Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.7.0
March 2018

ORACLE
FINANCIAL SERVICES

ORACLE

Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.7.0
March 2018

Part Number: E83847-01

Contents

About this Guide

This guide explains the concepts behind the Oracle Financial Services Enterprise Case Management (OFS ECM) application, and provides comprehensive instructions for system administration, daily operations, and maintenance.

This section focuses on the following topics:

- Who Should Use this Guide
- How this Guide is Organized
- Where to Find More Information
- Conventions Used in This Guide

Who Should Use this Guide

This *Administration and Configuration Guide* is designed for use by the Administrators. This user configures, maintains, and adjusts the system. The Administrator is usually an employee of a specific Oracle customer, who maintains user accounts and roles, assigns cases to users, manages case cesigner, configures and executes batch, and so on.

How this Guide is Organized

This *Administration and Configuration Guide*, includes the following chapters:

- *Chapter 1, About Oracle Financial Services Enterprise Case Management,* provides a brief overview of the Oracle Financial Services Enterprise Case Management application architecture, and its components.
- *Chapter 2, Getting Started,* provides the required day-to-day operations and maintenance of Enterprise Case Management application users, groups, and organizational units.
- *Chapter 3, Managing User Administration and Security Configuration,* provides instructions to set up and configure the Security Management System (SMS) to support ECM application, user authentication, and authorization.
- *Chapter 4, Pre Batch Execution Configuration,* provides the details of pre-batch configuration activities.
- *Chapter 5, Performing Batch Run,* provides the process to start, execute, and end batch.
- *Chapter 6, Loading Data,* provides the details to load the data from various sources to the ECM application.
- *Chapter 7, Configuring Correlation,* provides the concept and configuration of correlation.
- *Chapter 8, Scoring,* provides the concept behind scoring, methods, and types of scoring.
- *Chapter 9, Promoting to Case,* provides the configuration of promote to case activity.
- *Chapter 10, Configuring Processing Modelling Framework (PMF),* provides the concept of PMF, pre-configuration activities, and configuring workflows.

- *Chapter 11, Managing Case Designer,* provides step-by-step instruction to configure case class, case type, case attributes, case workflow, and case entities.

- *Chapter 12, General Configuration,* provides instructions to configure general parameters for case management.

- *Chapter 13, Configuring Administration Tools,* provides instructions to configure parameters specific to administration tools.

- *Chapter 14, Managing Case Assigner Editor,* provides details about ownership assignment of cases to various users.

- *Chapter 15, Configuring Actions,* provides procedures to configure the list of available actions.

- *Chapter 16, Configuring Web Application,* provides customization features available in the Web Application UI. This chapter contains information to configure session time out.

- *Appendix A, List of Processes and Tasks*, provides the details of batch processes and tasks.

Where to Find More Information

For more information about Oracle Financial Services Enterprise Case Management application, see the following documents in the Oracle Help Center (OHC):

- *Oracle Financial Services Enterprise Case Management Application Release Notes or ReadMe*

- *Oracle Financial Services Enterprise Case Management Application User Guide*

- *Oracle Financial Services Enterprise Case Management Application Installation Guide*

- *Oracle Financial Services Data Model (FSDM) Guide*

Additionally, you can find pertinent information in the OFSAAI documentation in the Oracle Help Center (OHC):

- *Oracle Financial Services Analytical Applications Infrastructure User Guide*

- *Oracle Financial Services Analytical Applications Infrastructure Installation and Configuration*

Conventions Used in This Guide

This table lists the conventions used in this guide.

Table 1. Conventions Used in This Guide

Convention	Description
Italics	- Names of books, chapters, and sections as references - Emphasis
Bold	- Object of an action (menu names, field names, options, button names) in a step-by-step procedure - Commands typed at a prompt - User input
`Monospace`	- Directories and subdirectories - File names and extensions - Process names - Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	Substitute input value

CHAPTER 1

About Oracle Financial Services Enterprise Case Management

This chapter provides a brief overview of the Oracle Financial Services Enterprise Case Management (OFS ECM) application.

The following sections are covered in this chapter:

- Introduction
- Administration and Configuration Activities

Introduction

Enterprise Case Management (ECM) supports the investigation and resolution of Anti-Money Laundering (AML), Know Your Customer (KYC), Customer Screening (CS), and third party events. A newly created case passes through various statuses as part of investigation and reaches closure through resolution actions. Enterprise Case Management supports the modification of the case details and the associated business data.

Investigation workflows can vary based on the type of case being investigated. The case investigation and resolution is supported by various actions, which can be specific to the case type. Access to types of cases and actions are controlled based on the user role and access privileges. Cases are generated from various sources and cases are also manually created in the ECM.

ECM supports product default case types that drive the Investigation workflow. Case types are configurable and can be defined by firms to meet their business need. ECM allows to design workflows using the Processing Modelling Framework. *Figure 1* depicts the ECM workflow.
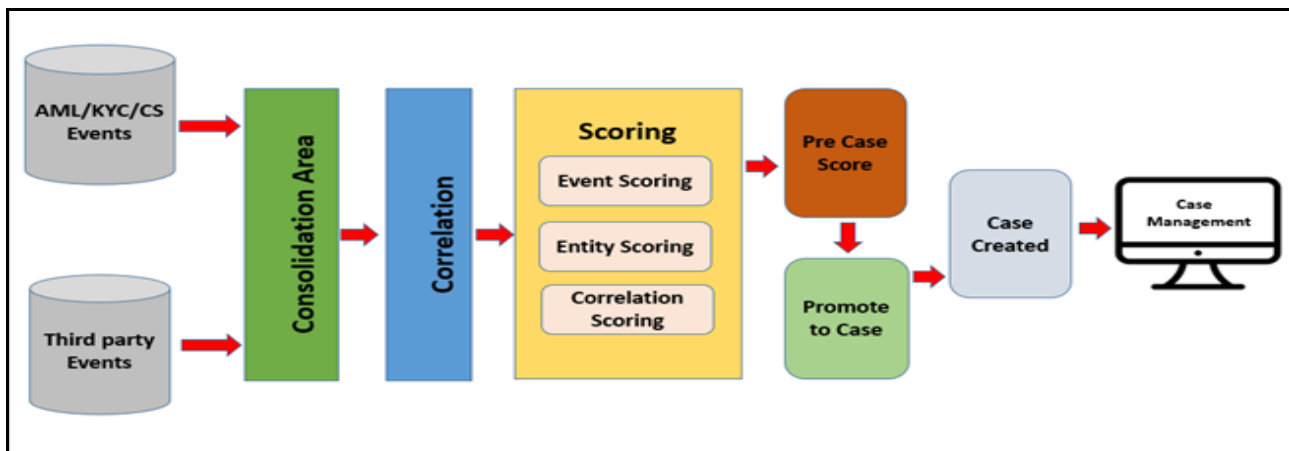
Figure 1. ECM Workflow

Administration and Configuration Activities

This section covers the following topics:

- Loading Data
- Correlation
- Scoring
- Promoted to Case
- Processing Modelling Framework
- Case Designer
- Case Assigner Editor
- Case Action Settings

Loading Data

Data is loaded from landing area to consolidated area in the ECM using processors and they are called connectors. The connector processes are used to bring the data from sources such as Oracle Behavior Detection (OBD), Oracle Know Your Customer (OKYC), Oracle Customer Screening (OCS), and third party application to ECM. These connectors are used for event processing. For more information, see the *Loading Data* section.

Correlation

After the event data is loaded from OBD, OKYC, OCS, or third party applications into ECM, you can correlate event-to-event based on business entities using configurable rule sets. This functionality is performed by the event correlation process. The group of events are identified for correlation based on business entities in an application (BD, KYC, CS or third party). For more information, see the *Configuring Correlation* section.

Scoring

Scoring is a methodology to score events, correlation, and entity (customer or account). Every event that is correlated is scored. Initial Scoring and Adjustment Scoring are two methods of scoring. Event Scoring, Entity Scoring, Correlation Scoring, Pre-case Scoring are types of scoring. Inline Processing Engine (IPE) is used to configure scoring rules. For more information, see the *Scoring* section.

Promoted to Case

Post scoring, the pre-case that crosses the promote to case threshold is promoted to case. Hence, the case is created for analysis. For more information, see the *Promoting to Case* section.

Processing Modelling Framework

The Enterprise Case Management Processing Modelling Framework (PMF) facilitates built-in tools for orchestration of human and automatic workflow interfaces. This enables the Administrator to create process-based ECM. It also enables the Administrator to model business processes and workflows. Workflows created using the

PMF are available in the Case Designer for the Administrator to associate with any Case Type. For more information, see the *Configuring Processing Modelling Framework (PMF)* section.

Case Designer

Case Designer allows the Administrator to configure Case Class, Case Type, and associated definitions. Based on the configuration, definitions are dynamically rendered in the Case Management application to investigate cases and take appropriate actions on them for case resolution. For more information, see the *Managing Case Designer* section.

Case Assigner Editor

The Case Assigner Editor allows the Administrator to view and modify the rules used to assign ownership of cases. The Case Assigner Editor allows the Administrator to create, modify, or delete a rule and define role-based assignment limits. For more information, see the *Managing Case Assigner Editor* section.

Case Action Settings

Case Action configuration allows the Administrator to adding new case statuses, configure case action data, configure standard comment data. The Administrator can configure whether or not the case actions require a comment, a reassignment, or a due-date. For more information, see the *Configuring Actions* section.

