

Oracle® Banking Enterprise Default Management

Administrator Guide

Release 2.11.0.0.0

F36758-01

December 2020

Oracle Banking Enterprise Default Management Administrator Guide, Release 2.11.0.0.0

F36758-01

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

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

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

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

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

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

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

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

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

Contents

Preface	9
Audience	9
Documentation Accessibility	9
Organization of the Guide	9
Related Documents	10
Conventions	10
1 User Administration with OIM	12
1.1 Creating Users in Oracle Identity Manager (OIM)	12
1.2 Creating Roles in Oracle Identity Manager (OIM)	16
1.3 Assigning Roles to Users in OIM	20
1.4 Locking Users in OIM	24
1.5 Unlocking Users in OIM	26
1.6 Resetting User Password in OIM	27
1.7 User Management Using the Admin Application	31
1.8 Unlocking Users in Oracle WebLogic Server (OWS) Administration Console ..	38
1.9 Creation of first time user to access OBEDM	43
2 User Management With Local Security	47
2.1 Create User or User Details	47
2.2 Define Application Roles	47
2.3 Define Enterprise Role	48
2.4 Password Policy Management	48
3 Setting Up The Bank And Branch	50
3.1 Common Services Day 0 Setup	50
3.1.1 Core Maintenances	50

3.1.1.1 Head Office Setup	50
3.1.2 Currency Maintenances	51
3.1.3 Calendar Maintenances	51
3.2 Accounting Day 0 Setup	52
3.3 Product Manufacturing Day 0 Setup	52
4 Application Monitoring Using Administration Application	54
4.1 Dynamic Monitoring Service (DMS)	54
4.1.1 Usage	54
4.1.2 Monitoring Application using the OPA001 page	55
4.1.2.1 Monitoring Application Performance (Fast path: OPA001)	55
4.1.2.1.1 Application Performance Summary	55
4.1.2.1.2 Log Level	56
4.1.2.1.3 Application Performance	56
5 Transparent Data Encryption (TDE)	62
5.1 Configuration	62
5.2 Installation	62
5.2.1 Prepare Scripts to Encrypt Sensitive Data	63
5.2.2 Create TDE Keystore	63
5.2.3 Edit sqlnet.ora file	64
5.2.4 Run Created Alter Script	64
6 Masking Customer Private Data	66
6.1 Configuration	66
6.2 Installation	67
6.2.1 Prepare Scripts to Encrypt Sensitive Data	67
6.2.2 Create Schema for RO and ERO User	67
6.2.3 Execute Created Scripts through Encryption Tool	68

List of Figures

Figure 1–1 Creating Users in OIM - Log in	12
Figure 1–2 Creating Users in OIM - Manage Section	13
Figure 1–3 Creating Users in OIM - Click Create	14
Figure 1–4 Creating Users in OIM - Enter User Details	15
Figure 1–5 Enter User Details (Continued)	16
Figure 1–6 Creating Roles in OIM - Manage Section	17
Figure 1–7 Creating Roles in OIM - Click Create	18
Figure 1–8 Creating Roles in OIM - Enter Role Details	19
Figure 1–9 Creating Roles in OIM - Role Created Successfully	20
Figure 1–10 Assigning Roles in OIM - Requesting Roles	21
Figure 1–11 Assigning Roles in OIM - Adding to Cart	22
Figure 1–12 Assigning Roles in OIM - Checkout Cart	23
Figure 1–13 Assigning Roles in OIM - Submit Cart	24
Figure 1–14 Locking Users in OIM	25
Figure 1–15 User Locked Successfully	26
Figure 1–16 Unlocking Users in OIM	27
Figure 1–17 Resetting User Password in OIM	28
Figure 1–18 Resetting User Password in OIM - Manually or Auto-generate	29
Figure 1–19 Resetting User Password in OIM - New Password	30
Figure 1–20 Password Reset Successfully	31
Figure 1–21 Adding a User	32
Figure 1–22 Enter Mandatory Details	33
Figure 1–23 Applying Changes	34
Figure 1–24 Adding User to a Group	35

Figure 1–25 Available and Assigned Roles	36
Figure 1–26 Adding User to Assigned Roles Table	37
Figure 1–27 Save Changes	38
Figure 1–28 OWS Log in	39
Figure 1–29 base_domain	40
Figure 1–30 Security tab	41
Figure 1–31 Unlock User	42
Figure 1–32 User Successfully Unlocked	43
Figure 1–33 Log in Oracle Fusion Middleware Control	44
Figure 1–34 Click Application Roles	45
Figure 1–35 Select Administrators Role	45
Figure 1–36 Add Principal	46
Figure 1–37 Create User	47
Figure 1–38 Define Application Role	48
Figure 1–39 Define Enterprise Role	48
Figure 1–40 Password Policy Management	49
Figure 3–1 Developers	54
Figure 3–2 IT Technical Staff	55
Figure 3–3 Monitoring Application Performance	55
Figure 3–4 Application Performance Summary	56
Figure 3–5 Log Level	56
Figure 3–6 Alert State	57
Figure 3–7 Select Task Code	59
Figure 3–8 Selection of Desired Transaction	59
Figure 3–9 Transaction Details	60
Figure 3–10 Transaction Metrics	60

Figure 3–11 Alert and Trend Details	60
Figure 3–12 Failure Events	61

List of Tables

Table 3–1 Alert State	57
Table 4–1 TDE Configuration	62
Table 5–1 TDE Configuration	66

Preface

This guide describes how to administer the Oracle Banking Enterprise Default Management application environment.

Oracle recommends that you review its contents before installing, or working with the product.

This preface contains the following topics:

- [Audience](#)
- [Documentation Accessibility](#)
- [Organization of the Guide](#)
- [Related Documents](#)
- [Conventions](#)

Audience

This guide is intended for the administrators of Oracle Banking Enterprise Default Management.

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 User Administration with OIM](#)

This chapter describes all user management related activities to be performed by an administrator.

[Chapter 2 User Management With Local Security](#)

This chapter describes the configurations to be done if local security option is configured instead of OIM based security.

[Chapter 3 Setting Up The Bank And Branch](#)

This chapter provides the process of setting up the bank and the branch commonly referred to as the Day 0 setups.

[Chapter 4 Application Monitoring Using Administration Application](#)

This chapter provides an overview on the various monitoring operations performed as an administrator using the application.

[Chapter 5 Transparent Data Encryption \(TDE\)](#)

This chapter describes the configuration, installation, and policy setup of Transparent Data Encryption (TDE).

[Chapter 6 Masking Customer Private Data](#)

This chapter describes the configuration, installation, and policy setup to mask customer private data categories as sensitive or Personally Identifiable Information (PII).

Related Documents

For more information, see the following documentation:

- For installation and configuration information, see the Oracle Banking Enterprise Default Management Installation Guide - Silent Installation.
- For a comprehensive overview of security, see the Oracle Banking Enterprise Default Management Security Guide.
- For the complete list of Oracle Banking licensed products and the third-party licenses included with the license, see the Oracle Banking Enterprise Default Management Licensing Guide.
- For information related to customization and extension, see the Oracle Banking Enterprise Default Management Extensibility Guides for Host and UI.
- For information on the functionality and features, see the Oracle Banking Enterprise Default Management Functional Overview document.

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 User Administration with OIM

This chapter describes all user management related activities to be performed by an administrator for the application.

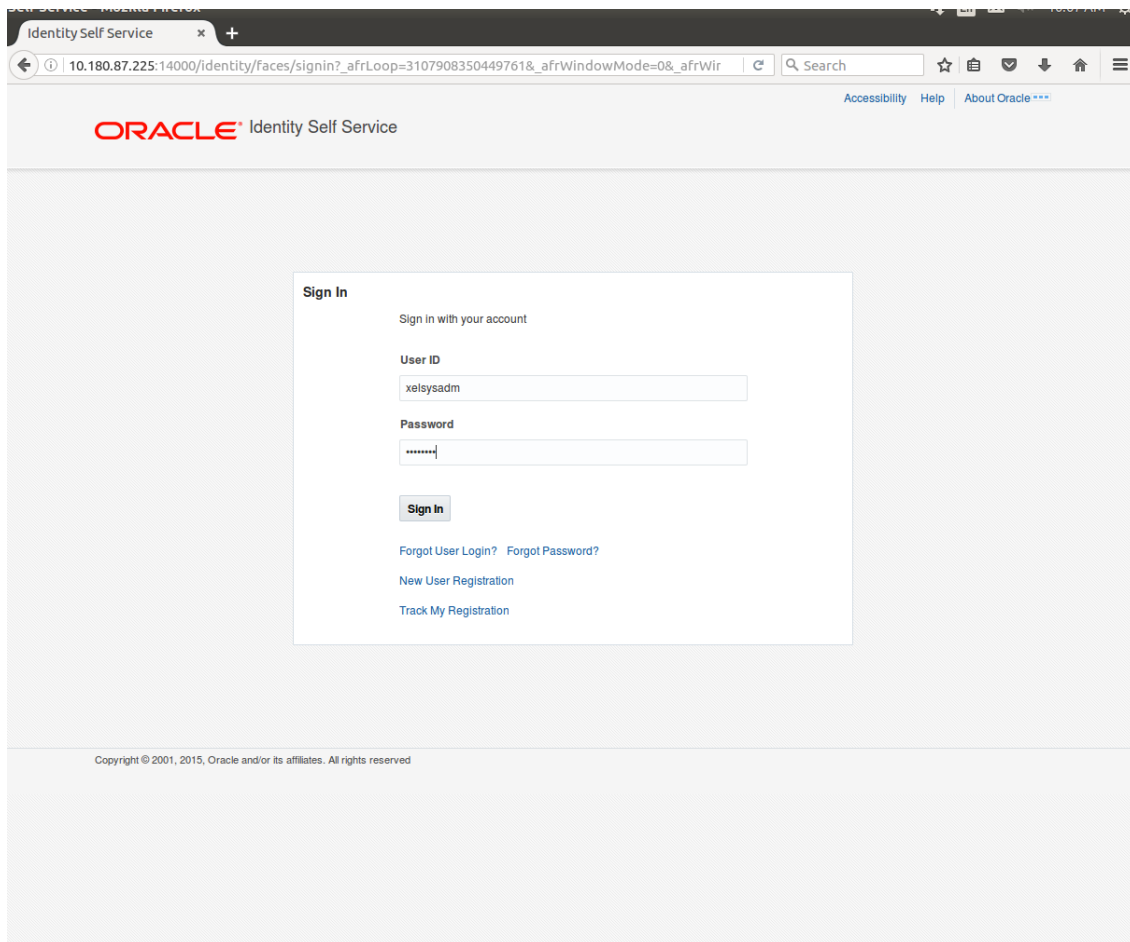
1.1 Creating Users in Oracle Identity Manager (OIM)

This section explains the procedure to create users in Oracle Identity Manager (OIM).

To create users in OIM:

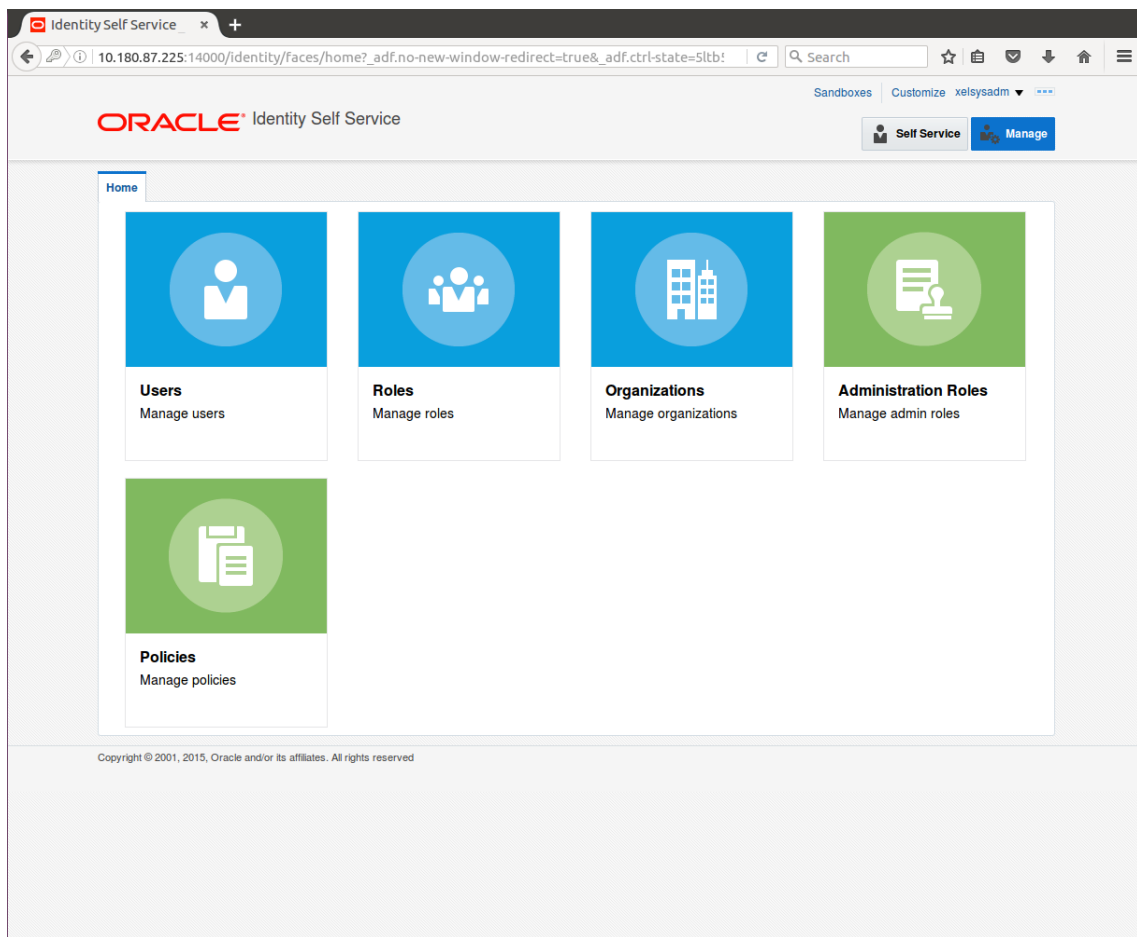
1. Log in to OIM with the User ID as **xelsysadm** and the relevant <Password>.

Figure 1–1 Creating Users in OIM - Log in



2. Click **Users** under the Manage section.

Figure 1–2 Creating Users in OIM - Manage Section



3. In the **Search Users** page, search for existing users. The Search Results appear.
4. Click **Create** in the Search Results section to create a new user.

Figure 1–3 Creating Users in OIM - Click Create

The screenshot shows the Oracle Identity Self Service interface. The main content area is titled 'Users' and contains a search bar and a table of users. The table has the following data:

User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account Status
HARRY	Harry Potter	Harry	Potter	Xellerate Users		Harry@gmail.com	Active	Unlocked
OIMINTERNAL	Internal User	OIMINTERNAL	OIMINTERNAL	Xellerate Users			Active	Unlocked
WEBLOGIC	Weblogic User	WEBLOGIC	WEBLOGIC	Xellerate Users			Active	Unlocked
XELSYSADM	System Administrator	System	Administrator	Xellerate Users		donotreply@ora...	Active	Unlocked

Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved.

5. In the **Create User** page, enter the required user details.

Figure 1–4 Creating Users in OIM - Enter User Details

The screenshot shows the Oracle Identity Self Service 'Create User' form. The browser address bar shows the URL: 10.180.87.225:14000/identity/faces/home?_adf.no-new-window-redirect=true&_adf.ctrl-state=ry1k. The page title is 'ORACLE Identity Self Service'. The breadcrumb navigation shows 'Home > Users > Create User'. The form is titled 'Create User' and has three action buttons: 'Submit', 'Save As...', and 'Cancel'. The form is organized into several sections:

- Request Information:** Includes 'Effective Date' (calendar icon) and 'Justification' (text area).
- Basic Information:** Includes 'First Name' (Clark), 'Middle Name', 'Last Name' (Kent), 'E-mail', 'Manager' (lookup icon), 'Organization' (Xellerate Users, lookup icon), 'User Type' (Other, dropdown), and 'Display Name'.
- Account Settings:** Includes 'User Login' (Clark), 'Password' (masked with asterisks, info icon), and 'Confirm Password' (masked with asterisks).
- Account Effective Dates:** Includes 'Start Date' and 'End Date' (calendar icons).
- Provisioning Dates:** (Section header, no visible fields).

Figure 1–5 Enter User Details (Continued)

The screenshot shows a web browser window with the URL `10.180.87.225:14000/identity/faces/home?_adf.no-new-window-redirect=true&_adf.ctrl-state=ry1k`. The page title is "Identity Self Service". The form contains the following sections and fields:

- Confirm Password:** A single text input field.
- Account Effective Dates:** Two date pickers for "Start Date" and "End Date".
- Provisioning Dates:** Two date pickers for "Provisioning Date" and "Deprovisioning Date".
- Contact Information:** A grid of fields including Telephone Number, Home Phone, Fax, Mobile, Pager, Home Postal Address, Postal Address, Postal Code, PO Box, State, Street, and Country.
- Preferences:** A dropdown for "Locale" and a text field for "Timezone".
- Other Attributes:** Fields for Common Name, Department Number, Employee Number, Generation Qualifier, Hire Date, Locality Name, Initials, and Title.

At the bottom of the page, there is a copyright notice: "Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved."

6. Click **Submit**.

On completion of this procedure the user gets created in OIM, and gets synced in OID.

