbox Parameters	28
Table 3–4 Collections User Provisioning Artifacts	31
Table 3–5 List of variables	41
Table 3–6 Code Key details	42
Table 3–7 UD_COLL_USR process form fields	64
Table 4–1 OBP Collections User Fields	79
Table 5–1 Response Codes for a Rejected Create User Task	89
Table 5–2 Tasks involved while modifying User fields	98
Table 6–1 OID schema attributes	105

List of Figures

Figure 3–1 Search and Select - Lookup Type	22
Figure 3–2 Search and Select - Lookup Type	23
Figure 3–3 Create Lookup Type - Clicking icon	24
Figure 3–4 Create Lookup Type - Dialog box	24
Figure 3–5 Enter Lookup Values	25
Figure 3–6 Edit Lookup Type	25
Figure 3–7 Lookup Type Creation	26
Figure 3–8 Oracle Identity System Administration - Sandbox tab	27
Figure 3–9 Manage Sandbox	27
Figure 3–10 Create Sandbox	27
Figure 3–11 Create Sandbox Dialog Box	28
Figure 3–12 Create Sandbox Parameters	28
Figure 3–13 Sandbox Creation Confirmation	28
Figure 3–14 Available Sandbox	29
Figure 3–15 Activate Sandbox	29
Figure 3–16 Activate Sandbox: Active	29
Figure 3–17 Deactivate Sandbox	30
Figure 3–18 Post Deactivating Sandbox	30
Figure 3–19 Publish Sandbox	30
Figure 3–20 Published Sandbox	30
Figure 3–21 System Management - Import	32
Figure 3–22 Deployment Manager - Import Screen	32
Figure 3–23 Deployment Manager - File Preview Dialog Box	33
Figure 3–24 Deployment Manager - Cancel Substitution Dialog Box	33

Figure 3–25 Deployment Manager - IT Resource Instance Data	34
Figure 3–26 Deployment Manager - Skip Parameter Value	34
Figure 3–27 Deployment Manager - View Selections	35
Figure 3–28 Deployment Manager - Import	36
Figure 3–29 Import Confirmation	36
Figure 3–30 Import Confirmation Dialog Box	36
Figure 3–31 Entering Lookup Value	37
Figure 3–32 Lookup Types Criteria Match	38
Figure 3–33 Oracle Identity System - System Administration	39
Figure 3–34 Search and Select - Lookup Type	39
Figure 3–35 Search Lookup Type	40
Figure 3–36 Edit Lookup Type	40
Figure 3–37 Adding a Lookup Type	41
Figure 3–38 Edit Lookup Types	42
Figure 3–39 Verifying Process Task Name	43
Figure 3–40 Oracle Identity Self Service	43
Figure 3–41 Create Role	44
Figure 3–42 Create Role - Values	44
Figure 3–43 Create Role - Attributes Tab	45
Figure 3–44 Create Role - Members Tab	45
Figure 3–45 Create Role - Add Rule	45
Figure 3–46 Create Role - Build Expression	46
Figure 3–47 Create Rule - Add	46
Figure 3–48 Create Rule - Select Operand Values	47
Figure 3–49 Create Rule - Build Expression	47
Figure 3–50 Create Rule - Build Expression Updated	48

Figure 3–51 Create Access Policy - Access Policies	49
Figure 3–52 Create Access Policy	49
Figure 3–53 Create Access Policy - Continue	50
Figure 3–54 Create Access Policy - Select Resources	51
Figure 3–55 Create Access Policy - Selected Resource	51
Figure 3–56 Create Access Policy - Select Resource	52
Figure 3–57 Select Resources - Process Details	52
Figure 3–58 Selecting Instance Name	53
Figure 3–59 Create Access Policy - Server Instance	54
Figure 3–60 Create Access Policy - Select Revoke or Disable Flag	54
Figure 3–61 Create Access Policy - Continue	55
Figure 3–62 Create Access Policy - Add	55
Figure 3–63 Create Access Policy - Select Roles	56
Figure 3–64 Create Access Policy - Verify Access Policy Information	56
Figure 3–65 Identity Self Service- Manage Tab	57
Figure 3–66 Roles Tab	57
Figure 3–67 List of Roles	58
Figure 3–68 Access Policy	58
Figure 3–69 Add Access Policy	59
Figure 3–70 Search Access Policy	59
Figure 3–71 Add Selected Policy	60
Figure 3–72 Apply Policy	60
Figure 3–73 Verify Policy	61
Figure 3–74 Create Form - Form Designer	62
Figure 3–75 Create Form - Resource Type	62
Figure 3–76 Create Form - Resource Type (Collection User)	63

Figure 3–77 Create Form Resource Type - Available Form Fields	63
Figure 3–78 Create Form Resource Type - Create	64
Figure 3–79 Manage Collections User Form	65
Figure 3–80 Creating Application Instance	65
Figure 3–81 Creating Application Instance - Search	66
Figure 3–82 Creating Application Instance - Delete	66
Figure 3–83 Creating Application Instance - Confirm Delete	67
Figure 3–84 Creating Application Instance - Delete Message	67
Figure 3–85 Creating Application Instance - System Management Tab	67
Figure 3–86 Creating Application Instance - Predefined Scheduled Jobs	68
Figure 3–87 Creating Application Instance - Mode Selection (Delete)	69
Figure 3–88 Creating Application Instance - Mode Selection (Revoke)	70
Figure 3–89 Creating Application Instance - Catalog Synchronization	71
Figure 3–90 Creating Application Instance - Create	71
Figure 3–91 Creating Application Instance - Attributes Tab	72
Figure 3–92 Creating Application Instance - Save	73
Figure 3–93 Creating Application Instance - Created Successfully	73
Figure 3–94 Create Lookup Type	74
Figure 3–95 Farm_OIM Domain	75
Figure 3–96 OIM Domain - Create Key	76
Figure 3–97 Collections Configuration	77
Figure 4–1 Create User - Mandatory and Optional Attributes	80
Figure 5–1 Oracle Identity Self Service Login Screen	81
Figure 5–2 OID User Screen	82
Figure 5–3 Create User Screen	82
Figure 5–4 Search and Select Organization	83

Figure 5–5 Create User	84
Figure 5–6 User Created	85
Figure 5–7 Verifying User name	85
Figure 5–8 View Account Summary	86
Figure 5–9 Modifying Account	87
Figure 5–10 Selecting Collections User Group	87
Figure 5–11 Submitting Request	88
Figure 5–12 Viewing Updated User Details	88
Figure 5–13 Viewing User Provisioning Tasks	89
Figure 5–14 Task Details	90
Figure 5–15 Status of User Provisioning to Collections	91
Figure 5–16 Open Provisioning Tasks	92
Figure 5–17 Manual Completion - Create User Provisioning Task	93
Figure 5–18 Searching User	94
Figure 5–19 Detailed Information about the User	94
Figure 5–20 Modify User Confirmation	95
Figure 5–21 Viewing Modified and Provisioned User Details	95
Figure 5–22 Catalog page	96
Figure 5–23 Submitting Request	96
Figure 5–24 Viewing Changes	97
Figure 5–25 Viewing User Provisioning Task	97
Figure 5–26 User Provisioning Status	99
Figure 5–27 Failed provisioning tasks	99
Figure 5–28 Task confirmation dialog box	100
Figure 5–29 Manual Completion - Create User Provisioning Task	102
Figure 5–30 Searching Users To Delete	102

Figure 5–31 View User Details	103
Figure 5–32 Delete User Screen	103
Figure 6–1 Viewing IT Resource Details and Parameters	105
Figure 6–2 OBP Collections Native Login screen	106
Figure 6–3 User Screen - User Navigation	107
Figure 6–4 User Screen - Main Tab	107
Figure 6–5 Searching Particular User	108
Figure 6–6 Search Result in User screen	108
Figure 6–7 OBP Collections Native Login screen	109
Figure 6–8 OBP Collections native - User Navigation	109
Figure 6–9 OBP Collections native - Main Tab	110
Figure 6–10 User Screen	111

Preface

This document covers the detailed configuration of OIM that is required to integrate with Collections.

Also, it covers functional flow and detail configuration required for user provisioning in Collections on default OIM installation. 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 for OBP Collections.

[Chapter 4 User Fields and Constraints](#)

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

[Chapter 5 Functional Flow](#)

This chapter provides information on user provisioning activities.

[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 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.
<code>monospace</code>	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 Enterprise Collections

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 called Oracle Internet Directory (OID), which is used for authentication and authorization purpose.

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

Oracle Identity Manager (OIM) is used to provision users in Collections when they are created in OBP.

3 Configuration

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

3.1 Prerequisites

Following is the list of prerequisites for configuring OIM:

1. You must install the following software:
 - Weblogic Server 12.2.1.2.0
 - SOA Suite 12.2.1.2.0
 - IAM Suite 11gR2 PS2 (11.1.2.3.0)
 - RCU 12.1.0.2.0
2. You must have administrative access to the following:
 - OIM Design Console
 - 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. Values of following fields are known:

Table 3–1 OBP Collection Connection Parameters

Field Name	Value	Description
webserviceUrl	<a href="http://<Host>:<Port>/com.ofss.fc.webservice/services/collection/ORMBUserProvisioningApplicationService">http://<Host>:<Port>/com.ofss.fc.webservice/services/collection/ORMBUserProvisioningApplicationService Where Host & Port: IP and Port of HOST Server where OBP Collections is deployed.	Host server webservice URL pointing to Collections (ORMB) User Provisioning service
sessionUserId	OBP Administrative user having access to Collections services. Also, same User must be present in Collections (ORMB) database as Administrative User.	

3.1 Prerequisites

Field Name	Value	Description
bankCode		Bank Code
transactionBranch		Transaction Branch
channel		Channel
marketEntity		Market Entity
businessUnit		Business Unit
isSecurityEnabled	true/false	This flag is used to enable security through OWSM policies. Provide value based on environment configuration.
securityParamLookup		Lookup containing client security policy properties in the form of key and value. Provide values as per client policy configured.
securityPolicy		Client security policy name as per service policy configured.

5. Check following artifacts are available as part of Collections release bundle:

- com.ofss.fc.extxface.wsdl.client.jar
- com.ofss.fc.extxface.oim.jar
- collections_oim_export.xml

3.2 Create OBP Collections System User

The following configuration is to create Collections System User for OIM. System User is required to authenticate OIM Collections 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 Collections using Collections native admin UI. Assign **CLNHOSTUSER** Group to User, to provide minimum access of Collections native admin screen. For more information, see {Color}Section 6.3, "Create Users in Collections."{Default ¶ Font}

3.3 OIM Configuration

This section provides information on OIM Configuration.

3.3.1 Configure Collections Jar files

Below is sample configuration for OIM JavaTask and ThirdParty jar. Copy below listed Collections jars for user provisioning to the specified location.

Table 3–2 Collection Jar files

Artifact	Location	Description
com.ofss.fc.extxface.wsdl.client.jar	<IDM_HOME>/server/apps/oim.ear/APP-INF/lib <IDM_HOME>/server/ThirdParty	Web service client to invoke Collections service to provision User. It should be treated as ThirdParty OIM jar . To ensure Collections java files exists, explode jar and check if package structure com\ofss\fc\extxface\app\collection\service\userprovisioning is present.
com.ofss.fc.extxface.oim.jar	<IDM_HOME>/server/JavaTasks	This jar file contains java class to create, update and delete User. It should be treated as OIM JavaTask jar . To ensure Collections java files exists, explode jar and check if package structure com\ofss\fc\extxface\oim\collection is present.

3.3.2 Configure Collections User Groups

As part of day zero configurations, administrators must add all Collections User Group to lookup definition LOOKUP.ORMB.USER.GROUPS in OIM, except Collections default User Group.

To know more about day zero configuration, see Oracle Banking Platform Collections Day Zero Setup Guide.

1. Log in to Oracle Identity System Administration. In the left pane, under Configuration, click **Lookups**.

Figure 3–1 Search and Select - Lookup Type



The **Search and Select: Lookup Type** window is displayed.

Figure 3–2 Search and Select - Lookup Type

Search and Select: Lookup Type

Search

Match All Any

Meaning

Code

Description

Meaning	Code	Description
No data to display.		

Lookup Values

Meaning	Code	Enabled	Sequence	Description
No data to display.				

2. Click **Create Lookup Type** icon on the toolbar. The **Create Lookup Type** dialog box is displayed.

Figure 3–3 Create Lookup Type - Clicking icon

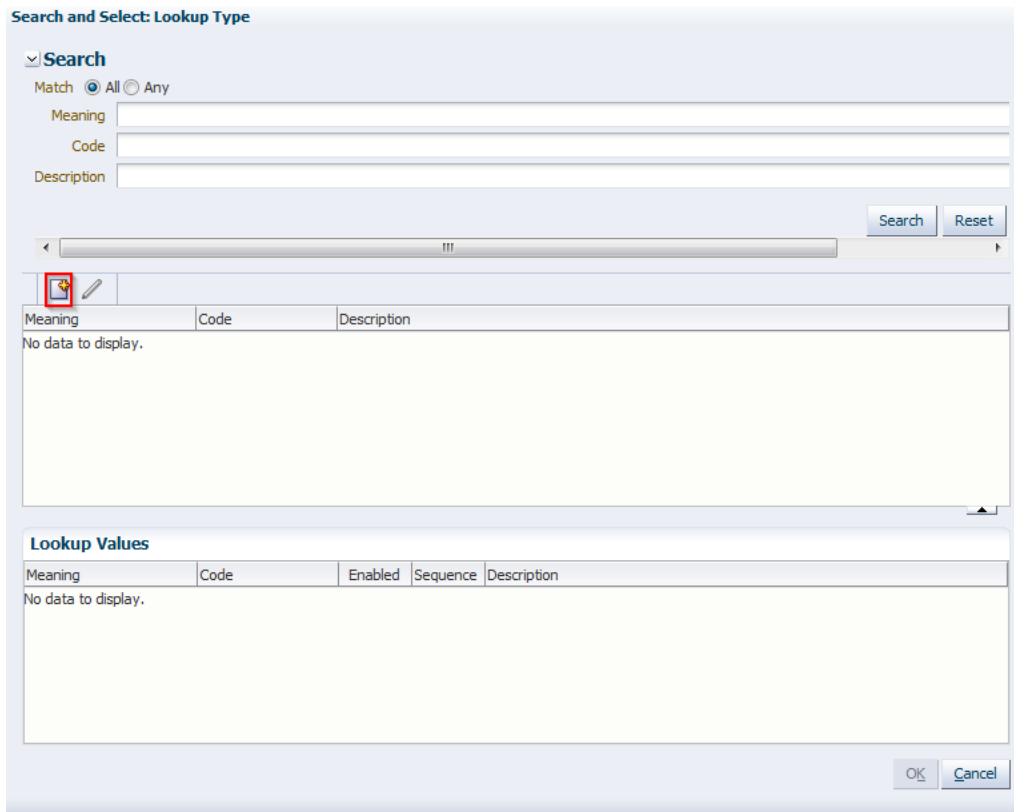
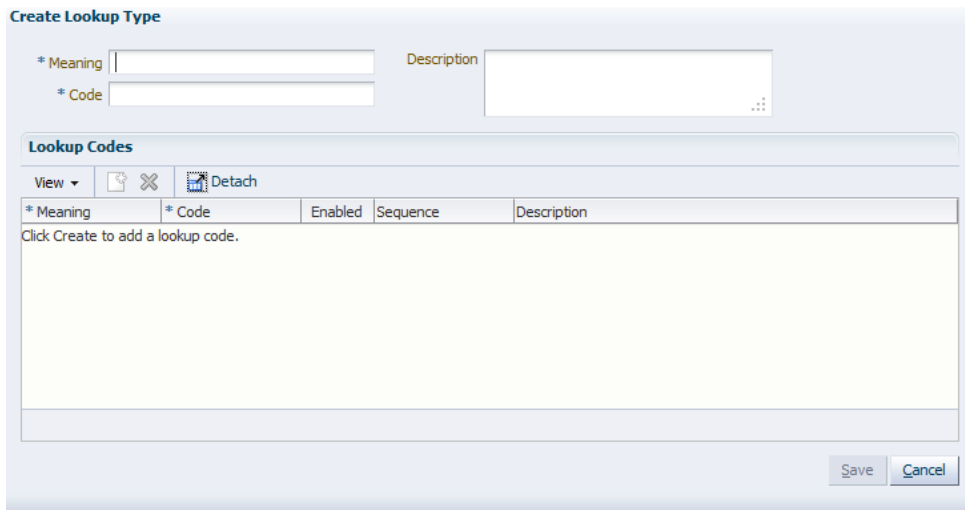


Figure 3–4 Create Lookup Type - Dialog box



3. Specify the following values:
 - **Meaning:** LOOKUP.ORMB.USER.GROUPS
 - **Code:** LOOKUP.ORMB.USER.GROUPS

- **Description:** Collections User Groups

Figure 3–5 Enter Lookup Values

Create Lookup Type

* Meaning: LOOKUP.ORMB.USER.GROUPS Description: Collections User Groups
 * Code: LOOKUP.ORMB.USER.GROUPS

Lookup Codes

View ▾ [Create] [Remove] [Detach]

* Meaning	* Code	Enabled	Sequence	Description
Click Create to add a lookup code.				

Save Cancel

- In the Lookup Codes section, click the **Create Lookup Code** icon. A row is added to the Lookup Codes section in which you can specify valid Collections ORMB User Group in **Meaning** and **Code**.
 - **Meaning:** C1_BSERVICES (This is a sample value, add values provided).
 - **Code:** C1_BSERVICES (This is a sample value, add values provided).
 - **Enabled:** Select the check box if you want to enable the lookup code.
 - **Sequence:** Number to specify a sequence for the lookup code. A lower number indicates higher priority. For example, 1 indicates highest priority

Figure 3–6 Edit Lookup Type

Edit Lookup Type

* Meaning: LOOKUP.ORMB.USER.GROUPS Description: Collections User Groups
 Code: LOOKUP.ORMB.USER.GROUPS

Lookup Codes

View ▾ [Create] [Remove] [Detach]

* Meaning	* Code	Enabled	Sequence	Description
C1_BSERVICES	C1_BSERVICES	<input checked="" type="checkbox"/>	1	

Save Cancel

- Similarly, repeat steps (step 4) to create as many lookup codes you want. To remove a lookup code, you can select the row for the code and click the Remove Lookup Code icon.

Note

Code should be a valid Collections User Group, else it would be treated as invalid while provisioning. The value in the Meaning field will be shown to user on Create User form.

- Click **Save**. The lookup type is created.

Figure 3–7 Lookup Type Creation

Search and Select: Lookup Type

Search

Match All Any

Meaning

Code

Description

Search Reset

Meaning	Code	Description
Audit.UserProfile.CustomP	Audit.UserProfile.Cus	
Catalog Risk Level	Lookup.Catalog.Risk.	
Global.Lookup.Language	Global.Lookup.Langua	
Global.Lookup.Region	Global.Lookup.Region	
LOOKUP.ORMB.USER.GRC	LOOKUP.ORMB.USER	Collections User Groups
Lookup.ACT_PROCESS_TR	Lookup.ACT_PROCES	
Lookup.Adapter Factory.A	Lookup.Adapter Fact	

LOOKUP.ORMB.USER.GROUPS: Lookup Values

Meaning	Code	Enabled	Sequence	Description
C1_BSERVICES	C1_BSERVICES	<input checked="" type="checkbox"/>		

OK Cancel

Note

- Lookup definition LOOKUP.ORMB.USER.GROUPS values can be imported or exported using OIM Deployment Manager, useful when migrating from one environment to other.
- Restart of OIM server is required after updating the lookup definition.

3.3.3 Collection Sandbox

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

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

Figure 3–8 Oracle Identity System Administration - Sandbox tab

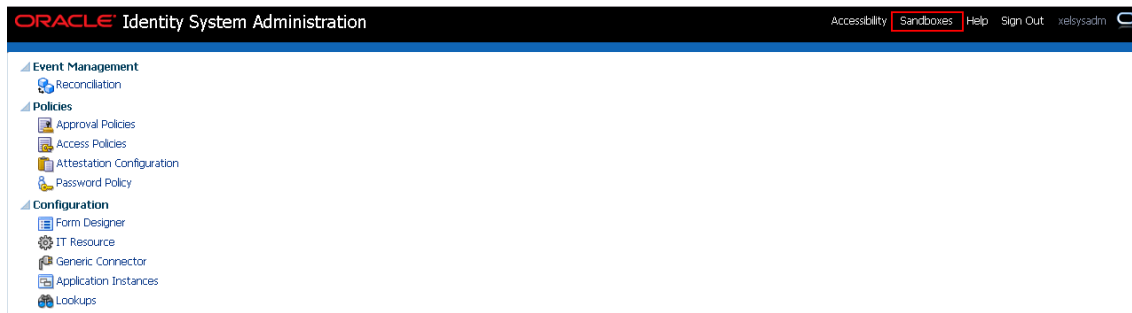
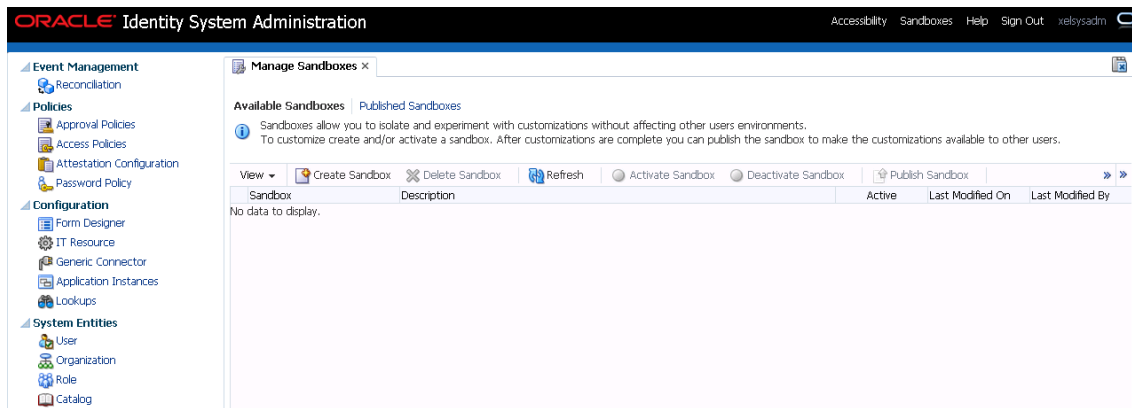


Figure 3–9 Manage Sandbox



3.3.3.1 Create Sandbox

To create a Sandbox, perform the following steps:

1. Click **Create Sandbox**. **Create Sandbox** page is displayed.

Figure 3–10 Create Sandbox

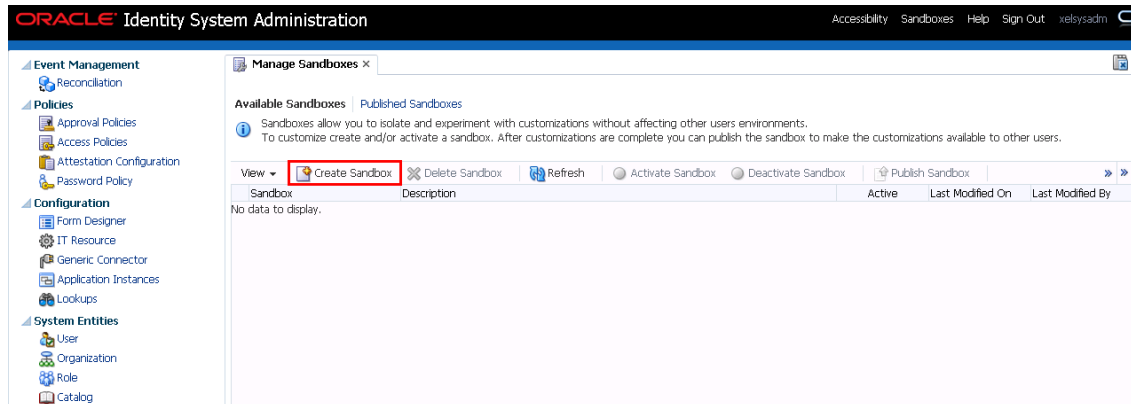


Figure 3–11 Create Sandbox Dialog Box



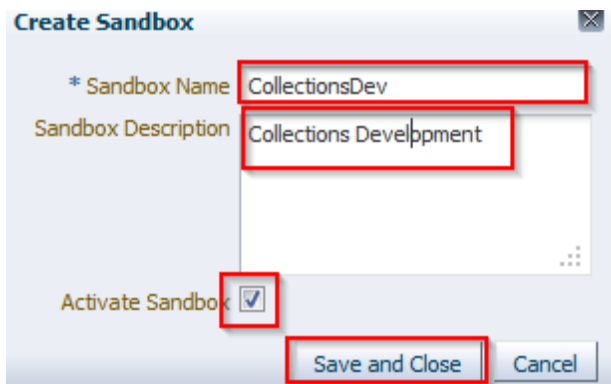
- Specify the following values:

Table 3–3 Create Sandbox Parameters

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

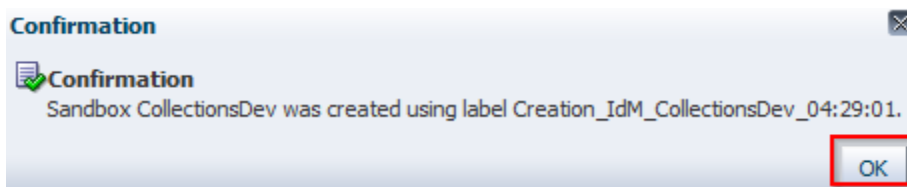
- Click **Save and Close**.

Figure 3–12 Create Sandbox Parameters



- Click **OK**. The **Confirmation** dialog box appears.

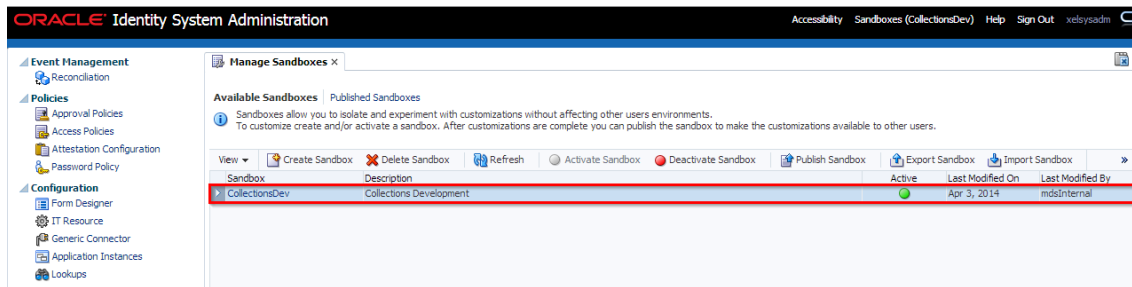
Figure 3–13 Sandbox Creation Confirmation



CollectionsDev sandbox is created and it is activated

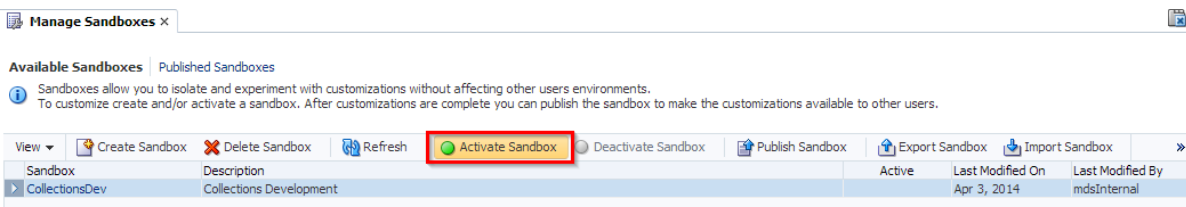
Note

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.

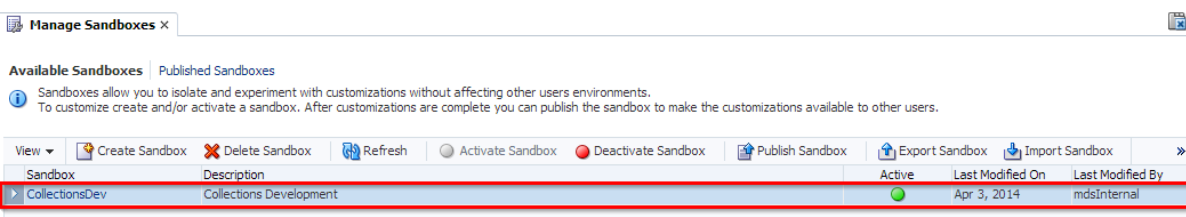
Figure 3–14 Available Sandbox**3.3.3.2 Activate Sandbox**

To activate a Sandbox, perform the following steps:

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

Figure 3–15 Activate Sandbox

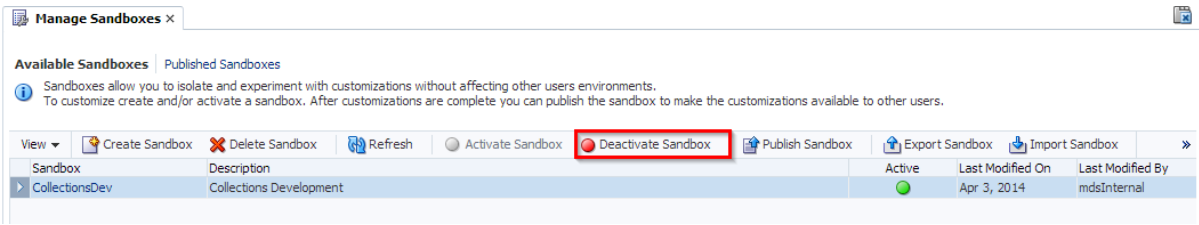
Sandbox is active now. It will be highlighted with green dot.

Figure 3–16 Activate Sandbox: Active**3.3.3.3 Deactivate Sandbox**

To deactivate a Sandbox, perform the following steps:

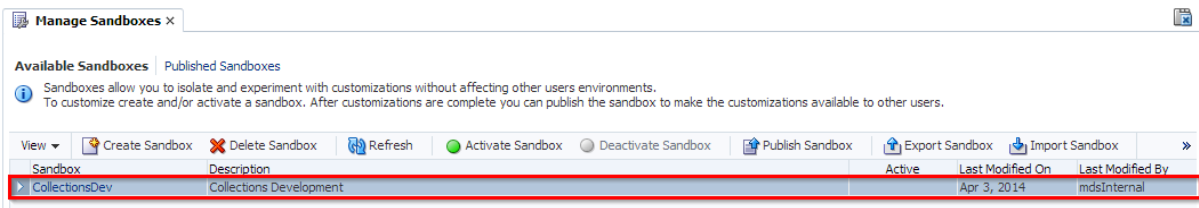
1. Select **CollectionsDev** sandbox and then click **Deactivate Sandbox** to deactivate sandbox.

Figure 3–17 Deactivate Sandbox



Sandbox is deactivated now.