CHAPTER 2 *Getting Started*

This chapter provides step-by-step instruction to login to the OFSECM application and manage the different features of the Oracle Financial Services Analytical Applications (OFSAA) application page.

The following sections are covered in this chapter:

- System Requirements
- Accessing OFSECM Application
- Managing OFSAA Administration Page
- Troubleshooting Your Display

System Requirements

The following applications are required to run the OFSECM application:

- Microsoft Internet Explorer (IE) version 9 or later.

  Earlier versions and other browsers are not supported and can produce errors, inaccurate data and display failures. For users of IE version 8.0, the browser should be run in compatibility mode.

- Adobe Acrobat Reader version 9.0, or later.

  You can download a free copy of the latest version of the Acrobat Reader at www.adobe.com.

- Java should be installed. JDK 1.6 (version 6) or above.

- The screen resolution of the system should be set to 1280 × 1024 or higher for proper display of the user interface (UI).

  For more information, see the *OFS Enterprise Case Management Installation Guide.*

Accessing OFSECM Application

Access to the Oracle Financial Services Case Management application depends on the Internet or Intranet environment. Oracle Financial Services Case Management is accessed through Microsoft Internet Explorer (IE) Chrome. Your system administrator provides the intranet address uniform resource locator (URL).

Your system administrator provides you with a User ID and Password. Login to the application through the OFSAA login page. You will be prompted to change your password on your first login. You can change your password whenever required after logging in. For security purpose, you can change the password. For more information, see *Change Password* section.

Note: Based on your firm's configuration, you can also login with Single Sign-On (SSO).

To access OFSECM Application, follow these steps:

1. Enter the URL into your browser using the following format:

   ```
   <scheme/ protocol>://<ip address/ hostname>:<port number>/<con-
   text-name>/login.jsp
   ```

   For example: https://myserver:9080/ofsaaapp/login.jsp

   The OFSAA login page is displayed.
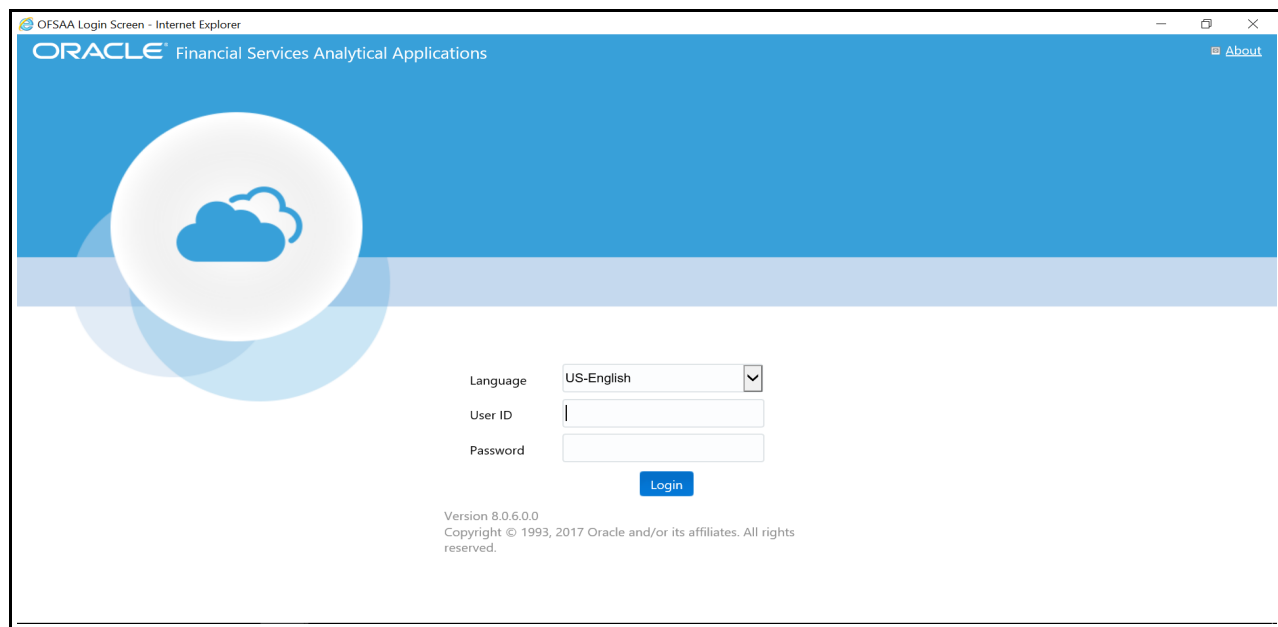
Figure 2. OFSAA Login Page

2. Select the Language from the Language drop-down list.

3. Enter your User ID and Password.

4. Click **Login**. The OFSECM Application landing page is displayed.
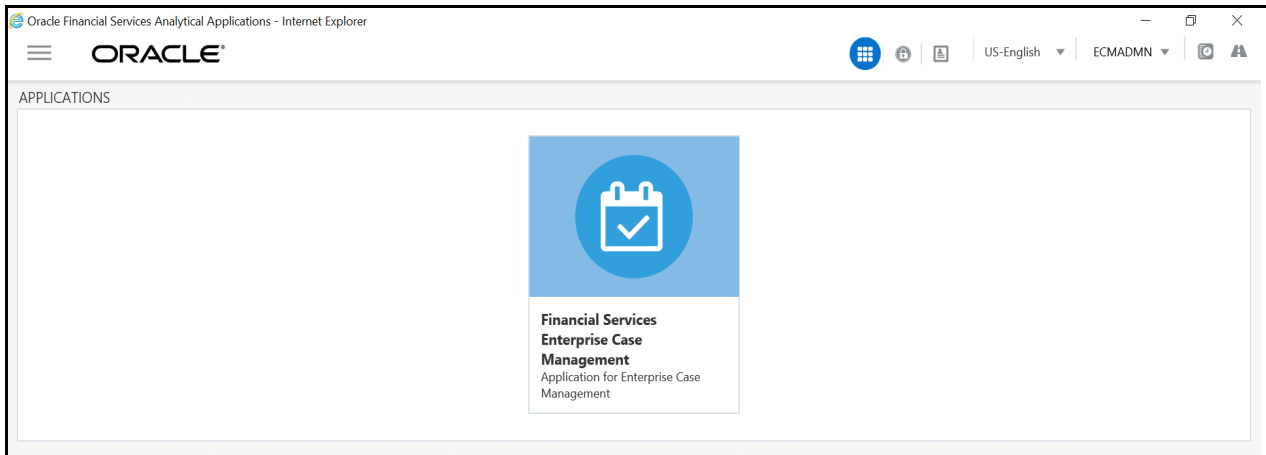
Figure 3. Case Management Page

Masthead

The masthead frame displays the user details along with the Language in the right hand corner in top frame of the window.
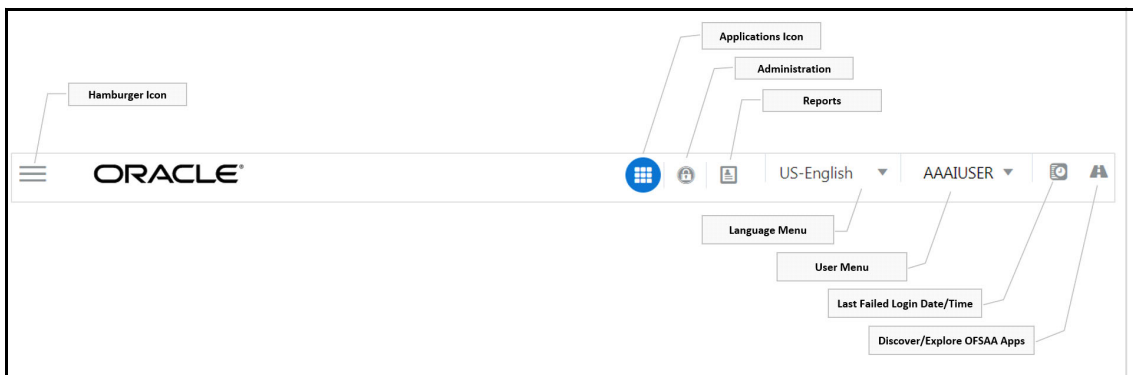
Figure 4. Masthead

The following are the components of Masthead:

- **Hamburger Icon**- This icon is used to trigger the Application Navigation Drawer.

- **Application Icon**- This icon is used to show the available Applications installed in your environment at any time.

- **Administration Icon**- This icon is used to go to the Administration module.

1. Click [icon] icon to view the last login details. It displays the last login date and time as well as the last failed login date and time.

2. Click [icon] icon to view the Information Domain to which you are connected. It also displays the setup details.

3. Click the logged in user name and sub menu is displayed.

4. Click **Preferences** to set the Home Page.

5. Click **Change Password** to change your password. For more information, see *Change Password* section. This option is available only if SMS Authorization is configured.

6. Click **Log Out** to exit Oracle Financial Services Analytical Applications Infrastructure. The built-in security system of Infrastructure ensures restricted access to the respective windows based on the user's role. This is based on the functions that you as a user are required to perform.

Change Password

For security purpose, you can change the password. This section explains how to change password.