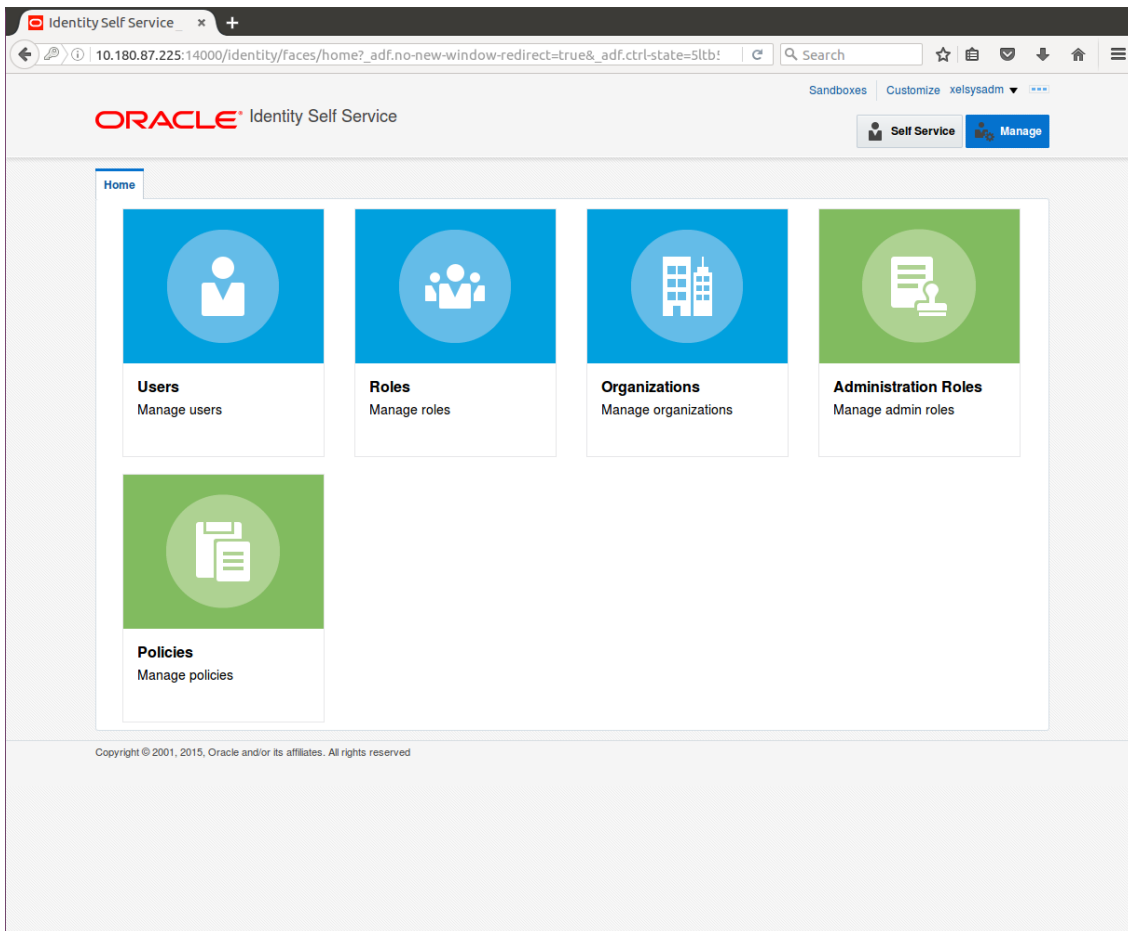
1.2 Creating Roles in Oracle Identity Manager (OIM)

This section explains the procedure to create roles in Oracle Identity Manager (OIM).

To create roles in OIM:

1. Click **Roles** under the Manage section.

Figure 1–6 Creating Roles in OIM - Manage Section



2. In the **Search Roles** page, search for existing roles. The Search Results appear.
3. Click **Create** in the Search Results section to create a new Role.

Figure 1–7 Creating Roles in OIM - Click Create

The screenshot shows the Oracle Identity Self Service interface. The browser address bar indicates the URL is `10.180.87.225:14000/identity/faces/home?_adf.no-new-window-redirect=true&_adf.ctrl-state=5ltb:...`. The page title is "ORACLE Identity Self Service". The user is logged in as "xelsysadm". The main content area is titled "Roles" and includes a search bar with "Name" selected. Below the search bar is an actions bar with buttons for "Create", "Open", "Delete", "Refresh", and "Detach". The "Create" button is highlighted. Below the actions bar is a table with the following data:

Name	Role Description
ALL USERS	Default role for all users
Administrators	Administrators role for SOA
BIReportAd...	Administrators role for BI Publisher Reports
OPERATORS	Operator role
SELF OPER...	Operator role for self registration
SYSTEM AD...	System Administrator role for OIM

Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved

4. Fill the role details.

Figure 1–8 Creating Roles in OIM - Enter Role Details

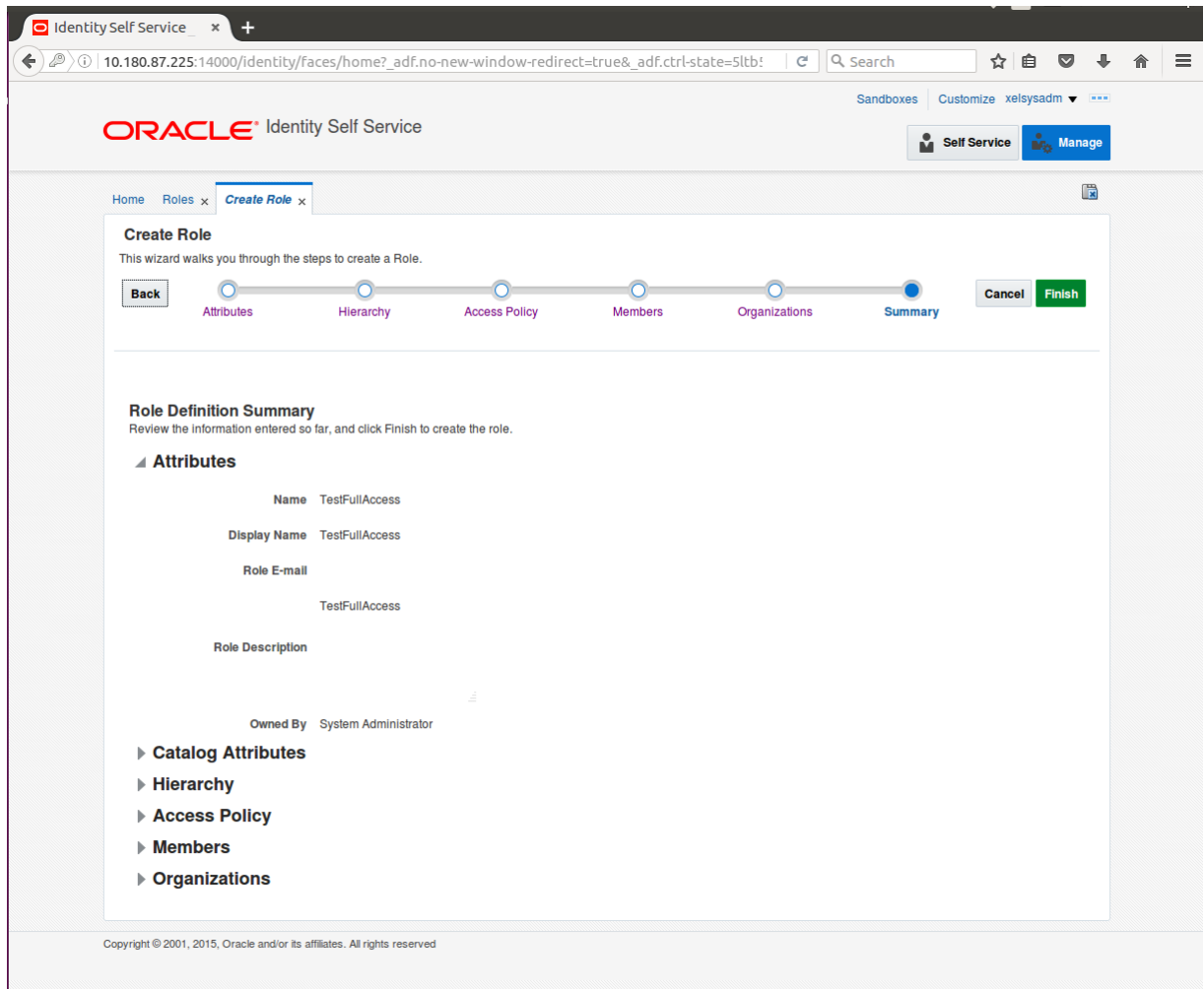
The screenshot shows the Oracle Identity Self Service interface. The browser address bar displays the URL: 10.180.87.225:14000/identity/faces/home?_adf.no-new-window-redirect=true&_adf.ctrl-state=51tb! . The page title is 'ORACLE Identity Self Service'. The user is logged in as 'xelsysadm'. The navigation menu includes 'Home', 'Roles', and 'Create Role'. The 'Create Role' wizard is active, showing a progress bar with steps: Back, Attributes (current), Hierarchy, Access Policy, Members, Organizations, and Summary. The 'Attributes' step is completed. The 'General Role Information' section contains the following fields: Name (TestFullAccess), Display Name (TestFullAccess), Role E-mail, Role Description (TestFullAccess), and Owned By (System Administrator). The 'Catalog Attributes' section contains the following fields: Category (Role), Audit Objective, Risk Level (dropdown), User Defined Tags, and Approver User.

5. Click **Finish**. The role is created successfully.

This role creates a group in OID.

While running the PIT (Policy Import tool), the Enterprise role (OIM role or OID group in this scenario) is mapped to the Application Role in OES.

Figure 1–9 Creating Roles in OIM - Role Created Successfully



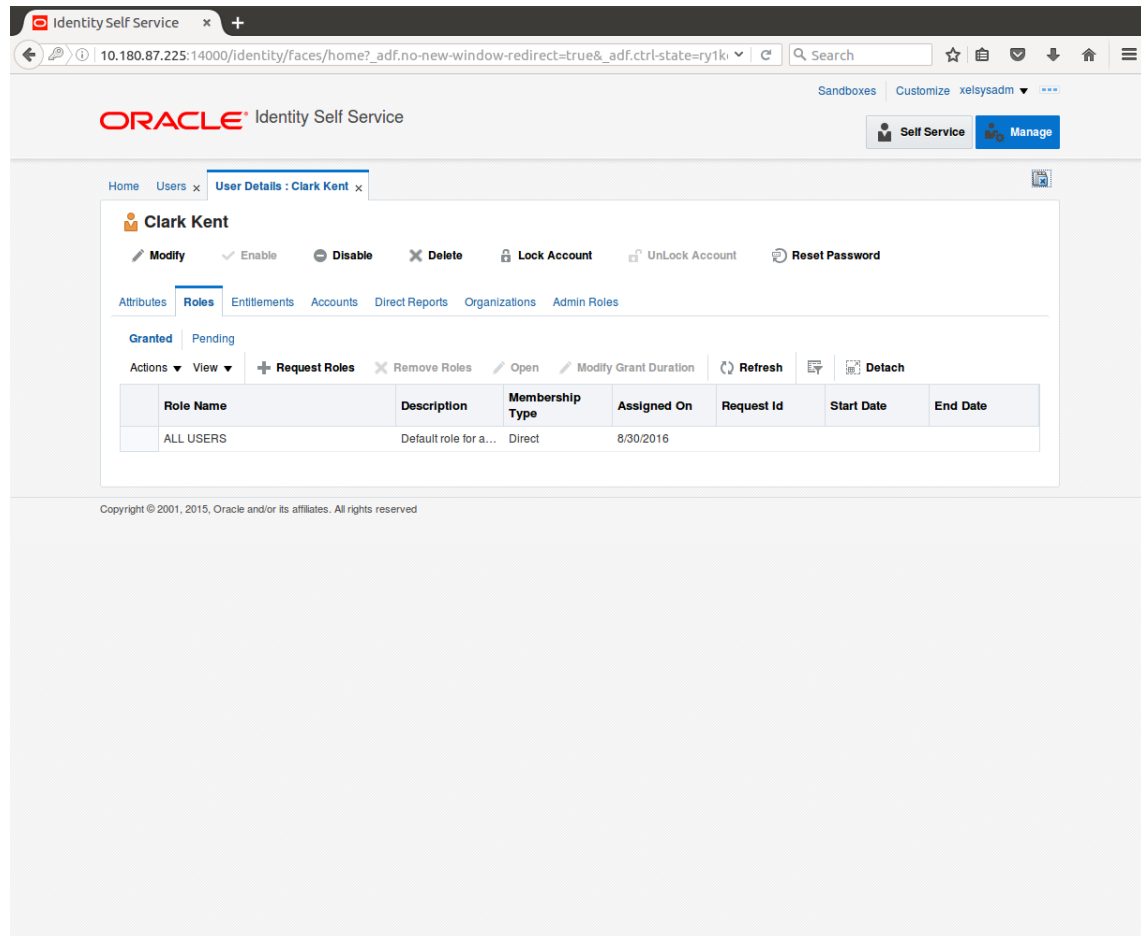
1.3 Assigning Roles to Users in OIM

This section explains how to assign roles to the user in OIM.

To assign a role to a user:

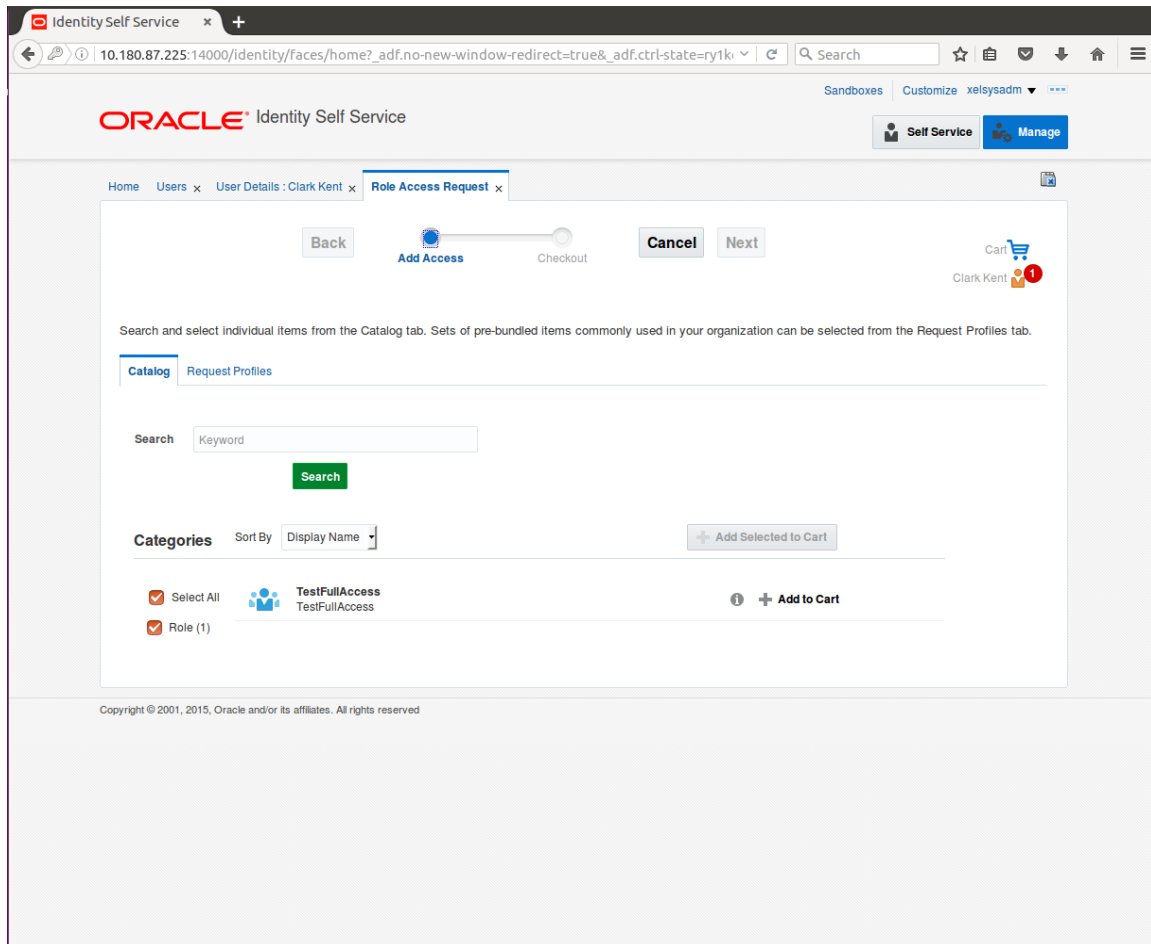
1. Log in to OIM.
2. Navigate to the **Roles Tab** under the User.
3. Click **Request Roles**.