Figure 3–18 Post Deactivating Sandbox

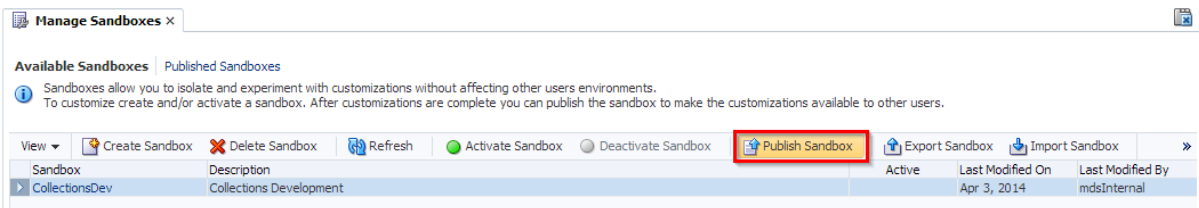


3.3.3.4 Publish Sandbox

To publish a Sandbox, perform the following steps:

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

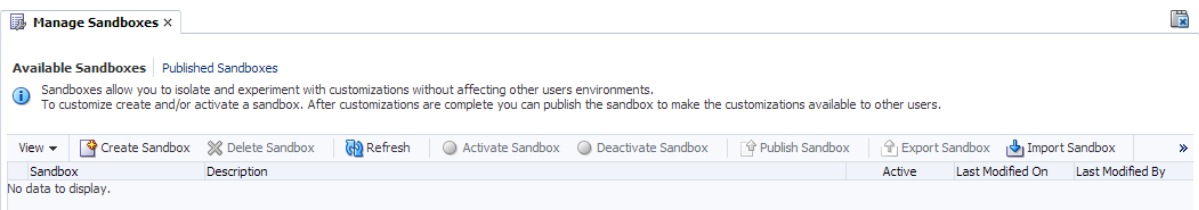
Figure 3–19 Publish Sandbox



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 3–20 Published Sandbox



3.3.4 Import Collections Configuration

Collections adapter configuration for User Provisioning must be imported. Below is the list of artifacts developed for Collections User Provisioning.

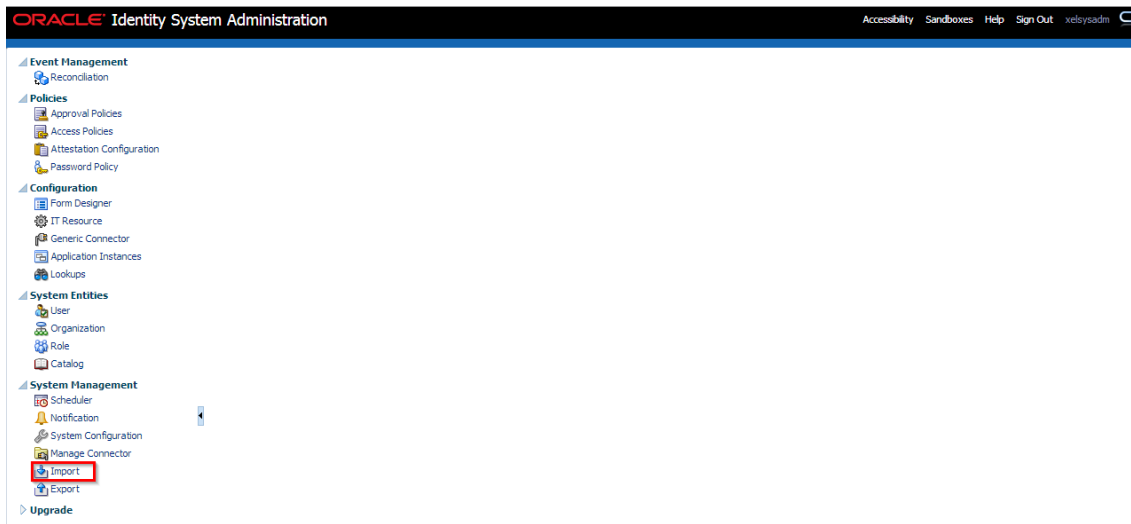
Table 3–4 Collections User Provisioning Artifacts

Artifact	Artifact Type	Description
Collections	Collections	It stores definition of connection parameters to connect OBP Collections system.
Collection Arguments	IT Resource Type	It stores parameters and its values required to make connection with OBP Collections. OIM uses this information to connect target Collections system.
Collections User Provisioning	Process Definition	This process definition contains process tasks for User provisioning Create User, Change First Name, Change Last Name, Change UserName, Change Email, Change End Date, Change Collections User Group and Delete User.
Collection User	Resource Object	This resource object is used for provisioning users in Collection. It contains Collections system details required for provisioning.
ORMB Create User	Task Adapter	This adapter is responsible to create user in Collections.
ORMB Update User	Task Adapter	This adapter is responsible to update user in Collections.
ORMB Delete User	Task Adapter	This adapter is responsible to delete user in Collections.
UD_COLL_USR	Process Form	This is Collections process form associated with Collections User Provisioning process. It holds relevant information about Collections User resource object.
CollectionsUserDetails	Pre-populate Adapter	The Adapter is used to pre-populate user details in the Collections resource form.

OBP Collections configuration can be imported in OIM by using deployment manager.

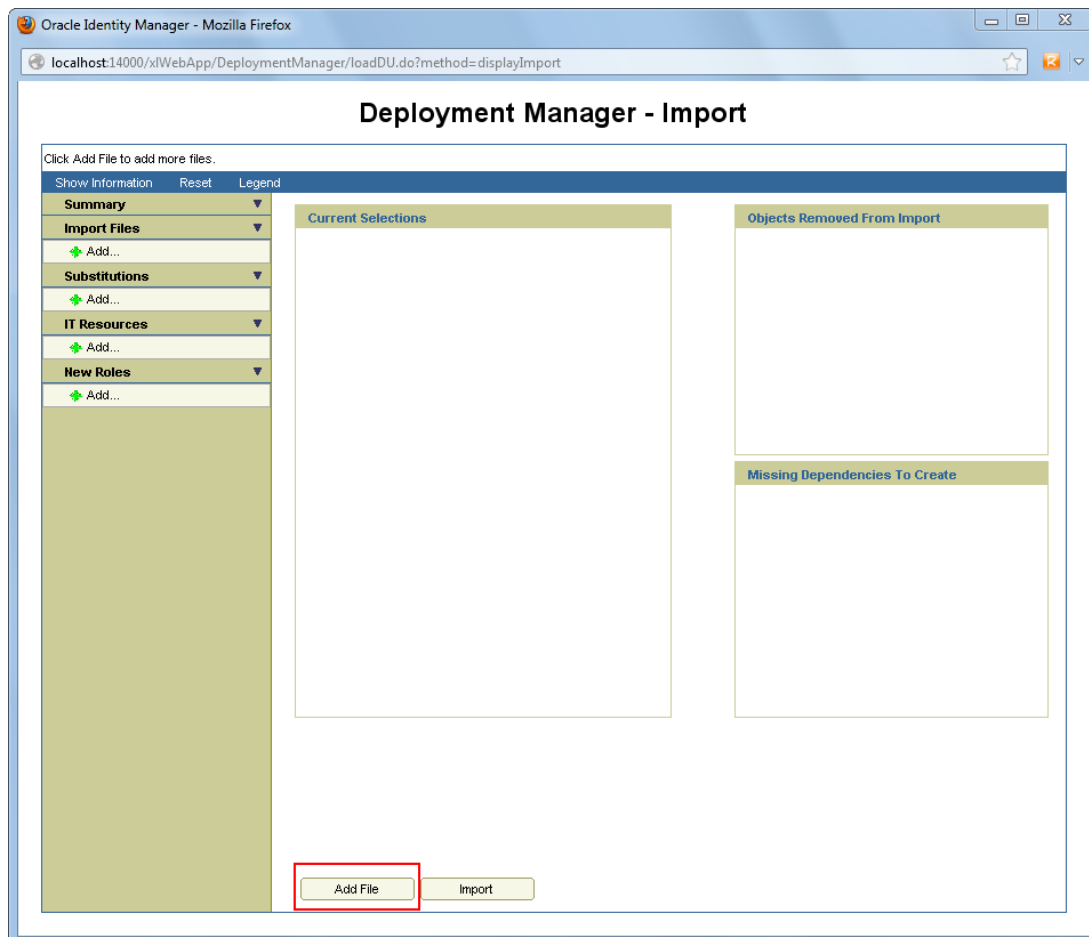
1. Log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Import**. The **Deployment Manager - Import** window is displayed.

Figure 3–21 System Management - Import



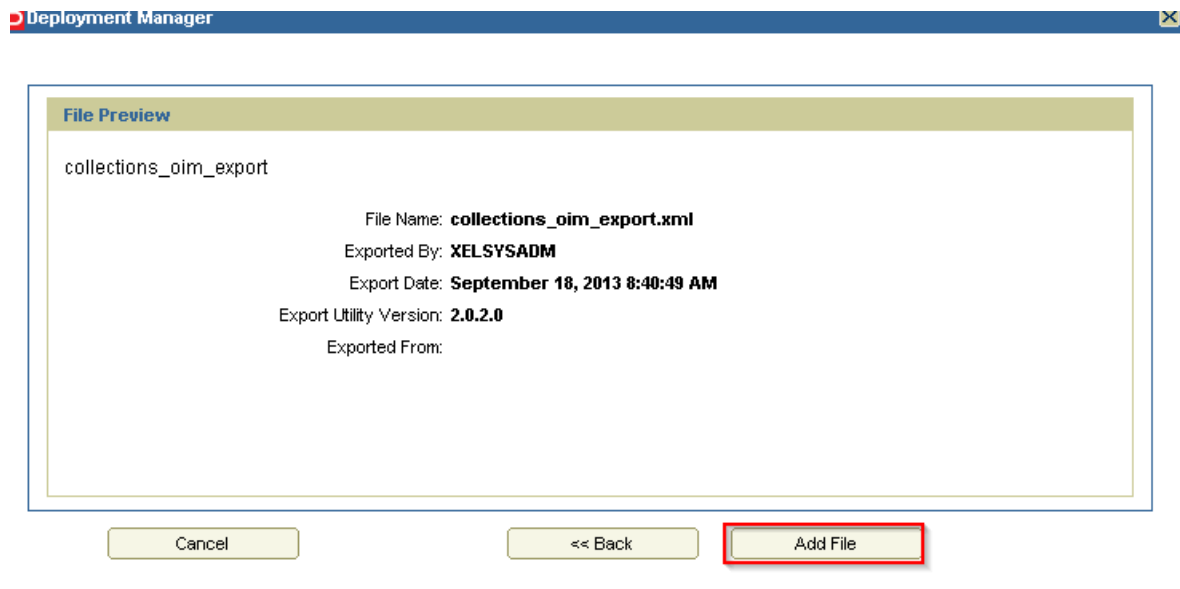
3. In the **Deployment Manager - Import** window, click **Add File** and open configuration file `collections_oim_export.xml` that is saved on your machine.

Figure 3–22 Deployment Manager - Import Screen



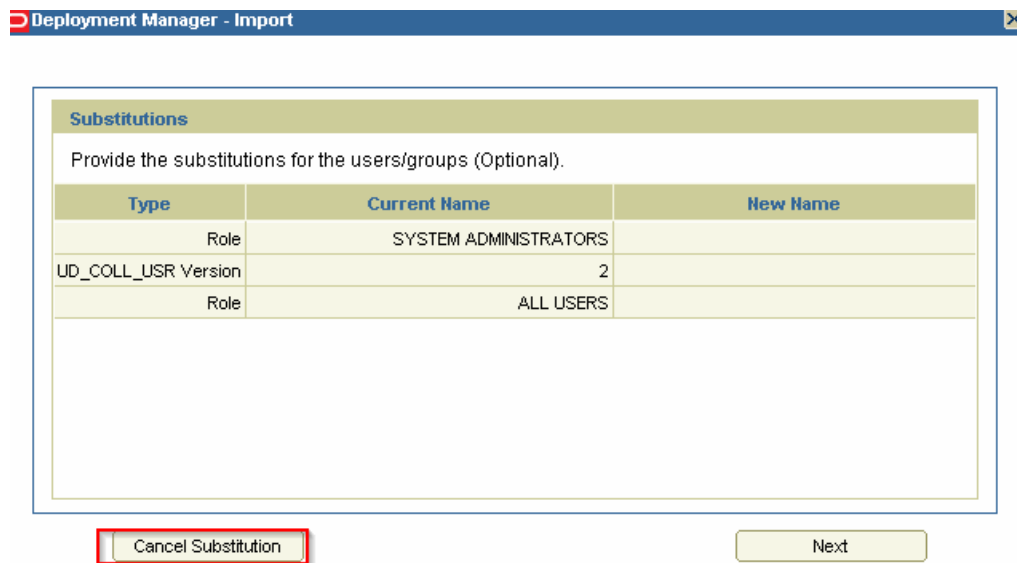
- The **Deployment Manager** dialog box opens with file name being imported. Click **Add File**.

Figure 3–23 Deployment Manager - File Preview Dialog Box



- Click **Cancel Substitution**.

Figure 3–24 Deployment Manager - Cancel Substitution Dialog Box

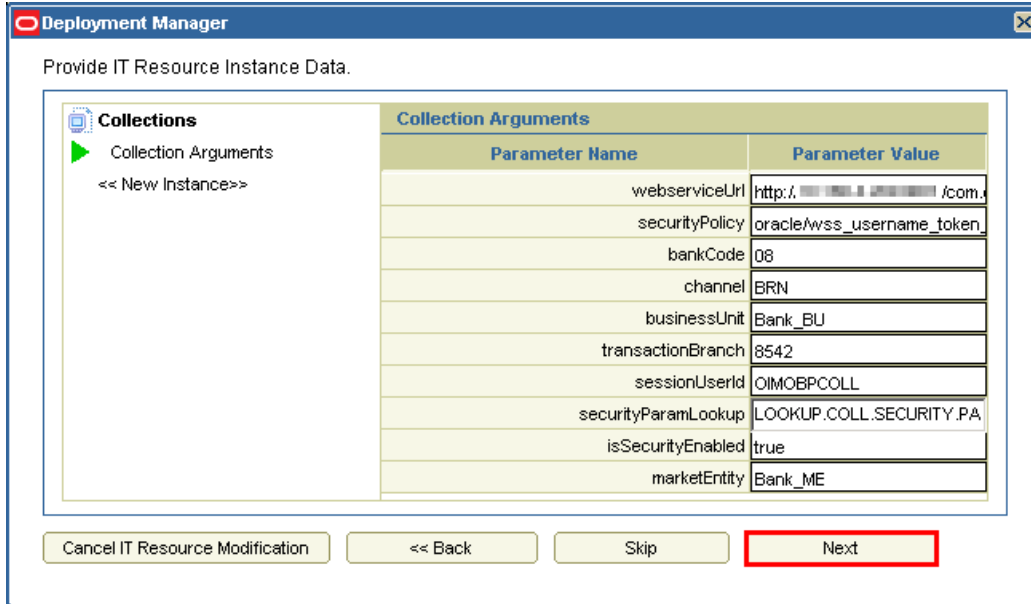


- Specify values for parameters in **Collection Arguments** section, see "Configuration" on page 19
- Click **Next**.

Note

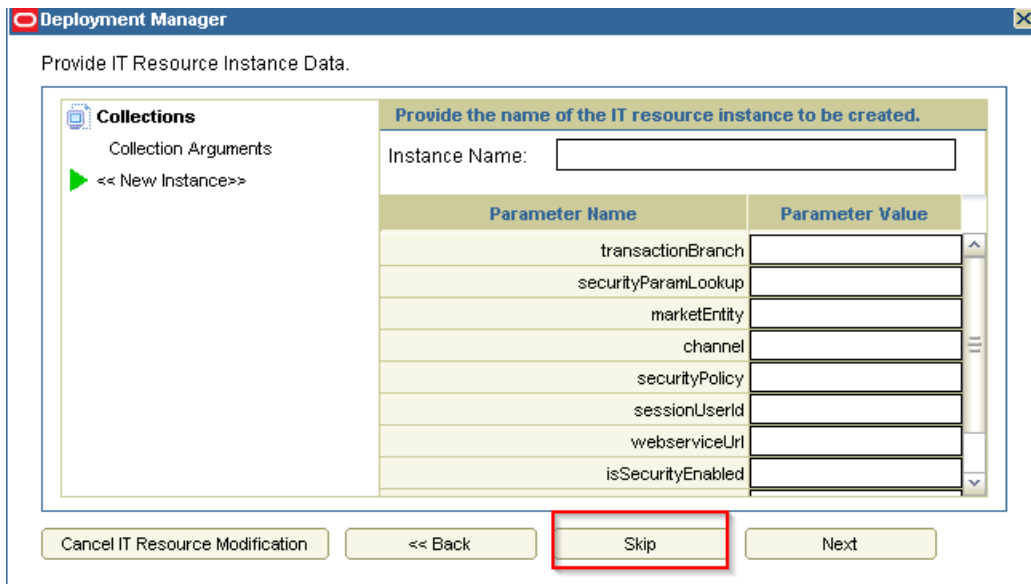
Parameter Value shown in image are sample values. Provide values as per your environment.

Figure 3–25 Deployment Manager - IT Resource Instance Data

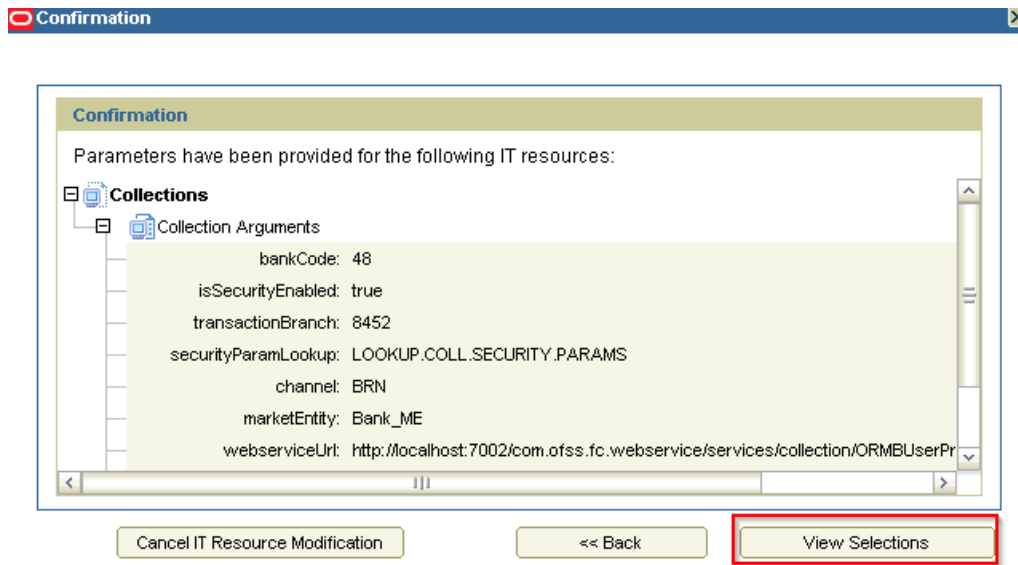


8. Click **Skip**.

Figure 3–26 Deployment Manager - Skip Parameter Value



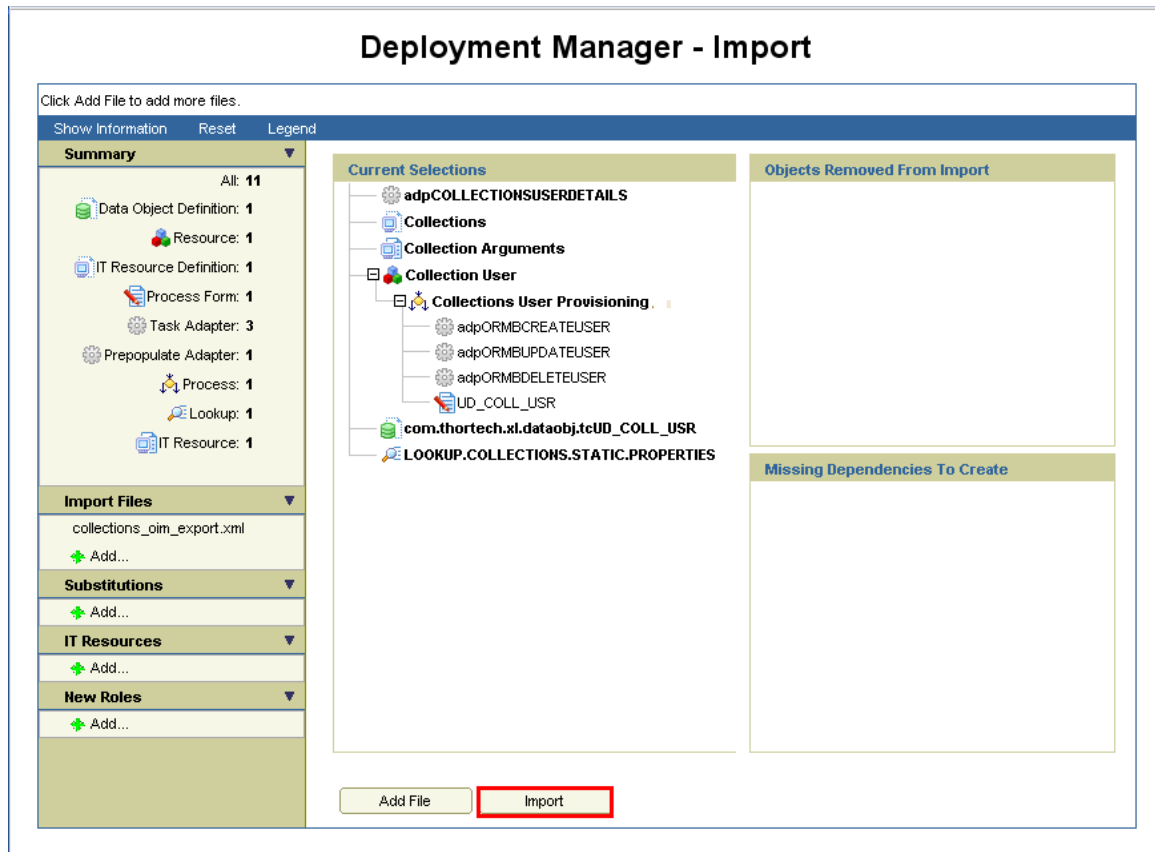
9. Click **View Selections**.

Figure 3–27 Deployment Manager - View Selections

Overview of all artifacts that have been added will be displayed. Total number of artifacts to be added must be 11. You can verify them in the **Summary** section for **All : 11**.

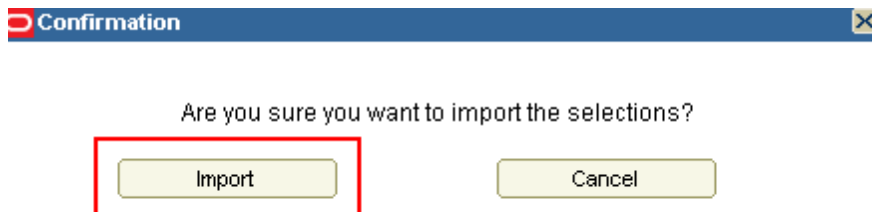
10. Click **Import**.

Figure 3–28 Deployment Manager - Import



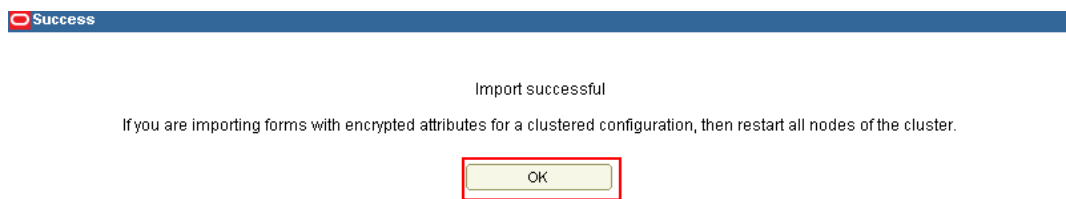
11. A **Confirmation** dialog box appears. Click **Import**.

Figure 3–29 Import Confirmation



12. On successful import of data, **Import successful** message will be displayed. Click **OK** and close **Deployment Manager - Import** window.

Figure 3–30 Import Confirmation Dialog Box



3.3.5 Verify and Override Date Format Lookup

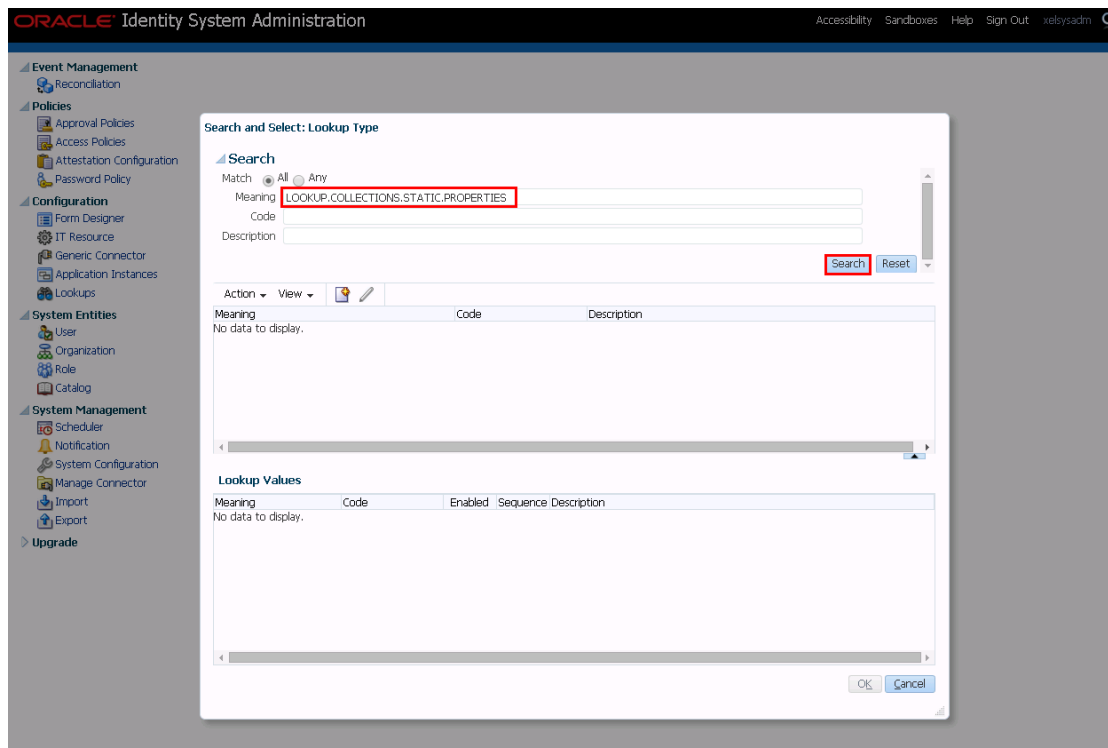
A lookup 'LOOKUP.COLLECTIONS.STATIC.PROPERTIES' has been added to map environment specific properties to OIM.

After successful import, verify whether the lookup type 'LOOKUP.COLLECTIONS.STATIC.PROPERTIES' has been imported properly along with the other configurations.

To verify the lookup type, perform the below mentioned procedures:

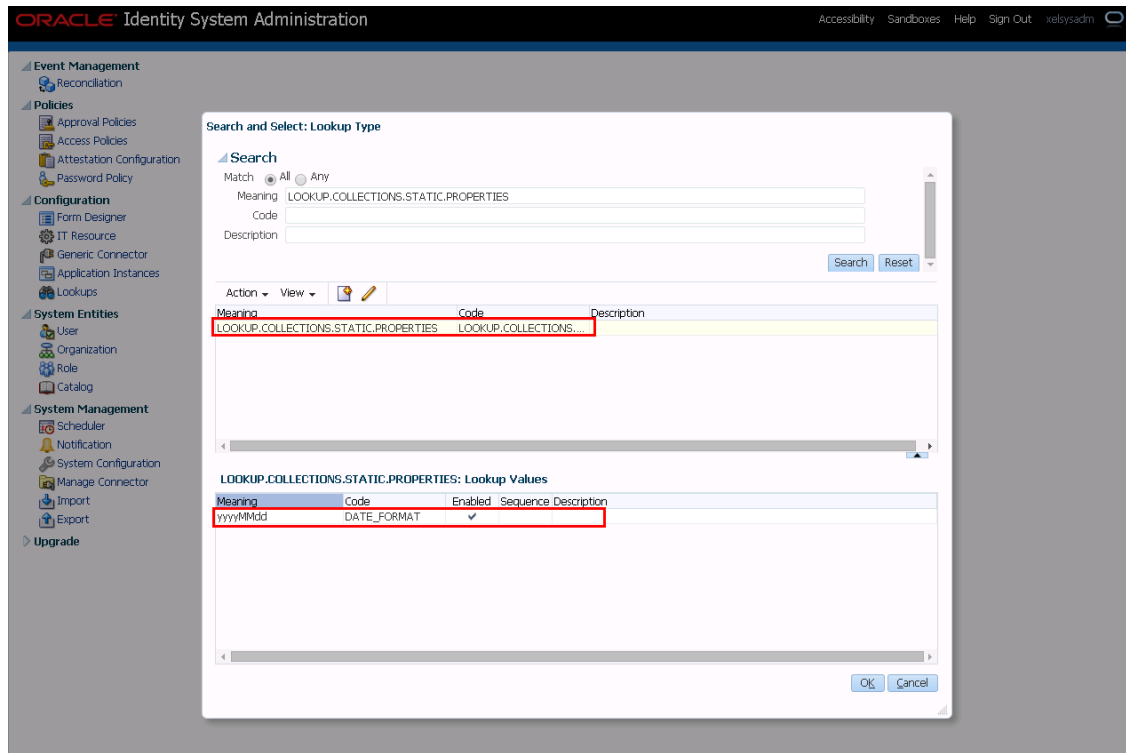
1. Log in to **Oracle Identity System Administration**.
2. In the left pane, under Configuration, click Lookups. The Search and Select: Lookup Type window is displayed.
3. In the **Meaning** field, enter the lookup value **LOOKUP.COLLECTIONS.STATIC.PROPERTIES**.

Figure 3–31 Entering Lookup Value



4. Click **Search**. The lookup types that match your search criteria get displayed in a tabular format.

Figure 3–32 Lookup Types Criteria Match



This look up type will be shipped along with the Collections adapter configuration. The default value of the **DATE_FORMAT** code for the lookup type will be 'yyyyMMdd' or the 'End Date' field on User form.

Meaning for the lookup code corresponds to the value for 'client.format.date' property in **root configuration properties**.

Before trying to provision a user, please verify that the Meaning for the DATE_FORMAT Code matches the property value of 'client.format.date' in the root configurations. If not, then edit the lookup type accordingly.