To change the password, follow these steps:

1. Navigate to OFSAA Applications page.
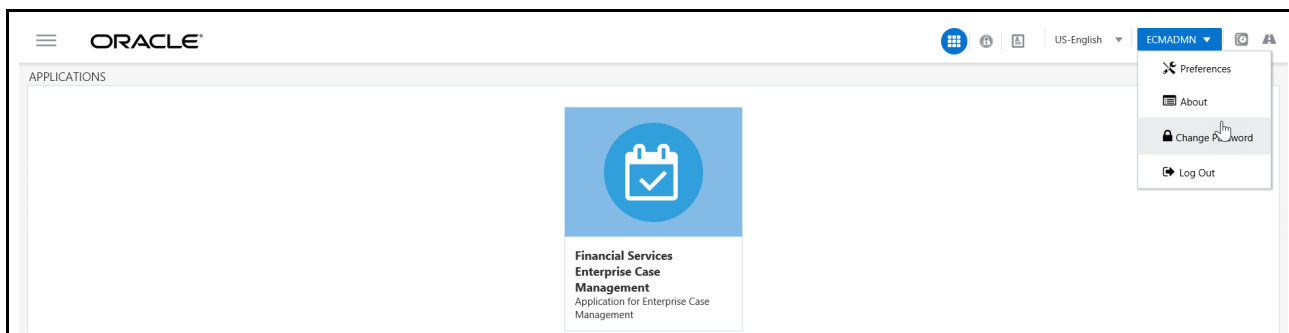
Figure 5. Change Password

2. Click the User drop-down list and select **Change Password**. The Change Password page is displayed.
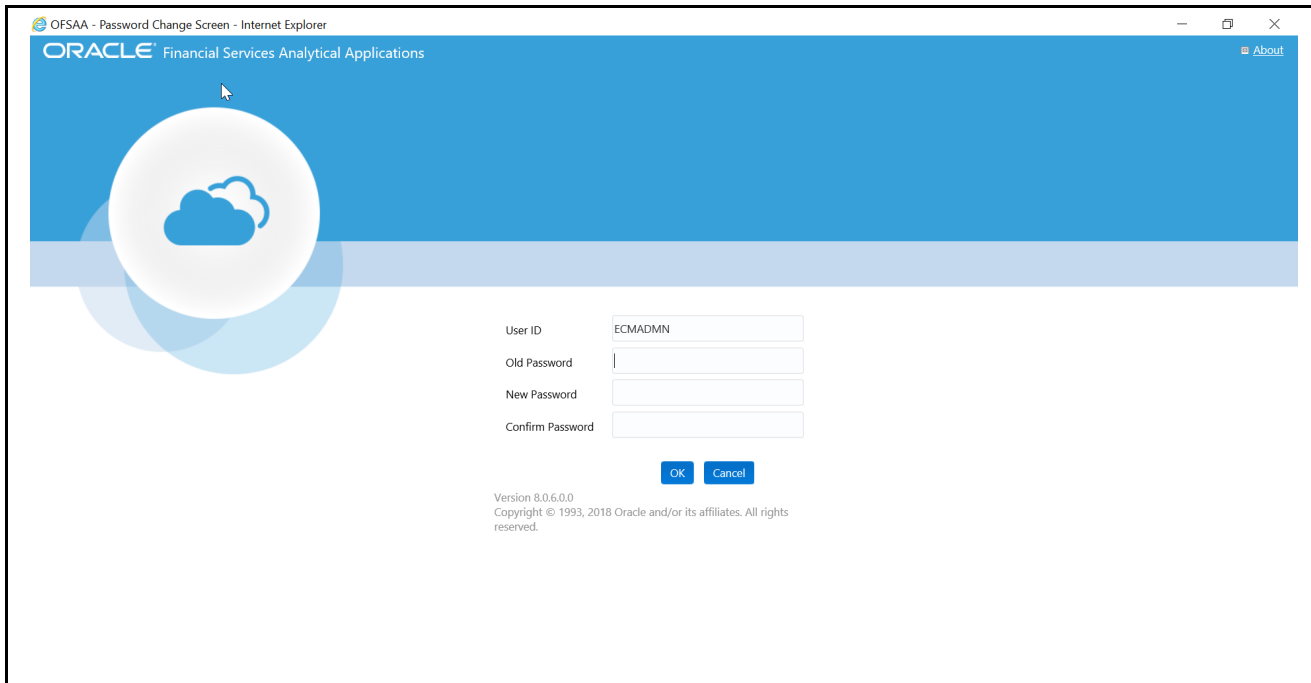
Figure 6. Change Password

3. Enter your old and new password in the respective fields.

4. Click **OK**. Your password is changed successfully. The application navigates back to the Login page where you can login with the new password.

Note: Your password is case-sensitive. If you have problems with the password, verify that the **Caps Lock** key is off. If the problem persists, contact your system administrator.

Copyright Information

To access copyright information, click the User drop-down list and select **About** in OFSAA login page.

The Copyright text displays in a new window.

Figure 7. Copyright Information

Selecting Applications

This section explains how to access required applications.

The OFSAA Applications page has multiple tabs and each tab has specific links to OFSAA Infrastructure and Application modules. The modules which you can access depend on your user role and the OFSAA Application you select. The relevant tabs and links are displayed.
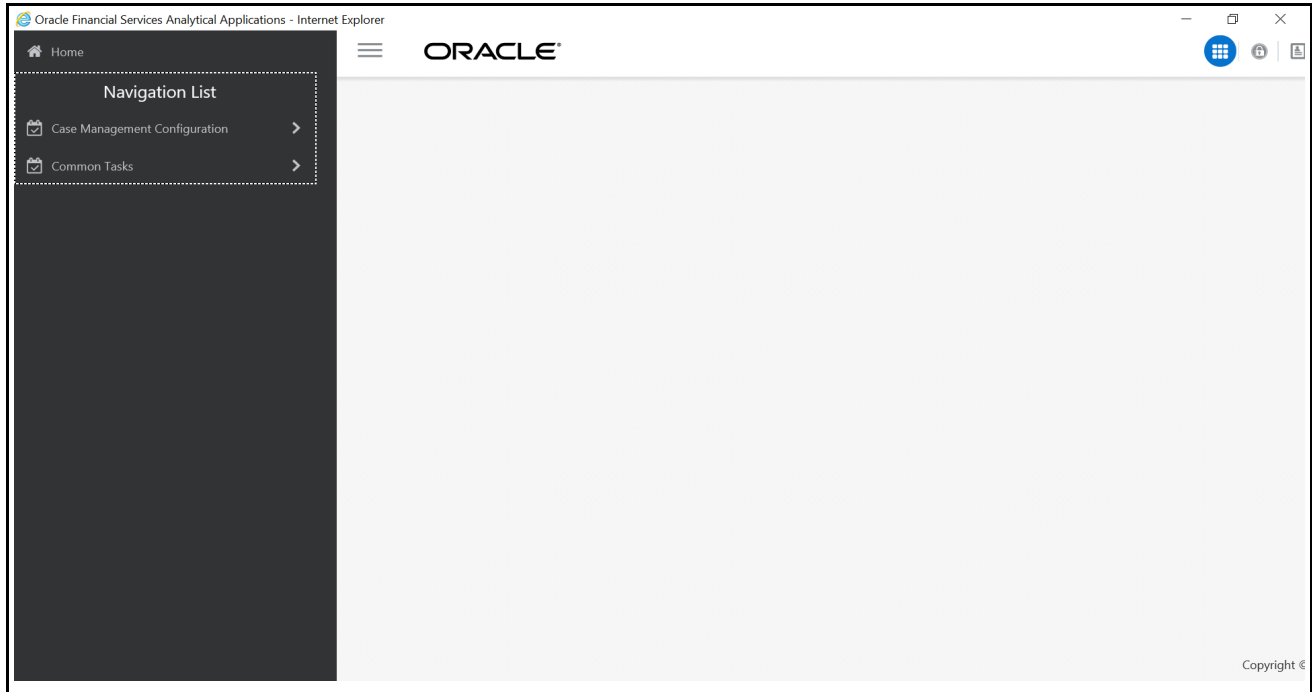
This page is divided into two panes:

- **Left Pane**: Displays menus and links to modules in a tree format based on the application selected in the Select Applications drop-down list.

- **Right Pane**: Displays menus and links to modules in a navigational panel format based on the selection of the menu in the Left pane. It also provides a brief description of each menu or link.

