Oracle® Banking Enterprise Product Manufacturing

Administrator Guide

Release 2.7.0.0.0

F11754-01

November 2018

ORACLE®

Oracle Banking Enterprise Product Manufacturing Administrator Guide, Release 2.7.0.0.0

F11754-01

Contents

List of Figures

List of Tables

Preface

This guide describes how to administer the Oracle Banking Enterprise Product Manufacturing application environment, including user administration, batch execution, application monitoring, and bank and branch setup.

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

This preface contains the following topics:

Audience

This guide is intended for the administrators of Oracle Banking Enterprise Product Manufacturing.

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 Users Administration

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

Chapter 2 Approvals Management

This chapter describes approvals configuration and worklist authorization related activities to be performed as an administrator.

Chapter 3 Data Management

This chapter describes data related activities to be performed as an administrator.

Chapter 4 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 5 Application Monitoring Using Administration Application

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

Chapter 6 Application Monitoring Using EM Plugin

This chapter provides an overview on the various monitoring operations performed as an administrator, using Enterprise Manger (EM) Plugin.

Chapter 7 Batch Shells in OBEPM

This chapter describes the batch shells used in OBEPM and their execution sequence.

Chapter 8 Configure ODI for Inbound Document Upload

This chapter provides the steps to configure ODI for uploading inbound documents.

Chapter 9 Additional Recommendations

This chapter provides specific recommendations to be considered for implementation.

Related Documents

For more information, see the following documentation:

- For installation and configuration information, see the Oracle Banking Enterprise Product Manufacturing Installation Guide - Silent Installation.
- For a comprehensive overview of security, see the Oracle Banking Enterprise Product Manufacturing 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 Product Manufacturing Licensing Guide.
- For information related to customization and extension, see the Oracle Banking Enterprise Product Manufacturing Extensibility Guide for Host, SOA, and UI.
- For information on the functionality and features, see the Oracle Banking Enterprise Product Manufacturing 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.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1 Users Administration

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

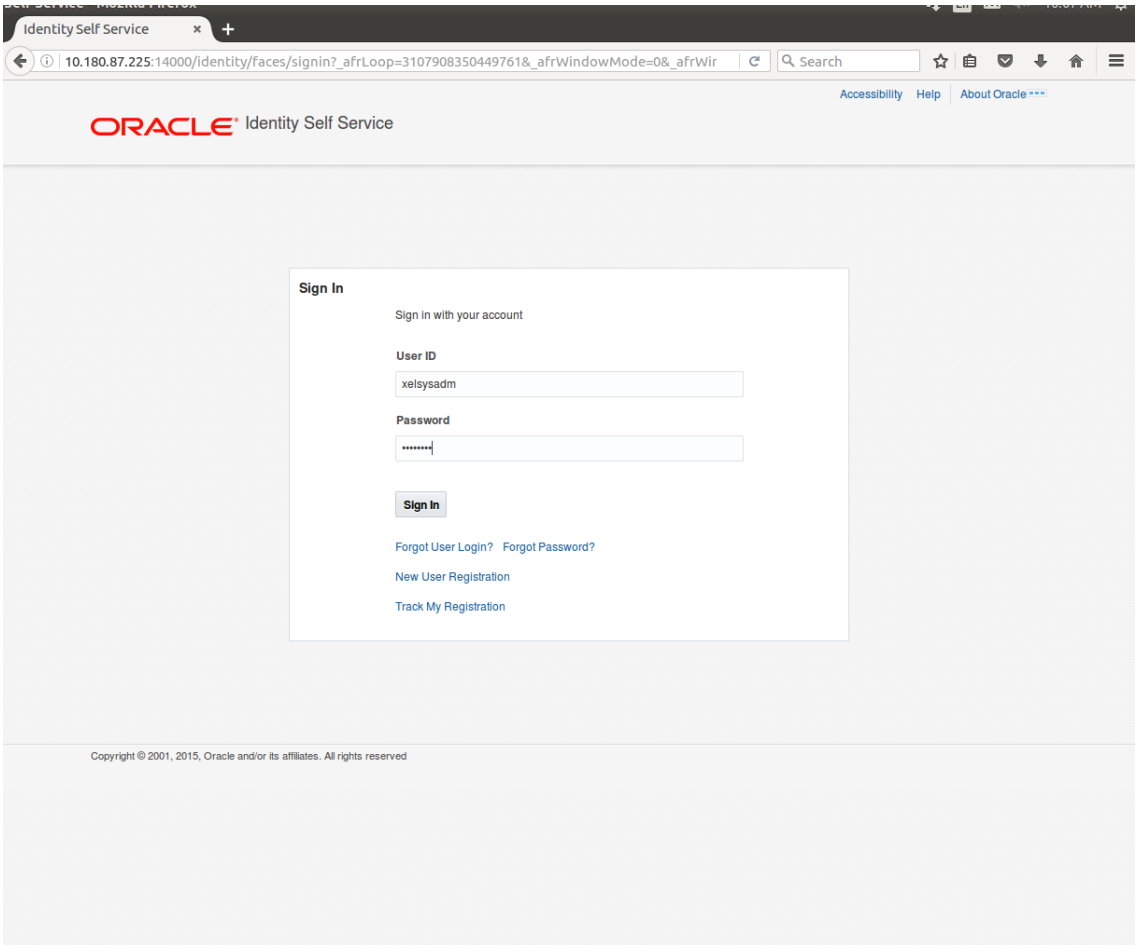
1.1 Creating Users in Oracle Identity Manager (OIM)

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

To create users in OIM:

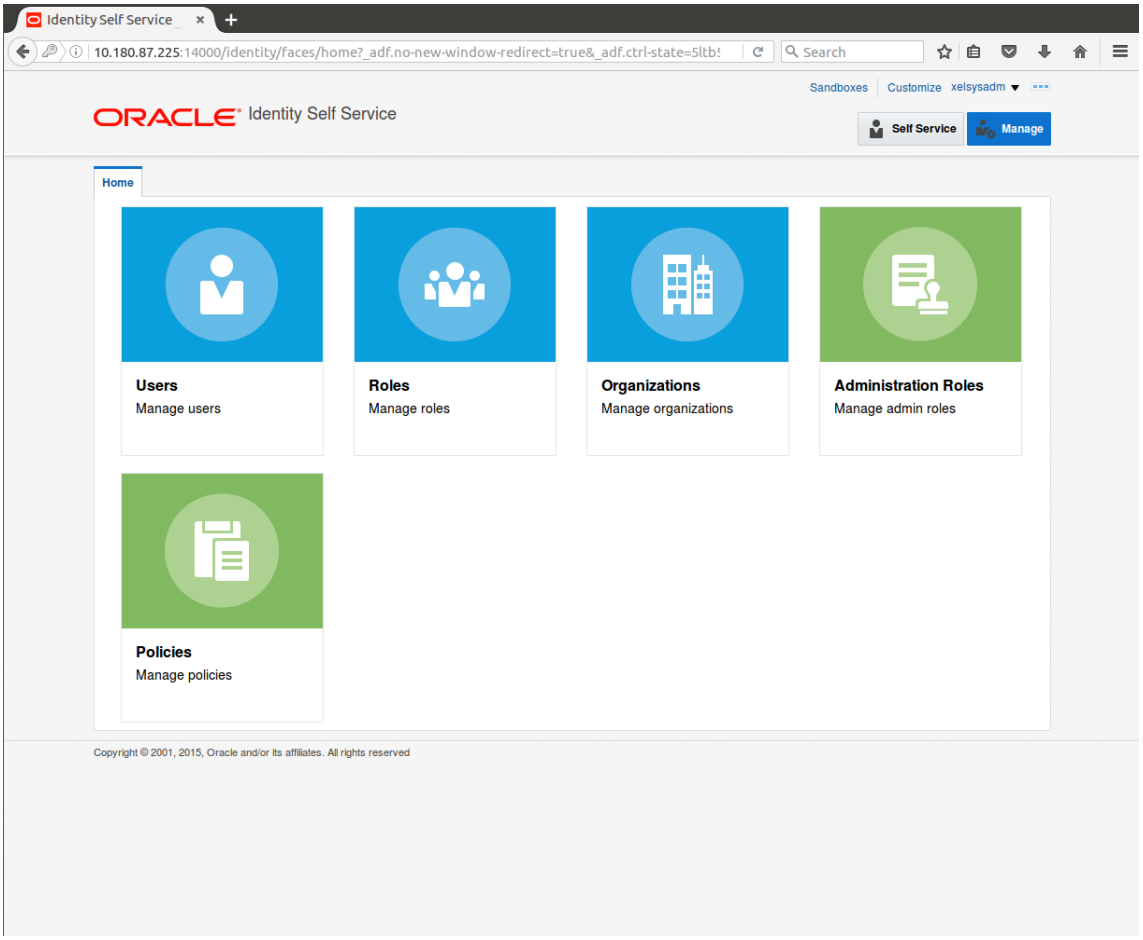
1. Log in to OIM with the User ID as **xelsysadm** and the relevant <Password>.

Figure 1–1 Creating Users in OIM - Log in



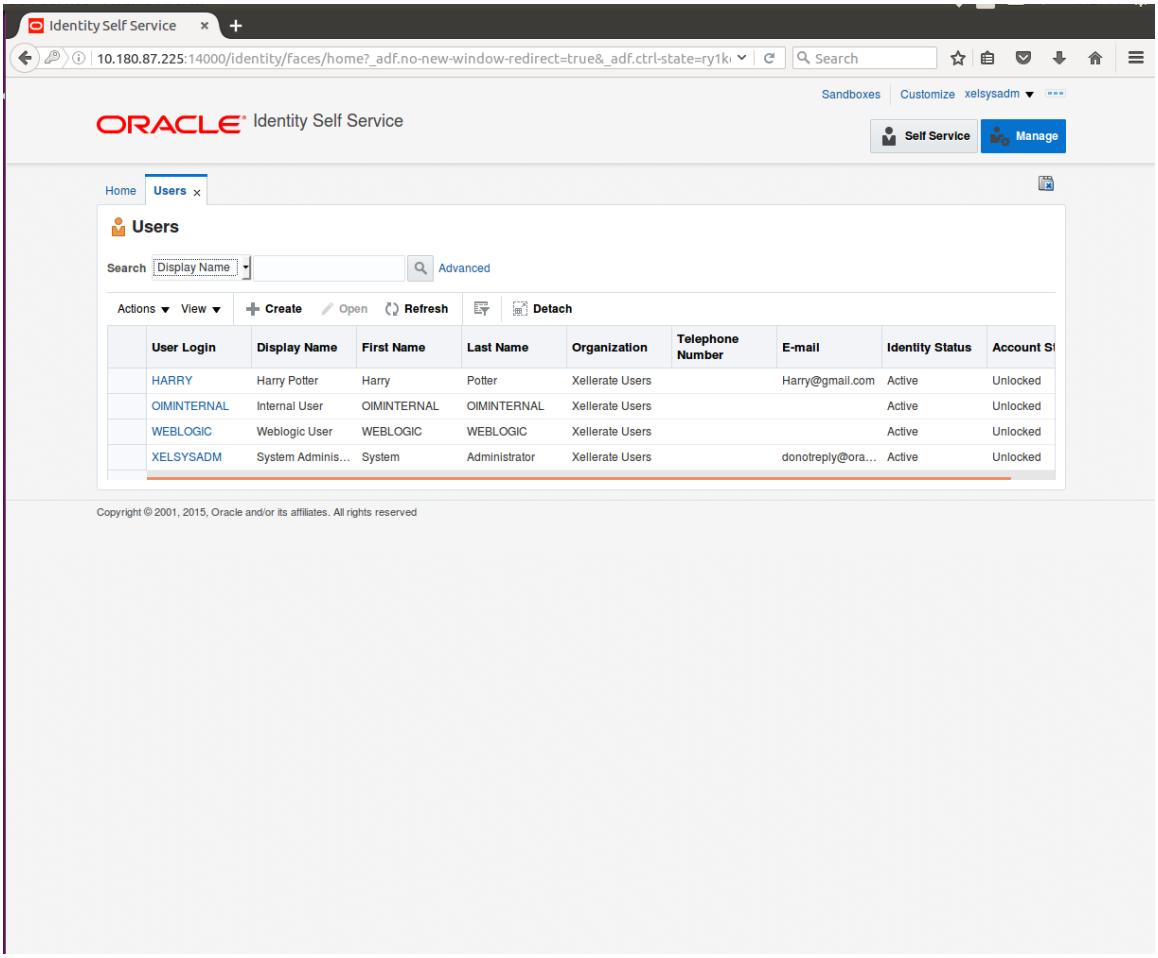
2. Click **Users** under the Manage section.

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



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

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

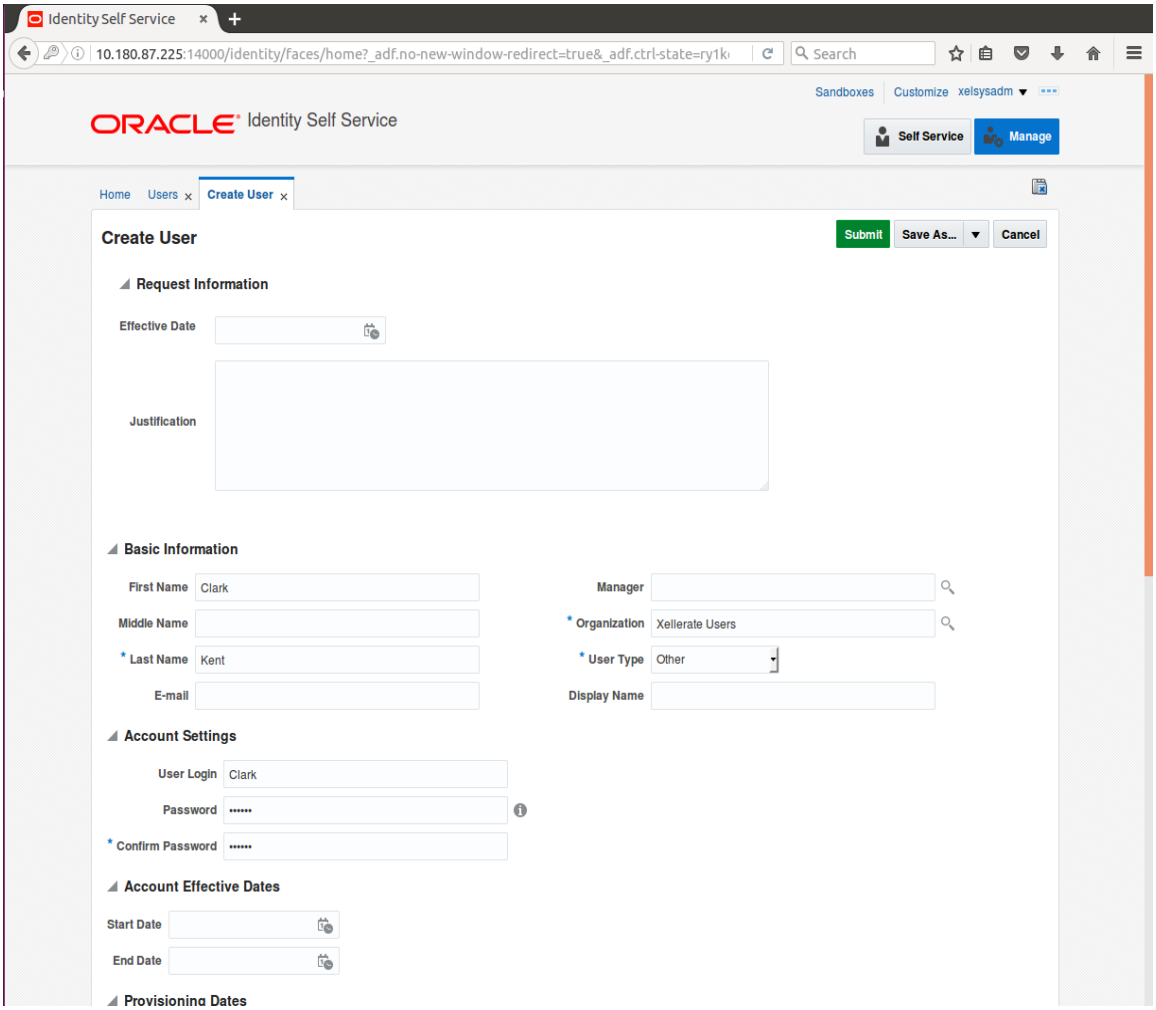
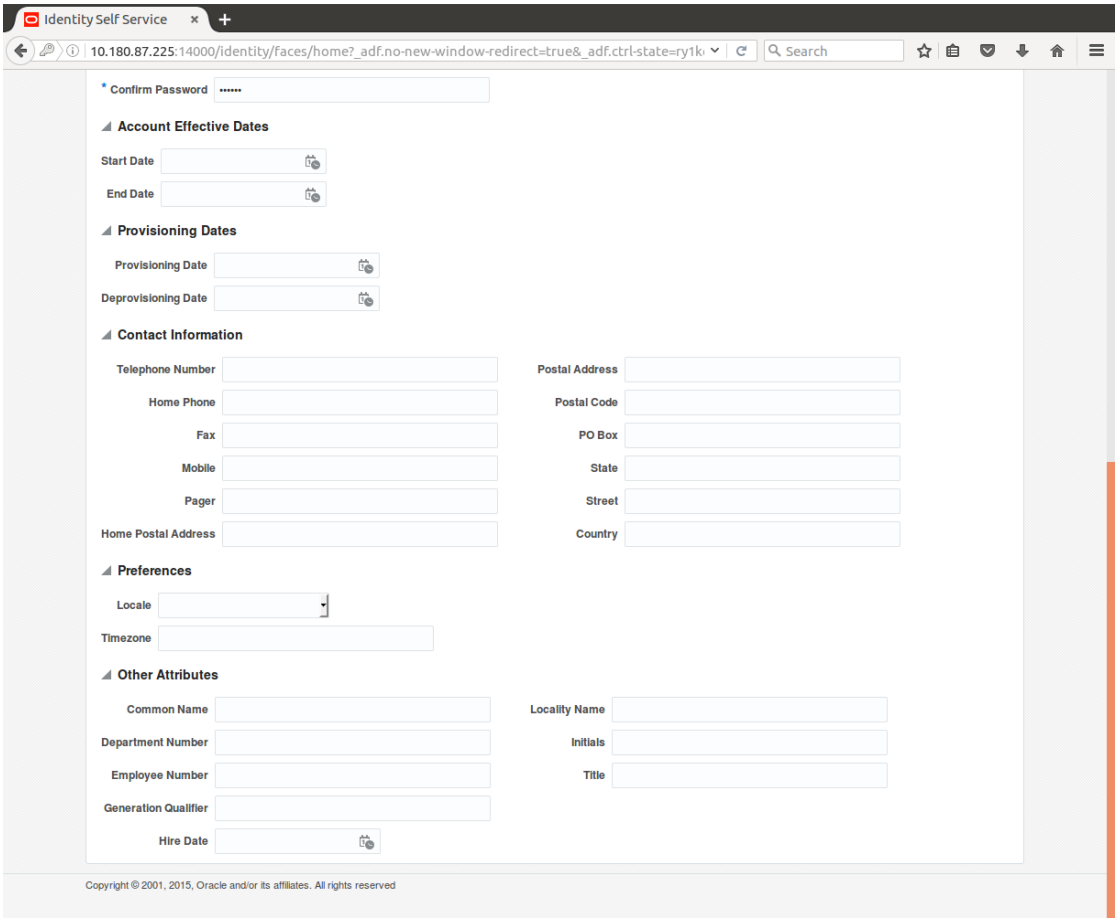


Figure 1–5 Enter User Details (Continued)



6. Click **Submit.**

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

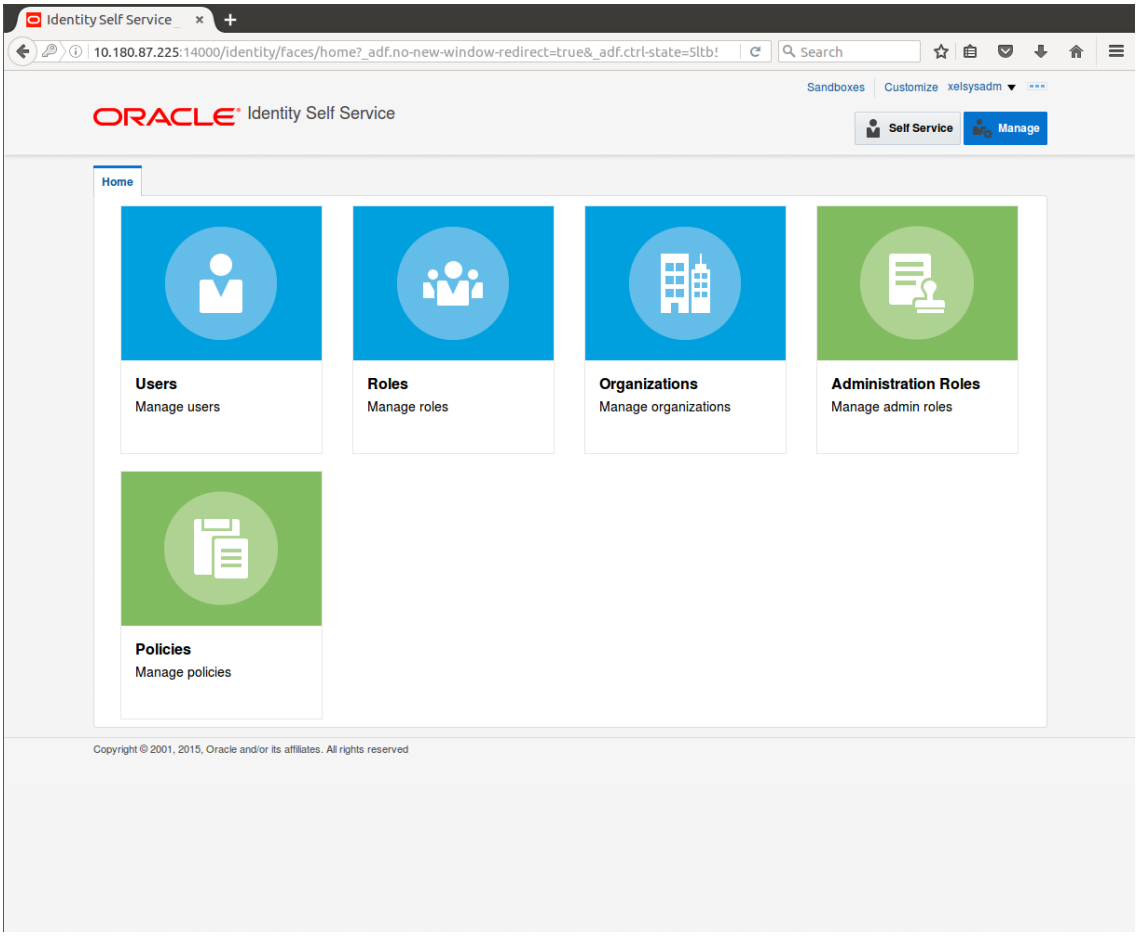
1.2 Creating Roles in Oracle Identity Manager (OIM)

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

To create roles in OIM:

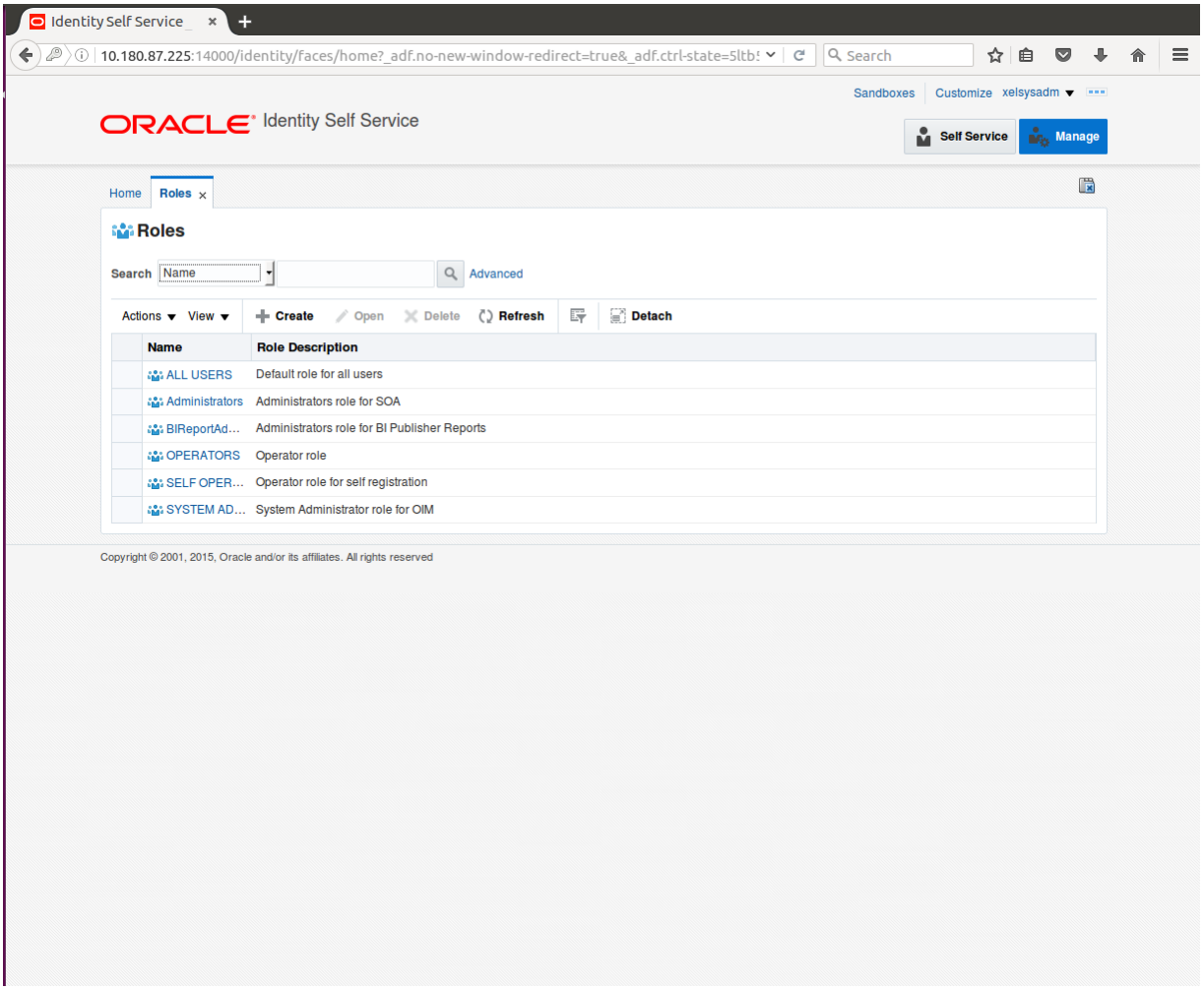
1. Click **Roles** under the Manage section.

Figure 1–6 Creating Roles in OIM - Manage Section



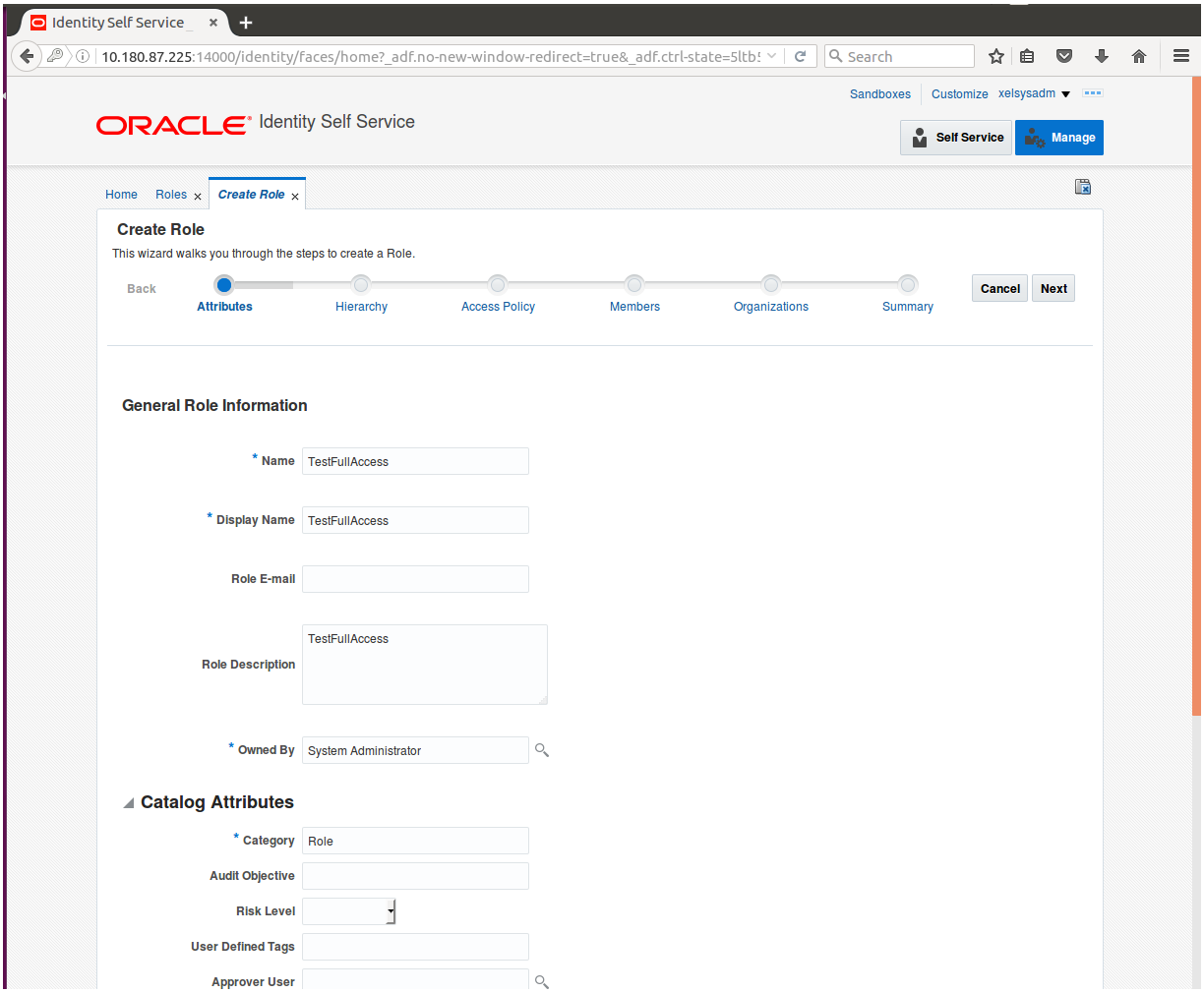
2. In the **Search Roles** page, search for existing roles. The Search Results appear.
3. Click **Create** in the Search Results section to create a new Role.

Figure 1–7 Creating Roles in OIM - Click Create



4. Fill the role details.

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

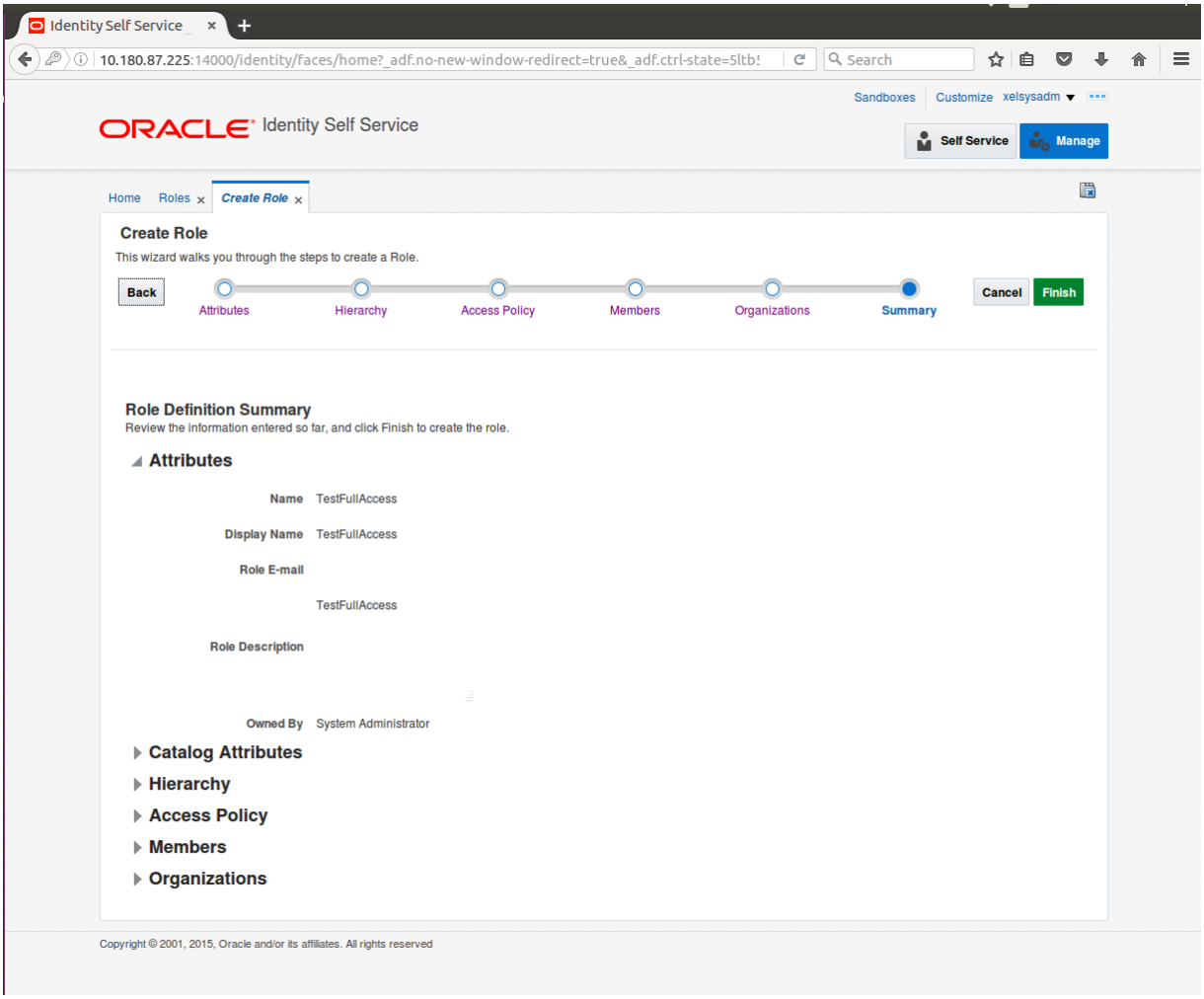


5. Click **Finish.** The role is created successfully.

   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



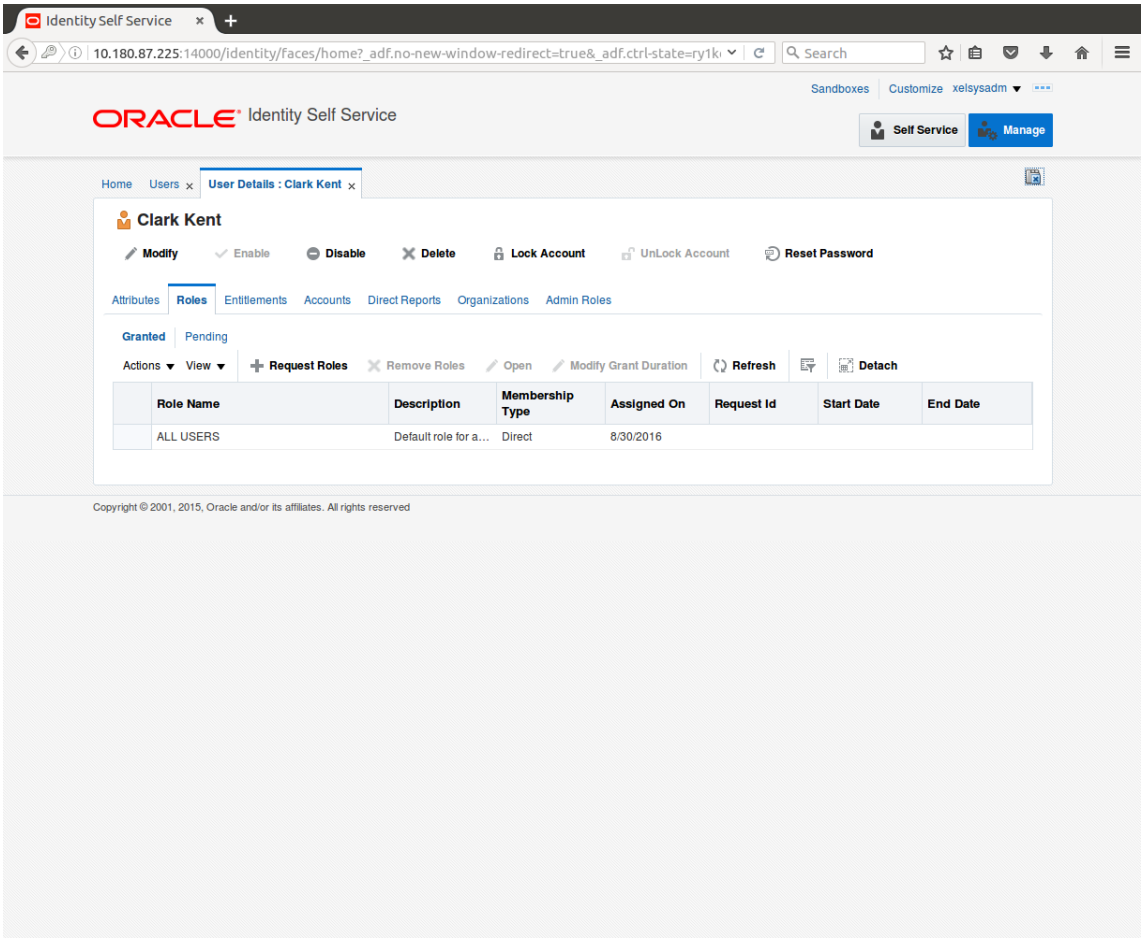
1.3 Assigning Roles to Users in OIM

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

To assign a role to a user:

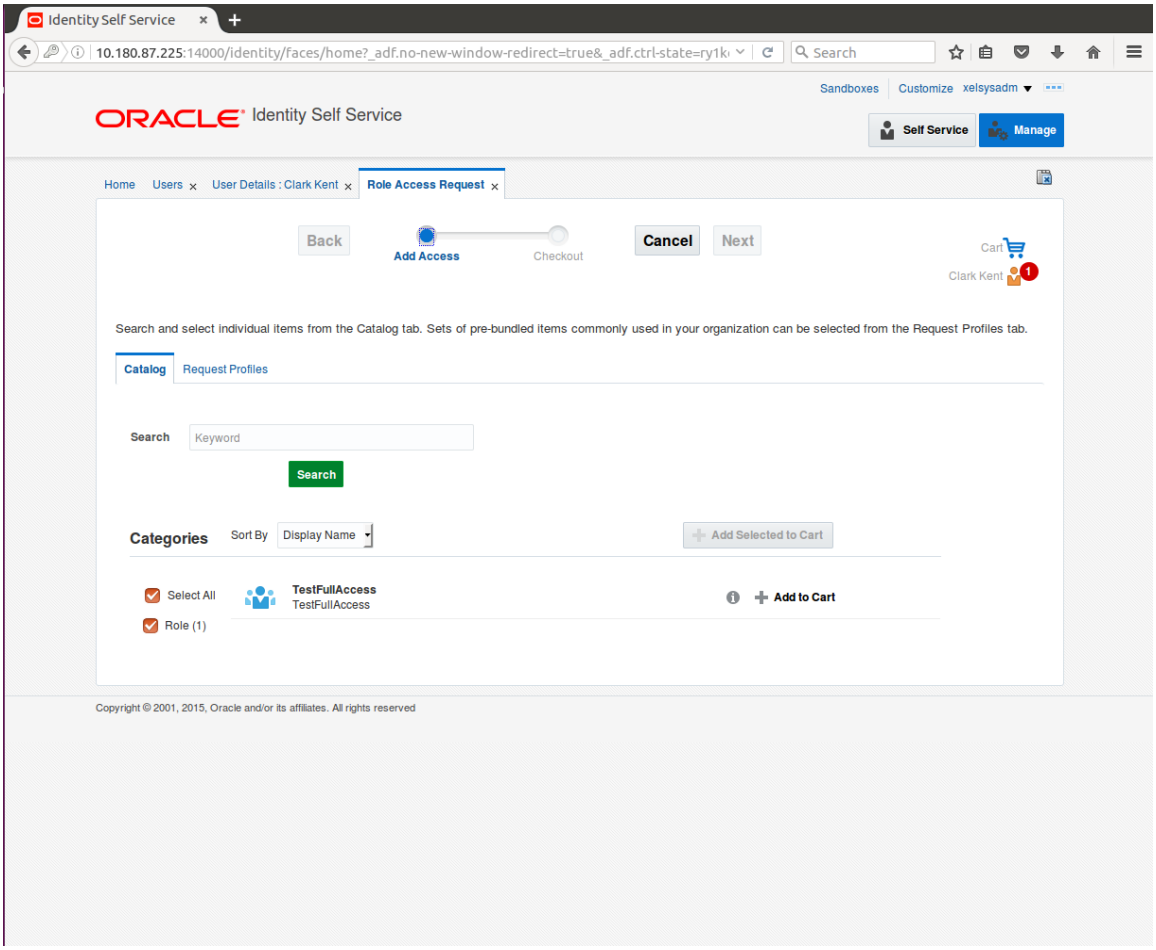
1. Log in to OIM.
2. Navigate to the **Roles Tab** under the User.
3. Click **Request Roles.**

Figure 1–10 Assigning Roles in OIM - Requesting Roles



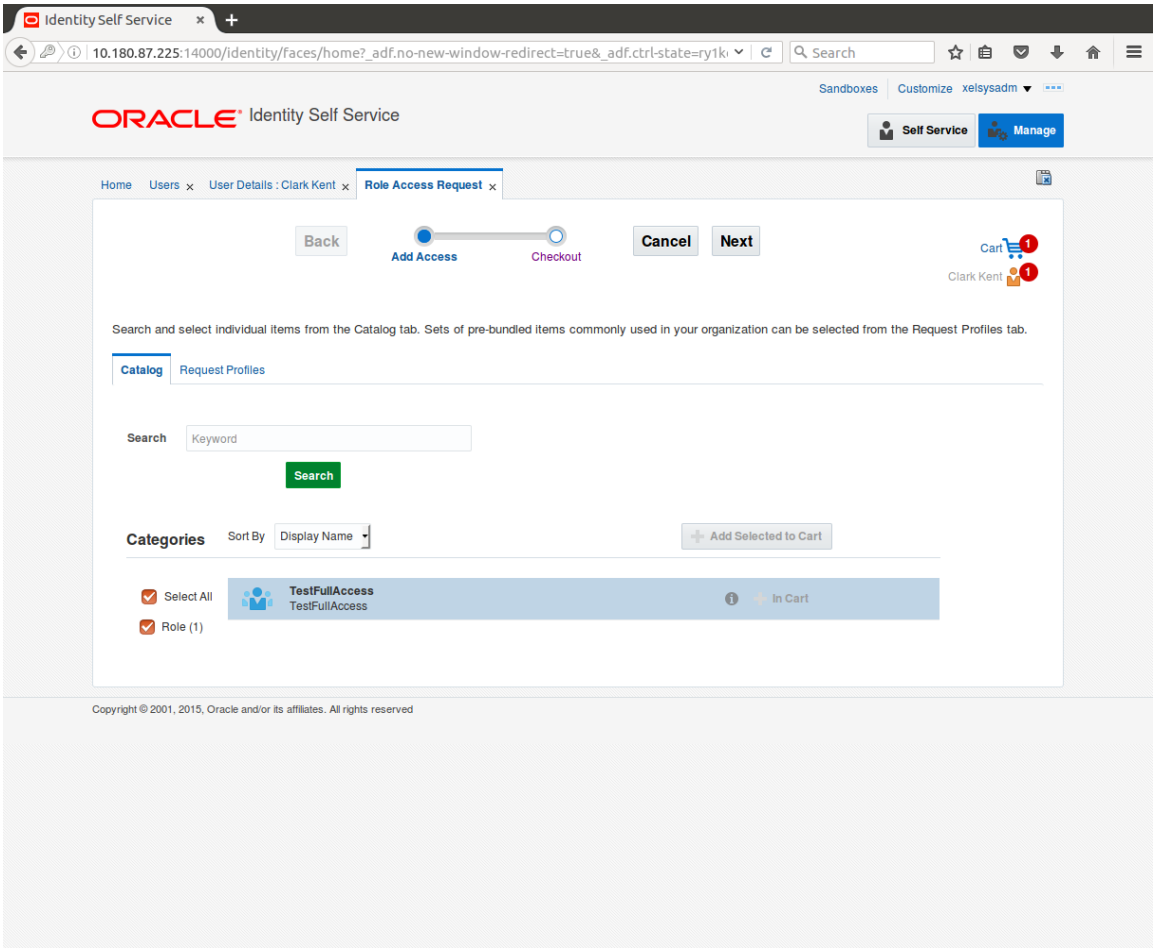
4. In the **Catalog** page, select the required role and click **Add to Cart.** The item gets added to the cart.

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



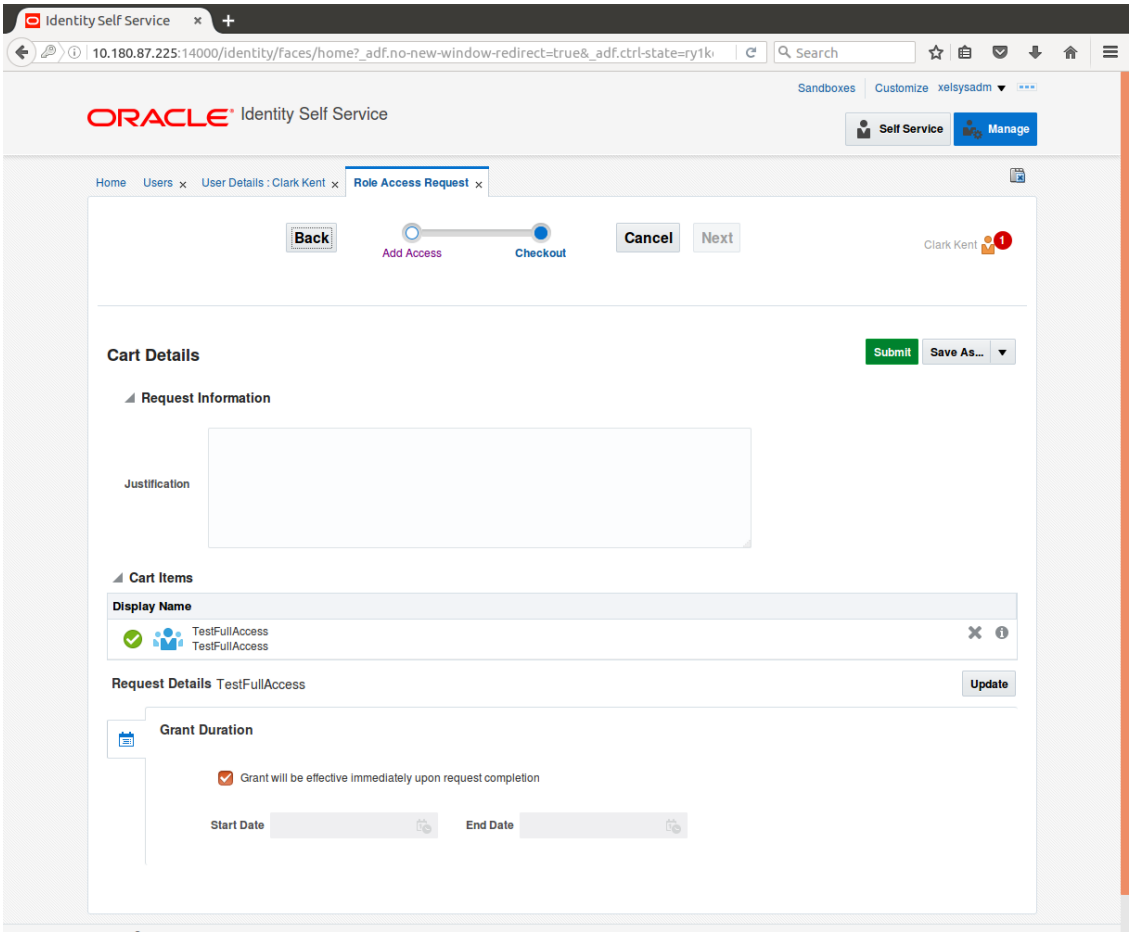
5. Click **Checkout.**

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

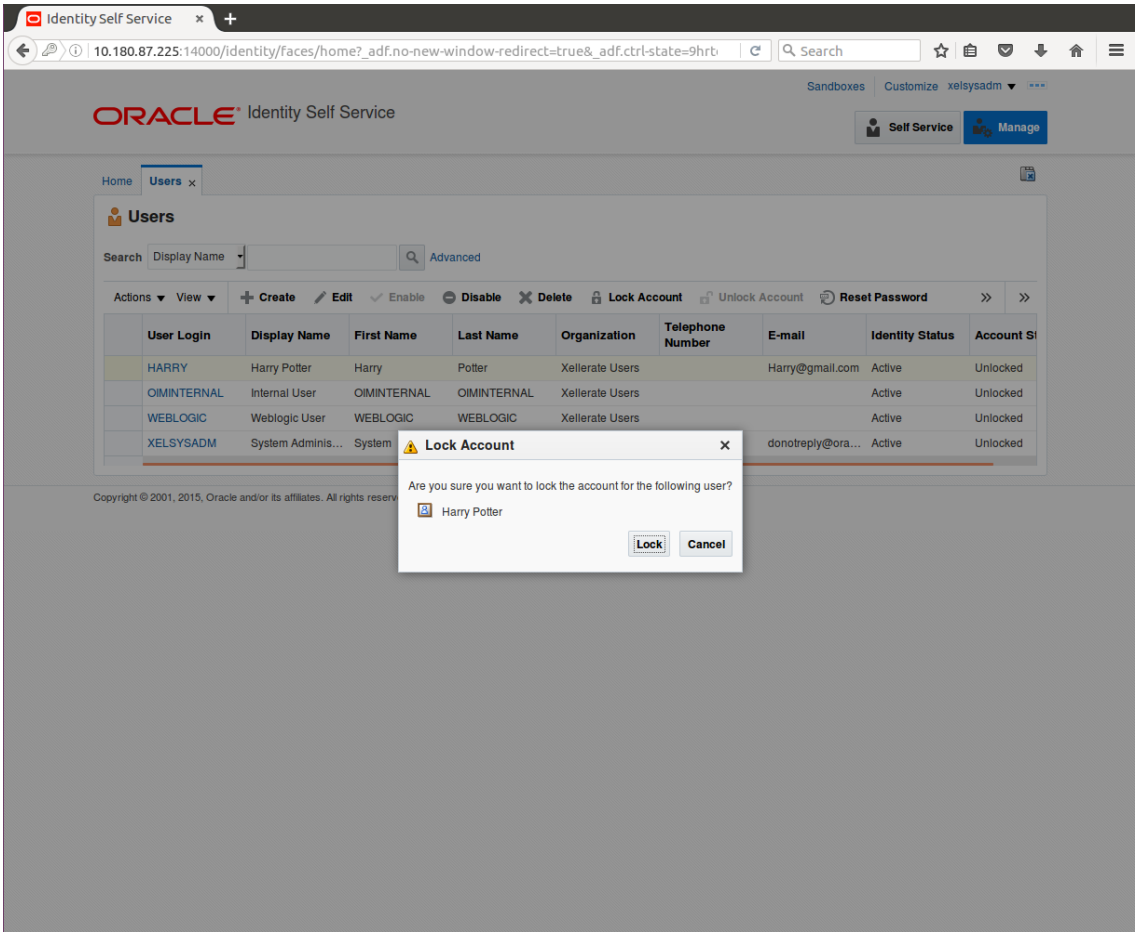
This section explains how to lock the user in OIM.