Figure 1–10 Assigning Roles in OIM - Requesting Roles



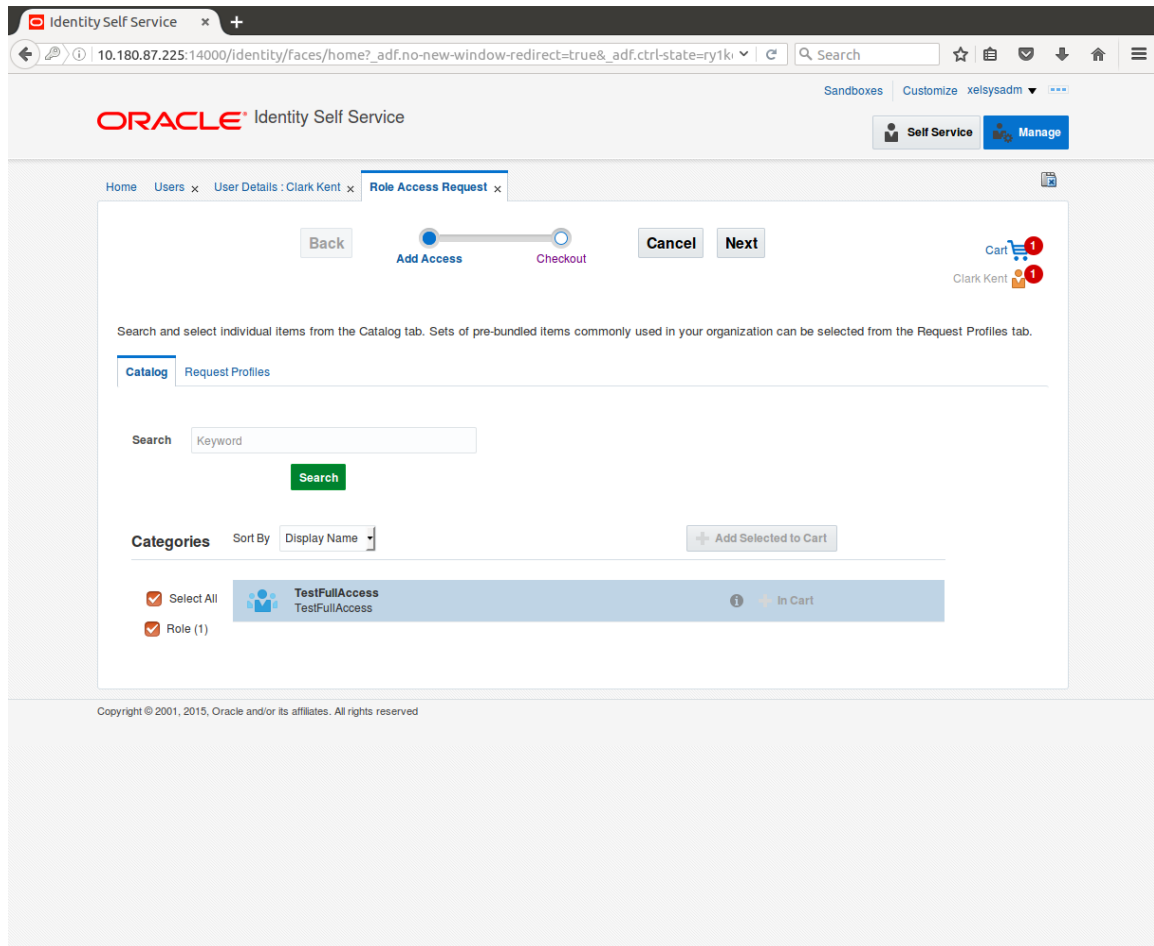
4. In the **Catalog** page, select the required role and click **Add to Cart**. The item gets added to the cart.

Figure 1–11 Assigning Roles in OIM - Adding to Cart



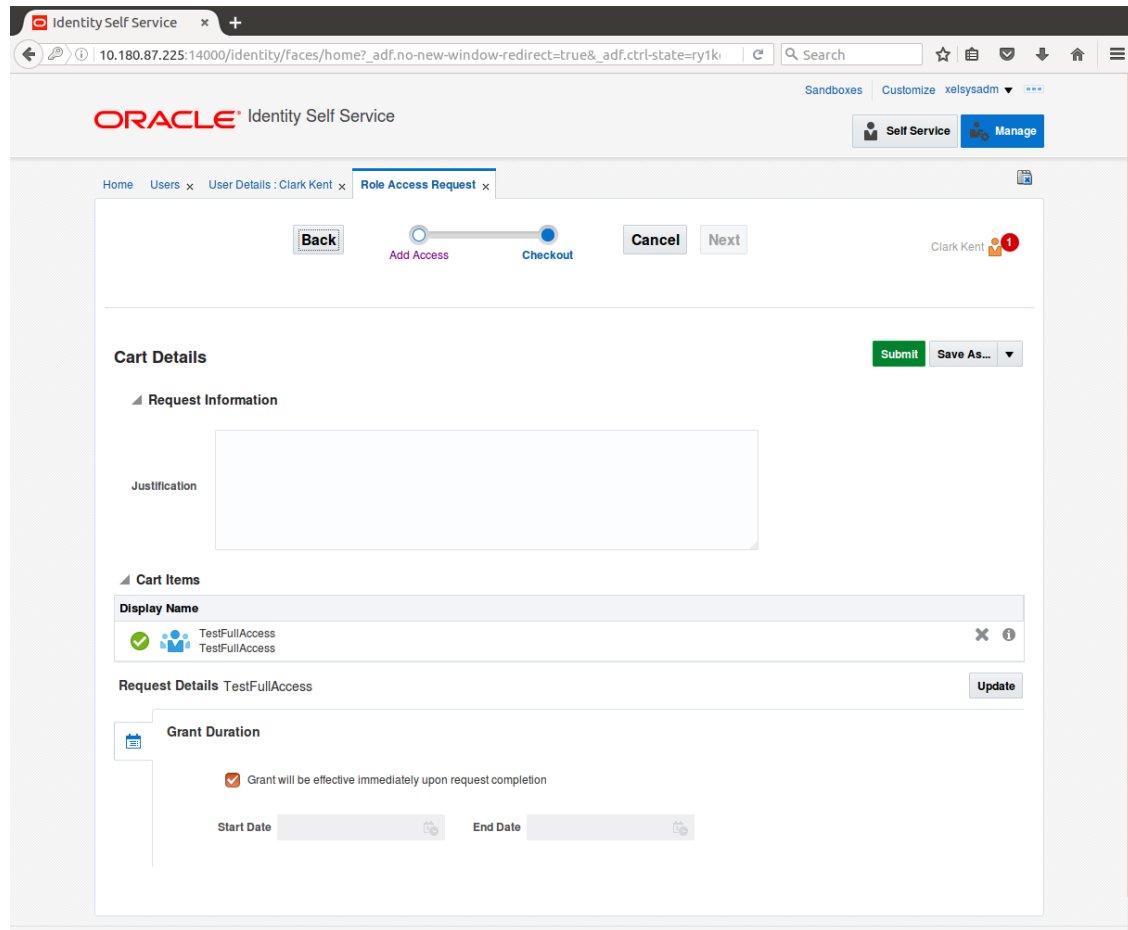
5. Click **Checkout**.

Figure 1–12 Assigning Roles in OIM - Checkout Cart



6. In the **Cart Details** page, click **Submit**.

Figure 1–13 Assigning Roles in OIM - Submit Cart



On completion of this procedure the role gets assigned to the user in OIM.

1.4 Locking Users in OIM

This section explains how to lock the user in OIM.

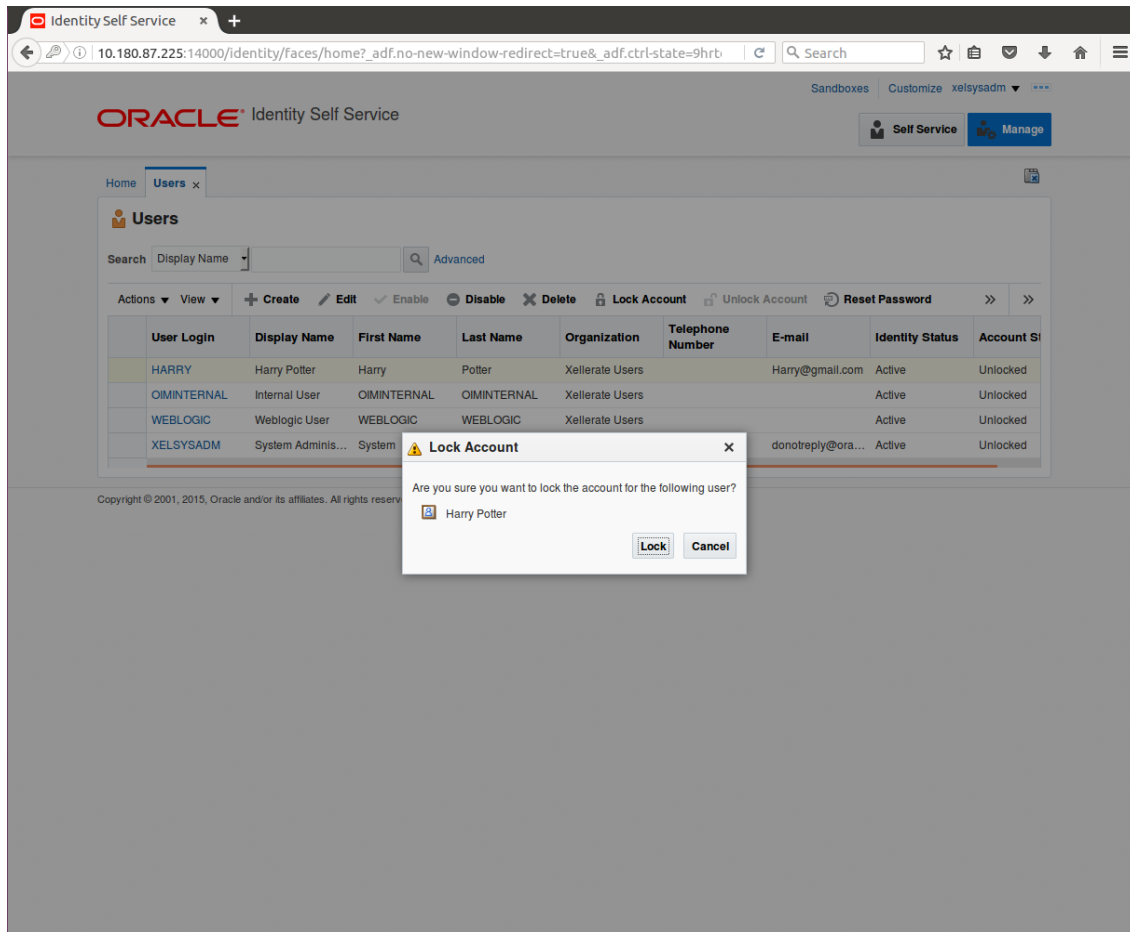
To lock a user:

1. Log in to OIM.
2. Click **Lock Account** to lock a user.

A message appears, Are you sure you want to lock the account for the following user?

3. Click **Lock**.

Figure 1–14 Locking Users in OIM



The user is locked successfully.

Figure 1–15 User Locked Successfully

Identity Self Service

Account locked successfully

Home Users x

Users

Search Display Name

Actions View

User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account Status
HARRY	Harry Potter	Harry	Potter	Xellerate Users		Harry@gmail.com	Active	Locked
OIMINTERNAL	Internal User	OIMINTERNAL	OIMINTERNAL	Xellerate Users			Active	Unlocked
WEBLOGIC	Weblogic User	WEBLOGIC	WEBLOGIC	Xellerate Users			Active	Unlocked
XELSYSADM	System Adminis...	System	Administrator	Xellerate Users		donotreply@ora...	Active	Unlocked

Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved

1.5 Unlocking Users in OIM

This section explains how to unlock the user in OIM.

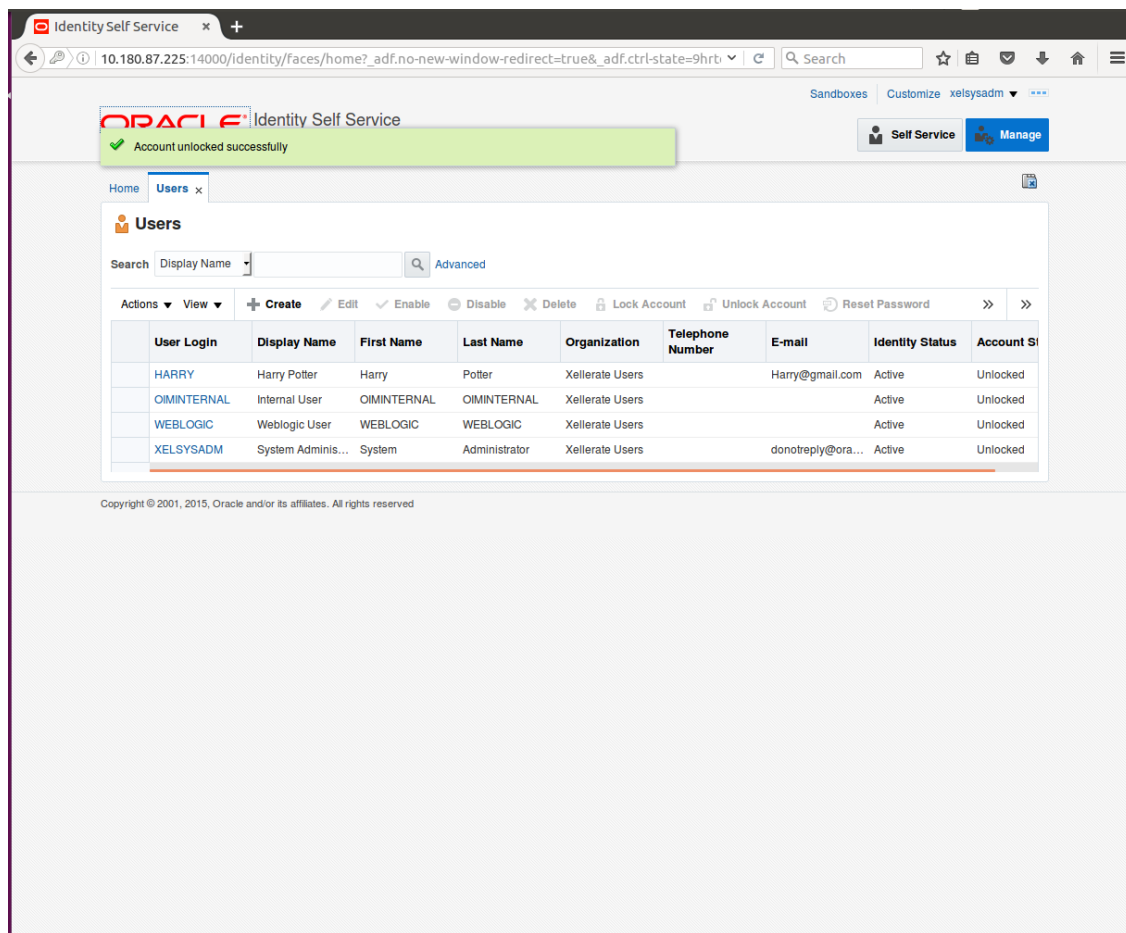
To unlock a user:

1. Log in to OIM.
2. Click **Unlock Account** to unlock a user.

A message appears, Are you sure you want to Unlock these users?

3. Click **Unlock**.

Figure 1–16 Unlocking Users in OIM



The user is unlocked successfully.

1.6 Resetting User Password in OIM

This section explains how to reset user password in OIM.

1. Log in to OIM.
2. Click **Reset Password** to reset a user password.

Figure 1–17 Resetting User Password in OIM

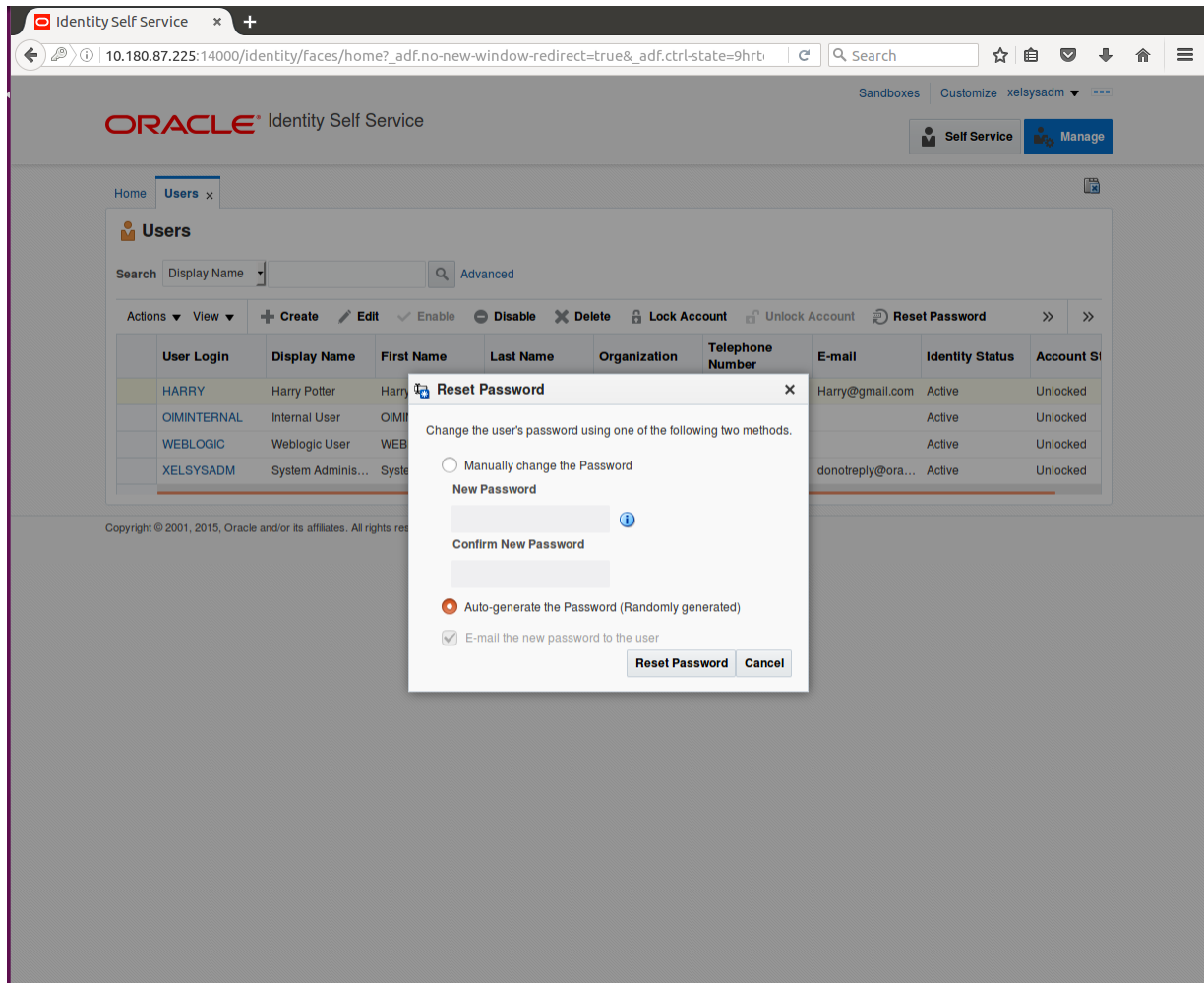
The screenshot shows the Oracle Identity Self Service interface. The browser address bar indicates the URL: 10.180.87.225:14000/identity/faces/home?_adf.no-new-window-redirect=true&_adf.ctrl-state=9hrt. The page title is 'ORACLE Identity Self Service'. The user is logged in as 'xelsysadm'. The 'Users' page is active, showing a search bar and a table of users. The 'Reset Password' action is highlighted for the 'XELSYSADM' user.