Note

- If the lookup type is not present, the user will not get provisioned and generic failure message will be displayed in Open tasks for Create User task.
 - If the lookup type is present but the Code is incorrect then the user will not get provisioned and a generic failure message will be displayed in Open tasks for Create User task.
 - If lookup type is present and the code is correct but the Meaning is not in sync with the format in root configurations, user will get provisioned to Collections but with incorrect date. Considering the current JODA date configuration, it will persist current system date.
-

3.3.6 Add Process Trigger

Process Triggers are used to define task name for user fields. This task name could be further configured in process definition and would be invoked when there is change in corresponding field. Below configuration is to add Process Trigger for user fields used for Collections User Provisioning:

1. Log in to Oracle Identity System Administration. In the left pane, under Configuration, click **Lookups**. The **Search and Select: Lookup Type** window is displayed.

Figure 3–33 Oracle Identity System - System Administration

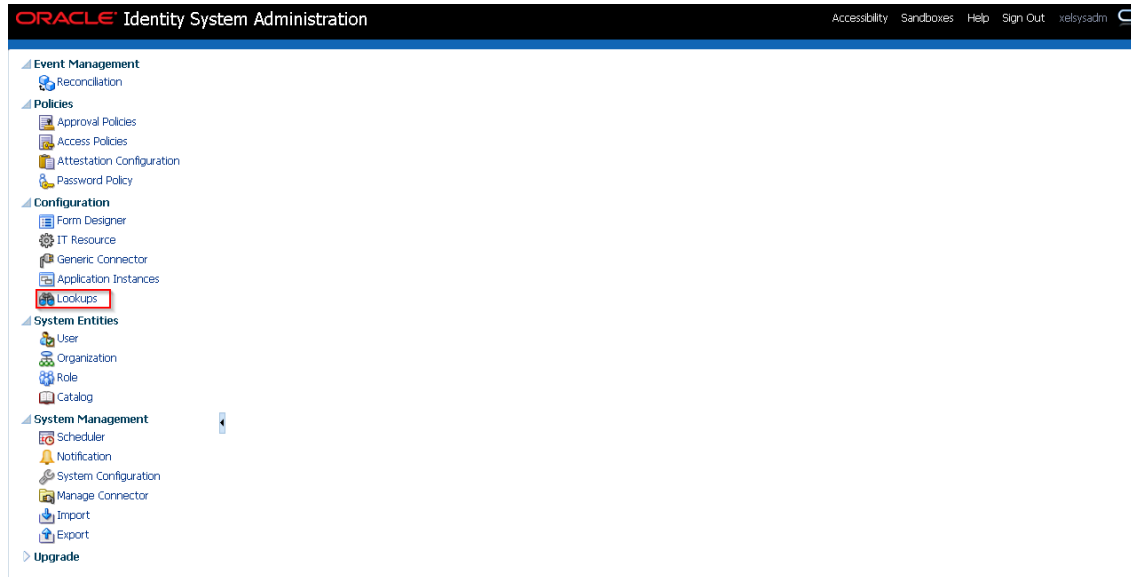
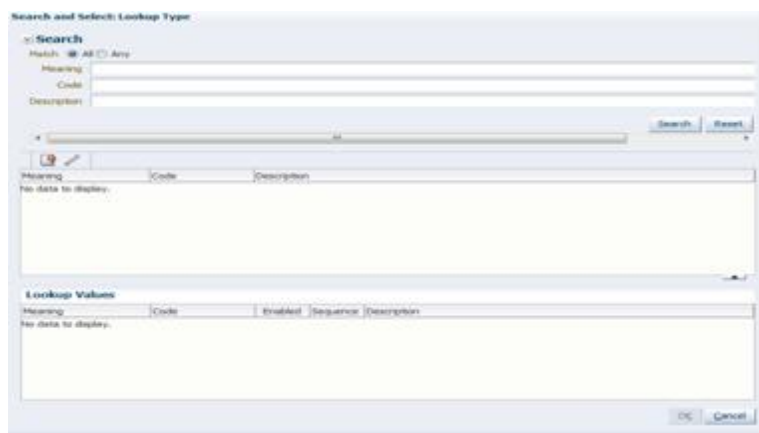
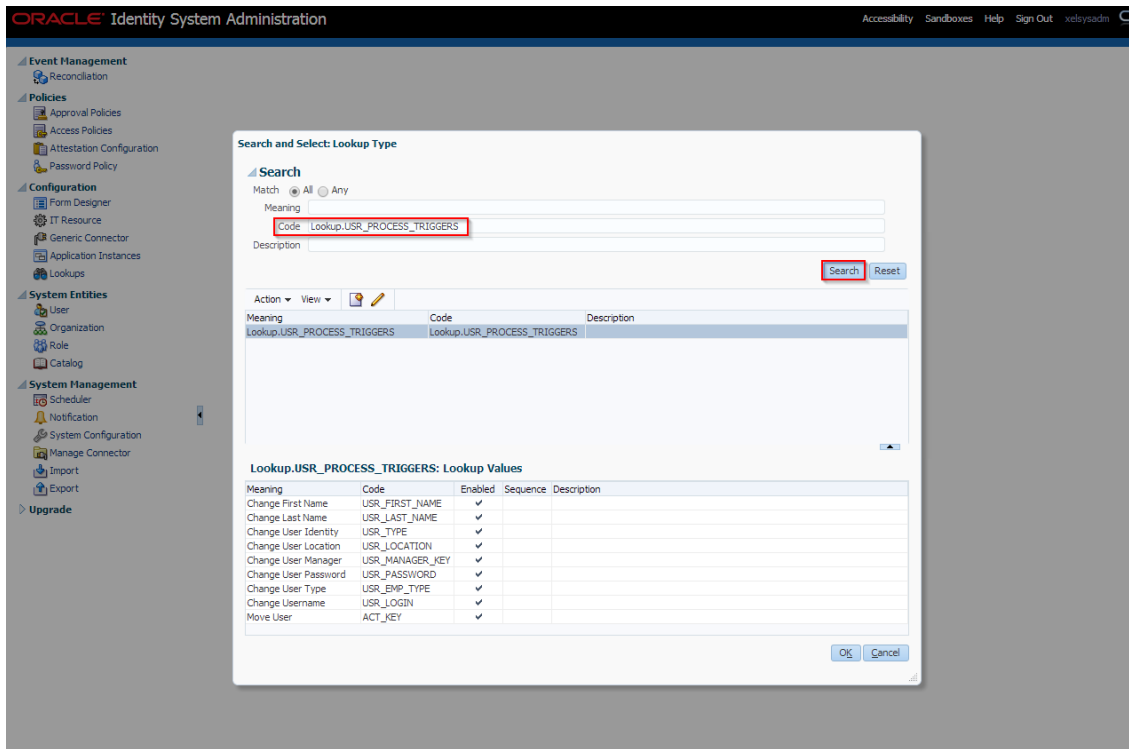


Figure 3–34 Search and Select - Lookup Type



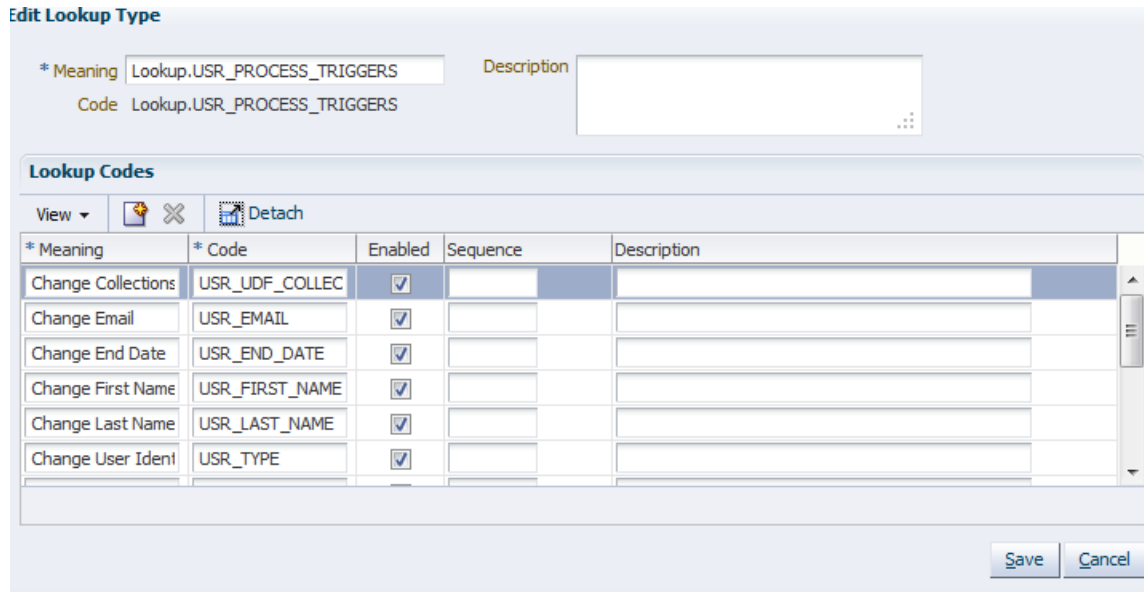
2. Add the following:
 - Code:** Lookup.USR_PROCESS_TRIGGERS
3. Click **Search**.

Figure 3–35 Search Lookup Type



4. Click **Edit** icon. Edit Lookup Type dialog window will open.

Figure 3–36 Edit Lookup Type



- Click **Add** icon. Add the following parameters in the row that appears.

Code: USR_EMAIL

Meaning: Change Email

Figure 3–37 Adding a Lookup Type

Edit Lookup Type

* Meaning Description

Code

Lookup Codes

View

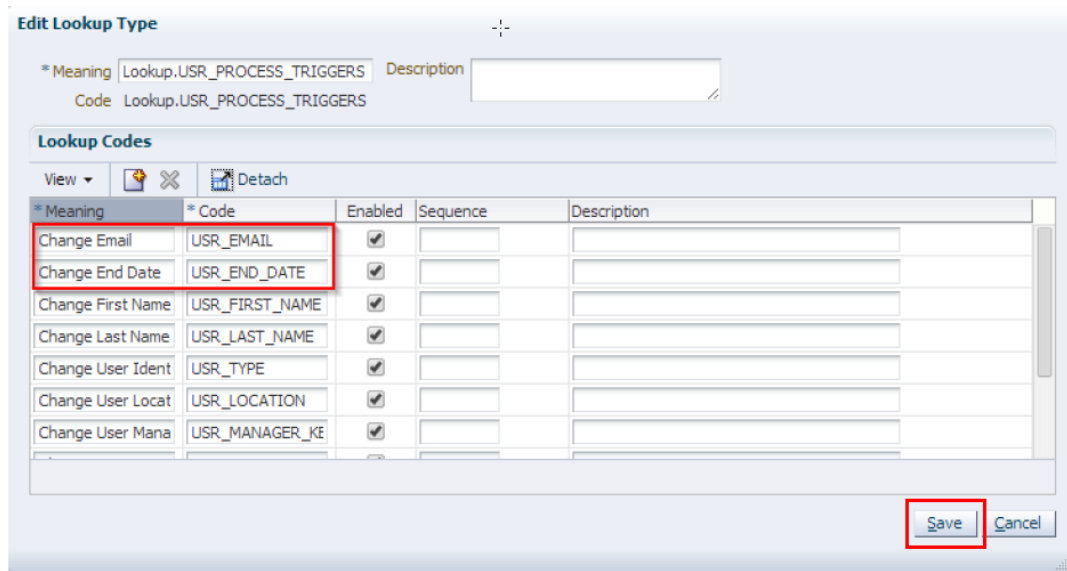
* Meaning	* Code	Enabled	Sequence	Description
Change Email	USR_EMAIL	<input checked="" type="checkbox"/>		
Change Email	USR_EMAIL	<input checked="" type="checkbox"/>		
Change End Date	USR_END_DATE	<input checked="" type="checkbox"/>		
Change First Name	USR_FIRST_NAME	<input checked="" type="checkbox"/>		
Change Last Name	USR_LAST_NAME	<input checked="" type="checkbox"/>		
Change User Ident	USR_TYPE	<input checked="" type="checkbox"/>		

- Similarly, add the following variables (repeat step 4) and then click **Save**.

Table 3–5 List of variables

Code Key	Meaning
USR_EMAIL	Change Email
USR_END_DATE	Change End Date

Figure 3–38 Edit Lookup Types



Note

Meaning value is used as Process definition Task name. If there is any change in meaning value, then corresponding name change must be done in Process definition task.

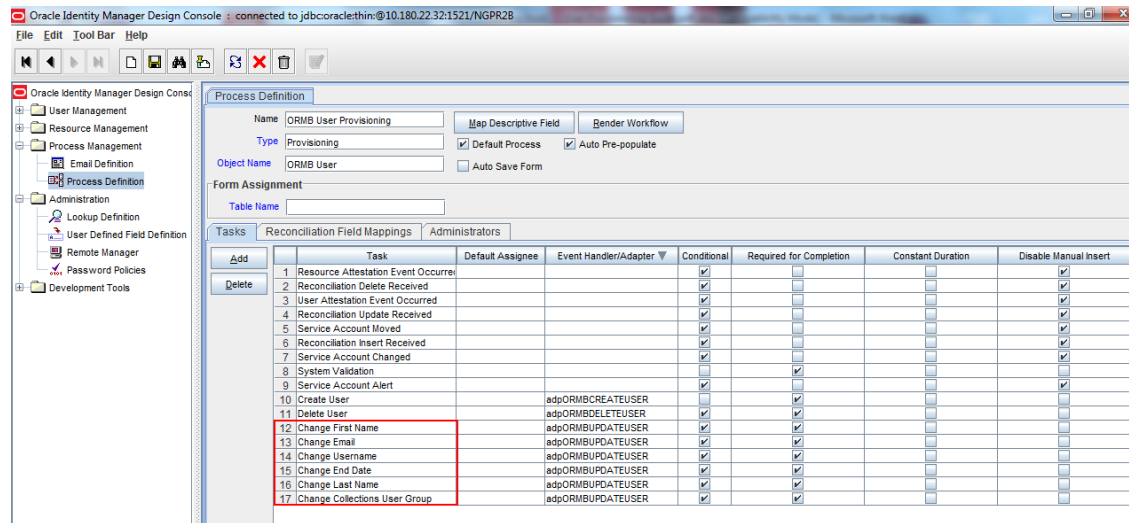
Below table lists the Code Key being used:

Table 3–6 Code Key details

Code	Meaning	Process Definition Task Name
USR_FIRST_NAME	Change First Name	Change First Name
USR_LAST_NAME	Change Last Name	Change Last Name
USR_EMAIL	Change Email	Change Email
USR_LOGIN	Change Username	Change Username
USR_END_DATE	Change End Date	Change End Date

To verify process task name in Process Definition login to design console and open Process Definition tab as shown below:

Figure 3–39 Verifying Process Task Name

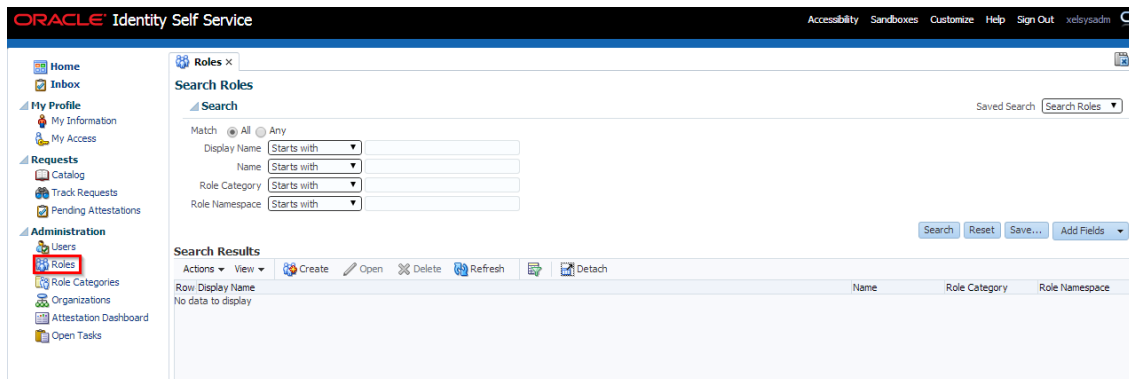


3.3.7 Create Collections Role

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

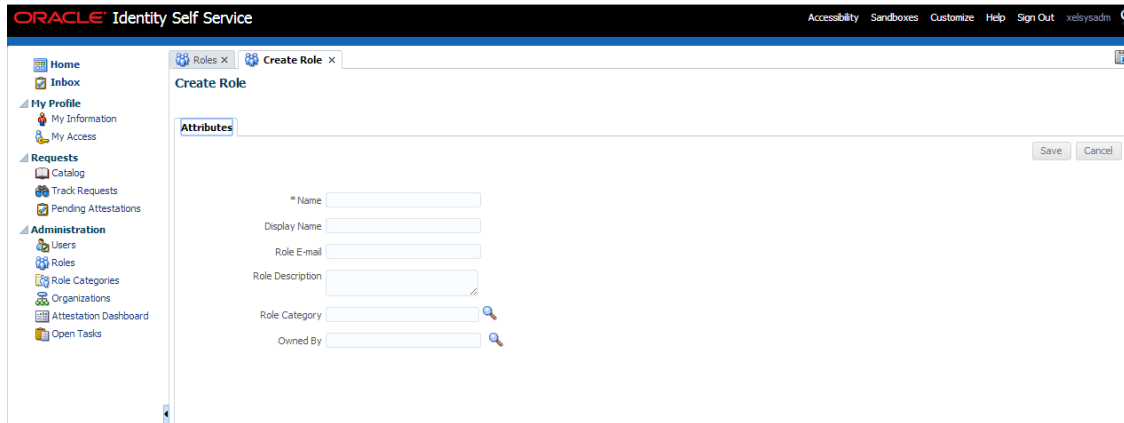
1. Log in to Identity Self Service.
2. Under **Administration**, click **Roles**. The Search Roles page is displayed.

Figure 3–40 Oracle Identity Self Service



3. Click **Create** on the toolbar. The Create Role page is displayed.

Figure 3–41 Create Role



4. Specify the following values and then click Save.

Name : COLL_USER

Display Name : COLL_USER

Role Description : Default Role for all Collections User

Role Category: Default

5. Click **Save**.

Figure 3–42 Create Role - Values

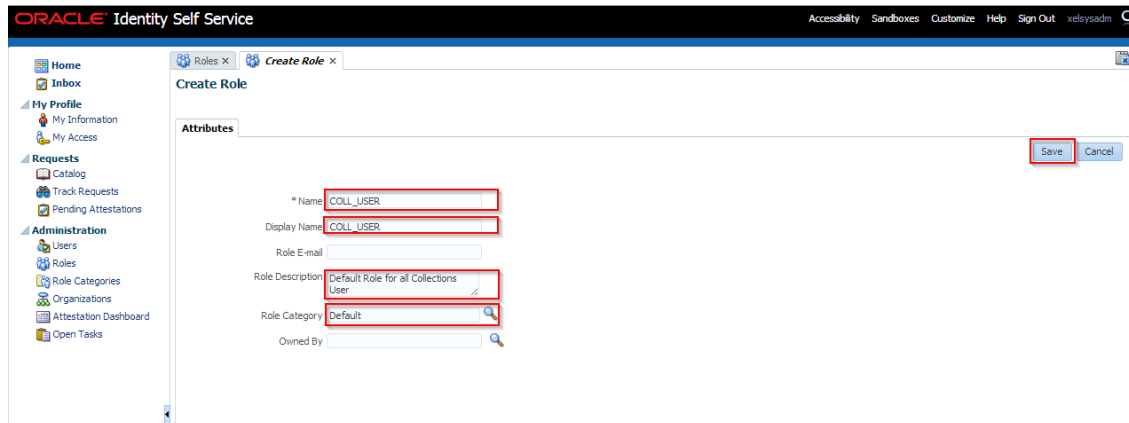
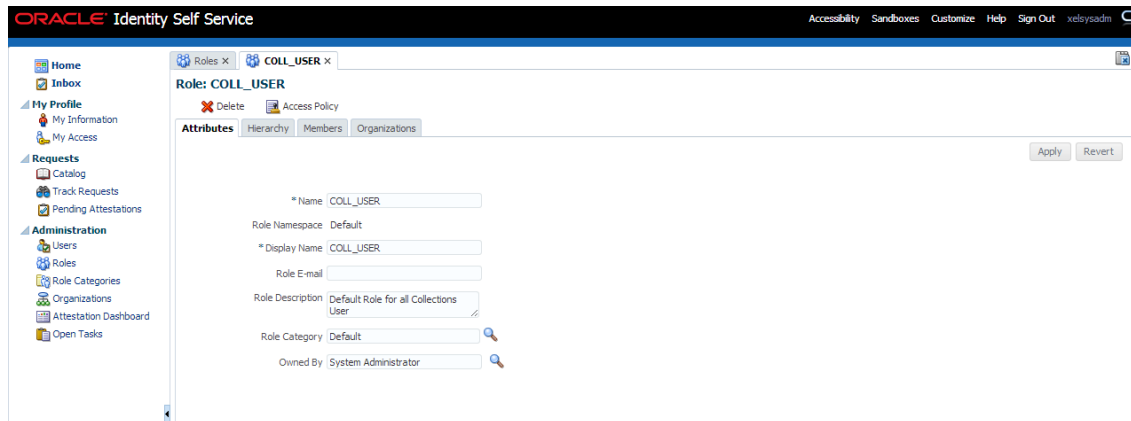
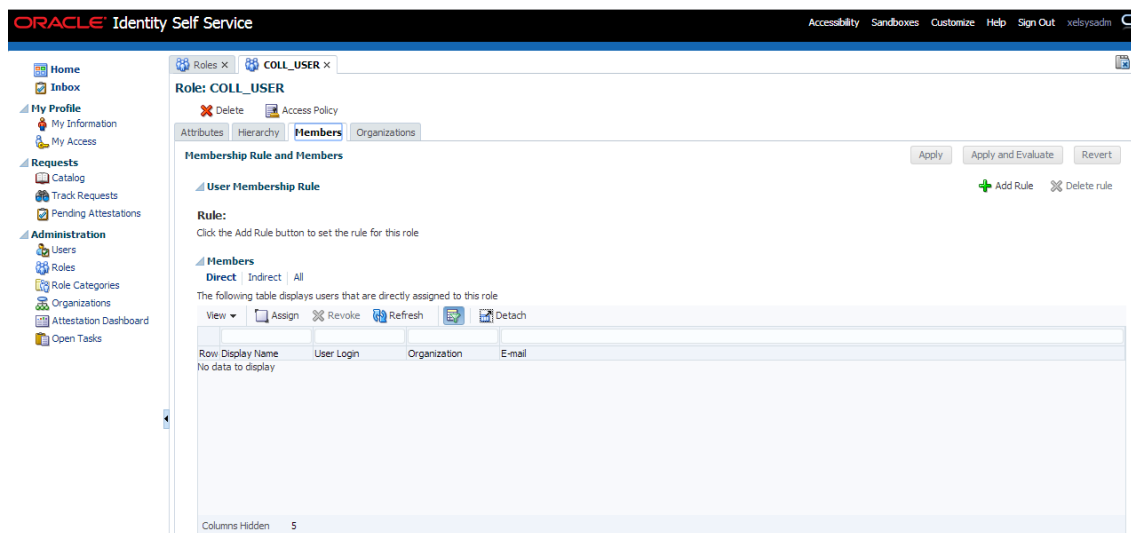


Figure 3–43 Create Role - Attributes Tab



6. Click **Members** tab. The Members tab is displayed.

Figure 3–44 Create Role - Members Tab



7. Click **Add Rule** under User Membership Rules. The User Membership Rules for COLL_USR dialog box is displayed.

Figure 3–45 Create Role - Add Rule

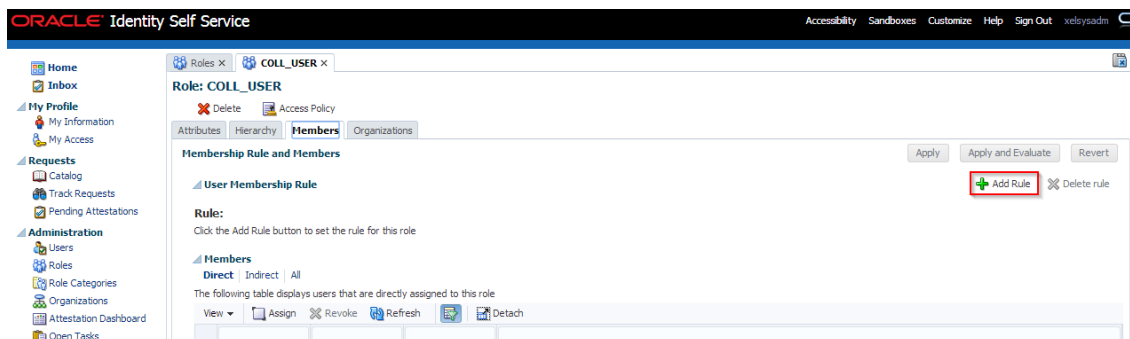
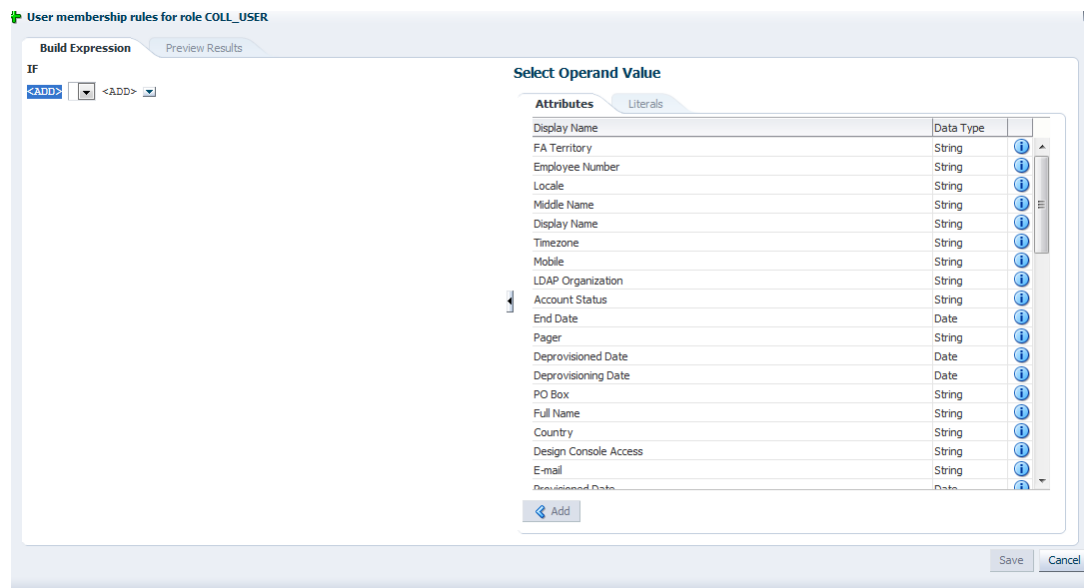


Figure 3–46 Create Role - Build Expression



8. Create Rule such that COLL_USR role is assigned to User that need to be provisioned to Collections. Here we have defined Rule Based on Organization.

Figure 3–47 Create Rule - Add

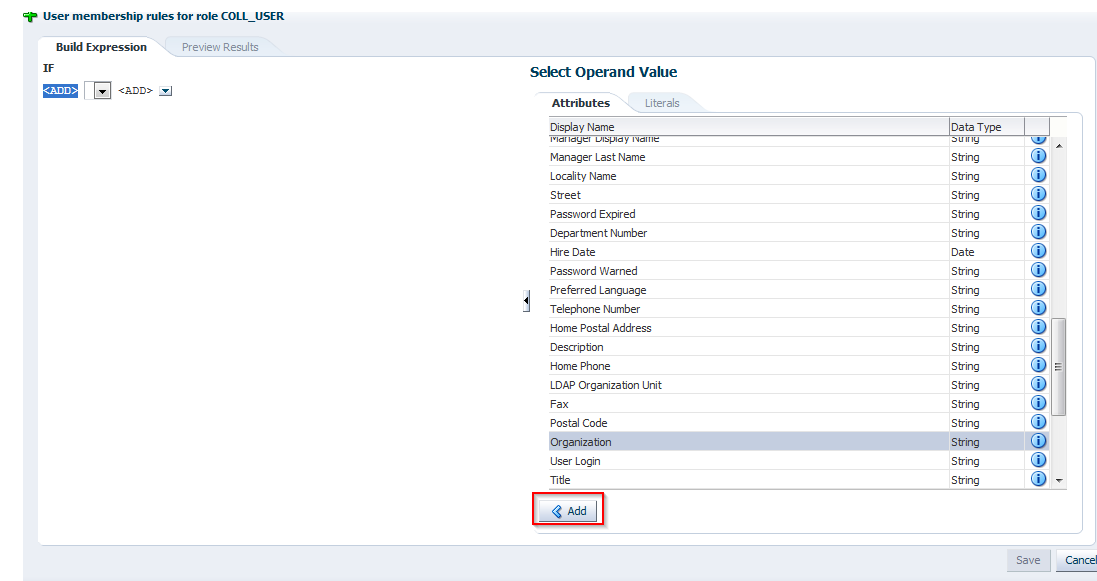


Figure 3–48 Create Rule - Select Operand Values

User membership rules for role COLL_USER

Build Expression Preview Results

IF

Organization = [dropdown] STRING

Select Operand Value

Attributes Literals

Required data type is String

Value | Requests

Add

Save Cancel

Figure 3–49 Create Rule - Build Expression

User membership rules for role COLL_USER

Build Expression Preview Results

IF

Organization = [dropdown] 'Requests'

And Or Remove

Select Operand Value

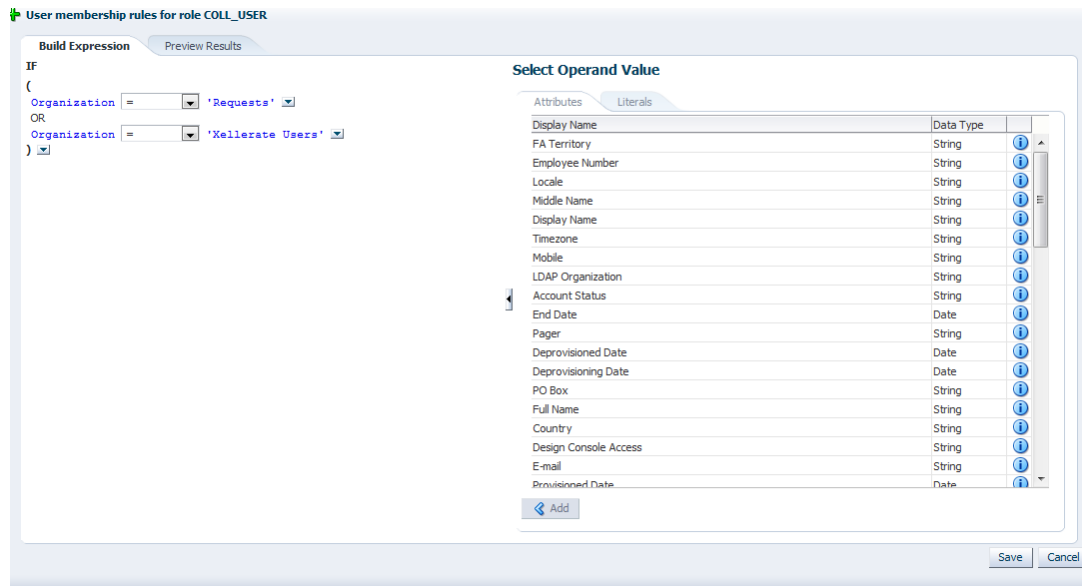
Attributes Literals

Display Name	Data Type	
FA Territory	String	(i)
Employee Number	String	(i)
Locale	String	(i)
Middle Name	String	(i)
Display Name	String	(i)
Timezone	String	(i)
Mobile	String	(i)
LDAP Organization	String	(i)
Account Status	String	(i)
End Date	Date	(i)
Pager	String	(i)
Deprovisioned Date	Date	(i)
Deprovisioning Date	Date	(i)
PO Box	String	(i)
Full Name	String	(i)
Country	String	(i)
Design Console Access	String	(i)
E-mail	String	(i)
Provisioned Date	Date	(i)

Add

Save Cancel

Figure 3–50 Create Rule - Build Expression Updated

**Note**

It is been observed that when Role membership rule is applied to a user its membership is not pushed to OID (that is, user is not added to Role in OID). To overcome this behavior enable schedule job 'LDAPSync Post Enable Provision Role Memberships to LDAP' in periodic mode (as per requirement).