To lock a user:

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

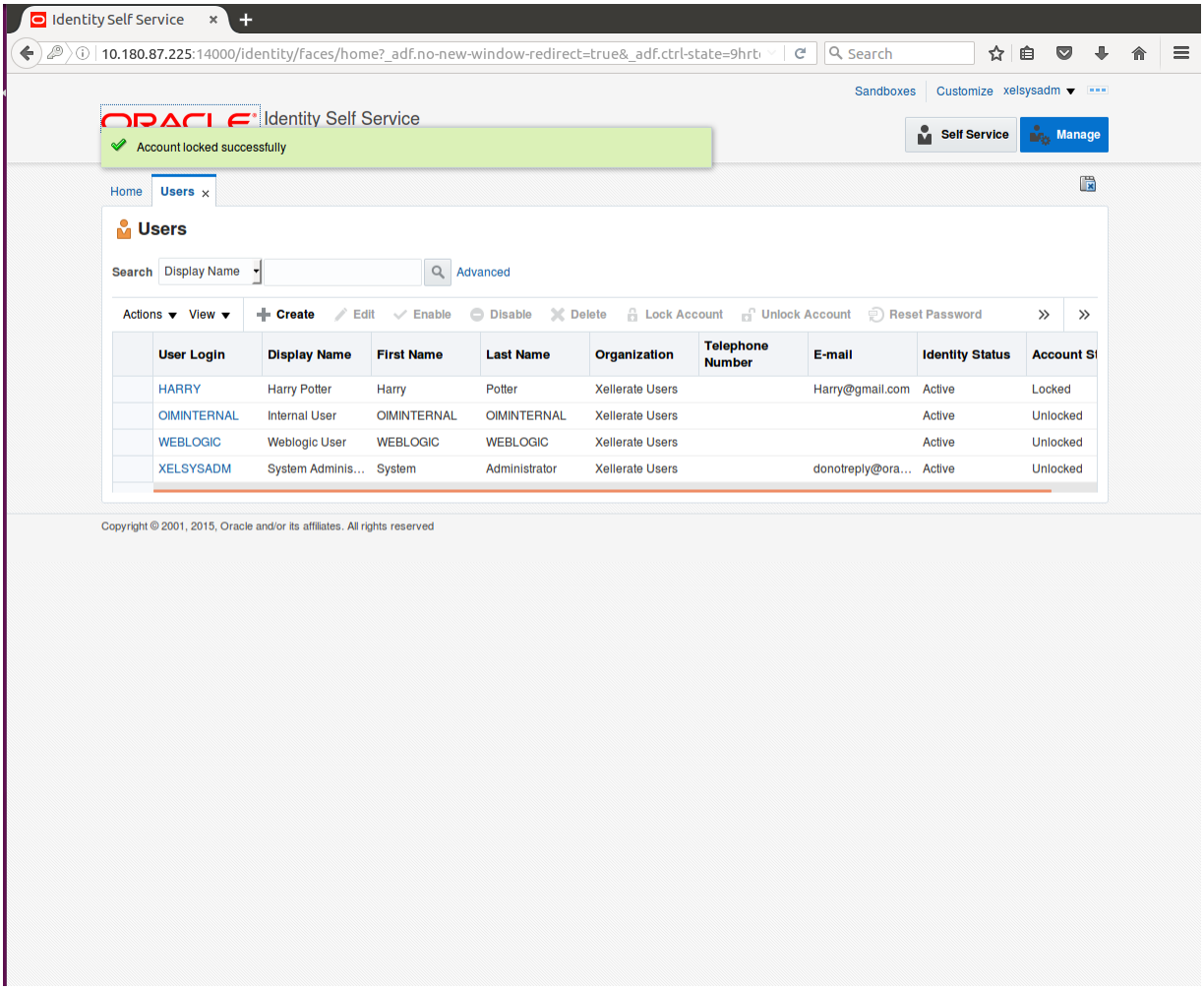
   A message appears, Are you sure you want to lock the account for the following user?
3. Click **Lock.**

Figure 1–14 Locking Users in OIM



The user is locked successfully.

Figure 1–15 User Locked Successfully



1.5 Unlocking Users in OIM

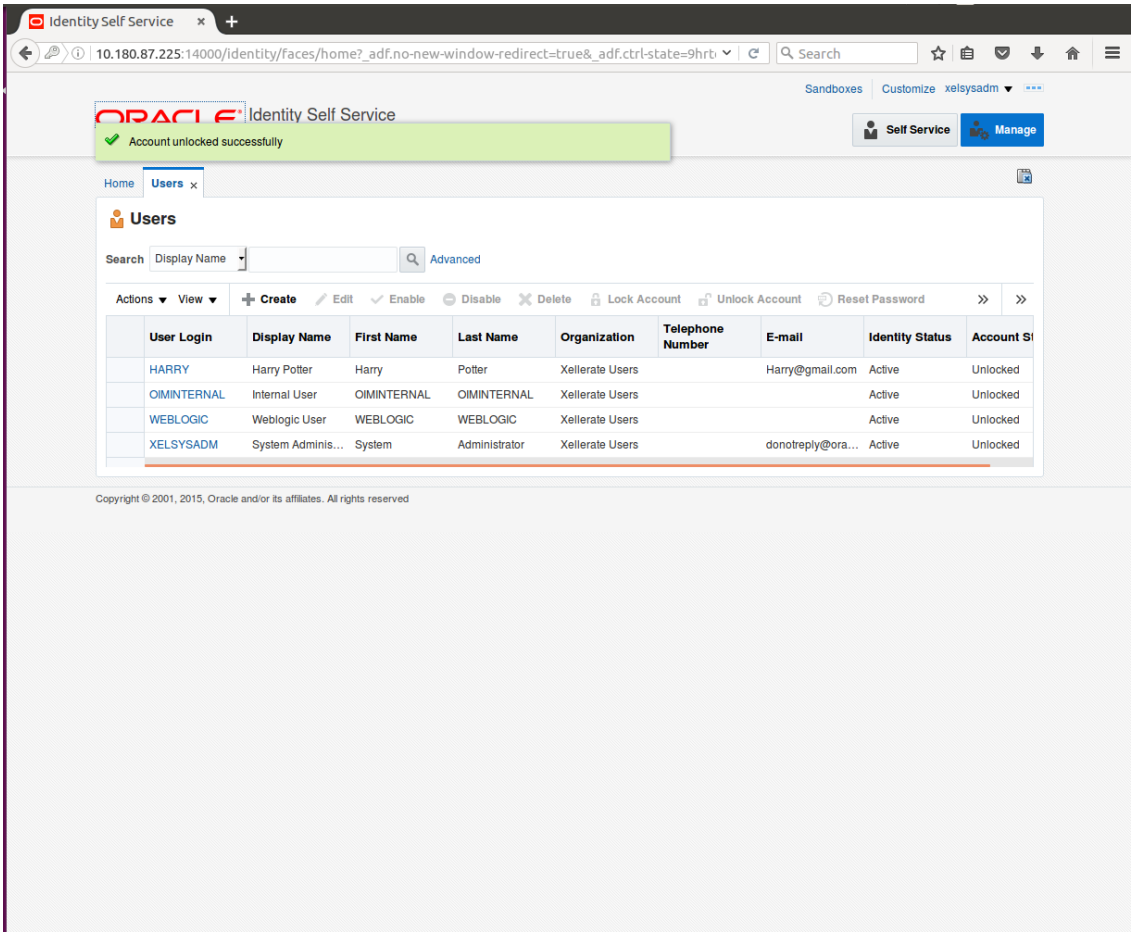
This section explains how to unlock the user in OIM.

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



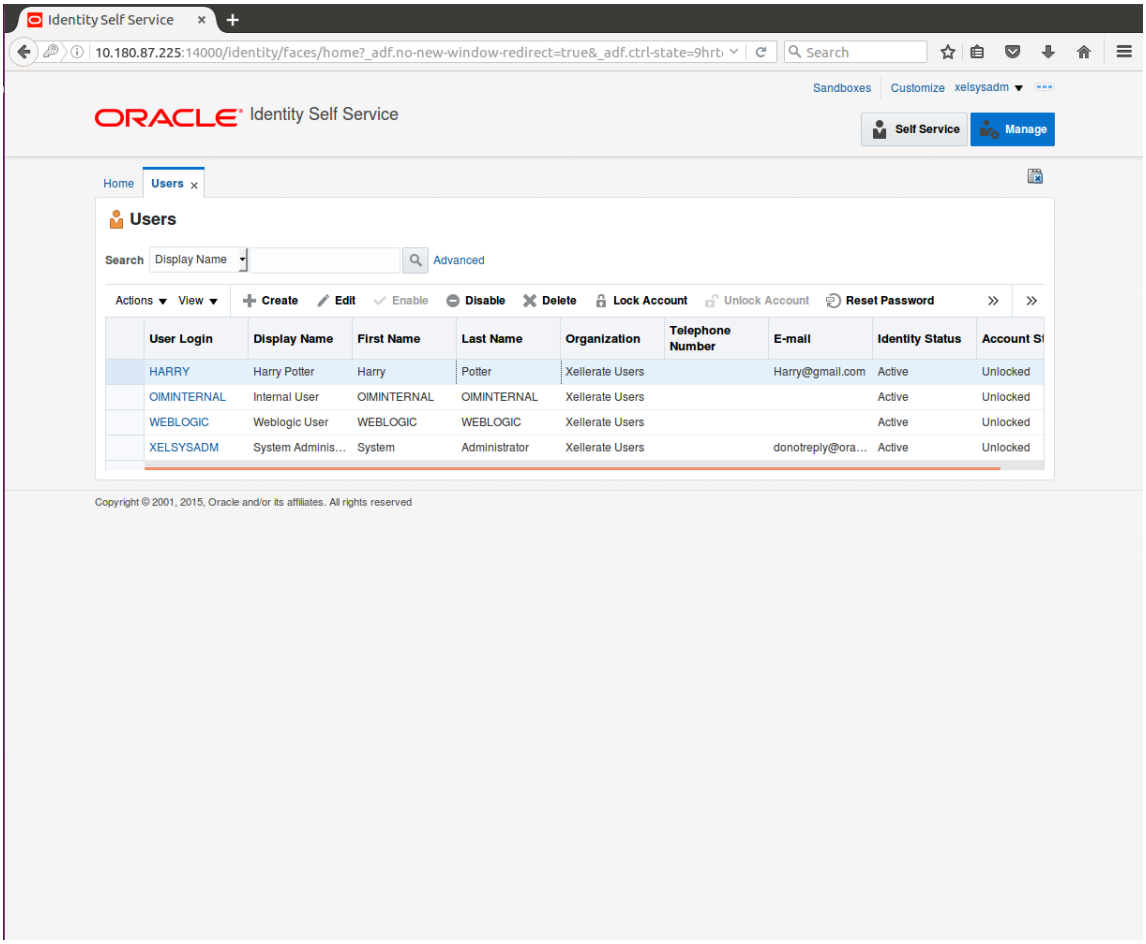
The user is unlocked successfully.

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.

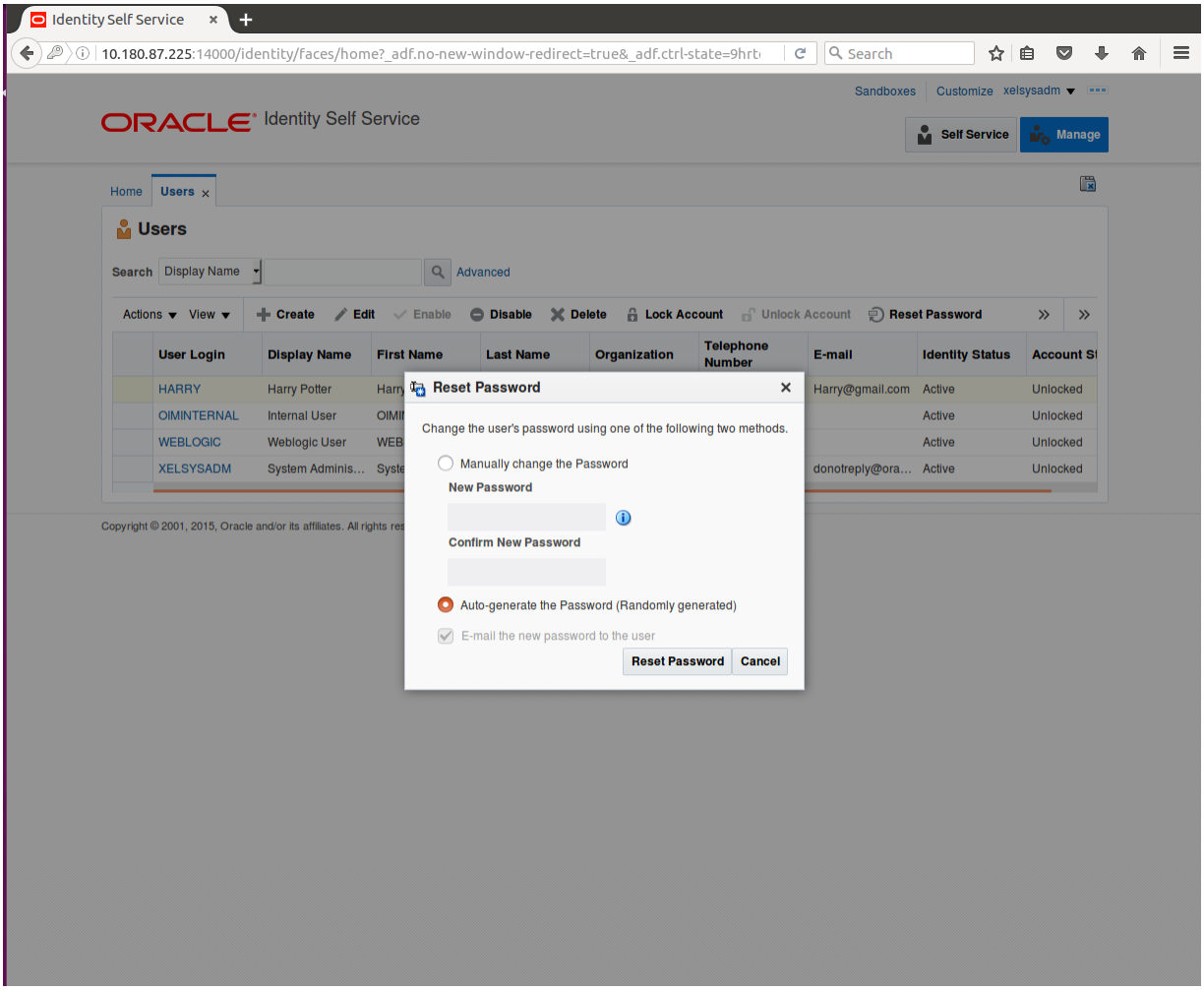
Figure 1–17 Resetting User Password in OIM



The **Reset Password** dialog box appears.

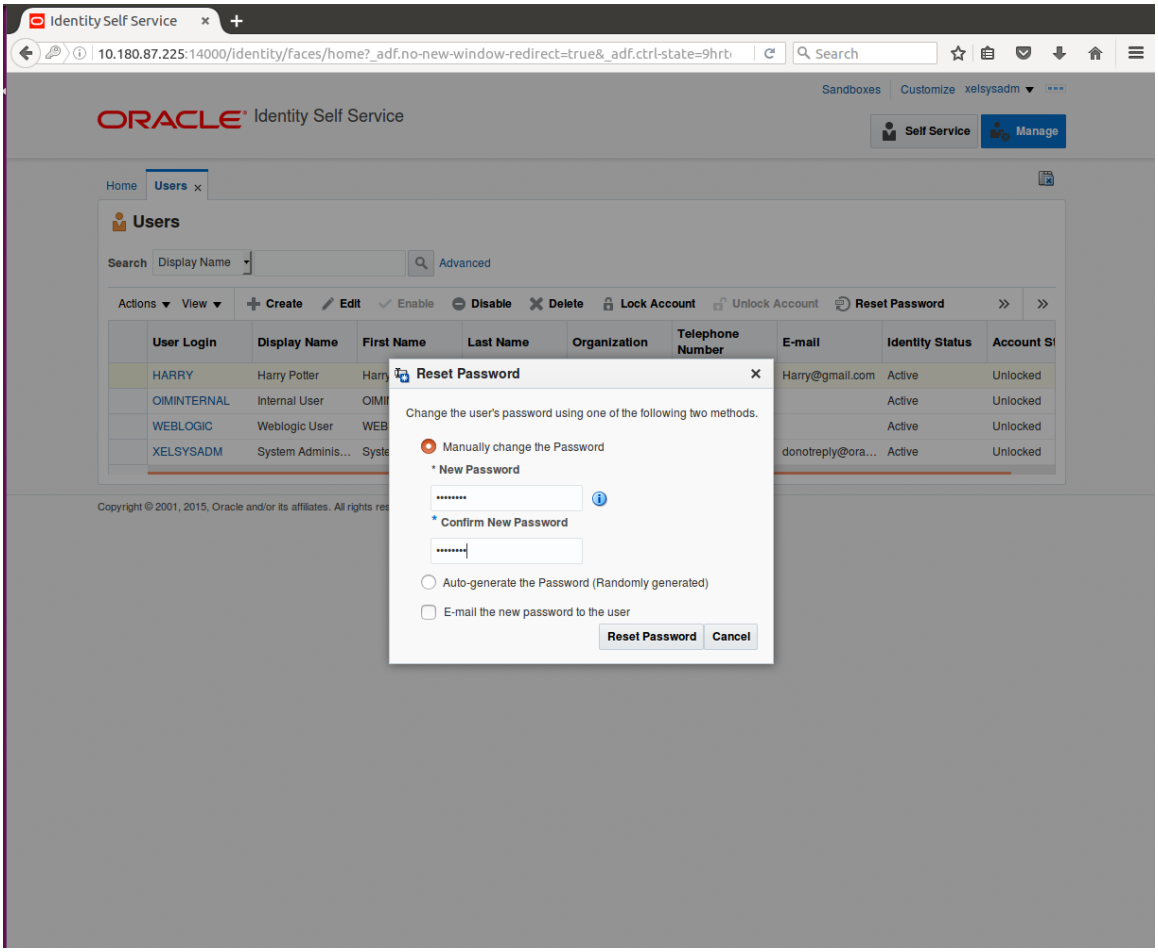
You can select either **Manually change the Password** option to change the password manually or select the **Auto-generate the password (Randomly generated)** option to enable auto generation of the password.

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



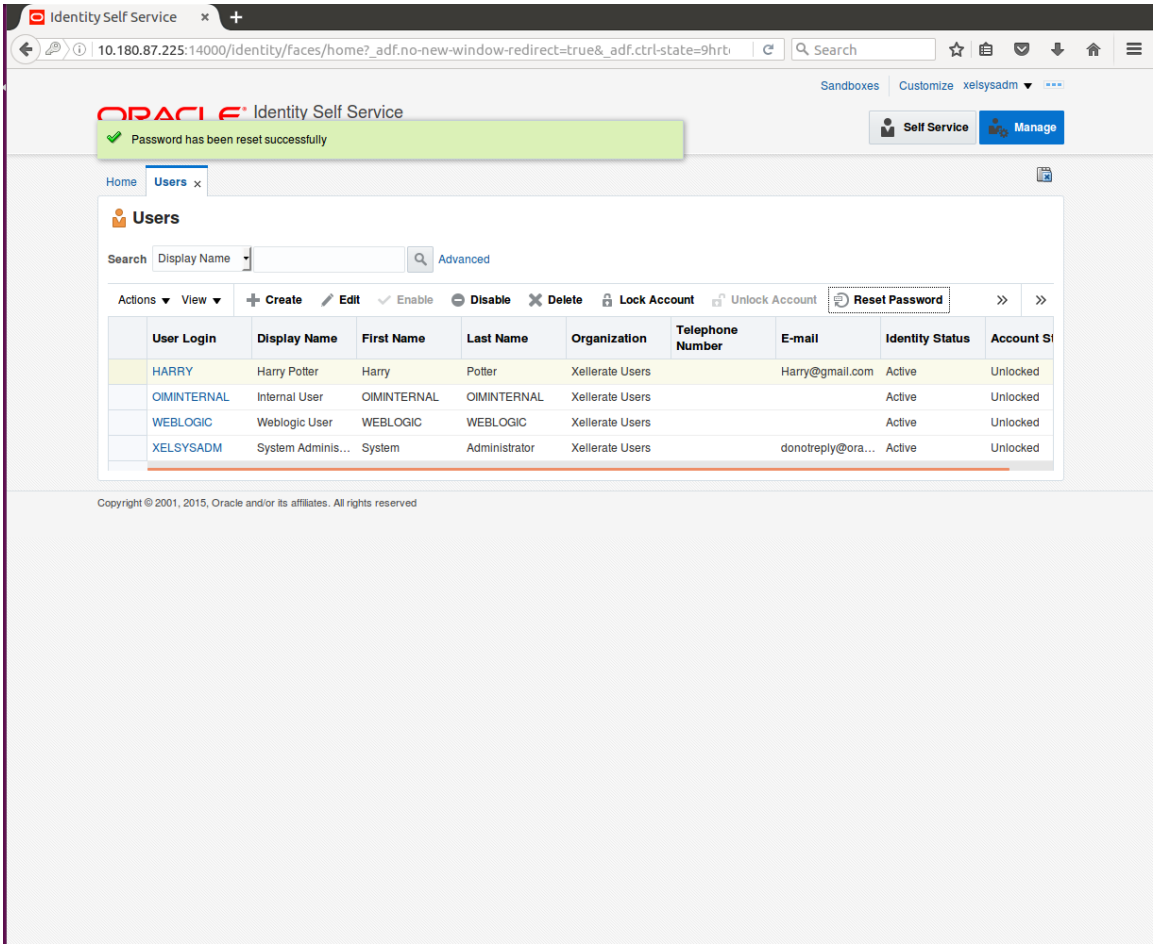
3. If you select the **Manually change the Password** option, enter the new password in the **New Password** and the **Confirm New Password** fields.

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

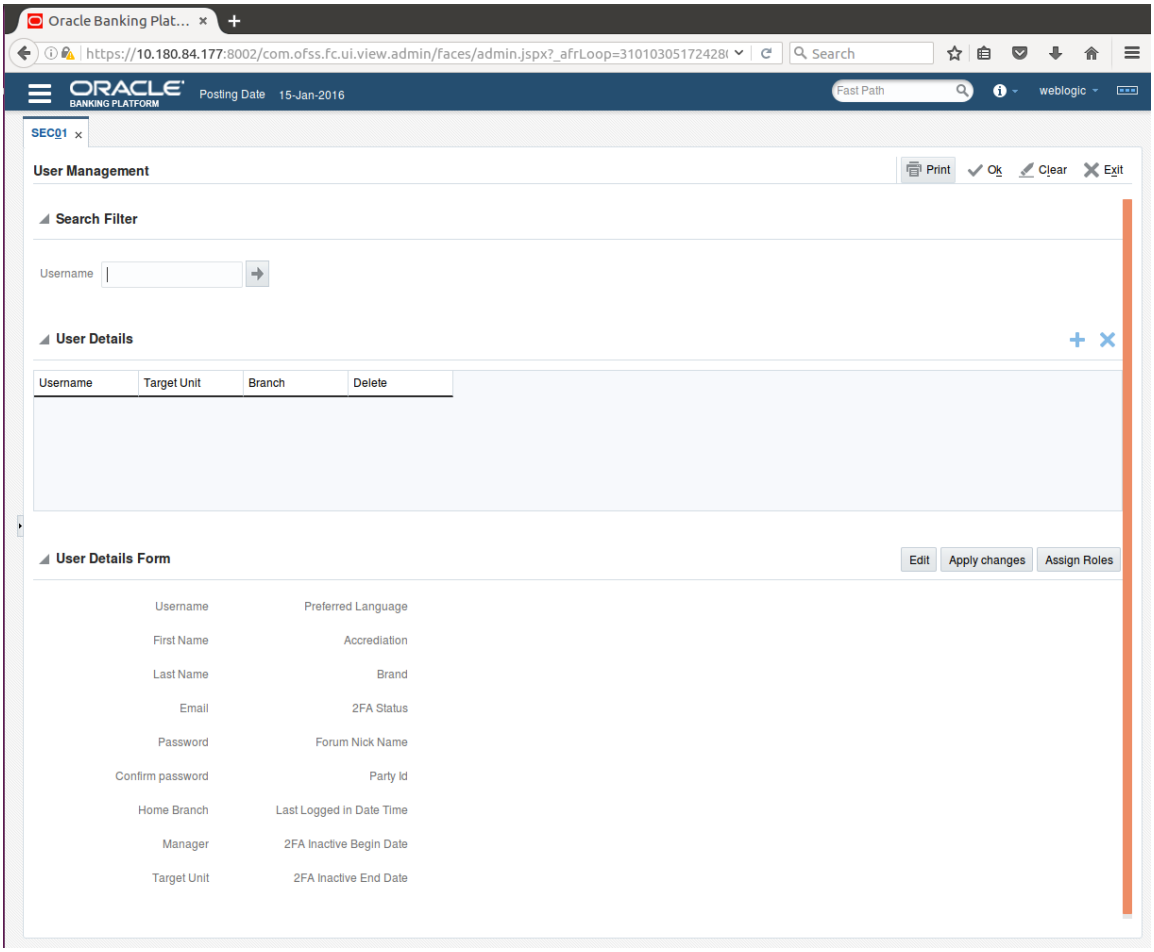
The User Management screen is a quick start UI, provided to create initial users and verify the OBEPM installation.

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:

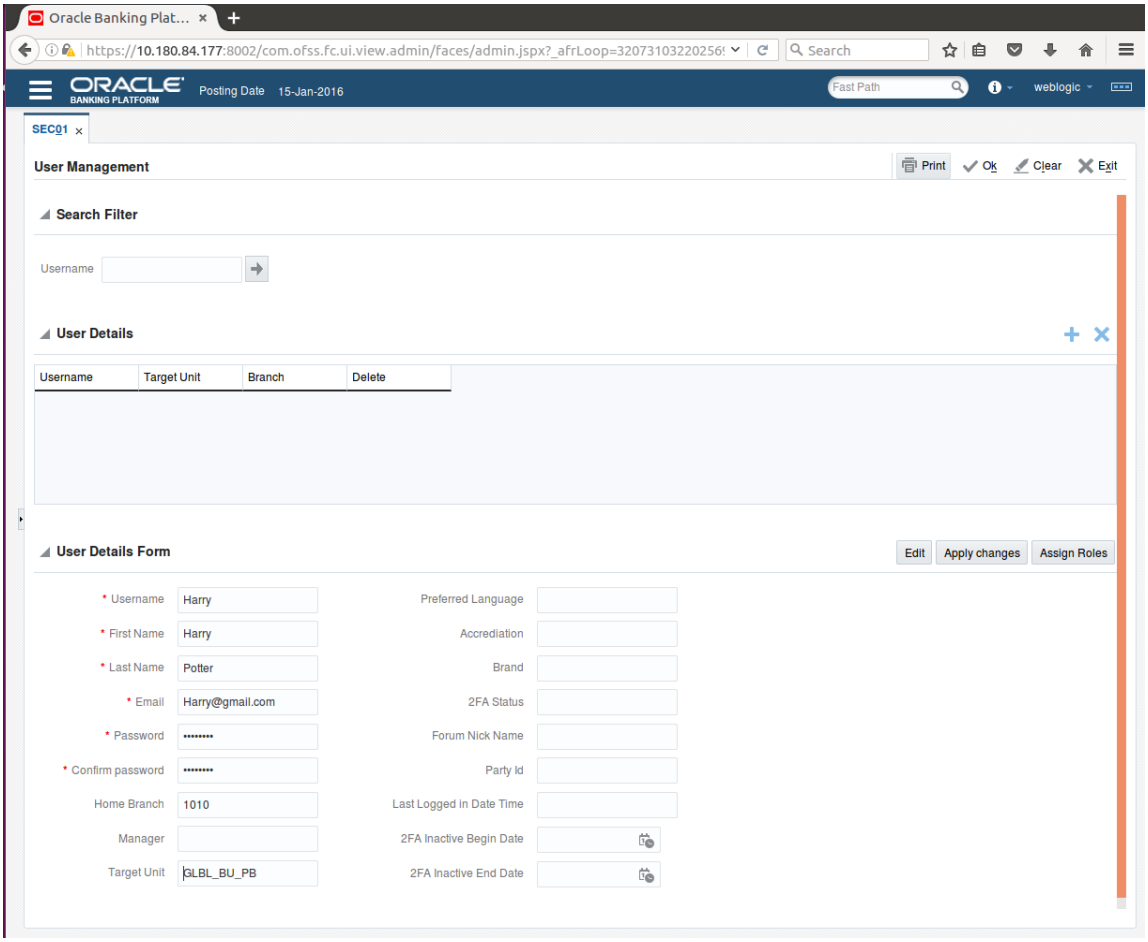
1. Click **Security** tab in **View Admin**.
2. Select **User Management**.
3. Click **+** icon to add a user.

Figure 1–21 Adding a User



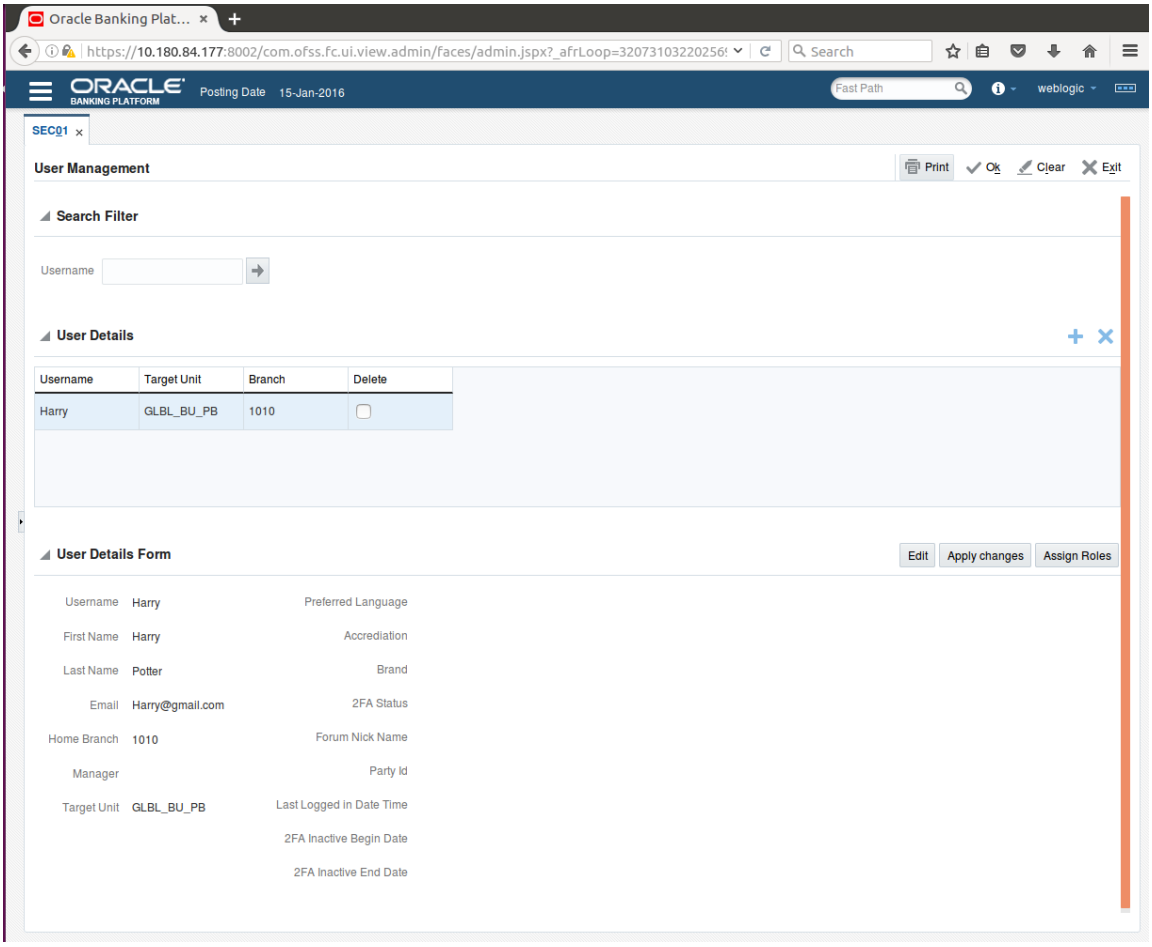
4. Enter the mandatory fields required for creating a user.

Figure 1–22 Enter Mandatory Details



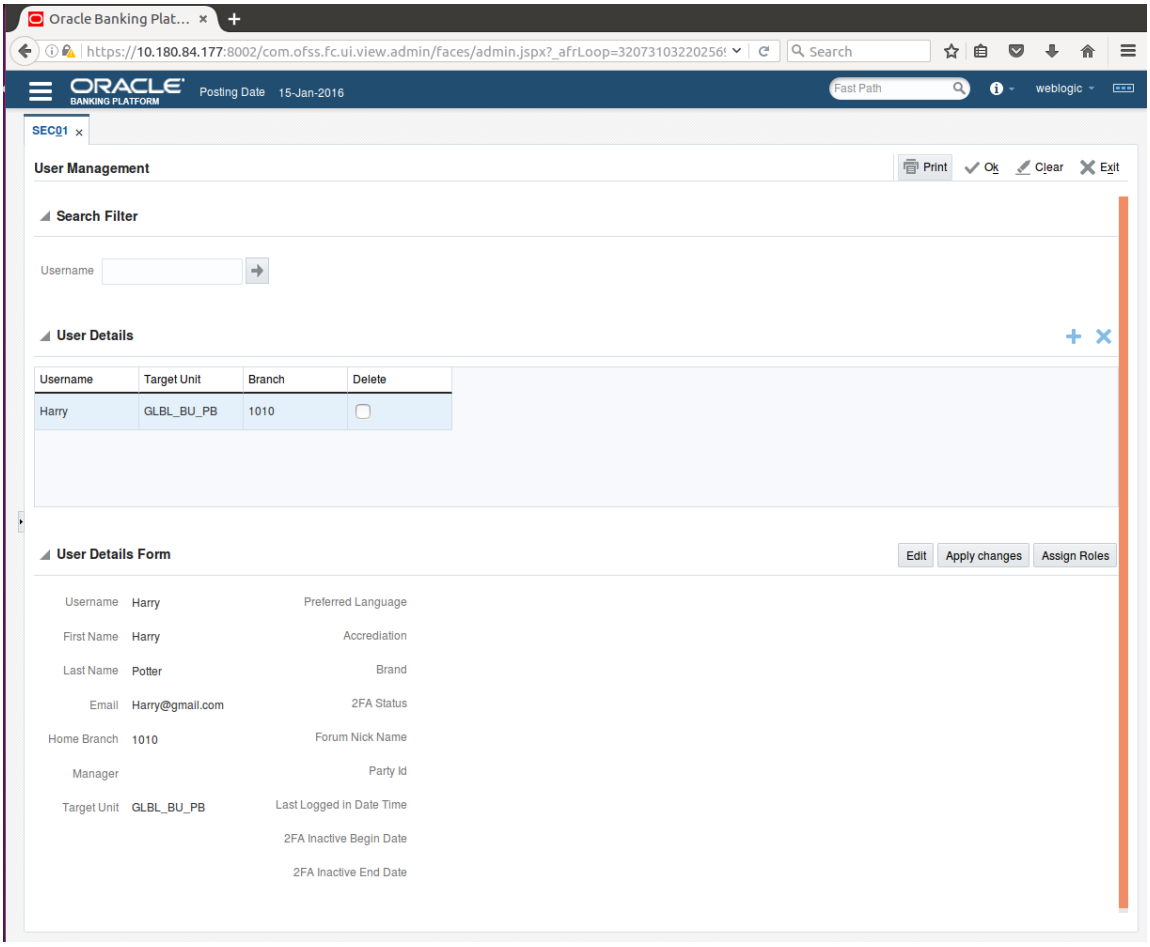
5. Click **Apply Changes** to save the user details locally.

Figure 1–23 Applying Changes



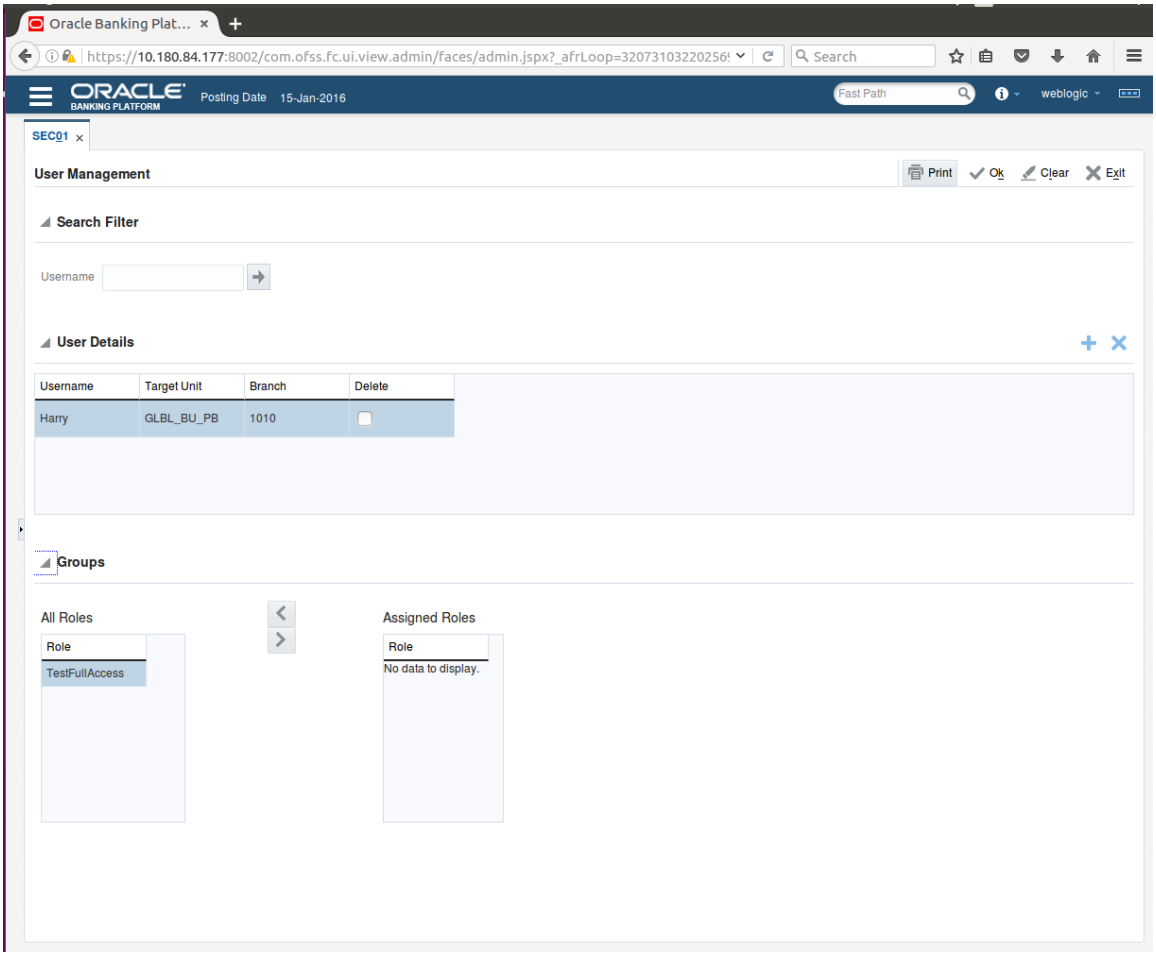
6. To add a user to a group, select the row containing the user and click **Assign Roles**.

Figure 1–24 Adding User to a Group



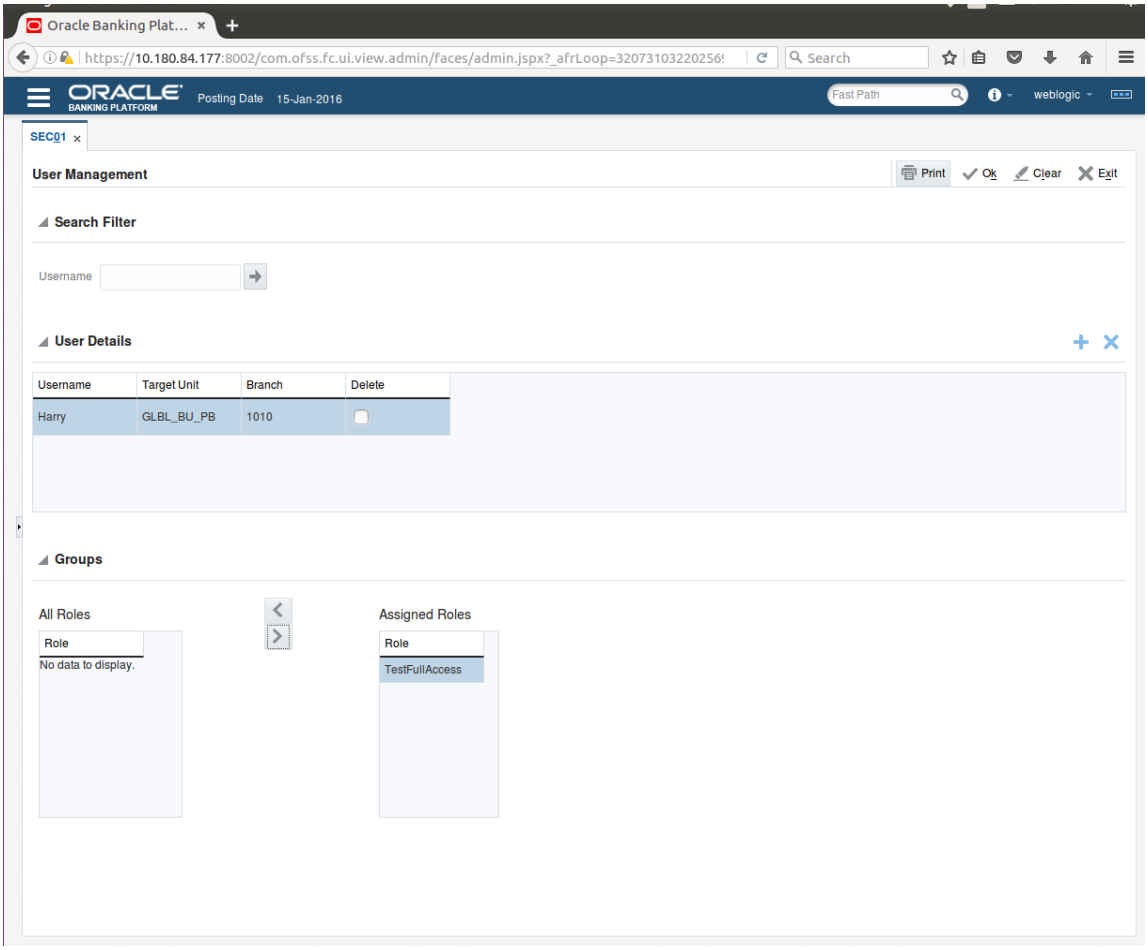
The available and assigned roles appear.

Figure 1–25 Available and Assigned Roles



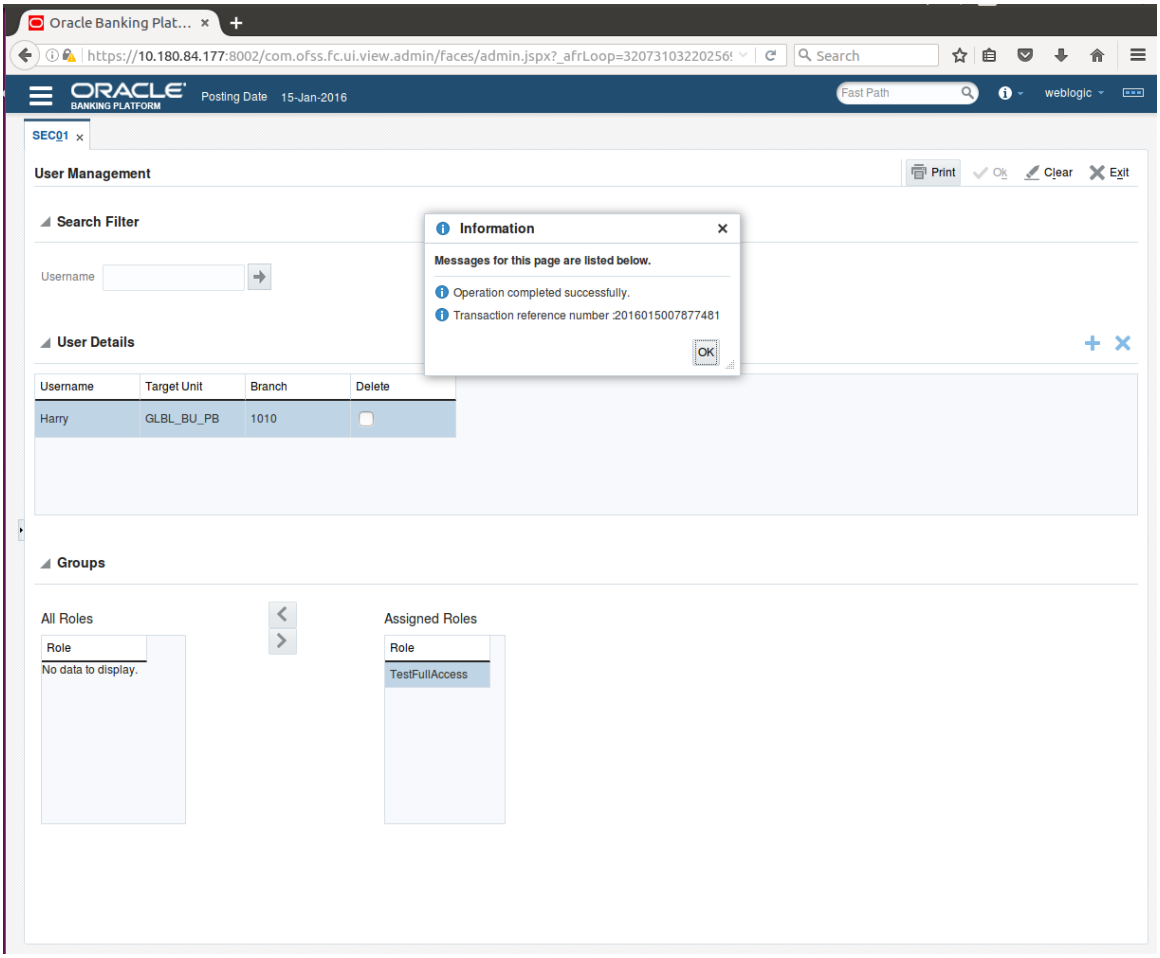
7. Select the group to add user and move it to the **Assigned Roles** table.

Figure 1–26 Adding User to Assigned Roles Table



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

Figure 1–27 Save Changes



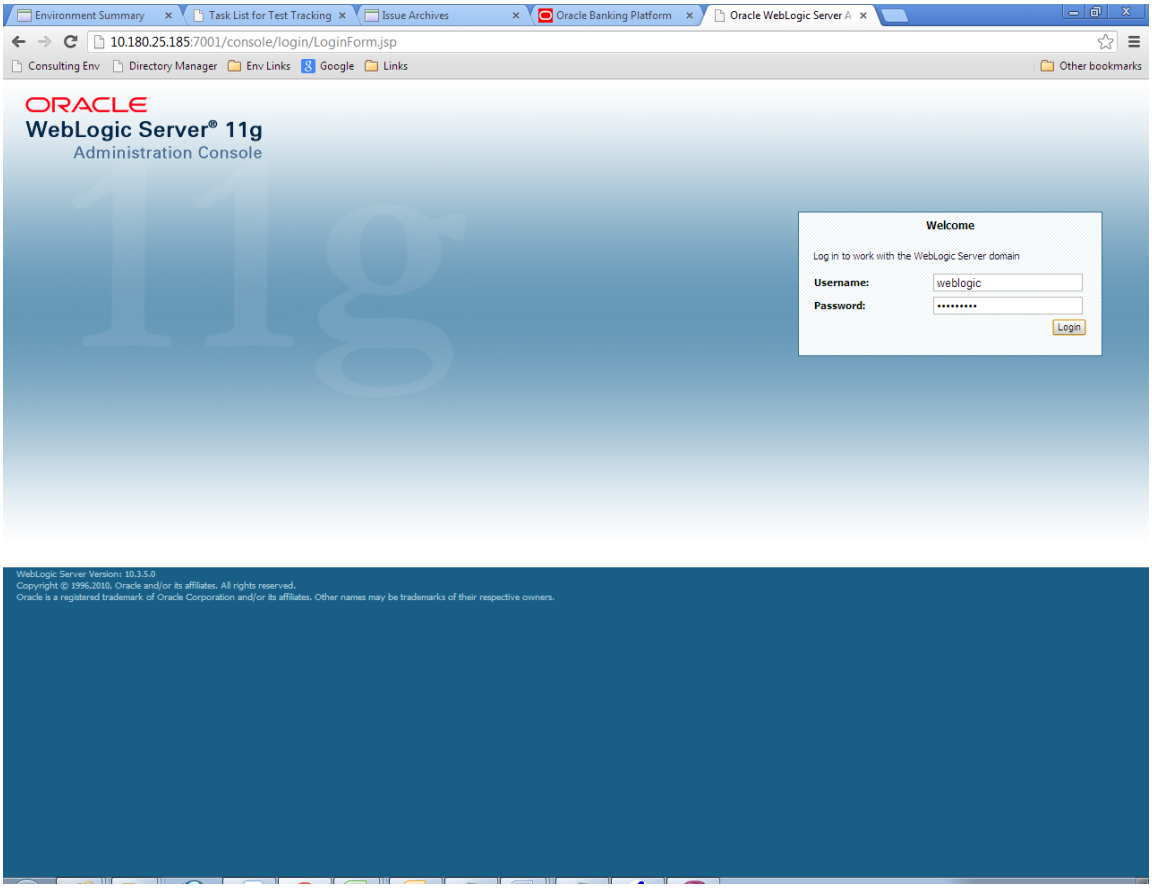
1.8 Unlocking Users in Oracle WebLogic Server (OWS) Administration Console

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:

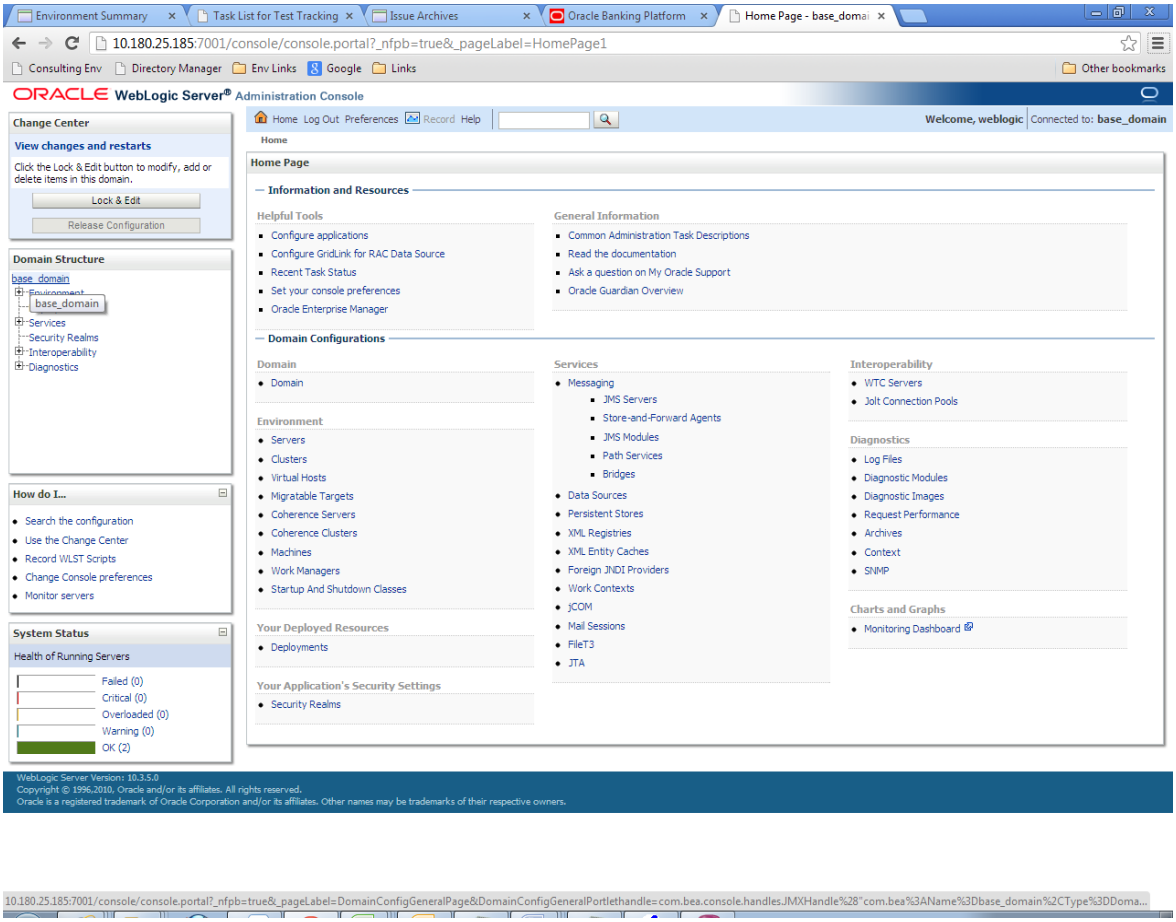
1. Log in to OWS. The **Home Page** of OWS Administration Console appears.