User Login	Display Name	First Name	Last Name	Organization	Telephone Number	E-mail	Identity Status	Account Status
HARRY	Harry Potter	Harry	Potter	Xellerate Users		Harry@gmail.com	Active	Unlocked
OIMINTERNAL	Internal User	OIMINTERNAL	OIMINTERNAL	Xellerate Users			Active	Unlocked
WEBLOGIC	Weblogic User	WEBLOGIC	WEBLOGIC	Xellerate Users			Active	Unlocked
XELSYSADM	System Administrator	System	Administrator	Xellerate Users		donotreply@ora...	Active	Unlocked

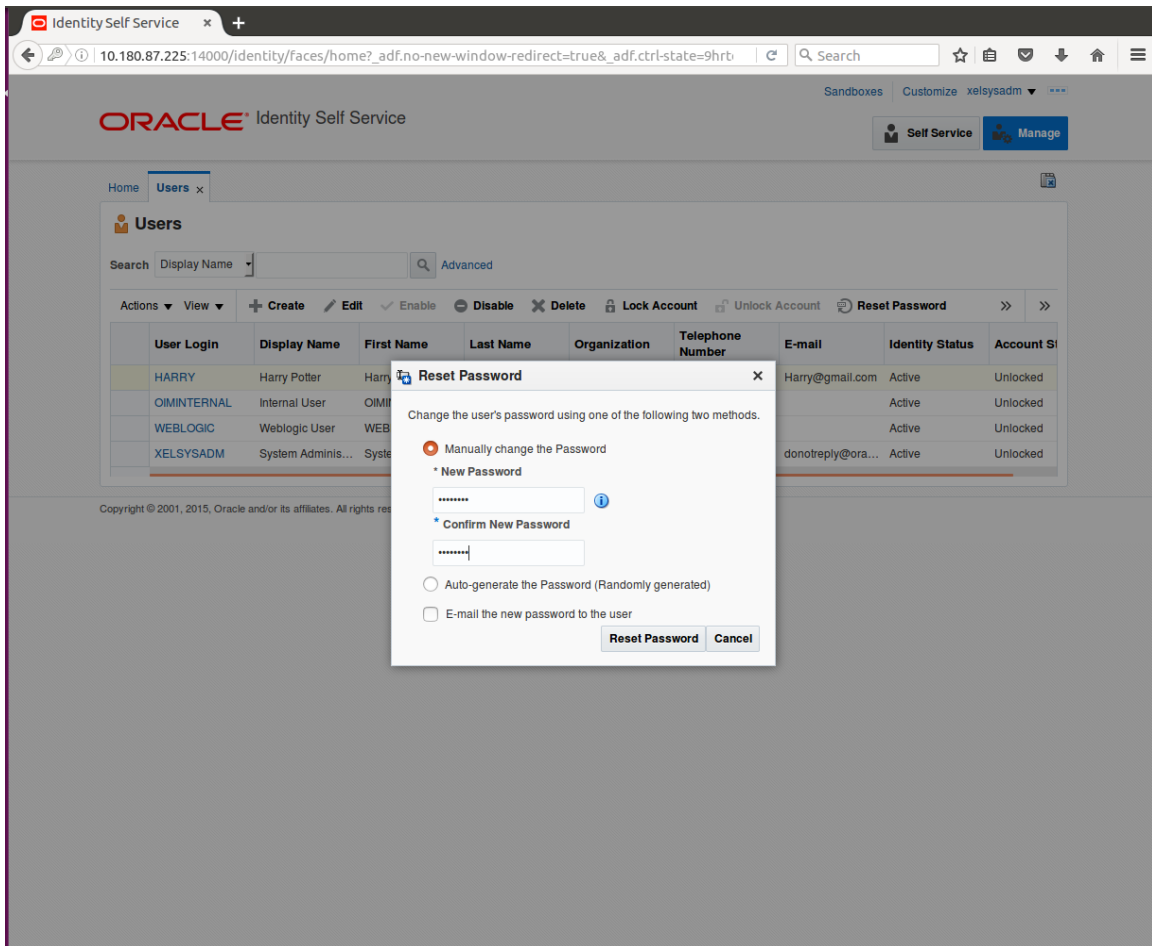
Copyright © 2001, 2015, Oracle and/or its affiliates. All rights reserved

The **Reset Password** dialog box appears.

You can select either **Manually change the Password** option to change the password manually or select the **Auto-generate the password (Randomly generated)** option to enable auto generation of the password.

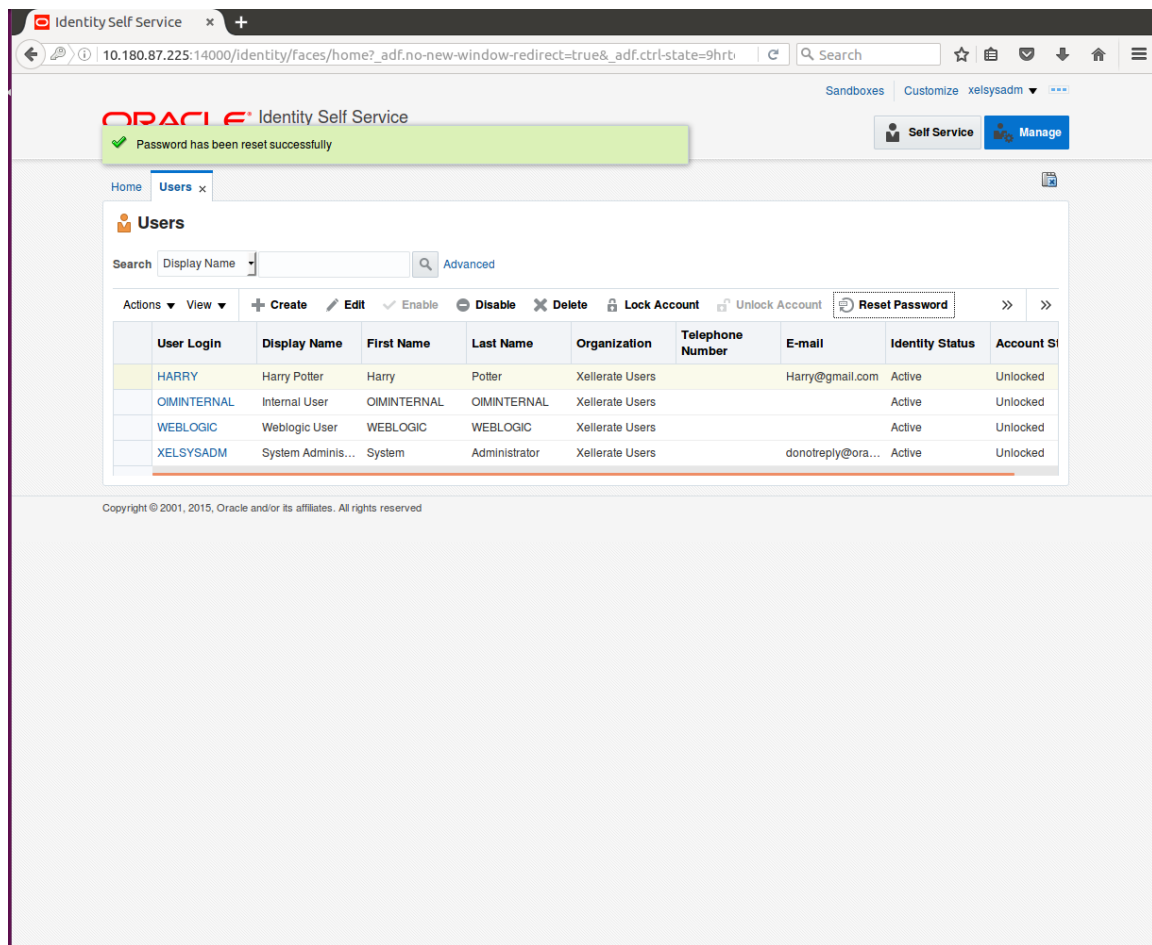
Figure 1–18 Resetting User Password in OIM - Manually or Auto-generate

3. If you select the **Manually change the Password** option, enter the new password in the **New Password** and the **Confirm New Password** fields.

Figure 1–19 Resetting User Password in OIM - New Password

The user password is reset successfully.

Figure 1–20 Password Reset Successfully



1.7 User Management Using the Admin Application

The User Management screen is a quick start UI, provided to create initial users and verify the OBEDM installation.

<https://<ui-server-name>:<ui-server-port>/com.ofss.fc.ui.view.admin/faces/admin.jspx>

To create initial users and verify the installation, perform the below mentioned steps:

1. Click **Security** tab in **View Admin**.
2. Select **User Management**.
3. Click **+** icon to add a user.

Figure 1–21 Adding a User

The screenshot displays the Oracle Banking Platform Admin Application interface. The browser address bar shows the URL: `https://10.180.84.177:8002/com.ofss.fc.ui.view.admin/faces/admin.jspx?_afrcLoop=31010305172428t`. The page title is "Oracle Banking Platform" and the date is "15-Jan-2016". The main content area is titled "User Management" and includes a "Search Filter" section with a "Username" input field and a search button. Below this is a "User Details" table with columns for "Username", "Target Unit", "Branch", and "Delete". The table is currently empty. At the bottom, there is a "User Details Form" section with buttons for "Edit", "Apply changes", and "Assign Roles". The form contains various fields for user information, including Username, Preferred Language, First Name, Accreditation, Last Name, Brand, Email, 2FA Status, Password, Forum Nick Name, Confirm password, Party Id, Home Branch, Last Logged In Date Time, Manager, 2FA Inactive Begin Date, Target Unit, and 2FA Inactive End Date.

Username	Target Unit	Branch	Delete
----------	-------------	--------	--------

Username	Preferred Language
First Name	Accreditation
Last Name	Brand
Email	2FA Status
Password	Forum Nick Name
Confirm password	Party Id
Home Branch	Last Logged In Date Time
Manager	2FA Inactive Begin Date
Target Unit	2FA Inactive End Date

4. Enter the mandatory fields required for creating a user.

Figure 1–22 Enter Mandatory Details

The screenshot displays the Oracle Banking Platform Admin Application interface. The page title is "User Management" and it includes a search filter and a table for user details. The "User Details Form" is expanded, showing various fields for user information. The fields are as follows:

Username	Target Unit	Branch	Delete

User Details Form

Username	Harry	Preferred Language	
First Name	Harry	Accreditation	
Last Name	Potter	Brand	
Email	Harry@gmail.com	2FA Status	
Password	*****	Forum Nick Name	
Confirm password	*****	Party Id	
Home Branch	1010	Last Logged In Date Time	
Manager		2FA Inactive Begin Date	
Target Unit	3LBL_BU_PB	2FA Inactive End Date	

Buttons: Edit, Apply changes, Assign Roles

5. Click **Apply Changes** to save the user details locally.

Figure 1–23 Applying Changes

The screenshot shows the Oracle Banking Platform Admin Application interface. The page title is "User Management". The search filter section has a "Username" input field with a search button. The "User Details" section contains a table with the following data:

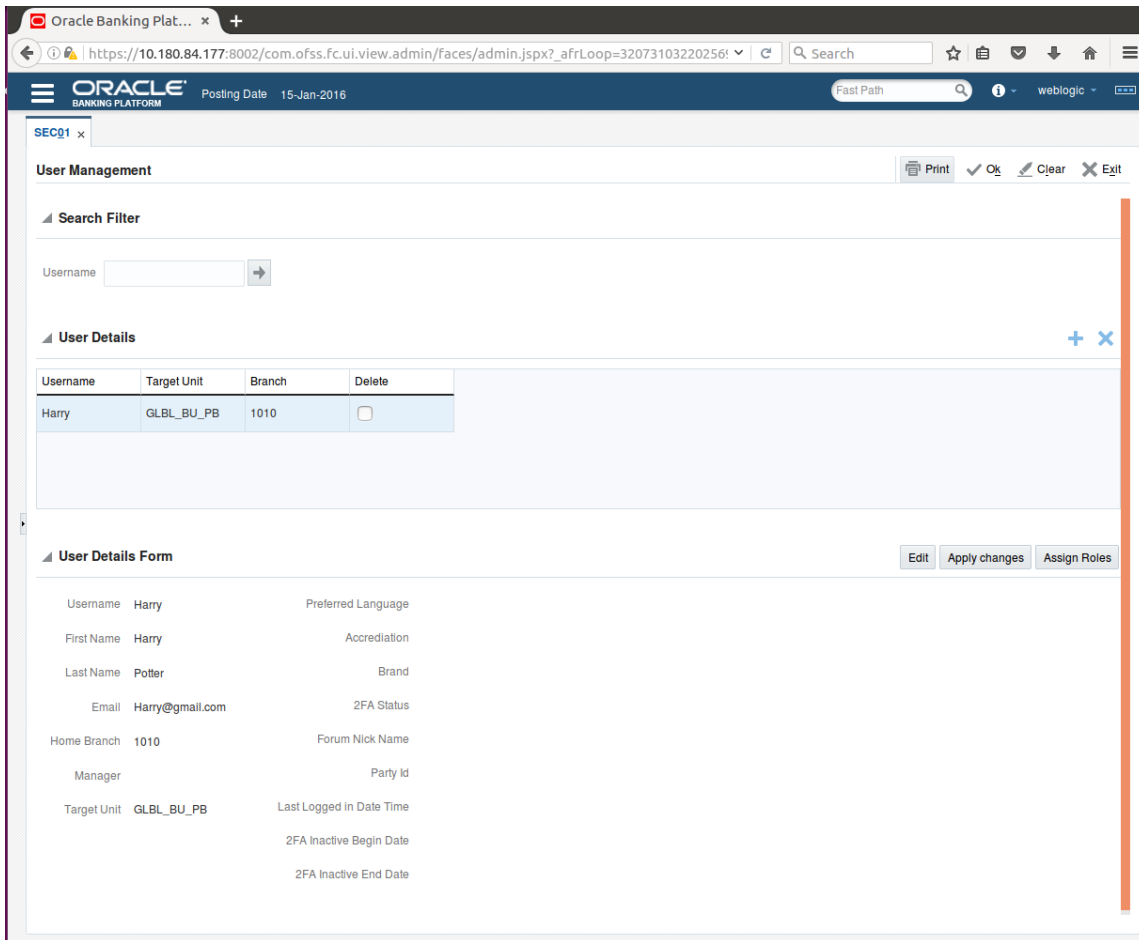
Username	Target Unit	Branch	Delete
Harry	GLBL_BU_PB	1010	<input type="checkbox"/>

Below the table is the "User Details Form" section, which includes buttons for "Edit", "Apply changes", and "Assign Roles". The form displays the following user details:

Username	Harry	Preferred Language
First Name	Harry	Accreditation
Last Name	Potter	Brand
Email	Harry@gmail.com	2FA Status
Home Branch	1010	Forum Nick Name
Manager		Party Id
Target Unit	GLBL_BU_PB	Last Logged In Date Time
		2FA Inactive Begin Date
		2FA Inactive End Date

6. To add a user to a group, select the row containing the user and click **Assign Roles**.

Figure 1–24 Adding User to a Group



The available and assigned roles appear.

Figure 1–25 Available and Assigned Roles

The screenshot displays the Oracle Banking Platform User Management interface. The page title is "User Management" and it includes a search filter for "Username" and a "User Details" section. The "User Details" section shows a table with one user, "Harry", associated with "GLBL_BU_PB" and "1010". Below this, the "Groups" section shows two tables: "All Roles" and "Assigned Roles". The "All Roles" table contains one role, "TestFullAccess", and the "Assigned Roles" table is empty, displaying "No data to display.".