To access ECM applications, follow these steps:

1. Navigate to OFSAA Applications page.

2. Select **Financial Services Enterprise Case Management**. The Enterprise Case Management page is displayed.

Figure 8. Navigation List

3. Click **Case Management Configuration**. The Case Management Details are displayed.
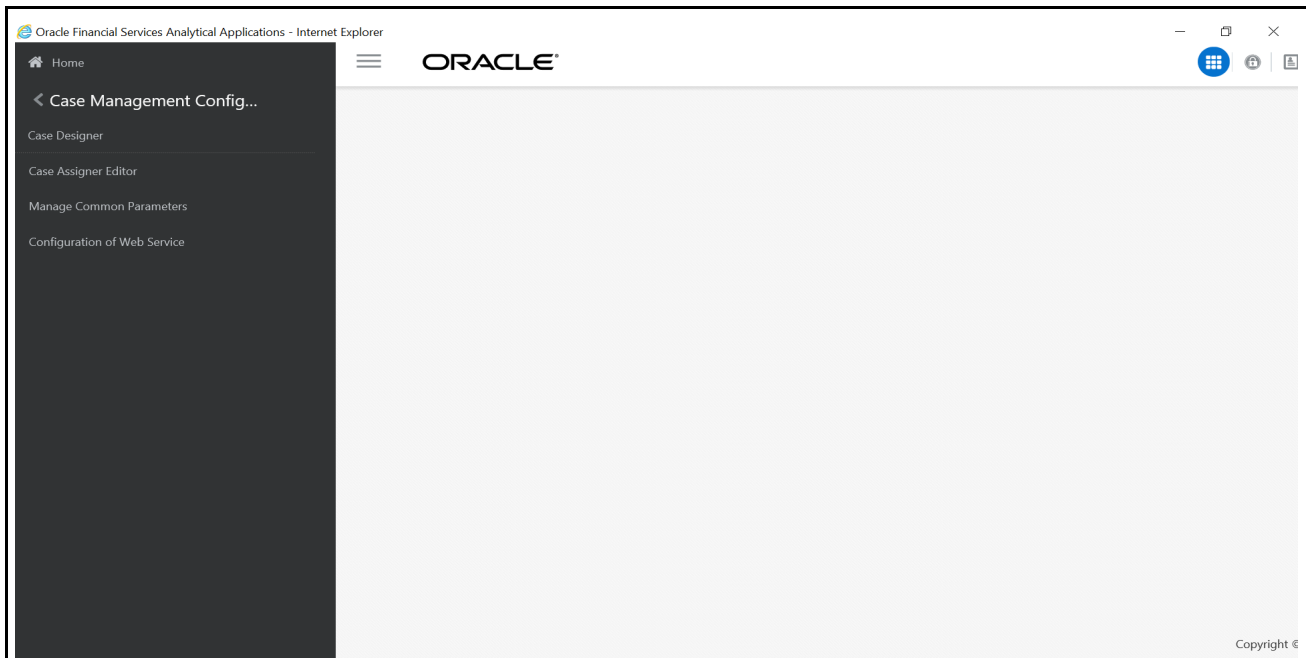
Figure 9. Enterprise Case Management Page

Managing OFSAA Administration Page

This section describes the different panes and tabs in the OFSAA Administration page.
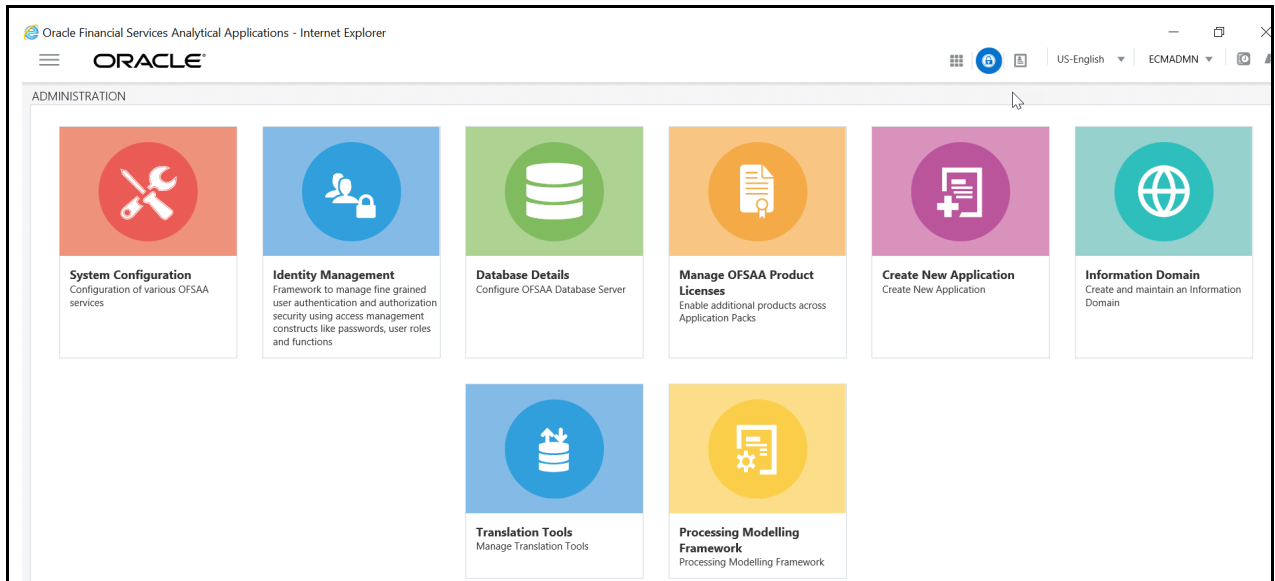
Figure 10. Administration Page

A common landing page is available for all users until a preferred application landing page has been set.

Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services ECM or with your display, the browser settings may be incompatible with running OFSAA applications. The following sections provide instructions to set the Web display options for OFSAA applications within Internet Explorer (IE).

Note: The following procedures apply to all versions of IE listed in the *System Requirements* section. Separate procedures are listed for each version where differences exist in the locations of settings and options.

This section covers following topics:

- Enabling JavaScript
- Enabling Cookies
- Enabling Temporary Internet Files
- Enabling File Downloads
- Setting Printing Options
- Enabling Pop-up Blocker
- Setting Preferences

Enabling JavaScript

JavaScript must be enabled in the browser. To enable JavaScript, follow these steps:

1. From the Tools menu, click **Internet Options**.

   The Internet Options dialog box displays.

2. Click the **Security** tab.

3. Click the **Local Intranet** icon as your Web content zone.

4. Click **Custom Level**.

   The Security Setting - Local Intranet Zone dialog box displays.

5. In the Settings list and under the Scripting setting, ensure that Enable is selected for all options.

6. Click **OK,** then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

Cookies must be enabled. If you have problems troubleshooting your display, contact your System Administrator.

Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page. To adjust your Temporary Internet File settings, follow these steps:

1. From the Tools menu, click **Internet Options**.

   The Internet Options dialog box displays.

2. On the General tab, click **Settings**.

   The Website Data Settings dialog box displays.

3. Select the **Every time I visit the webpage** option.

4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

File downloads must be available. To enable file downloads, follow these steps:

1. From the Tools menu, click **Internet Options**.

   The Internet Options dialog box displays.

2. Click the **Security** tab.

3. Click the **Local Intranet** icon as your Web content zone.

4. Click **Custom Level**.

   The Security Setting - Local Intranet Zone dialog box displays.

5. Under the Downloads section, ensure that **Enable** is selected for all options.

6. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

Printing background colors and images must be enabled. To enable this option, follow these steps:

1. From the Tools menu, click **Internet Options.**

   The Internet Options dialog box displays.

2. Click the **Advanced** tab.

3. In the Settings list, under the Printing setting, click **Print background colors and images**.

4. Click **OK** to exit the Internet Options dialog box.

Tip: For best display results, use the default font settings in your browser.

Enabling Pop-up Blocker

Some users may experience difficulty running the Oracle Financial Services ECM application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the *Allowed Sites* in the Pop-up Blocker Settings in the IE Internet Options.

To enable Pop-up Blocker, follow these steps:

1. From the Tools menu, click **Internet Options**.

   The Internet Options dialog box displays.

2. Click the **Privacy** tab.

3. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option**.**

The **Settings** is enabled.

4. Click **Settings** to open the Pop-up Blocker Settings dialog box.

5. In the Pop-up Blocker Settings dialog box, enter the URL of the application in Address of website to allow.

6. Click **Add**.

The URL appears in the Allowed sites list.

7. Click **Close**, then click **Apply** to save the settings.

8. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

The Preferences section enables you to set your OFSAA Home Page.

To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed.
   The Preferences screen is displayed.
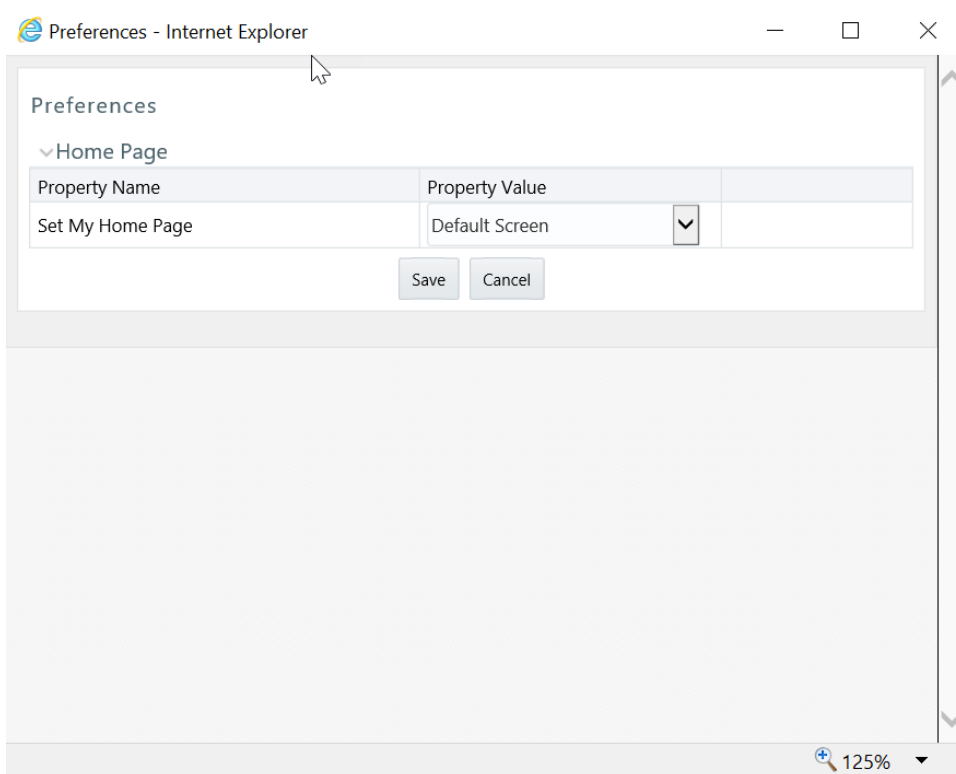
Figure 11. Preference screen.