Figure 1–28 OWS Log in



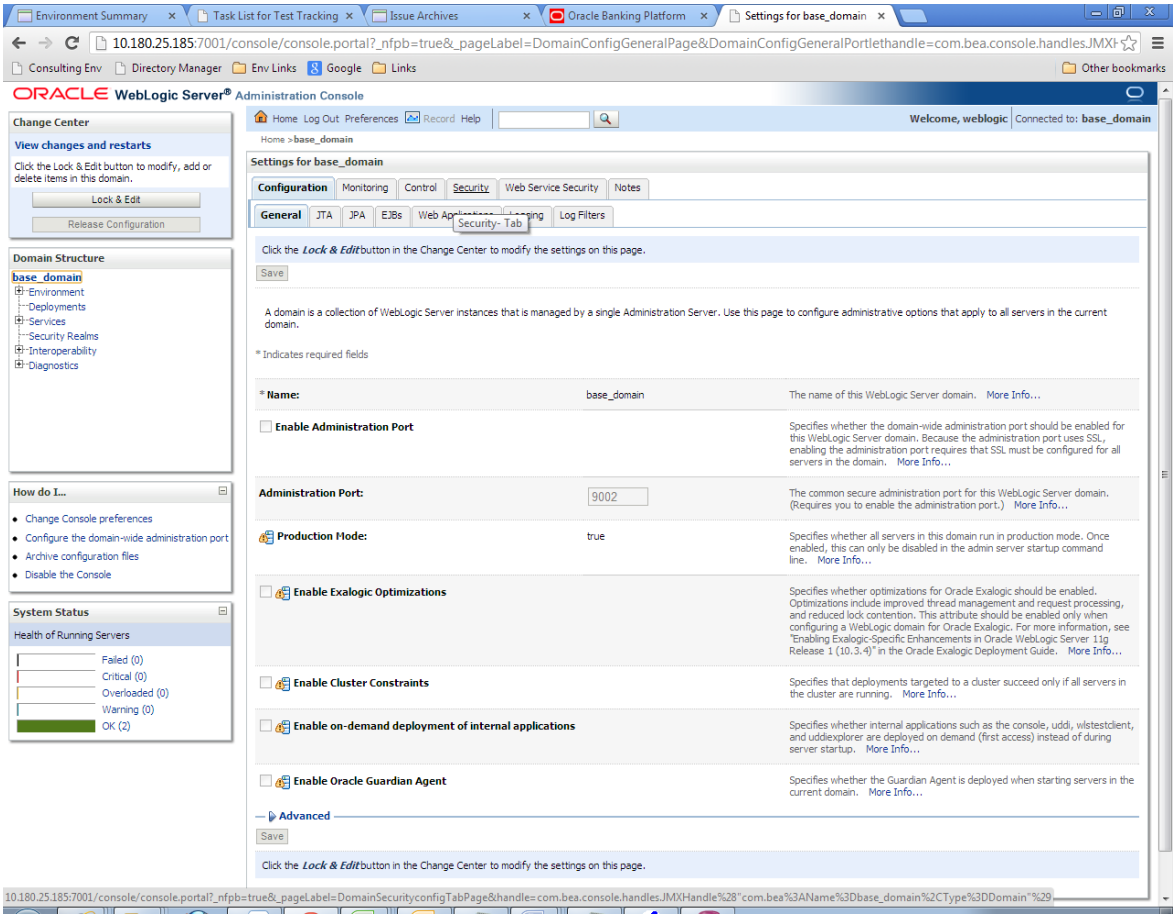
2. In the **Domain Structure** section, click the **base_domain** link.

Figure 1–29 base_domain



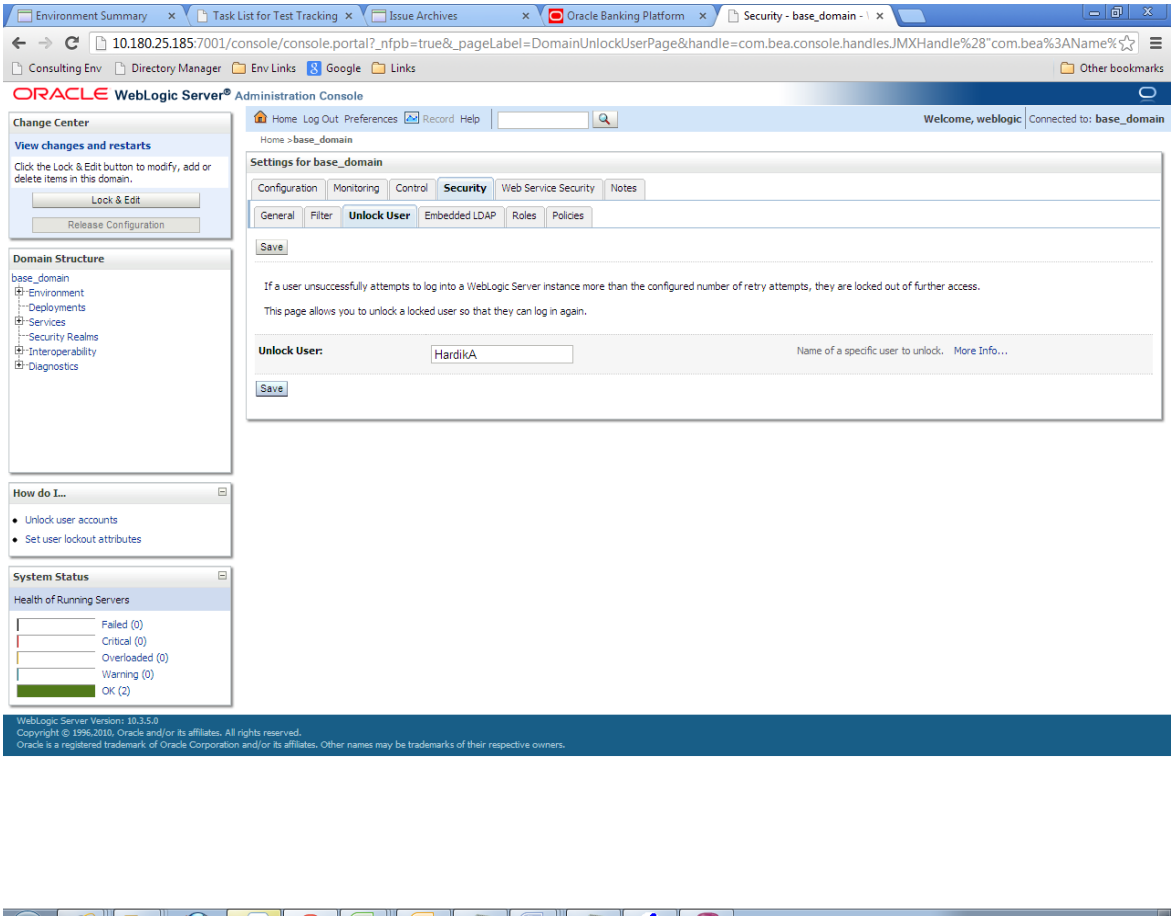
3. In the **Settings for base_domain** page that appears, click the **Security** tab.

Figure 1–30 Security tab



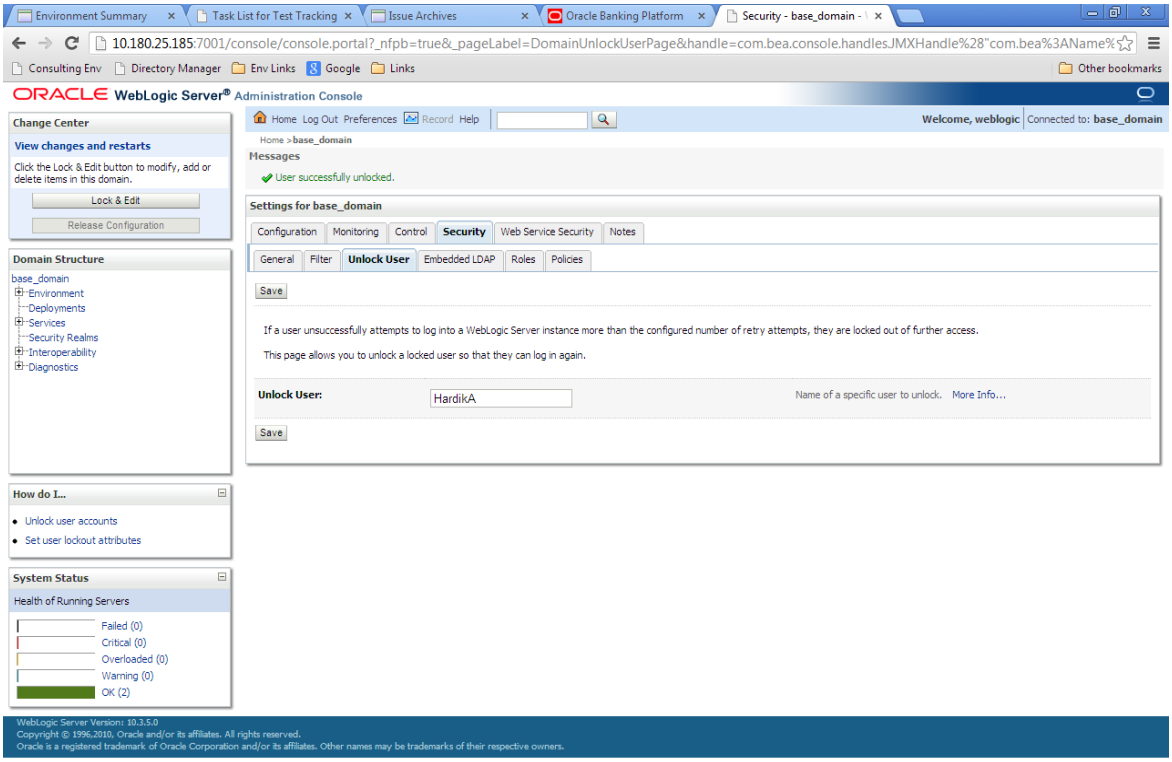
4. Click the **Unlock User** tab.
5. In the **Unlock User** field, enter the User ID to unlock the user.

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 OBEPM

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

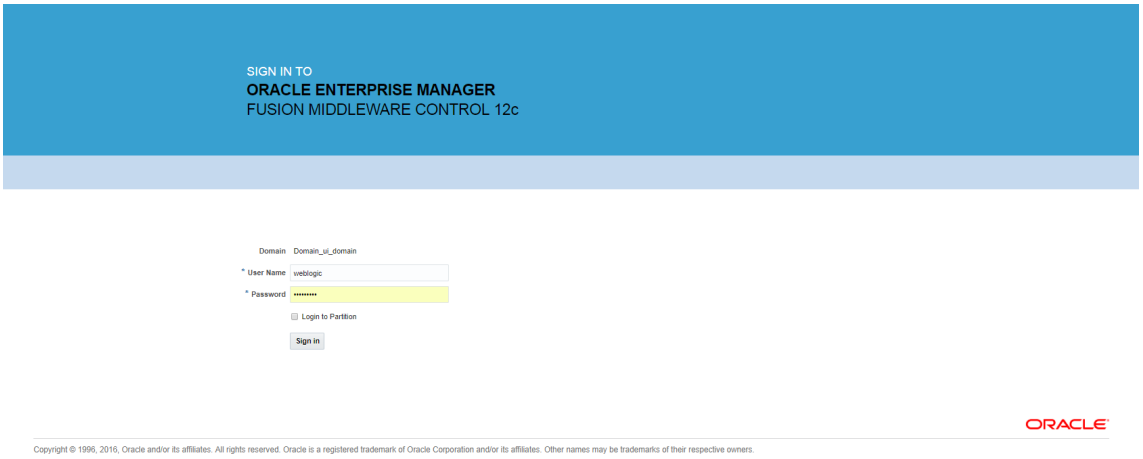


Figure 1–34 Click Application Roles

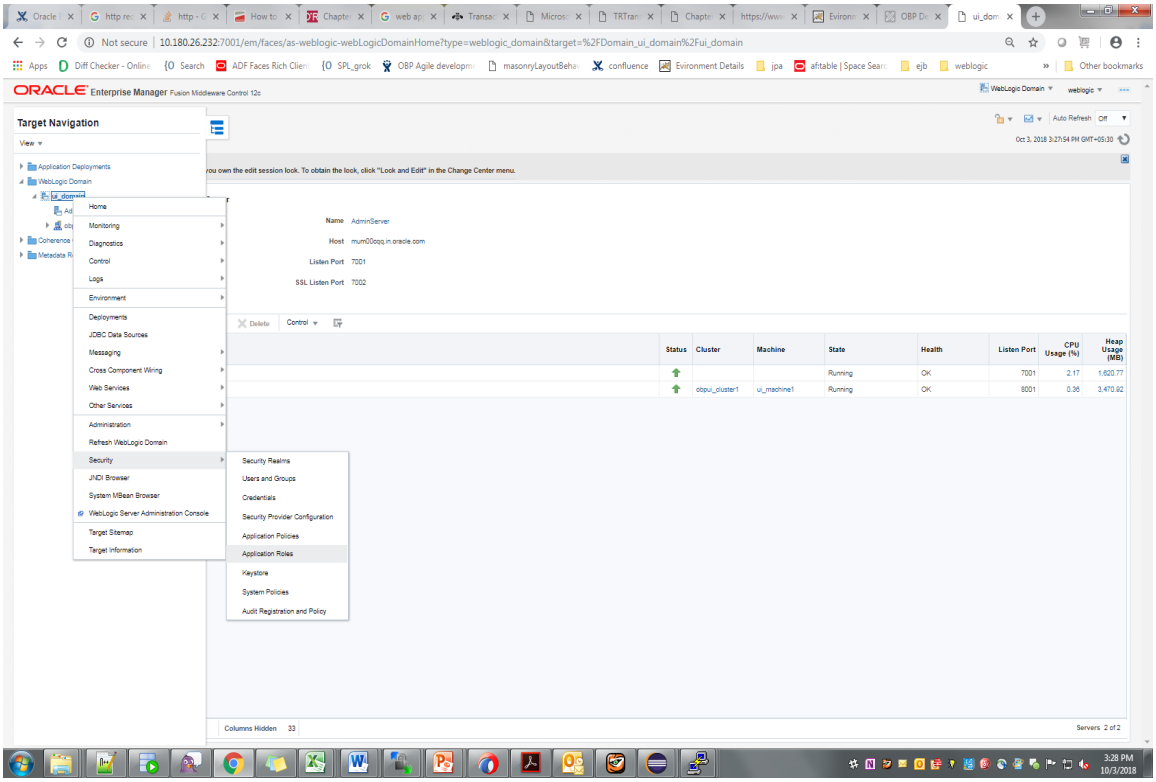


Figure 1–35 Select Administrators Role

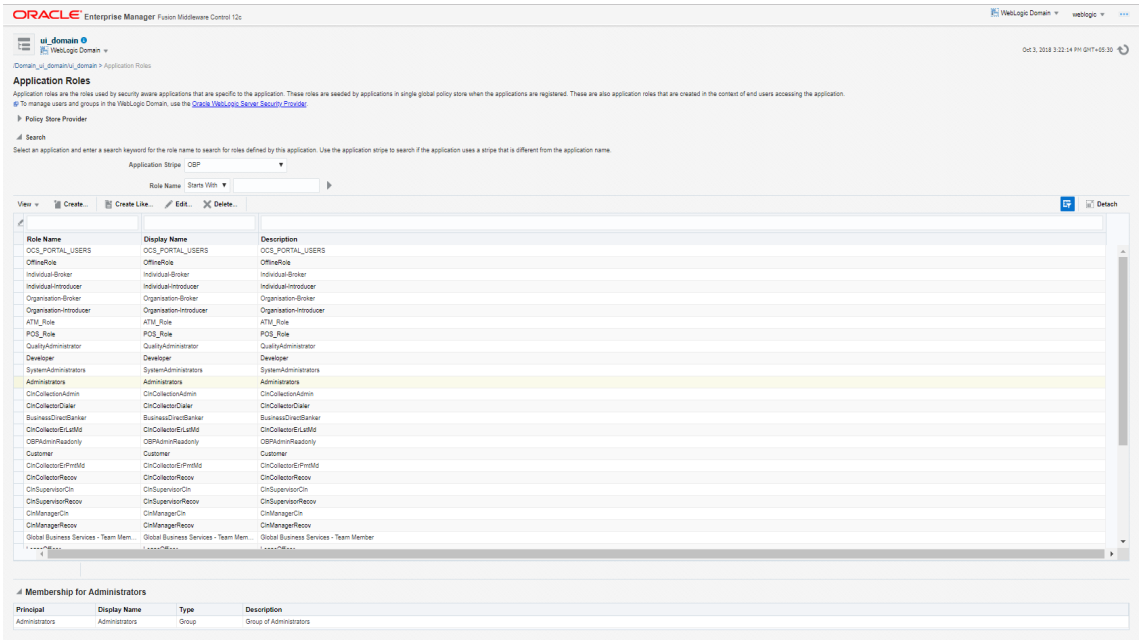
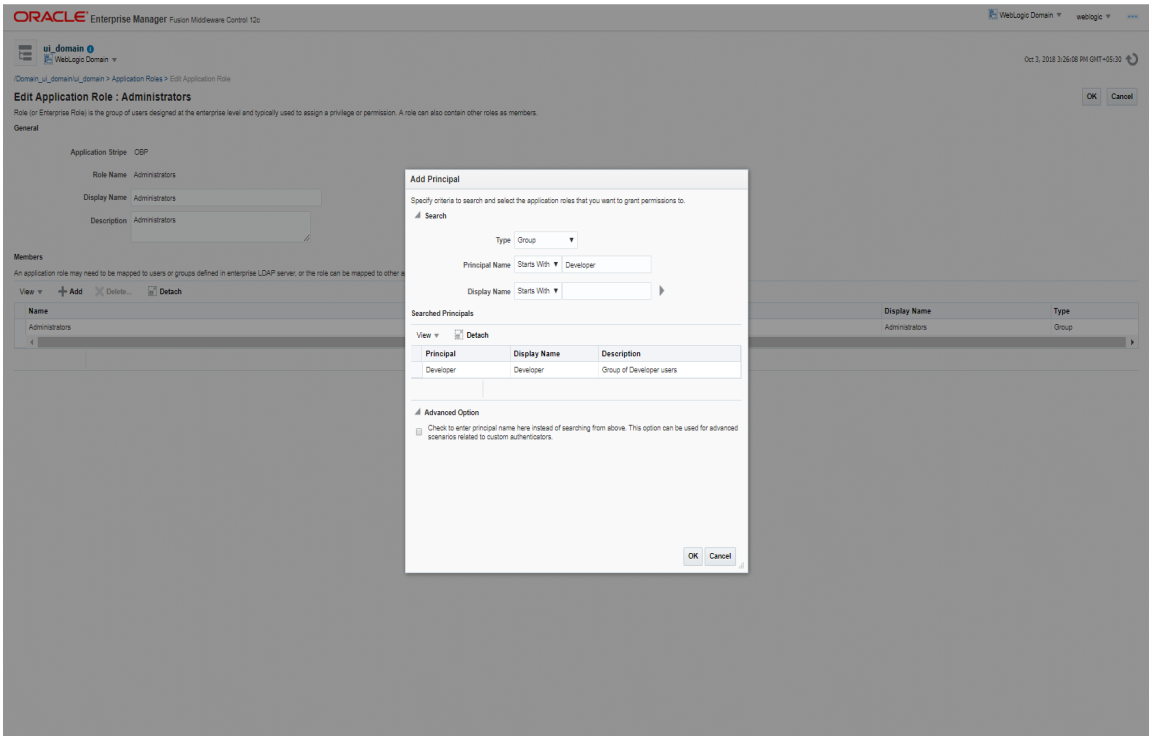


Figure 1–36 Add Principal



2 Approvals Management

This chapter describes approvals configuration and worklist authorization related activities to be performed as an administrator.

2.1 Enabling Worklist Authorization

This section explains the steps in enabling Worklist authorization. Following are the steps:

Step 1 Identify the Service Name

There can be two services for the same service. A normal 'app' service and 'appx' service. We need to identify both the services.

For example, Add Transaction Limit will have the following two services:

- com.ofss.fc.app.sms.service.limit.TransactionLimitApplicationService.addTransactionLimit
- com.ofss.fc.appx.sms.service.limit.TransactionLimitApplicationServiceSpi.addTransactionLimit

Step 2 Enable Dual Authorization

Once the services are identified, follow the below steps to enable Dual Authorization.

1. Log in to Oracle Banking Enterprise Product Manufacturing.
2. Navigate to **Artifact Dependency Map (Fast path: SM500)** page.
3. In the **Search Text** field, type the service-name or a part of it or enter phrase in the format TASK_CODE+search_text that helps to select the service using auto suggest behavior.

   For example, to search for a service for loan offer case, search text can be as follows:

   - loan offer
   - PM022+service+add loan offer
   - com.ofss.fc.appx.pm.service.core.offer.ln.LoanOfferApplicationServiceSpi.addLoanOffer

   Note

   Tips for faster searches:

   - For guided navigation to a resource (service, taskflow, ui-component), enter search text containing the resource description. (Example: 'loan offer', 'loan Offer Task Flow ', 'OK')
   - Selecting items from suggest item list will result in faster and accurate search.
   - For faster and finer searches, use 'task-code+keyword(UI_COMPONENT/SERVICE)(ignore case)+search text' pattern. (Example: 'PM022+UI_COMPONENT+validate'/ 'PM022+SERVICE+Add loan offer)

- For a combination of artifacts and general search, use 'task-code+search text' pattern. (Example: ' PM022+add loan offer')
- A maximum of 36 values are displayed where search criteria found eligible values.

Figure 2–1 Search for service using entire service name

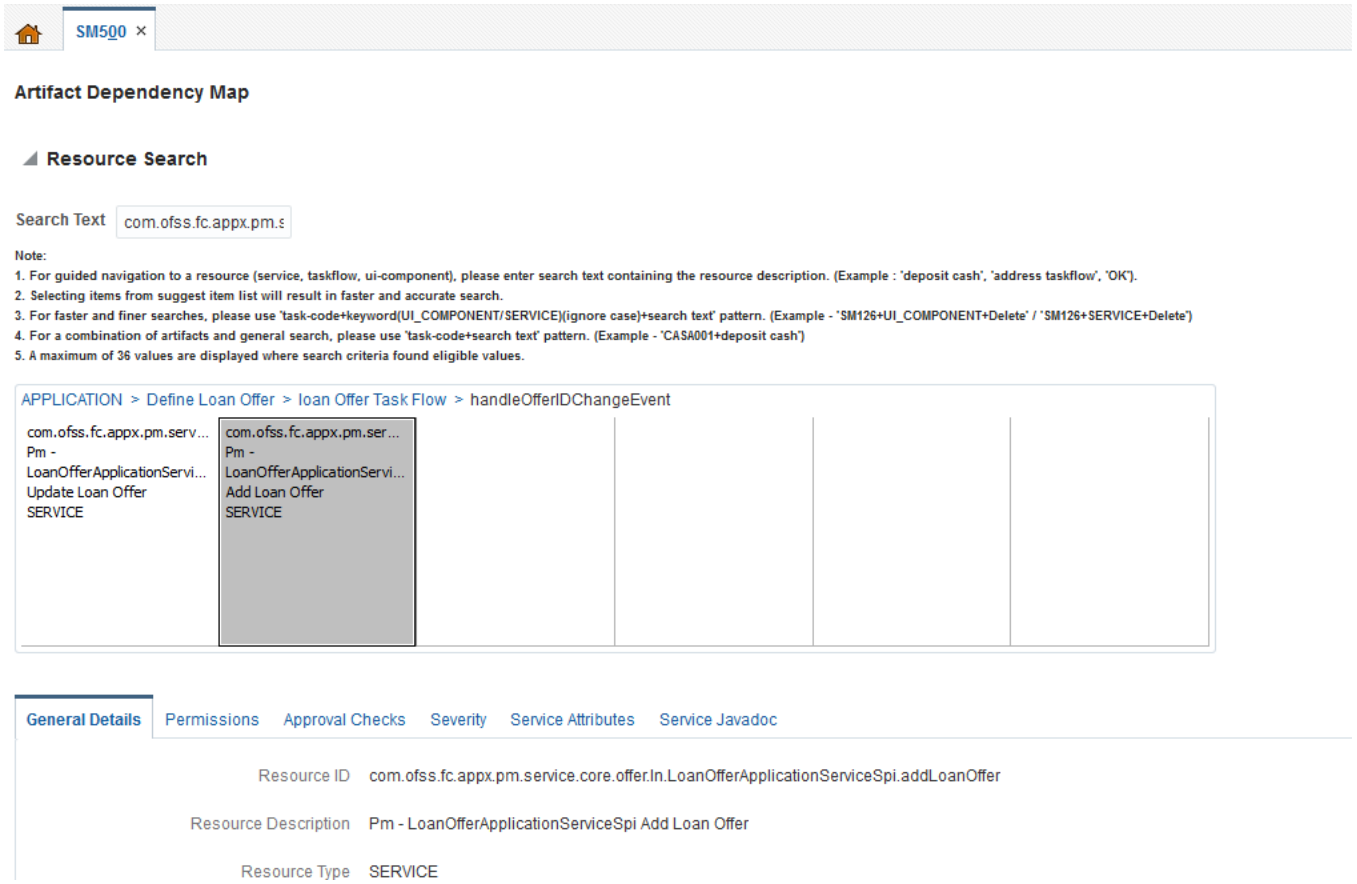
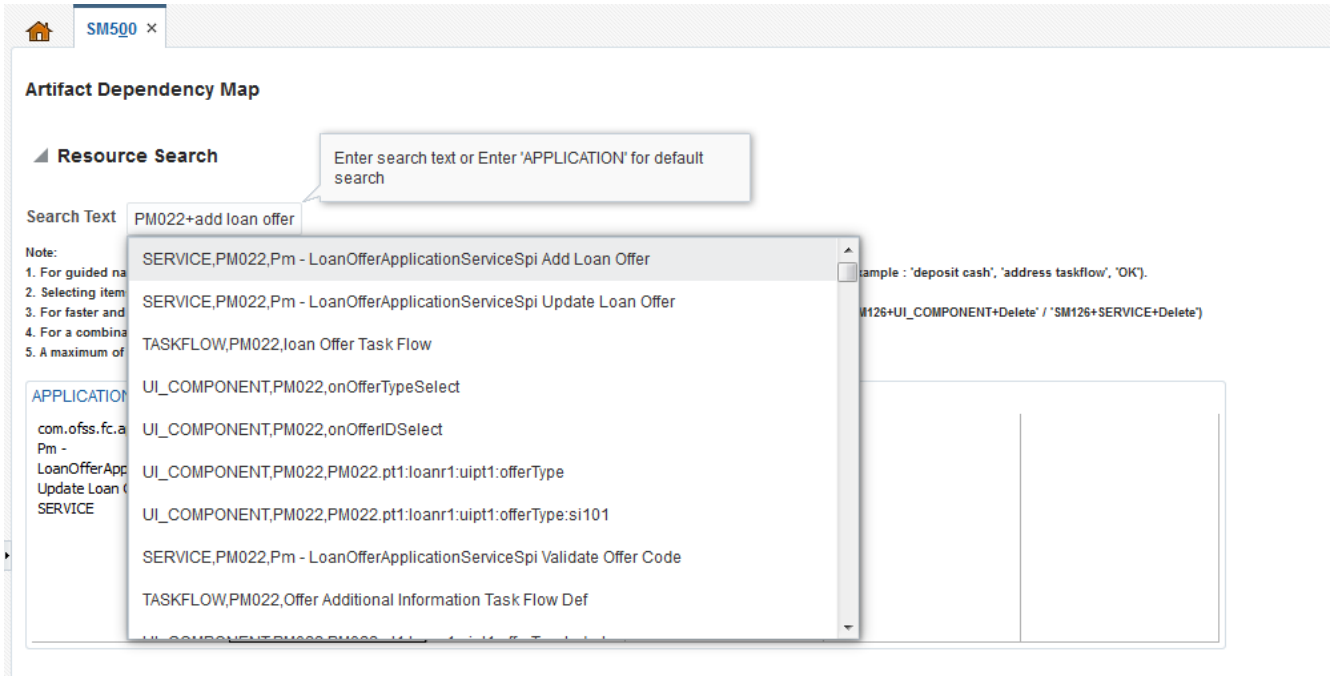
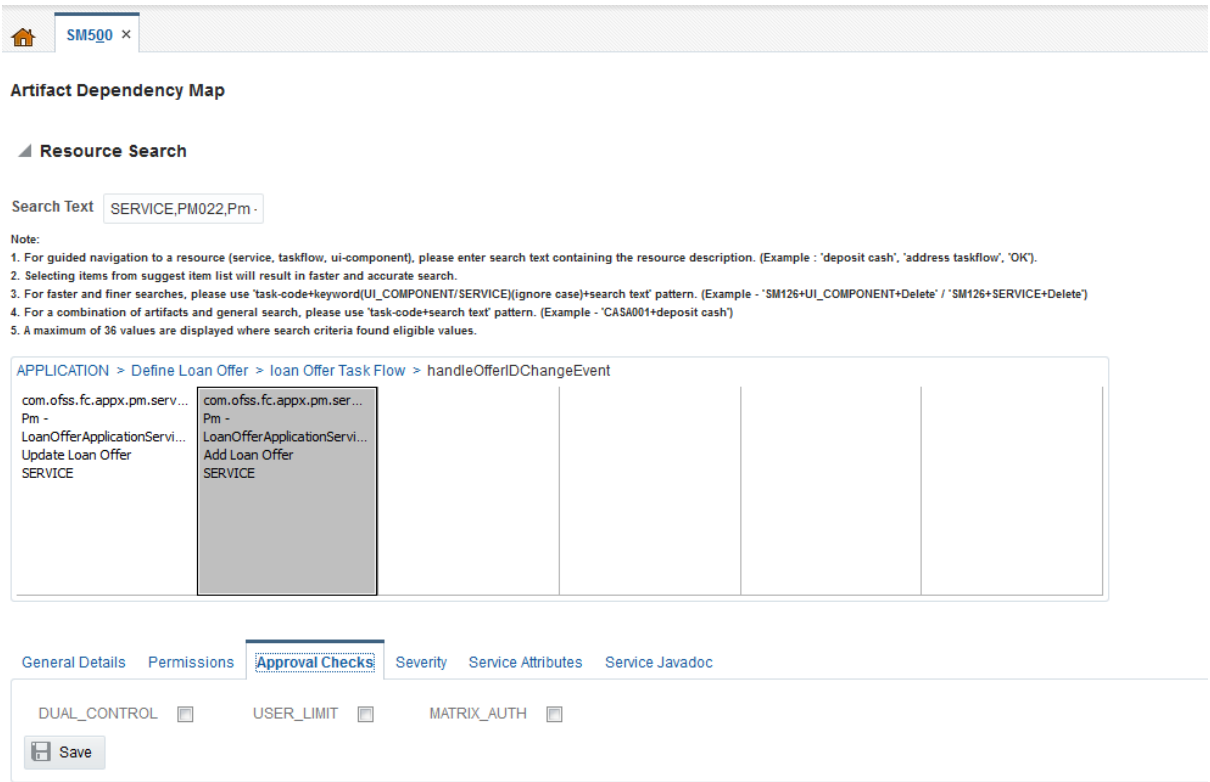


Figure 2–2 Search for service using TASK CODE + search text



4. Click the **Approval Checks** tab and add approval checks.

Figure 2–3 Add Approval Checks



Step 3 Configure Severity

Enabling of dual authorization alone will not send the transaction for approval. Hence, we need to configure Severity for the identified service, to enable the call for approval workflow.

This will be configured from the page **Artifact Dependency Map (Fast path: SM500).**

Follow the below steps to configure severity:

1. Log in to Oracle Banking Enterprise Product Manufacturing.
2. Navigate to the **Artifact Dependency Map (Fast path: SM500)** page.
3. In the **Search Text** field, type the service-name or a part of it or enter phrase in the format TASK_CODE+search_text that helps to select the service using auto suggest behavior.

   For example, to search for a service for loan offer case, search text can be as follows:

   - loan offer
   - PM022+service+add loan offer
   - com.ofss.fc.appx.pm.service.core.offer.In.LoanOfferApplicationServiceSpi.addLoanOffer

Figure 2–4 Search for service using entire service name

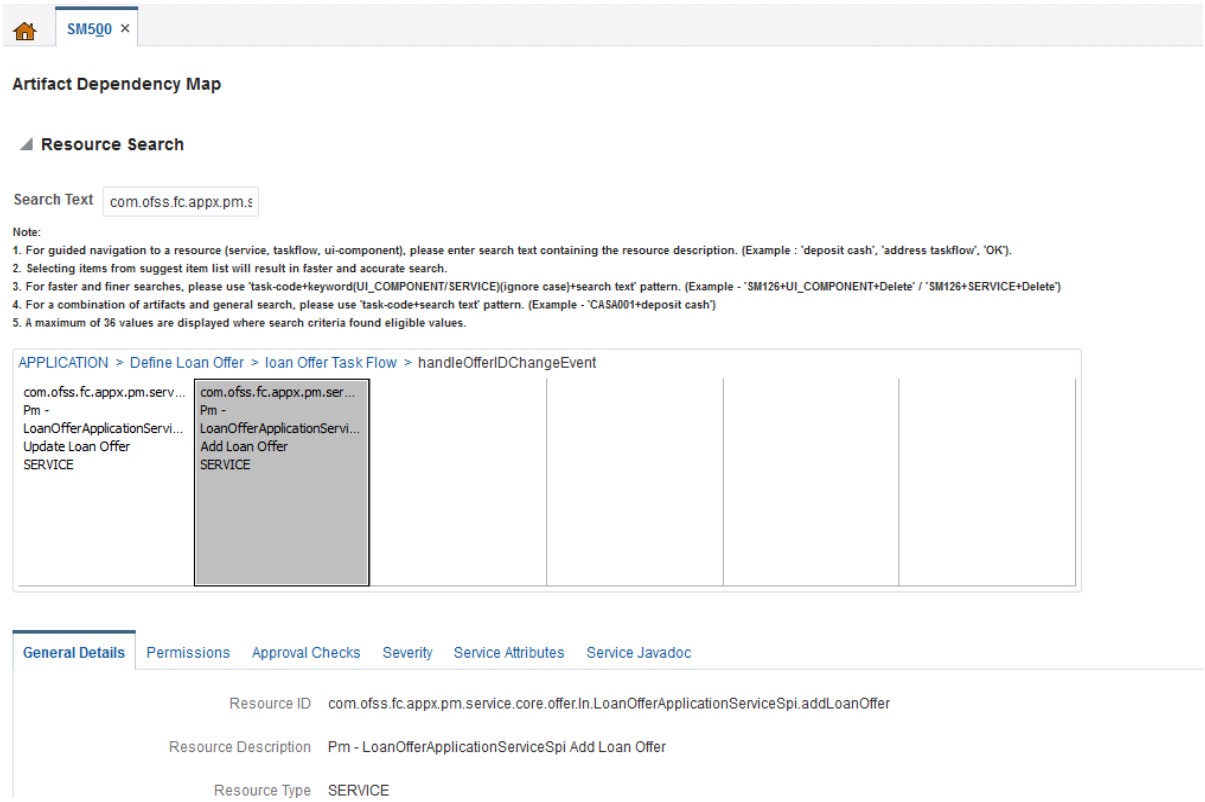
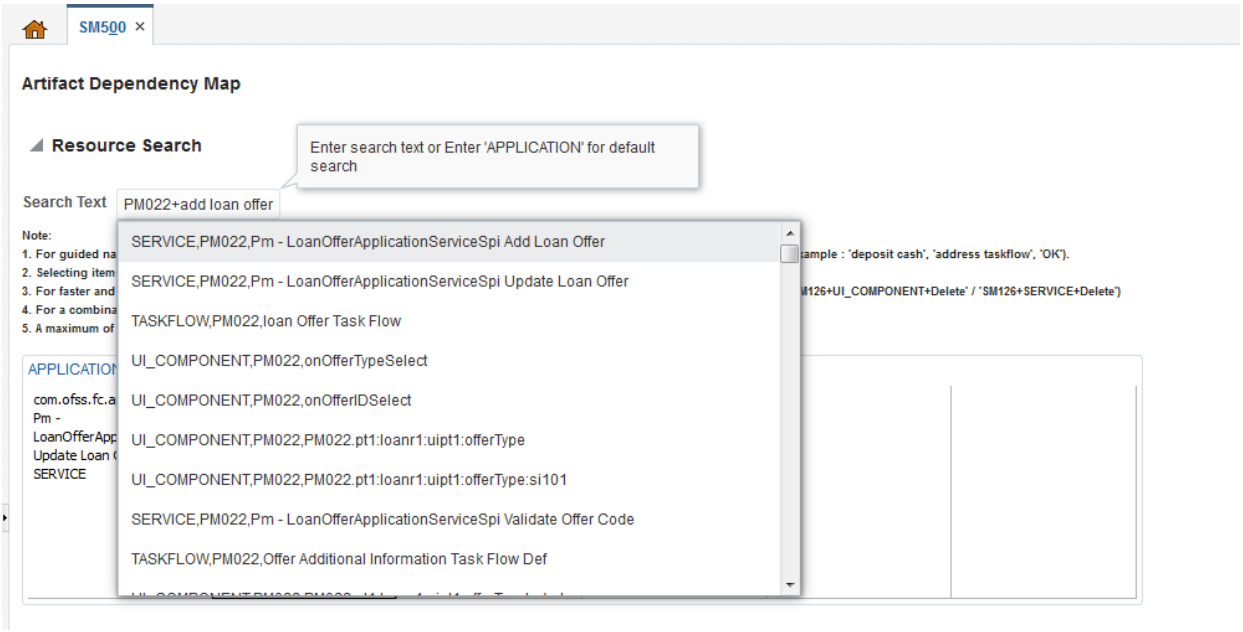
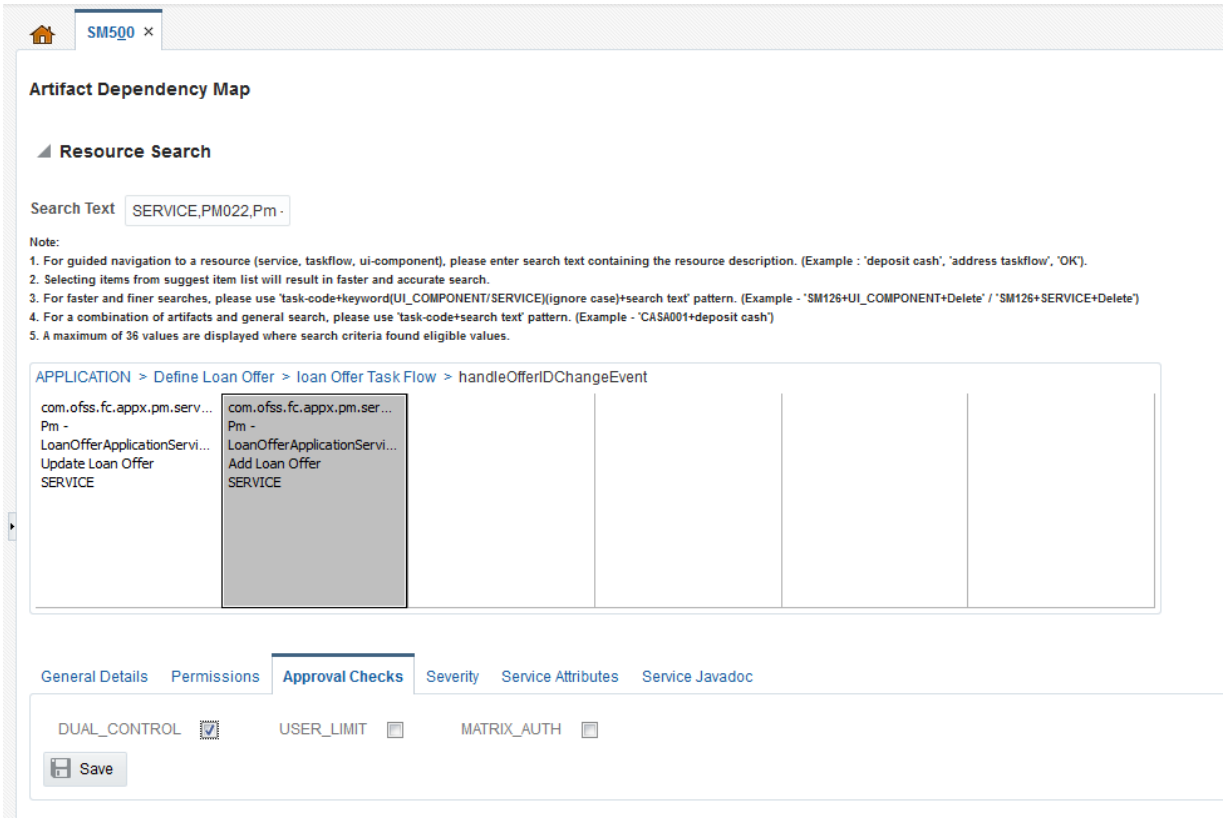


Figure 2–5 Search for service using TASK CODE + search text



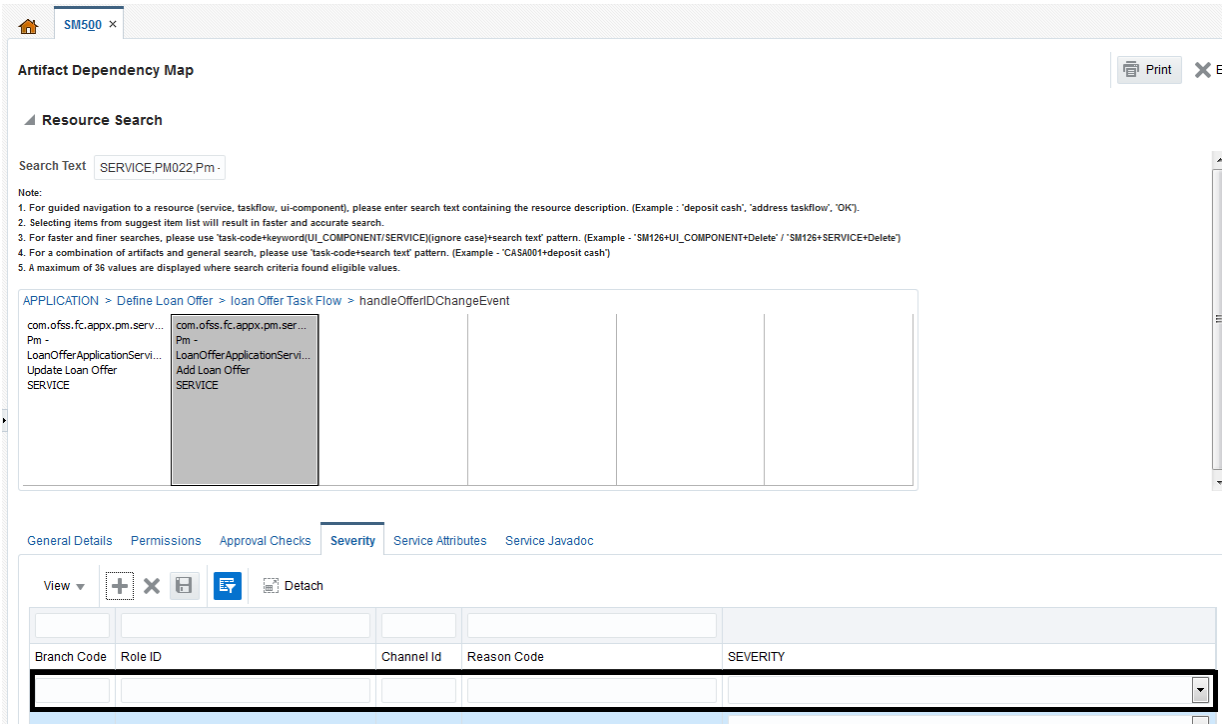
4. Ensure approval checks are added. If not, then configure the approval checks.

Figure 2–6 Dual Control



5. Click the **Severity** tab and update the severity, if already maintained. Otherwise, click the **Add** button in the toolbar to add new row in table.

Figure 2–7 Add New Severity



6. Enter the following details in the **Severity** tab.

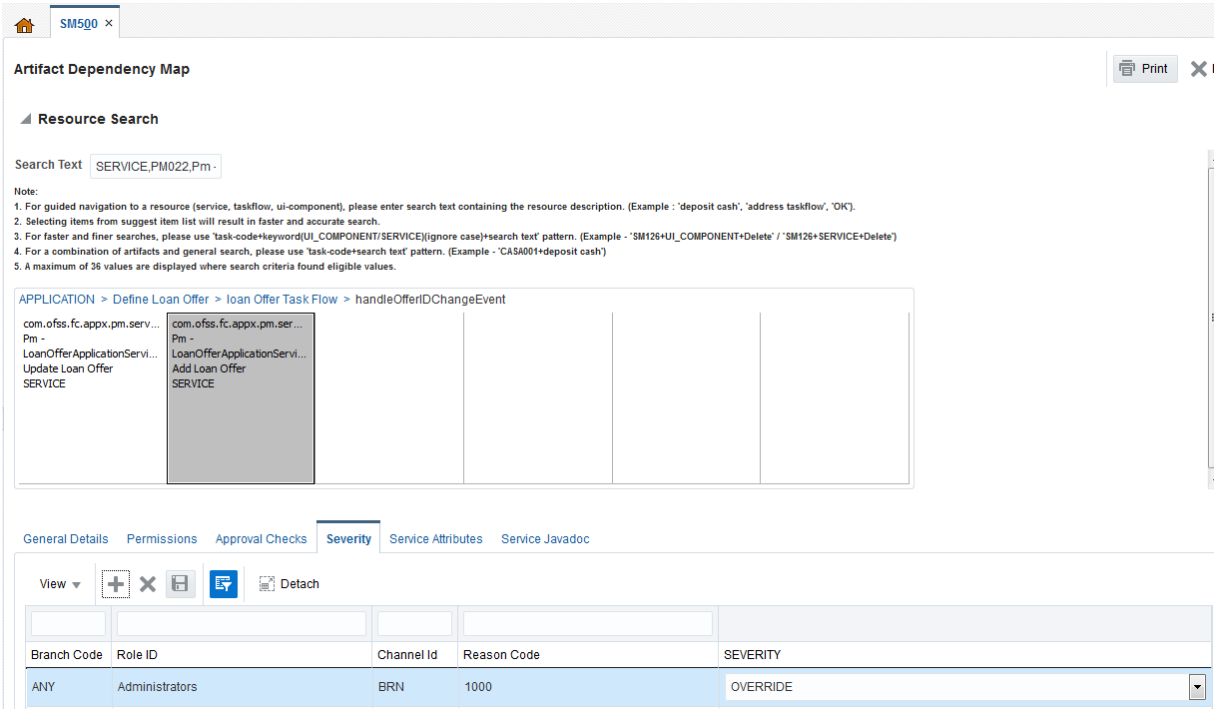
Branch Code	Branch code from which the transaction is to be performed. Specify ANY to configure for all branches. Example: 3010
Role ID	Security Role to which the user belongs and initiates the transaction.
Channel ID	Channels such as BRN, ATM, IB and so on, through which the transaction is performed.
Reason Code	Select Reason Code 1000 normal approval flow. See Section 2.2 Configuring Approvals for Reason Codes Other Than 1000 for more details.
Severity	This field contains four values as detailed below: ■ **Ignore:** Allows transaction to complete without any authorization, that is Auto Authorization. ■ **Override:** Transaction will be sent for Authorization. ■ **Notify:** In this case, the task is not sent for authorization, but the user is expected to confirm the transaction for

	proceeding ahead. This option is not applicable in case of Dual Authorization. ■ **Reject:** System does not allow to proceed with transaction.

To enable Dual Authorization, select **Override** option.

> **Note**
>
> At times you may also notice that the Severity Configuration is already set up. Do not change it.

Figure 2–8 Add Severity Details



7. Save newly added severity using the **Save** button in toolbar.

Figure 2–9 Save Severity Details

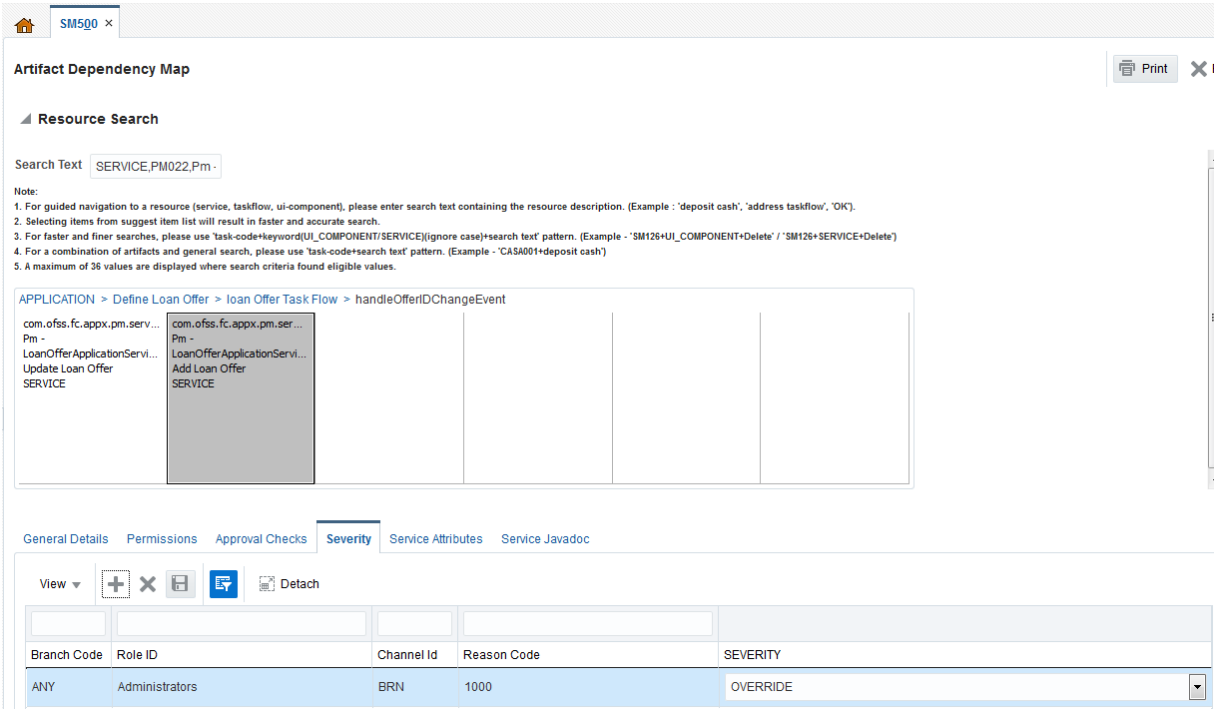
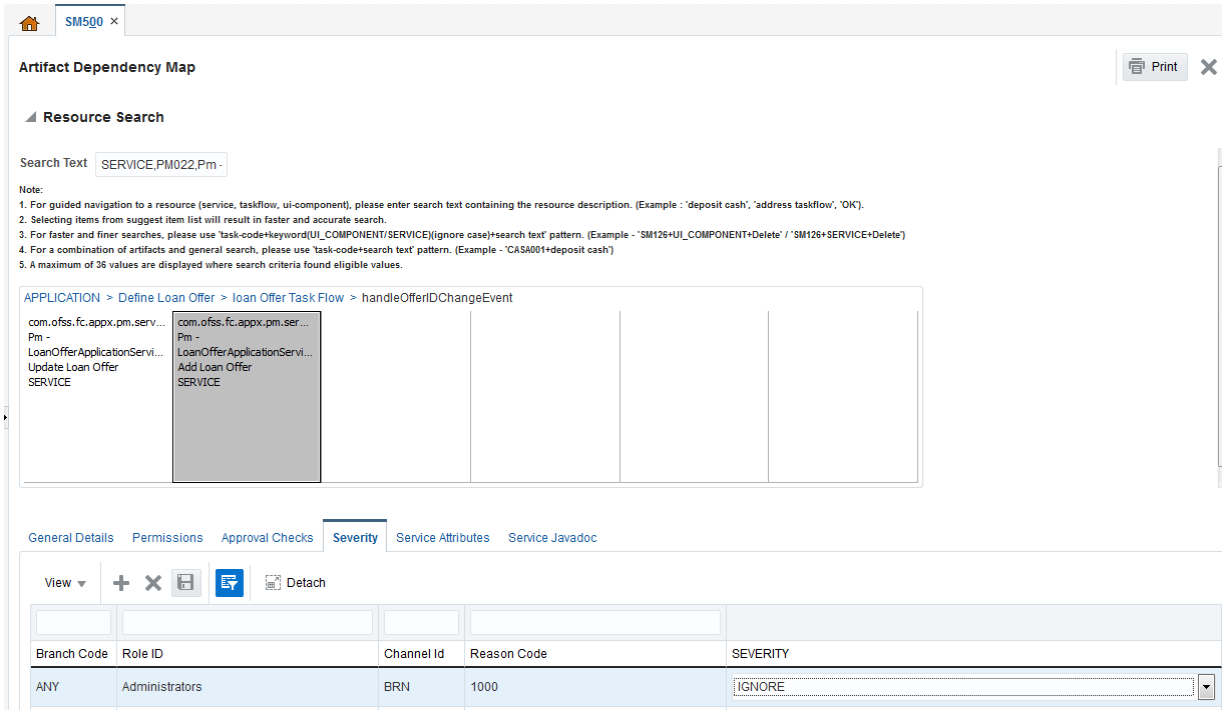


Figure 2–10 Update Severity and Save



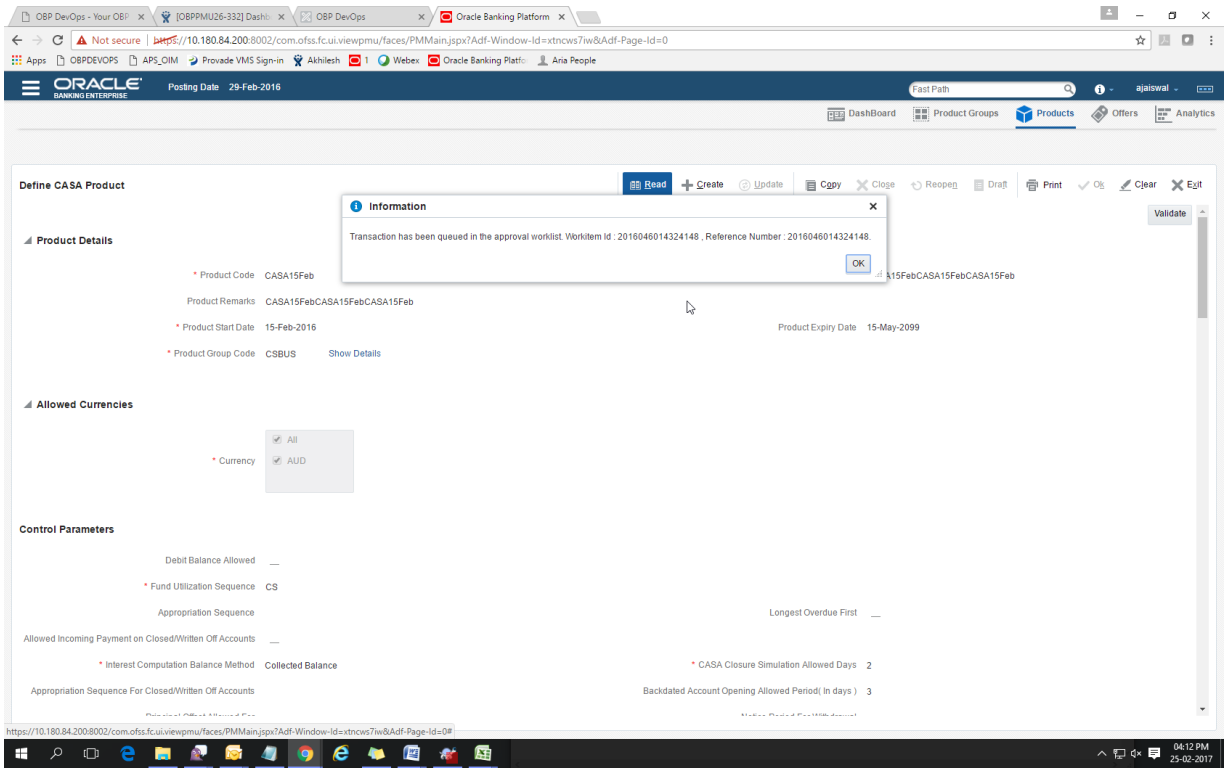
Step 4 Testing Approvals

Once the configurations are done, navigate to the screen for which approval is enabled.