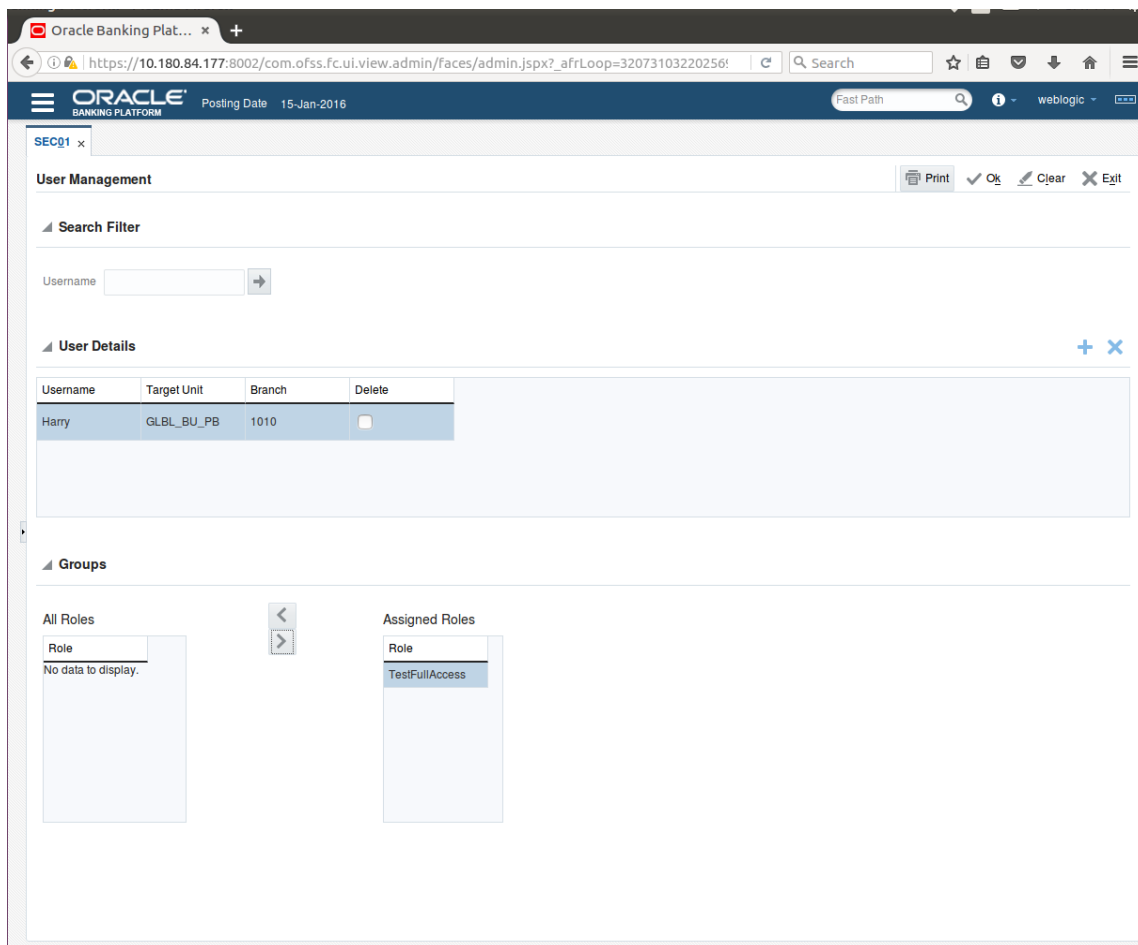
Username	Target Unit	Branch	Delete
Harry	GLBL_BU_PB	1010	<input type="checkbox"/>

Role
TestFullAccess

Role
No data to display.

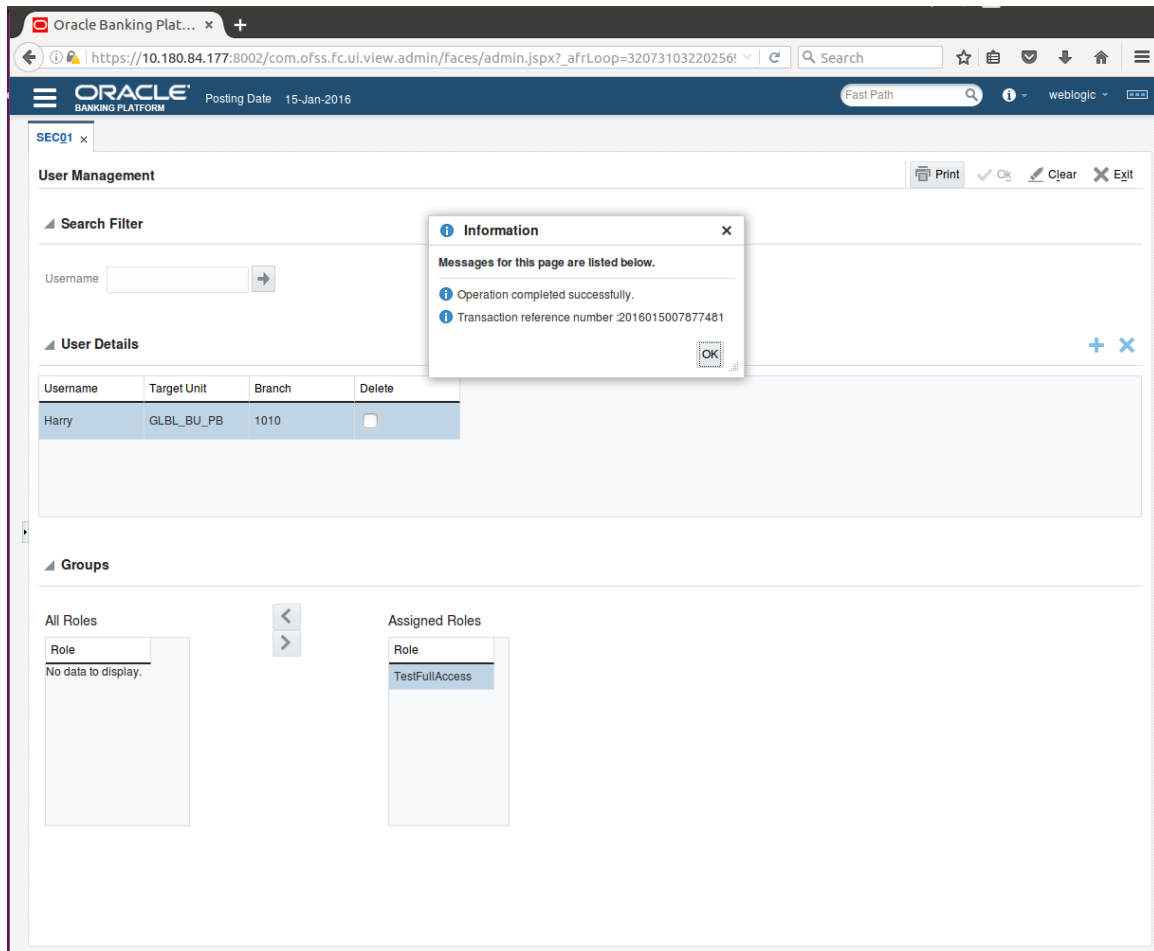
7. Select the group to add user and move it to the **Assigned Roles** table.

Figure 1–26 Adding User to Assigned Roles Table



8. Click **Ok** to save the changes.

Figure 1–27 Save Changes



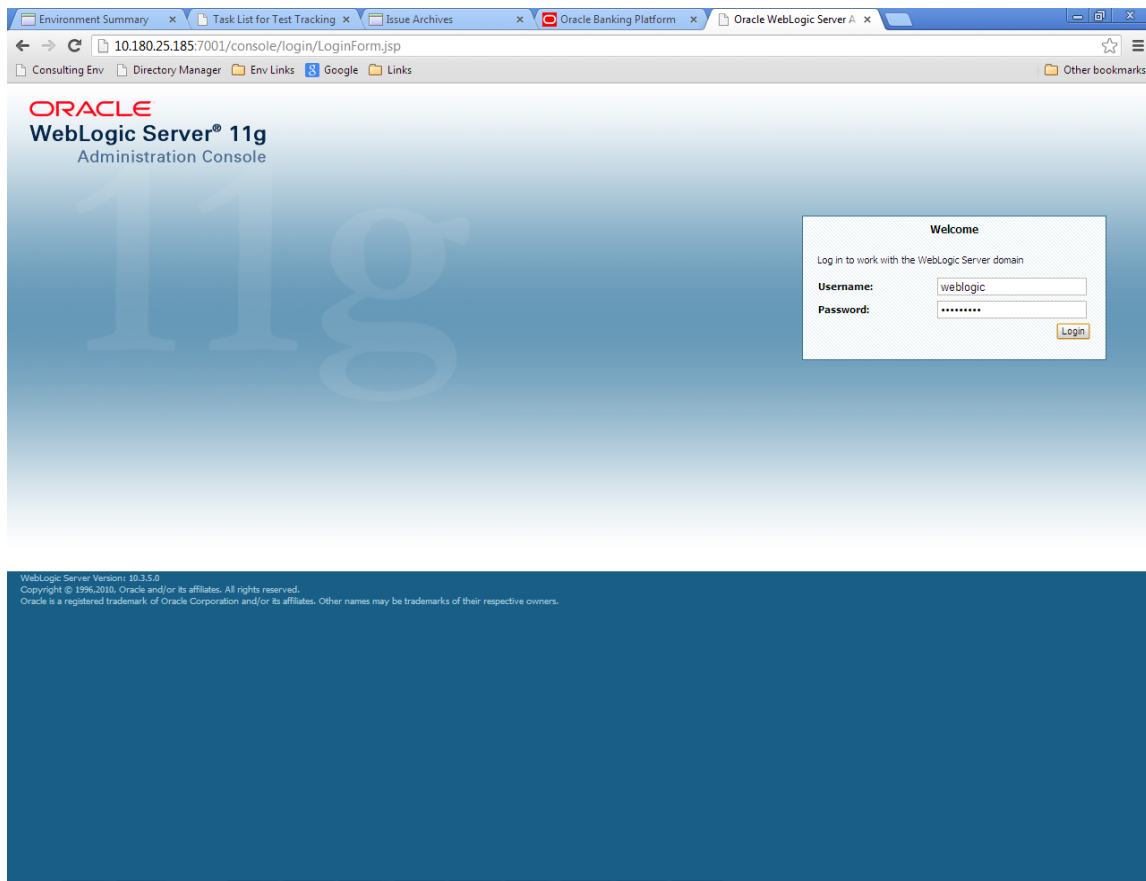
1.8 Unlocking Users in Oracle WebLogic Server (OWS) Administration Console

This section explains the procedure to unlock users in Oracle WebLogic Server (OWS) using Administration Console. If users unsuccessfully attempt to log in to a WebLogic Server instance for more than the configured number of retry attempts, they are locked out of further access. This procedure allows you to unlock locked users so that they can log in again.

To unlock a user in OWS:

1. Log in to OWS. The **Home Page** of OWS Administration Console appears.

Figure 1–28 OWS Log in



2. In the **Domain Structure** section, click the **base_domain** link.

Figure 1–29 base_domain

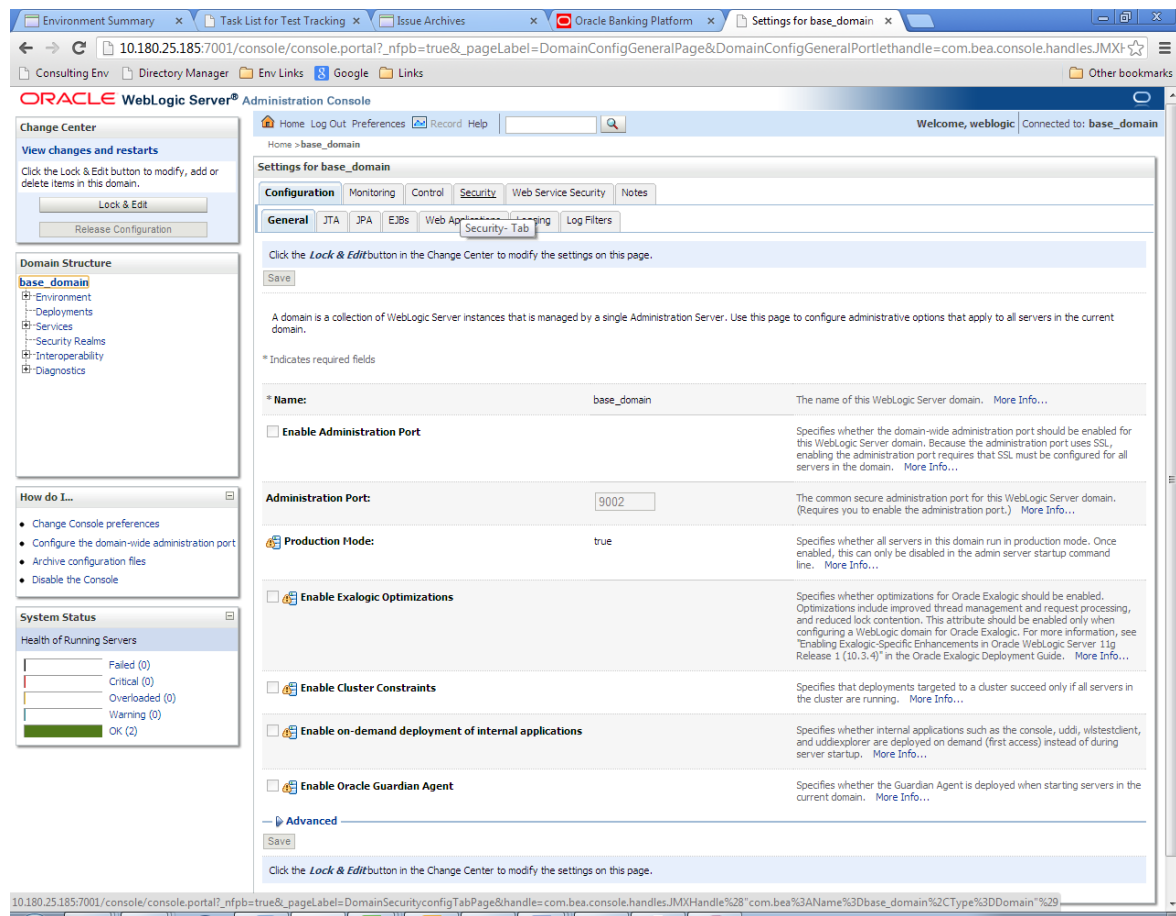
The screenshot displays the Oracle WebLogic Server Administration Console for the 'base_domain'. The interface includes a navigation menu on the left with sections like 'Change Center', 'Domain Structure', 'How do I...?', and 'System Status'. The main content area is titled 'Home Page' and contains several panels: 'Information and Resources' with helpful tools and general information; 'Domain Configurations' with a tree view showing 'Domain', 'Environment', 'Services', and 'Interoperability'; 'Environment' with a list of servers, clusters, and virtual hosts; 'Your Deployed Resources' with a list of deployments; and 'Your Application's Security Settings' with a list of security realms. The 'System Status' section shows a bar chart indicating the health of running servers, with 2 servers in the 'OK' state.

WebLogic Server Version: 10.3.5.0
Copyright © 1996-2010, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

10.180.25.185:7001/console/console.portal?_nfpb=true&_pageLabel=DomainConfigGeneralPage&DomainConfigGeneralPortleHandle=com.bea.console.handles.JMXHandle%28*com.bea%3AName%3Dbase_domain%2CType%3DDoma...

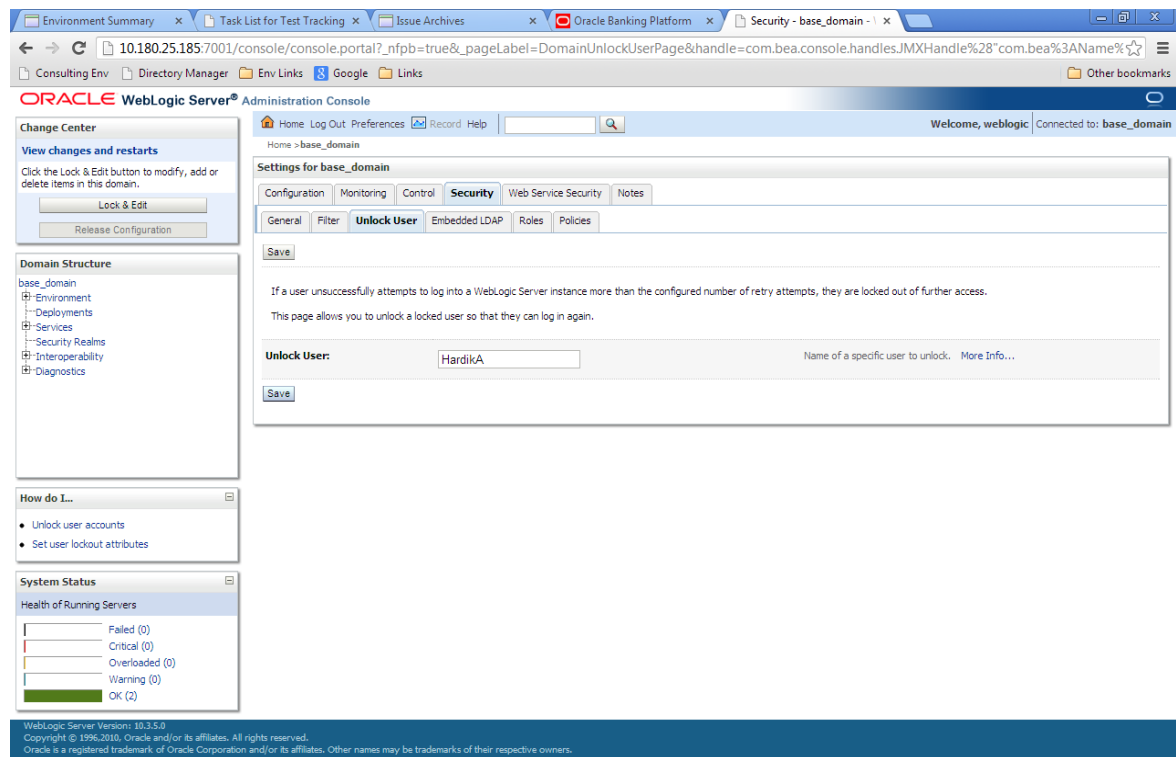
3. In the **Settings for base_domain** page that appears, click the **Security** tab.