2. In the Property Value drop-down list, select the application which you want to set as the Home Page.

   Note: Whenever new application is installed, the related value for that application is found in the drop-down list.

3. Click **Save** to save your preference.

Managing User Administration and Security Configuration

This chapter provides instructions to set up and configure the Security Management System (SMS) to support ECM application, user authentication, and authorization.

The following sections are covered in this chapter:

- About User Administration
- Administrator User Privileges
- User Provisioning Process Flow
- Managing User Administration
- Adding Security Attributes
- Mapping Security Attributes to Organizations and Users

About User Administration

User administration involves creating and managing users and providing access based on their roles. This chapter discusses the following:

- Administrator permissions
- Creating and mapping users and user groups
- Loading and mapping security attributes

Administrator User Privileges

Table 2 lists the access permissions of the ECM administrator.

Table 2. Access Permissions for Administrators

Privileges	Case Management Administrator
User Security Administration	X
Excel Upload	X
Web Service Configuration	X
Common Web Service	X
Preferences	X
User Administration	X
Security Management System	X
Security Attribute Administration	X
Manage Common Parameters	X
Case Management Configuration	X
Case Assigner Editor	X

Table 2. Access Permissions for Administrators

Privileges	Case Management Administrator
Unified Metadata Manager	X
Processing Modelling Framework	X
Case Designer	X

User Provisioning Process Flow
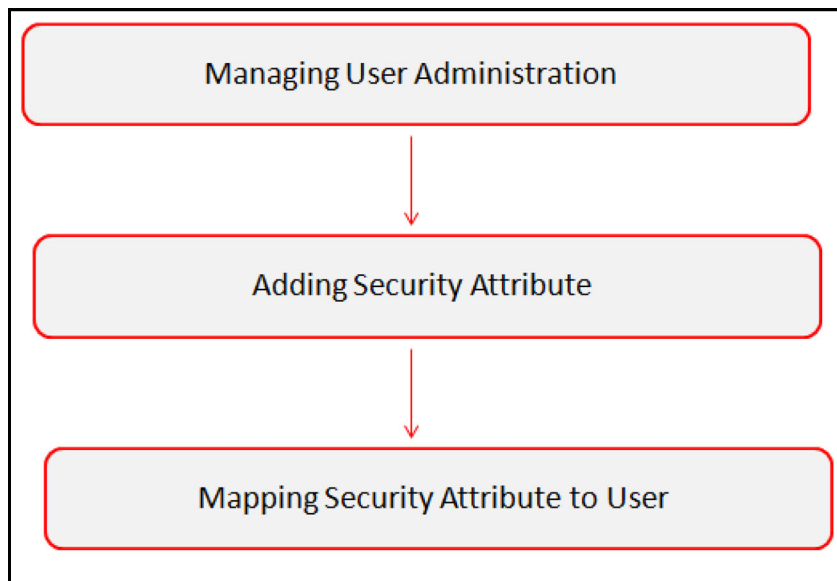
Figure 12. User Provisioning Process Flow

Table 3 lists the various actions and associated descriptions of the user administration process flow.

Table 3. User Provisioning Process Flow

Action	Description
Managing User Administration	Create users and map users to User Groups. The Administrator can provide access, monitor, and administer users.
Adding Security Attributes	Load security attributes using either Excel or SQL scripts.
Mapping Security Attributes to Organizations and Users	Map security attributes to users is to determine which security attributes control the user's access rights.

Requirements to Access ECM Application

A user gains access to the ECM application based on the authentication of a unique user ID and password.

To access the ECM application, you must fulfill the following conditions:

Table 4. Requirements

Applications	Conditions
Case Management	● Set of policies that associate functional roles with access to specific system functions ● Access to one or more case types ● One or more associated organizational affiliations that control the user's access to cases ● Access to one or more jurisdictions ● Access to one or more business domains
Administration Tools	Set of policies that associate the admin functional role with access to specific system functions

Managing User Administration

This section allows you to create, map, and authorize users defining a security framework which has the ability to restrict access to the ECM application.

Managing Identity and Authorization

This section explains how to create a user and provide access to the ECM application.

This section covers the following topics:

- Managing Identity and Authorization Process Flow
- Creating and Authorizing a User
- Mapping a User with a User Group

Managing Identity and Authorization Process Flow

Figure 13 shows the process flow of identity management and authorization.
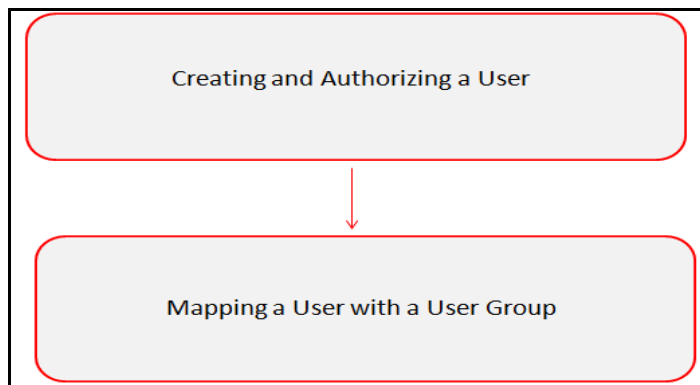
Figure 13. Managing Identity and Authorization Process Flow

Table 5 lists the various actions and associated descriptions of the user administration process flow:

Table 5. Administration Process Flow

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a user name, user designation, and dates between which the user is active in the system.
Mapping a User with a User Group	Map a user to a user group. This enables the user to have certain privileges of the mapped user group.

Creating and Authorizing a User

The SYSADMN and SYSAUTH roles can be provided to users in the ECM application. User and role associations are established using Security Management System (SMS) and are stored in the Config Schema. User security attribute associations are defined using Security Attribute Administration.
For more information on creating and authorizing a user, see *Chapter 9*, in *Oracle Financial Services Analytical Applications Infrastructure User Guide.*

Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload

To load user configuration data, follow these steps:

1. Navigate to Financial Services Enterprise Case Management, go to Common Tasks.

2. Select **Unified Metadata Manager.** Click **Data Entry Forms and Queries**.

3. Click **Upload**. Select **Config Schema Upload**.

4. Select the CSSMS_ATTRIB_MAST table in the **Select the table** drop-down list.

5. In **Select the File to Upload** field, click **Browse**. In **Choose File to Upload** window, specify the path of the data file (Microsoft Excel 2003/2007) which you want to upload. The CSSMS_ATTRIB_MAST.xlsx will be available in the `/STAGE/ExcelUpload/TEMPLATE` path inside the ftpshare folder.

6. Click **Select the Sheet** button, the Sheet Selector pop-up window is displayed. Select the required sheet from the drop-down list and click OK. If the excel contains multiple sheets, select the sheet from which data is to be uploaded. Else, by default the first sheet data is selected for upload.

7. In the Upload Type options, select one of the following:

   ■ Incremental: In this type of upload, the data in Excel sheet is inserted / appended to the target database object. The upload operation is successful only when all the data in the selected Excel Sheet is uploaded. In case of an error, the uploaded data will be rolled back.

   ■ Complete: In this type of upload, the data present in the selected database object is overwritten with the data selected Excel sheet. In case of an error, data in the selected database object will be reverted back to its original state.

8. Select Upload. If you have selected Complete upload type, you must need confirm to overwrite data in the confirmation dialog.

Creating or Editing User

To create or edit user, follow these steps:

1. Create or Edit the user for which you must map the Security Attributes.
   After loading the User configuration data into `CSSMS_ATTRIB_MAST`, a new section is displayed in User creation screen – User Attributes. This contains the following two fields. The Type of the Field is defined by the Type column in `CSSMS_ATTRIB_MAST.xlsx` file.

   ◼ Case Own Flag: The Own Case flag is required for taking ownership of the cases. Allowed Values are **Yes** and **No**.

   ◼ Line Organization: In the OOB CSSMS_ATTRIB_MAST.xlsx file, Type defined is 0 (Text box). User can provide it as 1 (Dropdown) if required and re-upload the Sheet using the Config Schema Upload.
   After updating the fields, click **Save**.

Figure 14. User Maintenance

Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user will have access to the privileges as per the role. The SYSADMN user maps a user to a user group in the ECM application.

Table 6 describes the Case Management User Roles and corresponding User Groups.

Table 6. Case Management Roles and User Groups

Role	Group Name	User Group Code
Case Analyst2	Case Analyst2 User Group	CMANALYST2UG
Case Supervisor	Case Supervisor User Group	CMSUPERVISORUG
Case Viewer	Case Viewer User Group	CMVIEWERUG
Case Administrator	Case Administrator User Group	CMMANADMNUG

Adding Security Attributes

This section explains about security attributes, the process of uploading security attributes, and mapping security attributes to users in the ECM application.