Run the following query to ensure that Collection Dashboard is shown as the default page after logging in.

```
update flx_fw_config_all_b set prop_value='Role' where prop_id='collection.roles' and CATEGORY_ID='BROPConfig';
```

where Role = configured user role.

3.3.8 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 COLL_USR. Also, COLL_USR is applied to user through membership rule. Thus, policy will be applied to user and the user would be provisioned to resource - Collection User.

Note

Here, we have used COLL_USR Role, but it can be changed as required.

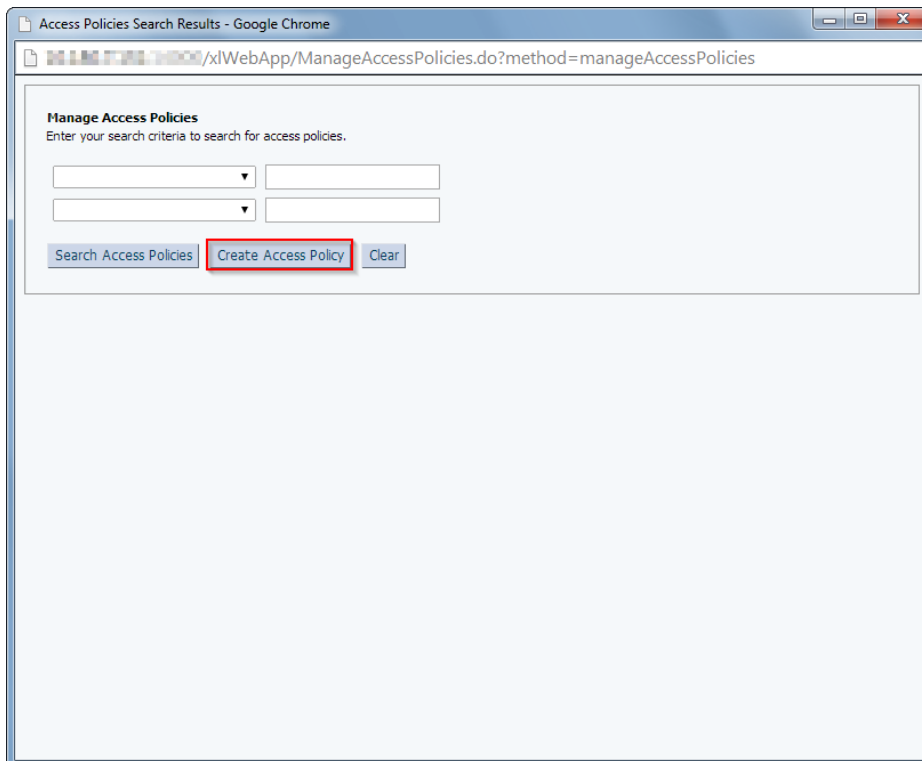
1. Log in to the Oracle Identity System Administration.
2. To open the Create Access Policies page, under Policies, click **Access Policies**. This displays Manage Access Policies dialog box.

Figure 3–51 Create Access Policy - Access Policies



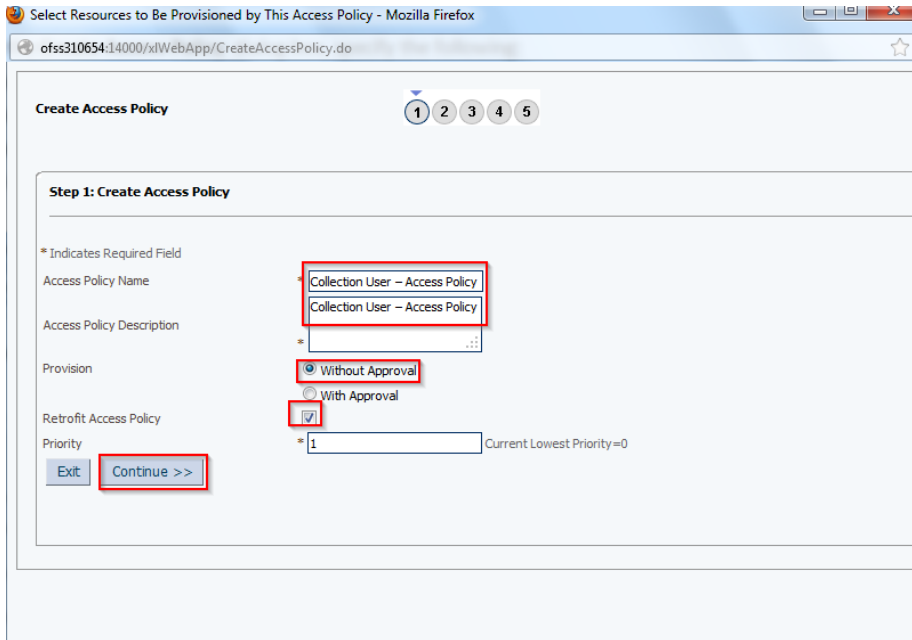
3. Click **Create Access Policy**.

Figure 3–52 Create Access Policy



4. In the **Create Access Policy** dialog box, specify the following:
Access Policy Name: Collection User - Access Policy
Access Policy Description: Collection User - Access Policy
Provision: Select radio button Without Approval
5. Click **Continue**.

Figure 3–53 Create Access Policy - Continue



6. Select **Collection User** check box.
7. Click **Add**.

Figure 3–54 Create Access Policy - Select Resources

Create Access Policy 1 2 3 4 5

Step 2: Select Resources

Specify the resources to be provisioned by this access policy.

* Indicates Required Field

Filter By Go

Results 1-1 of 1 First | Previous | Next | Last

<input type="checkbox"/>	<u>Resource Name</u>
<input checked="" type="checkbox"/>	Collection User

First | Previous | Next | Last

Add >>

<< Remove

Selected:

Exit << Back Continue >>

8. Click **Continue**.

Figure 3–55 Create Access Policy - Selected Resource

Create Access Policy 1 2 3 4 5

Step 2: Select Resources

Specify the resources to be provisioned by this access policy.

* Indicates Required Field

Filter By Go

Results 1-1 of 1 First | Previous | Next | Last

<input type="checkbox"/>	<u>Resource Name</u>
<input type="checkbox"/>	Collection User

First | Previous | Next | Last

Add >>

<< Remove

Selected:
Collection User

Exit << Back Continue >>

9. Click **Continue**.

Figure 3–56 Create Access Policy - Select Resource

Create Access Policy

1 2 3 4 5

Step 2: Select Resources

The subsequent pages will guide you through providing the data to associate with the following resources you selected to be provisioned by this Access Policy:

- Collection User

Exit << Back Skip This Step **Continue >>**

Figure 3–57 Select Resources - Process Details

Create Access Policy

1 2 3 4 5

Step 2: Select Resources

Provide the following process details for resource: **Collection User**:

Collections Server Instance [Clear](#)

First Name

Last Name

User Login

Email Id

End Date

Collections User Group [Clear](#)

Exit << Back Skip All Forms Continue >>

10. Select instance name for **Collection Server Instance** field from the lookup.

Figure 3–58 Selecting Instance Name

Lookup Form - Google Chrome

/xlWebApp/ITResourceLookupForm.do?method:

Select Collections Server Instance

Select the value to use in the field.

Filter By: Instance Name Go

Instance Name

Collection Arguments

Select Close

11. Select **Collection Arguments** as Collections Server Instance (IT Resource to be used to Provision User to Collections).
12. Click **Continue**.

Figure 3–59 Create Access Policy - Server Instance

Create Access Policy

1 2 3 4 5

Step 2: Select Resources

Provide the following process details for resource **Collection User**:

Collections Server Instance	<input type="text" value="Collection Arguments"/>	Clear
First Name	<input type="text"/>	
Last Name	<input type="text"/>	
User Login	<input type="text"/>	
Email Id	<input type="text"/>	
End Date	<input type="text"/>	
Collections User Group	<input type="text"/>	Clear

[Exit](#) [<< Back](#) [Skip All Forms](#) [Continue >>](#)

13. Select radio button **Revoke if no longer applies**.

Figure 3–60 Create Access Policy - Select Revoke or Disable Flag

Create Access Policy

1 2 3 4 5

Step 2: Select Revoke Or Disable Flag

Select if the resources need to be revoked or disabled if the access policy no longer applies.

Resource Name	Revoke if no longer applies	Disable if no longer applies
Collection User	<input checked="" type="radio"/>	<input type="radio"/>

[Exit](#) [<< Back](#) [Continue >>](#)

14. Click **Continue**.

Figure 3–61 Create Access Policy - Continue

Create Access Policy 1 2 3 4 5

Step 3: Select Resources

Specify the resources to be denied by this access policy.

* Indicates Required Field

Filter By

Results 1-1 of 1 First | Previous | Next | Last

<input type="checkbox"/>	Resource Name
<input type="checkbox"/>	Collector User

First | Previous | Next | Last

Selected:

15. Select **COLL_USERS** check box. Steps 15-17 are not displayed as shown in below figure (as per new OIM version- 11.1.2.3.0). To associate the access policy to a role, perform steps 19-28 after successfully creating Access Policy.
16. Click **Add**.
17. Click **Continue**.

Figure 3–62 Create Access Policy - Add

Create Access Policy 1 2 3 4 5

Step 4: Select Roles

Specify roles for this access policy.

* Indicates Required Field

Filter By

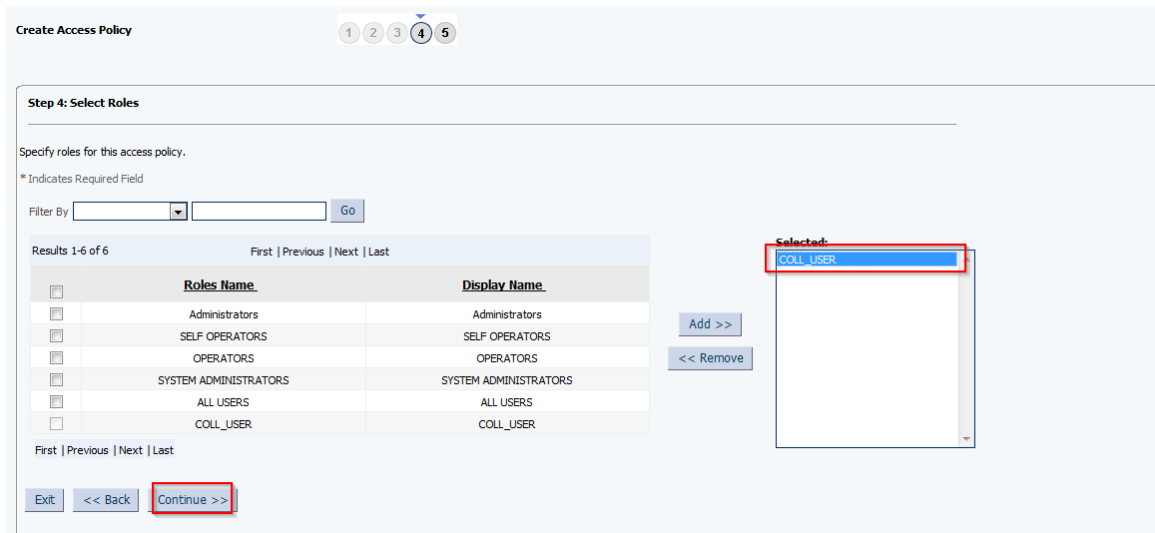
Results 1-6 of 6 First | Previous | Next | Last

<input type="checkbox"/>	Roles Name	Display Name
<input type="checkbox"/>	Administrators	Administrators
<input type="checkbox"/>	SELF OPERATORS	SELF OPERATORS
<input type="checkbox"/>	OPERATORS	OPERATORS
<input type="checkbox"/>	SYSTEM ADMINISTRATORS	SYSTEM ADMINISTRATORS
<input type="checkbox"/>	ALL USERS	ALL USERS
<input checked="" type="checkbox"/>	COLL_USER	COLL_USER

First | Previous | Next | Last

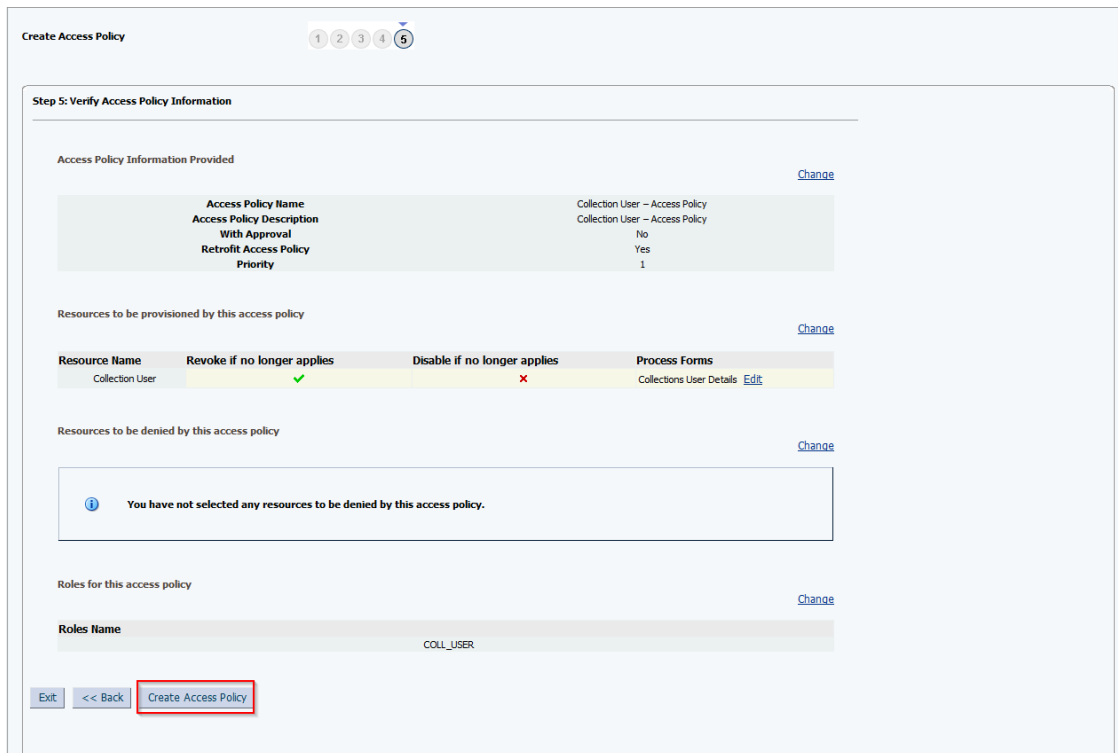
Selected:

Figure 3–63 Create Access Policy - Select Roles



18. Verify access policy details. Click **Create Access Policy**. It creates **Access Policy**.

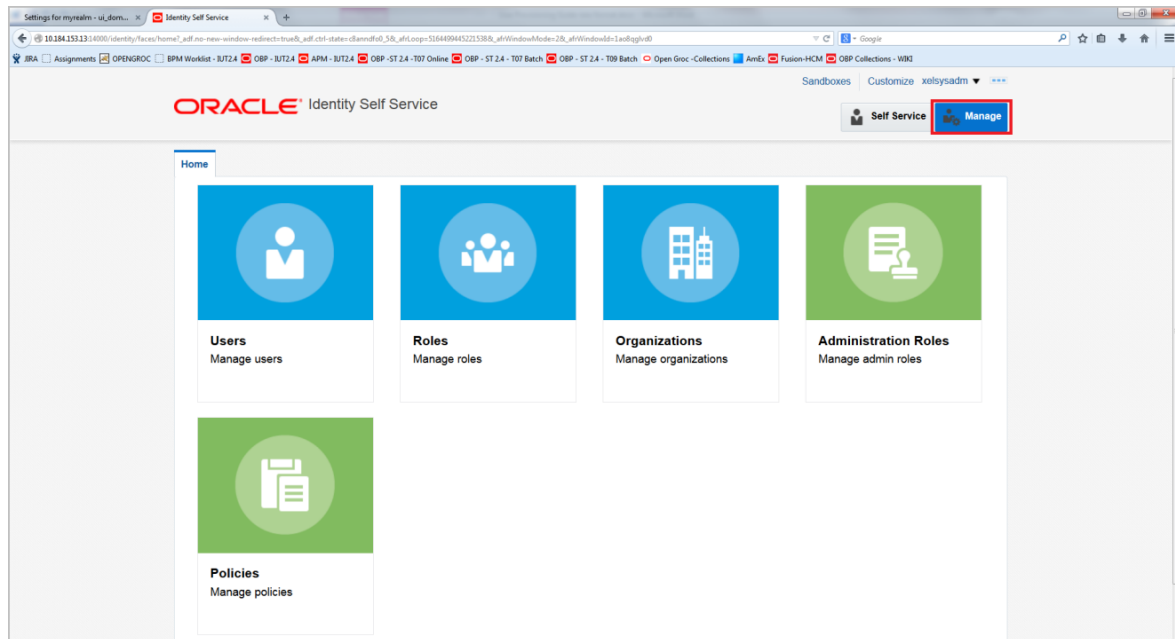
Figure 3–64 Create Access Policy - Verify Access Policy Information



To associate the access policy to a role, perform following steps:

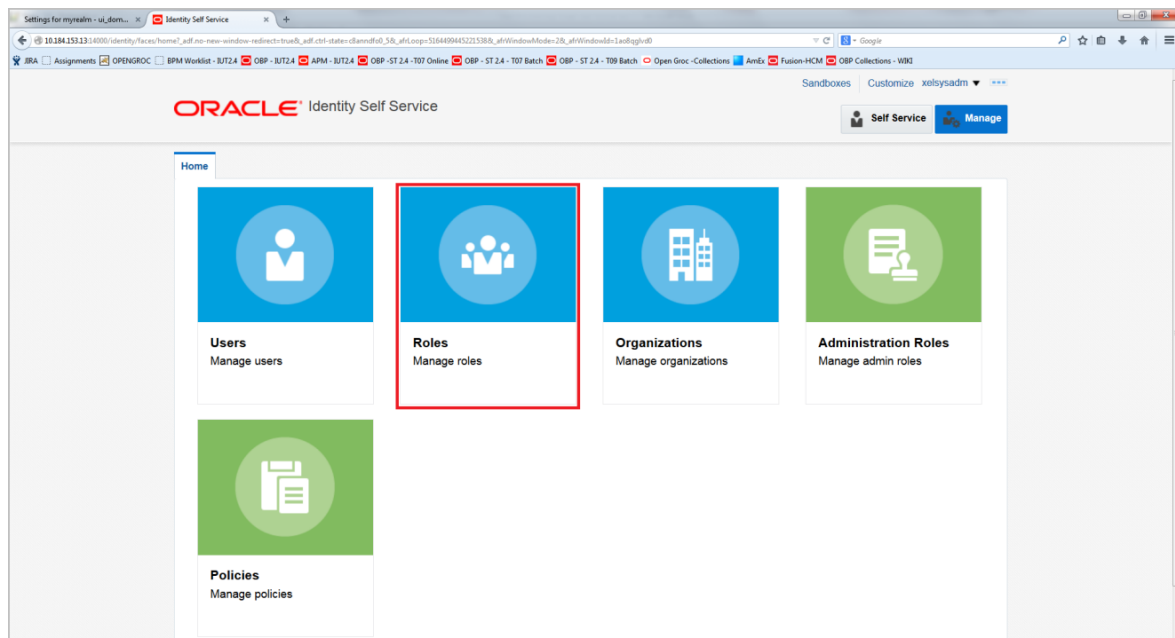
19. Log in to Identity Self Service (<OIM ip>:<port>/identity)
20. Click the **Manage** tab.

Figure 3–65 Identity Self Service- Manage Tab



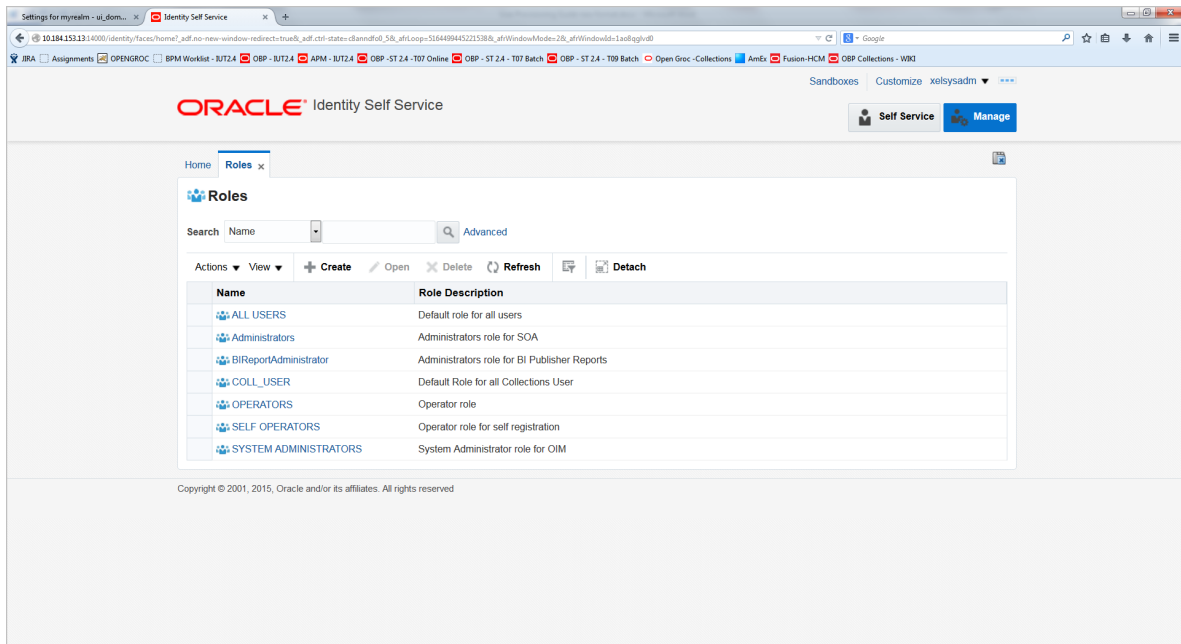
21. Click the **Roles** tab.

Figure 3–66 Roles Tab



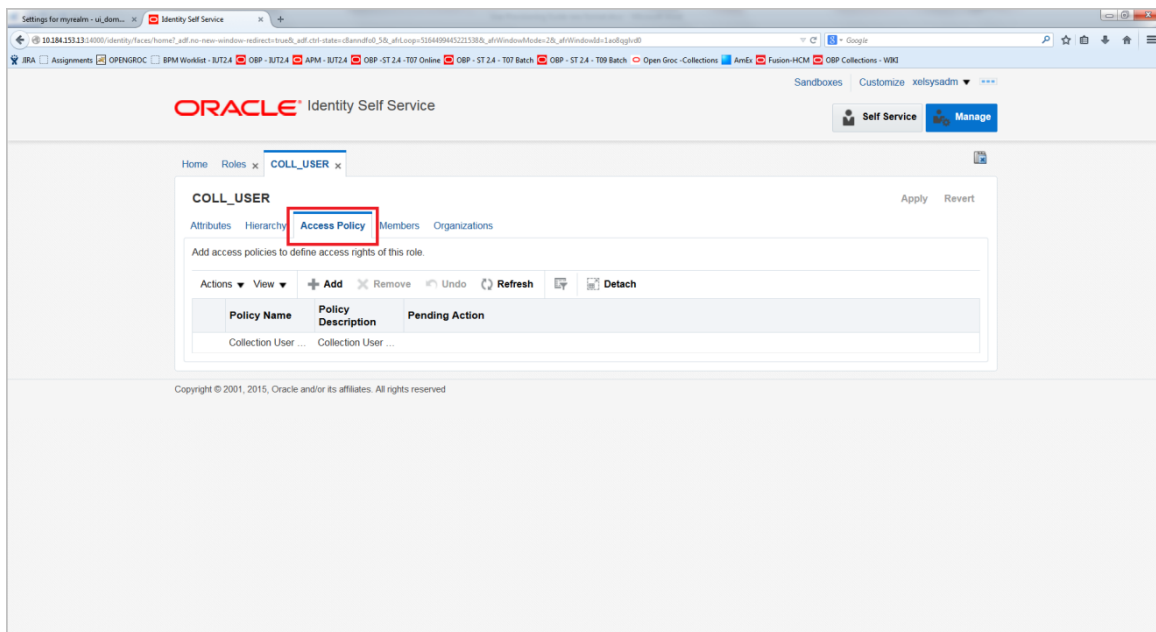
List of Roles configured in the system will be displayed, including the role created in [Section 3.3.7 Create Collections Role](#) (as per this document - COLL_USER).

Figure 3–67 List of Roles



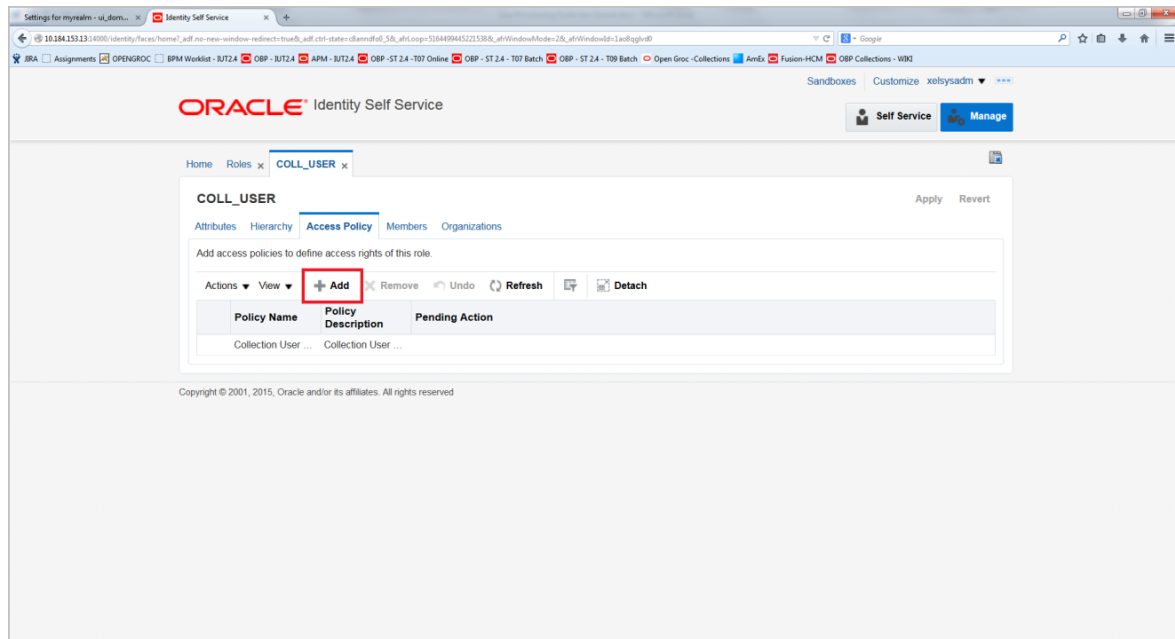
22. Click **COLL_USER**. This opens a new tab with 5 subtabs.
23. Click the **Access Policy** sub tab.

Figure 3–68 Access Policy



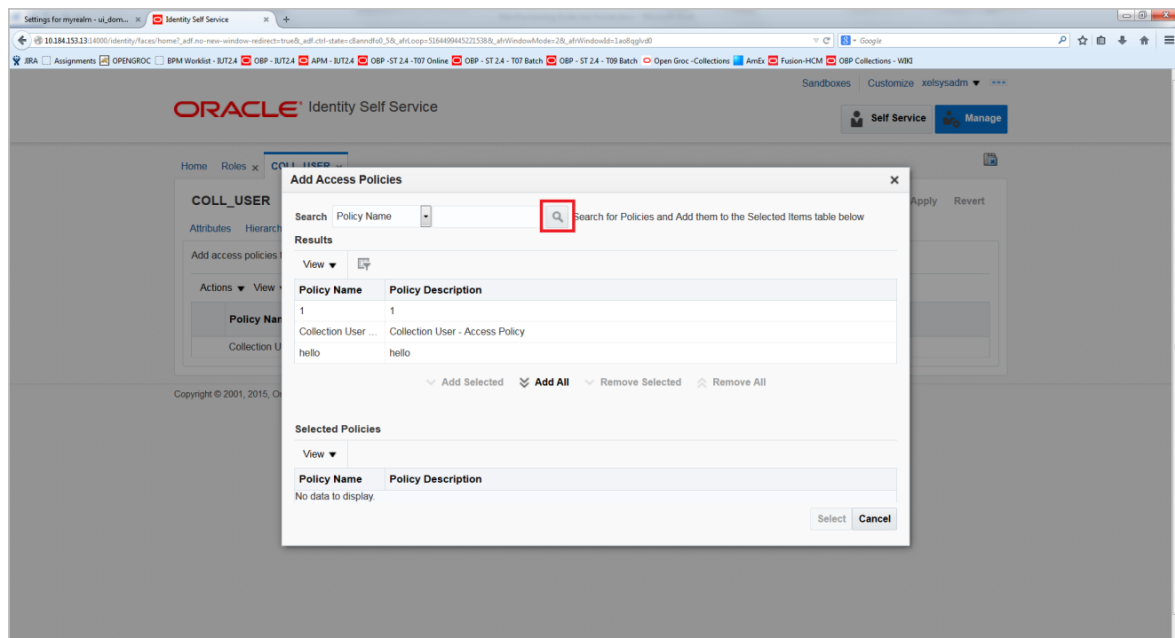
24. Click **Add** to associate an access policy with the role.