Figure 1–30 Security tab



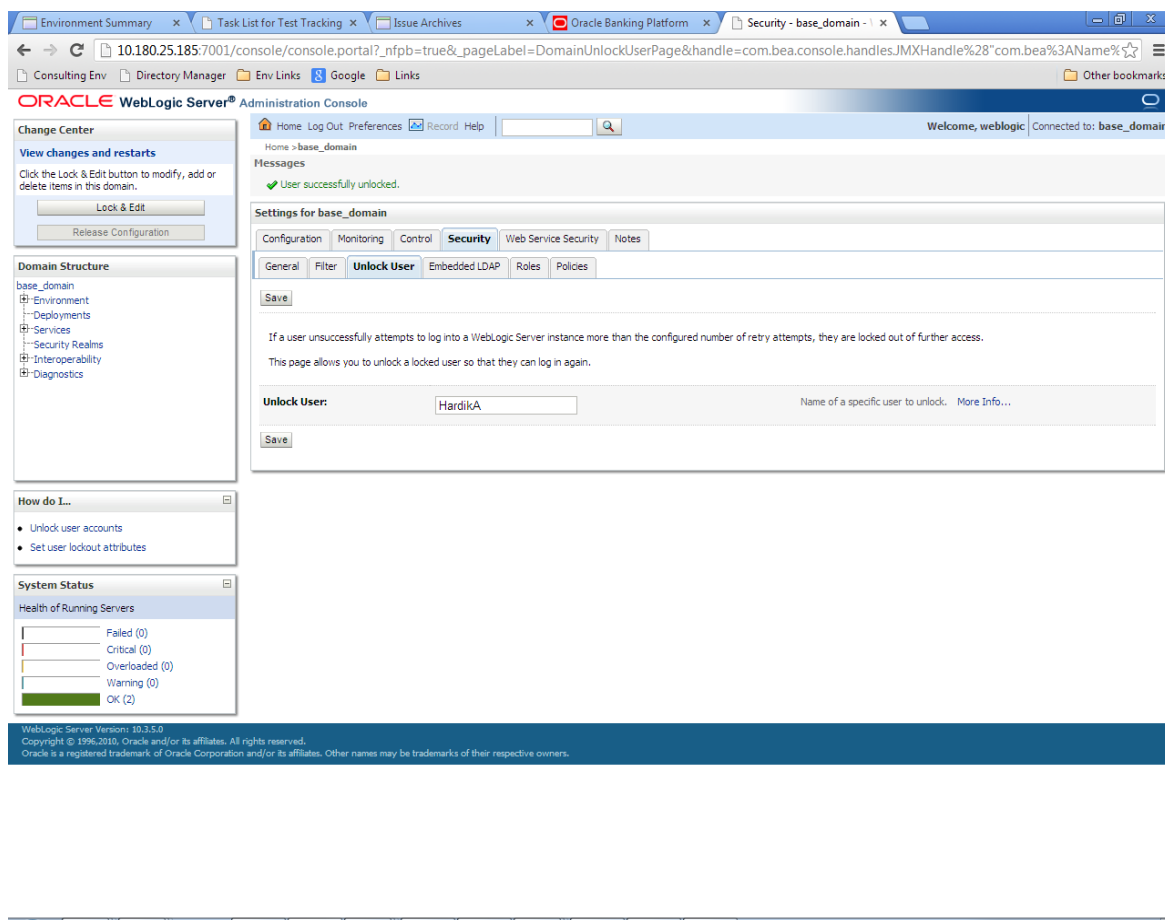
4. Click the **Unlock User** tab.
5. In the **Unlock User** field, enter the User ID to unlock the user.

Figure 1–31 Unlock User



6. Click **Save**. The message *User successfully unlocked* appears.

Figure 1–32 User Successfully Unlocked



On completion of this procedure the user gets unlocked in OWS.

1.9 Creation of first time user to access OBEDM

This section explains the procedure to create the first bank user having access to the application.

Note

Make the default authenticator as sufficient in host console and reorder it below OID Authenticator. Also change 'cn' attribute to 'uid' in the All Users Filter and User From Name Filter in OID Authenticator provider specific properties.

1. Log in to OIM using the admin user `xelsysadm`. Create a new role in OIM as described in [Section 1.2 Creating Roles in Oracle Identity Manager \(OIM\)](#). For example, Developer. This creates a group in OID (Developer).
2. Log in to admin application using the weblogic user. Create a user as described in [Section 1.7 User Management Using the Admin Application](#). For example, john.doe.

3. Add the user (john.doe) to the Developer.
4. Map the application role Administrators to the Enterprise Group Developer in EM (refer screenshots below). After doing this, the user should have access to all artifacts assigned to the 'Administrators' role. These access rights can be viewed in OES.

Figure 1–33 Log in Oracle Fusion Middleware Control

SIGN IN TO
ORACLE ENTERPRISE MANAGER
FUSION MIDDLEWARE CONTROL 12c

Domain Domain_01_domain

* User Name weblogic

* Password *****

Login to Partition

Sign in

ORACLE

Copyright © 1996, 2016, Oracle and/or its affiliates. All rights reserved. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

1.9 Creation of first time user to access OBEDM

Figure 1–34 Click Application Roles

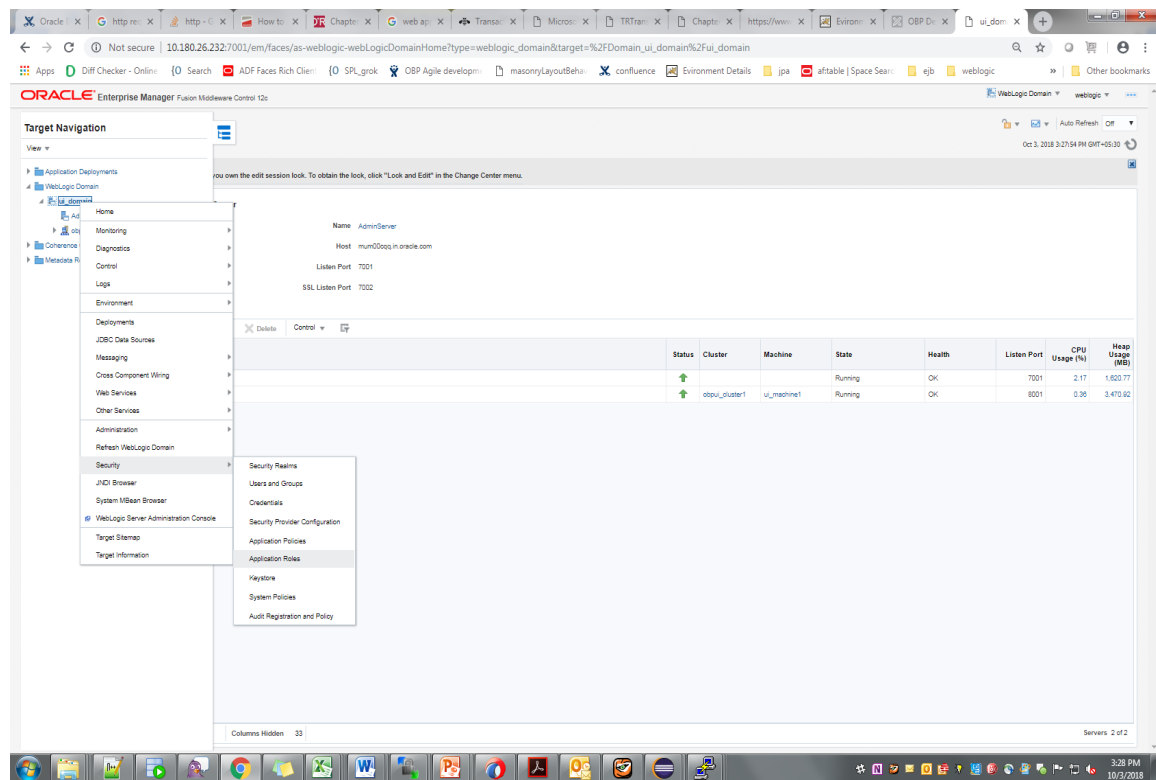


Figure 1–35 Select Administrators Role

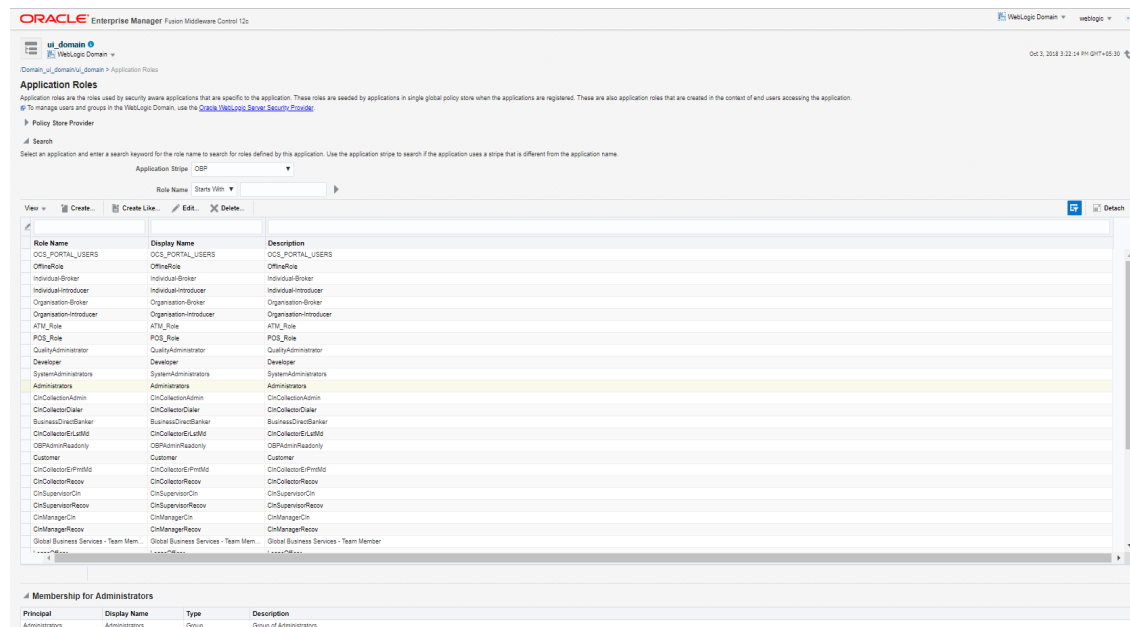
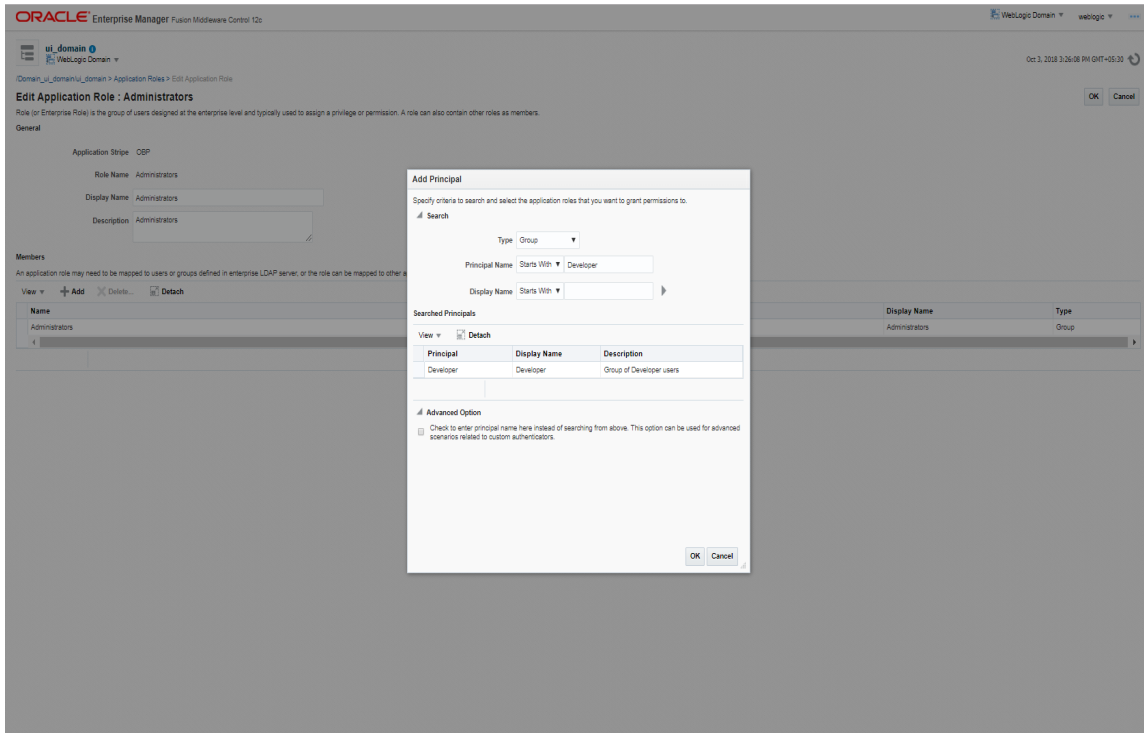


Figure 1–36 Add Principal



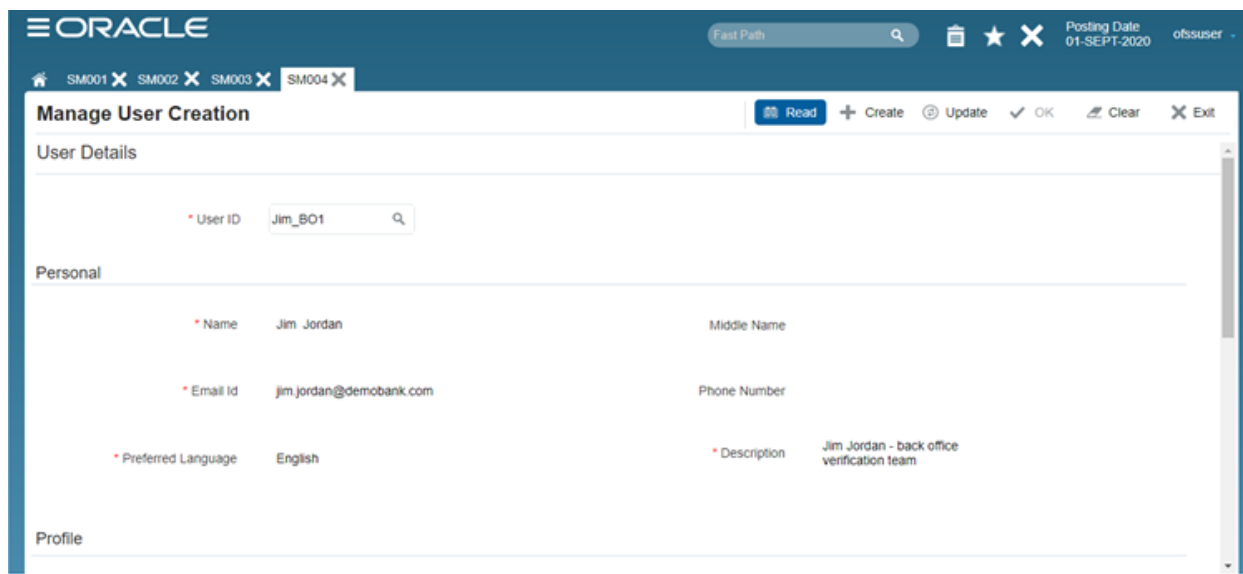
2 User Management With Local Security

This chapter describes the configurations to be done if local security option is configured, instead of OIM based security.

2.1 Create User or User Details

Using the Manage User Creation (SM004) screen, a new user can be created by filling in all the details. The users are mapped to the enterprise role in this screen.

Figure 1–37 Create User

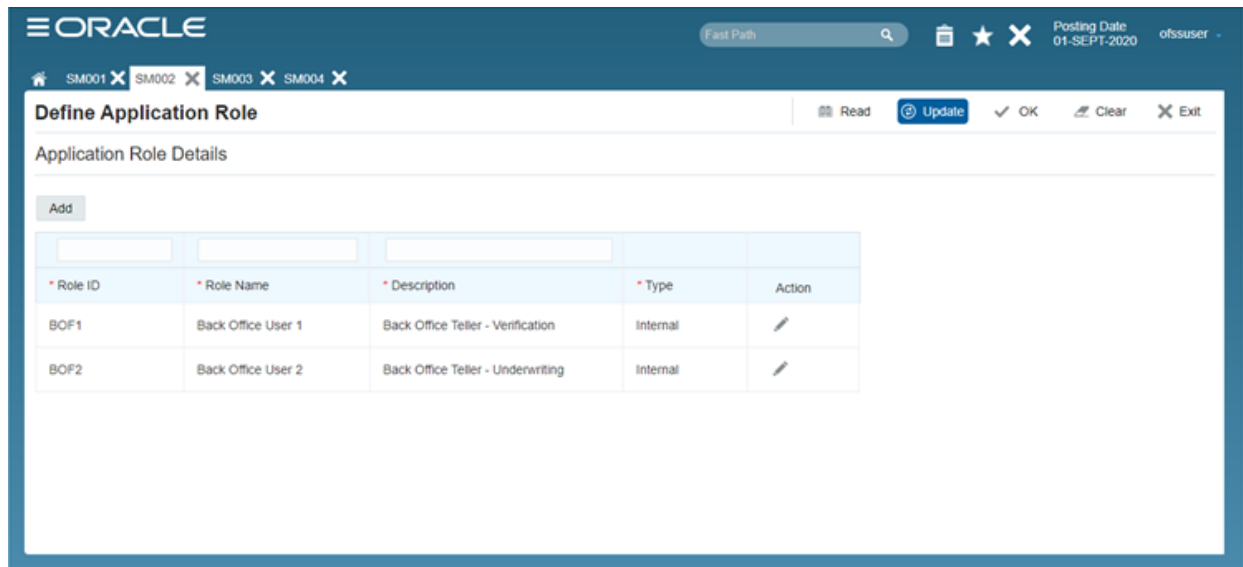


The screenshot displays the Oracle Manage User Creation (SM004) interface. The top navigation bar includes the Oracle logo, a search bar, and user information (Posting Date: 01-SEPT-2020, ofssuser). The main header shows the current screen (SM004) and a toolbar with actions: Read, Create, Update, OK, Clear, and Exit. The form is divided into sections: User Details, Personal, and Profile. The User Details section contains a User ID field with the value 'Jim_BO1'. The Personal section includes fields for Name (Jim Jordan), Middle Name, Email Id (jim.jordan@demobank.com), Phone Number, Preferred Language (English), and Description (Jim Jordan - back office verification team).