This section covers the following topics:

- Prerequisites
- Prerequisites
- Loading Security Attributes

Prerequisites

Update the FCC_SECURITY_ATTRIBUTES table before triggering the batch. This table contains the information about Jurisdiction, Business Domain and their attribute priority.

Table 7. FCC_SECURITY_ATTRIBUTES

Column Name	Description	Primary Key	Column Type	Nullable
V_ATTRIBUTE_TYPE	Type of the attribute. It should be Jurisdiction or Business Domain.	Y	VARCHAR2(50)	No
V_ATTRIBUTE_VALUE	Value of the attribute. For example, Jurisdiction name can be INDIA, AMEA, and so on. Business Domain can be Single-character code that represents a business domain (for example, a, b, or c).		VARCHAR2(50)	No
V_ATTRIBUTE_PRIORITY	Priority of the attribute. For example, value 1 for **Jurisdiction** type will have high Jurisdiction priority.		NUMBER	No

Here, the V_ATTRIBUTE_VALUE should be same as mentioned in V_JURISDICTION_CD and V_BUSINESS_DOMAIN_CD columns of FCC_EVENTS table. For example, if we have events generated with

V_JURISDICTION_CD as "AMEA" and V_BUSINESS_DOMAIN_CD as "a" then same should be updated in the respective column of FCC_SECURITY_ATTRIBUTES table.

About Security Attributes

Security Attributes help an organization classify their users based on their geography, jurisdiction, and business domain, in order to restrict access to the data that they can view.

You must map the roles with access privileges, and since these roles are associated with user groups, the users associated with the user groups can perform activities throughout the functional areas in the ECM application.

Types of Security Attributes

The following are the security attributes:

- Jurisdiction
- Business Domain
- Case Type
- Organization

Jurisdiction

OFS ECM application uses jurisdictions to limit user access to data in the database. Records from the Oracle client that the Administrator loads must be identified with a jurisdiction and users of the system must be associated with one or more jurisdictions. In the Case Management system, users can view only data or case associated with jurisdictions to which they have access. You can use a jurisdiction to divide data in the database. For example:

- **Geographical:** Division of data based on geographical boundaries, such as countries, states, and so on.
- **Organizational:** Division of data based on different legal entities that compose the client's business.
- **Other:** Combination of geographic and organizational definitions. In addition, it is client driven and can be customized.

In most scenarios, a jurisdiction also implies a threshold that enables use of this data attribute to define separate threshold sets based on jurisdictions. The list of jurisdictions in the system reside in the `KDD_JRSDCN` table.

Business Domain

Business domains are used for data access controls similar to jurisdiction, but have a different objective. The business domain can be used to identify records of different business types such as Private Client verses Retail customer, or to provide more granular restrictions to data such as employee data. The list of business domains in the system resides in the `KDD_BUS_DMN` table. The system tags each data record provided through the to one or more business domains. It also associates users with one or more business domains in a similar fashion. If a user has access to any of the business domains that are on a business record, the user can view that record.

The business domain field for users and data records is a multi-value field. For example, you define two business domains:

- **a:** Private Client
- **b:** Retail Banking

A record for an account that is considered both has `BUS_DMN_SET=ab`. If a user can view business domain **a** or **b**, the user can view the record. You can use this concept to protect special classes of data, such as data about executives of the firm. For example, you can define a business domain as *e: Executives*. You can assign this business domain to the employee, account and customer records that belong to executives. Thus, only specific users of the system have access to these records. If the executive's account is identified in the Private Client business domain, any user who can view Private Client data can view the executive's record. Hence, it is important not to apply many domains to one record.

The system also stores business domains in the `KDD_CENTRICITY` table to control access to Research against different types of entities. Derived External Entities and Addresses inherit the business domain set that is configured in `KDD_CENTRICITY` for those focus types.

Case Type

You must establish access permissions associated with the available Case Types. The Case Type is used for data access controls similar to business domains, but has a different objective. The Case Type can be used to identify records of different case types or to provide more granular restrictions to data such as case data.

The following tables are involved in the display of the Case Type in the Case Management UI and are specific to the Enterprise Case Management implementation.

- `KDD_CASE_TYPE_SUBTYPE`: Each record in the Case Type table represents a case type. Case Class is the top most definition through which a case is created.Case Type provides detailed classification of a case. When generated, a case should be mandatory assigned to one of the case types for further investigation.

Organization

Organizations are used for data access controls. Organizations are user groups to which a user belongs. The list of Organizations in the system resides in the `KDD_ORG` table.

Loading Security Attributes

This section covers the following topics:

- Loading Security Attributes through Excel
- Loading Security Attributes through SQL Scripts

For more information on loading Case type, see the *Managing Case Designer* section.

Loading Security Attributes through Excel

The Excel Upload process inserts the data into the appropriate dimension tables based on the pre-configured Excel Upload definitions installed during the application installation.

Note: Data which already exists must not be loaded again, as this results in failure of the upload. When uploading additional records, only the incremental records should be maintained in the Excel template with the correct unique identifier key.

- All template Excel files for Excel Upload are available in
  `ftpshare/STAGE/ExcelUpload/AMCMLookupFiles`
- All date values should be provided in `MM/DD/YYYY` format in the Excel worksheet.
- Whenever a record is deleted from the Excel worksheet, the complete row should be deleted (no blank active record should exist in the Excel worksheet).
- After selecting the Excel template, preview it before uploading.

Security attributes are loaded through Excel using the following templates:

Table 8. Security Attributes and Excel Templates

Security Attribute	Excel Template
Jurisdiction	`KDD_JRSDCN.xls`
Business Domain	`KDD_BUS_DMN.xls`
Organization	`KDD_ORG.xls`

Uploading Excel

To load the security attributes using excel, follow these steps:

1. Login as the Case Management Administrator. The ECM application home page is displayed.
2. Click **Case Management**. The Case Management page is displayed.
3. Mouse over the Administration menu and click **Excel Upload**. The *Excel Upload* dialog box is displayed.
4. Click **Excel Upload**.
5. Browse your system and select the Excel file.
6. Select **Sheet** from Sheet drop-down list.
7. Go to the Excel-Entity Mappings section. Click Arrow icon to select one or more Mapping IDs from the dialog box. The Excel is updated.

Loading Security Attributes through SQL Scripts

This section covers the following topics:

- Loading Jurisdictions
- Loading Business Domains
- Loading Organizations

Loading Jurisdictions

To load jurisdictions in the database, follow these steps:

1. Add the appropriate record to the KDD_JRSDCN database table as mentioned in *Table 9*.

Table 9. KDD_JRSDCN Table Attributes

Column Name	Description
JRSDCN_CD	Code (one to four characters) that represents a jurisdiction such as N for North, or S for South.
JRSDCN_NM	Name of the jurisdiction such as North or South.
JRSDCN_DSPLY_NM	Display name of the jurisdiction such as North or South.
JRSDCN_DESC_TX	Description of the jurisdiction such as Northern US or Southern US.

Note: The data in the KDD_JRSDCN database table is loaded through the Atomic schema.

2. Add records to the table using an SQL script similar to the following sample script:

```
INSERT INTO KDD_JRSDCN (JRSDCN_CD, JRSDCN_NM, JRSDCN_DSPLY_NM, JRSDCN_DESC_TX)
VALUES ('E', 'East', 'East', 'Eastern')
```

Note: The KDD_JRSDCN table is empty after system initialization and must be populated before the system starts operation.

Loading Business Domains

To load a business domain, follow these steps:

1. Add the appropriate user record to the KDD_BUS_DMN database table as mentioned in the *Table 10*.

Table 10. KDD_BUS_DMN Table Attributes

Column Name	Description
BUS_DMN_CD	Single-character code that represents a business domain such as a, b, or c.
BUS_DMN_DESC_TX	Description of the business domain such as Institutional Broker Dealer or Retail Banking.
BUS_DMN_DSPLY_NM	Display name of the business domain , such as INST or RET.

Note: The KDD_BUS_DMN table already contains predefined business domains for the Oracle client.

2. Add more records to the table using a SQL script similar to the following sample script:

```
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX, BUS_DMN_DSPLY_NM, MAN-
TAS_DMN_FL) VALUES ('a', 'Compliance Employees', 'COMP', 'N');
```

```
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX, BUS_DMN_DSPLY_NM, MAN-
TAS_DMN_FL) VALUES ('b', 'Executives'
'EXEC', 'N');

COMMIT;
```

3. Update the KDD_CENTRICITY table to reflect access to all focuses within the business domain with the following command:

```
update KDD_CENTRICITY set bus_dmn_st = 'a'
where KDD_CENTRICITY. CNTRY_TYPE_CD = 'SC'
```

Loading Organizations

To load an organization in the database, follow these steps:

1. Add the appropriate user record to the KDD_ORG database table as mentioned in *Table 11*.

Table 11. KDD_ORG Table Attributes

Column Name	Description
ORG_CD	Unique identifier for this organization.
ORG_NM	Short name for this organization that is used for display purposes.
ORG_DESC_TX	Description of this organization.
PRNT_ORG_CD	Parent organization of which this organization is considered to be a child. **NOTE:** This should reference an ORG_CD in the KDD_ORG table.
MODFY_DT	Last modified date and time for this organization record.
MODFY_ID	User ID of the user who last modified this organization data. **NOTE:** This should reference a user in the Investigation Owner table (KDD_REVIEW_OWNER.OWNER_SEQ_ID). You can also set the value to owner_seq_id 1, which is SYSTEM, if another suitable ID is not available.
COMMENT_TX	Additional remarks added by the user.