Let us consider **Define CASA Product** for example:

1. Log in to Oracle Banking Enterprise Product Manufacturing.
2. Navigate to the page **Define CASA Product.**
3. Enter the required details and click **Ok.** The message *Approval is required for the transaction* appears.

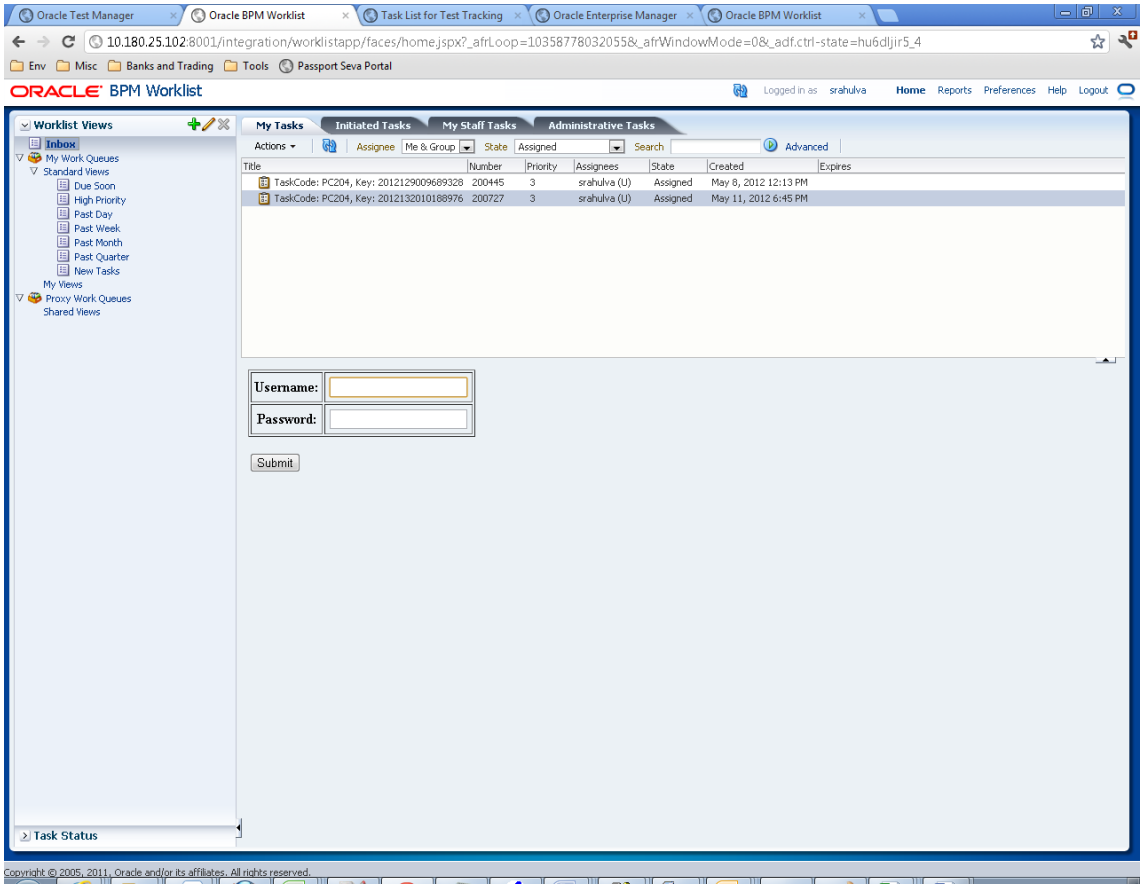
Figure 2–11 Define CASA Product



4. Now log in to the Oracle BPM Worklist application (BPEL Worklist) of the respective environment using the supervisor credential.
5. In **My Tasks**, select the work item assigned against your name.

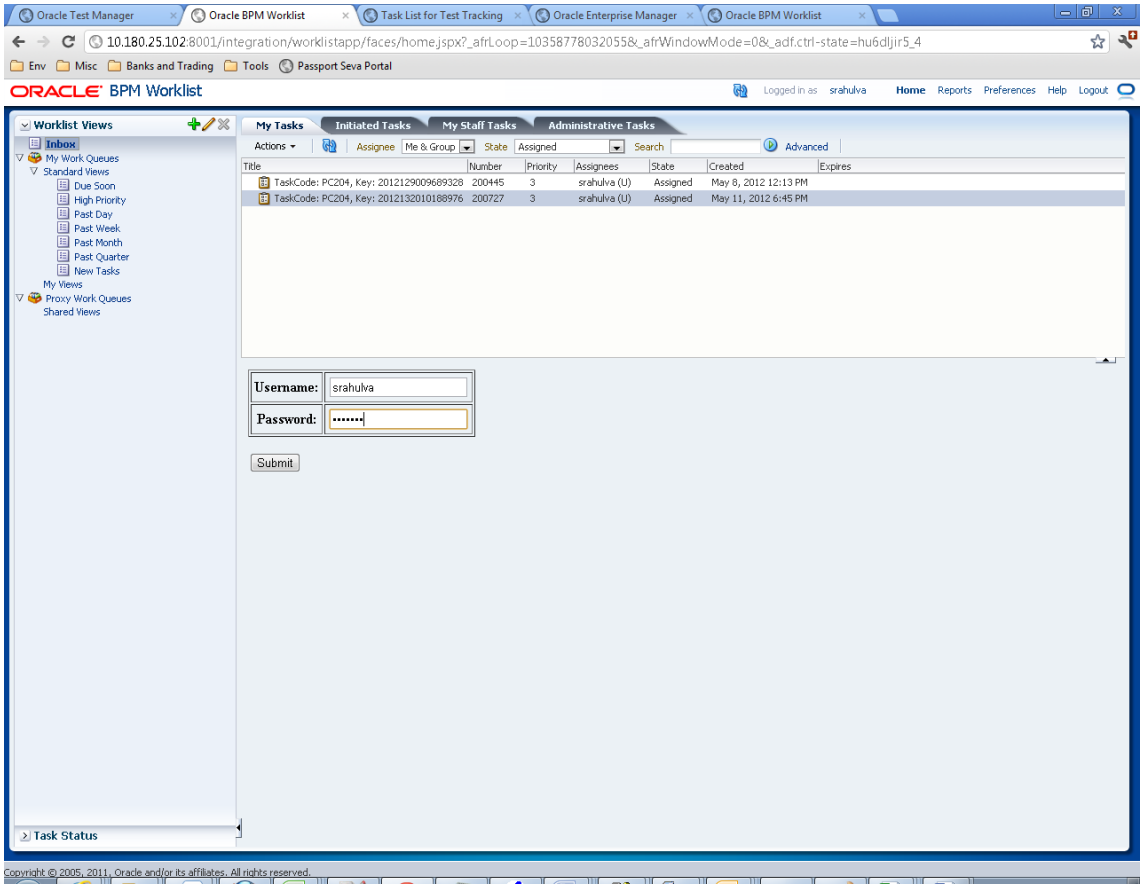
   The application prompts for Log in credentials again as shown in below figure.

Figure 2–12 Oracle BPM Worklist Log in



6. Enter the same user name and password to open the work item page.

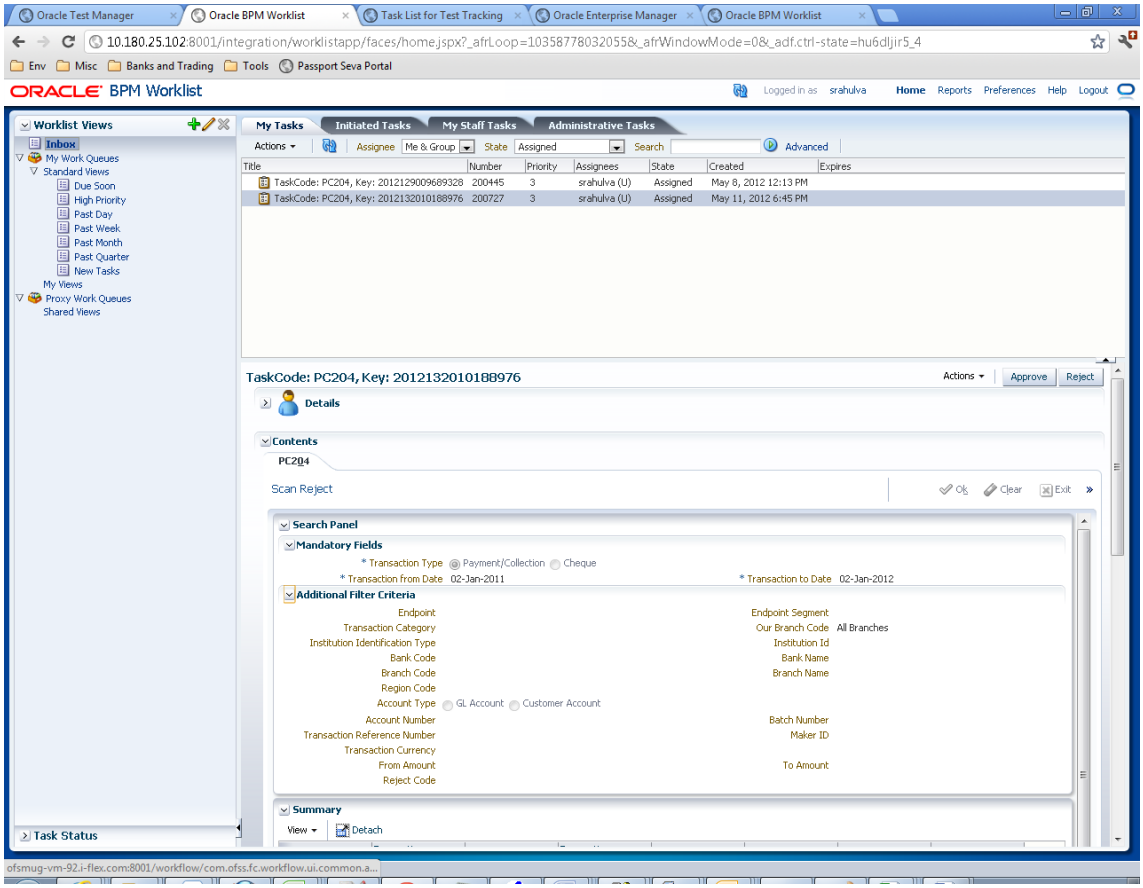
Figure 2–13 Enter Log in Credentials



7. On successful submission of the Log in credentials, you can see the snapshot of the OBEPM application page from which the transaction occurred and was sent for approval.
8. Verify whether the page displays the data entered in the OBEPM application when it was sent for approval.

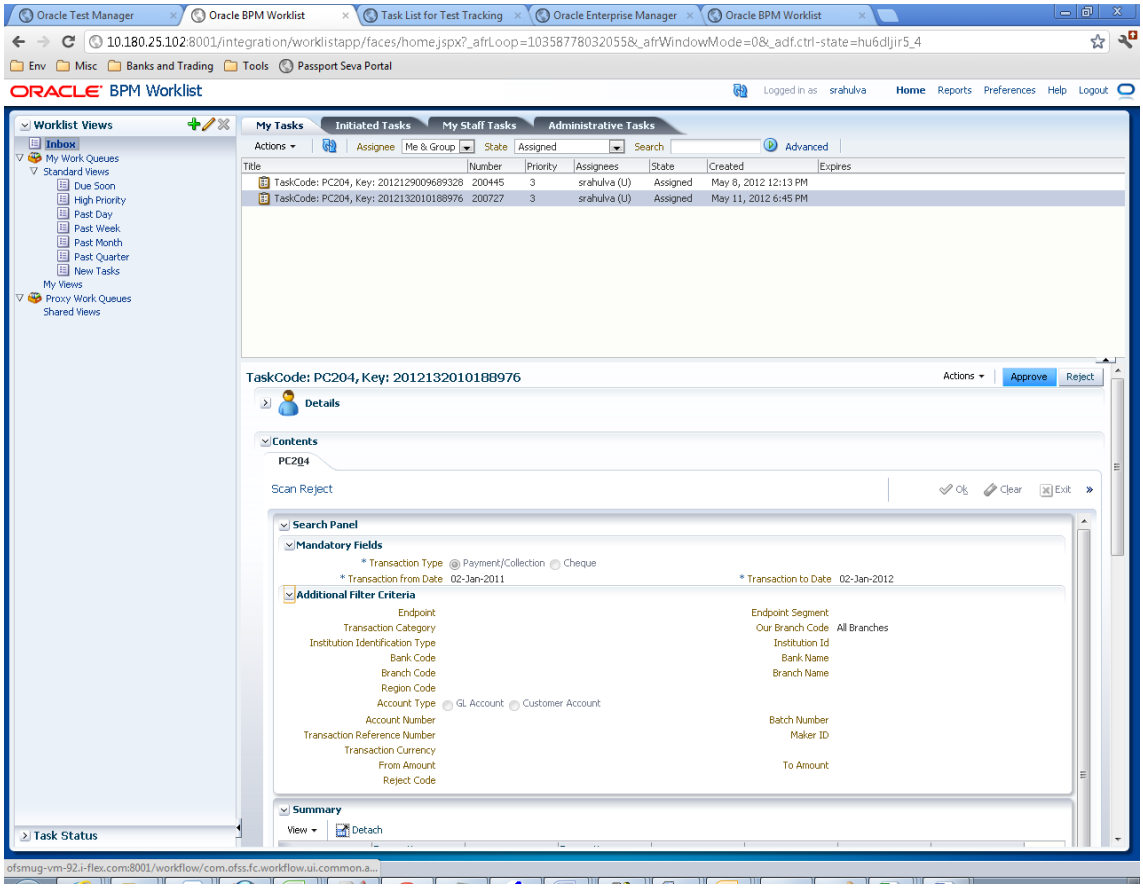
   You can see Approve and Reject option for the work item.

Figure 2–14 My Tasks - Work Item Details



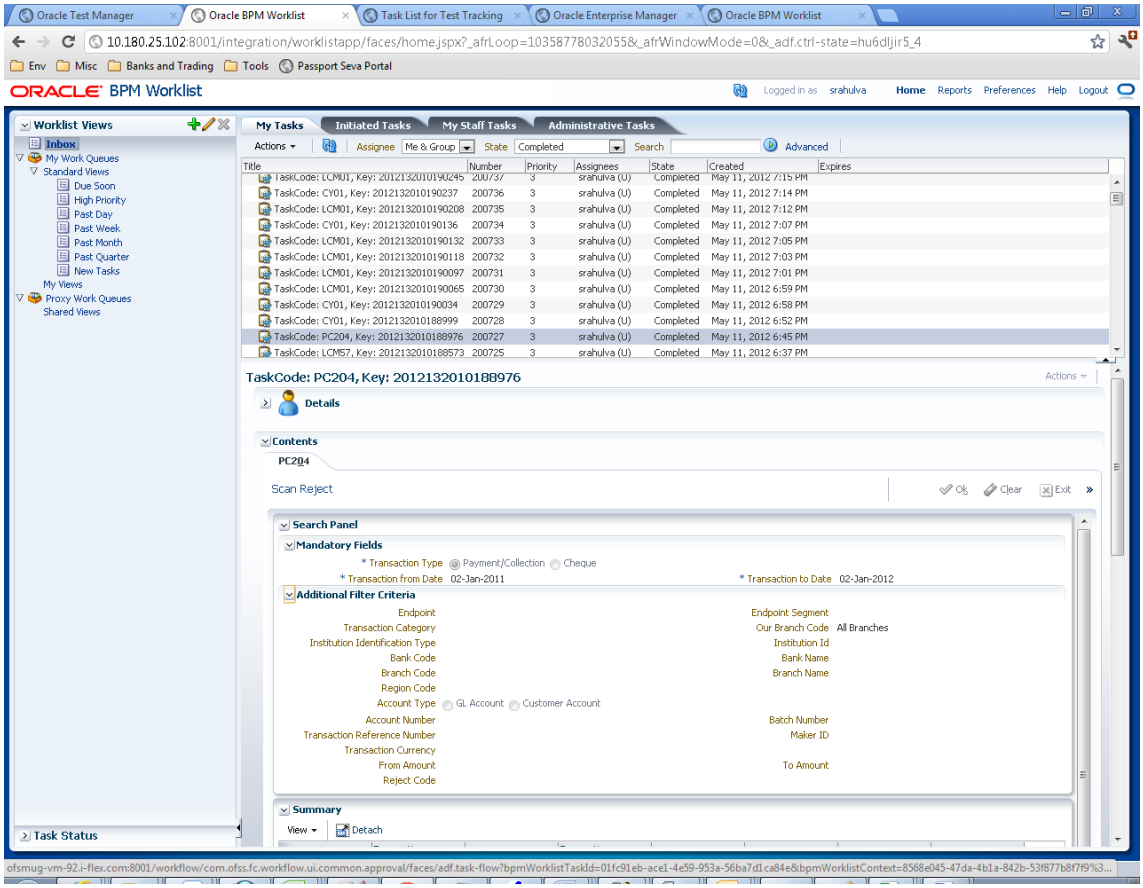
9. Click **Approve** or **Reject** to perform the appropriate action.

Figure 2–15 Approve or Reject Task



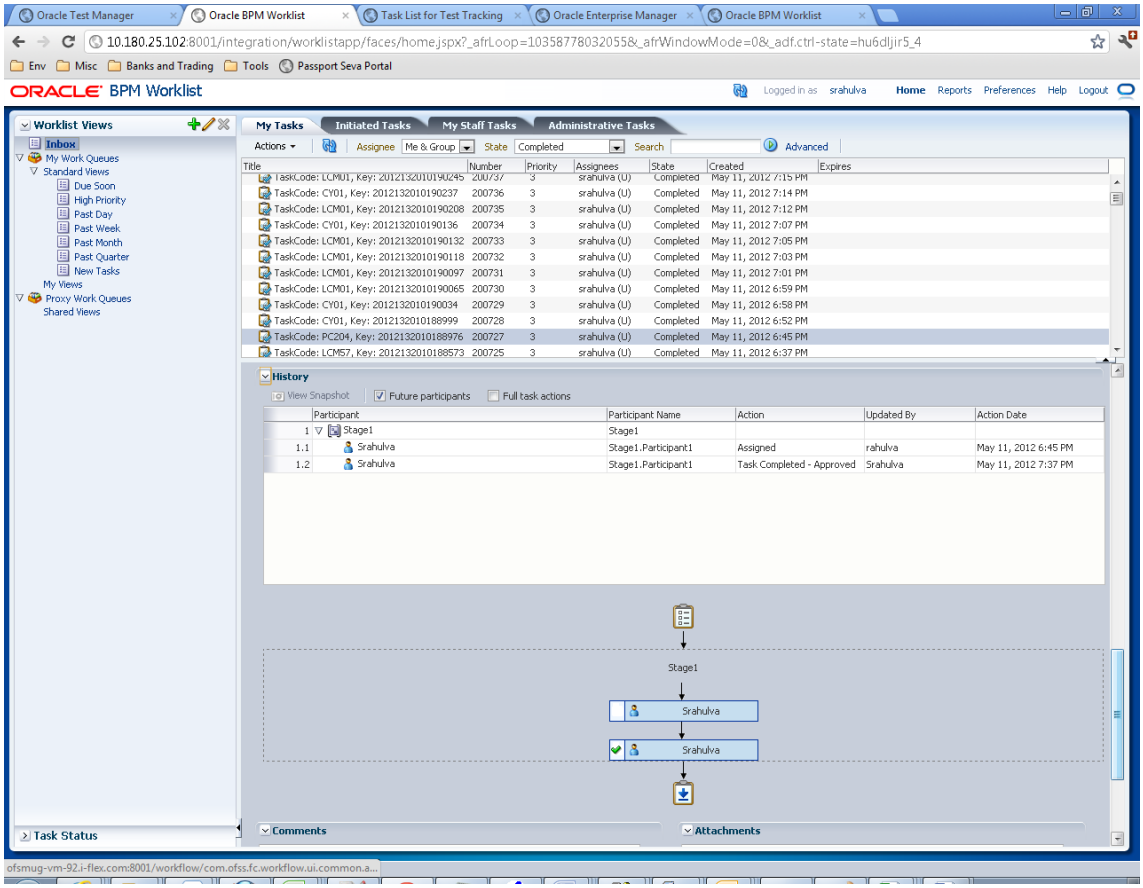
Once the transaction is approved, you can see the status of transaction as *Completed*. This can also be seen by selecting the option *Completed* from **State** list as shown in Figure 2–16.

Figure 2–16 Task Complete



10. Check the history of the work item by scrolling down.

Figure 2–17 Worklist Task History



2.2 Configuring Approvals for Reason Codes Other Than 1000

This section explains the steps in configuring approvals for reason codes other than 1000.

For configuring approvals for reason code other than 1000, like High severity memo and so on, you need to set up the same in OBEPM page **Artifact Dependency Map (Fast path: SM500)**.

Following are the steps to set up approval for other reason codes:

1. Log in to Oracle Banking Enterprise Product Manufacturing.
2. Navigate to the **Artifact Dependency Map (Fast path: SM500)** page.
3. In the **Search Text** field, type the service-name or a part of it or enter phrase in the format TASK_ CODE+search_text that helps to select the service using auto suggest behavior.

   For example, to search for a service for loan offer case, search text can be as follows:

   - loan offer
   - PM022+service+add loan offer
   - com.ofss.fc.appx.pm.service.core.offer.In.LoanOfferApplicationServiceSpi.addLoanOffer

Note

Tips for faster searches:

- For guided navigation to a resource (service, taskflow, ui-component), enter search text containing the resource description. (Example: 'loan offer', 'loan Offer Task Flow ', 'OK')
- Selecting items from suggest item list will result in faster and accurate search.
- For faster and finer searches, use 'task-code+keyword(UI_COMPONENT/SERVICE)(ignore case)+search text' pattern. (Example: 'PM022+UI_COMPONENT+validate'/ 'PM022+SERVICE+Add loan offer)
- For a combination of artifacts and general search, use 'task-code+search text' pattern. (Example: ' PM022+add loan offer')
- A maximum of 36 values are displayed where search criteria found eligible values.

Figure 2–18 Search for service using entire service name

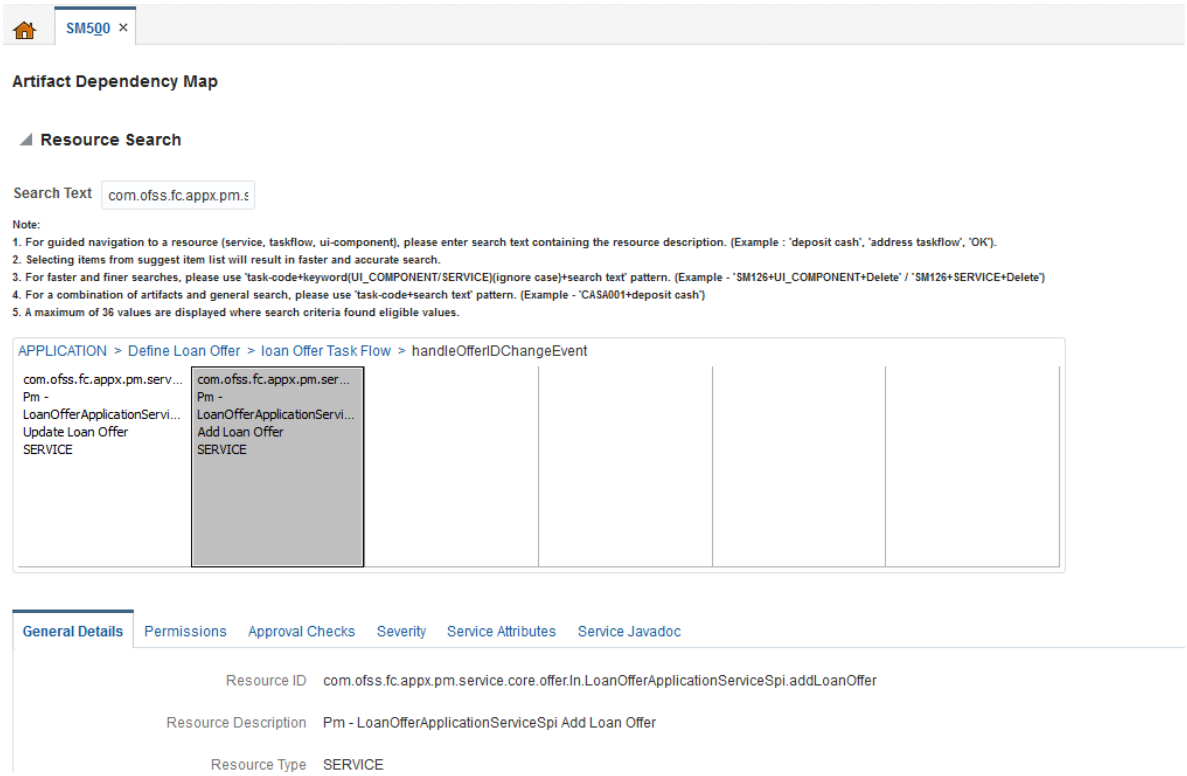


Figure 2–19 Search for service using part of service name

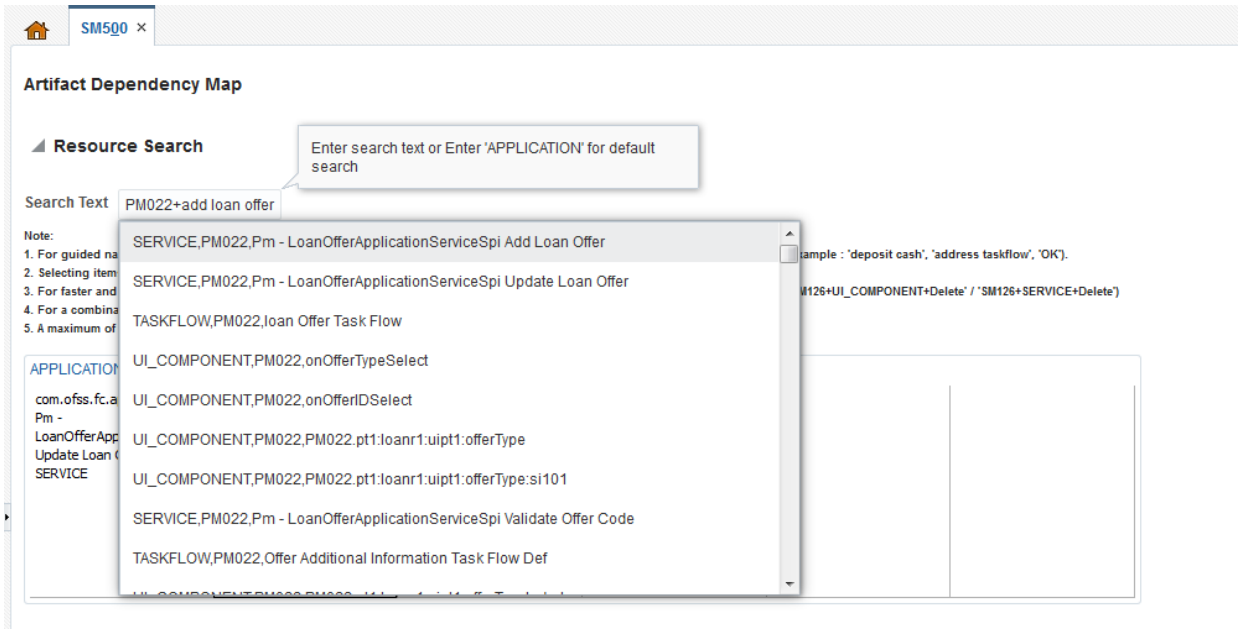
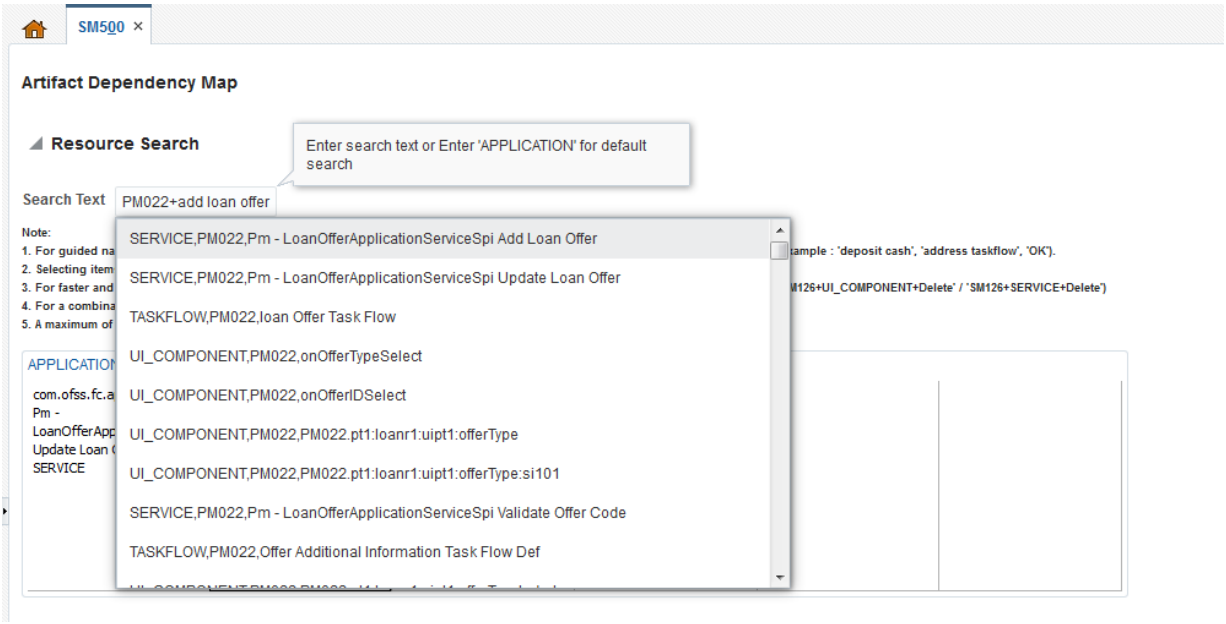


Figure 2–20 Search for service using TASK CODE + search text



4. Drill down to service level node following highlighted path (grey area).

Figure 2–21 Search results showing highlights

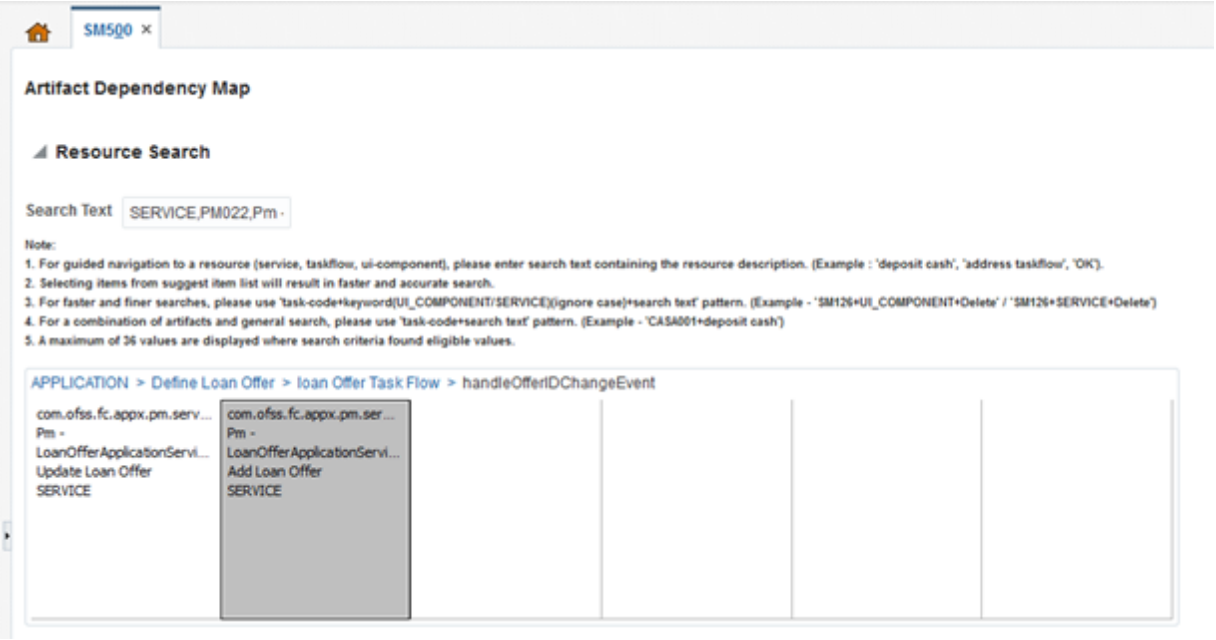
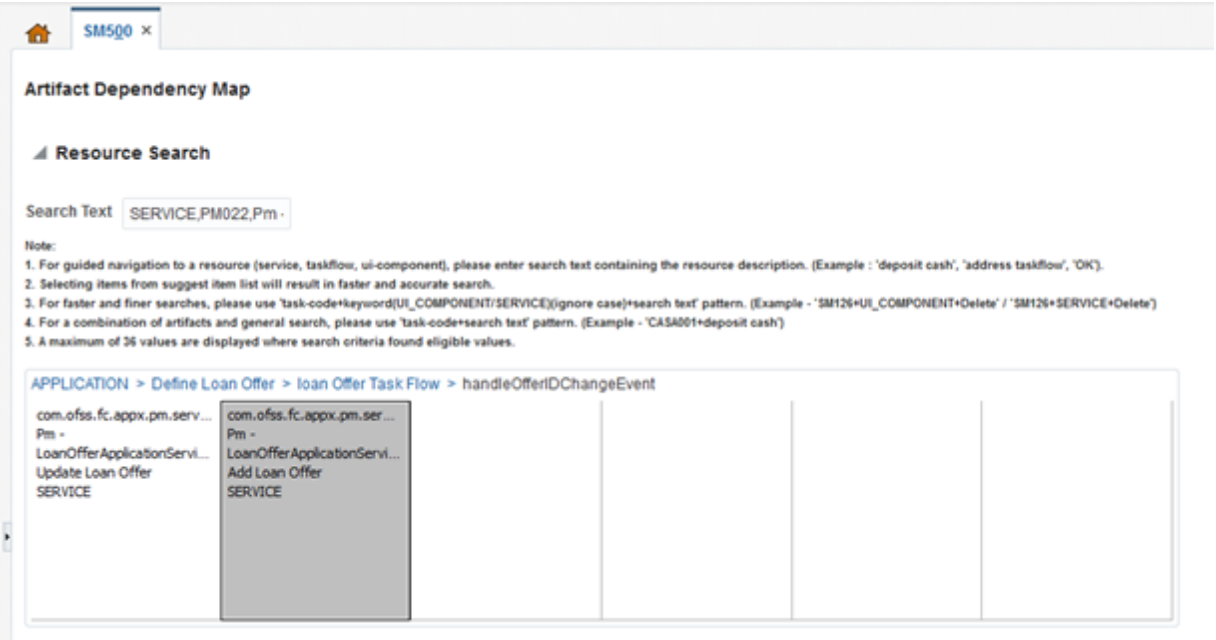
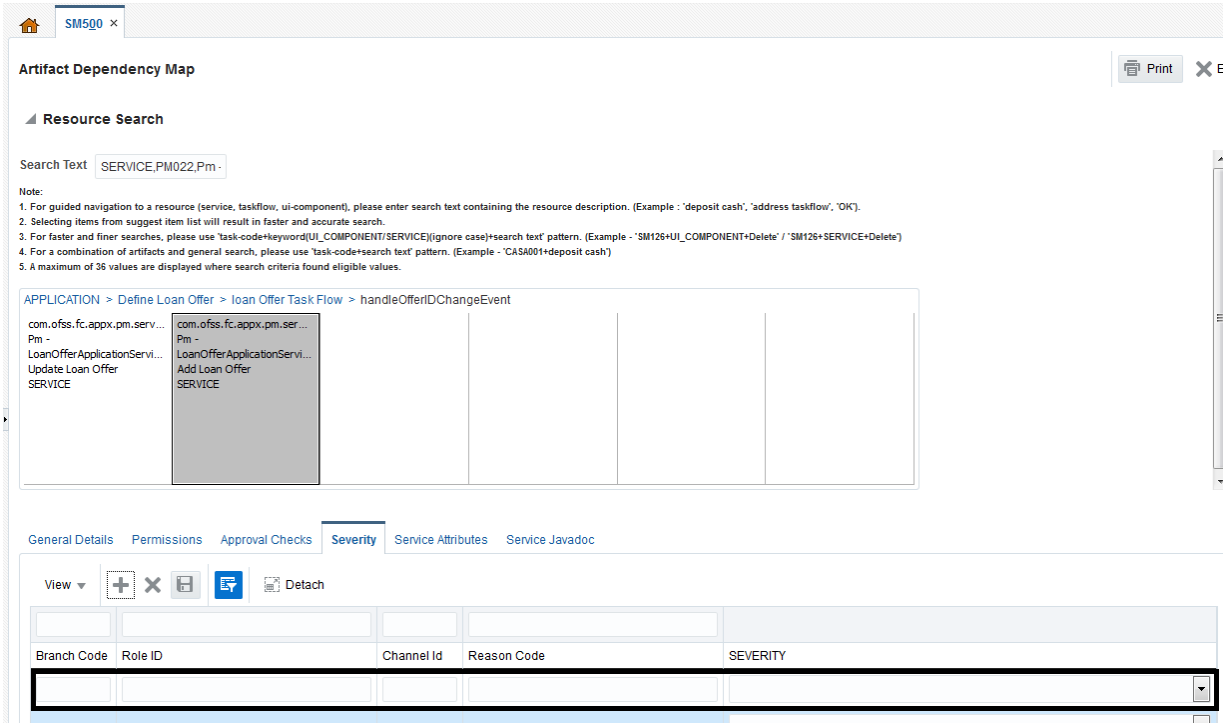


Figure 2–22 Drill down to service level



5. Click the **Severity** tab and update the severity, if already maintained. Otherwise, click the **Add** button in the toolbar to add new row in table.

Figure 2–23 Add New Severity



6. Enter the following details in the **Severity** tab.

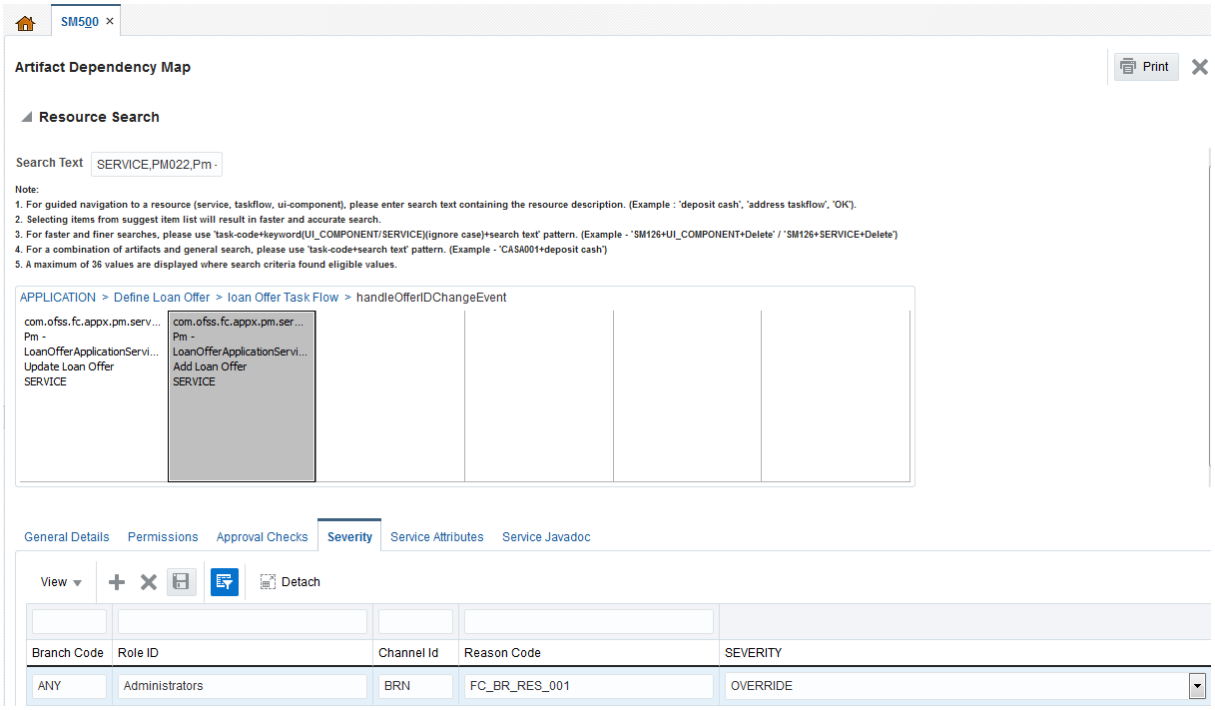
Branch Code	Branch code from which the transaction is to be performed. Specify ANY to configure for all branches. Example: 3010
Role ID	Security Role to which the user belongs and initiates the transaction.
Channel ID	Channels such as BRN, ATM, IB and so on, through which the transaction is performed.
Reason Code	Reason code for approval checks or overridable authorizations.
Severity	This field contains four values as detailed below: ■ **Ignore:** Allows transaction to complete without any authorization, that is Auto Authorization. ■ **Override:** Transaction will be sent for Authorization. ■ **Notify:** In this case, the task is not sent for authorization, but the user is expected to confirm the transaction for proceeding ahead. This option is not applicable in case of Dual Authorization. ■ **Reject:** System does not allow to proceed with transaction.

To enable Dual Authorization, select **Override** option.

Note

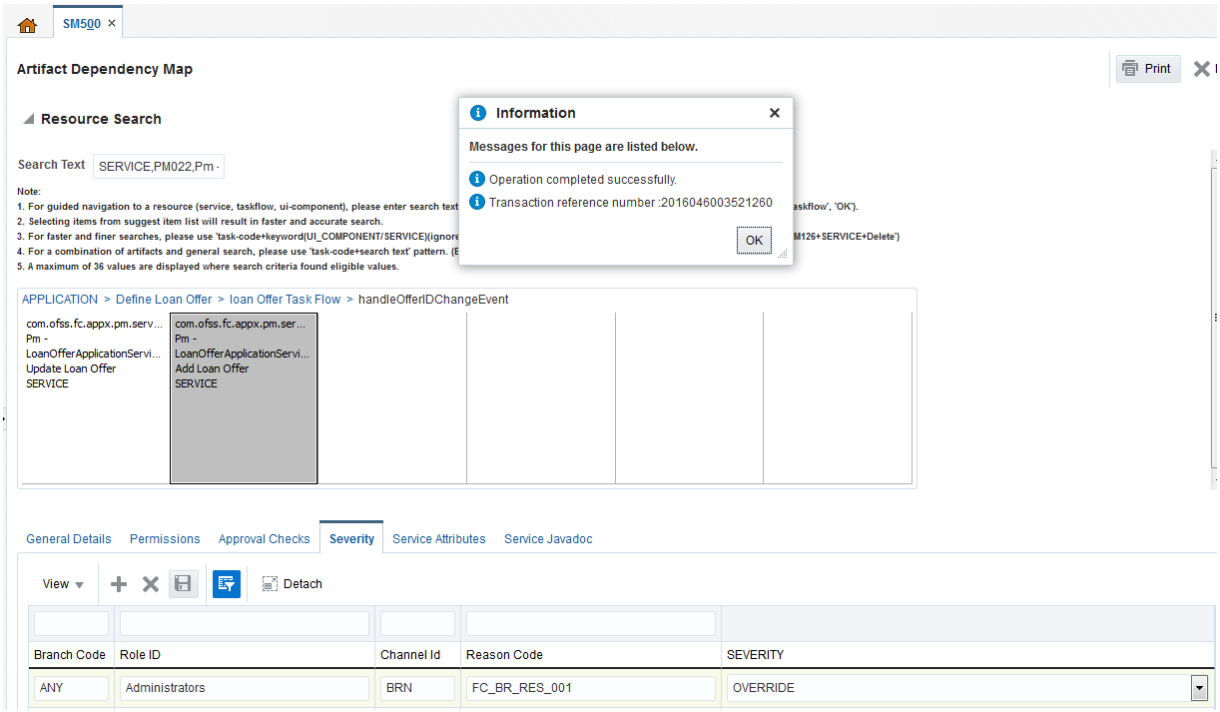
At times you may also notice that the Severity Configuration is already set up. Do not change it.

Figure 2–24 Add Severity Details



7. Save newly added severity using the **Save** button in toolbar.

Figure 2–25 Save Severity Details

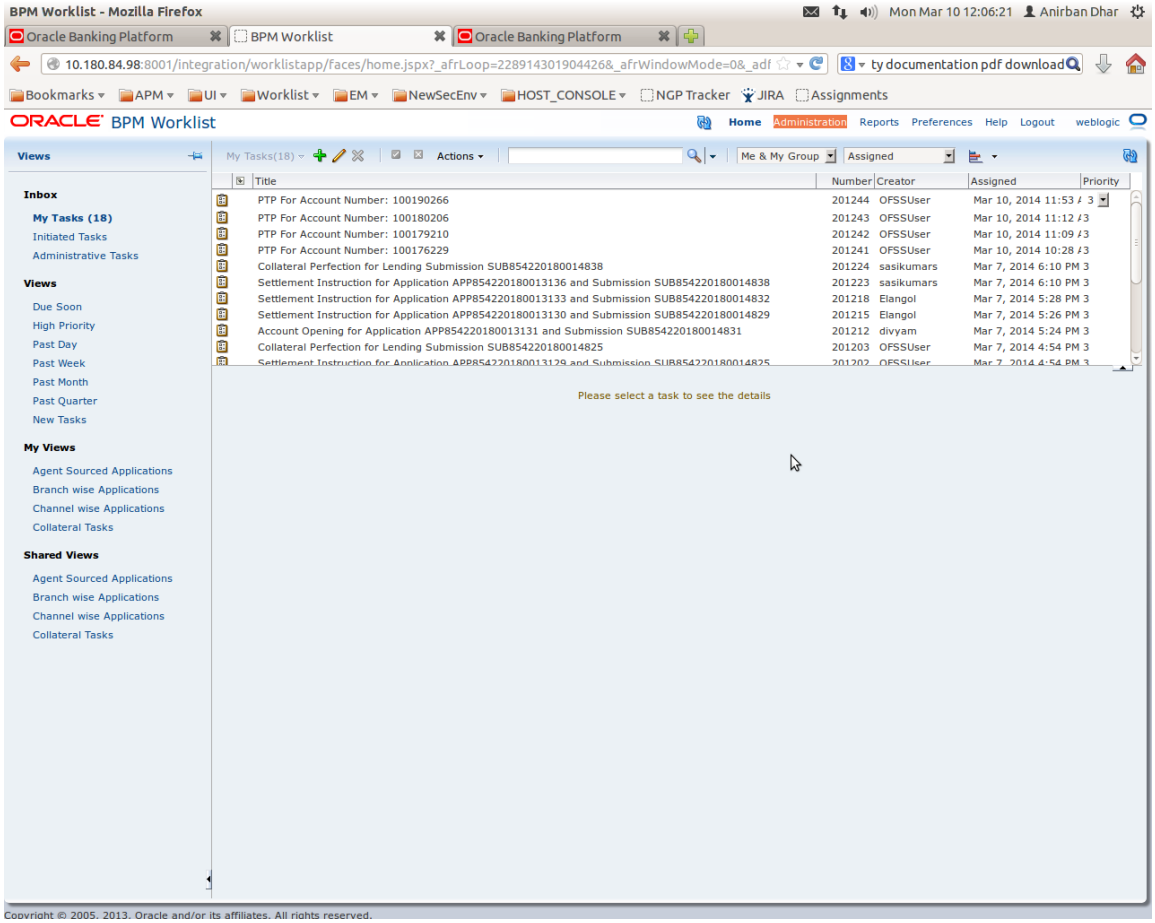


2.3 BPM Routing Rules Setup

This section describes the steps and the screens required to configure APM rules for DPA approval. Same can be referred for configuring any other routing rules based on facts available in human task payload.

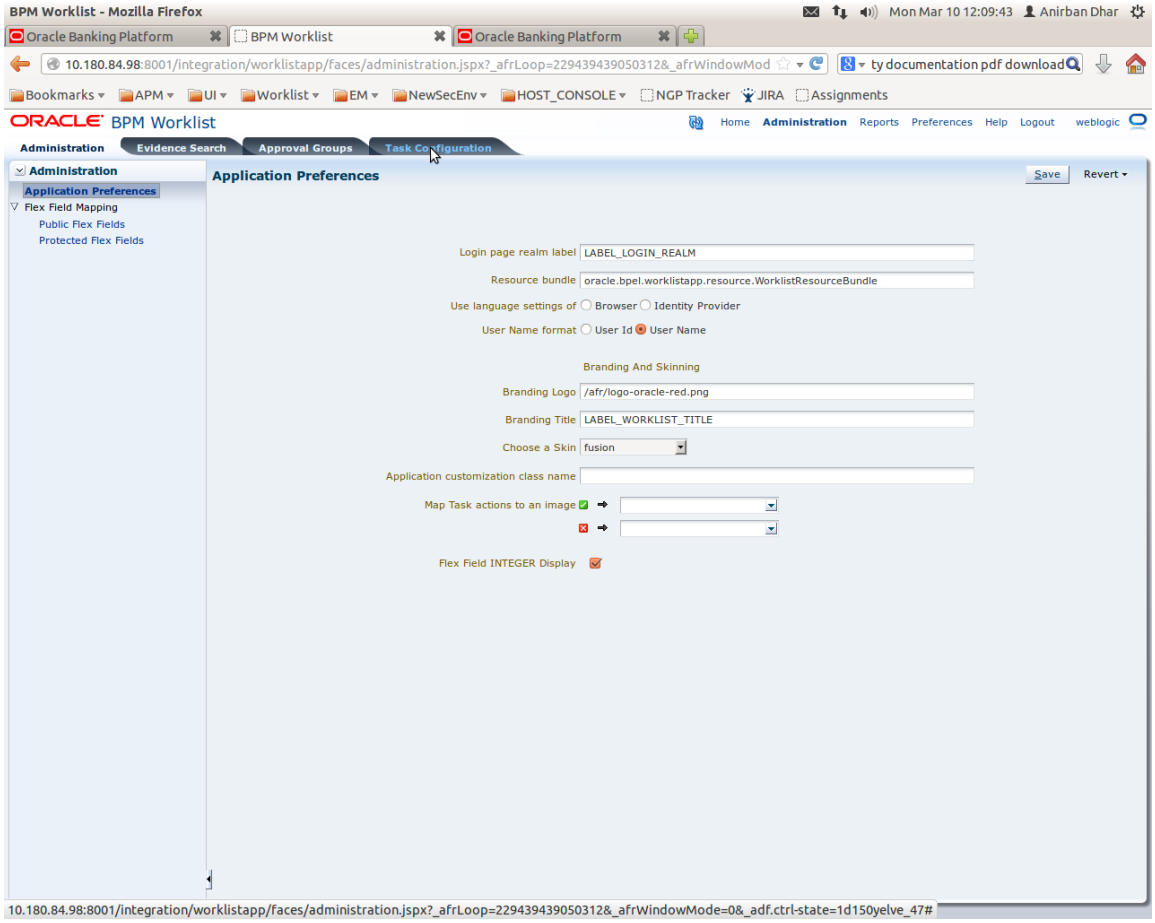
1. Log in to Worklist App using Weblogic / Weblogic1 [or any other user with administrators as role].
2. Click **Administration** link.