Figure 3–69 Add Access Policy



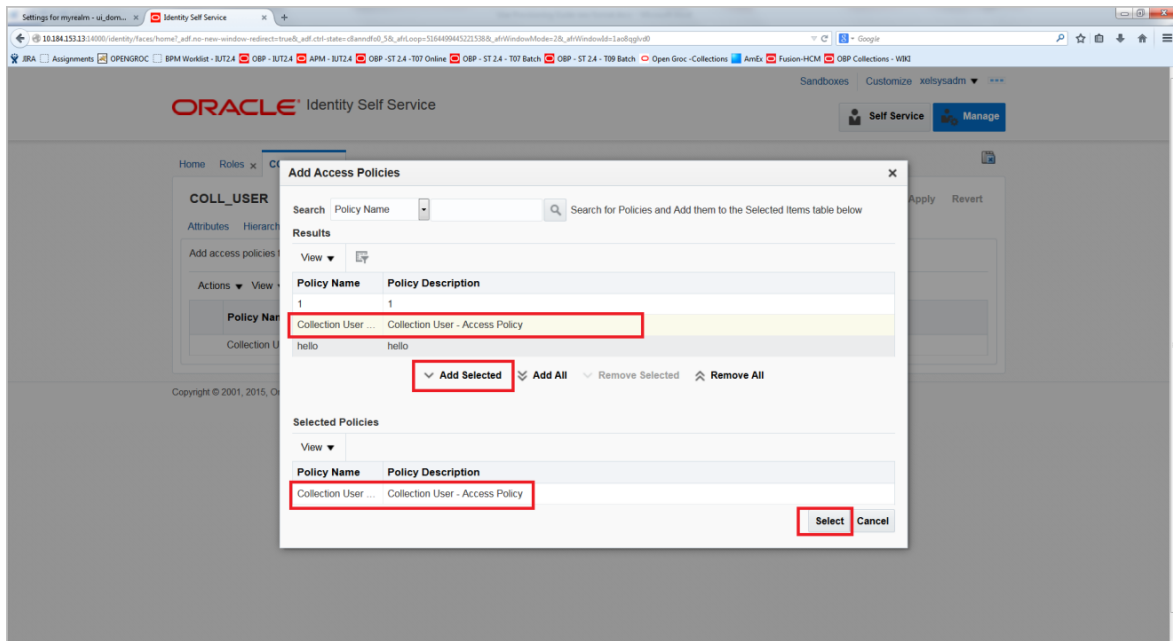
25. In the pop-up window, click the **Search** icon to display list of access policies.

Figure 3–70 Search Access Policy



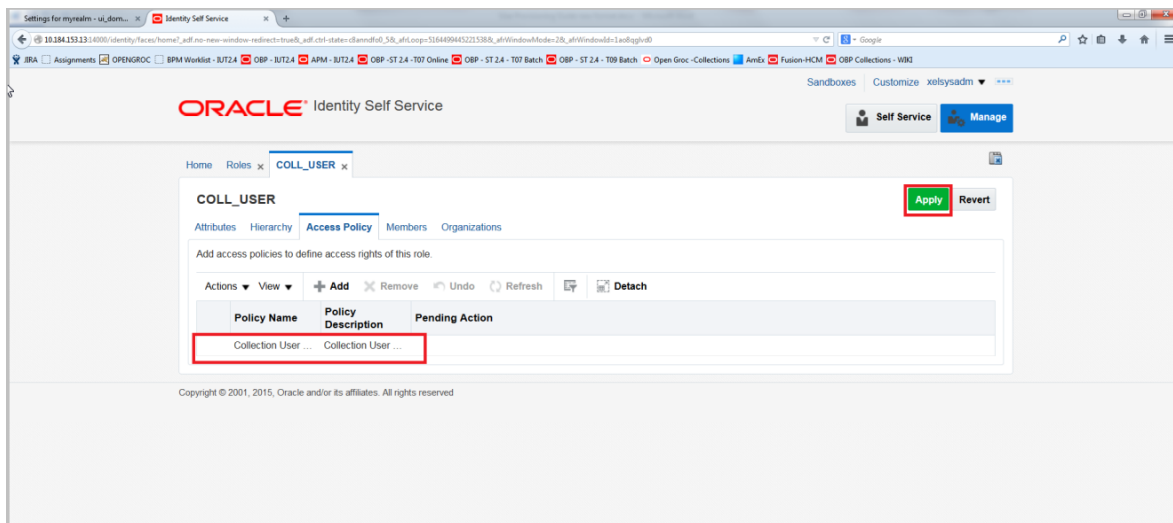
26. Select the access policy just created through the above steps, and click **Add Selected**. This will populate the selected access policy in the Selected Policies table.

Figure 3–71 Add Selected Policy



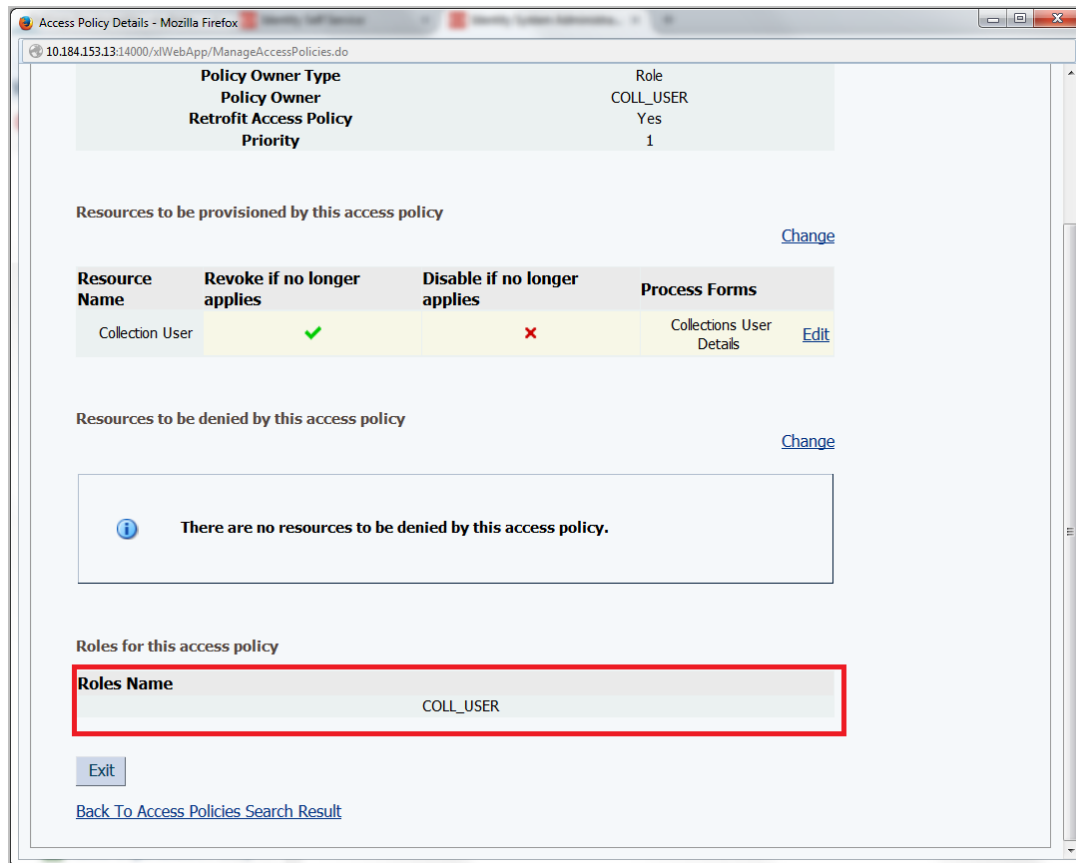
27. Click **Select**. The pop-up window closes and the access policy populates for the role.
28. Click **Apply** to finally associate the access policy with the role.

Figure 3–72 Apply Policy



29. Verify the access policy-role association from the **Access Policy** tab similar to step 18.

Figure 3–73 Verify Policy



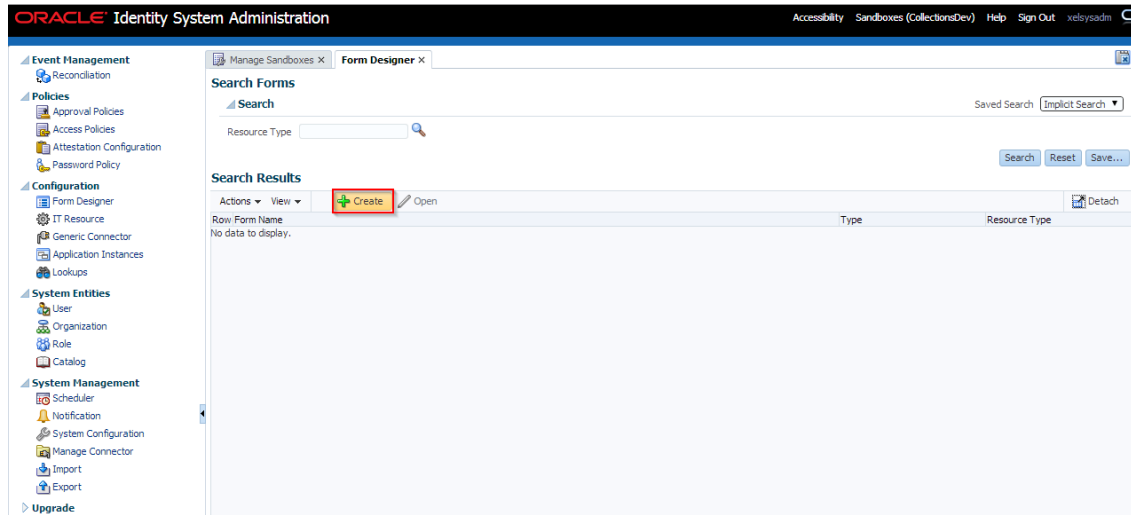
30. Restart OIM Admin and Managed Servers.

3.3.9 Create Form Associated with Application Instance

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

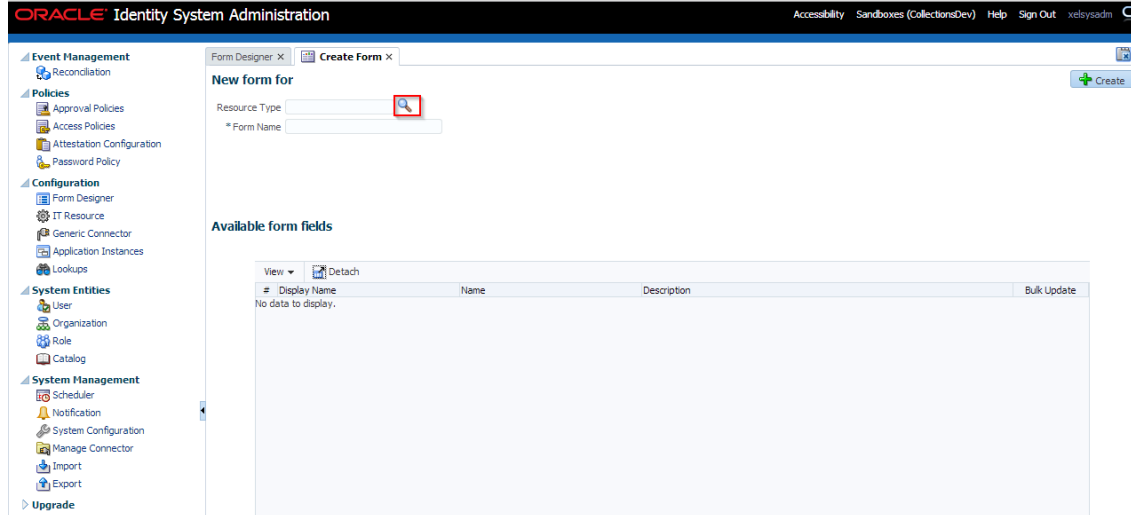
1. Log in to Oracle Identity System Administration.
2. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see [Chapter 3.3.3 Collection Sandbox](#)
3. In the left pane, under Configuration, click **Form Designer**. The **Form Designer** page is displayed.

Figure 3–74 Create Form - Form Designer



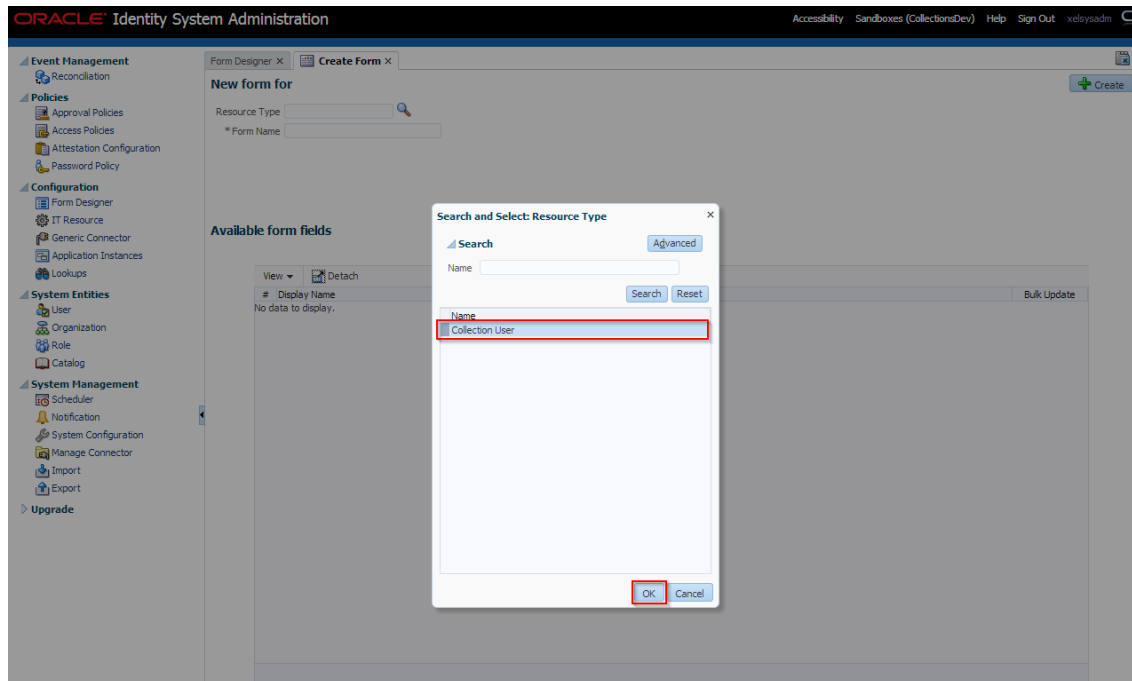
4. Click **Create** on the toolbar. The **Create Form** page is displayed.
5. In the **Resource Type** field, verify the name of the resource object with which the form is associated is displayed. To change the resource object name, click the Search icon next to the **Resource Type** field, and search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

Figure 3–75 Create Form - Resource Type



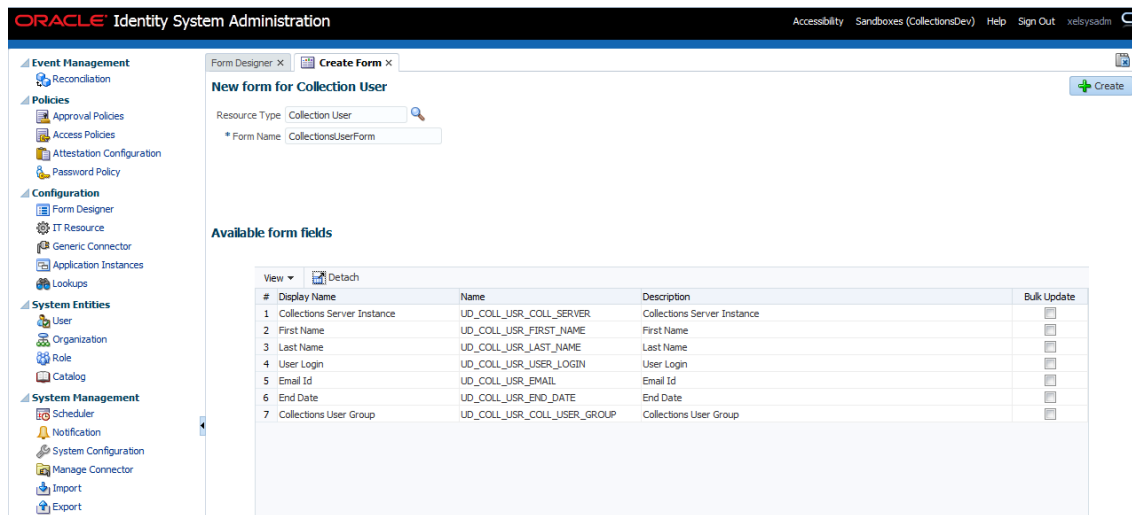
6. Select **Resource Type** as **Collections User** and provide a name for the form (for example, CollectionsUserForm).

Figure 3–76 Create Form - Resource Type (Collection User)



Available Form Fields will get displayed in the below section of the page.

Figure 3–77 Create Form Resource Type - Available Form Fields



Form fields corresponding to the UD_COLL_USR process form fields.

Below are the fields available for the form:

Table 3–7 UD_COLL_USR process form fields

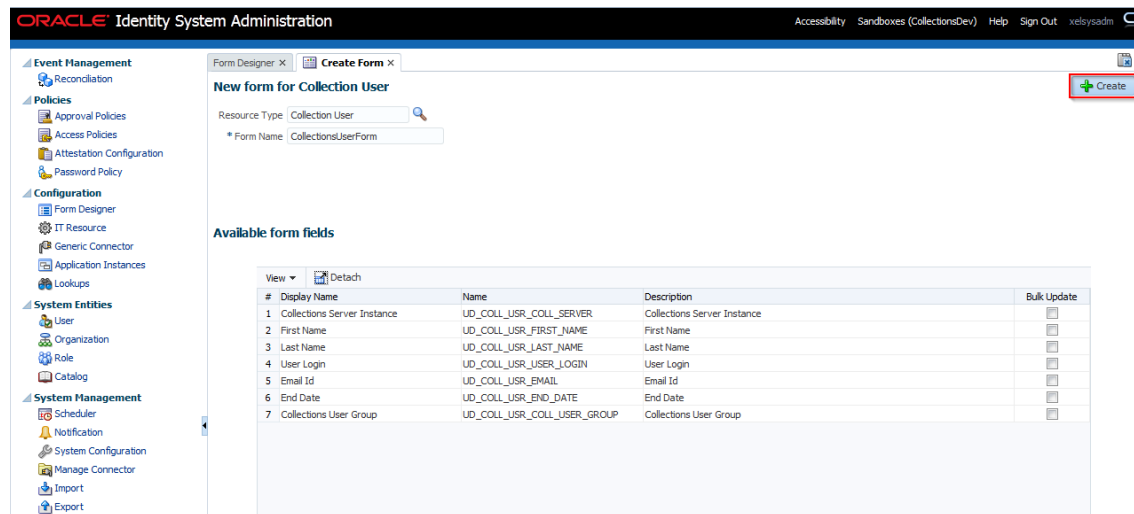
Display Name	Name	Length	Field Type
Collections Server Instance	UD_COLL_USR_COLL_SERVER		ITResourceLookupField
First Name	UD_COLL_USR_FIRST_NAME	256	Display Only Field
Last Name	UD_COLL_USR_LAST_NAME	256	Display Only Field
User Login	UD_COLL_USR_USER_LOGIN	256	Display Only Field
Email ID	UD_COLL_USR_EMAIL	256	Display Only Field
End Date	UD_COLL_USR_END_DATE	256	Display Only Field
Collections User Group	UD_COLL_USR_COLL_USER_GROUP	20	LookUpField

The **Collections Server Instance** field is used to specify the type of server for the IT resource. This field will not be visible in the **User Details** page.

7. Click **Create**.

A message is displayed stating that the form is created.

Figure 3–78 Create Form Resource Type - Create

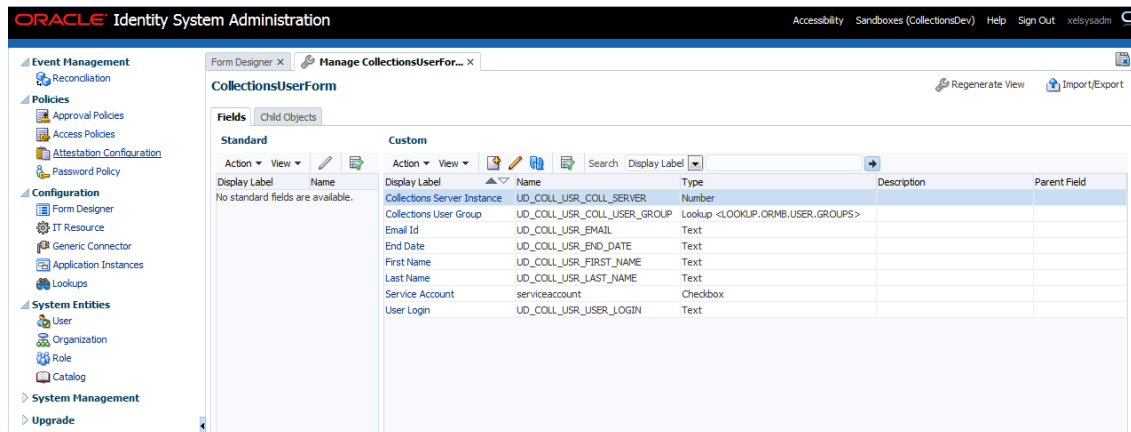


8. Refresh the **Search Results** in **Form Designer** page.

9. Select the **CollectionsUserForm** from the results.

Manage CollectionsUserForm page is displayed.

Figure 3–79 Manage Collections User Form



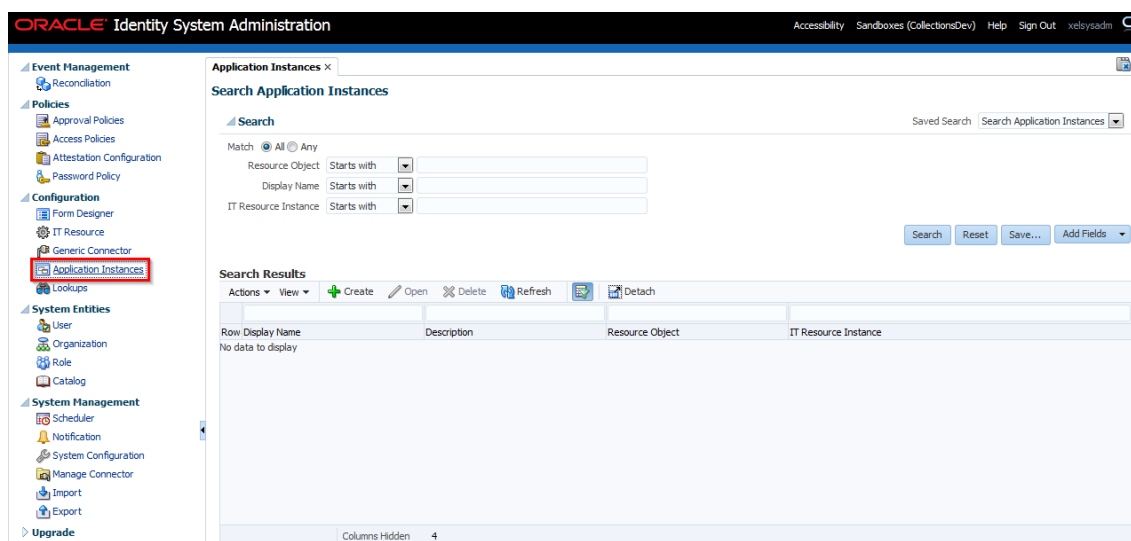
10. If required, you can export the sandbox to store all the changes made in your sandbox.
11. Publish the sandbox.

3.3.10 Create Application Instance

Application Instance wraps IT resource collection arguments and resource object collection user. Below is the configuration to create Collections Application Instance:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Application Instances**. The Application Instances page is displayed.

Figure 3–80 Creating Application Instance

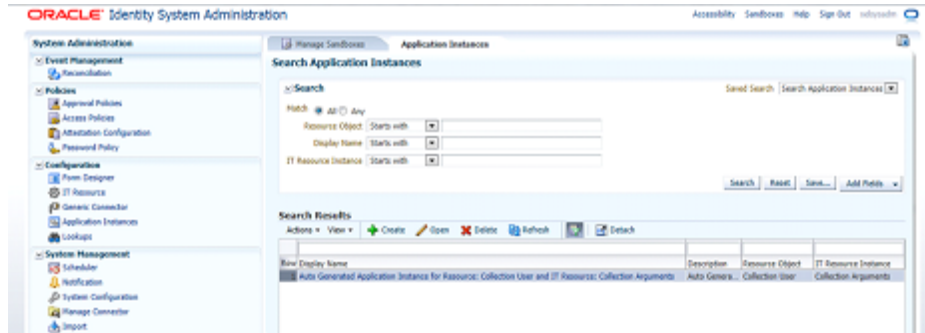


- Click **Search**. The search result is displayed in a tabular format.

If an **Auto Generated Application Instance for Resource** appears in the search results, you have to delete it using the steps below. If **Auto Generated Application Instance for Resource** does not show in the search results, skip below steps and move to step 4.

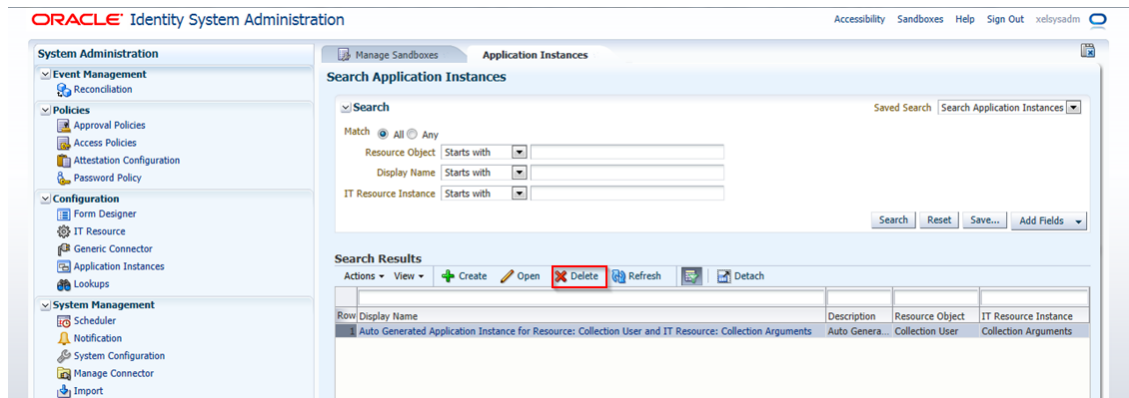
- Select **Auto Generated Application Instance for Resource: Collection User and IT Resource: Collection Arguments** row from the search results.

Figure 3–81 Creating Application Instance - Search



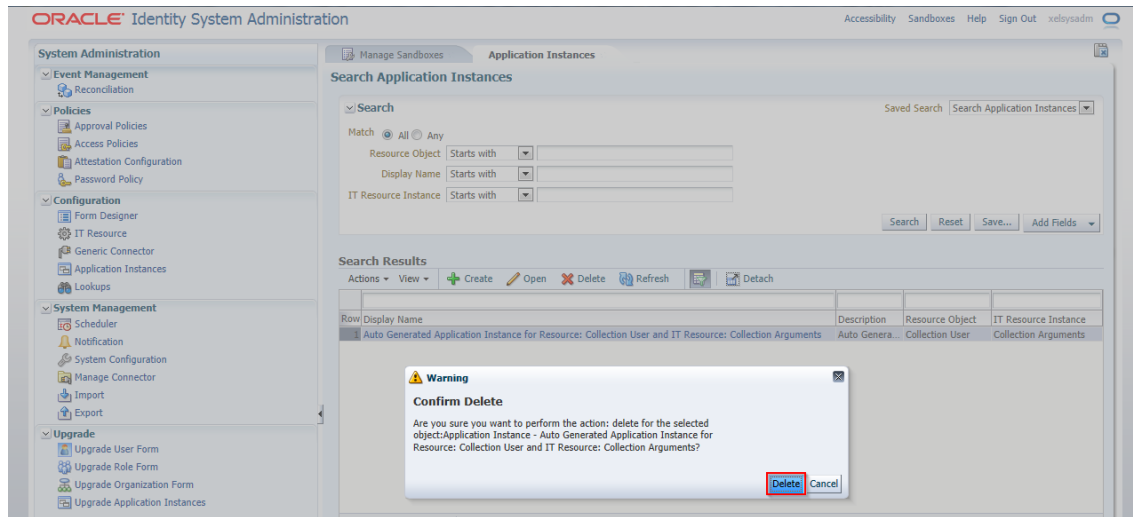
- From the Actions menu, select **Delete**. Alternatively, click **Delete** on the toolbar. A message box is displayed asking for confirmation.

Figure 3–82 Creating Application Instance - Delete



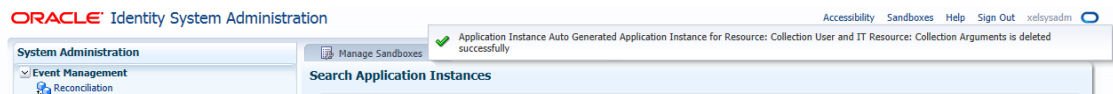
- Click **Delete** to confirm. The application instance is soft-deleted in Oracle Identity Manager.

Figure 3–83 Creating Application Instance - Confirm Delete



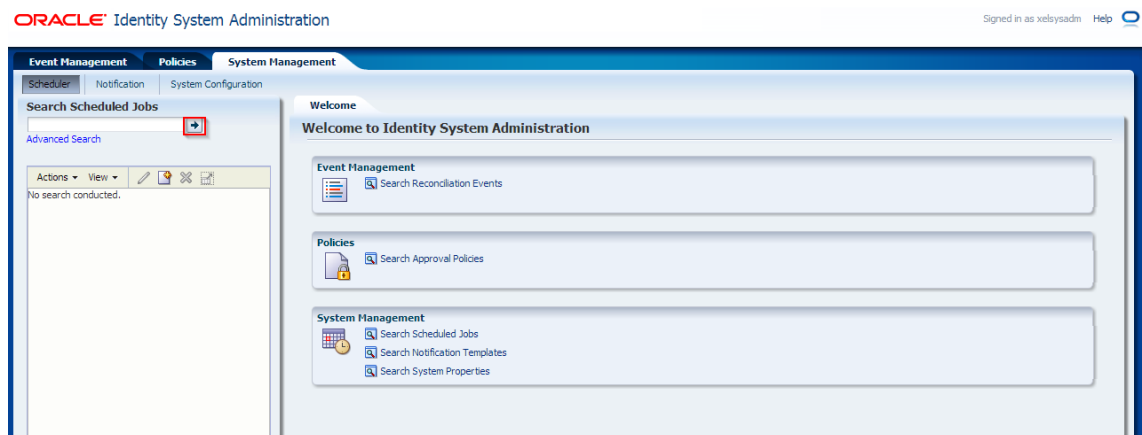
A message gets displayed that the application instance has been deleted successfully.