2.2 Define Application Roles

The application roles are created using the Define Application Role (Fast Path: SM002) screen. The application roles are used within the application. For more information, Oracle Banking Enterprise Default Management Security Guide.

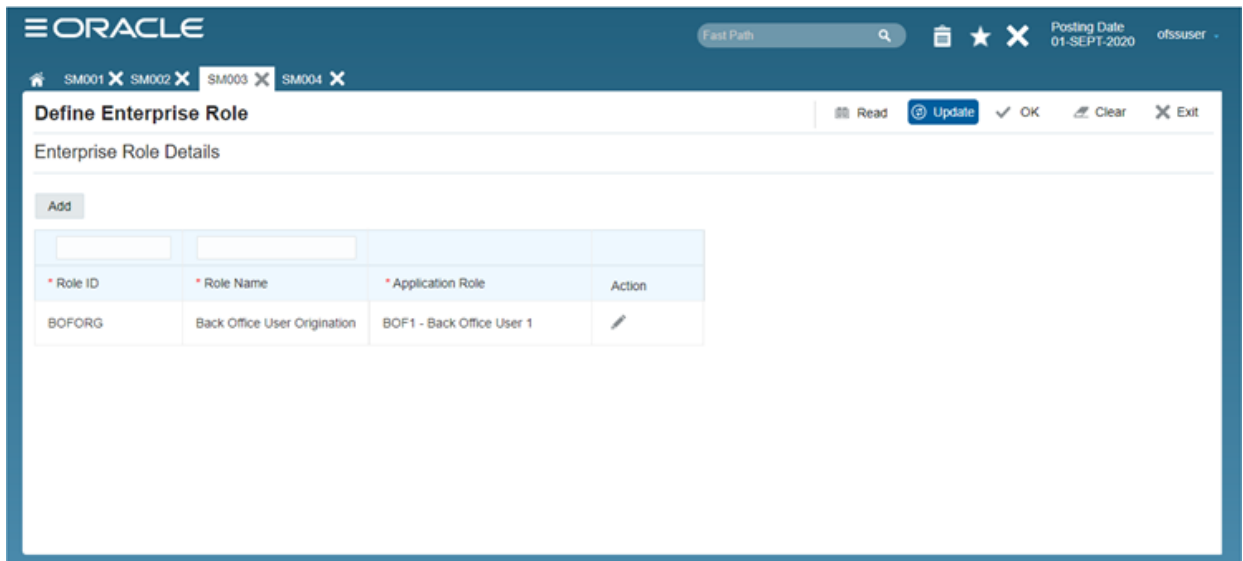
Figure 1–38 Define Application Role



2.3 Define Enterprise Role

The enterprise roles are used across organization. These roles are created and are mapped to application roles using the Define Enterprise Role (Fast Path: SM003) screen.

Figure 1–39 Define Enterprise Role



2.4 Password Policy Management

The Password Policy Management (Fast Path: SM001) screen covers the details of password policy to be managed by bank. All the prerequisites for password creation during user creation and password lifecycle are defined using this screen.

Figure 1–40 Password Policy Management

The screenshot displays the Oracle Password Policy Management interface. At the top, the Oracle logo is on the left, and a search bar labeled 'Fast Path' is on the right. Below the search bar, there are navigation tabs for 'SM001', 'SM002', 'SM003', and 'SM004'. The main title is 'Password Policy Management', followed by action buttons: 'Read', 'Create', 'Update', 'OK', 'Clear', and 'Exit'. The section is titled 'Policy Details' and contains the following configuration fields:

- * Minimum Length:
- * Maximum Length:
- * Minimum Numeric Characters:
- * Minimum Alphabet Characters:
- * Minimum Special Characters:
- * Maximum Special Characters:
- * Minimum Uppercase Characters:
- * Minimum Lowercase Characters:
- * Expires After: days
- * Warn After: days
- * Allow First/Last Name:
- * Allow User ID:

3 Setting Up The Bank And Branch

This chapter provides the process of setting up the bank and the branch commonly referred to as the Day 0 setups.

3.1 Common Services Day 0 Setup

The Common Services setup includes the following sections.

3.1.1 Core Maintenances

Core Entity Services seek to define the broad parameters within which the rest of the application functions. The service defines the bank, the various modules of the application that the bank may want to introduce, the languages and the time zones it operates in, the core parameters and structures of its various branches. The core entity services are also used by each of the different modules, and provide a variety of support functions to them.

The following Core Maintenances must be completed as a part of bank and branch setup:

- Bank Codes (Fast path: CS01)
- Bank Parameters (Fast path: CS03)
- Branch Parameters (Fast path: CS06)
- Country Codes (Fast path: CS09)
- Financial Cycle (Fast path: CS10)
- Define Payment Calender Codes (Fast path: CS15)
- Reason Codes (Fast path: CS16)
- State Codes (Fast path: CS17)
- Purpose Codes (Fast path: CS24)
- Bank Policy (Fast path: CS26)
- Transaction Code Maintenance (Fast path: CS44)
- Define Non-Financial Event Transaction Code Mapping (Fast path: CS45)
- Data Security Configuration (Fast path: CS50)

Note

To view the detailed procedure for each application page, see its context sensitive help in the application.

3.1.1.1 Head Office Setup

The Head Office branch creation is currently being done via seed data where the Branch Type is HO. Branch Type is a seed table with fixed values for all applicable branch types, that is uploaded to the application from the backend. After the creation of Head Office branch through seed data, you can proceed to create other branches from the application where the Branch Type is shown as a LOV (excluding HO).

The process to set up a head office branch is as follows:

1. Create a new bank code in the application through the page **Bank Codes (Fast path: CS01)**.
2. Set up the new bank parameters through the page **Bank Parameters (Fast path: CS03)**.
3. Modify the seed data for Branch Type to include the new bank code as HO and run the seed. Currently the seed will be for Bank Code 08. The head office branch is created via this seed data.
4. Proceed to create the other branches through the application using the page **Branch Parameters (Fast Path: CS06)**, that includes all branch types other than HO.

Note

To view the detailed procedure for each application page, see its context-sensitive help in the application.

3.1.2 Currency Maintenances

The Currency Services are a part of the common services of Oracle Banking Platform and serve to record and retrieve the various currency related information.

The following Currency Maintenances must be completed as a part of bank and branch setup:

- Currency Codes (Fast path: CY01)
- Amount Text (Fast path: CY02)
- Currency Pairs (Fast path: CY03)
- Currency Branch Parameters (Fast path: CY04)
- Currency Denomination (Fast path: CY05)
- Currency Rate Types (Fast path: CY06)
- Exchange Rates (Fast path: CY07)

Note

To view the detailed procedure for each application page, see its context-sensitive help in the application.

3.1.3 Calendar Maintenances

The calendar services are embedded in the common services and serve to record and retrieve the various holidays of the bank in a calendar year.

The following Calendar Maintenances must be completed as a part of bank and branch setup:

- Holiday Rule Maintenance (Fast Path: CAL01)
- Calendar Type Maintenance (Fast Path: CAL02)
- Adhoc Calendar Maintenance (Fast path: CAL03)

Note

To view the detailed procedure for each application page, see its context-sensitive help in the application.

3.2 Accounting Day 0 Setup

The Accounting module is supported by Module Accounting, Domain Accounting, and Accounting Services.

- Module Accounting handles transaction initiation, raises accounting event, and updates the customer account balances and Overdraft limits, and invokes account services.
- Domain Accounting provides the services such as input, authorize, delete, and reverses to the modules to enable the module to initiate appropriate action on the transactions. Domain accounting also validates data and lookup accounting template, builds domain entries, and performs currency conversions.
- Accounting Services pick up the entries formed by the domain accounting and perform GAAP accounting, netting, currency position, Inter Branch entries, tanking of unauthorized transactions, suspense posting, generation of P&L entries for year end, and hand off data to product ledger.

The following Accounting maintenances must be completed as a part of bank and branch setup:

- Define System Defined Elements (Fast path: AS013)
- Define Accounting Configuration (Fast path: AS001)
- GAAP Summary (Fast path: AS005)
- Define Bank Parameter (Fast path: AS002)
- Define Branch Parameter (Fast path: AS003)
- Define SDE Range (Fast path: AS012)
- System Defined Elements Class Summary (Fast path: AS011)
- Define Accounting Ledger (Fast path: AS009)
- Define Accounting Ledger (Additional) Details (Fast path: AS010)
- Define Accounting Ledger Group (Fast path: AS008)
- Define Inter Branch Parameters (Fast path: AS006)
- Define Domain Category Accounting Template (Fast path: AS016)
- Define Domain Role Mapping (Fast path: AS019)

Note

To view the detailed procedure for each application page, see its context-sensitive help in the application.

3.3 Product Manufacturing Day 0 Setup

Following are the required setups:

Prerequisites

Following are the prerequisites for Product Manufacturing Day 0 Maintenances:

- Common Services: Purpose Code, Currency Code, Calendar Maintenance, Bank Policy
- Accounting Template Maintenance

- DMS maintenance: Document Type Definition (Fast path: CNM01), Document Category Definition (Fast path: CNM02), Document Policy Definition (Fast path: CNM03)
- Risk Indicators Impacts Cross-Reference (Fast path: ACCT010)
- Rate Chart Maintenance (Fast path: PR004)
- Index/Margin Index Code Definition (Fast path: PR005)
- Price Policy Chart Maintenance (Fast path: PR007)
- Price Definition (Fast path: PR006)
- Charge Attribute Definition (Fast path: PR008)

Day 0 Maintenances

The following Product Manufacturing Maintenances must be completed as part of bank and branch set up:

- Define Hardship Relief Policy (Fast path: PM006)
- Define Interest Rule (Fast path: PM011)
- Define Domain Category Settlement Mode (Fast path: PM030)

Note

To view the detailed procedure for each application page, see its context-sensitive help in the application.

4 Application Monitoring Using Administration Application

This chapter provides an overview on the various monitoring operations performed as an administrator using Administration application.

4.1 Dynamic Monitoring Service (DMS)

The aim is to monitor different channels involved in performing transactions with OBEDM. The monitoring parameters consists of channels, services, trends (current behavior of execution), and time metrics. The monitoring is performed by DMS (Dynamic Monitoring Service).

What is DMS?

The Oracle Dynamic Monitoring Service (DMS) provides a set of Java APIs that measure and report performance metrics, trace performance and provide a context correlation service for Fusion Middleware and other Oracle products. Along with the APIs, DMS provides interfaces to enable application developers, support analysts, system administrators, and others to measure application-specific performance information.

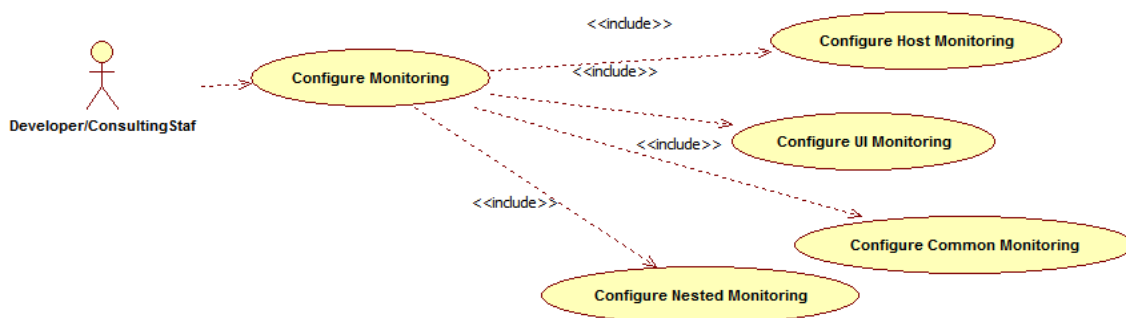
4.1.1 Usage

The usage of DMS is defined by the role of the user. Based on their roles, users can either take part in configuration of services for DMS or monitor the statistics collected via DMS.

Developers

These are the set of people who configure the monitoring services that are the part of OBEDM system. The configuration can be made either for available services or for new services.

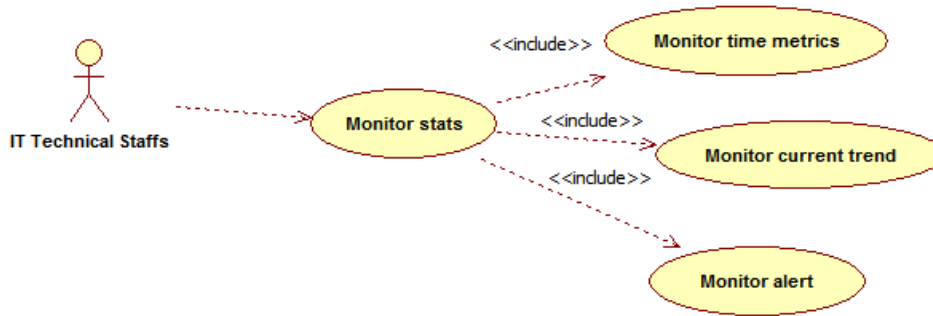
Figure 3–1 Developers



IT Technical Staff

This consists of set of people who monitor the DMS statistics generated for the service. With the help of various metrics generated they can analyze the behaviour of the target service. For example, 'time taken to execute' service could indicate need of optimization of the service.

Figure 3–2 IT Technical Staff



4.1.2 Monitoring Application using the OPA001 page

Once DMS statistics are captured for a particular Channel and transactions involving it, it requires a UI representation to understand the statistics in a readable form so that one can analyse the behaviour. The monitoring activities are mainly carried out by IT Technical staff.

4.1.2.1 Monitoring Application Performance (Fast path: OPA001)

This page gives the monitoring statistics of different channels and the transactions occurring through it. It gives the time metric of the transactions, trend of the current transactions, and alert for the channel.

Figure 3–3 Monitoring Application Performance

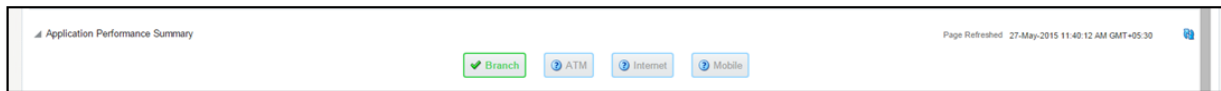
The screenshot shows the 'Monitor Application Performance' page. It includes a summary section with filters for Branch, ATM, Internet, and Mobile. Below the summary is a table with columns for Alert, Channel, Module, Layer, Transaction, Task Code, Trend, Alert Event Time, Trend Reference Queue, Last Alert User, Time in milliseconds (Average, Max, Min, Total), Transaction Count (Success, Failure), and Amount (Debit, Credit).

Alert	Channel	Module	Layer	Transaction	Task Code	Trend	Alert Event Time	Trend Reference Queue	Last Alert User	Time in milliseconds				Transaction Count		Amount	
										Average	Max	Min	Total	Success	Failure	Debit	Credit
Branch	ORIGINATION	Spi		Perform Auto Decision	-	↓	27-May-2015 11:39:37	4147, 5047, 3252, 3994, ...	arun	4,563	6,463	2,890	36,501	8	0	-	-
Branch	TD	Baking Bean		Mixed Paym_ UI	TD002	↓	27-May-2015 10:46:53	881, 936, 2143, 2616, 6816	-	4,155	19,078	861	58,167	14	0	-	-
Branch	PARTY	Spi		Add Or Update Party Financial Profile	-	↓	27-May-2015 11:39:21	6739, 2380, 1740, 758, 1, ...	arun	3,993	11,972	758	35,936	9	0	-	-
Branch	CASA	Baking Bean		Alternate Accounts Save_ UI	CASA037	↓	27-May-2015 10:39:16	465, 2720	-	1,593	2,720	465	3,185	2	0	-	-
Branch	ACCOUNT	Spi		Recommend Bundles	VL000	↓	27-May-2015 11:36:01	424, 901, 399, 1103, 1927	arun	1,528	10,281	306	56,535	37	0	-	-
Branch	CONTENT	Spi		Deliver And Save Documents	OR247	↓	27-May-2015 10:38:39	1308, 1359, 1420, 1303, ...	asavant	1,515	2,339	1,303	10,602	7	2	-	-
Branch	ORIGINATION	Spi		Submit Create Offer	OR223	↓	27-May-2015 10:40:22	1025, 1271, 1170, 1288, ...	asavant	1,362	2,006	972	9,537	7	0	-	-

The overall page can be subdivided into 3 sub parts on the basis of information they provide:

4.1.2.1.1 Application Performance Summary

This section gives the information about the different channels of OBEDM through which transactions are taking place. The information is about the health and active channels. The 'Refresh Button' on top of this section gets the latest (refreshed) metrics.

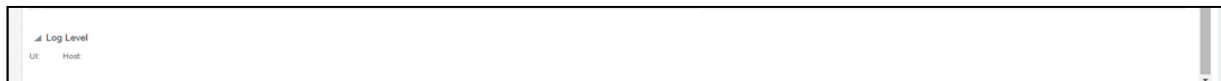
Figure 3–4 Application Performance Summary

Following are the few notification about the channels:

- Denotes transactions not present for the channel
- Denotes normal status that is, the number of alerts are less than the specified limit
- Denotes warning status that is, the number of alerts are in the warning range
- Denotes critical status that is, number of alerts exceeds the limit

4.1.2.1.2 Log Level

This section gives logger level information for the host and UI server.

Figure 3–5 Log Level

4.1.2.1.3 Application Performance

This section gives the metrics for the transaction. Metrics include timing, alert, trending information. Certain filters can be applied over the metric table. Initially only 100 (Initial page size which is configurable) transactions are displayed. To display all the transactions, 'ALL' button is to be clicked.