Figure 2–26 Worklist App - Administration Link



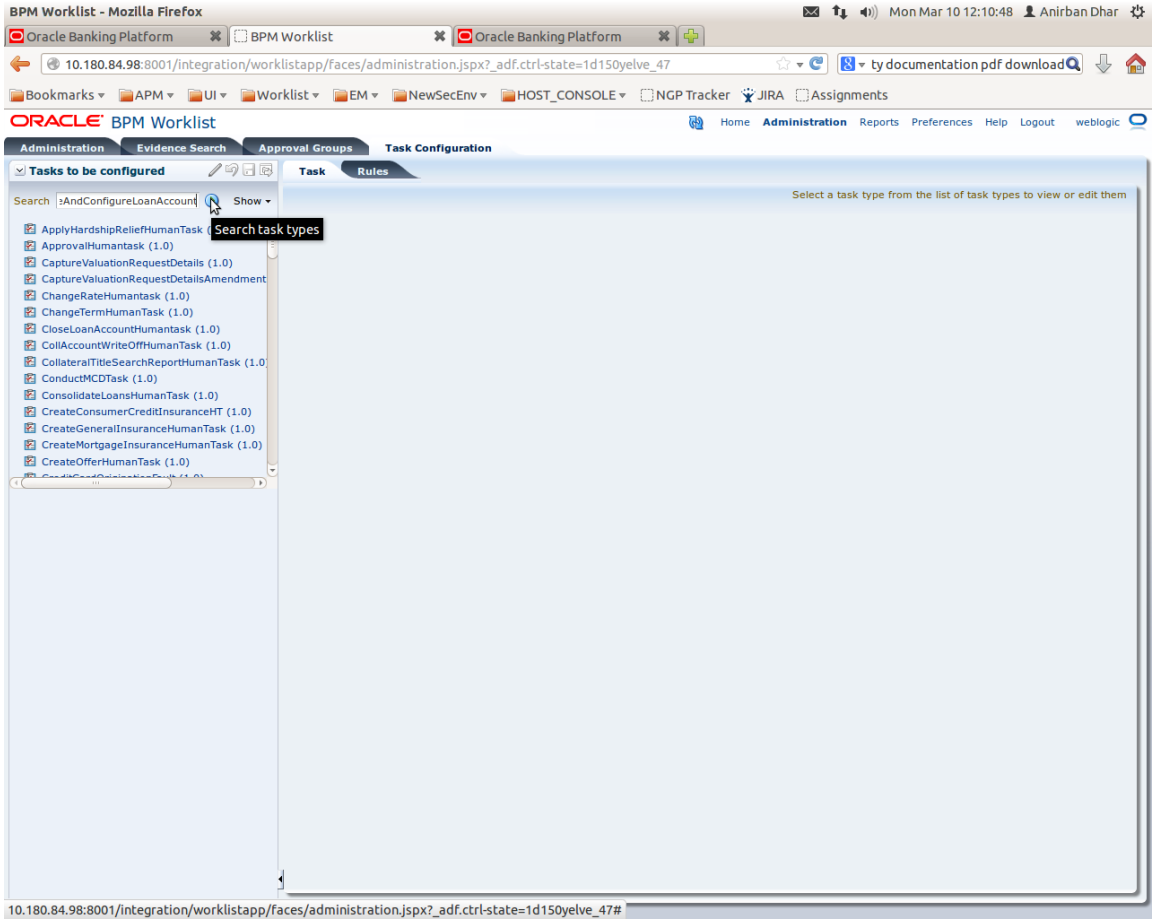
3. Navigate to **Task Configuration** tab.

Figure 2–27 Task Configuration



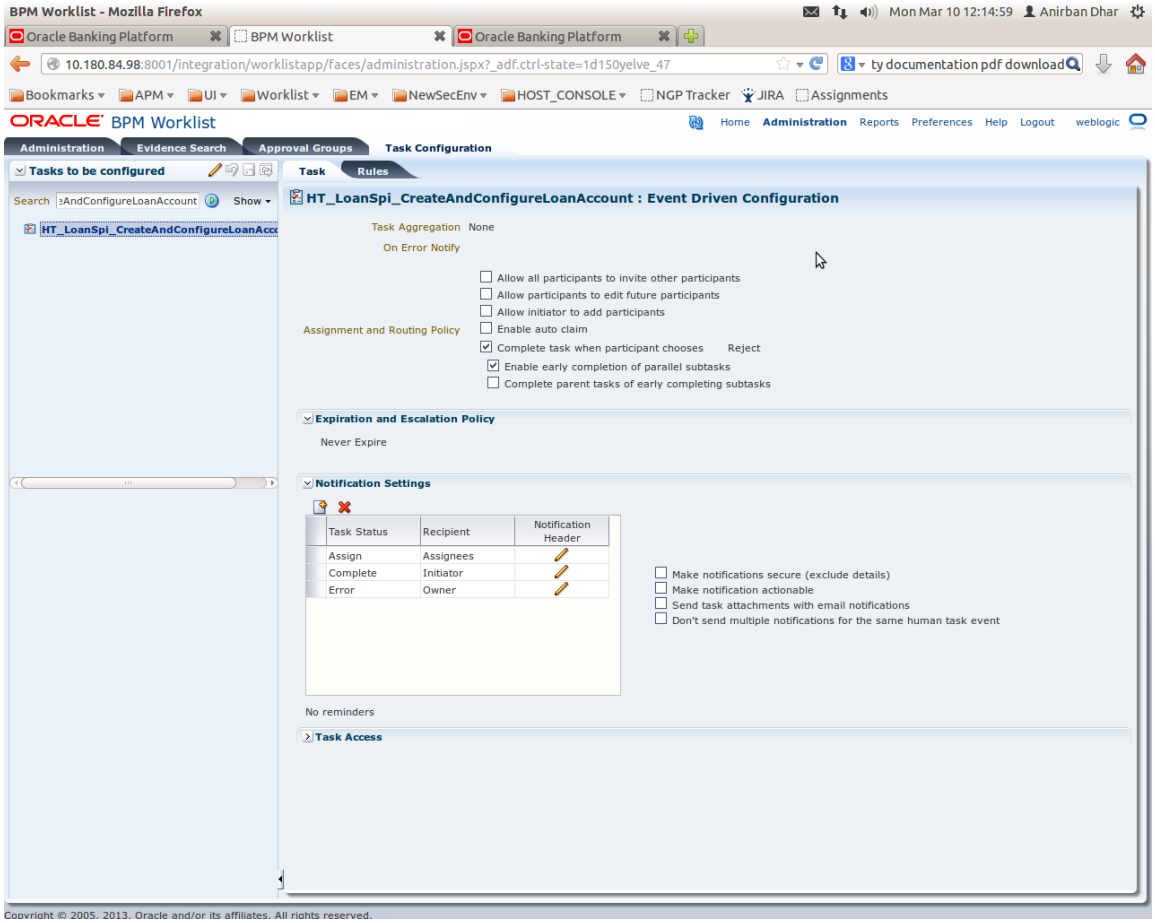
4. Search the task by inputting the name of the task in the search bar. For example, HT_LoanSpi_CreateAndConfigureLoanAccount or *CreateAndConfigureLoan*

Figure 2–28 Search Task Types



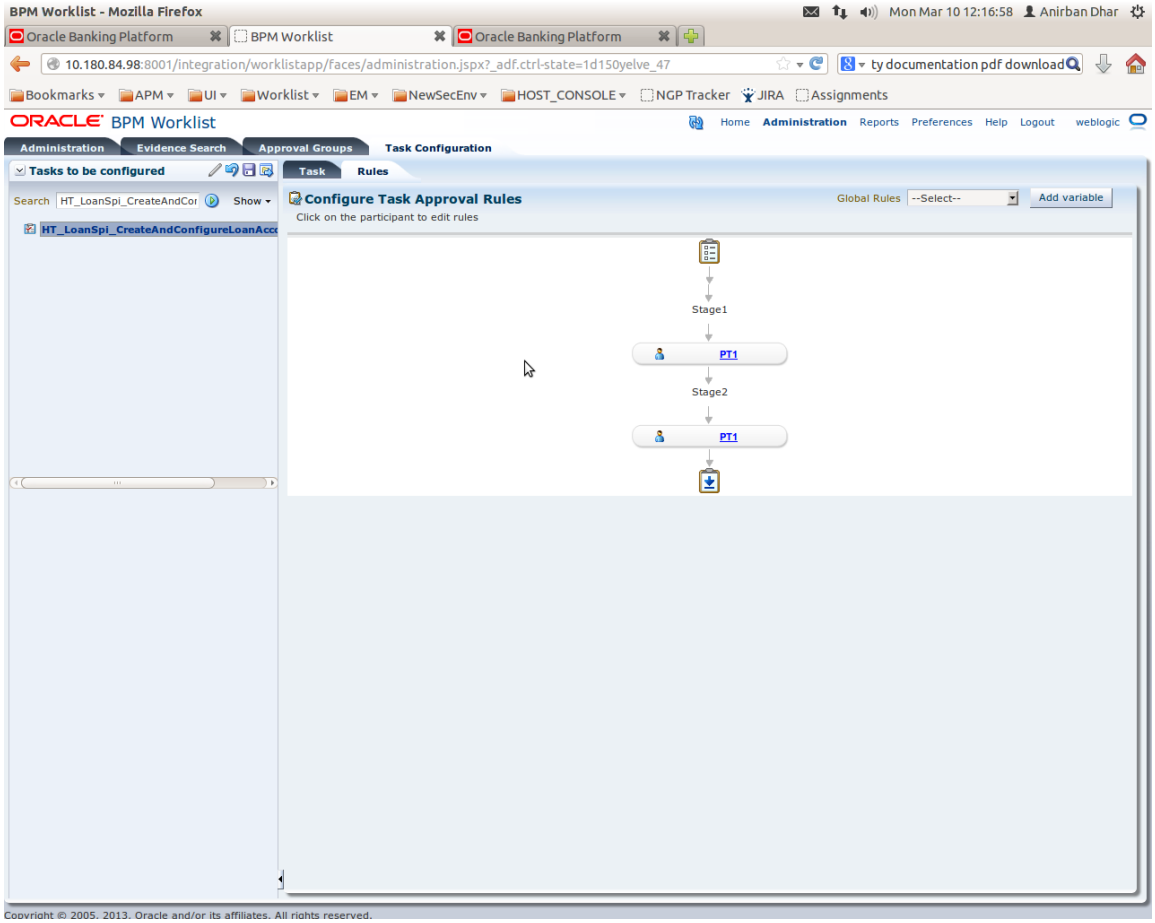
5. Click the result to open the task for editing.

Figure 2–29 Task Editing



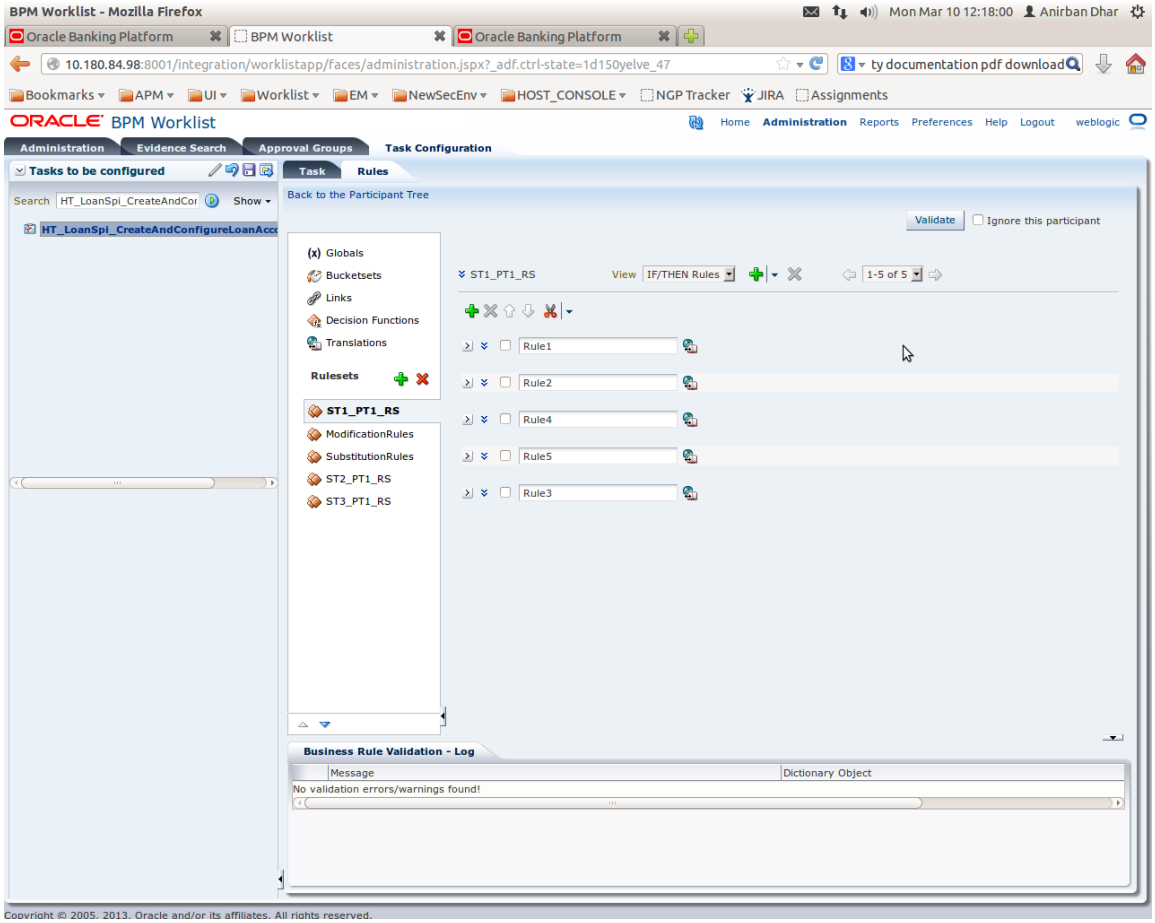
6. Click the **Edit** icon.

Figure 2–30 Configuring Rules - Edit Icon



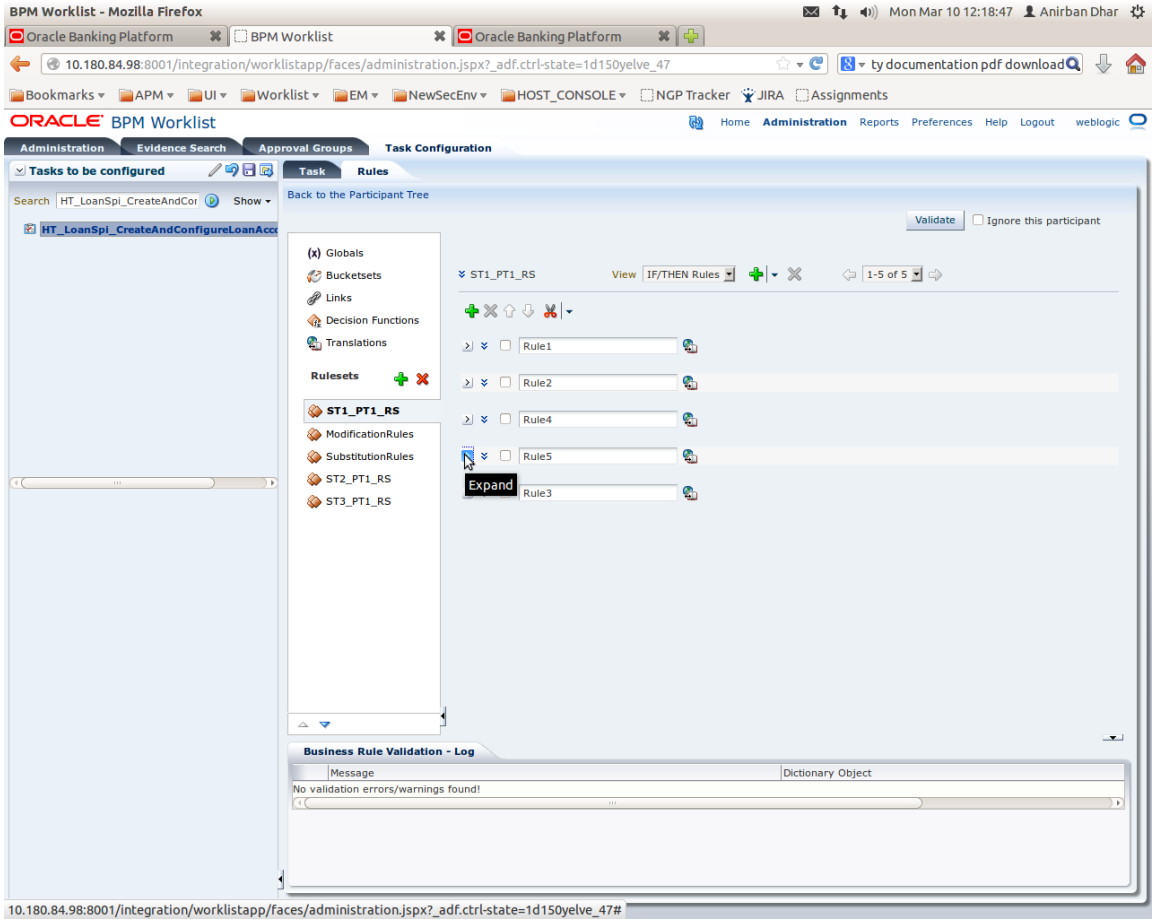
7. Navigate to **Rules** tab for configuring rules.
8. Click participant to edit rule for that stage. For example, stage 1 -> PT1)

Figure 2–31 Configuring Rules - Rules tab



9. Expand the **Rule** to configure. For example, Rule 5.

Figure 2–32 Expand Rule



10. Expand the **Advance Settings** panel.

Figure 2–33 Advanced Settings

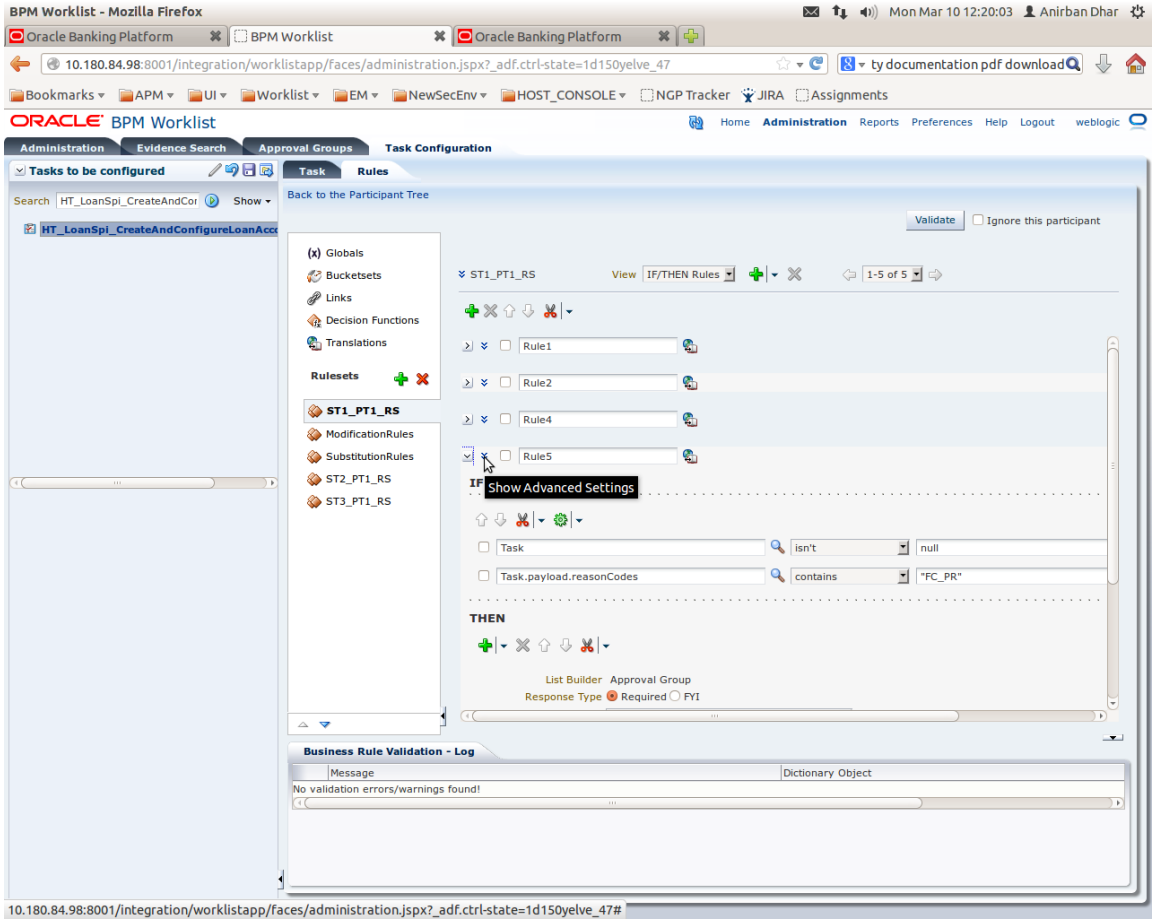
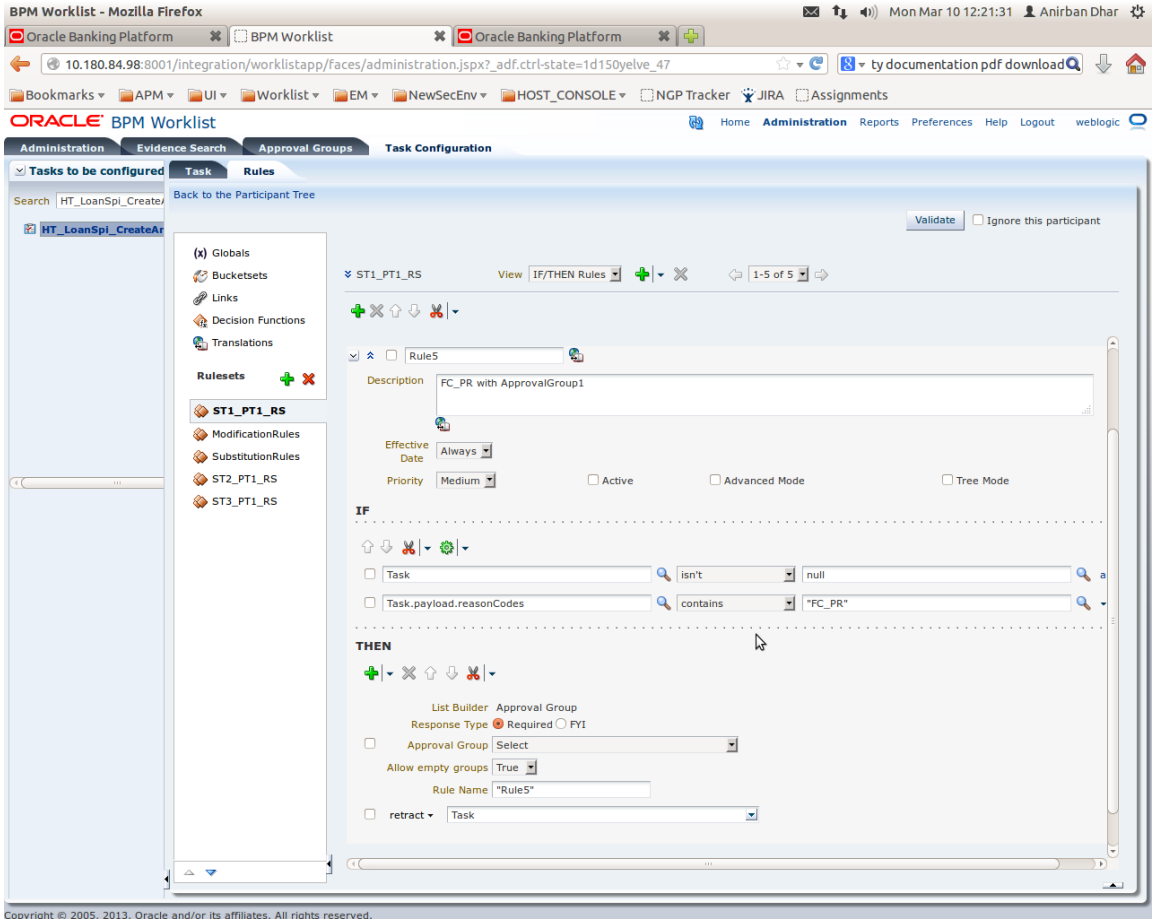
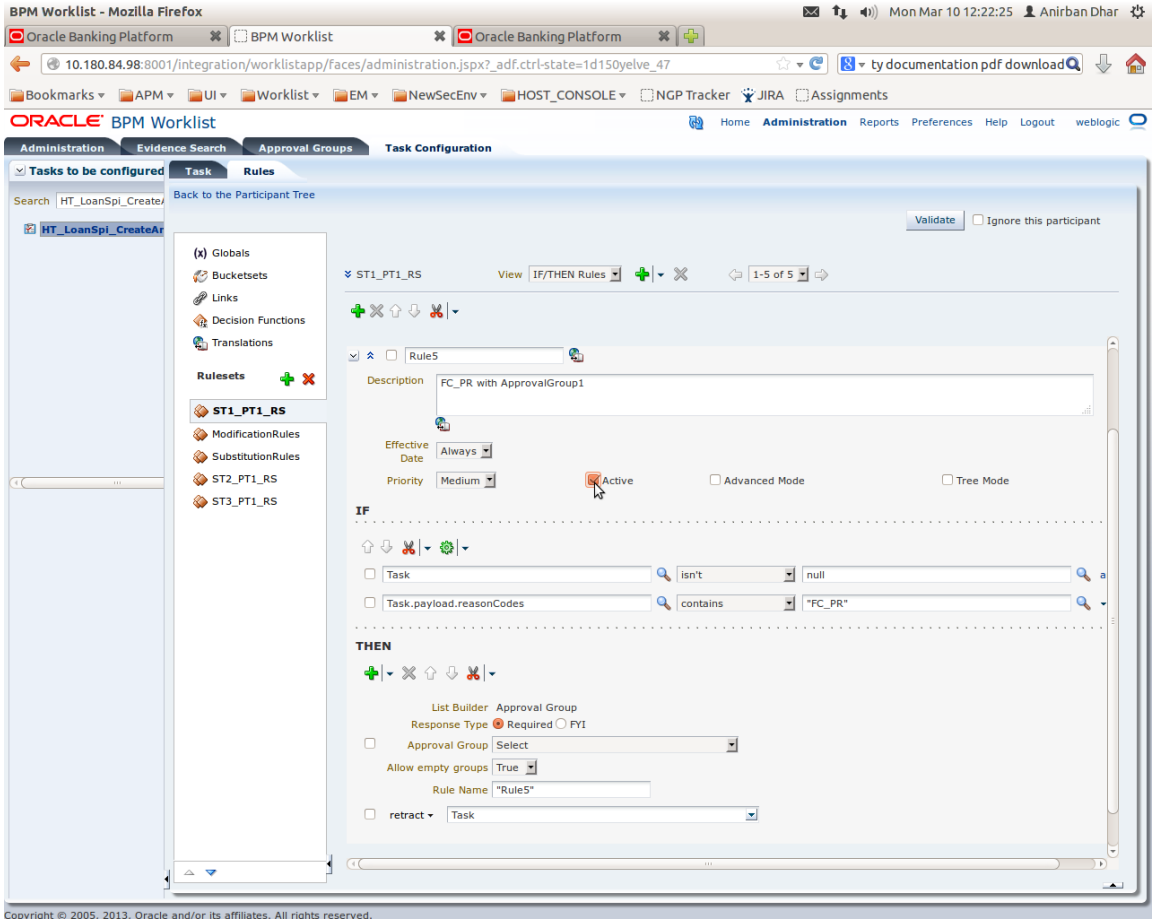


Figure 2–34 Rule Expansion



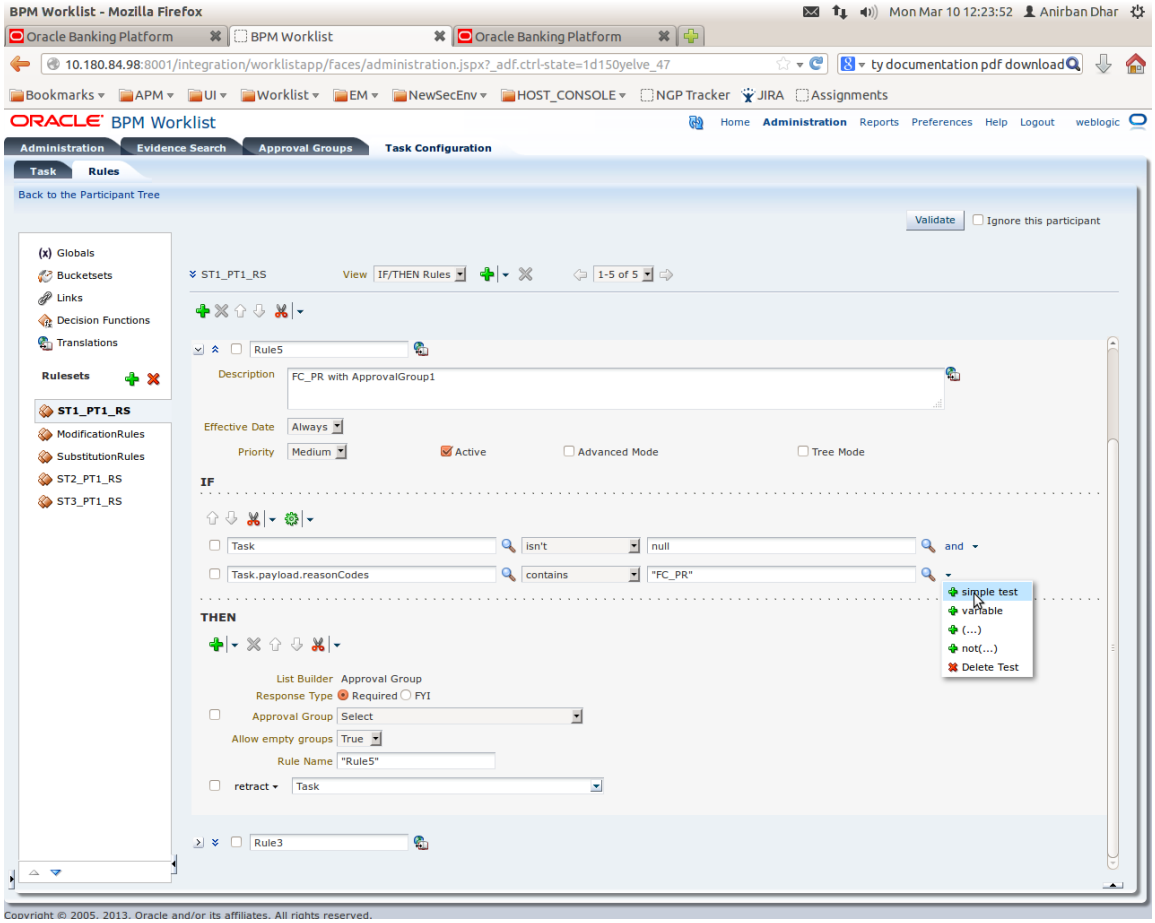
11. Click **Active** check box to enable a particular rule.

Figure 2–35 Enabling Rule



12. Click the drop-down arrow to add a new row of condition and select **Simple Test**.

Figure 2–36 Adding New Row of Condition



13. Expand **Task ->Payload** and then select the **fact**.

Figure 2–37 Expanding Payload

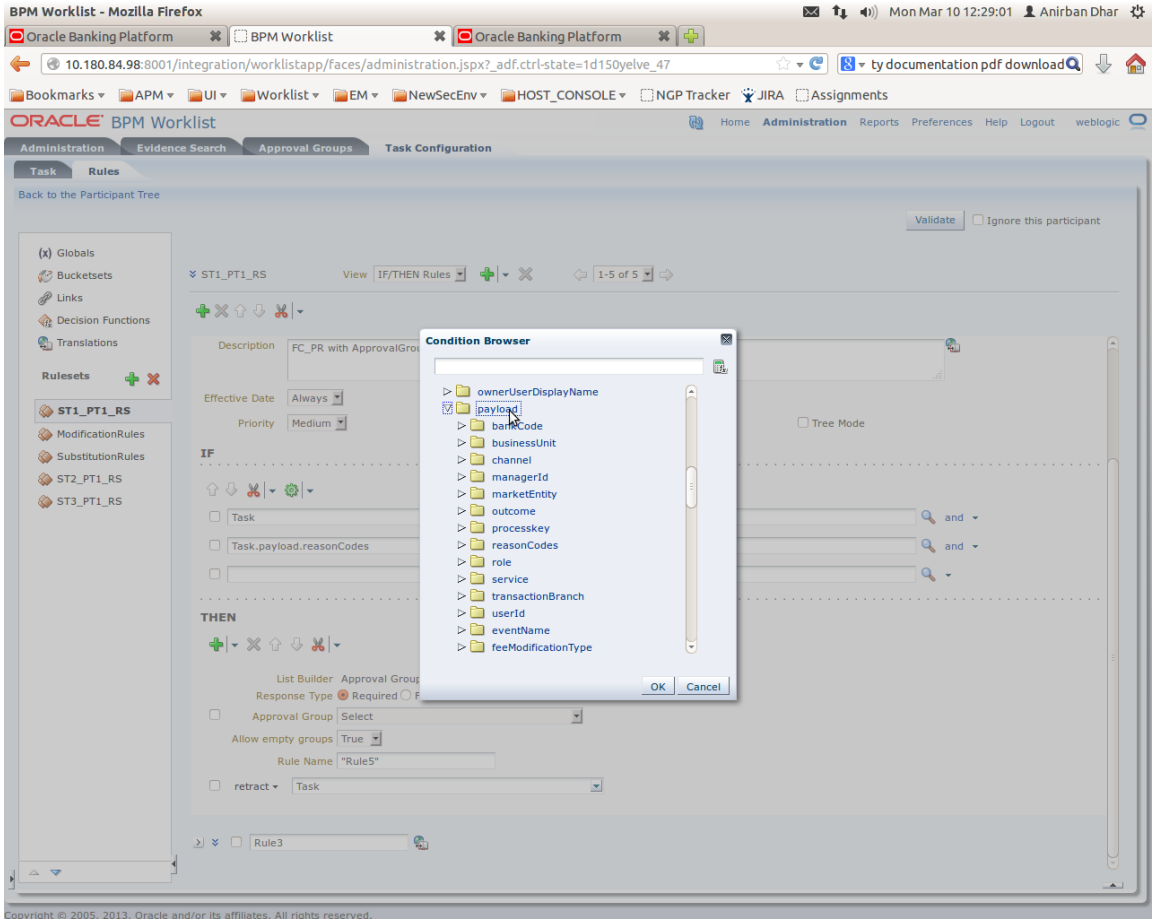
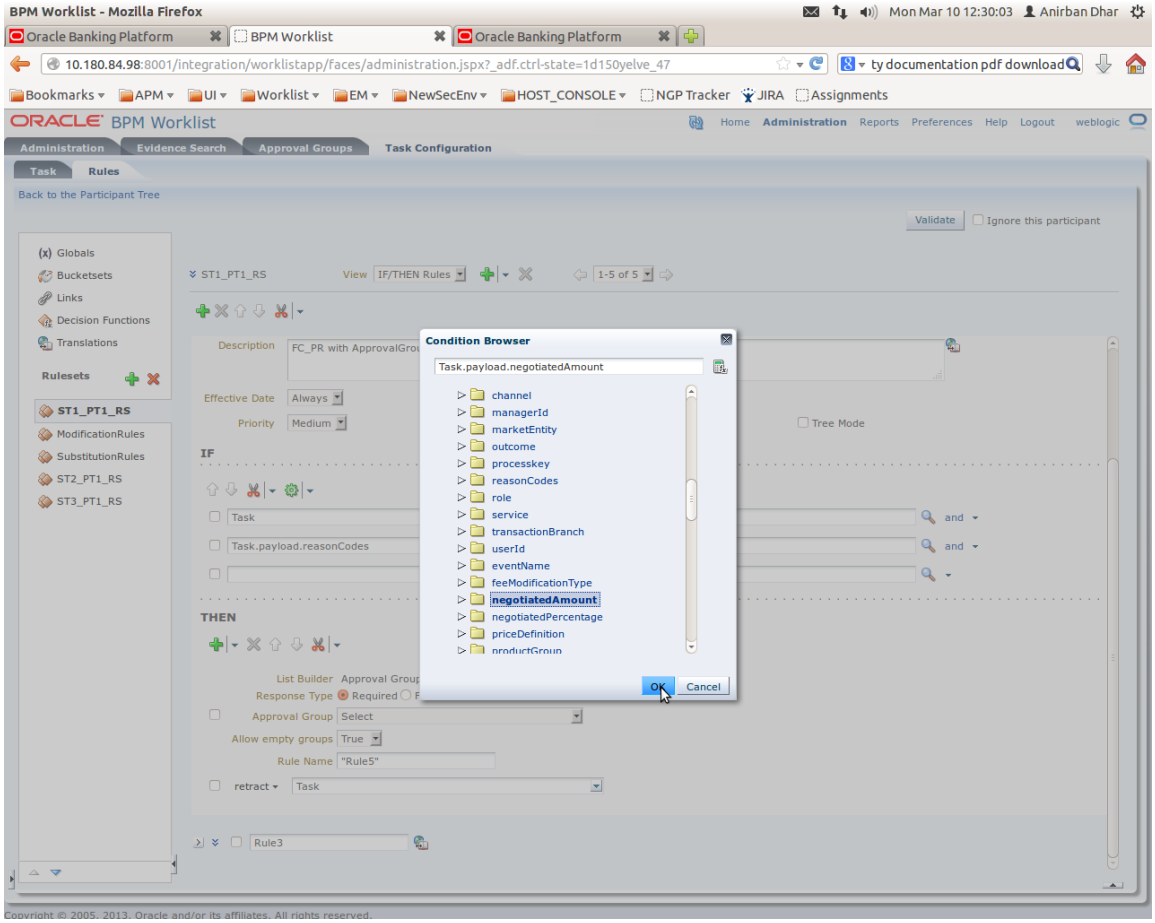
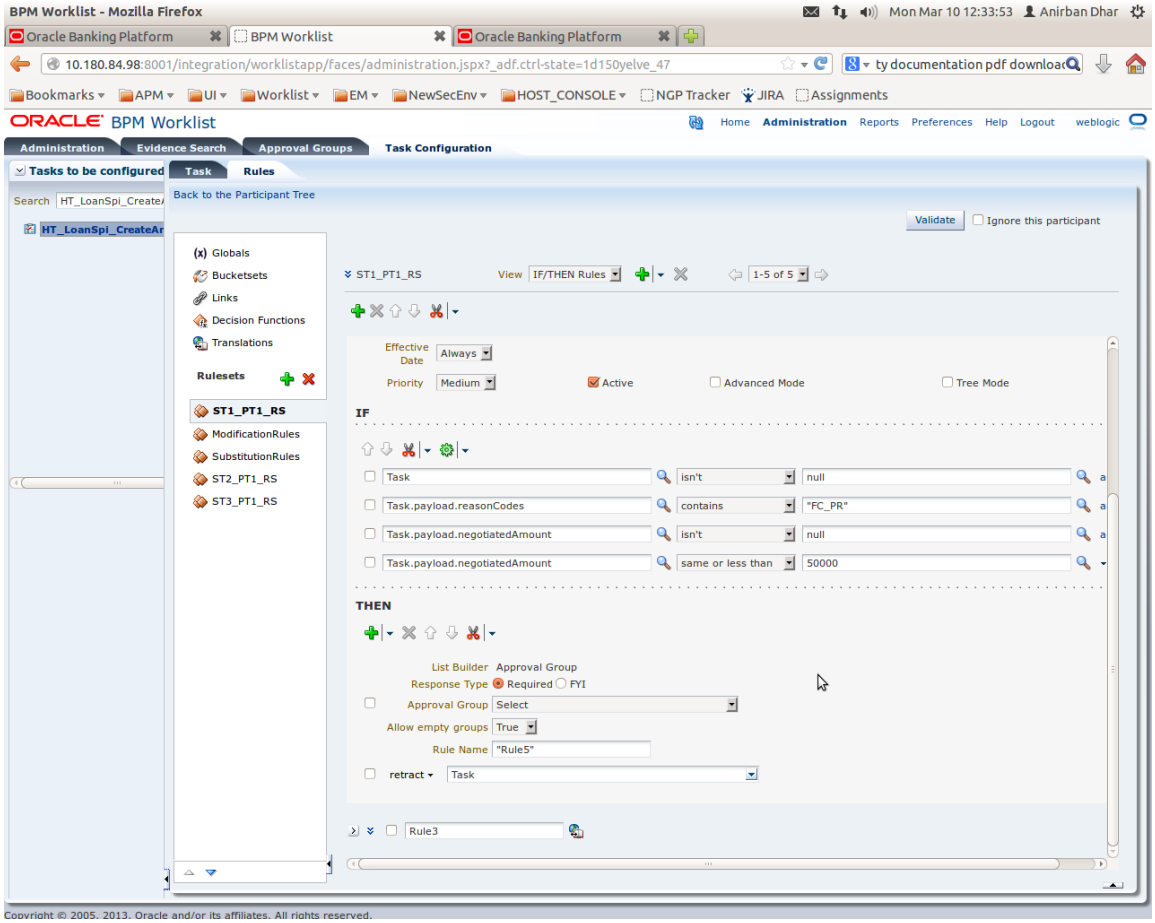


Figure 2–38 Selecting Fact



14. Update the fact value as per condition required for routing.

Figure 2–39 Updating Fact Value

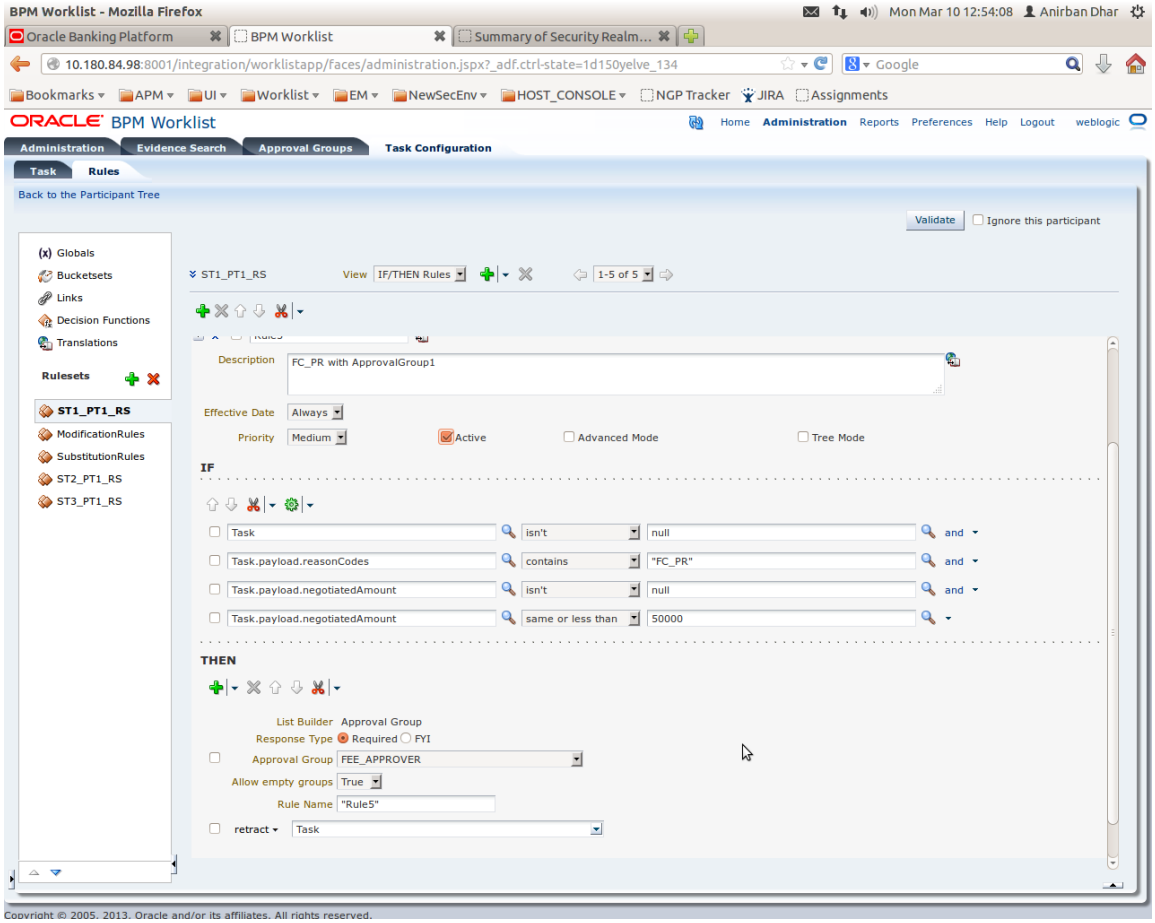


Note

Negotiated Amount should be multiplied by 10000. For example, if you want to set limit for $5 negotiated amount, then in BPM rule you need to put fact value as 50000.

15. Select **Approver Group** from the option list. For example, select FEE_APPROVER.

Figure 2–40 Select Approver Group



16. Save and commit the rule and the task.

    You can follow similar steps to configure rules on different stages. Ensure the desired rule is active.

    If no rule is evaluated, then the task will be auto rejected by workflow system.

3 Data Management

This chapter describes data related activities to be performed as an administrator.

3.1 Batch Execution

Batch Execution refers to bulk processing of records to perform business operations in real-time environment. Business operations include complex processing of large volumes of information, that is most efficiently processed with minimal or no user interaction using Batch Execution.

The batch process is run through the **End of Day (Fast path: EOD10)** page with a varied combination of category, job code and job type for a particular business day.

This section explains the steps involved in Batch Execution.

> **Note**
>
> To view the detailed procedure to be followed in the application page **End of Day (Fast Path: EOD10)**, see its context-sensitive help in the application.

3.1.1 Database Backup

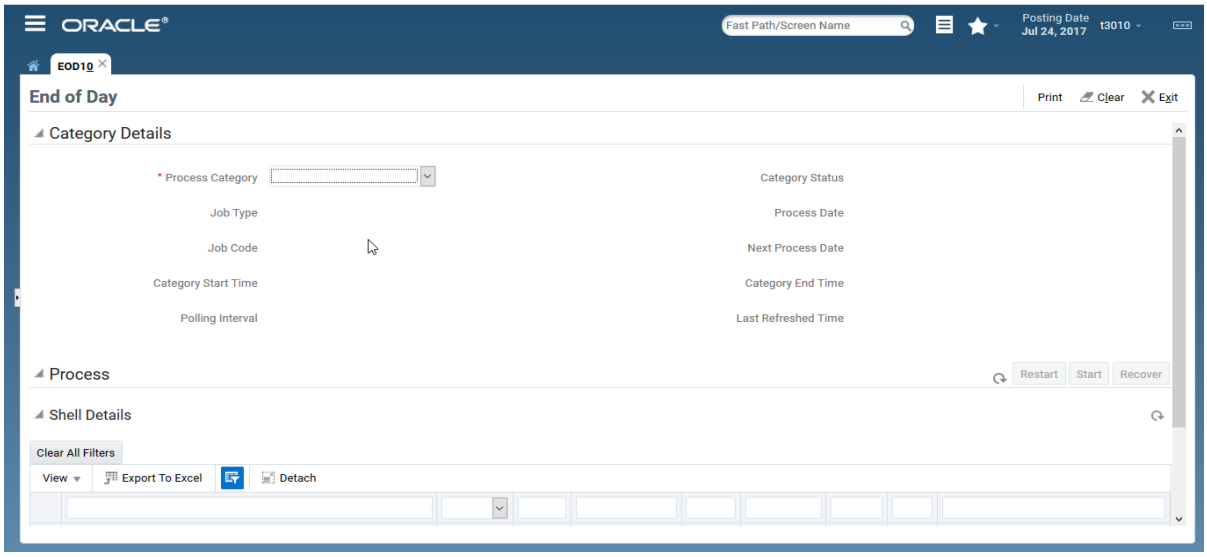
Perform Database Backup before starting with the Batch Execution.

3.1.2 Navigate to End of Day Page

To navigate to the End of Day page:

1. Log in to Admin Application.
2. Navigate to *End of Day* page either by entering the Fast path **EOD10** or through the menu **Administration > End of Day.**

Figure 3–1 End of Day (Fast path: EOD10)



3.1.3 Cutoff Category Execution

This category marks the logical closure of business in the system to ensure that all online transactions during batch run get processed with the next process date.

To execute the Cutoff category:

1. Select the relevant **Category Details** as shown in the table below:

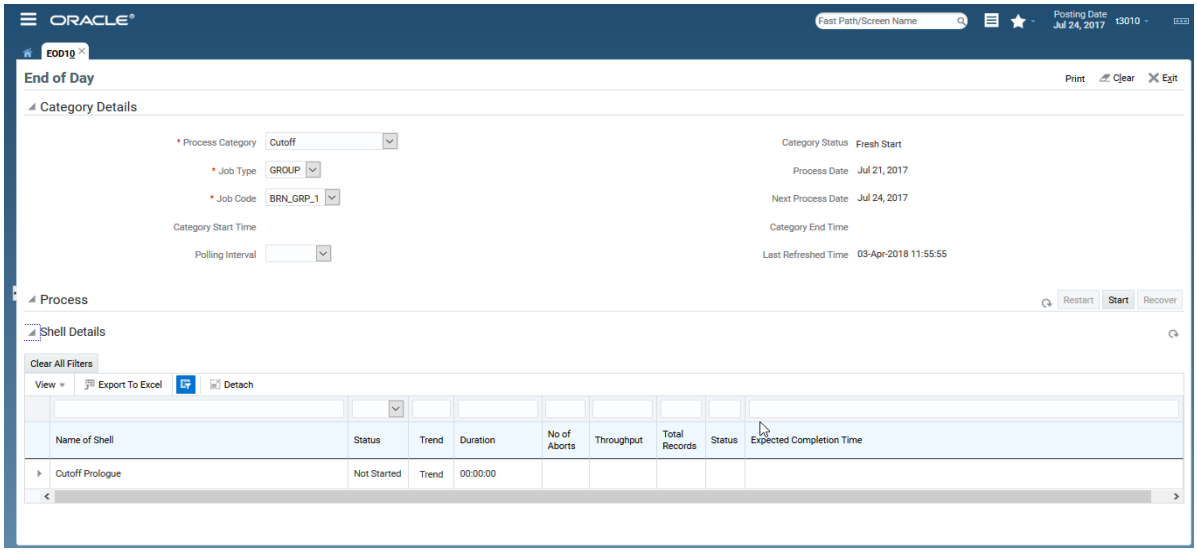
Process Category	Cutoff
Job Type	GROUP
Job Code	BRN_GRP_1

2. Click the **Refresh** button. The rest of the **Category Details** and the **Process Details** appear.

   Here, the **Shell State** is *Not Started.*

   The **Category Status** is *Fresh Start*.

Figure 3–2 Cutoff Category - Not Started



3. Verify the **Process Date** and the **Next Process Date.**
4. Click the **Start** button to begin the execution.

   Once the process starts the **Category Status** and the **Shell State** of currently running process display *In Progress*.