Figure 3–84 Creating Application Instance - Delete Message



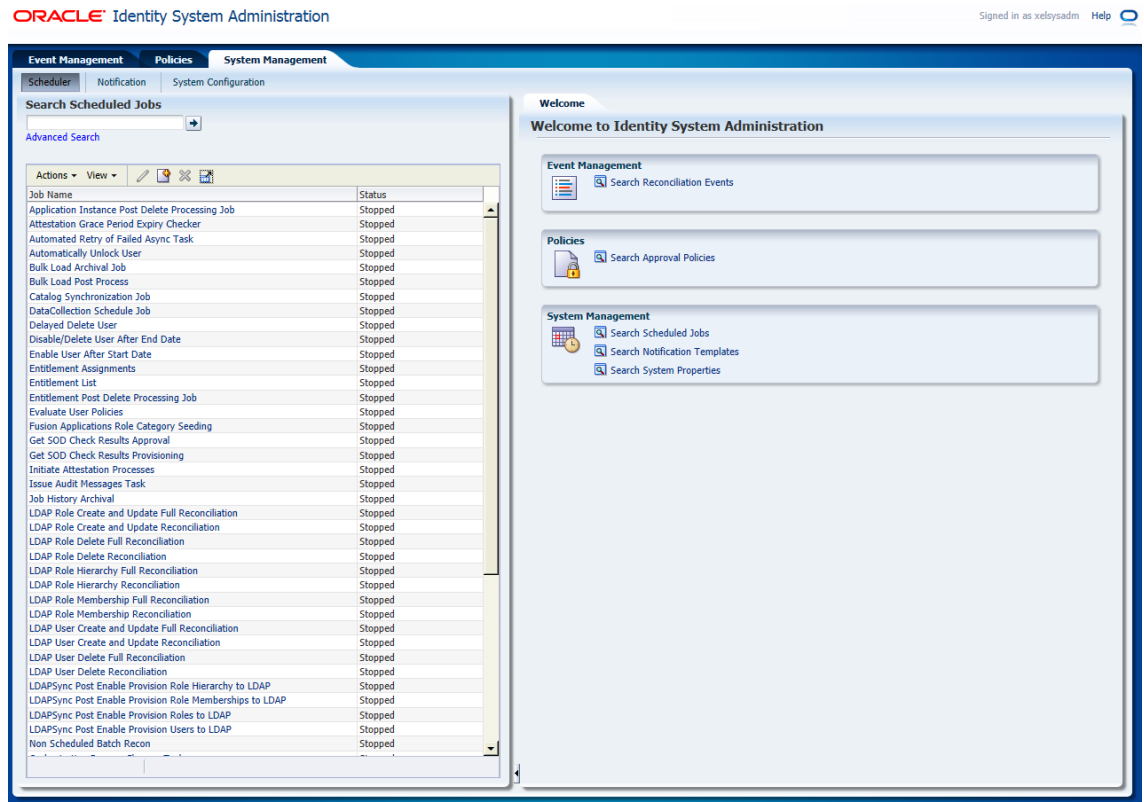
- d. Login to Oracle Identity System Administration. In the left pane, click **Scheduler** under **System Management**.
- e. A new window opens for Advanced System Administration. Click the **System Management** tab, and then click **Scheduler** tab.
- f. Click the search icon next to the Search Scheduled Jobs field.

Figure 3–85 Creating Application Instance - System Management Tab



A list of all predefined scheduled jobs is displayed

Figure 3–86 Creating Application Instance - Predefined Scheduled Jobs

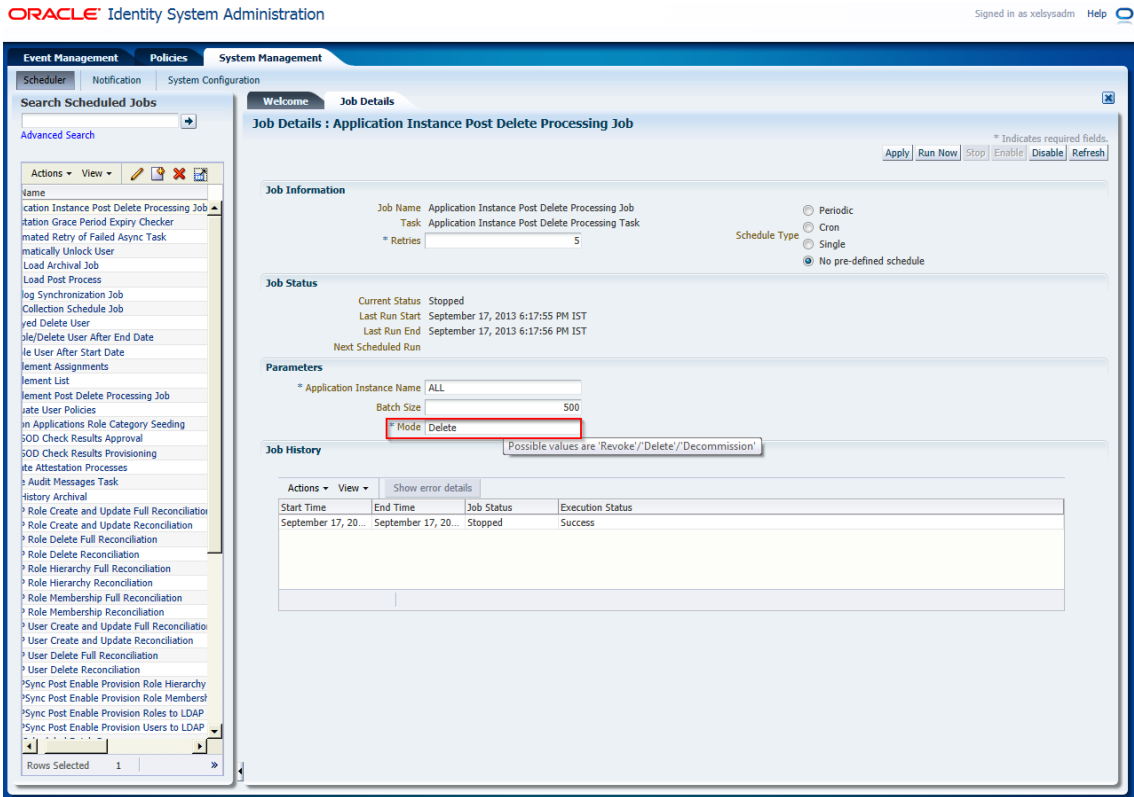


- g. Select **Application Instance Post Delete Processing Job** from the list.
- h. Run the Application Instance Post Delete Processing Job scheduled job using the Delete Mode. For this, enter Mode as **Delete** in Job Details page.

Note

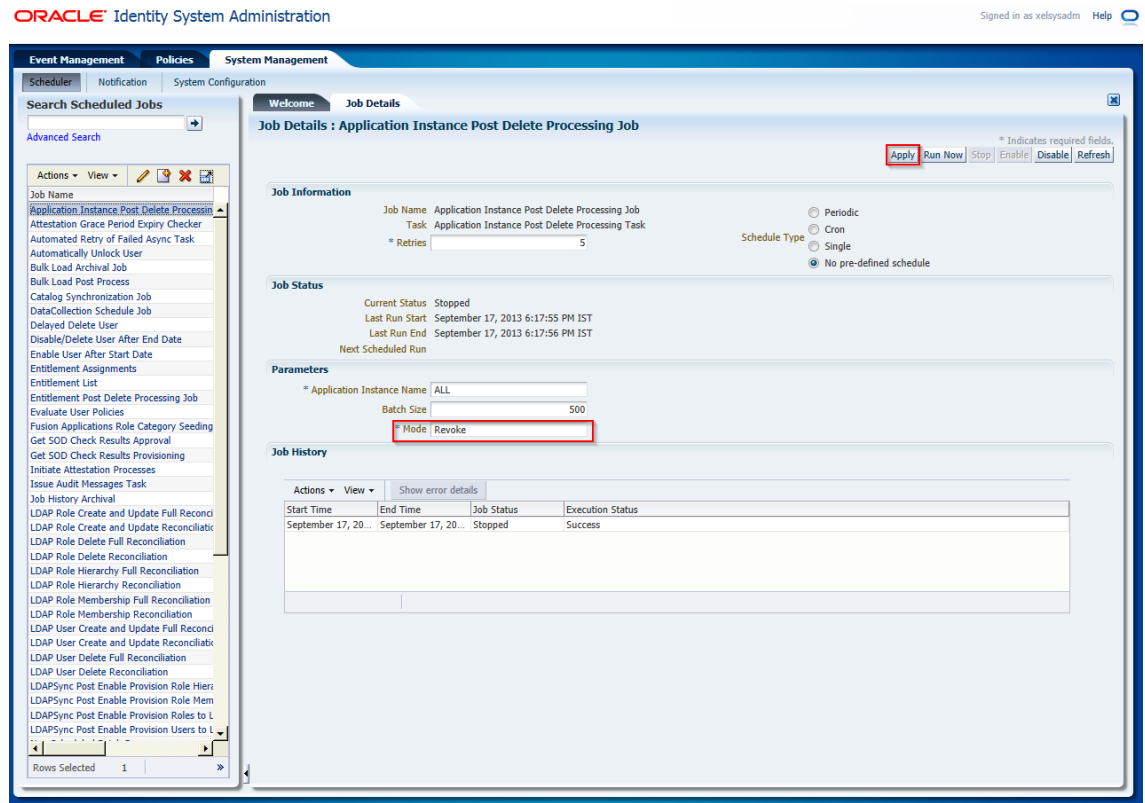
Using the Delete mode hard-deletes the accounts from all provisioning tasks and targets, and subsequently from Oracle Identity Manager.

Figure 3–87 Creating Application Instance - Mode Selection (Delete)



- i. Click **Refresh** to check the Job Status.
- j. Change the value of mode back to 'Revoke'.
- k. Click **Apply**.

Figure 3–88 Creating Application Instance - Mode Selection (Revoke)



- I. Run the Catalog Synchronization Job scheduled job.
 - To do this, select **Catalog Synchronization Job** from the Search scheduled tasks list.
- m. Click **Run Now** from the Job Details page.

Figure 3–89 Creating Application Instance - Catalog Synchronization

The screenshot displays the Oracle Identity System Administration interface. On the left, a sidebar lists various system management tasks, with 'Catalog Synchronization' selected. The main area shows the 'Job Details' for the 'Catalog Synchronization Job'. The 'Run Now' button is highlighted in red. The job information includes the name 'Catalog Synchronization Job', task 'Catalog Synchronization Task', and a start date of 'January 24, 2014 6:16:15 (GMT+05:30) Calcutta - India Time (IT)'. The job status is 'Stopped', and the next scheduled run is 'March 20, 2014 2:06:38 PM IST'. The job history table shows several successful runs.

Start Time	End Time	Job Status	Execution Status
March 20, 2014 2:06:38 PM IST	March 20, 2014 2:06:38 PM IST	Stopped	Success
March 20, 2014 1:06:38 PM IST	March 20, 2014 1:06:38 PM IST	Stopped	Success
March 20, 2014 12:06:38 PM IST	March 20, 2014 12:06:38 PM IST	Stopped	Success
March 20, 2014 11:06:38 PM IST	March 20, 2014 11:06:38 PM IST	Stopped	Success
March 20, 2014 10:06:38 PM IST	March 20, 2014 10:06:38 PM IST	Stopped	Success
March 20, 2014 9:06:38 PM IST	March 20, 2014 9:06:38 PM IST	Stopped	Success
March 20, 2014 8:06:38 PM IST	March 20, 2014 8:06:38 PM IST	Stopped	Success
March 20, 2014 7:06:38 PM IST	March 20, 2014 7:06:38 PM IST	Stopped	Success
March 20, 2014 6:06:38 PM IST	March 20, 2014 6:06:38 PM IST	Stopped	Success
March 20, 2014 5:06:38 PM IST	March 20, 2014 5:06:38 PM IST	Stopped	Success

This scheduled job identifies the soft-deleted application instances, and removes them from the catalog list.

- Click **Create** on the toolbar. The **Create Application Instance** page is displayed.

Figure 3–90 Creating Application Instance - Create

The screenshot displays the Oracle Identity System Administration interface for creating a new application instance. The 'Create' button is highlighted in red. The search results table is empty, showing 'No data to display'. The interface includes a search bar and a toolbar with various actions like 'Create', 'Open', 'Delete', 'Refresh', and 'Detach'.

Row Display Name	Description	Resource Object	IT Resource Instance
No data to display			

Figure 3–91 Creating Application Instance - Attributes Tab

The screenshot shows the Oracle Identity System Administration interface. The left sidebar contains a navigation menu with categories like Event Management, Policies, Configuration, System Entities, and System Management. The main content area is titled 'Create Application Instance' and is currently on the 'Attributes' tab. The form contains the following fields and controls:

- Name:** A text input field with an asterisk indicating it is a required field.
- Display Name:** A text input field with an asterisk indicating it is a required field.
- Description:** A large text area with a search icon on the right.
- Disconnected:** A checkbox.
- Resource Object:** A text input field with an asterisk and a search icon.
- IT Resource Instance:** A text input field with an asterisk and a search icon.
- Form:** A dropdown menu with a search icon.
- Parent Application:** A text input field with a search icon.

At the top right of the form, there are buttons for 'Save' and 'Cancel', and a note that asterisks denote required fields.

5. Specify following values:

Name: Collections

Display Name: Collections

Description: Collections application instance

Resource Object: Collection User (click Search icon to search)

IT Resource Instance: Collection Arguments (click Search icon to search)

Form: CollectionsUserForm

Note

The form attached to the application instance is created in section [Chapter 3.3.9 Create Form Associated with Application Instance](#).

6. Click **Save**.

Figure 3–92 Creating Application Instance - Save

Oracle Identity System Administration

Application Instances X Create App Instance X

Create Application Instance

Attributes

* Required Field Save Cancel

* Name Collections

* Display Name Collections

Description Collections application instance

Disconnected

* Resource Object Collection User

* IT Resource Instance Collection Arguments

Form CollectionsUserForm Edit Refresh

Parent Application Instance

Application instance is created successfully.

Figure 3–93 Creating Application Instance - Created Successfully

Oracle Identity System Administration

Application Instances X Search Application Instances

Search

Match All Any

Resource Object Starts with

Display Name Starts with

IT Resource Instance Starts with

Search Reset Save... Add Fields

Search Results

Actions View Create Open Delete Refresh Detach

Row	Display Name	Description	Resource Object	IT Resource Instance
1	Collections	Collections application instance.	Collection User	Collection Arguments

Columns Hidden 4

3.3.11 Security Configuration

Relevant client security policy must be configured mapping to service policy.

Default service policy configured for Collections User Provisioning is '**oracle/wss_saml_or_username_token_service_policy**'. Below configuration is required to configure client security policy.

Note

Current implementation is tested with '**oracle/wss_username_token_client_policy**' client security policy.

1. You must enable security flag to **true** in IT Resource Collections Arguments (`isSecurityEnabled = true`). If `isSecurityEnabled` flag is false then security policies are not applied.
2. Provide relevant client side policy name in IT Resource Collections Arguments (`securityPolicy = oracle/wss_username_token_client_policy`).
3. Required properties for policy are to be provided in the form of key-value pair in Lookup.

Create lookup LOOKUP.COLL.SECURITY.PARAMS and add properties in Code and meaning fields. Configured Lookup name must be provided in IT Resource Collections Arguments (`securityParamLookup = LOOKUP.COLL.SECURITY.PARAMS`).

Meaning: oracle.wsm.csf-key

Code: obp-collections

Figure 3–94 Create Lookup Type

Edit Lookup Type

* Meaning: LOOKUP.COLL.SECURITY.PARAMS Description:

Code: LOOKUP.COLL.SECURITY.PARAMS

Lookup Codes

View

* Meaning	* Code	Enabled	Sequence	Description
oracle.wsm.csf-key	obp-collections	<input checked="" type="checkbox"/>	<input type="text"/>	<input type="text"/>

Further configured key value pair would be added programmatically in **BindingProvider Request Context**.

4. User credentials must be stored in the Weblogic Credential Store for **oracle/wss_username_token_client_policy** client policy.
 - Log in to weblogic domain Enterprise Manager where OIM is deployed `http://<host>:<port>/em/`.
 - Navigate to **Farm_OIMDomain > Weblogic Domain > OIMDomain**.
 - Right click to open **Security > Credentials**.

Figure 3–95 Farm_OIM Domain

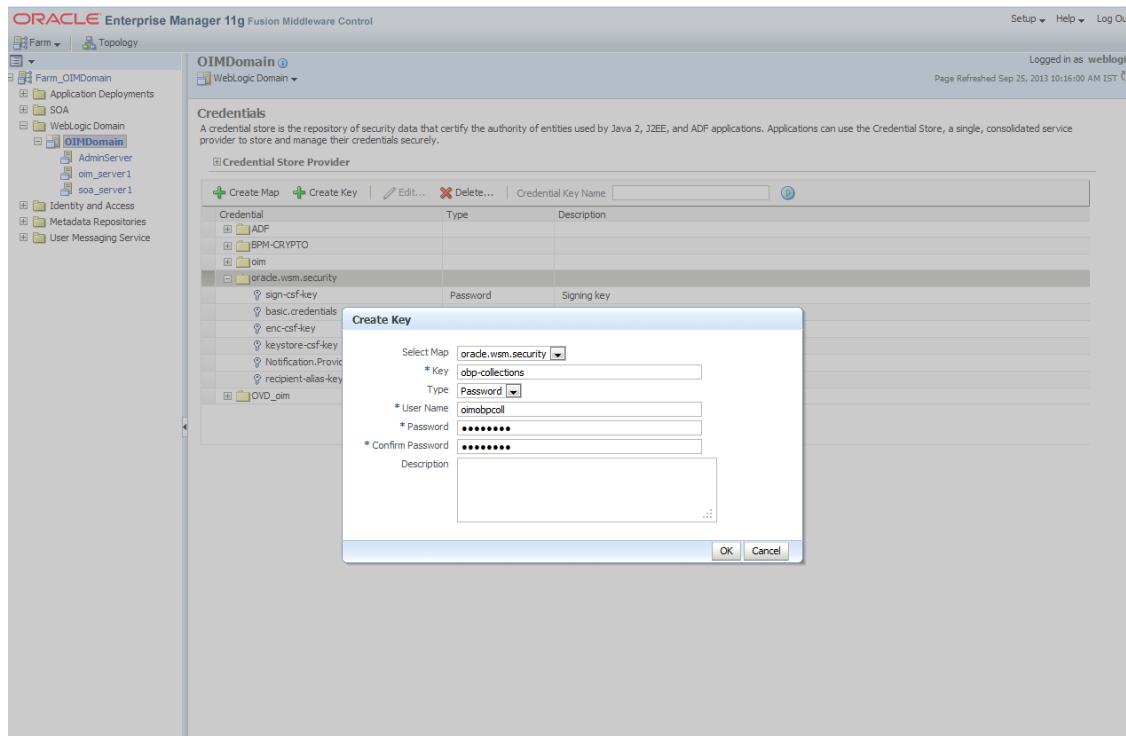
The screenshot shows the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The main view is for the 'Farm_OIMDomain'. A green circle indicates 100% health, and the status is 'Up (44)'. A table lists various components and their status:

Name	Status	Host	CPU Usage (%)
AdminServer	Up	ofss310654.in.orac	0.00
oim_server 1	Up	ofss310654.in.orac	0.00
soa_server 1	Up	ofss310654.in.orac	0.00
oim(11.1.2.0.0)	Up	ofss310654.in.orac	
mids-owsm	Up	ofss310654.in.orac	
mids-soa	Up	ofss310654.in.orac	
usermessagingservice-email (soa_server1)	Up	ofss310654.in.orac	
usermessagingserver (soa_server 1)	Up	ofss310654.in.orac	

The 'Farm Resource Center' section provides links for 'Before You Begin', 'Typical Administration Tasks', and 'Other Resources'.

5. Create key under **oracle.wsm.security** node named **obp-collections** as shown below. Provide system user (**OIMOBPCOLL**) and password as created above.

Figure 3–96 OIM Domain - Create Key



Note

Service policies are configured in **OBPSecurityAnnotations.properties**. Collections User Provisioning service policy is configured by adding below entry in the properties file:

```
com.ofss.fc.app.collection.service.userprovisioning.ORMBUserProvisioningApplicationService=oracle/wss_saml_or_username_token_service_policy
```

Further this configuration would be read in OBP programmatically and '**oracle/wss_saml_or_username_token_service_policy**' policy would be attached to '**com.ofss.fc.app.collection.service.userprovisioning.ORMBUserProvisioningApplicationService**' service.

3.4 OBP-Collections Configuration

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

- **Default User Group:** Default Collections User Group. It is used by system only; user should not add it manually. See the OBP Collections Day Zero Setup guide to get configured default user group.
- **User Display Profile:** Display profile value for OBP Collection 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 OBP Collections admin screens.

Figure 3–97 Collections Configuration

The screenshot displays the Oracle OBP Collection Admin interface. The page title is "Feature Configuration". The breadcrumb navigation shows "Main" and "Messages". The "Feature Name" is "C1-USRPROV". The "Feature Type" is "User Provisioning". The "Description" is "UserProvisioning custom properties".

Below the description, there is a table titled "Options" with the following data:

	Option Type	Sequence	Value	Detailed Description
+ [trash]	Default User Group	1	CLNHOSTUSER	Default user group value. It is used by system only.
+ [trash]	User Display Profile	1	NORTHAM	Display profile value for user
+ [trash]	User Expiry Date	1	2100-01-01	Default user expiry date value. It should be in format YYYY-MM-DD.

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 OBP Collections 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 OBP Collections.

The following table lists OBP Collections User fields (provisioned from OIM) and its constraints.

Table 4–1 OBP Collections User Fields

Field Name in OIM	Field Name in ORMB	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	Collections User Group represents User Group in OBP Collections. For every User, default User Group is populated in OBP Collections.
End Date	Date	N	Y	User's Log in expiry date.	

Note

- User creation from Native Collections is primarily discouraged. But in case of any failure in provisioning through OIM you can create or update the users through Native Collections screen. Below are the constraints to be followed when user is to be created through Native Collections:
 - Collections does not support User login 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 screen.
-

Figure 4–1 Create User - Mandatory and Optional Attributes

The screenshot shows the Oracle Identity Self Service 'Create User' form. The form is divided into several sections, each with a red box highlighting specific attributes. Red arrows point from these boxes to a red box labeled 'Collections mandatory attributes'. A green box highlights the 'End Date' field, with a green arrow pointing to a green box labeled 'Collections optional attribute'.

Form Sections and Attributes:

- Justification and Effective Date:** Justification, Effective Date
- Basic Information:** First Name, Middle Name, Last Name, Email, Manager, Organization, User Type, Display Name
- Account Settings:** User Login, Password, Confirm Password
- Account Effective Dates:** Start Date, End Date
- Provisioning Dates:** Provisioning Date, Deprovisioning Date
- Contact Information:** Telephone Number, Home Phone, Fax, Mobile, Pager, Home Postal Address, Postal Address, Postal Code, PO Box, State, Street, Country
- Preferences:** Locale, Timezone
- Other Attributes:** Common Name, Locality Name

Annotations:

- Red boxes (Mandatory Attributes):** First Name, Middle Name, Last Name, Email, User Login, Password, Confirm Password, Start Date, End Date, Provisioning Date, Deprovisioning Date.
- Green box (Optional Attribute):** End Date.

5 Functional Flow

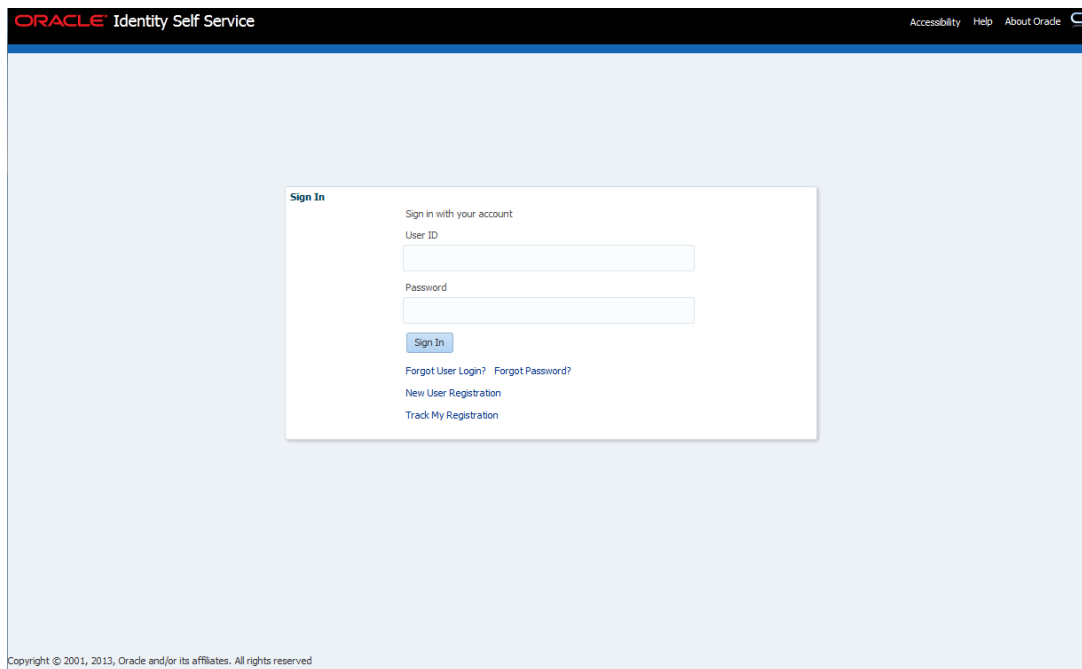
This chapter provides information on user provisioning activities.

5.1 Add Users in Collections

To add a user in OBP Collections, follow the steps:

1. Log in to Oracle Identity Self Service.

Figure 5–1 Oracle Identity Self Service Login Screen



2. In the left pane, under Administration, click **Users**.

The **Users** page is displayed.

5.1 Add Users in Collections

Figure 5–2 OID User Screen

The screenshot shows the Oracle Identity Self Service interface. On the left, the 'Administration' menu is expanded, and 'Users' is selected. The main content area is titled 'Users X' and contains a search form. The search form has a 'Match' dropdown set to 'Any' and several input fields for search criteria: User Login, First Name, Last Name, Identity Status, E-mail, Start Date, End Date, Display Name, Account Status, and Organization. Below the search form is a 'Search Results' section with a toolbar containing 'Create', 'Refresh', and 'Detach' buttons. The 'Create' button is highlighted with a red box. The search results table is currently empty, showing 'No data to display'.

3. Click **Create** on the toolbar to display the **Create User** page.

Figure 5–3 Create User Screen

The screenshot shows the 'Create User' form in the Oracle Identity Self Service interface. The form is titled 'Create User' and has a 'Submit' button. It is divided into several sections: 'Justification and Effective Date' with a 'Justification' text area and an 'Effective Date' field; 'Basic Information' with fields for First Name, Middle Name, Last Name, E-mail, Manager, Organization, User Type, and Display Name; 'Account Settings' with fields for User Login, Password, and Confirm Password; 'Account Effective Dates' with fields for Start Date and End Date; 'Provisioning Dates' with fields for Provisioning Date and Deprovisioning Date; 'Contact Information' with fields for Telephone Number, Home Phone, Fax, Mobile, Pager, Home Postal Address, Postal Address, Postal Code, PO Box, State, Street, and Country; and 'Preferences' with fields for Locale and Timezone.

4. In the **Create User** screen, specify the following values. For example:

First Name: Harry

Last Name: Potter

Email: harry.potter@oracle.com

Organization: Requests (required for OIM)

User Type: Employee (required for OIM)

User Login: HARRYPOTTER

Password: *****

Confirm Password: *****

End Date: Oct 30, 2018

Figure 5–4 Search and Select Organization

Search and Select: Organization

Search Advanced

Match All Any

Organization Name

Type

Organization Status

Parent Organization Name

Search Reset

Organization Name	Type
Xellerate Users	System
Top	System
Requests	System

OK Cancel

Figure 5–5 Create User

5. Click **Submit** to save user details in OID.

Once user data is saved successfully, the **Attributes** screen appears. A confirmation message appears to confirm that the user is successfully added to OID.

Note

Successful user creation in OID does not guarantee that the user is provisioned to Collections.

Figure 5–6 User Created

The screenshot displays the Oracle Identity Self Service interface for user management. The user profile for Harry Potter is shown with various tabs and sections:

- Attributes:**
 - Basic Information:** First Name: Harry, Middle Name, Last Name: Potter, Xellerate Type: false, E-mail: harry.potter@oracle.com, Manager, Organization, Requests, User Type: Employee, Account Status: Unlocked, User Login: HARRYPOTTER, Identity Status: Active, Display Name: Harry Potter.
 - Account Effective Dates:** Start Date, End Date: 10/30/2014.
 - Provisioning Dates:** Provisioning Date, Deprovisioning Date.
 - Contact Information:** Telephone Number, Home Phone, Fax, Mobile, Pager, Home Postal Address, Postal Address, PO Box, Street, State, Postal Code, Country.
 - Preferences:** Locale, Timezone.
 - Other Attributes:** Common Name: Harry Potter, Initials, Department Number, Employee Number, Hire Date, Title, Locality Name, Generation Qualifier.

OIM Schedule job Evaluate User Policies ran at scheduled interval. Access policy is applied and Process Task **Create User** of Process Definition **Collections User Provisioning** is triggered to provision user in Collections. If user data is successfully validated then user would be added to Collections.

6. Search added User and browse to **Accounts** tab. In the Browse tab, if the Resource Name is **Collections User** and Status is **Provisioned** then user is successfully added to OBP Collections.

Figure 5–7 Verifying User name

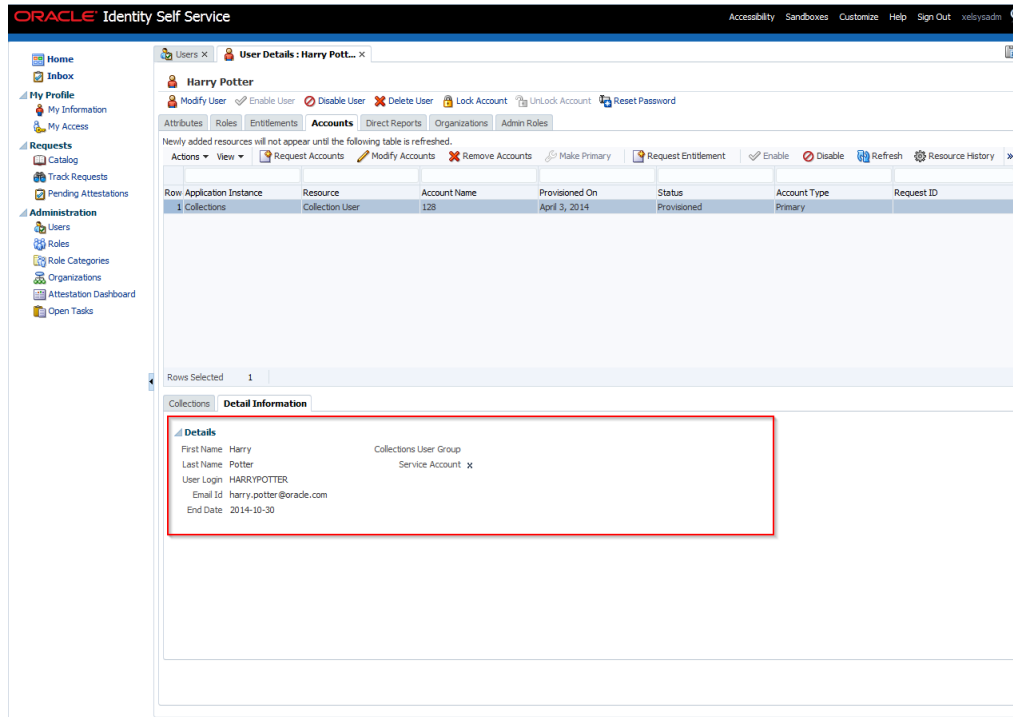
The screenshot shows the Oracle Identity Self Service interface with the **Accounts** tab selected for user Harry Potter. A table displays the account details:

Row	Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID
1	Collections	Collection User	128	April 3, 2014	Provisioned	Primary	

For more information, see [Chapter 6.2 Verify Users in Native Collections](#).