2. Add more records to the table using a SQL script similar to the following sample script.

```
INSERT INTO KDD_ORG (ORG_CD,ORG_NM,ORG_DESC_TX,PRNT_ORG_CD,MODFY_DT,MOD-
FY_ID,COMMENT_TX) VALUES ('ORG1','COMPLIANCE ORG','DEPARTMENT FOR INVESTIGA-
TION','ORG1 PARENT ORG','01-JUN-2014',1234,'ADDING KDD_ORG ENTRIES')
```

Mapping Security Attributes to Organizations and Users

This section covers the following topics:

- Introduction
- Prerequisites for Mapper Maintenance
- Using Mapper Maintenance

Introduction

The Mapping Security Attributes to Users functionality enables you to determine which security attribute controls an user's access. You can map the usergroups to security attributes using the security mapper. An Administrator maps each usergroup to Access Control metadata and Security attributes which control the user's access permissions. This is done using the Map Maintenance window.

The following are members in the Mapper:

- Usergroups
- Organization
- Jurisdiction
- Business Domain
- Case Type

Prerequisites for Mapper Maintenance

The following are the prerequisites for Mapper Maintenance:

- Loading Security Attributes Data
- Configuring Function
- Resaving Metadata
- Loading User Configuration Data

Loading Security Attributes Data

To load security attribute data, follow these steps:

1. Load the security attribute data into the following table:

Security Attribute	Table Name
Organization	KDD_ORG
Jurisdiction	KDD_JRSDCN
Business Domain	KDD_BUS_DMN

For more information, see the *Loading Data*.

Configuring Function

User can configure the Usergroups to displayed them in the Mapper window. To configure the function, follow these steps:

1. Provide the Function code in the `KDD_INSTALL_PARAM` table for param_name='`ECM Security Function`'. By default, CMACCESS function is provided.

2. All the User Groups mapped to that Function are displayed in the Mapper.

Note: The owner role should be updated in ATTR_1_VALUE_TX column. Update the owner name as mentioned in **DEFAULT_CASE_OWNER_1** to **ATTR_1_VALUE_TX** column of KDD_INSTALL_PARAM table.

Note: Update the column ATTR_3_VALUE_TX for PARAM_ID=7 with the RRS URL in KDD_INSTALL_PARAM table where you want to post the case.

For more information, see the *Configuring Administration Tools*.

Resaving Metadata

Data modifications to the Master, Reference, Base tables reflect in the Hierarchy/Derived Entity values. To enable this, Metadata re-save is required after data load into those Master/Reference/Setup table on which the hierarchy/Derived Entity is defined.

You can re-save Hierarchy/Derived Entity using Save Metadata screen.

Hierarchy Re-save

1. Login as a ECM Admin user.

2. Navigate to Financial Services Enterprise Case Management and select Common Tasks.

3. Select Utilities and click **Save Metadata**.

4. Select Hierarchy and select the below mentioned Hierarchies. To select them, use **>>** button and click **Save**.

   - ECM_User Group

   - ECM_Organization

   - ECM_Jurisdiction

   - ECM_Business Domain

   - ECM_Case Type

Derived Entity Re-save

1. Login as a ECM Admin user.

2. Navigate to Financial Services Enterprise Case Management and select Common Tasks.

3. Select Utilities and click **Save Metadata**

4. Select Derived Entity and select the below mentioned Derived Entities. To select them, use **>>** button and click **Save**.

   - DE_GRPMAST

   - DE_GROUP

   - DE_ROLE

   - DE_ROLE_FUNCTION_MAP

   - Derived Entity on Usergroup Dataset

Loading User Configuration Data
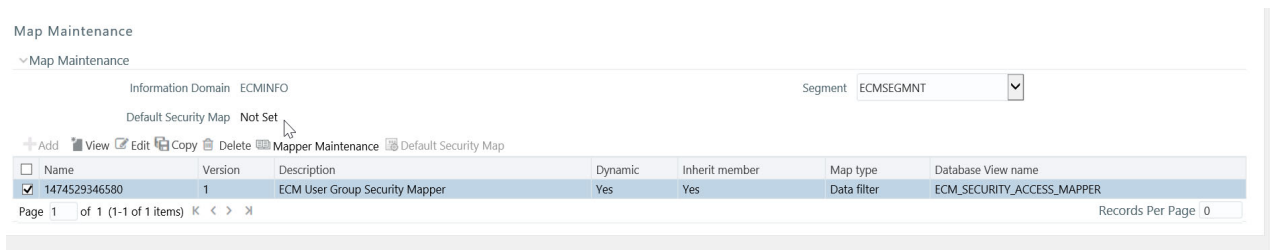
Load the User configuration data into CSSMS_ATTRIB_MAST table using Excel Upload if not done during before User creation. For more information, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Create or Edit the user for which you must map the Security Attributes. For more information, see the *Managing Identity and Authorization*.

Using Mapper Maintenance

The Line Organization and Own Case Flag parameters are mapped using the User Maintenance screen and the mapping of Security Attributes to a Case Investigation User (via usergroup) is done through the Map Maintenance.

1. Login as an ECM Admin user.

2. Navigate to Financial Services Enterprise Case Management and go to Common Tasks.

3. Select Unified Metadata Manager and click Business Metadata Management, and click **Map Maintenance**.

4. Select ECM User Group Security Mapper from the Mapper List. Click **Map Maintenance**.

5. User Group Security mapper window is displayed. Click **Add**.
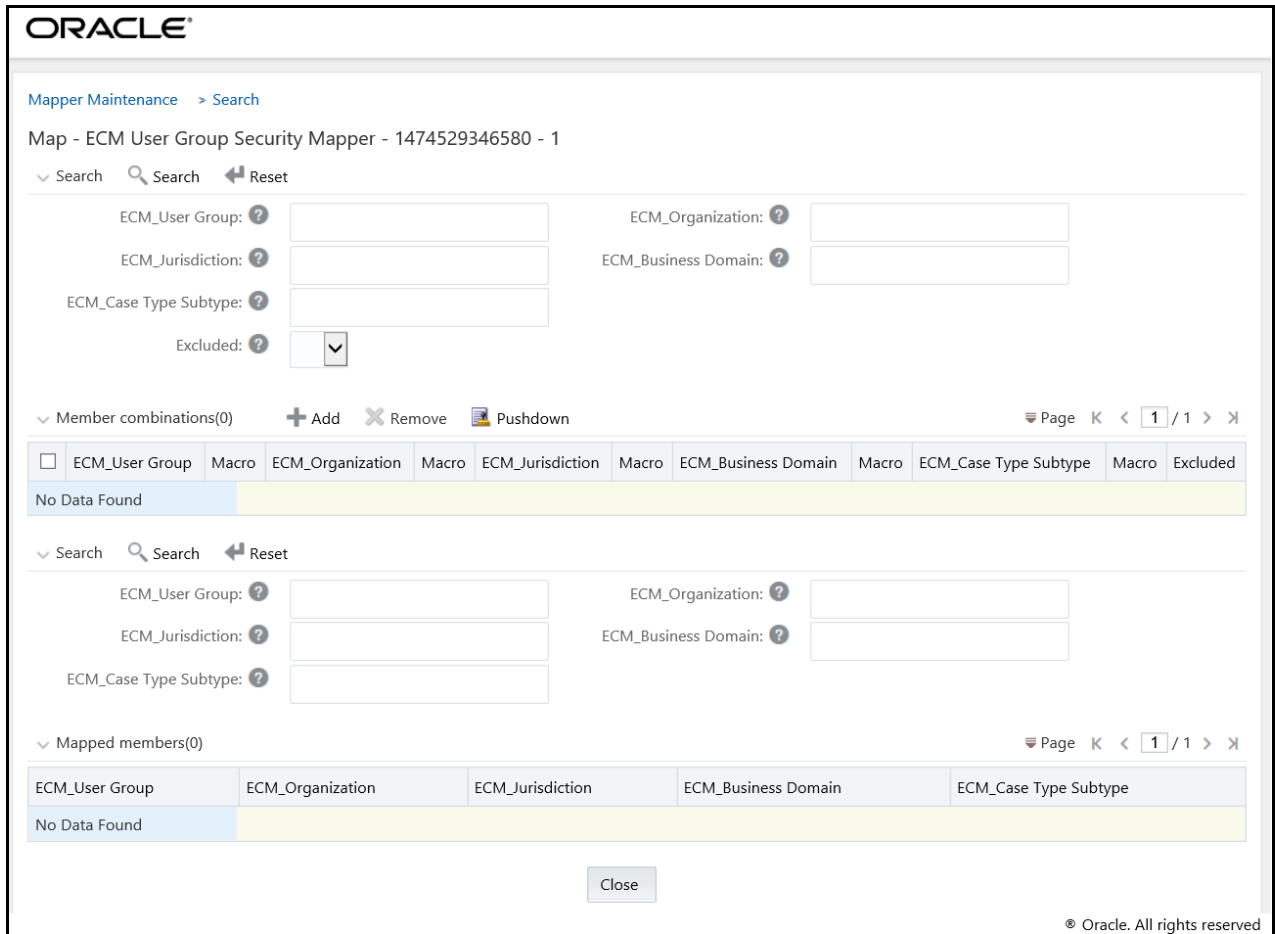
Figure 15. User Group Security Mapper window

6. The Add Mapping Screen is displayed with all the Hierarchies.

■ Usergroups of the users for the Security Attributes are mapped. Lists all User groups which are mapped to the Function code mentioned in KDD_INSTALL_PARAM.