Figure 3–3 Cutoff Category - Start

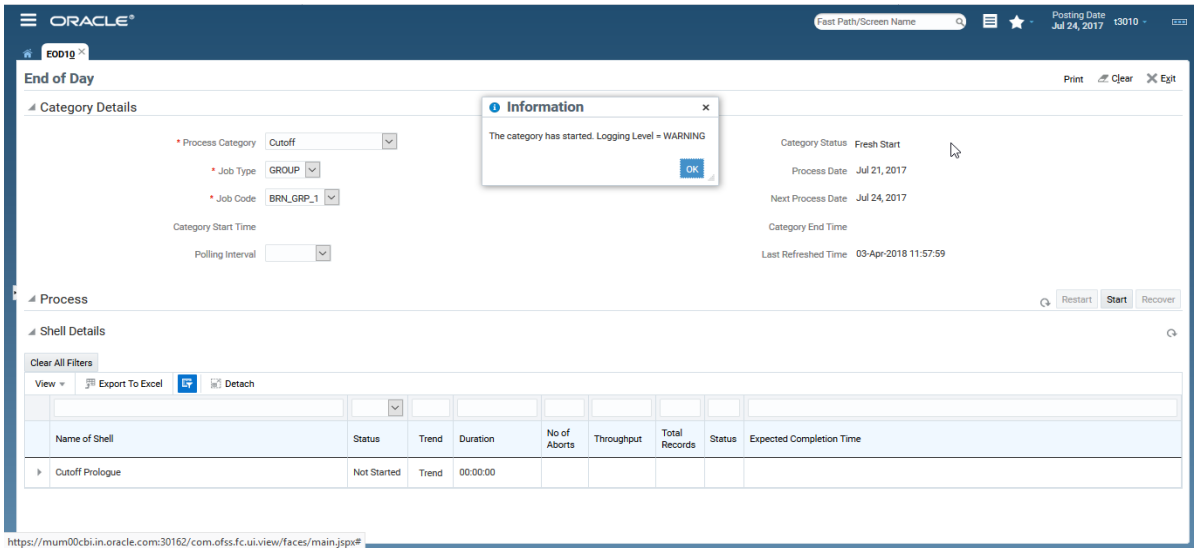
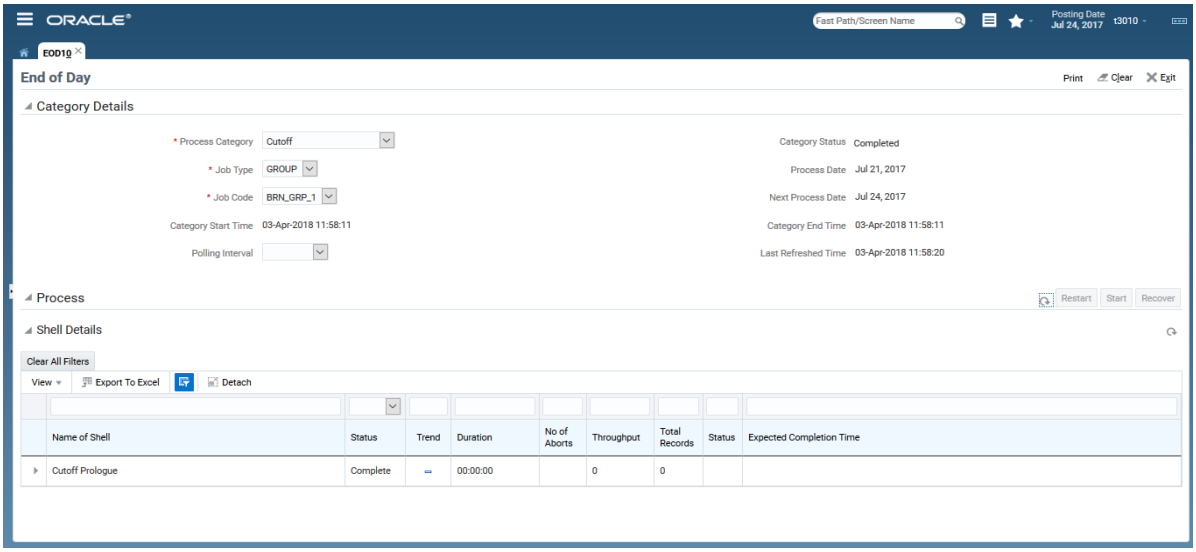


Figure 3–4 Cutoff Category - Complete



5. On completion of the category, the **Category Status** and the **Shell State** of all the processes display *Completed.*

3.1.4 End of Day (EOD) Category Execution

This category performs the tasks required to mark closure of a business day in a bank. For example, value date cleaning, instruction expiry, auto disbursement instruction execution, bundle expiry, report generation and so on. Each task or transaction is performed by a shell in a predefined dependency and sequence.

To execute the End of Day category:

1. Select the relevant **Category Details** as shown in the table below:

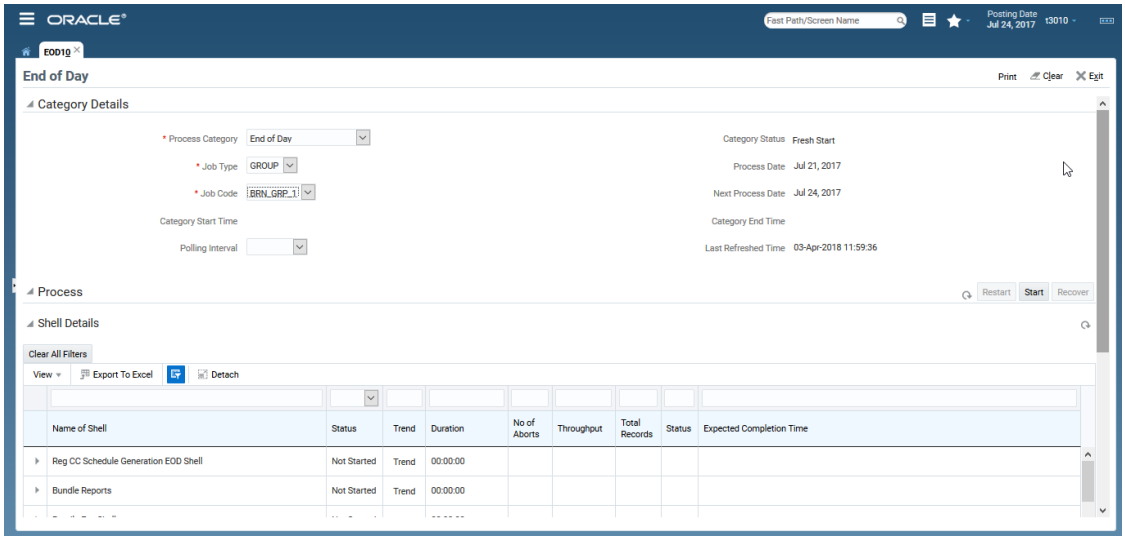
Process Category	End of Day
Job Type	GROUP
Job Code	BRN_GRP_1

2. Click the **Refresh** button. The rest of the **Category Details** and the **Process Details** appear.

   Here, the **Shell State** is *Not Started.*

   The **Category Status** is *Fresh Start.*

Figure 3–5 EOD Category - Not Started



3. Verify the **Process Date** and the **Next Process Date.**
4. Click the **Start** button to begin the execution.

   Once the process starts the **Category Status** and the **Shell State** of currently running process display *In Progress*.

Figure 3–6 EOD Category - Start

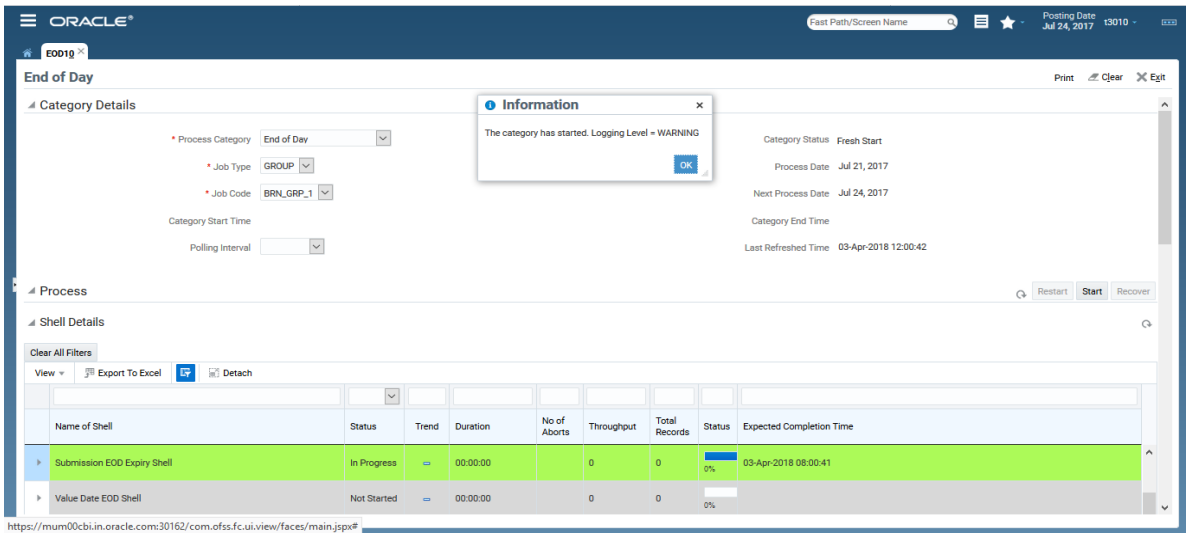
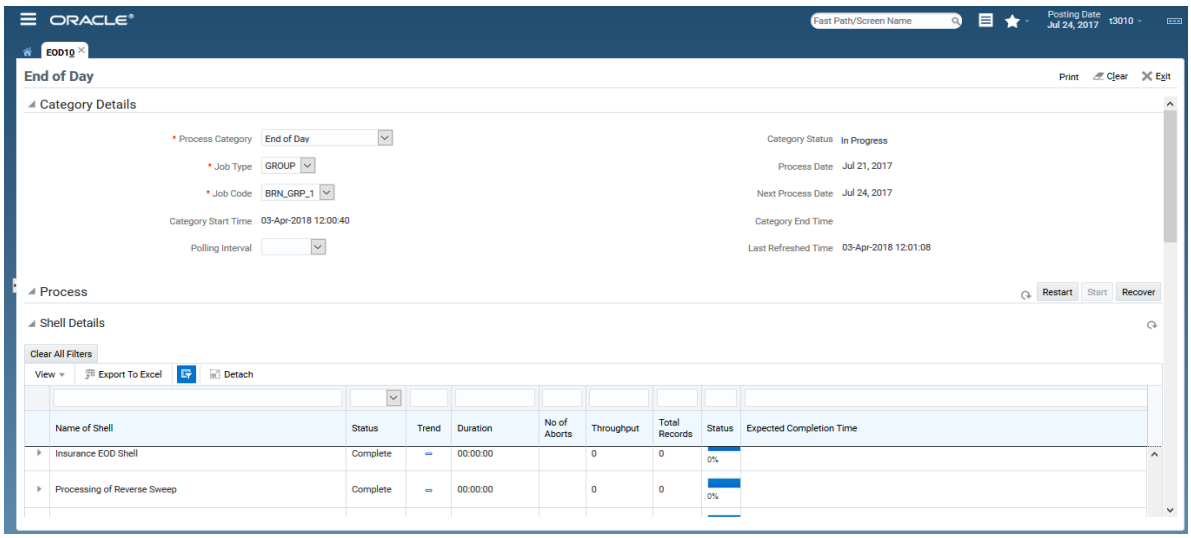
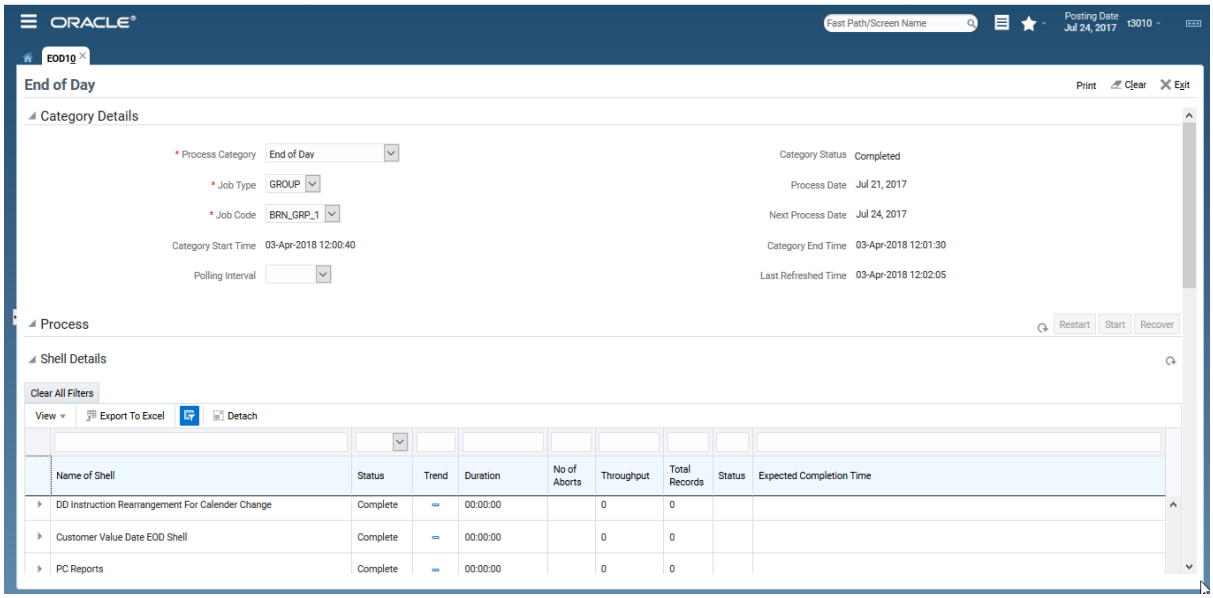


Figure 3–7 EOD Category - In Progress



5. On completion of the category, the **Category Status** and the **Shell State** of all the processes display *Completed.*

Figure 3–8 EOD Category - Complete



3.1.5 Beginning of Day (BOD) Category Execution

This category performs the tasks required for opening a business day in a bank. For example, loan account charging, periodic repayment instruction execution, period fee charging, and report generation. Each task or transaction is performed by a shell in a predefined dependency and sequence.

To execute the Beginning of Day category:

1. Select the relevant **Category Details** as shown in the table below:

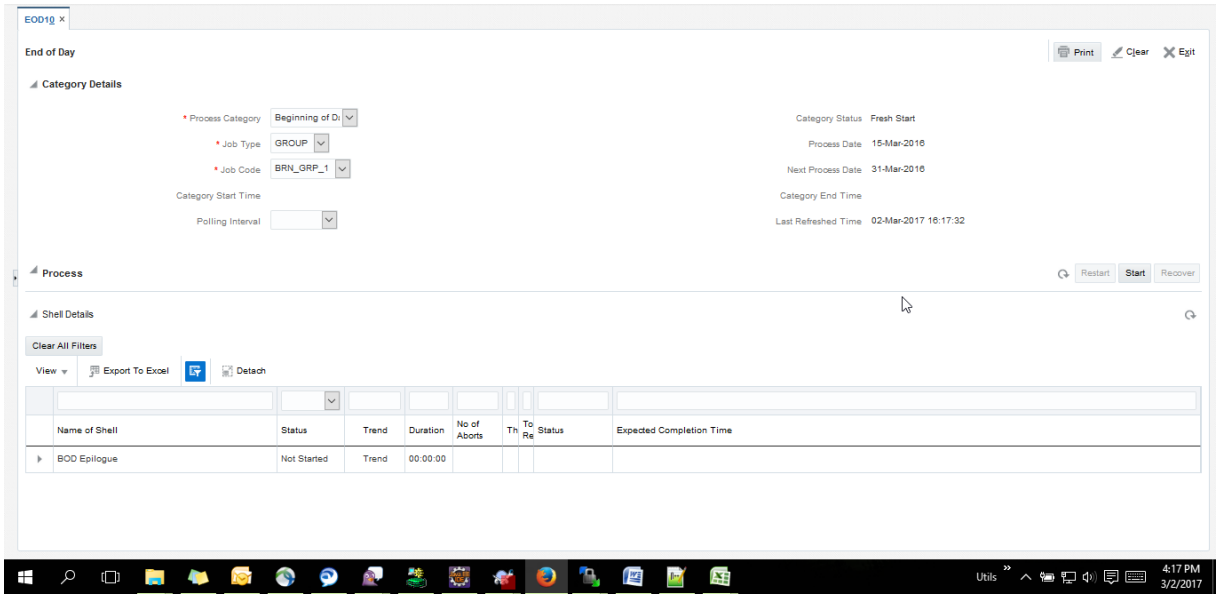
Process Category	Beginning of Day
Job Type	GROUP
Job Code	BRN_GRP_1

2. Click the **Refresh** button. The rest of the **Category Details** and the **Process Details** appear.

   Here, the **Shell State** is *Not Started.*

   The **Category Status** is *Fresh Start.*

Figure 3–9 BOD Category - Not Started



3. Verify the **Process Date** and the **Next Process Date.**
4. Click the **Start** button to begin the execution.

   Once the process starts the **Category Status** and the **Shell State** of currently running process display *In Progress*.

Figure 3–10 BOD Category - Started

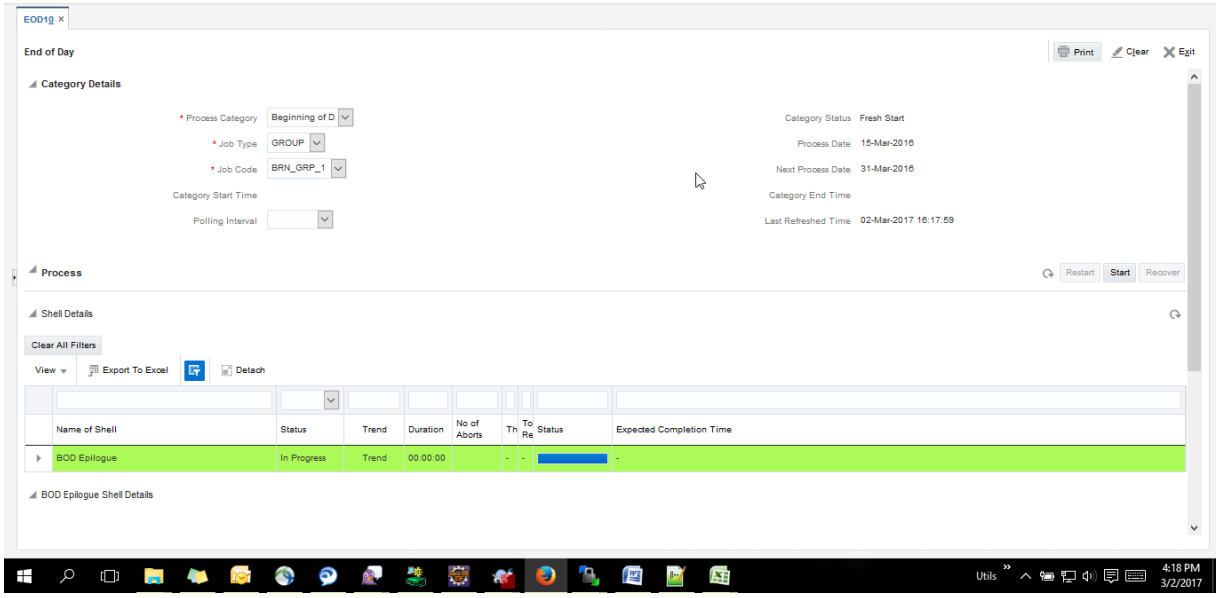
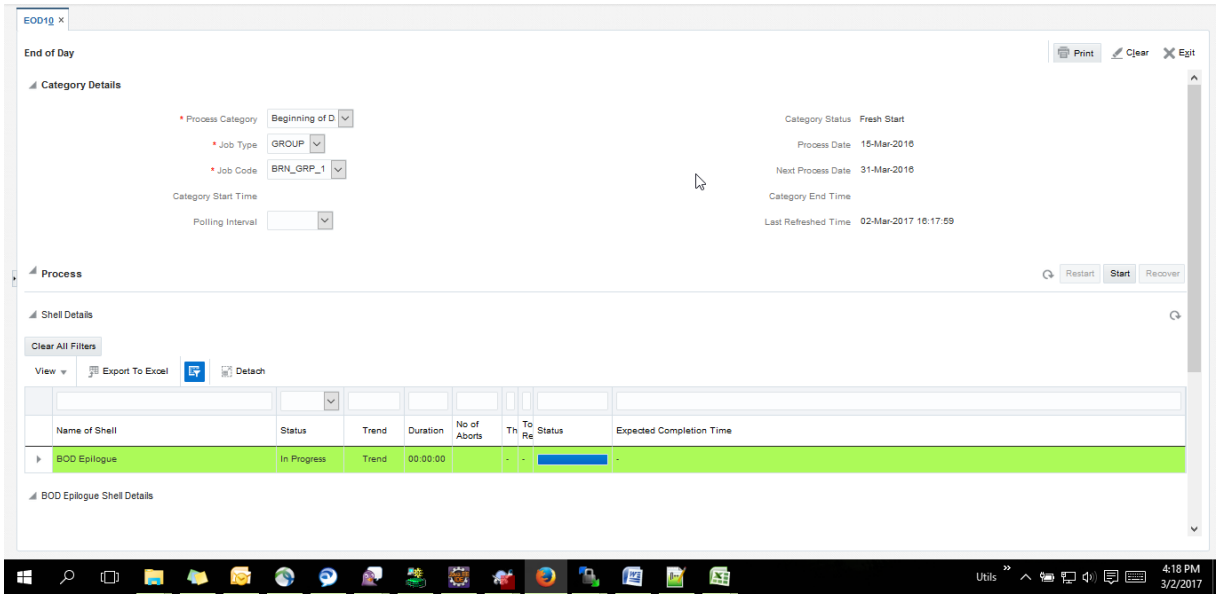
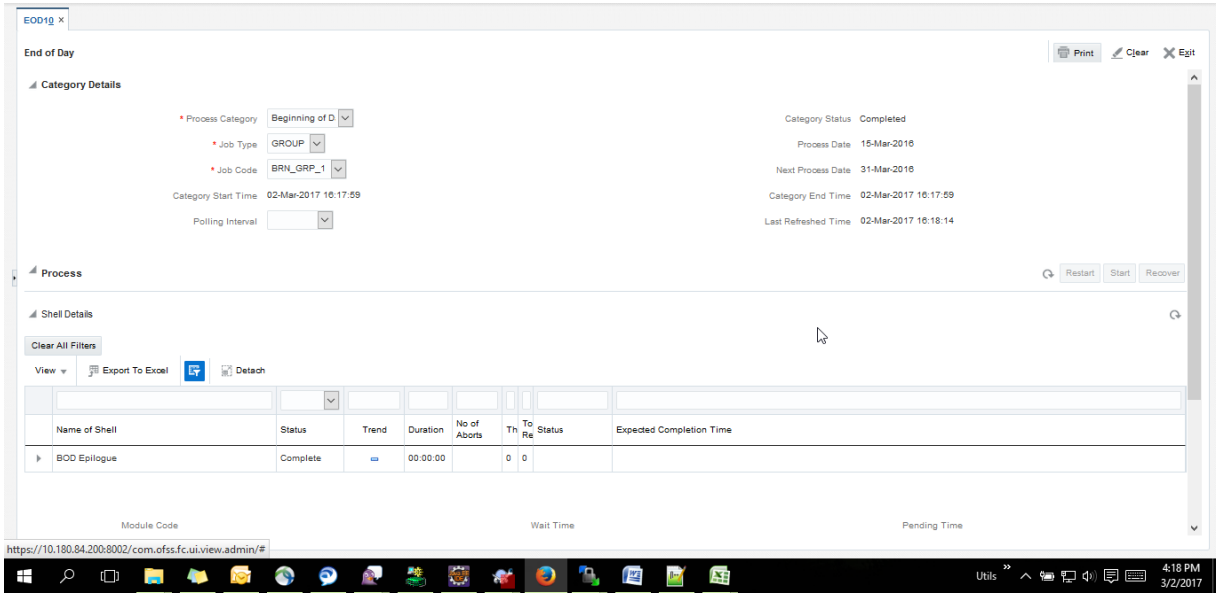


Figure 3–11 BOD Category - In Progress



5. On completion of the category, the **Category Status** and the **Shell State** of all the processes display *Completed.*

Figure 3–12 BOD Category - Completed



3.2 Batch Exception Recovery

Batch Exception Recovery refers to mechanism to allow support and business users perform actions on the records that were skipped during batch execution. During batch execution, if the number of failures due to business exception is less than pre-configured threshold, such records are skipped for future processing.

The batch exception recovery can be done using the Batch Exception Recovery (Fast Path: OPA007) page. It is recommended that user in support or operations role, checks this page after every batch processing is completed for any PENDING records.

This section explains the steps involved in Batch Exception Recovery.

Batch exception recovery actions can be broadly classified in two categories:

- Actions for Support/Operations user (Performed on Batch Exception Recovery page)
- Actions for Business user (Viewed in worklist application and actioned using application screens, data patches.)

In its entire life cycle, the batch exception record will go through the above mentioned actions starting with PENDING and ending with either IGNORED or REPROCESSED. Support or Operations user acts on exception record using the Batch Exception Recovery page.

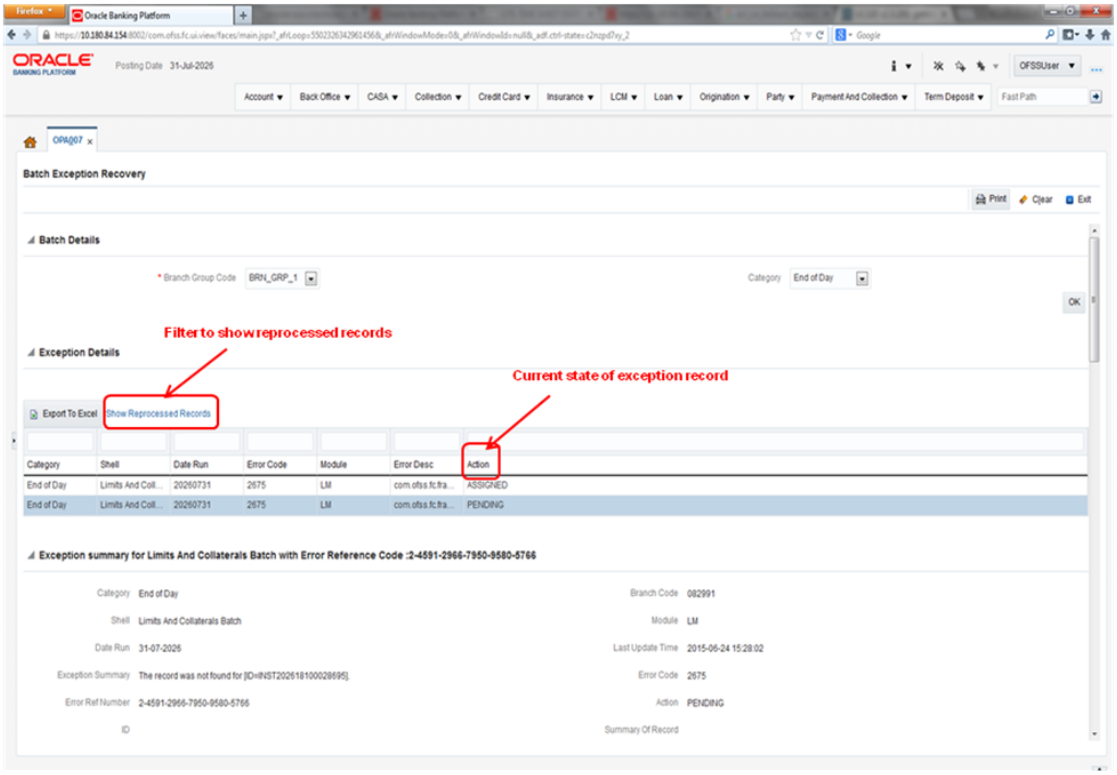
To navigate to the Batch Exception Recovery page:

1. Log in to Admin Application.
2. Navigate to Batch Exception Recovery page either by entering the Fast path OPA007 or through the menu Administration --> Batch Exception Recovery.
3. Select the relevant Category Details as shown in the following table:

Branch Group Code	BRN_GRP_1
Category	End of Day

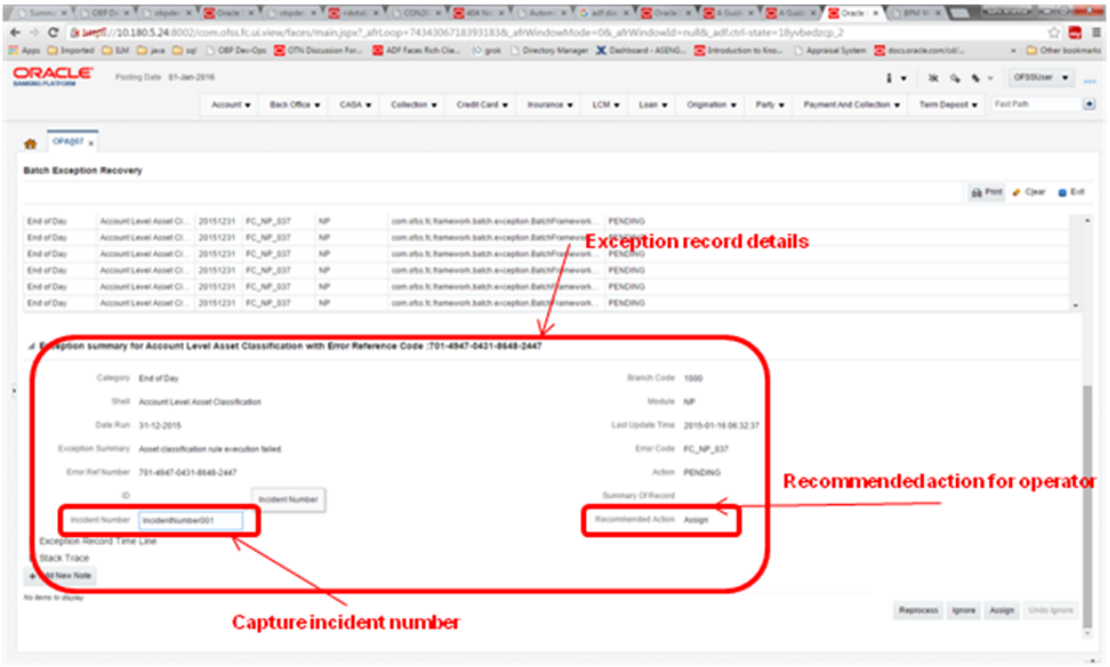
4. Click OK. The Exception Details appear.

Figure 3–13 Exception Details



5. Select an exception record. The additional details such as Stack Trace and Comments appear. One of the important attributes is Recommended Action for the operator.

Figure 3–14 Exception Record Details



6. Check the Stack Trace and Comments. It is recommended that if the current action on an exception record is PENDING and there are no Comments, click Assign to create a task for business user to take appropriate corrective actions on the exception record. Also, look for the Recommended Action. By looking at the Stack Trace, if the support or operator users find a similar previous incident, they can capture the same in the Incident Number field as shown in the above figure.

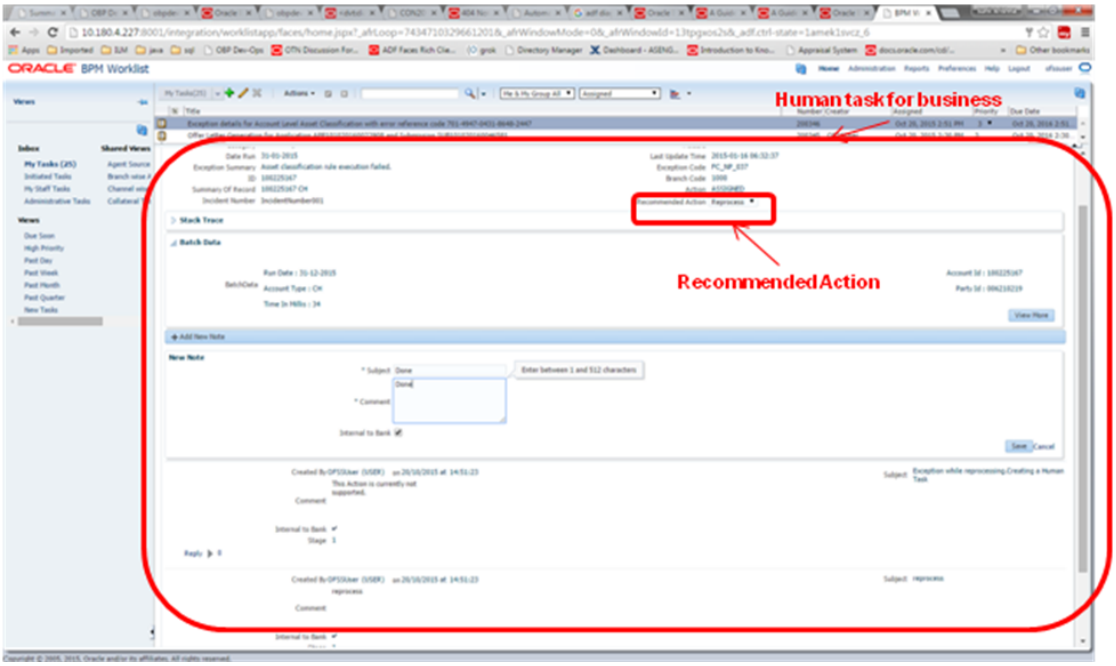
> **Note**
>
> It is mandatory to capture valid meaningful Comments while performing any action on the exception record.

Business user acts on exception record using the Worklist Application

To navigate to the Worklist page:

1. Log in to worklist application.
2. All the exception records with action as ASSIGNED will appear as a task in the worklist. Select the task to act on.

Figure 3–15 Exception record in Worklist application



3. Click Claim to claim the task.
4. Check the Stack Trace, Batch Data, Incident Number and Comments.
5. Perform appropriate actions using relevant screens, data patches.
6. Capture comments in Comments section. These comments will be used by the support user to further act on the exception record.
7. Select the mandatory Recommended Action for the support or operator user.
8. Click Done to complete the task. The exception record moves into PENDING state and will be visible to the support user to take further action.

> **Note**
>
> It is mandatory to capture valid meaningful Comments while performing any action on the exception record.

4 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.

4.1 Common Services Day 0 Setup

The Common Services setup includes the following sections.

4.1.1 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)
- Business Group (Fast path: CS02)
- Bank Parameters (Fast path: CS03)
- Branch Parameters (Fast path: CS06)
- Country Codes (Fast path: CS09)
- Financial Cycle (Fast path: CS10)
- 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)

Note

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

4.1.1.1 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.

4.1.2 Currency Maintenances

The Currency Services are a part of the common services 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)
- Currency Branch Parameters (Fast path: CY04)
- Currency Denomination (Fast path: CY05)
- Currency Rate Types (Fast path: CY06)

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

4.1.3 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.

4.2 OBEPM Setup

OBEPM is a flexible and competent framework for defining products. It has list of tasks to be performed for defining a new product. Each task should be completed parallel or sequentially by respective departments in a

bank. It can be mandatory, conditional or non mandatory. The product manufacturing is complete if the respective mandatory tasks are complete.

Prerequisites

Following are the prerequisites for Day 0 Maintenances:

- Asset Classification (AC) Plans Maintenance (Fast path: NP002)
- Asset Classification (AC) Codes Maintenance (Fast path: NP003)
- Document Type Definition (Fast path: CNM01)
- Global Parameter (Fast path: LCM48)
- LTV Matrix (Fast path: LCM52)
- Facility Category (Fast path: LCMS53)

Day 0 Maintenances

The following maintenances must be completed as a part of bank and branch set up:

- Define CASA Bank Policy (Fast path: PM002)
- Define TD Bank Policy (Fast path: PM003)
- Define Loan Bank Policy (Fast path: PM004)
- Define Bundle Bank Policy (Fast path: PM005)
- Define Hardship Relief Policy (Fast path: PM006)
- Define Statement Policy (Fast Path: PM007)
- Define Dormancy Policy (Fast path: PM008)
- Define Credit Policy (Fast path: PM009)
- Define Product Group
- Define Interest Rule (Fast path: PM011)
- Define TD Interest Payout Plan (Fast path: PM012)
- Define CASA Product
- Define Loan Product
- Define TD Product
- Define Credit Card Product
- Define Product Interest Linkage (Fast path: PM017)
- Link Dependent Offers (Fast path: PM018)
- Define Bonus Interest Parameters (Fast path: PM019)
- Define CASA Offer
- Define TD Offer
- Define Loan Offer
- Define Credit Card Offer
- Define Campaigns (Fast path: PM024)

- Link Offers for Principal Offset Facility (Fast path: PM025)
- Define Offer Bundle (Fast path: PM026)
- Define Transaction Restriction (Fast path: PM027)
- Link Product Group to Business Group (Fast path: PM028)
- Define Unclaimed Policy (Fast path: PM029)
- Define Domain Category Settlement Mode (Fast path: PM030)
- Define Product Settlement Mode (Fast path: PM031)
- Define Debit Card Feature (Fast path: PM039)
- Define Affinity (Fast path: PM042)
- Define Question Sets (Fast path: PM046)
- Define Investment Product
- Define Investment Offer
- Define Insurance Product
- Define Insurance Offer
- Installment Rule Details (Fast path: PM058)
- Loan Schedule Type (Fast path: PM059)

Note

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

5 Application Monitoring Using Administration Application

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

5.1 Dynamic Monitoring Service (DMS)

The aim is to monitor different channels involved in performing transactions with application. The monitoring parameters consists of channels, services, trends (current behavior of execution), and time metrices. 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.

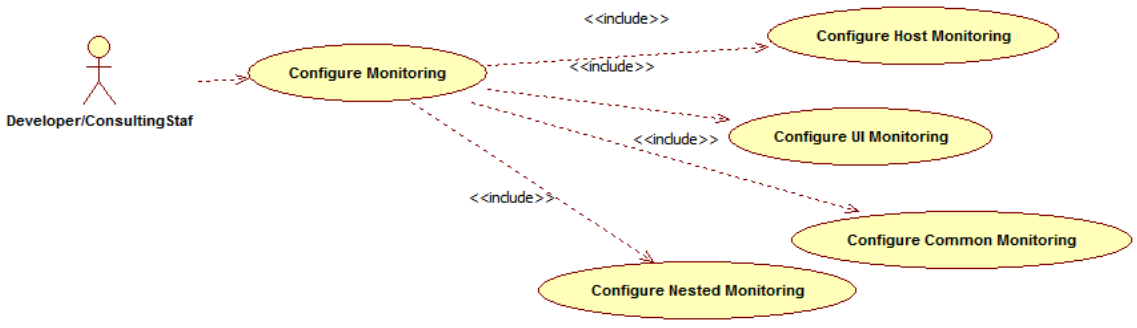
5.1.1 Usage

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 the system. The configuration can be made either for available services or for new services.

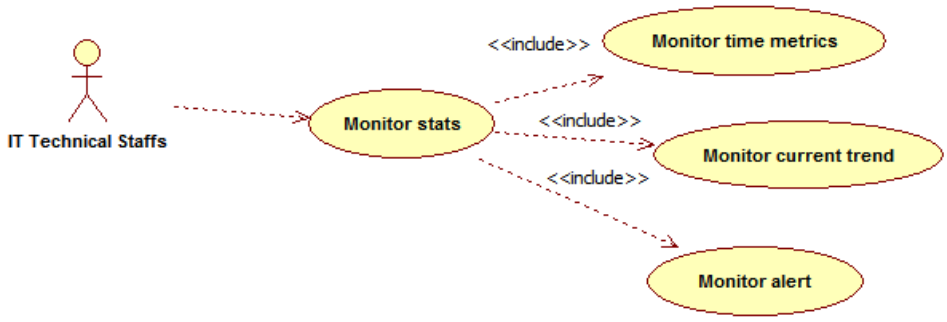
Figure 5–1 Developers



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 5–2 IT Technical Staff



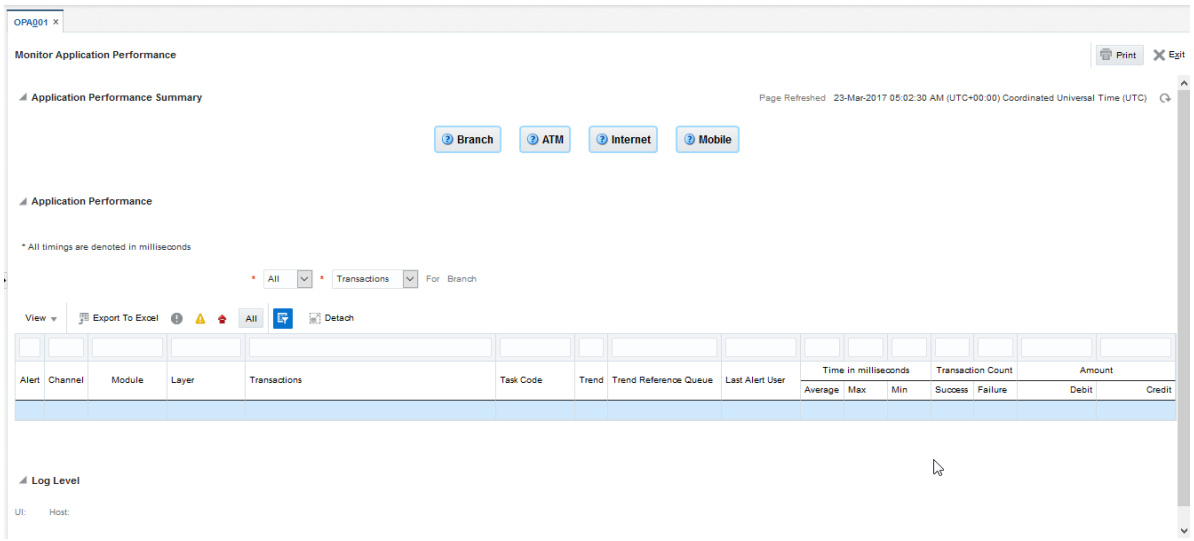
5.1.2 Monitoring Application using the OPA001 page

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.

5.1.2.1 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 5–3 Monitoring Application Performance



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

5.1.2.1.1 Application Performance Summary

This section gives the information about the different channels 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 5–4 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

5.1.2.1.2 Log Level

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

Figure 5–5 Log Level

5.1.2.1.3 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

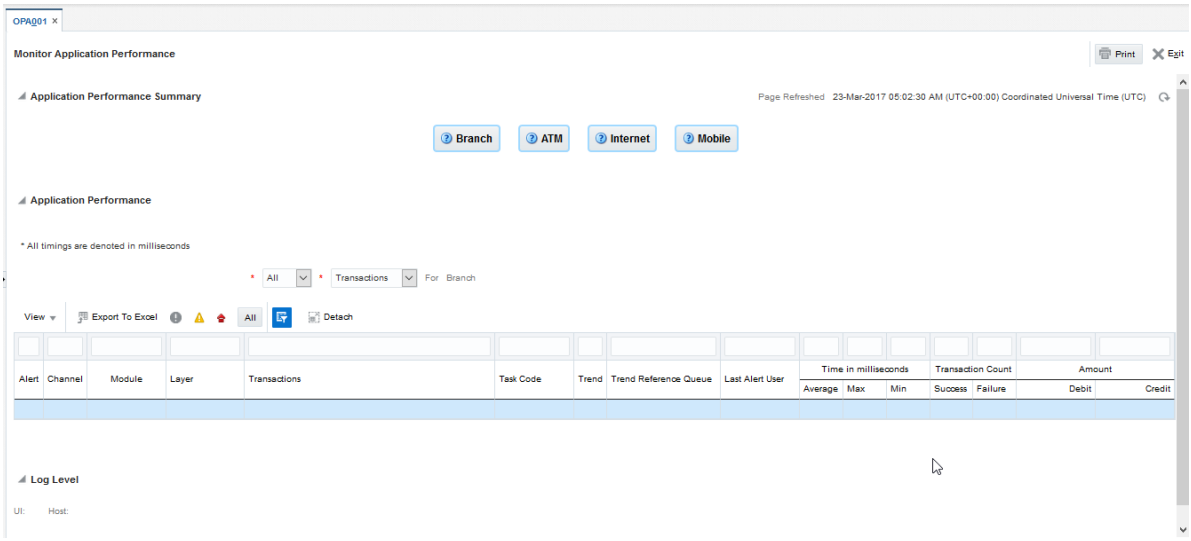
Indicates trending of execution timings of transaction. It is calculated by algorithm namely, Exponential Moving Average where if the execution time goes above the specified limit which is calculated by adding average execution time of the transaction and allowed limit (varies logarithmically to execution 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 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 5–6 Alert State



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

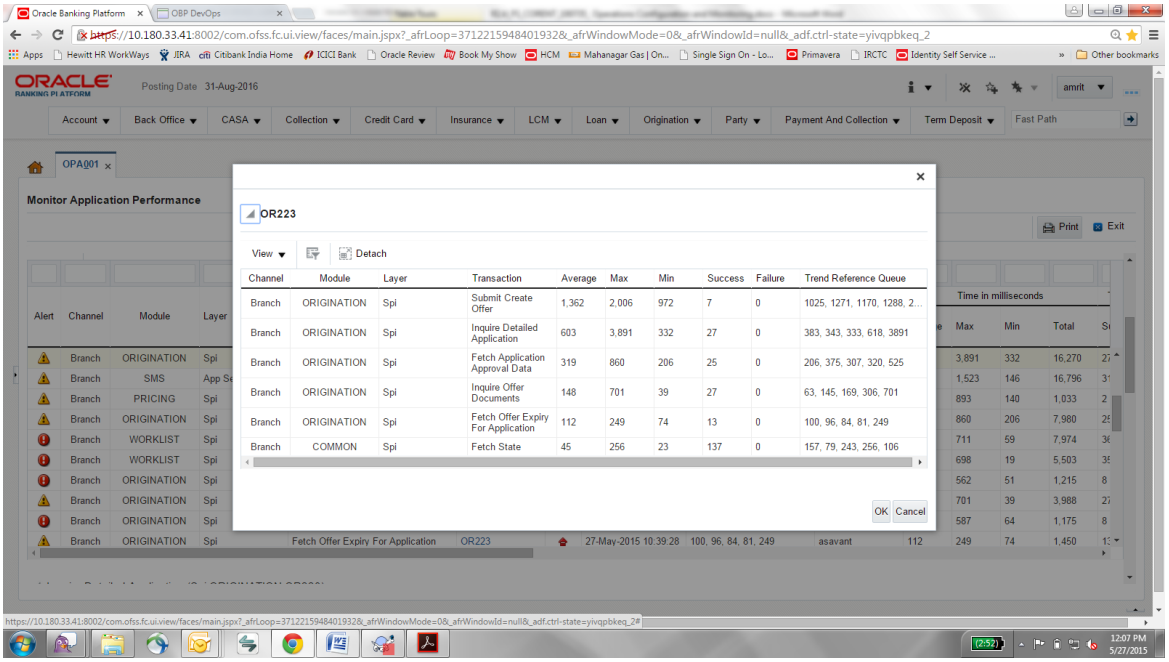
Table 5–1 Alert State

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	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 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 the application)

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

Figure 5–7 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 5–8 Selection of Desired Transaction

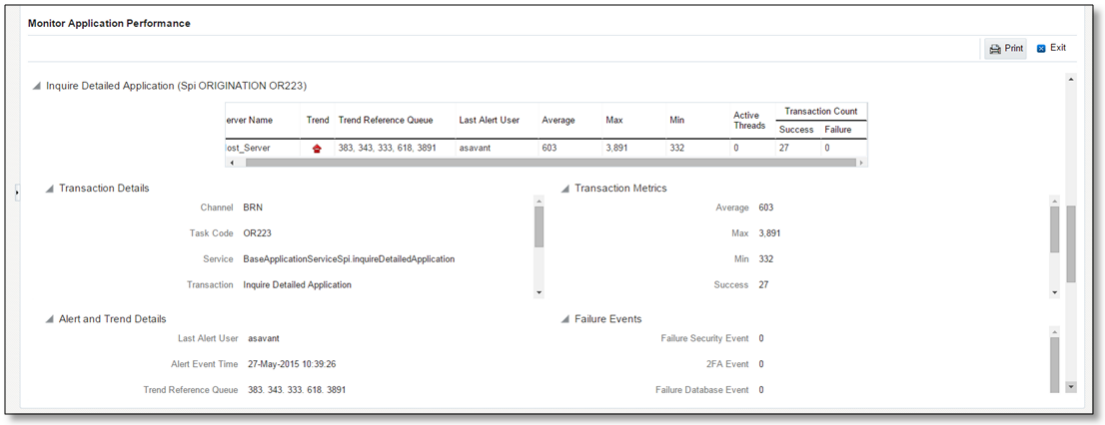


Figure 5–9 Transaction Details

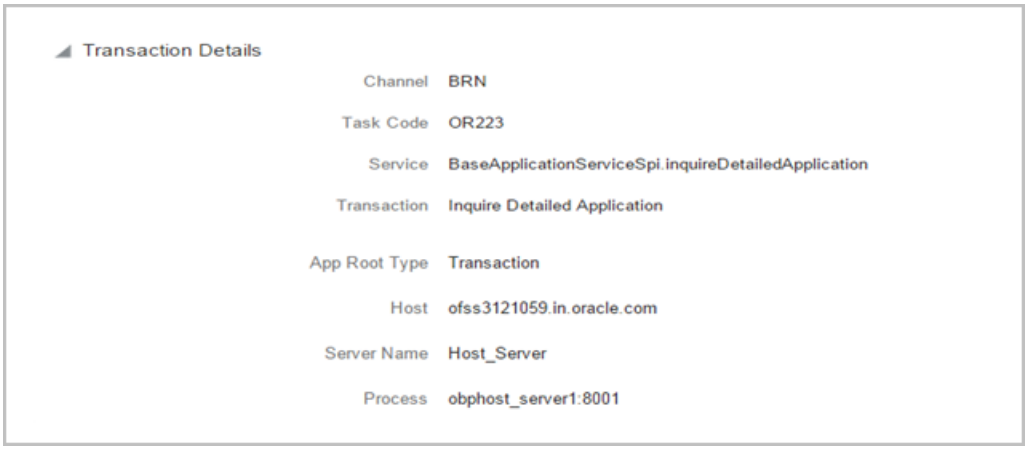


Figure 5–10 Transaction Metrics

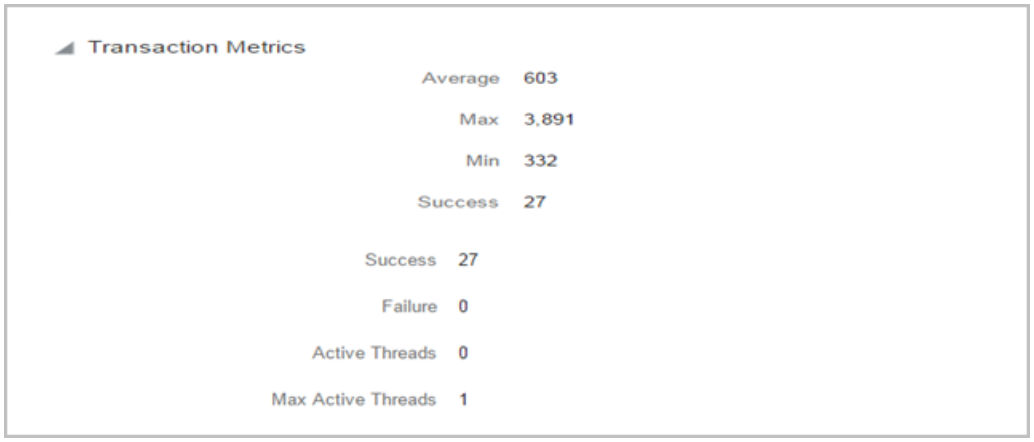


Figure 5–11 Alert and Trend Details

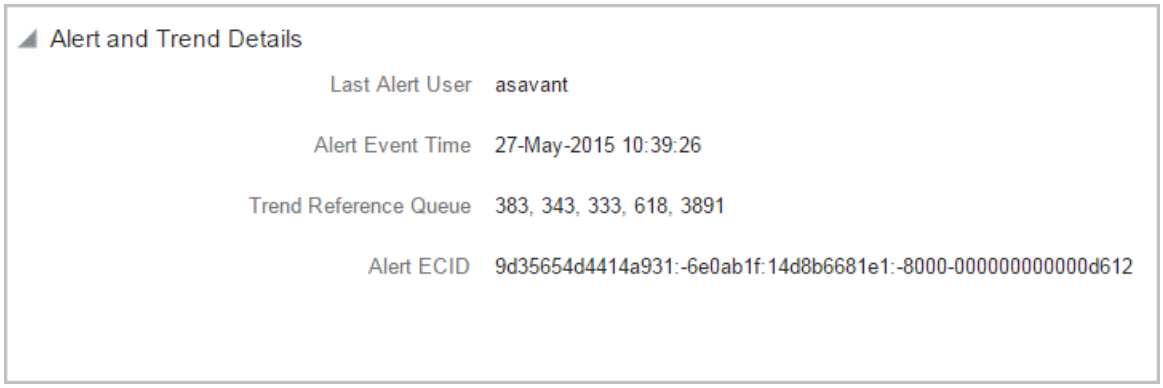


Figure 5–12 Failure Events

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.

5.2 Batch Performance Monitoring

Most of the enterprise applications would require bulk processing of records to perform business operations in real time environments. These business operations include complex processing of large volumes of information that is most efficiently processed with minimal or no user interaction. Such operations would typically include time based events (for example, month-end calculations, notices or correspondence), periodic application of complex business rules processed repetitively across very large data sets (for example, rate adjustments). Batch monitoring includes monitoring of all such batch processes. These batch processes generate huge statistics, which needs to be monitored in order to understand and improve its performance. OPA003 page is used to monitor these processes in detail along various metrices like duration, throughput, aborts, and so on.

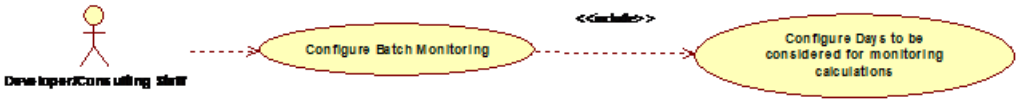
5.2.1 Use Cases

The overall use cases for the whole Batch monitoring operation are divided into two units on the basis of actor that works over batch monitoring operations. The different actors along with their use cases are as below:

Developers

These are the set of people who configure the monitoring services that are the part of the system. The configuration can be made in the properties file BatchStatistics.properties. Configuration include the number of previous batch runs to be considered for calculation for monitored metrics.

Figure 5–13 Developers



IT Technical Staff

This consists of set of people who monitor the Batch statistics generated during the batch run.