7. In the **Accounts** tab, click each account to view a summary of the account.

Figure 5–8 View Account Summary



The fields and values displayed in **Detail Information** of the account are as below:

- **First Name:** Harry
- **Last Name:** Potter
- **User Login:** HARRYPOTTER
- **Email Id:** harry.potter@oracle.com
- **End Date:** 2018-05-30
- **Collections User Group:** (Blank)
- **Service Account:** (Disabled)

Note

Service accounts are general administrator accounts that are used for maintenance purposes. It differs from a regular account by a flag. This flag is set by the user requesting the resource, or by the administrator directly provisioning the resource. Since this feature is not used currently, this checkbox will be disabled on the **User Details** page.

8. To add a user group, select the account for which you want to add the User Group.
9. From the **Actions** menu, select **Modify**. Alternatively, click **Modify Accounts** on the toolbar.

The **Modify Account** page is displayed.

10. Select the required group from the **Collections User Group** lookup (for example, C1_BSERVICES) and submit the request from the Catalog page (Modify Account page). For this, select the required group from the **Search and Select: Collections User Group** pop-up window and click **Ok**.

Figure 5–9 Modifying Account

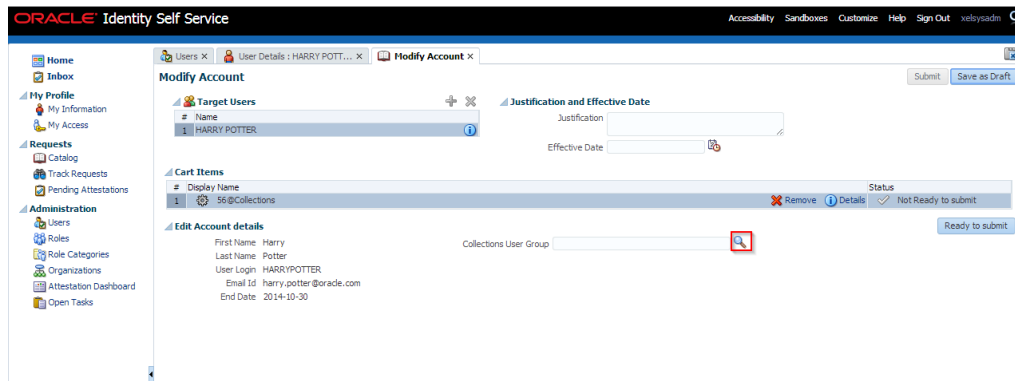
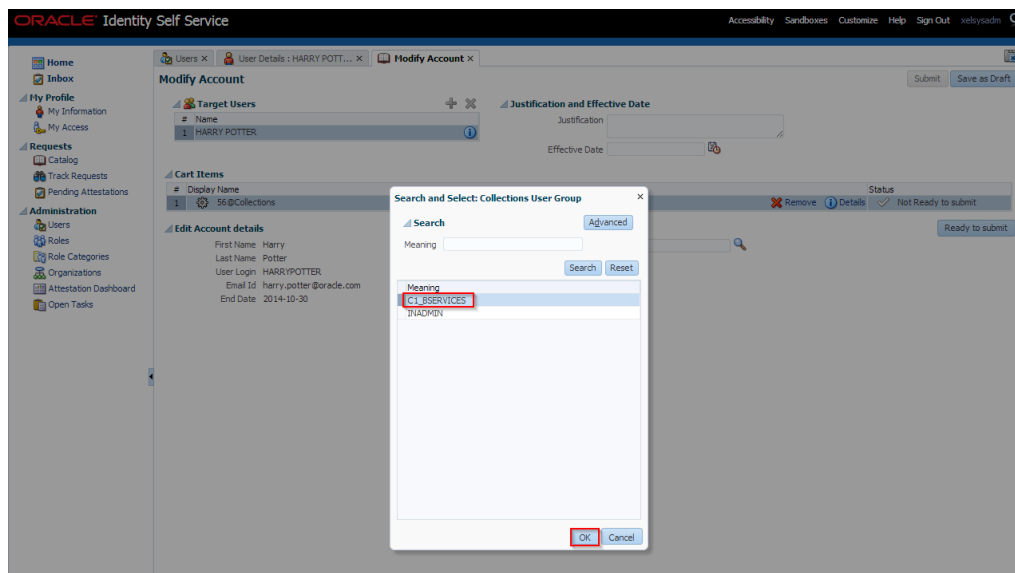


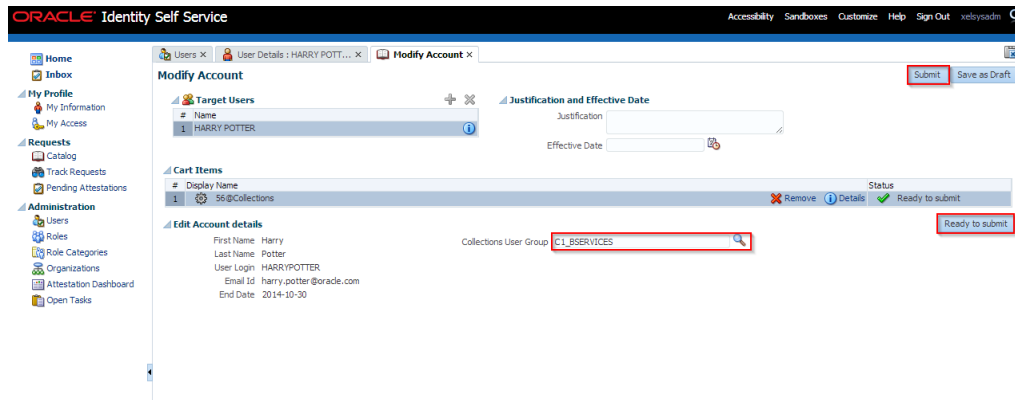
Figure 5–10 Selecting Collections User Group



11. Click **Ready to Submit** and **Submit**, respectively to submit the request.

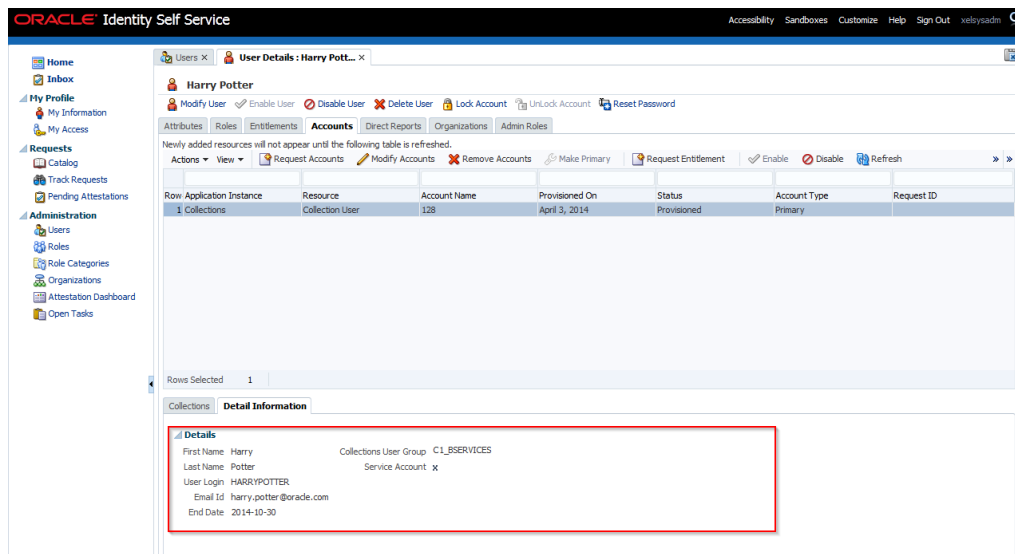
5.1 Add Users in Collections

Figure 5–11 Submitting Request



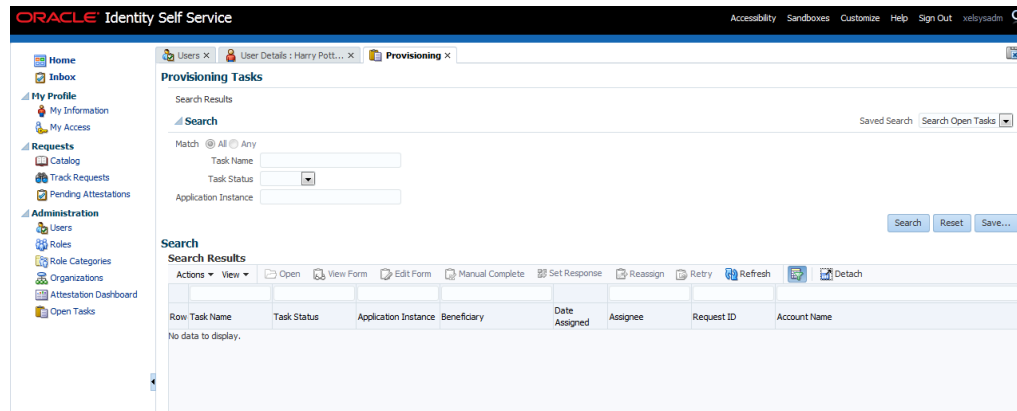
12. Go back to **Accounts** tab in **User Details** page and refresh the resources table. Click the required account's row to view the latest changes in the **Detail Information** section.

Figure 5–12 Viewing Updated User Details



13. To view status of all User provisioning tasks, navigate to **Open Tasks** and search for **Collections** Application Instance. All failed Collections provisioning task will be shown (Task Status = Rejected) and successful task are not shown.

Figure 5–13 Viewing User Provisioning Tasks



If task status is **Rejected** then check all mandatory attributes required for Collections User Provisioning are populated. For more information, see [Chapter 4 User Fields and Constraints](#)

Open the Rejected task in **Provisioning Tasks** page to check the cause of failure while creating the user.

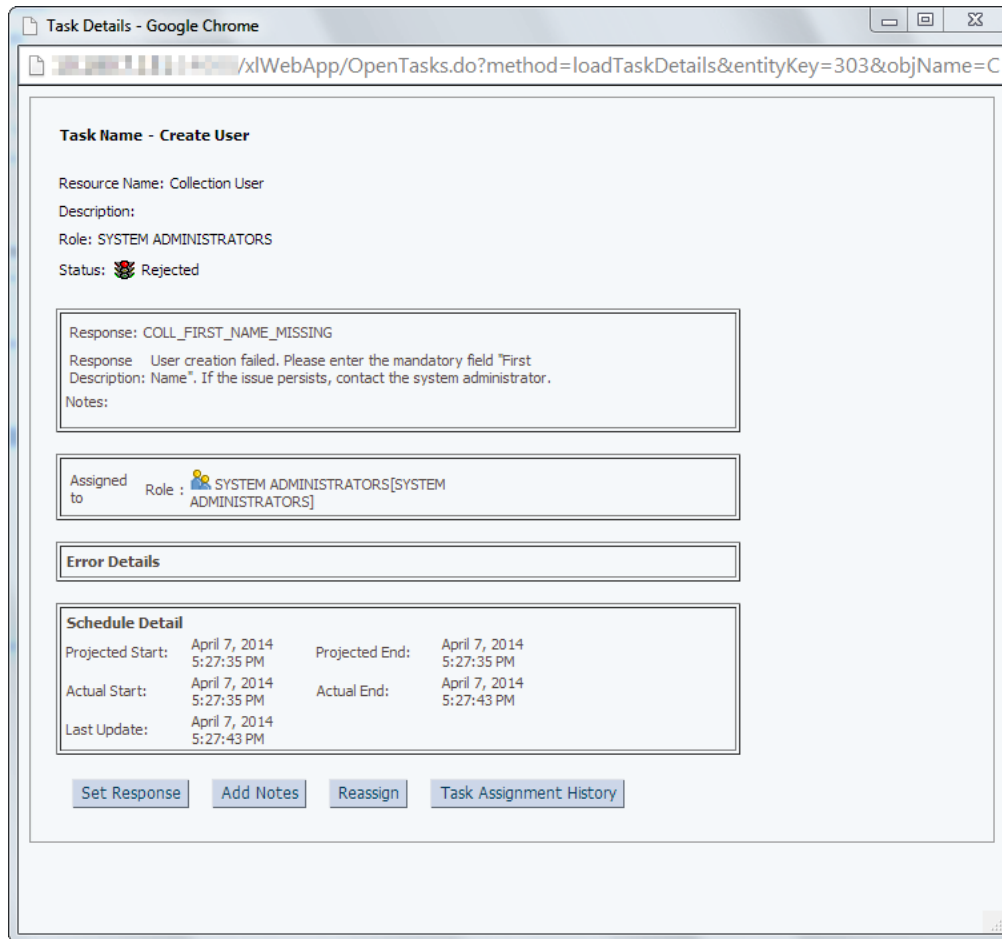
Below are the response codes and descriptions shown in the **Task Details** page for a Rejected Create User task:

Table 5–1 Response Codes for a Rejected Create User Task

S. No.	Scenario	Response	Response Description
1	User already exists in Collections but not in OIM/OID	COLL_DUPLICATE_USR	User creation failed. User with the given 'User Login' already exists in Collections. Please provide a unique User Login Id. If the issue persists, contact the system administrator.
2	First Name is missing	COLL_FIRST_NAME_MISSING	User creation failed. Please enter the mandatory field 'First Name'. If the issue persists, contact the system administrator.
3	Last Name is missing	COLL_LAST_NAME_MISSING	User creation failed. Please enter the mandatory field 'Last Name'. If the issue persists, contact the system administrator.
4	Email Id is missing	COLL_EMAIL_ID_MISSING	User creation failed. Please enter the mandatory field 'E-mail'. If the issue persists, contact the system administrator.

For example, if the **First Name** is missing while creating user, task details will appear as below for that **Create User** task.

Figure 5–14 Task Details



- If mandatory attributes are missing, populate them and resubmit the request. Check Resource status in Accounts tab, if status is **Provisioned**, then user details are successfully provisioned to Collections. Further, user can mark that Provisioning task as **Manual Complete** to remove task from rejected list.
- If all mandatory attributes are present and still the provisioning task status is **Rejected**, then contact your administrator. Administrator can check log files and resolve problem. Further User can **Retry** provisioning task.

14. Alternate Flow:

- **Populated Mandatory Fields only:** See [Chapter 4 User Fields and Constraints](#)
 - All required fields are populated with valid data.
 - User will be successfully added to Collections.
 - See **Step 6** to validate successful addition of user.

- Collections User Group not added:
 - All fields are populated with valid data, except Collections User Group is not added.
 - User will be successfully added to Collections with default User Group (default access is provided).
 - See [Chapter 6.2 Verify Users in Native Collections](#) to validate successful addition of user.
- **Fields constraints are Violated:** See [Chapter 4 User Fields and Constraints](#).
 - a. Mandatory fields missing or fields length is not valid or incorrect email format data is populated.
See [Chapter 4 User Fields and Constraints](#) for complete list of fields and its constraints.
 - b. Click **Save**.
Some of the fields that have client side validation would be highlighted with error on **Create User** screen. Note that only some validations belong to client side.
 - c. After rectifying validations errors, click **Save**.
Only client side errors are resolved and some of the fields may still violate constraints.
 - d. After Evaluate User Policies job run is completed, check the status of user provisioning to Collections, locate the **Accounts** tab. If the **Resource Name** is **Collection User** and the **Status** is **Provide Information**, then user is not provisioned to Collections.

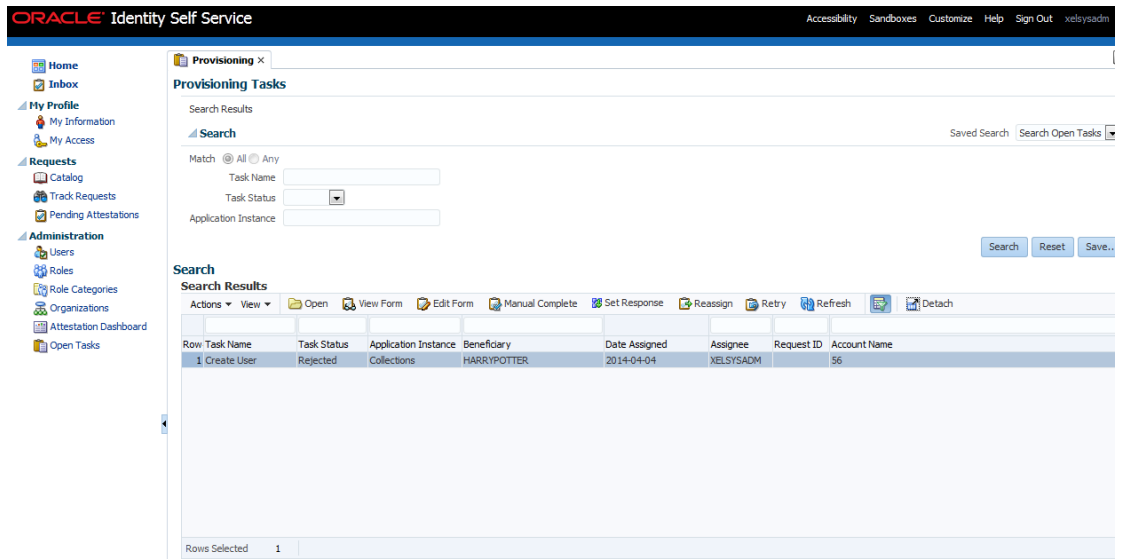
Figure 5–15 Status of User Provisioning to Collections

The screenshot shows the Oracle Identity Self Service interface for user 'Harry Potter'. The 'Accounts' tab is active, displaying a table with the following data:

Row	Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID
1	Collections	Collection User	128	April 3, 2014	Provide Information	Primary	

- e. Also, check open provisioning tasks. Create User task status would be **Rejected** for user whose details need to be provisioned.

Figure 5–16 Open Provisioning Tasks



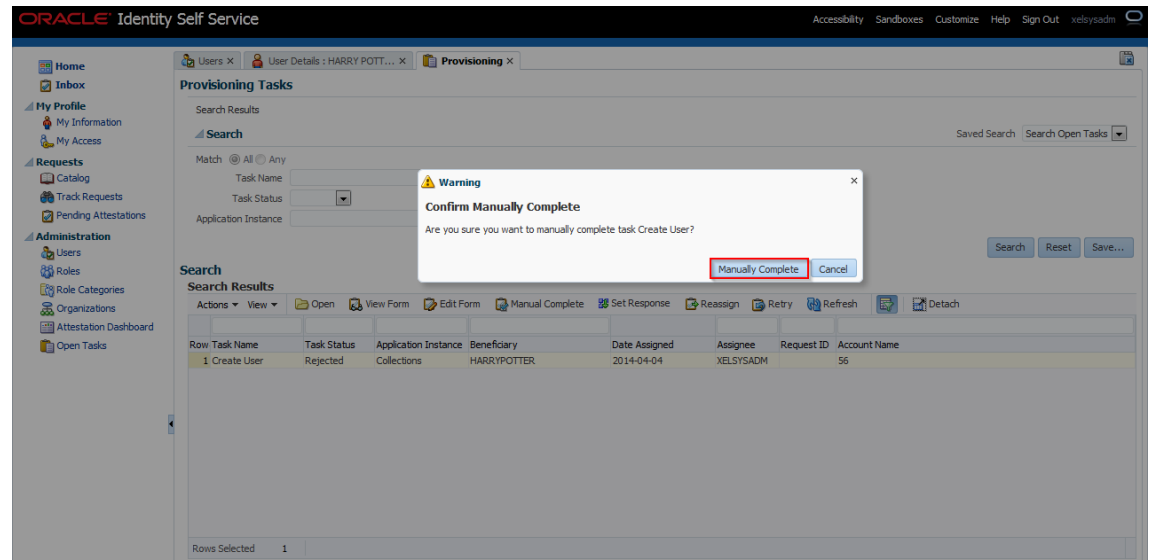
- f. Modify user details to make it valid. See [Chapter 4 User Fields and Constraints](#).
- g. Click **Submit**. If all fields are valid, user would be provisioned to Collections.

Note

If the field length exceeds specified limit then it would be truncated and saved in OBP Collections.

- h. See **Step g** to validate successful addition of user. If the user details are successfully provisioned then mark Create User provisioning task of user as **Manually Complete** to remove entry from rejected task status list.

Figure 5–17 Manual Completion - Create User Provisioning Task



- Duplicate User Login/Email Not Allowed:
 - Duplicate User Login Id and Email is not allowed.
 - If user tries to add duplicate user login error will be displayed.
- User is expired on addition (When End Date is less than or equal to Current Date):
 - All fields are populated with valid data. End date is populated with less than or equal to current date/today's date.
 - Since the user is already expired, it is not provisioned to Collections and there is no Status available in the **Resource** tab.
 - There is no way to bring the user to Collections (even by modifying end date to greater than current date). As the expired user is considered in delete state.
 - If there is a need to activate the user again, delete the earlier user details and add the user with end date > current date.

5.2 Modify Users in Collections

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

Figure 5–18 Searching User

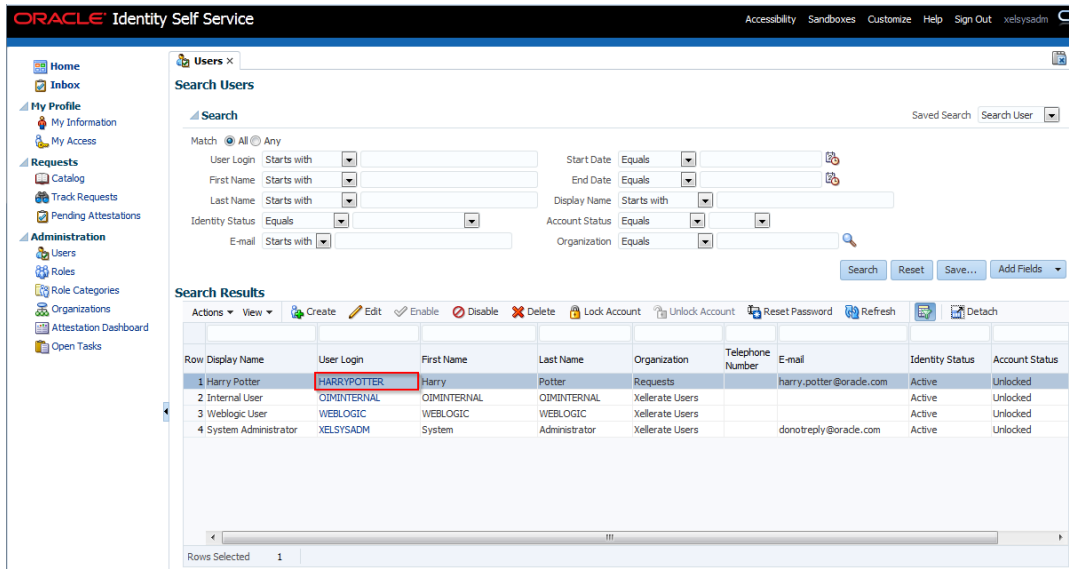
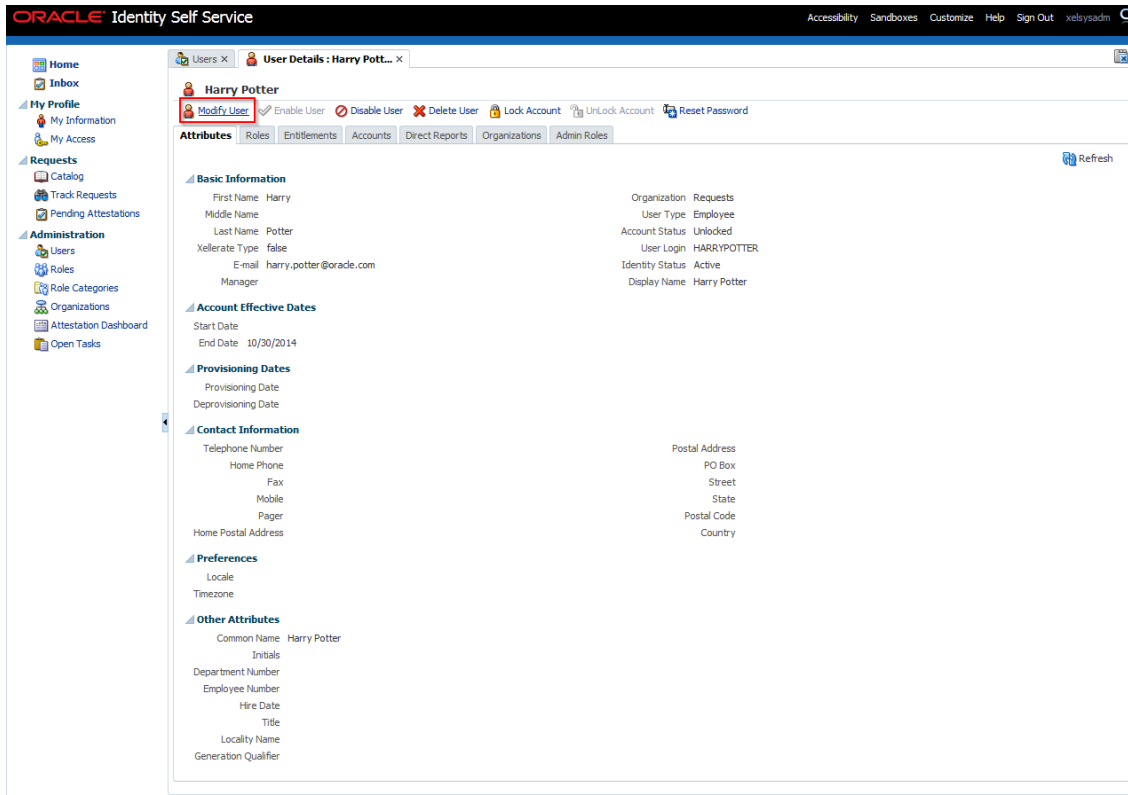


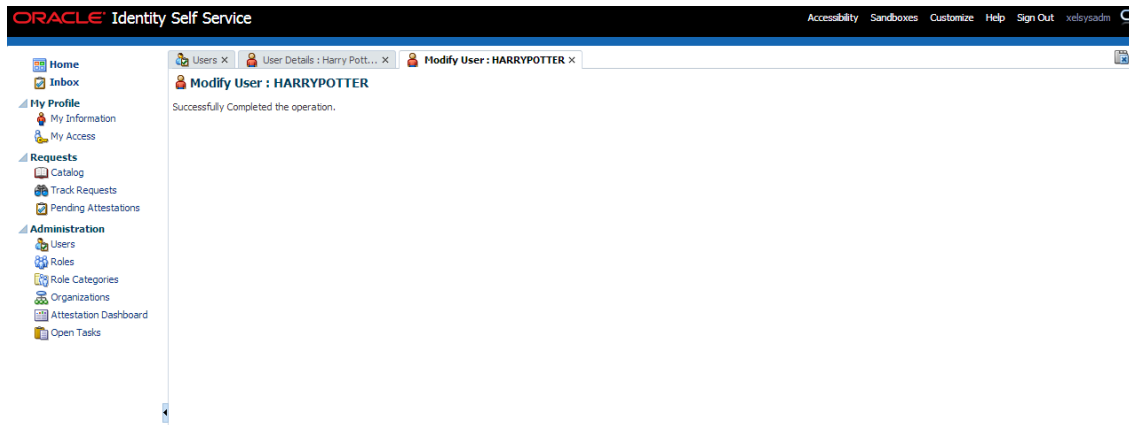
Figure 5–19 Detailed Information about the User



To modify a user, perform the below steps:

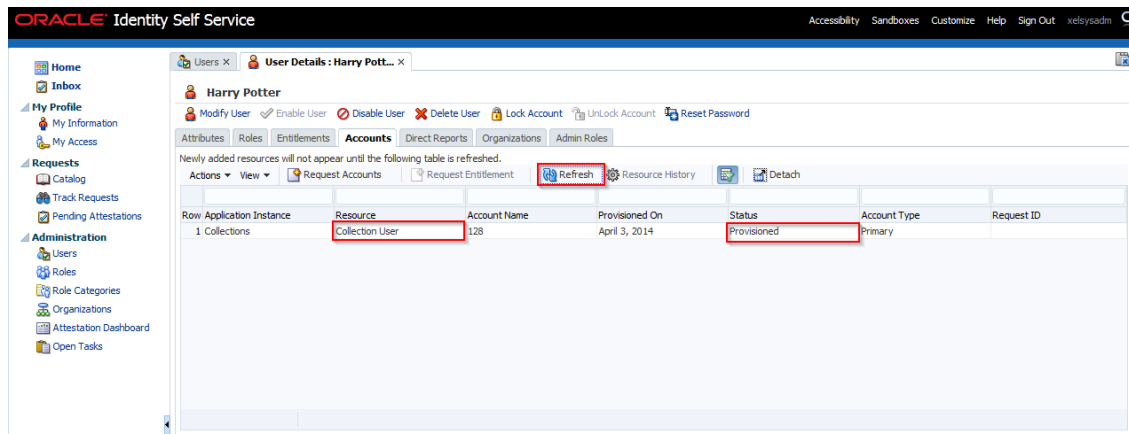
1. Click **Modify User** to open Modify User page. Modify the user details as per the requirement.
2. Click **Submit**. If the user details are valid (that is, if it does not violate any validation) then user details would be modified. A message will be displayed on successful completion of the modify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

Figure 5–20 Modify User Confirmation



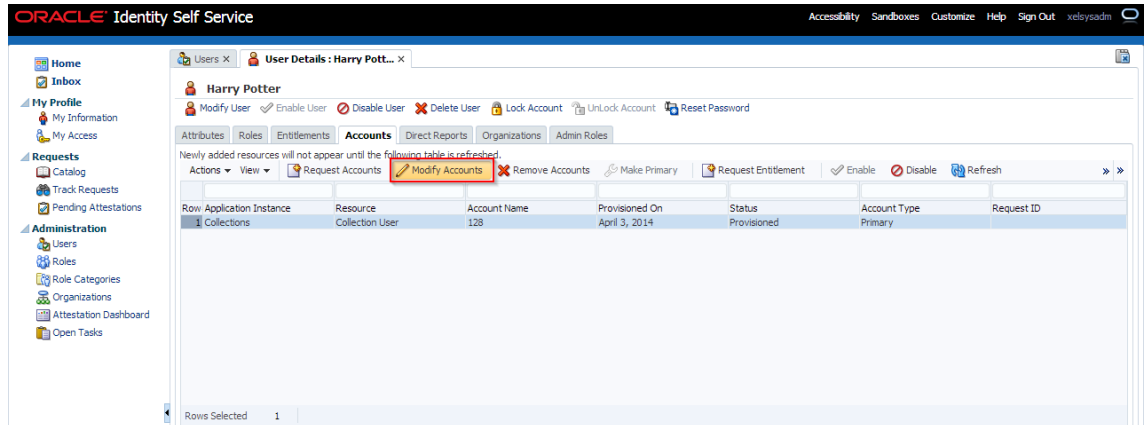
3. In User Details page locate **Accounts** tab. If Resource Name is **Collection User** and Status is **Provisioned** then user details are successfully modified and provisioned to Collections.
4. If the data does not appear when the user is added, click **Refresh**.