Trend

Indicates trending of execution timings of transaction. It is calculated by algorithm namely, Exponential Moving Average where if the execution time goes above the specified limit which is calculated by adding average execution time of the transaction and allowed limit (varies logarithmically to execution time); the transaction is considered as trending upwards and vice-versa for downwards trend.

However, if the execution time is with the range, trend is considered as neutral.

Alert

Indicates alerting state of the transaction. A transaction is given weight based on its properties namely, transaction type, timing category and OBEDM module. The weight gives the offset allowed for transaction execution time. If the current transaction time is greater than average transaction time + offset, it is marked as alert. Initially it is marked as 'Critical' and after sometime the state is marked as 'Warning'.

Figure 3–6 Alert State

The screenshot displays the 'Monitor Application Performance' window. At the top, there's a summary section with filters for Branch, ATM, Internet, and Mobile. Below this is a table with columns for Alert, Channel, Module, Layer, Transaction, Task Code, Trend, Alert Event Time, Trend Reference Queue, Last Alert User, Time in milliseconds (Average, Max, Min, Total), Transaction Count (Success, Failure), Amount (Debit, Credit), Trend Reference, Nested Status, Alert EOD, and Service. The table lists several transactions with their respective alert states and performance metrics.

The table below explains each column of the table present in the given snapshot.

Table 3–1 Alert State

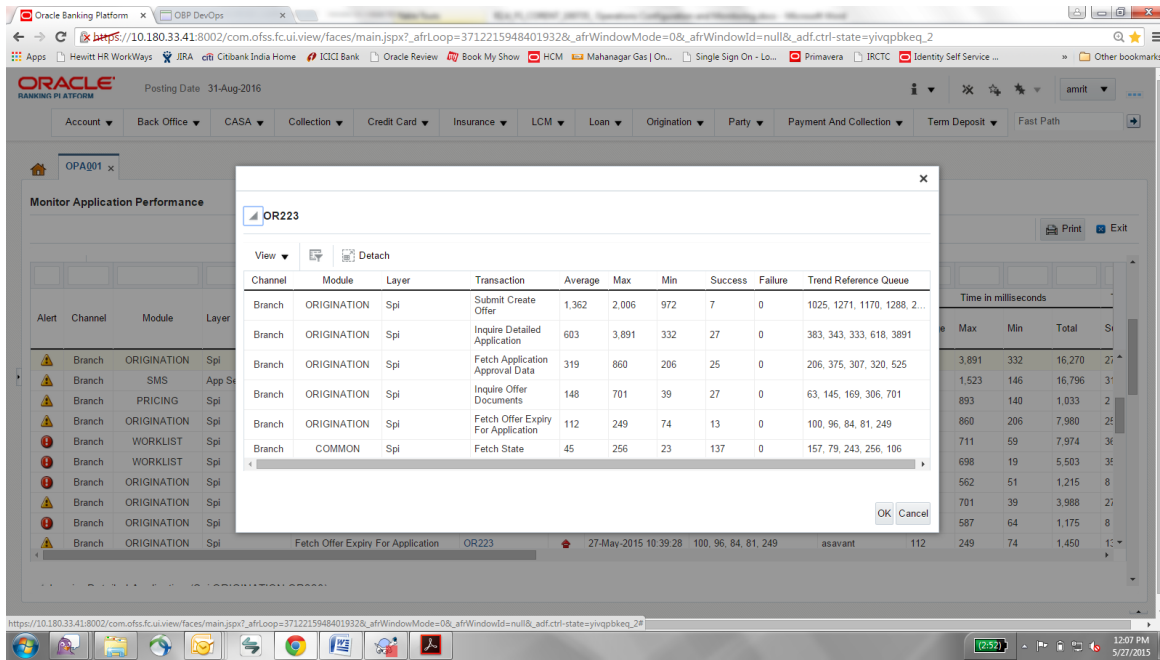
Sr. no.	Column Name	Description
1	Alert	Alert state of the transaction Valid Values: BLANK: No alert, Warning: Alert in past (default 5 minutes), Critical: Alerted Transaction
2	Channel	Channel through which the transaction occurred Valid Values: Branch, ATM, and POS.
3	Module	OBEDM module of which transaction is a part
4	Layer	Configured Noun generation layer. Backing Bean for UI and Spi and App Service for Host.
5	Transaction	Name of the transaction
6	Task Code	Task code of the OBEDM page by which the transaction was triggered
7	Trend	Trending of transaction Valid Values: Upwards, Downwards, Neutral
8	Alert Event Time	Time at which last alert occurred for the transaction
9	Trend Reference Queue	Execution time of last n transactions (n=5)
10	Last Alert User	Teller who performed the last alerted transaction
11	Average Time	Average execution time
12	Max Time	Maximum time of execution of the transaction

Sr. no.	Column Name	Description
13	Min Time	Minimum time of execution of the transaction
14	Total Time	Total time of execution
15	Success Count	Number of times transaction executed successfully
16	Failure Count	Number of times transaction failed.
17	Debit Amount	Amount debited after transaction
18	Credit Amount	Amount credited after transaction
19	Trend Reference	Execution time of last transaction
20	Nested Status	Nested Status
21	Alert ECID	ECID of the last alerted transaction
22	Service	Service name of the transaction
23	Completed Operations	Number of completed transactions
24	Active Threads	Active Threads
25	Max Active Threads	Maximum active threads
26	Host	Host name
27	Process	Process Name
28	Server Name	Server name
29	App Root Type	Root type of noun
30	Failure Security Event	Failure due to security error
31	2FA Event	Authentication error
32	Failure Database Event	Failure due to database error
33	Failure Technical Event	Failure due to technical error
34	Failure Outbound Event	Failure due to outbound call (call outside OBEDM)

One can select any of the task code which opens a popup with information about that task code only.

4.1 Dynamic Monitoring Service (DMS)

Figure 3–7 Select Task Code



Detailed Transaction View

This section gives the detailed view of a selected transaction. The desired transaction can be selected from the table (metric table). Click on any row to display a detailed view of the transaction.

Figure 3–8 Selection of Desired Transaction

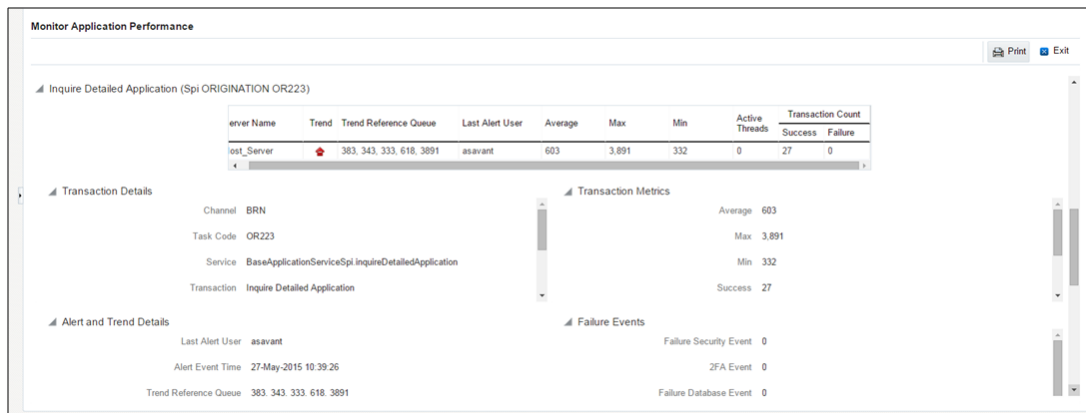


Figure 3–9 Transaction Details

Transaction Details	
Channel	BRN
Task Code	OR223
Service	BaseApplicationServiceSpi.inquireDetailedApplication
Transaction	Inquire Detailed Application
App Root Type	Transaction
Host	ofss3121059.in.oracle.com
Server Name	Host_Server
Process	obphost_server1:8001

Figure 3–10 Transaction Metrics

Transaction Metrics	
Average	603
Max	3,891
Min	332
Success	27
Success	27
Failure	0
Active Threads	0
Max Active Threads	1

Figure 3–11 Alert and Trend Details

Alert and Trend Details	
Last Alert User	asavant
Alert Event Time	27-May-2015 10:39:26
Trend Reference Queue	383, 343, 333, 618, 3891
Alert ECID	9d35654d4414a931:-6e0ab1f:14d8b6681e1:-8000-000000000000d612

Figure 3–12 Failure Events



Configurations

The below mentioned configurations can be made in `DMSConfig.properties`:

- **Channel Status:** Number of alerts for which the channel shows 'Critical and 'Warning' status can be configured
- **Alert Status:** The time after which a 'Critical' alert changes to 'Warning' is configurable
- **Initial Page Size:** Every time host data is fetched only rows equal to page size are displayed. The page size is configurable

These configurations can be made in `DMSConfig.properties`.

5 Transparent Data Encryption (TDE)

This chapter describes the configuration, installation, and policy setup of Transparent Data Encryption (TDE).

Transparent Data Encryption is a technology used to encrypt database files. This feature enables you to protect sensitive data in database columns stored in operating system files by encrypting it. Then, to prevent unauthorized decryption, it stores encryption keys in a security module external to the database.

5.1 Configuration

The following is the classification of information related to OBEDM. This information is used to drive TDE configuration.

Table 4–1 TDE Configuration

Classification	Details	Access and Distribution	Action
Public	This information is not sensitive, and there is no value with it remaining confidential to Bank.	No restrictions	No Encryption
Confidential Internal	It is important that this information remains confidential to Bank.	May be accessed by and distributed to all support person. Distribution to third parties must be authorized by the information owner and requires that an appropriate confidential disclosure agreement be in place.	No Encryption
Confidential Restricted	It is very important that this information remains confidential to Bank and that access within bank is restricted on a need-to-know basis.	Internal access/distribution must be on a business need-to-know basis. Not authorized for information unless the information is encrypted using Oracle-approved encryption.	Need to set encryption rule during TDE
Confidential Highly Restricted	It is essential that this information remains confidential to Bank and that access within bank is restricted on a need-to-know basis.	Internal access/distribution must be very limited and is on a stringent business need-to-know basis. Not authorized for information unless the information is encrypted using Oracle-approved encryption.	Need to set encryption rule during TDE

All tables in OBEDM are classified based on above classification and columns of those tables are marked based on sensitivity.

5.2 Installation

This section explains the installation process.

5.2.1 Prepare Scripts to Encrypt Sensitive Data

Database administrator needs to create alter script to encrypt sensitive data. The utility tool (obpencryption.sh) is used to create this alter script for TDE. To run the tool, the following prerequisites are required.

Prerequisites

- Create a folder "obpencryption" where user wants to run the tool.
- Upload Sensitive_Data_List.xlsx, obp-encryption-script-gen.jar, obpencryption.sh, DB_RESOURCEBUNDLE.properties. These files are available in maskingencryption.zip. The maskingencryption.zip is part of host.zip available in installer.
- Update database details in DB_RESOURCEBUNDLE.properties file before running the script.
- Update value "encryptLocation" variable with obp encryption path in obpencryption.sh at line 6.

For example: `encryptLocation="/scratch/app/product/obpencryption"`

Run Encryption Tool

- Create update scripts for all the tables containing sensitive data. Run obpencryption.sh with TDE and ENCRYPT.

For example: `/obpencryption.sh TDE ENCRYPT`

5.2.2 Create TDE Keystore

Perform these steps to create keystore which is required for encryption and decryption. Perform the following steps.

- Create keystore location with `mkdir -p <location>`.

For example: `mkdir -p /scratch/app/admin/TDE/encryption_keystore/`

- Log in to database with `sysdba`.

For example: `sqlplus / as sysdba`

- Run the following sql instruction:

- ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '{Keystore loaction}' IDENTIFIED BY {Password}

For example: `SQL>ADMINISTER KEY MANAGEMENT CREATE KEYSTORE '/scratch/app/admin/TDE/encryption_keystore/' IDENTIFIED BY myPassword`

- ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY welcome1 CONTAINER=ALL;

For example: `SQL>ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY welcome1 CONTAINER=ALL;`

- ADMINISTER KEY MANAGEMENT CREATE KEY using tag 'KEY5' IDENTIFIED BY welcome1 WITH BACKUP CONTAINER =all;

For example: `SQL>ADMINISTER KEY MANAGEMENT CREATE KEY using tag 'KEY5' IDENTIFIED BY welcome1 WITH BACKUP CONTAINER =all;`

- ADMINISTER KEY MANAGEMENT SET KEY using tag 'KEY5' IDENTIFIED BY welcome1 WITH BACKUP CONTAINER=ALL

For example: `SQL>ADMINISTER KEY MANAGEMENT SET KEY using tag 'KEY5' IDENTIFIED BY welcome1 WITH BACKUP CONTAINER=ALL;`

- Check the encryption keys generated.

For example: `SQL> SELECT con_id, key_id FROM v$encryption_keys;`

- Check the wallet status.

For example: `SQL> SELECT * FROM v$encryption_wallet;`

5.2.3 Edit sqlnet.ora file

Perform this step to enter the TDE wallet location.

- Take a backup of sqlnet.ora file before update for TDE.
- Add entries of sqlnet.ora file as follows:

```
ENCRYPTION_WALLET_LOCATION =
(SOURCE =(METHOD = FILE)(METHOD_DATA =
(DIRECTORY = {Keystore location})
```

For example:

```
ENCRYPTION_WALLET_LOCATION =
(SOURCE = (METHOD = FILE) (METHOD_DATA =
(DIRECTORY = /scratch/app/admin/TDE/encryption_keystore/)
```

5.2.4 Run Created Alter Script

- Get TDE_Encryption.sql script from obpencryption/generatedScript/tde.
- Log in to database.
- Run TDE_Encryption.sql.

6 Masking Customer Private Data

This chapter describes the configuration, installation, and policy setup to mask customer private data categories as sensitive or Personally Identifiable Information (PII).

6.1 Configuration

The following is the classification of information related to OBEDM. This information is used to drive TDE configuration.

Table 5–1 TDE Configuration

Classification	Details	Access and Distribution	Action
Public	This information is not sensitive, and there is no value with it remaining confidential to Bank.	No restrictions	No Encryption
Confidential Internal	It is important that this information remains confidential to Bank.	May be accessed by and distributed to all support persons. Distribution to third parties must be authorized by the information owner and requires that an appropriate confidential disclosure agreement is in place.	No Encryption
Confidential Restricted	It is very important that this information remains confidential to Bank and that access within bank is restricted on a need-to-know basis.	Internal access/distribution must be on a business need-to-know basis. Not authorized for information unless the information is encrypted using Oracle-approved encryption.	Need to set encryption rule during masking Tables containing this type of data will be accessed through view for RO user. Synonym needs to be created for the tables and views containing this type of data for RO and ERO user.
Confidential Highly Restricted	It is essential that this information remain confidential to Bank and that access within bank is restricted on a need-to-know basis.	Internal access/distribution must be very limited and is on a stringent business need-to-know basis. Not authorized for information unless the information is encrypted using Oracle-approved encryption.	Need to set encryption rule during masking. Tables containing this type of data will be accessed through view for RO user. Synonym needs to be created for the tables and views containing this type of data for RO and ERO user.

All tables in OBEDM are classified based on above classification and columns of these tables are marked based on sensitivity.

6.2 Installation

This section explains the installation process.

6.2.1 Prepare Scripts to Encrypt Sensitive Data

Database administrator needs to create the following script for masking sensitive data.

- View creation script of the tables containing sensitive data and mask them for RO (Read only) user.
- Synonym creation script of created view of the containing sensitive data for RO (Read only) user.
- Synonym creation script of tables containing sensitive data for ERO (E Read only) user.

The utility tool (obpencryption.sh) is used to create above script. To run the tool, the following prerequisites are required.

Prerequisites

- Create a folder "obpencryption" where user wants to run the tool.
- Upload Sensitive_Data_List.xlsx, obp-encryption-script-gen.jar, obpencryption.sh, DB_RESOURCEBUNDLE.properties. These files are available in maskingencryption.zip. The maskingencryption.zip is part of host.zip available in installer.
- Update database details in DB_RESOURCEBUNDLE.properties file before running the script.
- Update value "encryptLocation" variable with obp encryption path in obpencryption.sh at line 6.

For example: `encryptLocation="/scratch/app/product/obpencryption"`

Run Encryption Tool for View Creation script and mask data

- Create view creation scripts for all the tables containing sensitive data after mask. Run obpencryption.sh with MASK and VIEWCREATE as parameter.

For example: `/obpencryption.sh MASK VIEWCREATE`

Run Encryption Tool for Synonym Creation script for RO user

- Create synonym creation scripts for all the created containing sensitive data. Run obpencryption.sh with MASK and SYNONYMRO as parameter.

For example: `/obpencryption.sh MASK SYNONYMRO`

Run Encryption Tool for Synonym Creation script for ERO user

- Create synonym creation scripts for all the tables containing sensitive data. Run obpencryption.sh with MASK and SYNONYMEERO as parameter.

For example: `/obpencryption.sh MASK SYNONYMEERO`

6.2.2 Create Schema for RO and ERO User

To create schema for RO and ERO user, execute the following steps.

- Create Read-Only (RO) and E Read-Only (ERO) user for accessing masked data from view and table.
- Grant for proper access.

6.2.3 Execute Created Scripts through Encryption Tool

Run all created scripts through the encryption tool for the following task.

- Mask sensitive data for RO user.
- Create view for tables contain sensitive data.
- Create synonym to access the view.
- Create synonym to access the table for ERO user.

To do the above tasks, perform the following steps.

- Get all view creation scripts from obpencryption /generatedScript/masking/viewforRO location and run after logging in to database.
- Get synonym creation script (MaskingSynonymForRO.sql) for RO user from obpencryption/generatedScript/masking/synonymForRO and run after logging in to database.
- Get synonym creation script (MaskingSynonymForERO.sql) for ERO user from obpencryption/generatedScript/masking/ synonymForERO and run after logging in to database.