Figure 5–14 IT Technical Staff

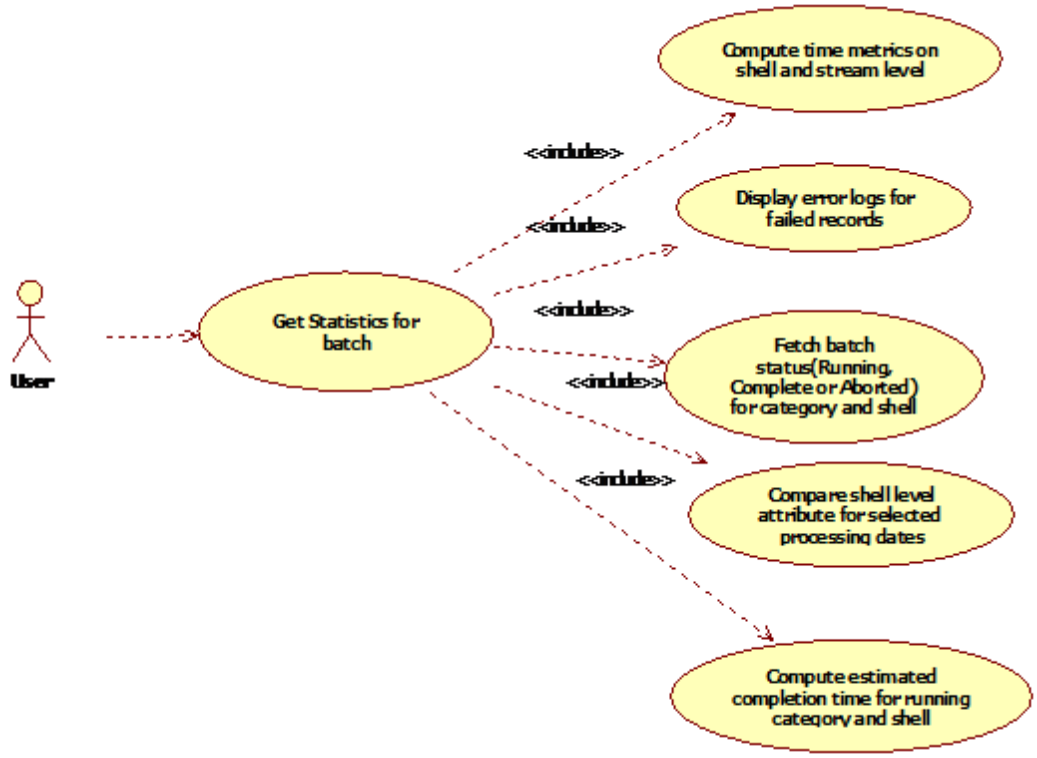


Figure 5–15 IT Technical Staff - Monitor Batch Stats

5.2.2 Monitoring Batch Performance Using OPA003 page

Once batch starts it needs UI representation to easily understand and interpret the batch stats. By monitoring these stats, one can understand the bottle necks of the batch process and hence can work in a way to improve batch performance.

5.2.2.1 Monitor Batch Performance (Fast path: OPA003)

This page takes category, job code, job type, and processing date as input and provides monitoring stats for shells running for selected category.

Figure 5–16 Batch Performance Monitoring

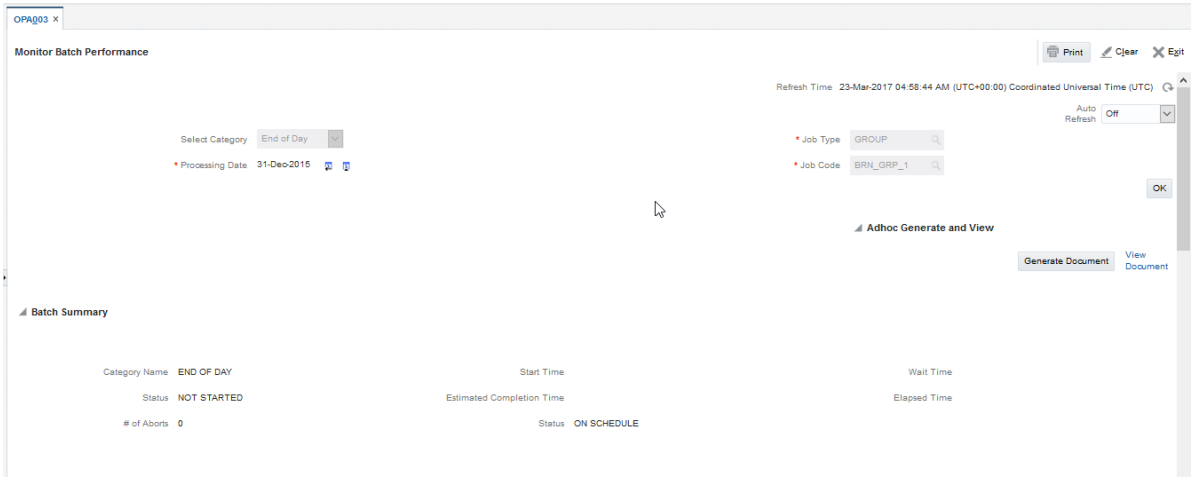


Figure 5–17 Batch Performance Monitoring - Shell Details

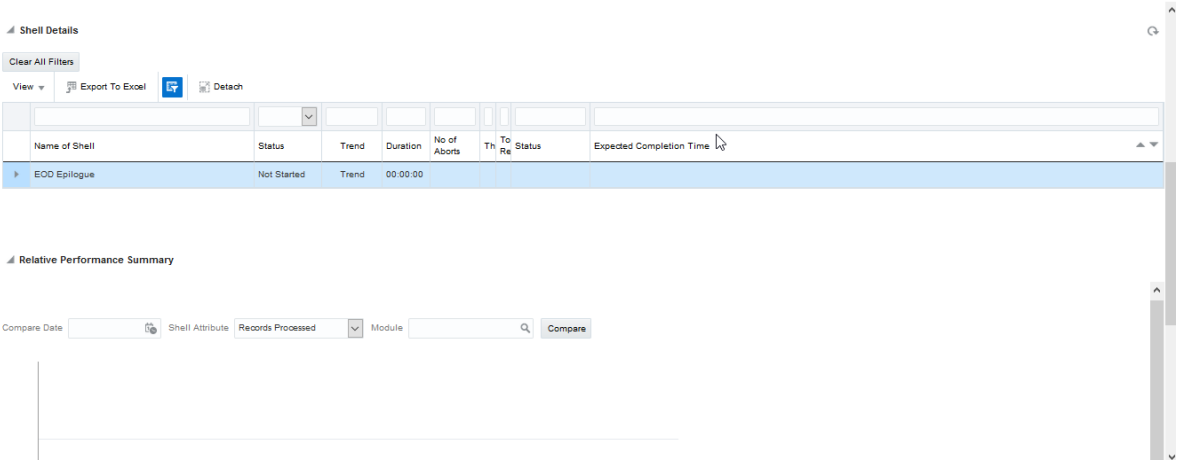
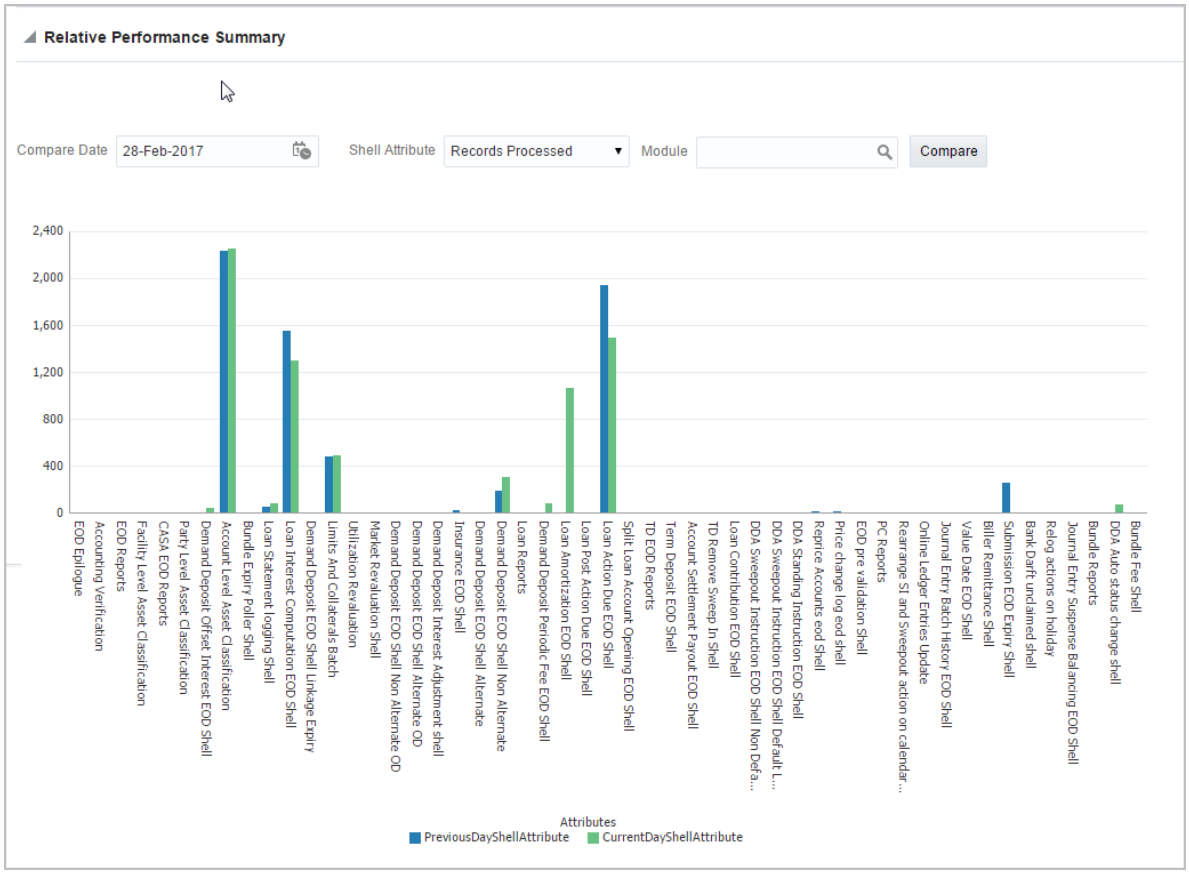


Figure 5–18 Batch Performance Monitoring - Relative Performance Summary



The batch statistics are monitored at different levels as follows:

- Category Level
- Shell Level
- Record level

Category Details

The parameter monitored at category level as given as below:

Table 5–2 Category Details

Attribute Name	Description
Category Name	Name of category for example, EOD (End Of Day)
Status	Indicates status of selected category. Valid Values: COMPLETE, RUNNING, ABORTED.
Start Time	Indicates start time of category. The time is represented in DD-MM-YYYY hh:mm:ss format.
End Time	Indicates end time of category. The time is represented in DD-MM-YYYY hh:mm:ss format.

Attribute Name	Description
Wait Time	It is the time for which category is in Aborted state. Wait time for category denotes the time for which batch was halted.
Execution Time	It the time for which category is in Running state.
Number Of Aborts	Indicates number of times category was aborted.
Total Time	It is the total time taken by category to complete. Time taken for category is summation of wait and execution time.
Estimated Completion Time	It is the predicted time for category completion. This time is calculated based on number of incomplete and pending shells for the current running category. The averaged value of previous run duration is considered for calculating estimated time. Similar calculation is done for estimating completion time for shell. This attribute is displayed only during batch run. It is not displayed once batch is complete
Time Status	The status of category (that is, delayed or early) denotes whether category is running slow or fast. This value is calculated based on average of historical data. This attribute is displayed only during batch run. It is not displayed once batch is complete

Shell Details

This level displays statistics of all shells corresponding to selected category. The parameters monitored at shell level are given below:

Table 5–3 Shell Details

Attribute Name	Description
Name of shell	Represents name of shell
Trend	Valid Values: UPWARD, DOWNWARD, NEUTRAL. It denotes the trend based on historical data for time required by shells to complete.
Status	Valid Values: Complete, Running, Aborted, Not Started. Indicates status of shell
Duration	It is the time required by shell to complete.
Start Time	Indicates start time of shell. The time is represented in DD-MM-YYYY hh:mm:ss format.
End Time	Indicates the time at which shell is completed. The time is represented in DD-MM-YYYY hh:mm:ss format.
Wait Time	It is the time for which shell is in aborted state.
Expected Completion Time	Indicates the estimated time for a shell to complete.
Failed Records	Number of failed records for a shell
Records Processed	Number of records processed in a shell
Number of Streams	Number of streams denote number of processes running in parallel for a shell. On proper analysis of historical data of stream count, number of records and duration for particular shell one can optimize throughput for it.

Attribute Name	Description
Throughput	It is the average processing time for one record. Throughput is denoted in millisecs.

Figure 5–19 Shell Details

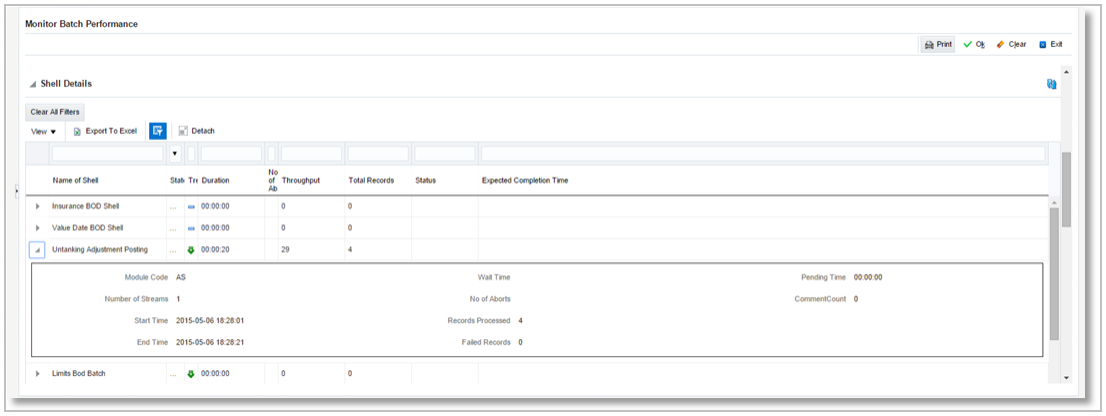
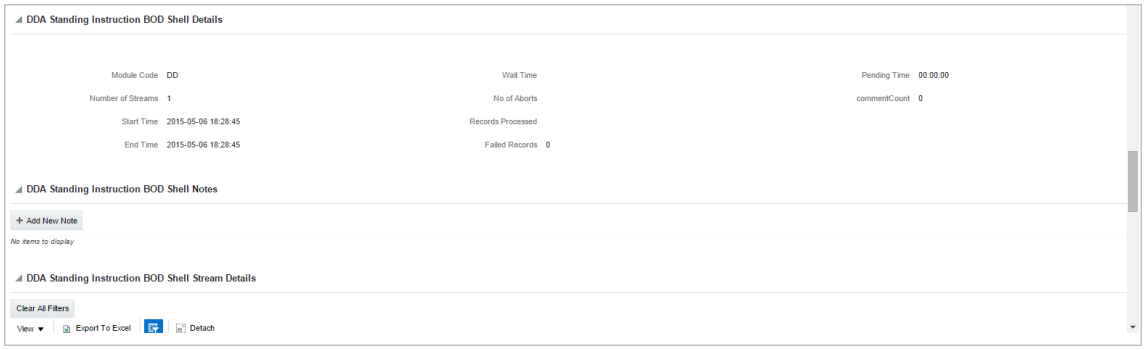


Figure 5–20 Shell Details - DDA Standing Instructions



Note

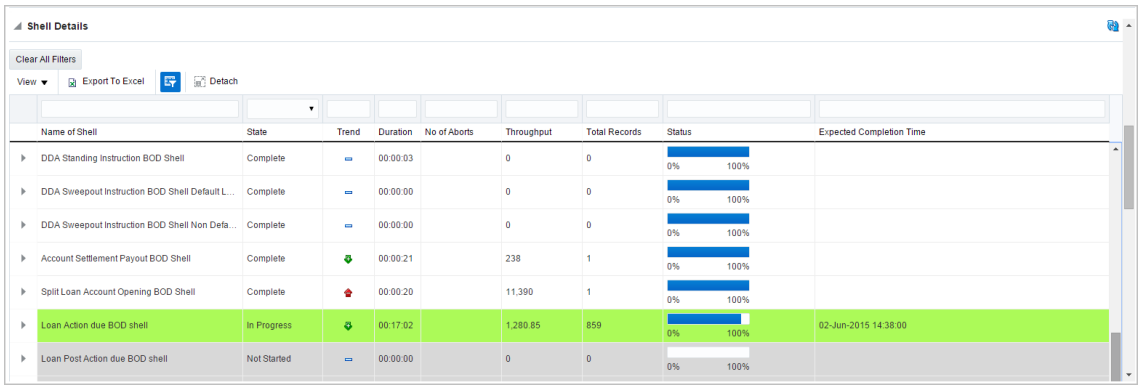
Note the following:

- Trend for a particular shell is decided based on comparison of time statistics (that is, current run time and historical data for previous batch runs). Number of previous batch run to be considered is configurable. It is configured in the property file that is, (BatchStatistics.properties). The trend and other estimated time seems more realistic if number of previous run days configured in property file are more.

- Trend gives an idea whether a particular shell is running fast or slow compared to previous runs though it is important to consider number of records being processed in that shell.

The following figure shows the view displayed during batch run. Few extra parameters like estimated completion time for shell and category are monitored during batch run.

Figure 5–21 View of Batch Run



Comments Table

Comments Table is rendered based on row click of shell details table.

- In case of batch abort, it is important to know the reason behind abort and how that is fixed. Comments table serves this purpose as one can log the details regarding fix and reason behind shell abort. Multiple comments can be captured for particular shell.
- Also one can query historical data for comments. The historical data of comments can be used to analyse the reason behind failure of particular shell.

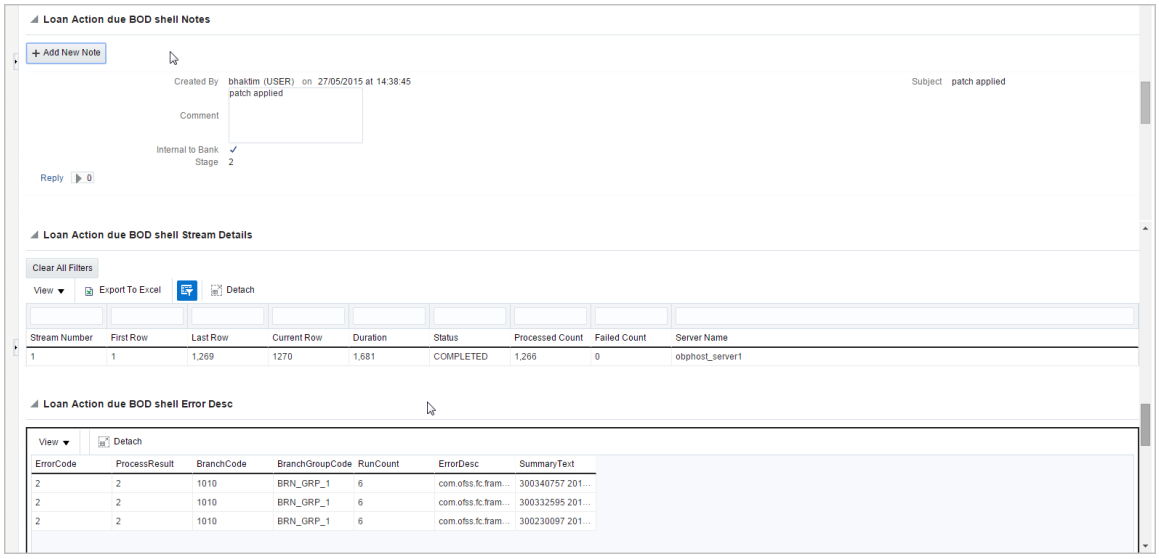
Stream Details Table

Stream Details table is rendered based on row click of shell details table.

Table 5–4 Stream Details

Attribute Name	Description
Stream Number	Indicates the number of a stream in which the record is being processed
First Row	Indicates the start sequence number of a record, processing in a particular stream.
Last Row	Indicates the end sequence number of a record, processing in a particular stream.
Duration	It is the time required for stream to complete.
Status	Valid Values: COMPLETED, RUNNING. It indicates the status of selected stream
Processed Count	Number of records processed in a stream
Server Name	Name of a server running the stream

Figure 5–22 Stream Based Shells



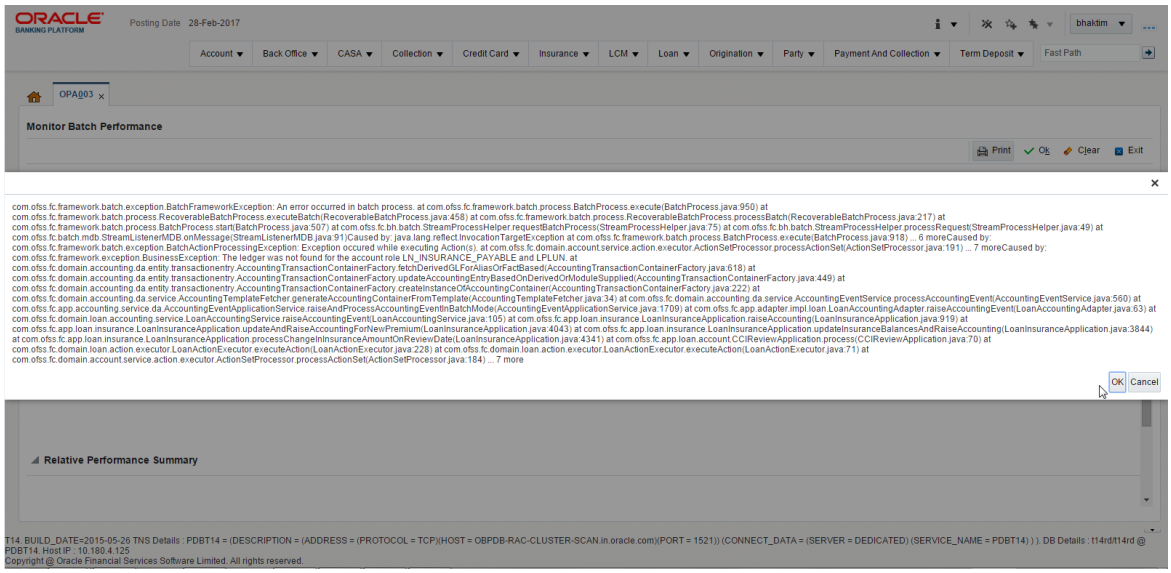
Note

Shells are categorized into two types that is, Stream based shells and Report based shells. Figure 5–22 displays the view for stream based shells.

Exception Log

On row click of the driver level details, it pops up a window showing the stack trace of failed records if present. One can analyse and know the reason behind the failure of that particular record.

Figure 5–23 Exception Log



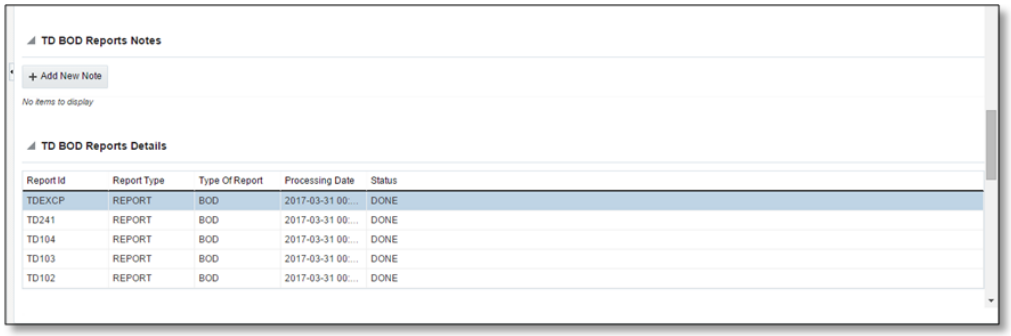
Reports Table

For Report based shells different parameters related to report processing are monitored. The monitored parameters are given below:

Table 5–5 Reports Table

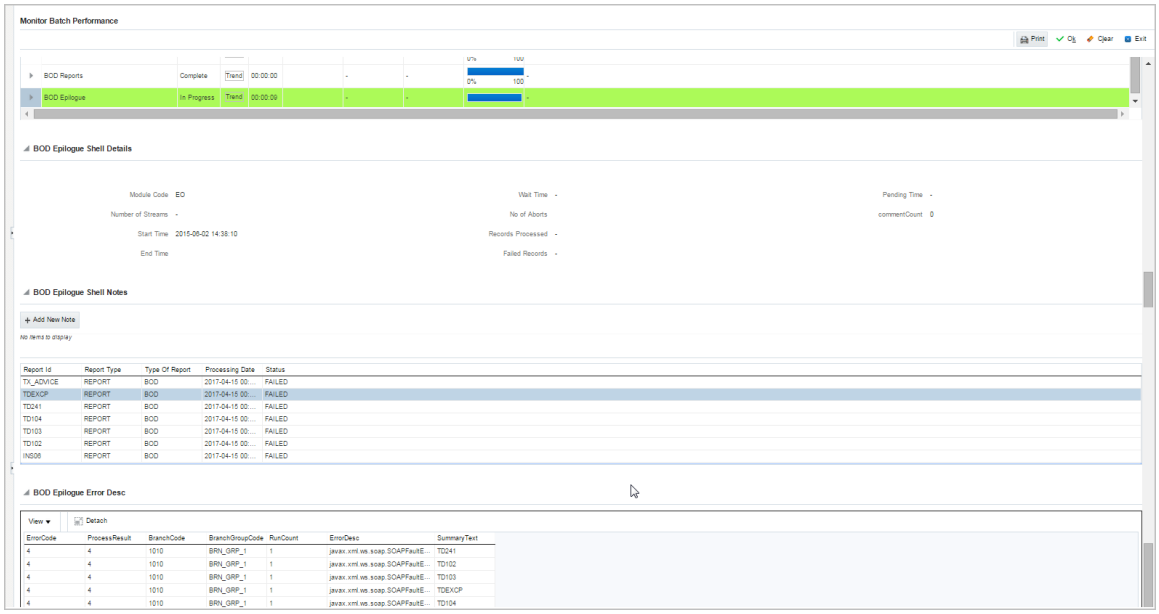
Attribute Name	Description
Report Id	ID to uniquely identify report
Report Type	Report
Type Of Report	Indicates type of reports. Reports are classified based on category.
Processing Date	Indicates processing date of report.
Status	Indicates the status of the report. Valid Values: DONE, PENDING, RUNNING, ABORTED.
Error Message	Error message represents the reason for report failure. No message is displayed in case of successful run.

Figure 5–24 Report Based Shells



The status of report based shell during batch run is shown in Figure 5–25:

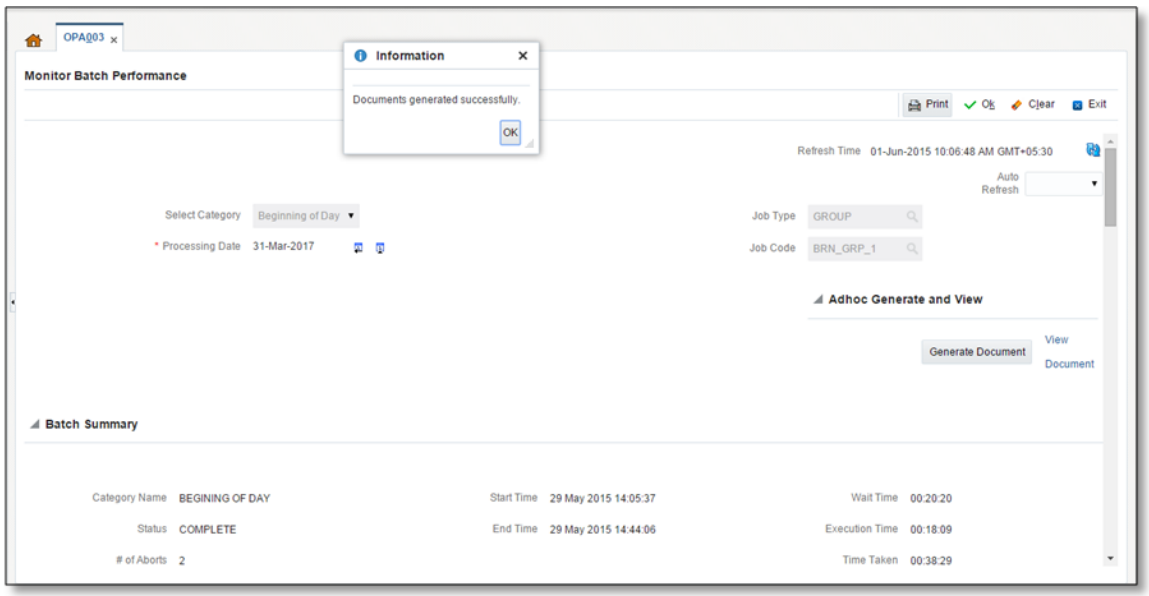
Figure 5–25 Status of Report Based Shell



Exception Report

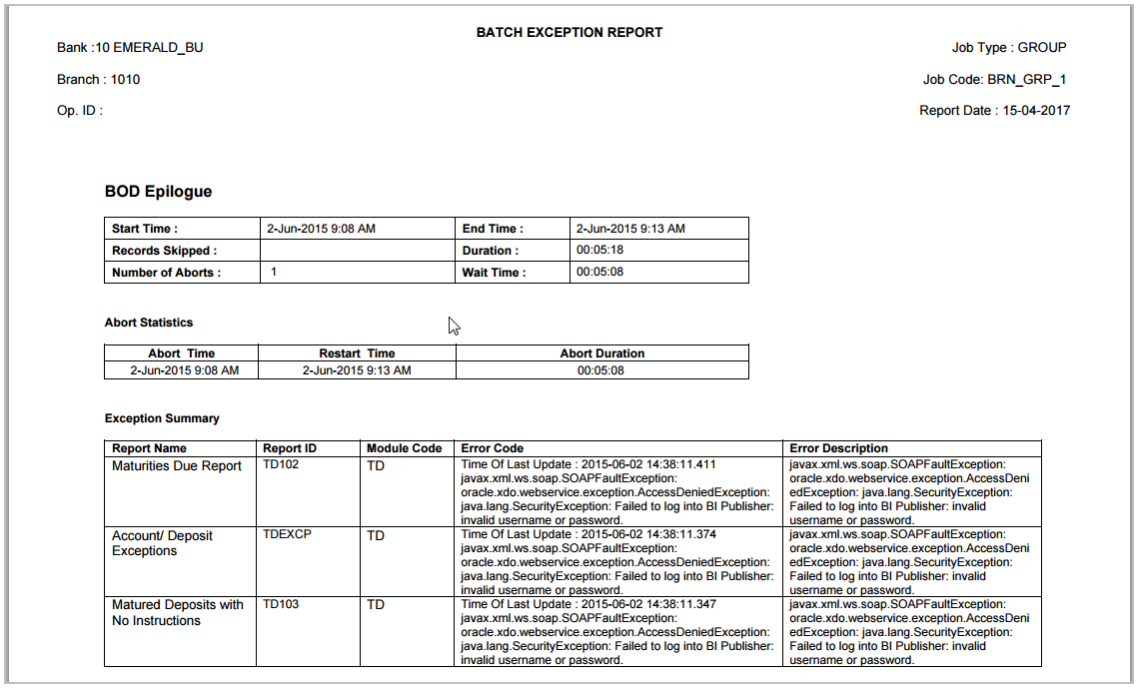
On click of Generate Document, it generates a report for aborted shells with information like Abort count and exception log.

Figure 5–26 Exception Report



The different parameter monitored at shell level and exception logs for all aborted shells are part of exception report. Figure 5–27 displays sample report for a particular shell.

Figure 5–27 Sample Report



BATCH EXCEPTION REPORT

Bank :10 EMERALD_BU

Branch : 1010

Op. ID :

Job Type : GROUP

Job Code: BRN_GRP_1

Report Date : 15-04-2017

BOD Epilogue

Start Time :	2-Jun-2015 9:08 AM	**End Time :**	2-Jun-2015 9:13 AM
Records Skipped :		**Duration :**	00:05:18
Number of Aborts :	1	**Wait Time :**	00:05:08

Abort Statistics

Abort Time	Restart Time	Abort Duration
2-Jun-2015 9:08 AM	2-Jun-2015 9:13 AM	00:05:08

Exception Summary

Report Name	Report ID	Module Code	Error Code	Error Description
Maturities Due Report	TD102	TD	Time Of Last Update : 2015-06-02 14:38:11.411 javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.	javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.
Account/ Deposit Exceptions	TDEXCP	TD	Time Of Last Update : 2015-06-02 14:38:11.374 javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.	javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.
Matured Deposits with No Instructions	TD103	TD	Time Of Last Update : 2015-06-02 14:38:11.347 javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.	javax.xml.ws.soap.SOAPFaultException: oracle.xdo.webservice.exception.AccessDeniedException: java.lang.SecurityException: Failed to log into BI Publisher: invalid username or password.

Exception Log Table

The figure below provides the details of the exception log.

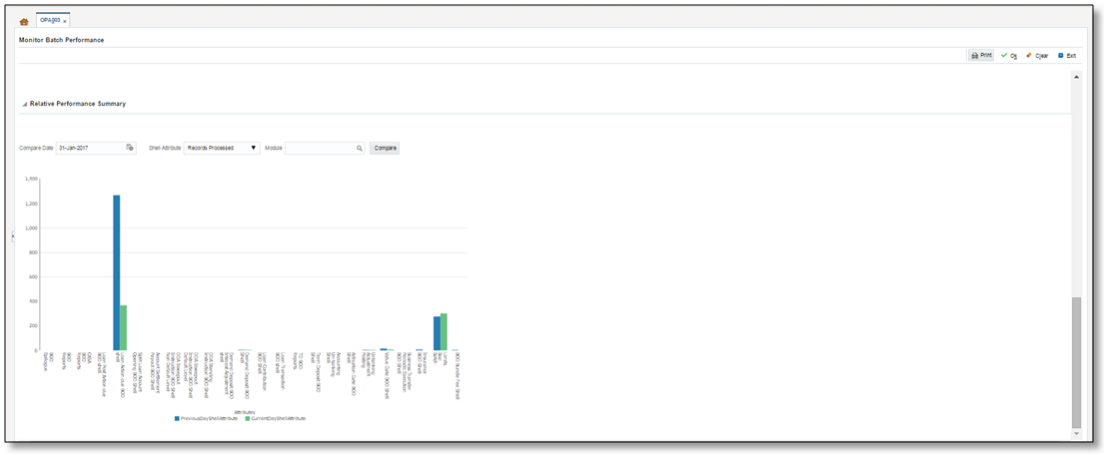
Figure 5–28 Exception Log Table

ERROR CODE	ERROR DESCRIPTION	SUMMARY
kException: An error occurred in batch process.862-8203-0444-6360		
Time Of Last Update : 2013-09-11 11:28:51.438 Error reference Number :862-8182-2552-7227Error msg :An error occurred in batch process.Error cause :com.ofss.fc.framework.batch.exception.BatchFrameworkException: An error occurred in batch process.862-8182-2552-7227	com.ofss.fc.framework.batch.exception.BatchFrameworkException: An error occurred in batch process. at com.ofss.fc.framework.batch.process.BatchProcess.execute(BatchProcess.java:910) at com.ofss.fc.framework.batch.process.RecoverableBatchProcess.executeBatch(RecoverableBatchProcess.java:432) at com.ofss.fc.framework.batch.process.RecoverableBatchProcess.processBatch(RecoverableBatchProcess.java:	
Time Of Last Update : 2013-09-11 11:28:53.868 Error reference Number :862-8206-5767-2044Error msg :An error occurred in batch process.Error cause :com.ofss.fc.framework.batch.exception.BatchFrameworkException: An error occurred in batch process.862-8206-5767-2044	com.ofss.fc.framework.batch.exception.BatchFrameworkException: An error occurred in batch process. at com.ofss.fc.framework.batch.process.BatchProcess.execute(BatchProcess.java:910) at com.ofss.fc.framework.batch.process.RecoverableBatchProcess.executeBatch(RecoverableBatchProcess.java:432) at com.ofss.fc.framework.batch.process.RecoverableBatchProcess.processBatch(RecoverableBatchProcess.java:	

5.2.3 Histogram of Shell Attribute Comparison

This section provides graphical view for comparing shell attributes for any two selected dates. The processing date, shell attribute and module name are taken as input to this table. The output is displayed as bar graph in which X axis represents the name of the shell and Y axis denotes value of shell attribute. For each shell two records are displayed, these records corresponds to the dates for which the data is being compared.

Figure 5–29 Graphs

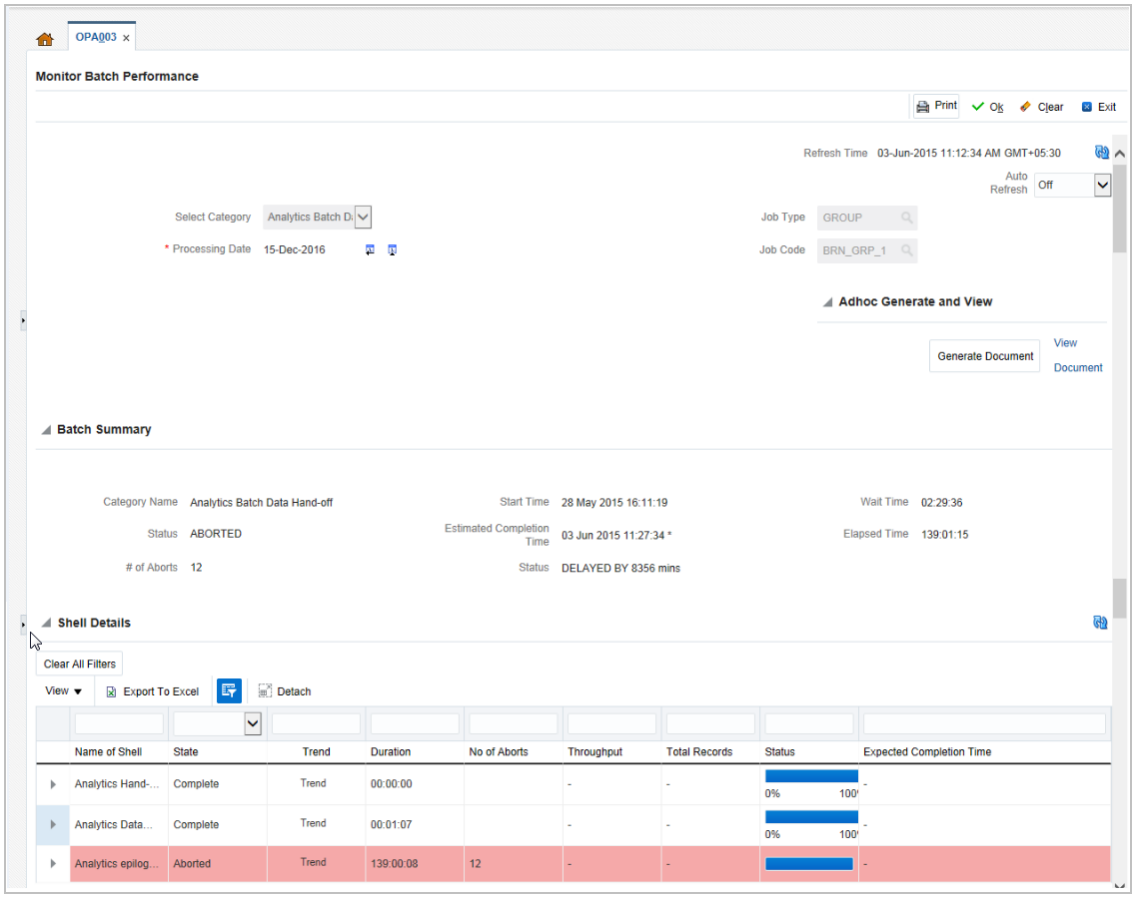


5.3 ODI Batch Handoff Monitoring

This section provides, top package level execution details for monitoring of ODI handoff. The input for these details are category ID, branch group code, branch group type, and processing date.

Figure 5–30 describes the input parameters for the batch handoff monitoring and the shell details like name of shell, start time, end time, number of aborts.

Figure 5–30 Input Parameters for Batch Handoff



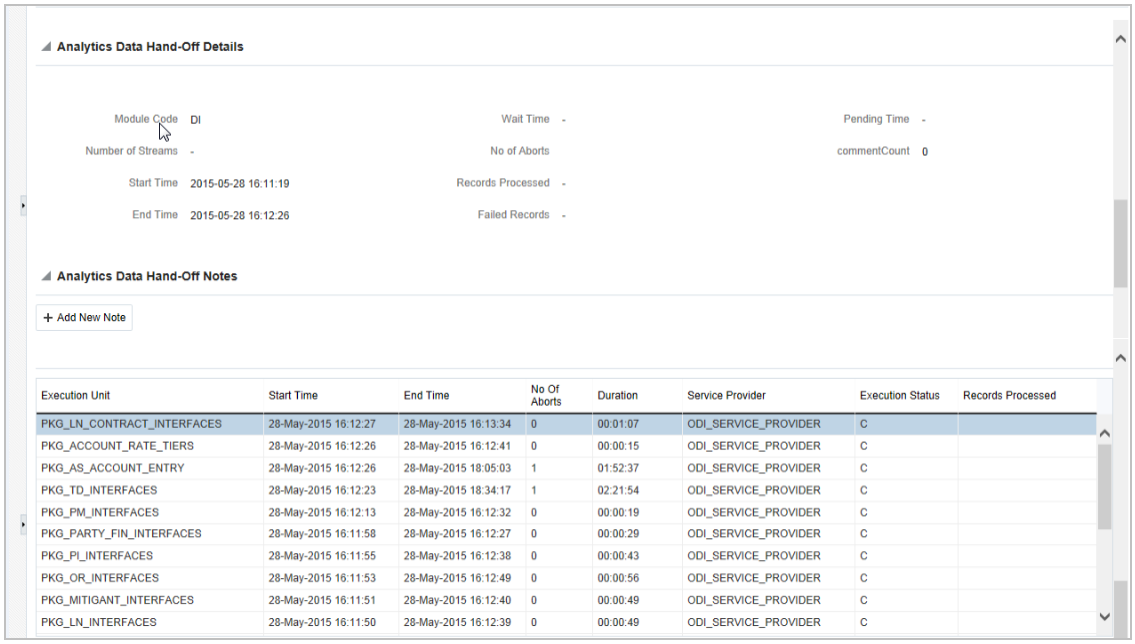
Execution Unit

On click of the analytics data Handoff shell, the below table is shown with the execution unit (top level package) level details:

This table contains the following attributes:

- Execution unit name
- Start time of execution of the execution unit
- End time of execution of the execution unit
- Number of aborts of the execution unit
- Duration of execution of the execution unit
- Service provider for ETL process (ODI)
- Execution status of the execution unit, that is, complete, running, and aborted
- Records processed at the stage level in ETL process

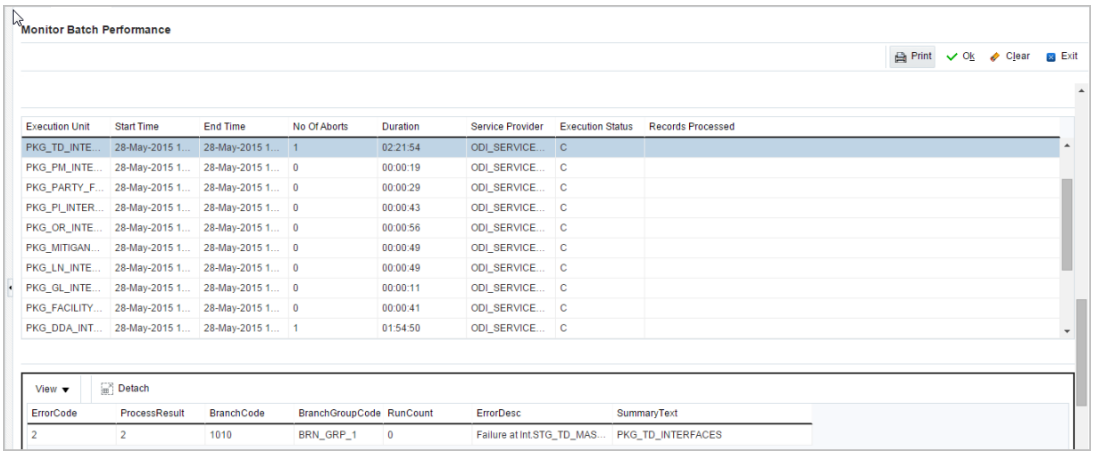
Figure 5–31 Execution Unit



Abort Statistics

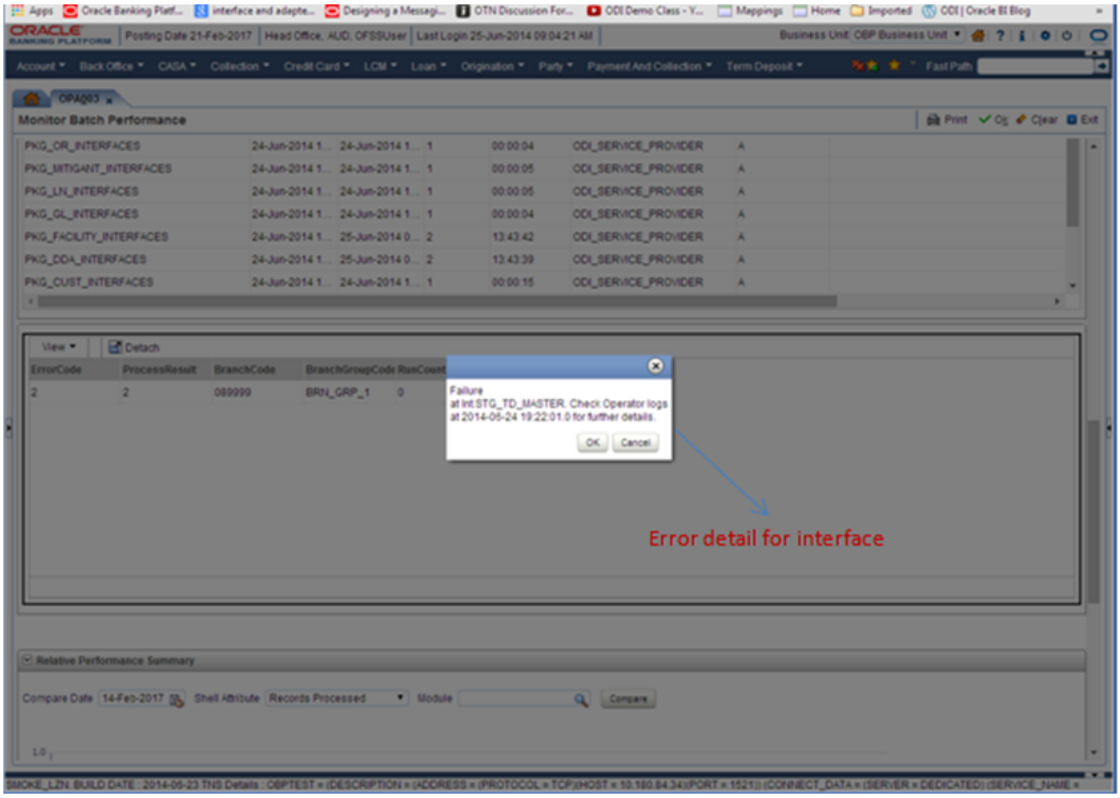
On click of aborted execution unit, the below table is shown with the abort details like run count, the actual error description, and summary of the exception containing the interface name for which the exception occurred.

Figure 5–32 Abort Statistics



On click of the error description table, the error description message appears as shown in Figure 5–33:

Figure 5–33 Failure Error Description



6 Application Monitoring Using EM Plugin

This chapter provides an overview on the various monitoring operations performed as an administrator, using Enterprise Manger (EM) Plugin.

6.1 Monitoring Application Using EM Plugin

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

6.1.1 Oracle Enterprise Manager (EM)

Oracle Enterprise Manager is the application where all the monitoring data exists. It includes server and machines status, performance, and monitoring statistics.

All the servers are monitored by EM including Host, UI, SOA, and so on.

We have a view corresponding to every environment containing all the components which include outbound components.

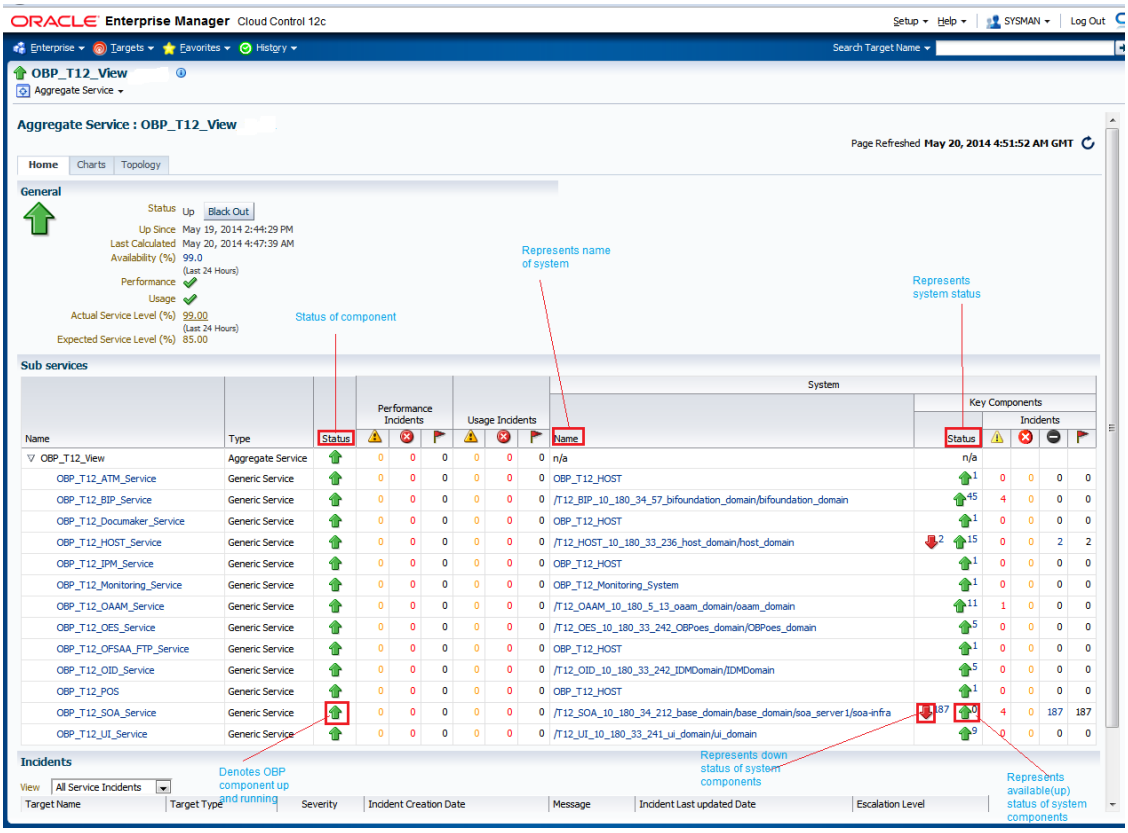
Some notations in EM are provided below:

Table 6–1 Notations in EM

	Indicates component is down
	Indicates component is up and running
	Indicates Alerts
	Indicates Warnings
	Indicates metric collection error
	Indicates healthy status

Figure 6–1 shows the environment view in Oracle Enterprise Manager:

Figure 6–1 Oracle Enterprise Manager



The views in Figure 6–1 include UI, Host, and SOA servers.

Security Stacks components such as OAAM, OID, OES, outbound components such as BIP, IPM, Documaker, ATM and POS channels are also part of the environment view.

Each component can be further explored for details by clicking on the links provided for them.

6.1.2 UI

For UI, all the managed servers created under Weblogic cluster can be monitored. EM provides the following information for UI Cluster:

- Active Session about all Managed Servers
- CPU Usage
- Heap Usage
- Request Processing Time

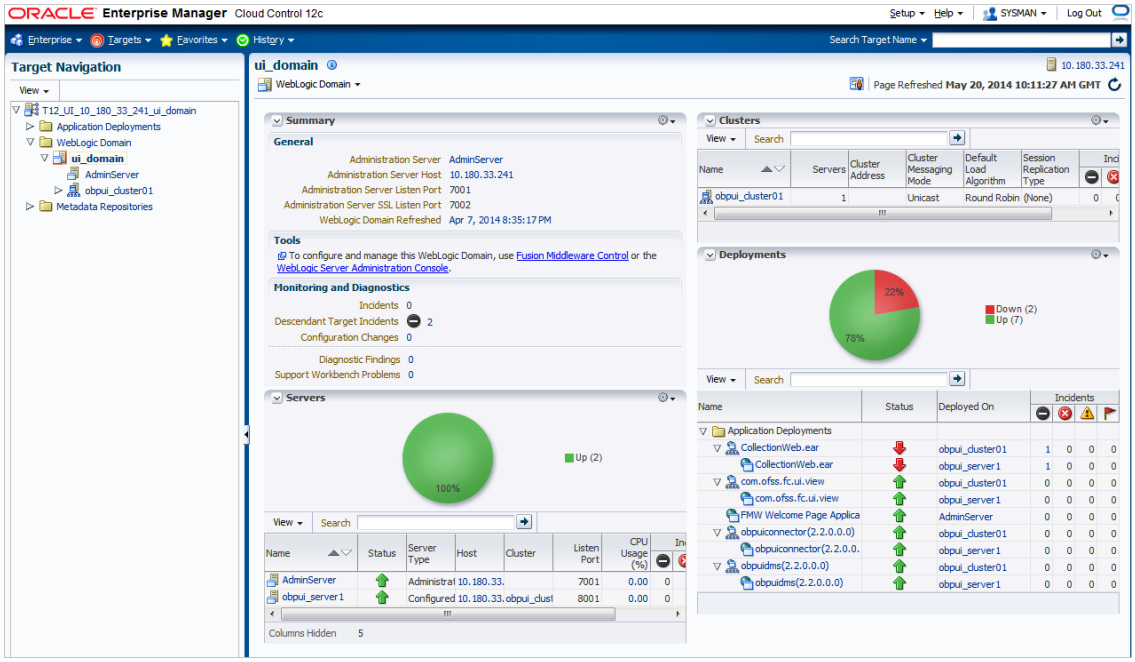
Figure 6–2 UI Cluster in EM

UI is hosted on WebLogic domain, so the EM target of UI machine is WebLogic domain. EM gives the following information for UI:

- Server Performance Statistics
- Up/Down Status
- List of deployed applications
- Incidents or Alerts; if any

Figure 6–3 displays the WebLogic domain for UI.