Figure 5–21 Viewing Modified and Provisioned User Details



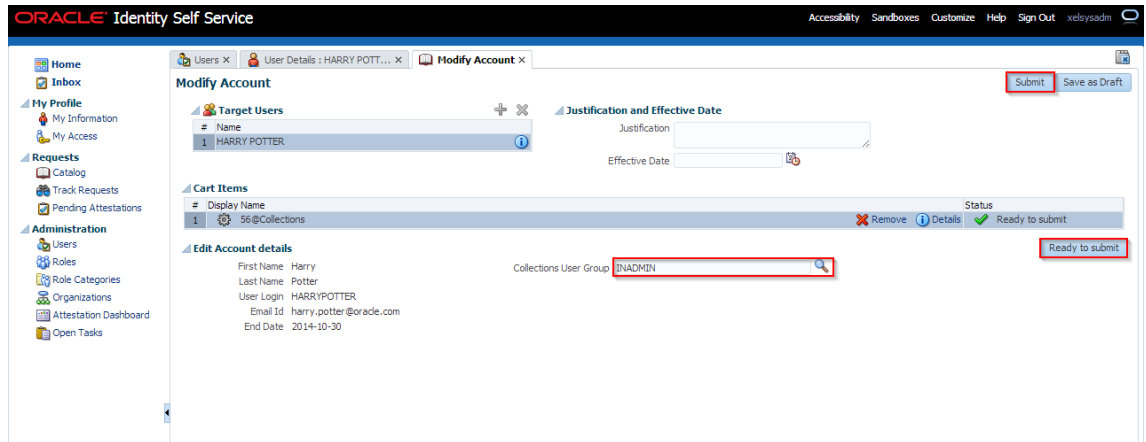
5. Select the account to view the modified values in **Detail Information** section.
6. To modify the Collections User Group, follow the below steps:
 - a. In the **Accounts** tab, select the account that you want to modify.
 - b. From the **Actions** menu, select **Modify**. Alternatively, click **Modify Accounts** on the toolbar. The **Catalog** page is displayed.

Figure 5–22 Catalog page



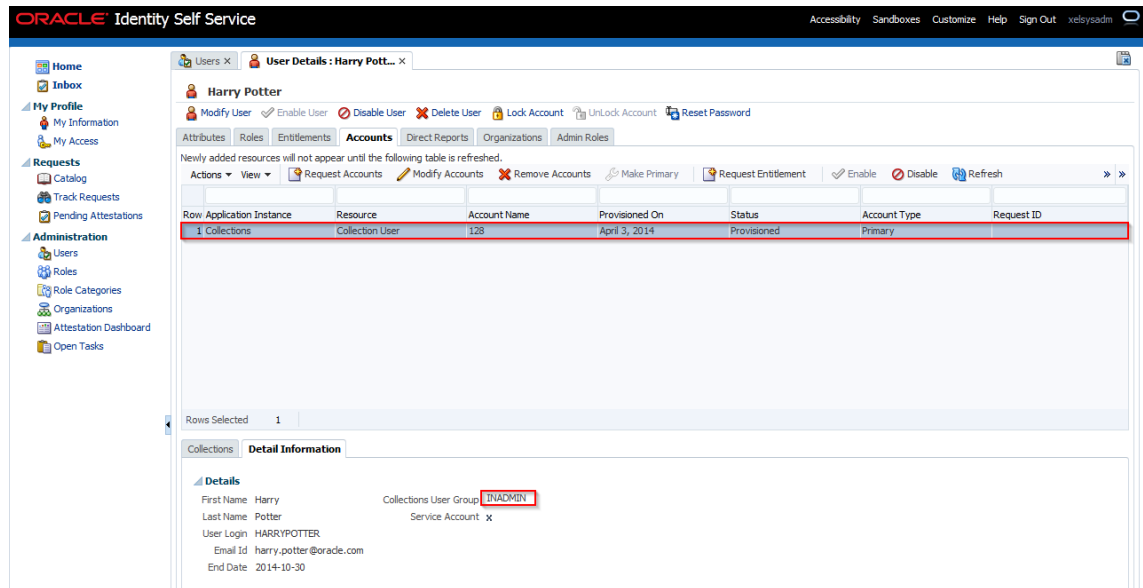
- c. Select the required group (for example, INADMIN) from **Collections User Group**, lookup and submit the request from the **Catalog** page. The account will be modified after the request is approved.
- d. Select the required group from the **Search and Select: Collections User Group** pop-up window.
- e. Click **Ok**.
- f. Click **Ready to Submit** and **Submit**, respectively to submit the request.

Figure 5–23 Submitting Request



- g. 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.

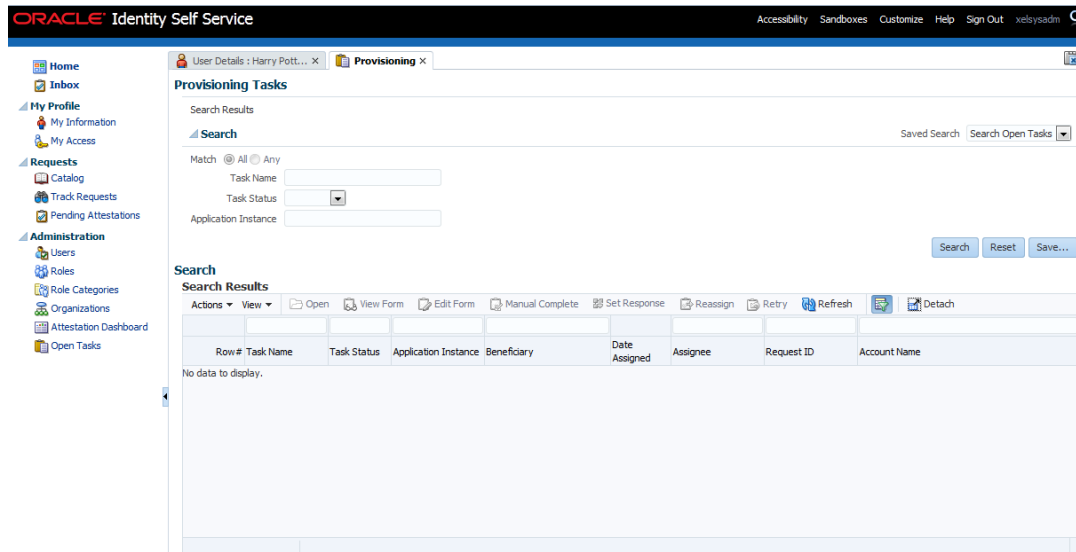
Figure 5–24 Viewing Changes



Currently, we are not making use of the Service Account feature, so the check box will remain disabled on the **User Details** page.

- To view status of all User Provisioning tasks, navigate to **Open Tasks** and search for **Collections** Application Instance. All failed Collections provisioning task will be shown (Task Status = Rejected) and successful task are not shown.

Figure 5–25 Viewing User Provisioning Task



If task status is **Rejected** then check all mandatory attributes required for Collections User Provisioning are populated. See [Chapter 4 User Fields and Constraints](#).

- If mandatory attributes are missing, populate them and resubmit the request. Check Resource status in **Accounts** tab, if status is **Provisioned**, then user details are successfully provisioned to Collections. Further, the user can mark that provisioning task as **Manual Complete** to remove the task from rejected list.
- If all mandatory attributes are present and still provisioning task statuses is **Rejected**, then contact your administrator. Administrator can check log files and resolve problem. Further, user can **Retry** provisioning task.

For each field modification, OIM triggers different Process Task. So in all, if six fields are modified then six requests for modification will be sent to OBP Collections. This is technical limitation with current implementation.

Each provisioning task holds all user provisioning fields. If the number of user fields are modified, then all provisioning task for particular request will either fail or success.

Following table lists task invoked when user field is modified:

Table 5–2 Tasks involved while modifying User fields

User Field	Task Name
First Name	Change First Name
Last Name	Change Last Name
Collection User Group	Collections User Group Updated
Email	Change Email
End Date	Change End Date
User Login	Change User Name

8. Alternate Flow:

- **Fields constraints are Violated:** See [Chapter 4 User Fields and Constraints](#)

- a. Mandatory fields removed or updated field's length is not valid or incorrect email format data is populated.

See [Chapter 4 User Fields and Constraints](#) for complete list of fields and its constraints.

- b. Click **Submit**.
- c. Some of the fields having client side validation would be highlighted with error on Modify User form. Note, only some validations are client side.
- d. After rectifying validations errors, click **Submit**. User would be updated to OID.
- e. Only client side errors are resolved and some of the fields are still violating constraints.
- f. To check the status of user provisioning to Collections, traverse to **Accounts** tab. Resource Name is **Collection User** and Status is **Provide Information** then user is not provisioned to Collections.

Sometimes data doesn't appear as soon as user is added. Click **Refresh**.

For example, First Name is removed and Last Name is modified. Since one of mandatory field is missing for Collections User Provisioning, provisioning request failed.

Figure 5–26 User Provisioning Status

The screenshot shows the Oracle Identity Self Service interface for user 'Harry Potter'. The 'Accounts' tab is selected, showing a table with the following data:

Row	Application Instance	Resource	Account Name	Provisioned On	Status	Account Type	Request ID
1	Collections	Collection User	128	April 3, 2014	Provide Information	Primary	

The failed provisioning task will be listed in open tasks list. Provisioning task will be equal to number of fields modified.

Figure 5–27 Failed provisioning tasks

The screenshot shows the Oracle Identity Self Service interface for user 'Harry Potter' in the 'Provisioning' tab. The search results table is as follows:

Row #	Task Name	Task Status	Application Instance	Beneficiary	Date Assigned	Assignee	Request ID	Account Name
1	Change Email	Rejected	Collections	HARRYPOTTER	2014-04-04	XELSYSADM		128
2	Change First Name	Rejected	Collections	HARRYPOTTER	2014-04-04	XELSYSADM		128

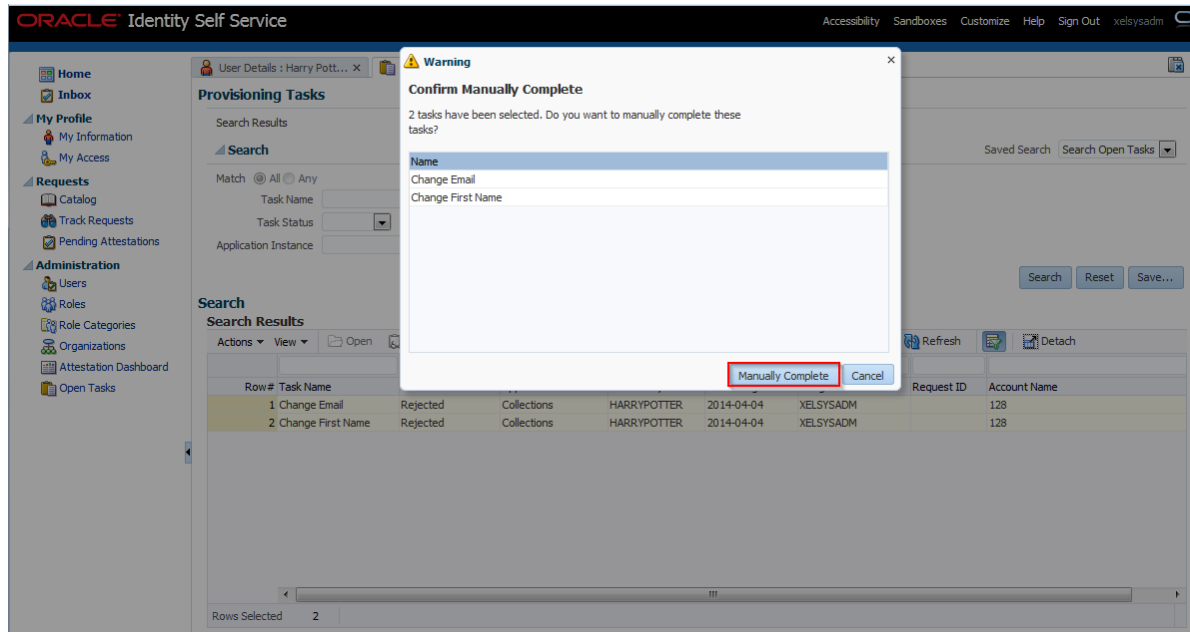
- g. Modify the user details to make it valid. See [Chapter 4 User Fields and Constraints](#).
- h. Click **Submit**. If all fields are valid, user would be provisioned to Collections.

Note

If field length exceeds specified limit, then it would be truncated and saved in Collections.

- i. See Step 4 to validate successful modification of User.
- j. Once modified, user details are successfully provisioned. User can mark failed provisioning task as **Manually Complete**.

Figure 5–28 Task confirmation dialog box



- **Modify User Login (Not Supported):**
 - Though user can modify the User Login from User form, it is not supported in Collections. **User Login** is primary key in Collections.
 - If the user tries to modify User Login then new user would be created in Collections with new **User Login**. Earlier user still persists.
 - User has to manually delete earlier user (User Login before modification) in Collections.

Note

If some manual changes have been done from the Collections Admin screens to earlier user, then the same has to be done to new user.

- Duplicate User Login is not allowed.
- **Modify Collections User Group:**
 - If **User Group** value is changed, then earlier would be updated with new Group in Collections.

- If User Group selection is removed from the drop-down list, then unselected group would be deleted from Collections. Only default group would be present, that is groups populated from native Collections native Admin Screen.
- Collection modifies User Group value based on old and new value of Collections User Group received from OIM. It deletes old value and adds new value sent for User Group. Old value of User Group is value being modified and new value is value being added from OIM. Collection User Group of successfully provisioned user is modified multiple times, if user provisioning to Collections fails due to some error. In such cases, the problem is rectified and user is provisioned successfully, but its last provisioned User Group cannot be deleted, only new user Group can be added. This is because last provisioned old values state is lost from OIM as it has been modified multiple times in between. User must delete last provision User Group by using Collections Admin screens.

It is recommend whenever user is modified and provisioning status for Collections User is **Provide Information** (exception occurred /validation failed) then user should first rectify the problem (for example, if field validation is failing then correct it) and provision user successfully (resource **Collection User** status is **Provisioned**) before making further modifications to User Group.

- **Modify End Date:**

- End Date represents User expiry in Collections.
- Once User is successfully provisioned then User can be deactivated by modifying end date \leq current date/today's date. Similarly, user can be activated again by modifying end date $>$ current date/today's date.

5.3 Delete Users in Collections

Once user is successfully provisioned it can be deleted from OBP Collections. Collections supports soft delete that is, it only expires User. User deletion request for Collections will only trigger when **Create User** provisioning task is complete for that particular request i.e., 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.

5.3 Delete Users in Collections

Figure 5–29 Manual Completion - Create User Provisioning Task

The screenshot shows the Oracle Identity Self Service interface. The left sidebar contains navigation options: Home, Inbox, My Profile (My Information, My Access), Requests (Catalog, Track Requests, Pending Attestations), and Administration (Users, Roles, Role Categories, Organizations, Attestation Dashboard, Open Tasks). The main content area is titled "Provisioning Tasks" and includes a search panel with fields for Task Name, Task Status, and Application Instance. Below the search panel is a "Search Results" table with columns: Row, Task Name, Task Status, Application Instance, Beneficiary, Date Assigned, Assignee, Request ID, and Account Name. The table contains one row: 1 Create User, Rejected, Collections, HARRYPOTTER, 2014-04-04, XELSYSADM, 56. The "Rows Selected" indicator shows 1 row.

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 5–30 Searching Users To Delete

The screenshot shows the Oracle Identity Self Service interface for the "Users" section. The left sidebar is the same as in Figure 5-29. The main content area is titled "Users" and includes a "Search Users" panel with various search criteria: User Login, First Name, Last Name, Identity Status, E-mail, Start Date, End Date, Display Name, Account Status, and Organization. Below the search panel is a "Search Results" table with columns: Row, Display Name, User Login, First Name, Last Name, Organization, Telephone Number, E-mail, Identity Status, and Account Status. The table contains four rows: 1 Harry Potter (User Login: HARRYPOTTER), 2 Internal User (User Login: OIMINTERNAL), 3 Weblogic User (User Login: WEBLOGIC), and 4 System Administrator (User Login: XELSYSADM). The "Rows Selected" indicator shows 1 row.

Figure 5–31 View User Details

The screenshot shows the Oracle Identity Self Service interface for user management. The user details for Harry Potter are displayed, including basic information, account effective dates, provisioning dates, contact information, preferences, and other attributes. The 'Delete User' link is highlighted in red.

Section	Field	Value
Basic Information	First Name	Harry
	Middle Name	
	Last Name	Potter
	Xellerate Type	false
	E-mail	harry.potter@oracle.com
Account Effective Dates	Start Date	
	End Date	12/31/2014
Provisioning Dates	Provisioning Date	
	Deprovisioning Date	
Contact Information	Telephone Number	
	Home Phone	
	Fax	
	Mobile	
	Pager	
	Home Postal Address	
Preferences	Locale	
	Timezone	
Other Attributes	Common Name	Harry Potter
	Initials	
	Department Number	
	Employee Number	
	Hire Date	
	Title	
	Locality Name	
Generation Qualifier		

Click **Delete User** link to delete user.

Figure 5–32 Delete User Screen

The screenshot shows the Oracle Identity Self Service interface for user management. The user details for Harry Potter are displayed, including basic information, account effective dates, provisioning dates, contact information, preferences, and other attributes. The 'Delete User' link is highlighted in red.

Section	Field	Value
Basic Information	First Name	Harry
	Middle Name	
	Last Name	Potter
	Xellerate Type	false
	E-mail	harry.potter@oracle.com
Account Effective Dates	Start Date	
	End Date	12/31/2014
Provisioning Dates	Provisioning Date	
	Deprovisioning Date	
Contact Information	Telephone Number	
	Home Phone	
	Fax	
	Mobile	
	Pager	
	Home Postal Address	
Preferences	Locale	
	Timezone	
Other Attributes	Common Name	Harry Potter
	Initials	
	Department Number	
	Employee Number	
	Hire Date	
	Title	
	Locality Name	
Generation Qualifier		

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

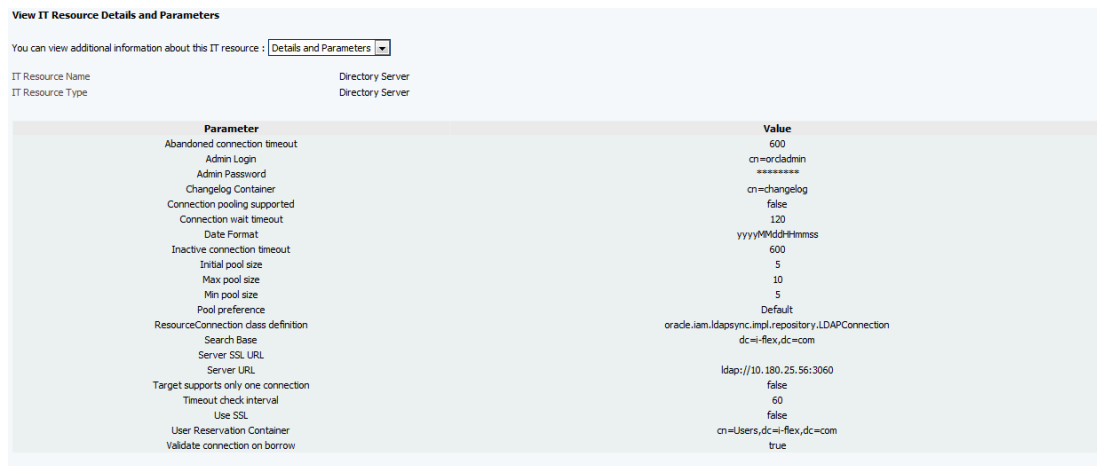
To verify OIM configuration, follow the steps:

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 6–1 Viewing IT Resource Details and Parameters



2. When tried to create User from OIM, exception was thrown 'Unable to find attributes in OID schema.' for following attributes. If similar 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 6–1 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

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

1. Log in to OBP Collections Native UI using administrative credentials.

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

Figure 6–2 OBP Collections Native Login screen



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

Figure 6–3 User Screen - User Navigation

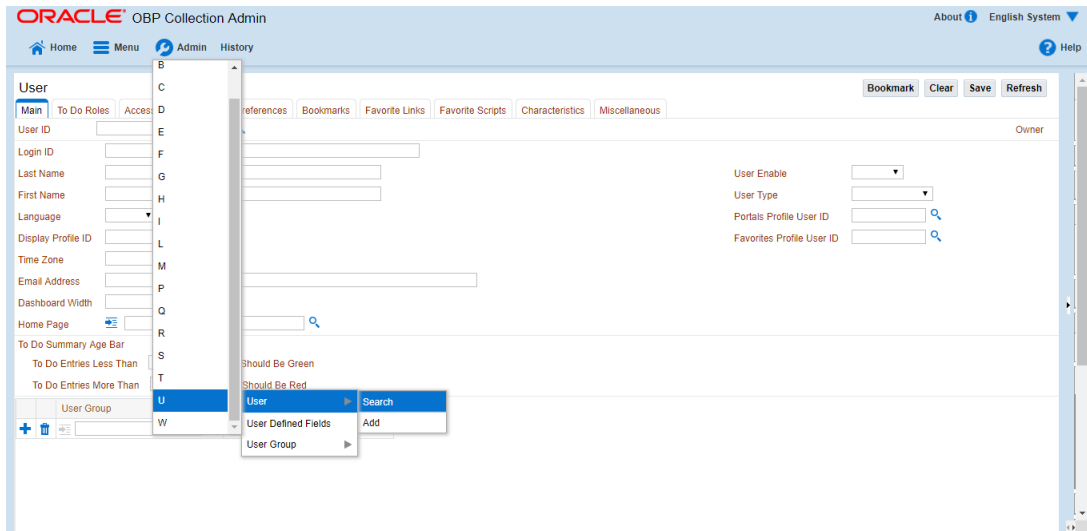
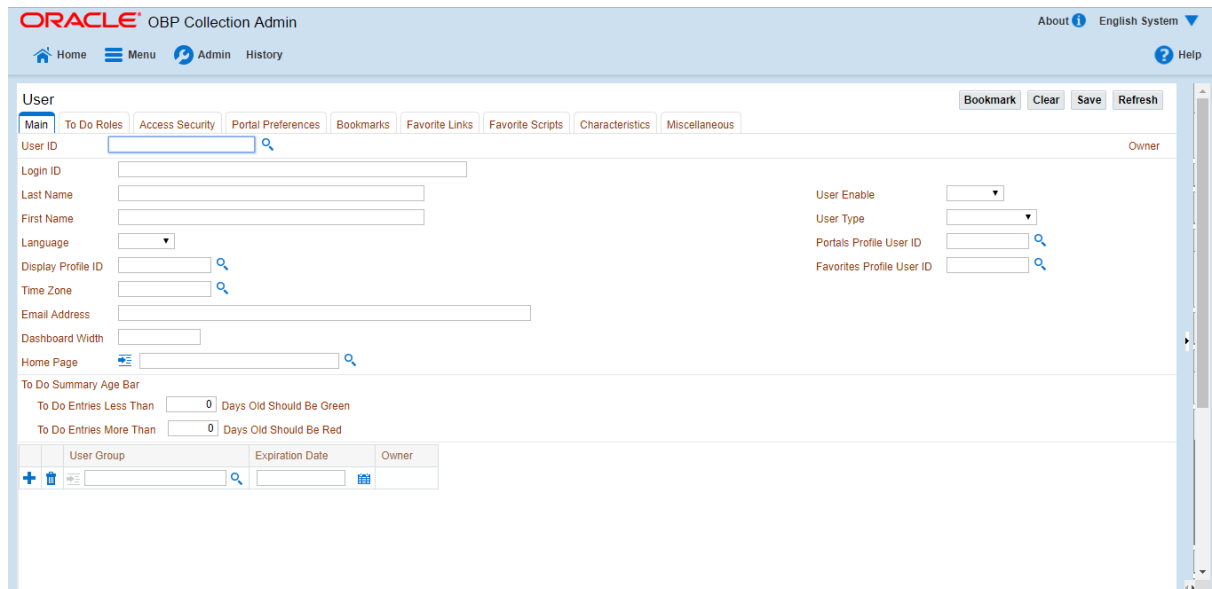


Figure 6–4 User Screen - Main Tab



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

Figure 6–5 Searching Particular User

User ID

Login ID

Last Name

First Name

User ID	Login ID	Last Name	First Name	User Type
---------	----------	-----------	------------	-----------

Figure 6–6 Search Result in User screen

Oracle OBP Collection Admin

Home Menu Admin History

User Bookmark Previous Item Next Item Clear Save Refresh

Main To Do Roles Access Security Portal Preferences Bookmarks Favorite Links Favorite Scripts Characteristics Miscellaneous

User ID **HARRYPOT** Owner Customer Modification

Login ID **HARRYPOTTER**

Last Name **Potter** User Enable **Enable**

First Name **Harry** User Type

Language **English** Portals Profile User ID

Display Profile ID **NORTHAM** North America Favorites Profile User ID

Time Zone

Email Address **harry.potter@oracle.com**

Dashboard Width **200**

Home Page

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	Expiration Date	Owner
ALL_SERVICES System User Group	12-31-2100	Customer Modification
C1_CLSERVICES All Services(C1- Collection Admin)	12-31-2100	Customer Modification

6.3 Create Users in Collections

Follow below steps to create user in Collections.

1. Log in to OBP Collections native UI using administrative credentials.

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

Figure 6–7 OBP Collections Native Login screen

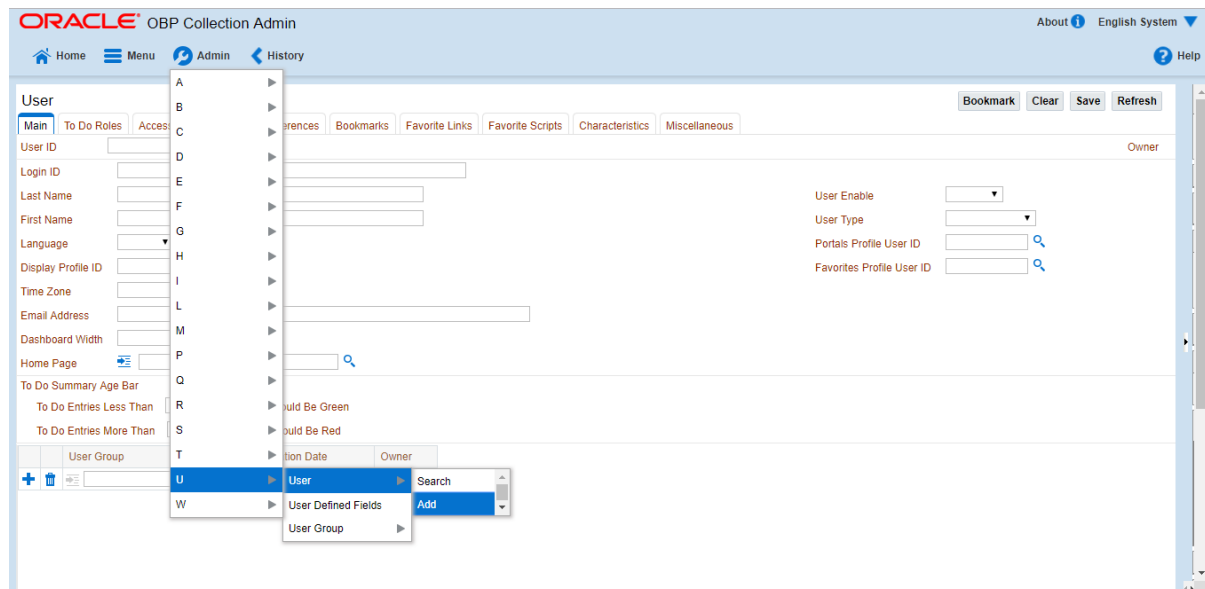


The login screen features a blue header with a gear icon and the text "Sign In To OBP Collection Admin". Below the header are input fields for "User ID" and "Password", followed by a "Login" button. At the bottom, there is a "Language" dropdown set to "English" and the Oracle logo.

OBP Collection Admin V2.6.1.0.0
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 6–8 OBP Collections native - User Navigation



The screenshot shows the Oracle OBP Collection Admin interface. The top navigation bar includes "Home", "Menu", "Admin", and "History". The "Admin" menu is expanded, showing a list of options from A to W. The "U" option is selected, and a sub-menu is displayed with "User", "User Defined Fields", and "User Group". The "User" option is further expanded to show "Search" and "Add". The main content area displays the "User" form with various input fields and a "User Group" dropdown.

Figure 6–9 OBP Collections native - Main Tab

The screenshot displays the Oracle OBP Collection Admin interface for creating a user. The page is titled 'User' and includes a navigation bar with 'Home', 'Menu', 'Admin', and 'History'. The main content area contains several input fields and dropdown menus for user configuration. The fields include User ID, Login ID, Last Name, First Name, Language, Display Profile ID, Time Zone, Email Address, Dashboard Width, and Home Page. There are also dropdown menus for User Enable and User Type, and search fields for Portals Profile User ID and Favorites Profile User ID. At the bottom, there is a table for User Group, Expiration Date, and Owner.

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 6–10 User Screen

ORACLE OBP Collection Admin About English System

Home Menu Admin History Help

User Bookmark Duplicate Delete Clear Save Refresh

Main | To Do Roles | Access Security | Portal Preferences | Bookmarks | Favorite Links | Favorite Scripts | Characteristics | Miscellaneous

User ID: OIMOBPCO

Owner: Customer Modification

Login ID: OIMOBPCOLL

Last Name: OIMOBPCOLL

First Name: OIMOBPCOLL

Language: English

Display Profile ID: NORTHAM North America

Time Zone:

Email Address: OIMOBPCOLL@oracle.com

Dashboard Width: 200

Home Page: c1_crmhTabMenu ORMB Portal

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	Expiration Date	Owner
CLNHOSTUSER	01-01-2100	Customer Modification

OIMOBPCOLL User is successfully created in Collections.