Figure 6–3 WebLogic Domain for UI



The performance metric includes metrics like CPU Utilization, Memory Utilization, Active Sessions and are default metrics provided by EM.

The following figure displays the metrics chart.

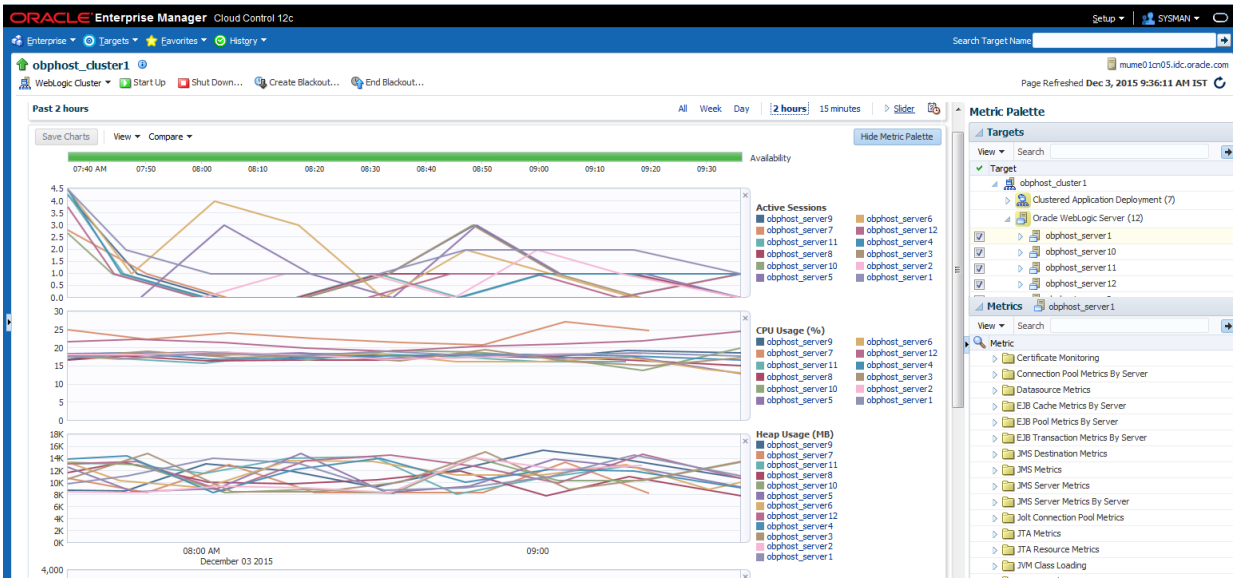
Figure 6–4 Metrics Chart

6.1.3 Host

For Host, all the managed servers created under Weblogic cluster can be monitored. EM provides the following information for Host Cluster:

- Active Session about all Managed Servers
- CPU Usage
- Heap Usage
- Request Processing Time

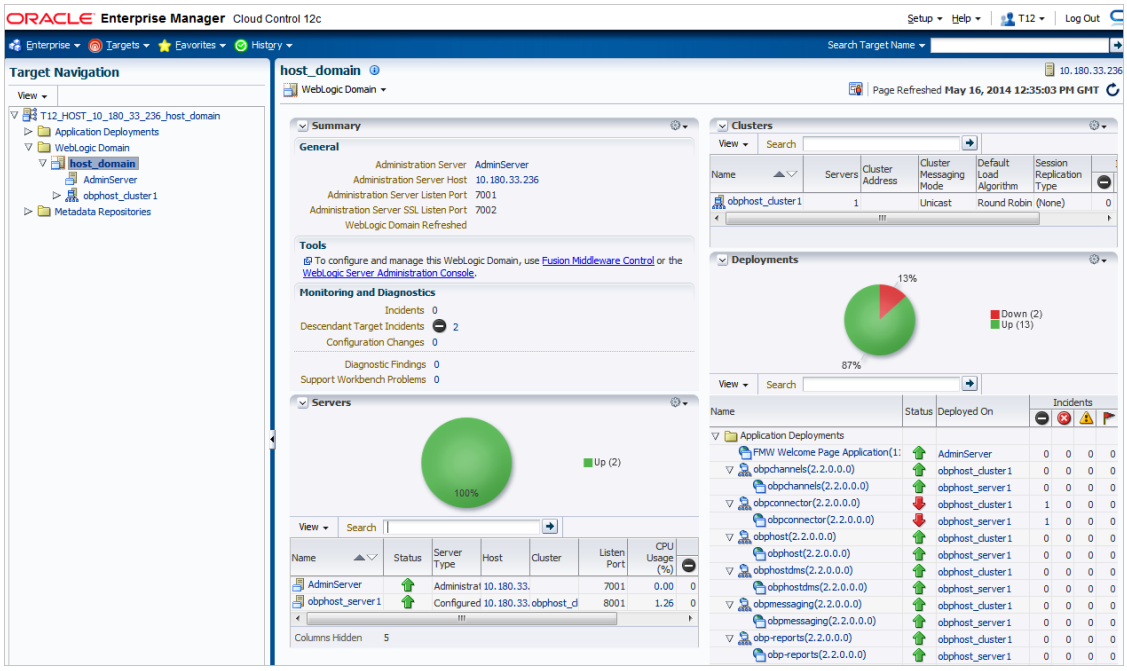
Figure 6–5 Host Cluster in EM



Similar to UI, Host is also deployed on WebLogic domain and has similiar metrics like UI.

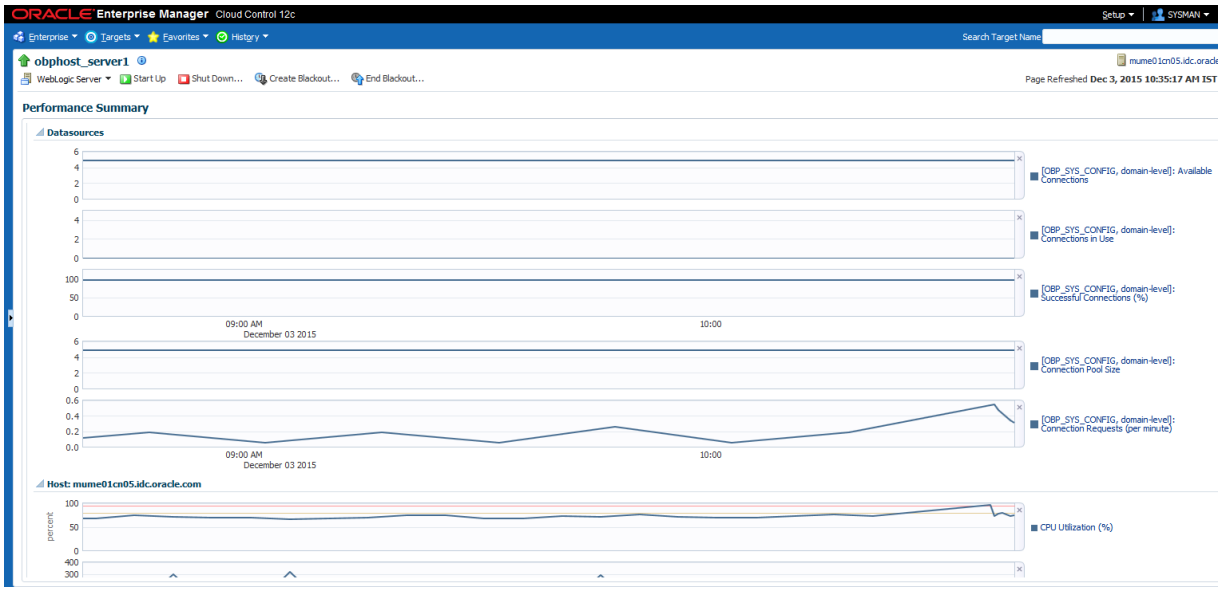
The following figure displays the Host target in EM.

Figure 6–6 Host Target in EM



The following figure displays the metric charts.

Figure 6–7 Metrics Chart

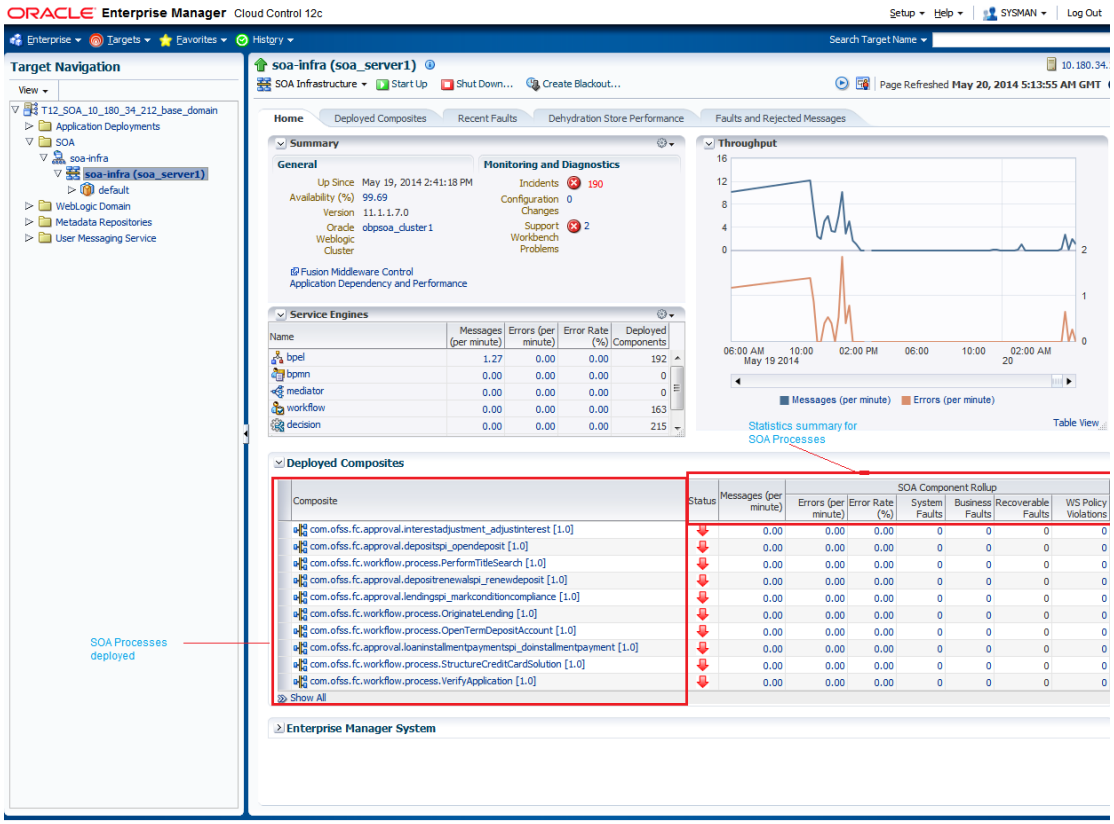


6.1.4 SOA

SOA server is deployed on WebLogic domain where the SOA processes are deployed.

The process list can be seen in the list of deployed applications. The other metrics remain same as for WebLogic domain in EM. Figure 6–8 displays the process list.

Figure 6–8 Viewing Process List



6.1.5 Security Stack (OID, OES, OAAM)

OID, OES and OAAM are also deployed as WebLogic domain.

Figure 6–9 OID WebLogic Domain

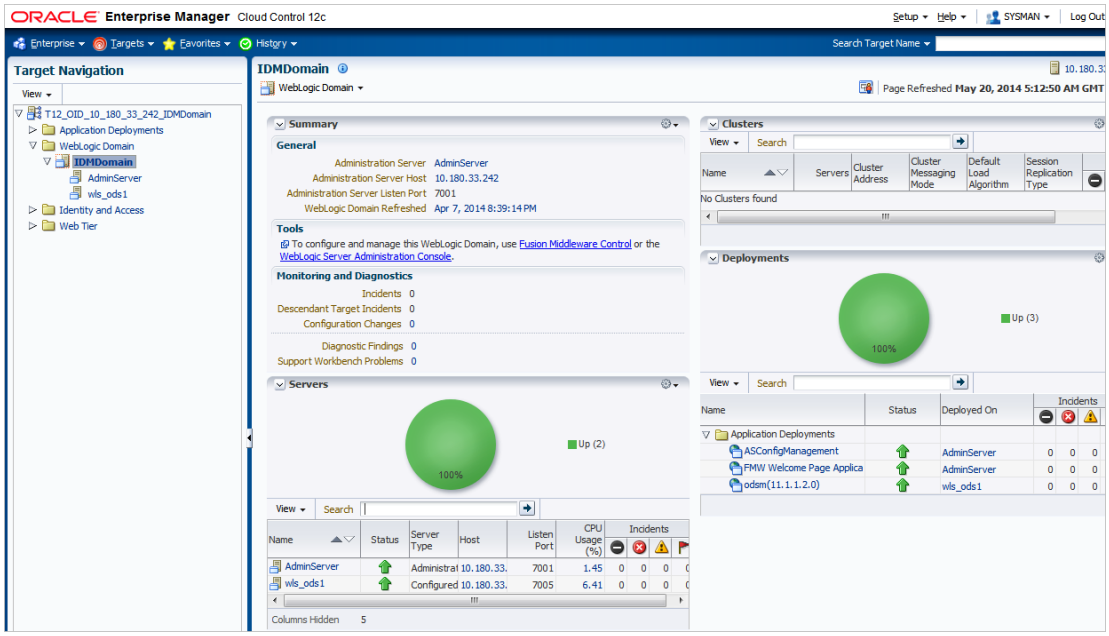


Figure 6–10 OES WebLogic Domain

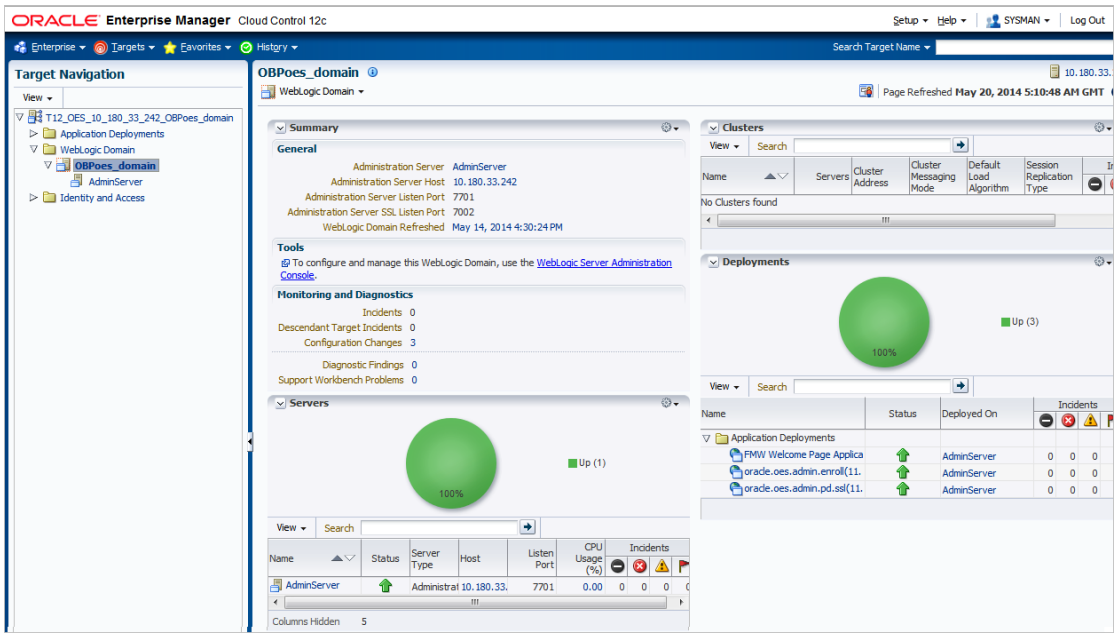
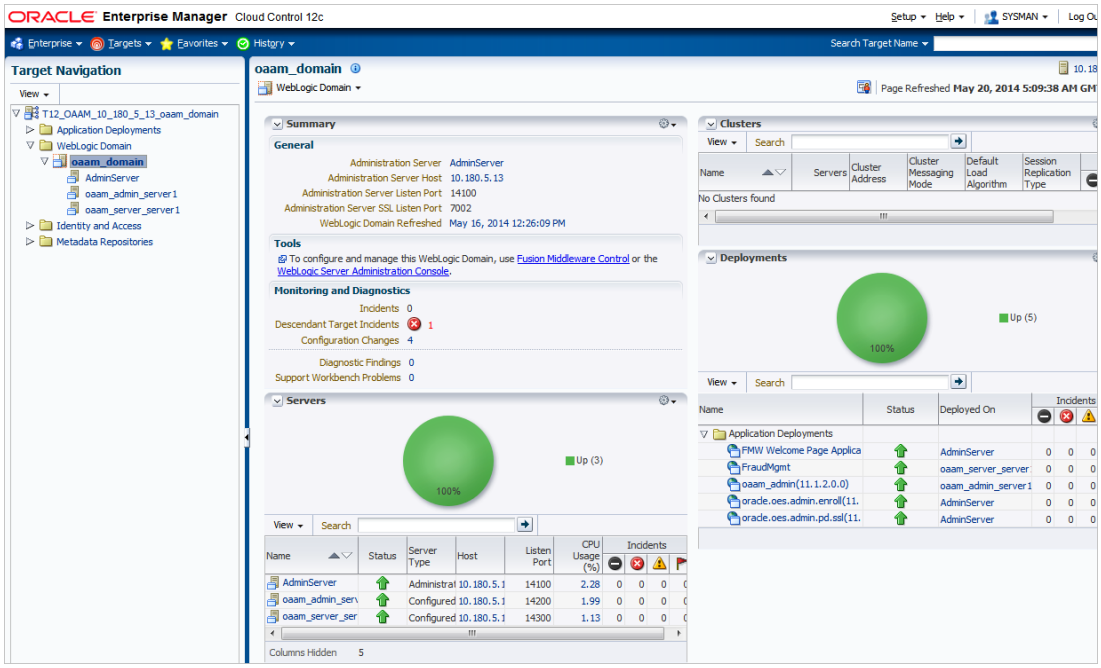


Figure 6–11 OAAM WebLogic Domain



6.1.6 Document Generation Outbound Components (Documaker, BIP, IPM)

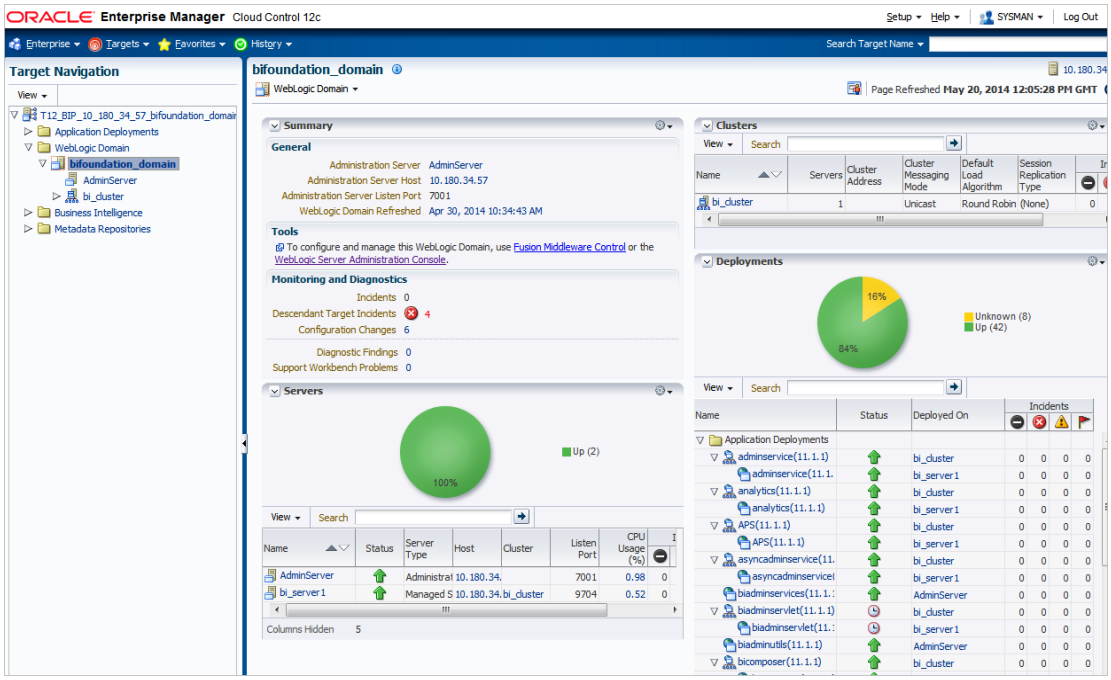
These are not part of the application, but we monitor these so as to detect the cause of failure in case the document generation fails at any point of time.

A webservice is invoked for generating the documents from the application with BIP as well as documaker. From EM, we check whether that webservice is up and running or not, which gives the status of these components. Figure 6–12 displays the status from EM.

Figure 6–12 Document Generation Status

BIP is also deployed on WebLogic domain.

Figure 6–13 BIP Deployment



6.1.7 Monitoring Views

Monitoring views show the batch and application performance statistics along with server performance history. It consists of Batch Monitoring and Application Monitoring tabs which show detailed view of batch performance and application performance statistics along with the server performance statistics on which they are running.

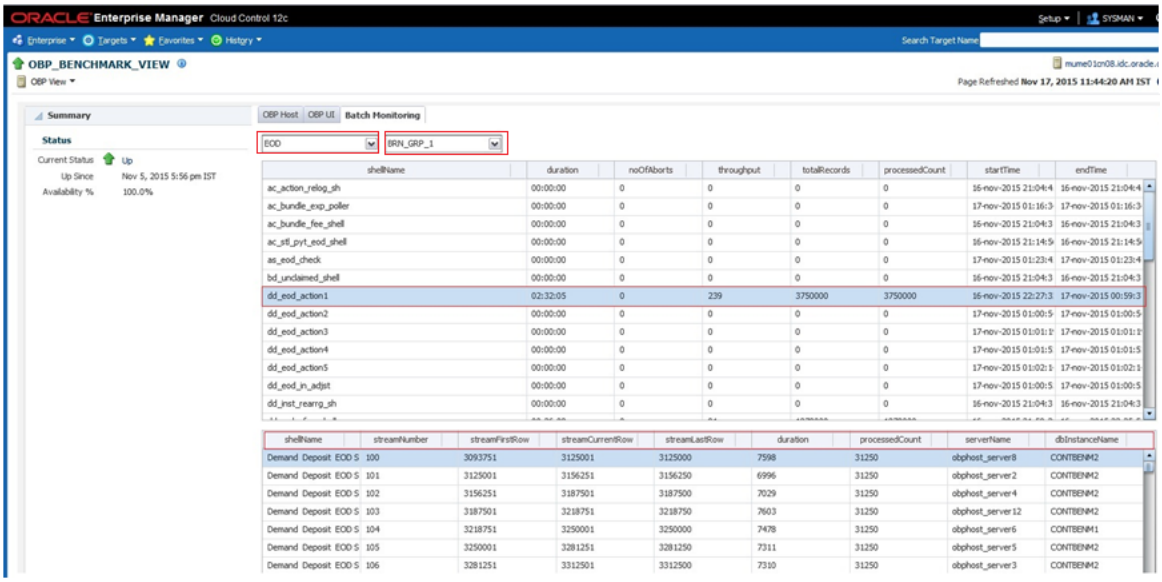
Batch Monitoring

This shows detailed view for host and database server performance charts along with batch performance statistics.

The batch performance statistics are the details of the categories run in the application. The date for which category details are shown is the last run date. The categories include EOD, CutOff, Internal System EOD and BOD.

To get the details of a particular category, select it from the combo box. This will display the list of shells in the category in the table below. From the table, select the desired shell, the shell details provides the stream details of the selected shell.

Figure 6–14 Database Server Info



The streams can run in different servers. To get the details of the performance of the server in which the stream is executed, select the stream. The charts below gives the performance summary of the server in which the stream is executed and the database performance.

The following figure displays the status from EM.

Figure 6–15 Batch Monitoring Status

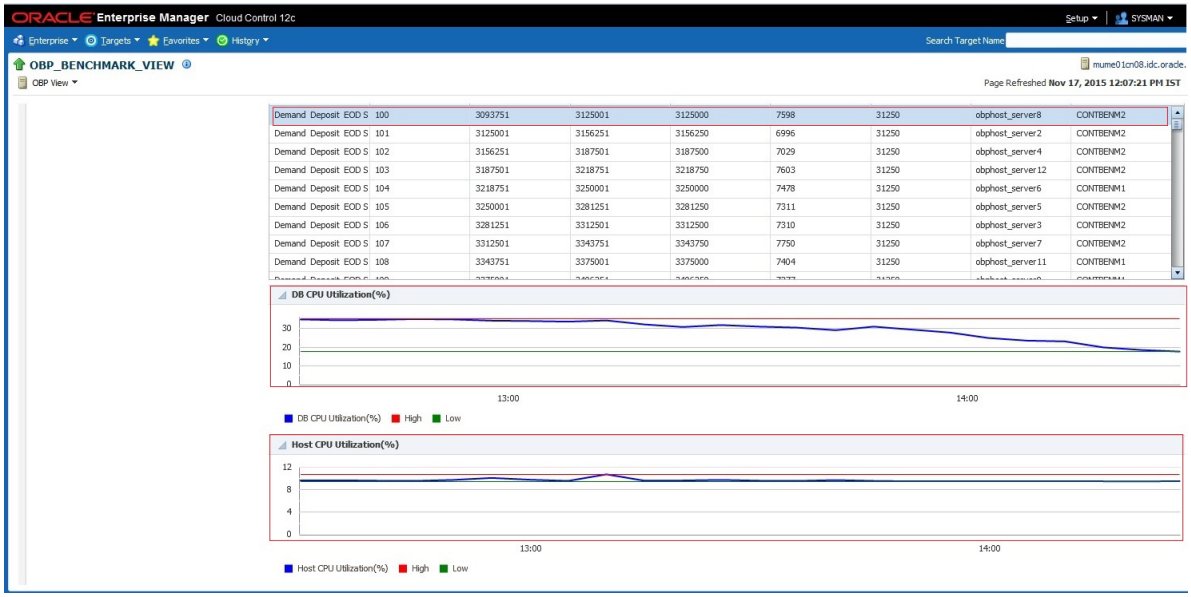
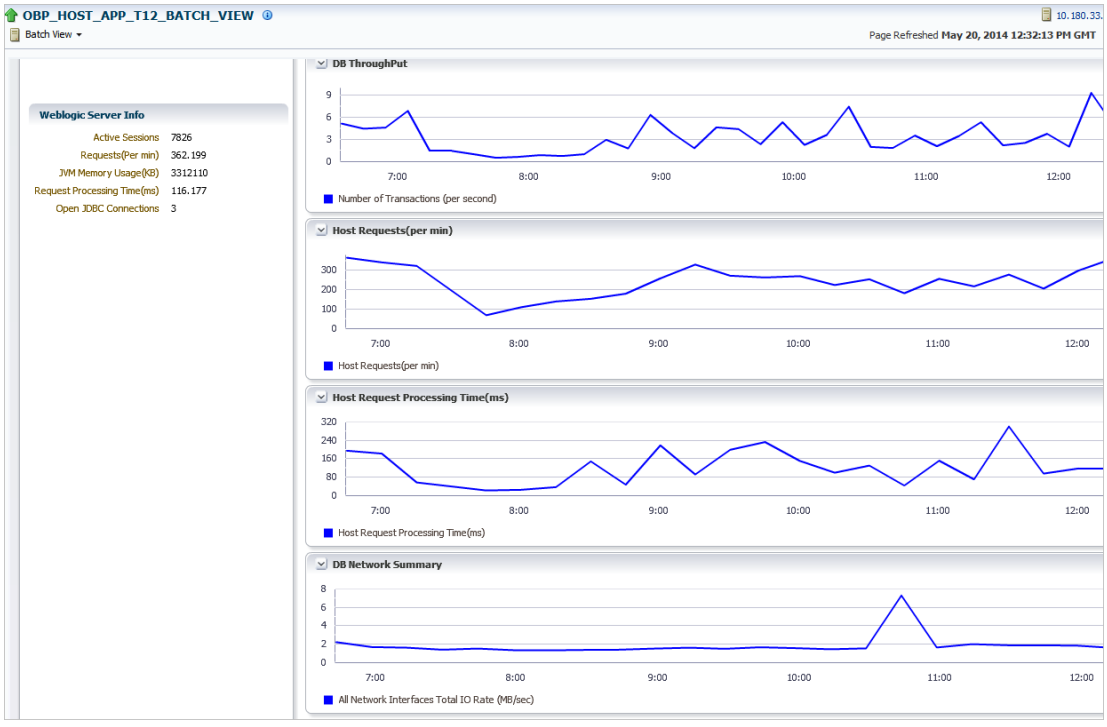


Figure 6–16 Batch Configuration

Figure 6–17 WebLogic Service Info



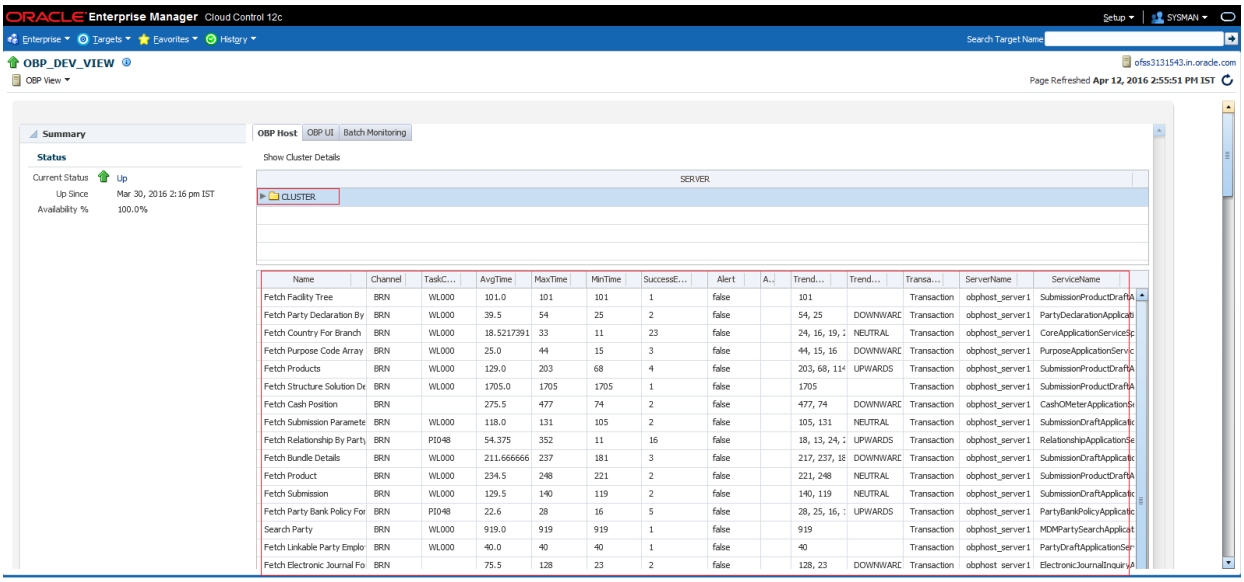
Application Monitoring

Application Monitoring shows detailed view of UI and host clusters and servers.

There are two separate tabs for UI and host. Same details are shown for both the servers. To get details of the cluster, click the Show cluster details link, which gives the cluster information in the data grid.

If you click on CLUSTER, then application metric will be displayed for all the server participating in the HOST cluster.

Figure 6–18 Application Metrics for all servers in cluster



Expand it to get the list of all the servers. Each server can be further selected to get the details at the server level. On clicking the server, the application metrics are displayed in the table as shown in the below figure.

Also, details of each metric along with the metric historical chart format can be seen on selecting any metric from the table.

Performance history graphs also gets displayed on selection of server from the cluster details table as shown below:

Figure 6–19 Application Metrics for selected server

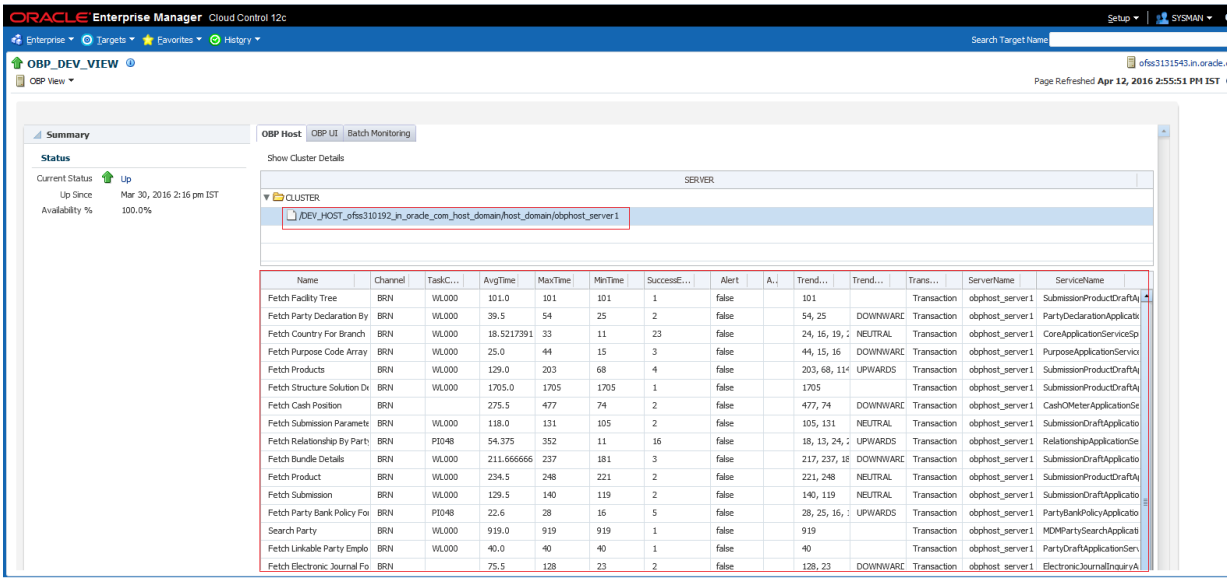
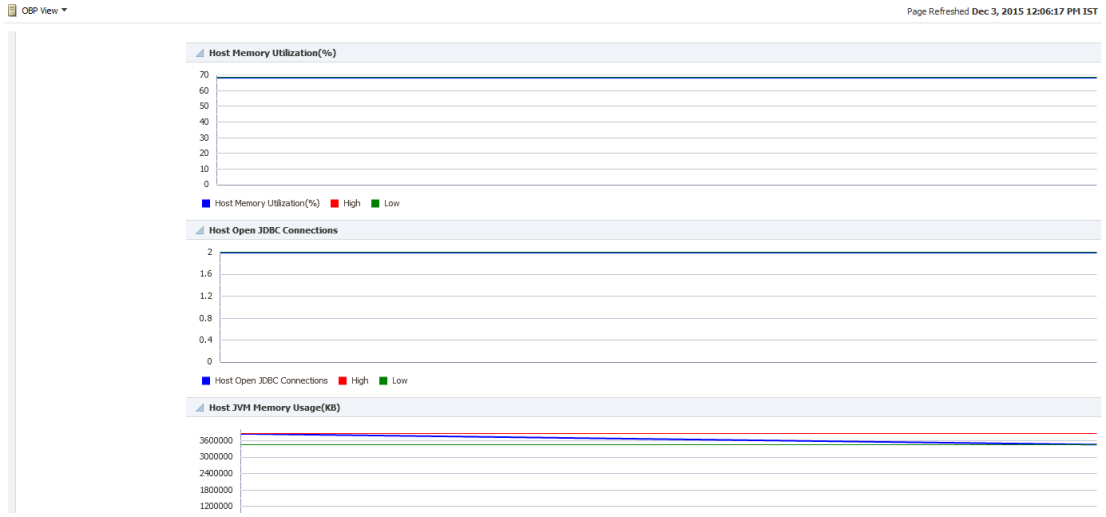


Figure 6–20 Performance History Graphs

Figure 6–21 Performance History Graphs - Continuation



7 Batch Shells in OBEPM

This chapter describes the batch shells used in OBEPM and their execution sequence.

7.1 Batch Shells Description

The following table lists the batch shells along with their detailed description.

Table 7–1 Shell Description

Sr. No.	Process Category	Category Description	Shell	Shell Description	Module Code	Detailed Description
1	3	Cut Off	co_ cutoff_ prologue	Cutoff Prologue	CO	This shell is used to indicate that the cut off has been started by setting the flg_cutoff_run_ today in flx_cs_branch_dates_b to 'Y'. (This flag is set back to 'N' at the end of the EOD category.)
2	1	End of Day	eod_ epilogue	EOD Epilogue	EO	This shell waits for all the reports to be generated and changes the Process date.
3	2	Beginning of Day	bod_ epilogue	BOD Epilogue	EO	This shell waits for all the reports to be generated.
4	2	Beginning of Day	reset_ branch_ dates	Branch Dates Reset	EO	This shell changes the branch dates for user.
5	17	Sales Offer Handoff Shell	pm_ sales_ offer_hoff	Sales Offer Handoff Shell	PM	It shell populates the staging area for the Product data elements.
6	17	Analytics Hand-Off Shell	handoff_ shell	Analytics Hand-Off Shell	DI	This shell initiates all ODI scenario execution defined in FLX_DI_ETL_JOB_DEFINITION table.
7	17	Analytics epilogue Shell	epilogue_ shell	Analytics epilogue Shell	DI	This shell checks all running ODI scenario execution status. If any error occurs, the scenario execution is restarted after resolve.

7.2 Batch Shells Execution Sequence

The following table presents the execution sequence of the batch shells.

Table 7–2 Shell Execution Sequence

Sr. No.	Process Category	Category Description	Category Significance	Shell Execution Sequence	Shell	Shell Description	Module Code	Required Shells	Required Shell Description
1	3	Cut Off	Mandatory	1	co_cutoff_ prologue	Cutoff Prologue	CO		
2	1	End of Day	Mandatory	2	eod_epilogue	EOD Epilogue	EO	handoff_ shell	Analytics Hand-Off Shell
3	2	Beginning of Day	Mandatory	4	bod_epilogue	BOD Epilogue	EO		
4	2	Beginning of Day	Mandatory	4	reset_ branch_dates	Branch Dates Reset	EO	bod_ epilogue	BOD Epilogue
5	17	Sales Offer Handoff Shell	Mandatory	3	pm_sales_ offer_hoff	Sales Offer Handoff Shell	PM		

8 Configure ODI for Inbound Document Upload

This chapter provides the steps to configure ODI for Inbound Document Upload.

For document upload ODI execution, complete the following configurations:

1. Configuring the Input directory:
    a. For example, if input directory is /scratch/odi/InboundDocument/Upload/lendingZone/
    b. Update the configuration in the table using the following SQL:

        update FLX_FW_ODI_SUB_INTERFACE_TYPE set IN_FILE_ PATH=/scratch/odi/InboundDocument/Upload/lendingZone/ ' where SUB_INTERFACE_ ID='9551';

    c. Note that the SUB_INTERFACE_ID='9551' should not be changed.
2. Configure the Schema directory:
    a. Provide the directory where all the schemas are present.

        Framework configuration:

        update FLX_FW_ODI_SUB_INTERFACE_TYPE set SCHEMA_FILE_PATH = '/scratch/odi/InboundDocument/Upload/schema/' where SUB_INTERFACE_ID ='7002';

    b. Copy all the schema for ODI mediapack zip from directory schema to the new directory which is configured for framework.
    c. Provide schema file for Document Upload.

        update FLX_FW_ODI_SUB_INTERFACE_TYPE set schema_file_ path='D:\work\odi\inDocUpload\InboundDocument\Upload\schema\scan_images_ request.0.1.XSD' where SUB_INTERFACE_ID='9551';

3. Configure Temporary directory:

    update FLX_FW_ODI_SUB_INTERFACE_TYPE set temp_file_path= '/scratch/odi/InboundDocument/Upload /lendingZonetmp/' where SUB_INTERFACE_ID='9551';

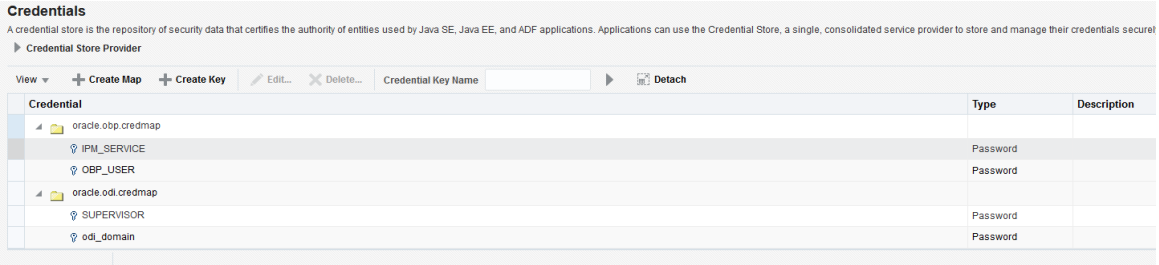
4. Configure Archive directory:

    update FLX_FW_ODI_SUB_INTERFACE_TYPE set archive_file_ path=/scratch/odi/InboundDocument/Upload/archieve/' where SUB_INTERFACE_ID='9551';

5. Create users in connector: Create two credential maps:
    - oracle.obp.credmap: This has two keys.
        - IPM_SERVICE: It has the username and password of IPM. It is used to upload the documents to IPM.
        - OBP_USER: It is required to make web service call to OBP.

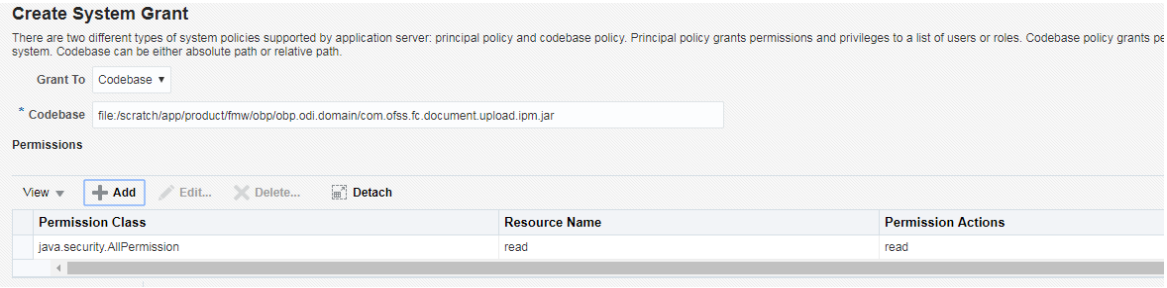
- oracle.odi.credmap
  - SUPERVISOR: It has supervisor username and password.
  - odi_domain: It has domain username and password.

Figure 8–1 Credentials



6. Provide permission to the java project for fetching the user credentials. Provide read permission to Java binary com.ofss.fc.document.upload.ipm.jar from EM.

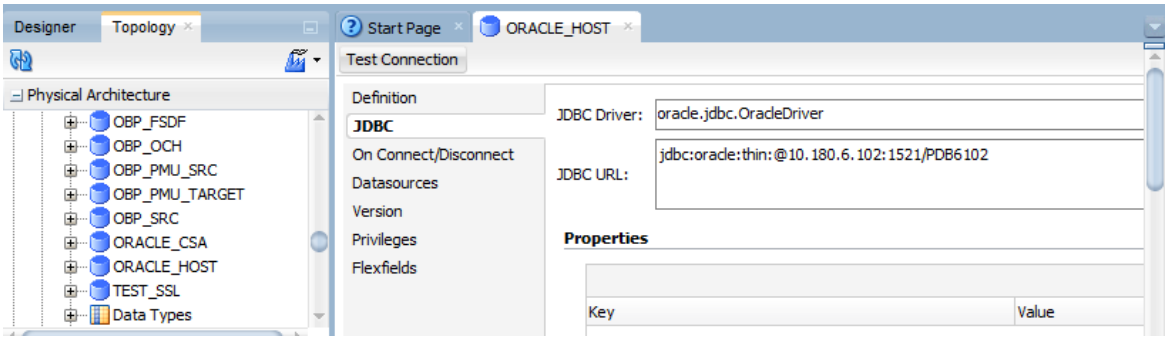
Figure 8–2 Example of premissions



7. Configuring IPM URL:
   a. update FLX_FW_ODI_SUB_INTERFACE_TYPE set GEFU_IN_FILE_PATH='http://${IPM-HOSTNAME}:${IPM-PORT}/imaging/ws' where SUB_INTERFACE_ID='9551';
   b. Replace ${IPM-HOSTNAME} with IPM Hostname or IP address.
   c. Replace ${IPM-PORT} with IPM Server port number.
8. Configure config/properties/OutboundWebserviceConfig.properties to provide OBP Host web service configuration.
   a. Replace ${OBP-HOST-IP} with OBP Host IP address or hostname.
   b. Replace ${OBP-HOST-PORT} with OBP Host managed server port.

9. Provide FJ Connection Details in ODI Topology data server ORACLE_HOST.

Figure 8–3 Connection details



9 Additional Recommendations

This chapter provides specific recommendations to be considered for implementation:

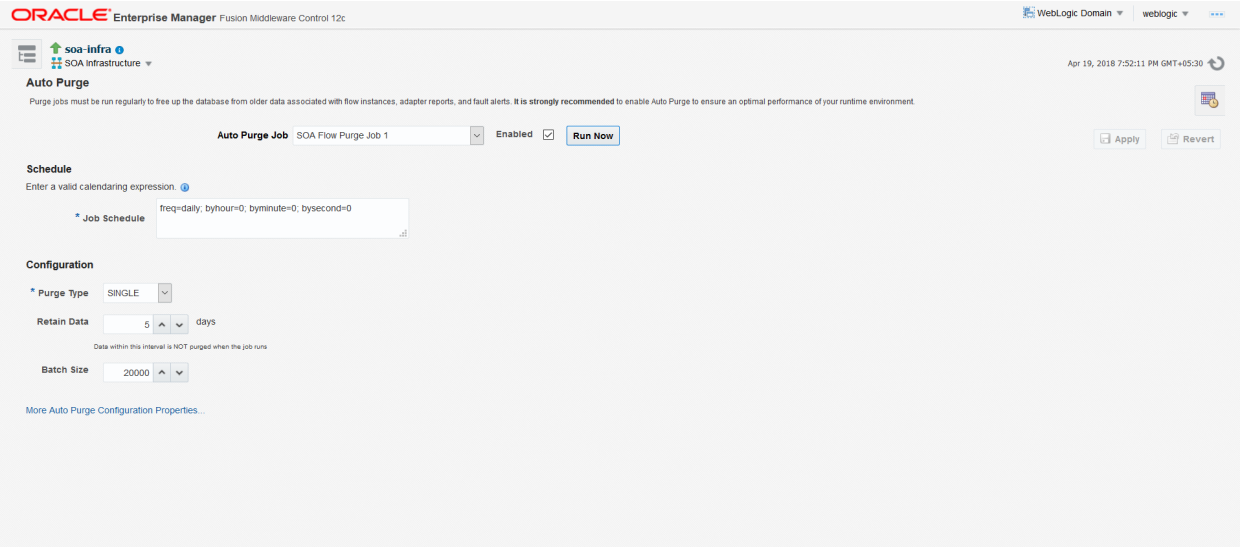
9.1 SOA Related

This section mentions certain recommendations for setting up the properties on SOA server.

9.1.1 Enable Auto Purge Job

- Oracle SOA Suite team strongly recommends periodic purging of composite instances. Purge instances as soon as they are available for purge.
- SOA suite 12c comes up with default purge job enabled with retention period of 7 days.
- It is recommended to keep this default job enabled in the production.

Figure 9–1 Auto Purge

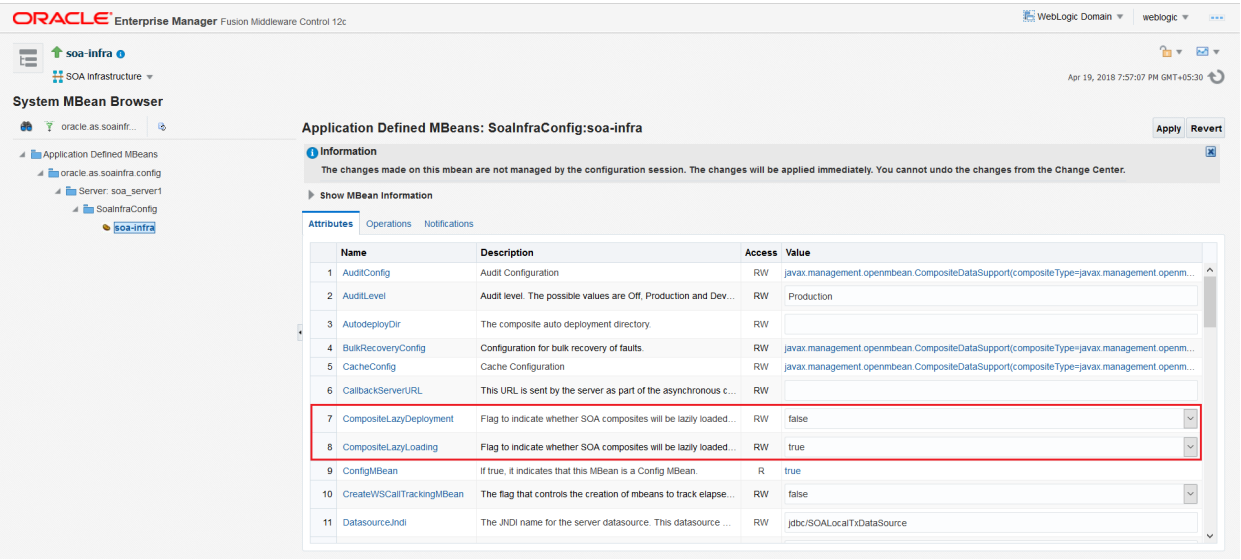


9.1.2 Enable Lazy Loading

- 12c supports lazy loading of composites on deployment as well as server startup.
- **CompositeLazyDeployment**: Loads the composites lazily on deployment.
  - More useful for non-production environments where there is frequent deployment of all the composites.
- **CompositeLazyLoading**: Loads the composites lazily on server start up.
- It is recommended to keep the default settings unchanged, that is CompositeLazyDeployment as false and CompositeLazyLoading as true in production environment.

- This will reduce the SOA server startup time.
- To confirm the settings, in SOA EM console, go to soa-infra > SOA Administration > Common Properties. Click More SOA Infra Advanced Configuration Properties link.

Figure 9–2 Lazy Loading Settings



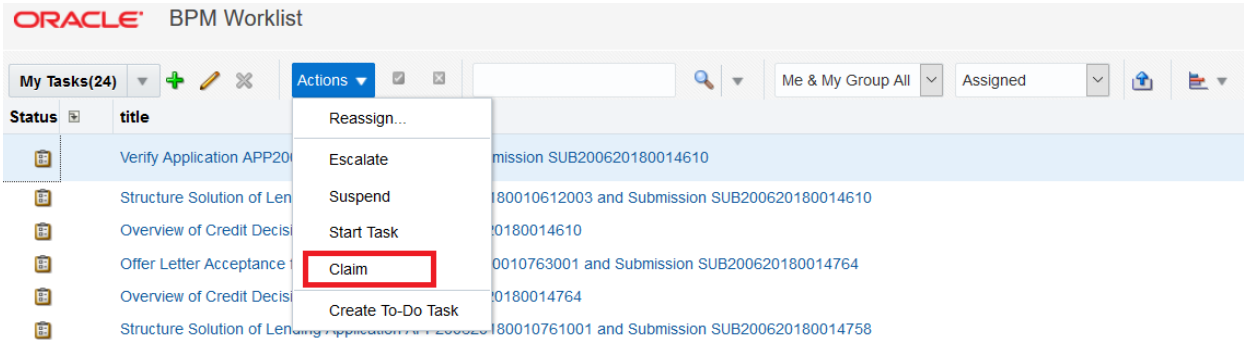
9.2 BPM Worklist Related

This section mentions certain recommendations on usage of BPM worklist.

9.2.1 Disable Claim Action from Task Details Page

- Always claim the task using worklist action menu.
- Claim option is disabled by default inside task details page.
- It can be enabled (configurable), if needed (but not recommended).
- Disabling this option helps to avoid loading of task details page twice, that is before claiming the task and after claiming the task.

Figure 9–3 Claim Action



9.2.2 Always Open Human Task Details in External Window

- BPM worklist supports two options to display the task details.
  - **Same Window**: Human task details are opened in the same browser window just below the worklist grid.
  - **External Window**: Human task details are opened in the new browser window (as a child popup).
- It is strongly recommended to make use of **External Window** option.
  - Human task details can be seen in full-screen mode.
  - Avoids unnecessary loading the task details page if user is browsing through the list of human tasks in worklist grid.
- This option can be enabled from worklist administration page.

Figure 9–4 Enable External Window option