■ Organization: A User or Organization's access to other Organization depends on the selection(s) made for this organization parameter. For example, if a user is mapped to Org1 and Org2, then user can access these two organizations, but other security attributes are also should match.

■ Jurisdiction: Mapping of one or more jurisdictions to a usergroup, gives the privilege of accessing cases that belong to the mapped jurisdiction.

■ Business Domain: Mapping of one or more business domains to a usergroup gives privilege of accessing cases that belong to the mapped business domains.

■ Case Type: Mapping of one or more Case Types to a usergroup gives them the privilege of accessing cases that belong to the mapped Case Type.

7. Select the required values from each hierarchies and click **Go**. Click **Save**.

8. Click **Save**. You are directed to previous screen, where the Member combinations can be viewed.All the changes gets saved in ECM_SECURITY_ACCESS_MAPPER table and respective view ECM_SECURITY_ACCESS_MAPPER_VW.

Note: For more information on Mapper, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide.*

Updating Control Access tables from Mapper

To reflect the changes to KDD_REVIEW_OWNER table and other control access mapping tables, you need to run the ECM Security Batch. The following process you need to follow:

- Batch Maintenance

- Batch Execution

- Batch Monitor/Checking the Execution Status

Changing ICC Batch Ownership to ECM Admin from SYSADMN user

All updates made to all the user profiles through User Maintenance UI, and Mapping done using Map Maintenance are imported from CSSMS_USER_PROFILE table of OFSSAAI configuration schema to KDD_REVIEW_OWNER table with the help of ICC Batch.

By default, the ICC Batch used for ECM Security Batch is automatically assigned to SYSADMN user during Installation. To view the batches in Batch Maintenance, follow these steps:

1. Execute the following queries in Config Schema of the Database:

   Syntax:

   ```
   begin
   AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP
   ('fromUser','toUser','infodom');
   end;
   ```

   OR

   ```
   begin
   AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP ('fromuser','touser');
   end;
   ```

   Here,

   - **fromUser** indicates the user who currently owns the batch

   - **toUser** indicated the user to which the ownership has to be transferred

   - Infodom is optional parameter, if specified the ownership of batches pertaining to that Infodom will be changed.

   For example:

   ```
   begin
   AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP('SYSADMN','ECMADMN','ECMINFO');
   end;
   ```

Batch Maintenance

The seeded Batches are viewed from the Batch Maintenance operation. To view this, follow these steps:

1. Navigate to Common Tasks and select Operations and click Batch Maintenance.

Note: If it is not visible to the Admin User, then you have to execute the steps mentioned in *Changing ICC Batch Ownership to ECM Admin from SYSADMN user*.

2. Select the `<Infodom>_ECM_SECURITY_BATCH` and select the Task1. Click **Edit** from the Task Details section.

3. Modify the **Parameter List**. Seeded values are `p_create_id`.

4. For the Parameter List-Syntax is '`p_create_id`','`p_user_id`'.

   ■ `op_create_id`: Current Admin User who is going to execute the Batch.

   ■ `op_user_id`: User(s) for which the Security Attribute Mapping changed through the Security Mapper.
   This can be changed in following two ways:

   ■ Use Case 1: If 'Parameter List', values are given as 'ECMADMN','', then Batch populates kdd_review_owner and its mapping tables for all the Users which are mapped through the Security Mapper where ECMADMN is the current logged in Admin User.

   ■ Use Case 1: If 'Parameter List', values are given as 'ECMADMN','USER1,USER2', then Batch populates `kdd_review_owner` and its mapping tables for only the Users USER1 and USER2 which are mapped through the Security Mapper where ECMADMN is the current logged in Admin User.

5. Define the 'Parameter List' values, click **Save.**

Batch Execution

The seeded Batches are executed from the Batch Execution operation.

1. Navigate to Common Task and select Operations and then click Batch Execution. The Batch Execution window is displayed.

Figure 16. Batch Execution

2. Before executing a Batch, check if the following services are running on the application server:

- ICCserver

- Router

- AM Server

- Message Server

Note: For more information, see the *Oracle Financial Services Analytical Applications Infrastructure Guide.*

3. The seeded batch (<Infodom>_ECM_SECURITY_BATCH) must be executed for the required MIS Date in this screen.

4. Select <Infodom>_ECM_SECURITY_BATCH and provide the Current Date in the Information Date section.

5. Click **Execute Batch**.

Batch Monitor/Checking the Execution Status

The status of execution can be monitored using the Batch Monitor screen.

1. Navigate to Common Task and select Operations and then click **Batch Monitor**. The Batch Monitor window is displayed.

Note: For more information on configuration and execution of a batch, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

---

2. Following are the status messages in Batch Monitor:

   ■ N: Not Started

   ■ O: On Going

   ■ F: Failure

   ■ S: Success

3. The execution log is accessed on the application server from the following directory:
   `$FIC_DB_HOME/log/date`.
   The file name has the batch execution ID. After the Batch is successful, the mappings for the User(s) is reflected in `KDD_REVIEW_OWNER` and its mapping tables. The Audit is recorded in the respective Audit Tables.

CHAPTER 4 — Pre Batch Execution Configuration

This chapter provides the details of pre batch configuration activities. ECM application batch comprises of the various processes. For more information, see the *Performing Batch Run*.

Configure the following activities before executing a batch:

- Start a Batch
- Correlation
- Correlation Case Type Mapping
- Case Priority

Start a Batch

Perform the following activities before starting a batch:

1. Add a new entry in the `FCC_PROCESSING_GROUP` table. For example, `N_GROUP_ID` can be 100 or 104 and `V_GROUP_NAME` can be E2E BATCH ALL SOURC or MAN. For examples E2E BATCH ALL SOURCE and MAN are the group names provide in the table `FCC_PROCESSING_GROUP`. `N_GROUP_ID` should be next greater numeric value.

Table 12. FCC_PROCESSING_GROUP **(Metadata Table)**

Column Name	Primary Key	Column Type	Nullable
N_GROUP_ID	Y	NUMBER(10)	No
V_GROUP_NAME		VARCHAR2(50)	No

2. Configure the parameters in Process UI (under components) from FCC_PROCESSING_GROUP table. For example:
   ```
   "MAN","","ALL","START","IND"
   ```

   This is required to indicate the name of Group for which processes are executing. Here, MAN is the Group Name.

   For more information, see the *Start Batch Run* section.

When Start Batch run is executed, it loads the data into FCC_BATCH_RUN table.

Correlation

Perform the following activities before defining correlation:

- Initiating Correlation
- Configuring Correlation Rules
- Activating or Deactivating the Correlation Rules

Initiating Correlation

Before executing the batch, trigger the shell file (`initiateCorrelation.sh`) to load all query definitions. This shell script must be run if there are changes in query definitions or in paths defined for correlation.

To initiate the correlation, follow these steps:

1. Navigate to `$FIC_HOME/ficdb/bin`.

2. Execute `initiateCorrelation.sh`. This populates the data in business entity path tables (`FCC_CORR_BUS_ENTITY_PATH` and `FCC_CORRELATION_BUS_ENTITY_CFG`). For more information, see the Using Business Entity Paths section.

Configuring Correlation Rules

After events are correlated to business entities, the event-to-business entity relationships is used to correlate events to each other. Events are grouped into a correlation if they share common business entities, and if they meet the criteria defined in the Event Correlation Rules. The logic of an Event Correlation Rule is defined in the `FCC_CORRELATION_RULE` table.

The following is an example of the rule logic defined in `FCC_CORRELATION_RULE` table:

Table 13. FCC_CORRELATION_RULE

Column Name	Primary Key	Column Type	Nullable
N_CORRELATION_RULE_SKEY	Y	NUMBER(10)	No
V_RULE_NAME		VARCHAR2(50)	No
N_PATH_PRECEDENCE		NUMBER	No
V_EVENT_FILTER_OPERATIONS		VARCHAR2	No
V_EVENT_LINK_OPERATIONS		VARCHAR2	Yes
N_LOOKBACK_VALUE		NUMBER(10)	Yes
V_LOOKBACK_UNIT		VARCHAR2(50)	Yes
F_EXTEND_FLAG		VARCHAR2	No
V_CASE_STATUS		VARCHAR2	No
V_STATUS		VARCHAR2	No
F_CORRELATION_REQUIRED_FLAG		VARCHAR2	
F_LOOKBACK_PROCESS_IND			Yes

- `N_CORRELATION_RULE_SKEY` *(required)*:This is the correlation rule unique Identification number.

- `V_RULE_NAME` *(required)*: Defines the name of correlation rule.

- `N_PATH_PRECEDENCE` *(required)*: Number indicating the maximum precedence value that a business entity shared between events must have to be considered a correlation by this rule. The lower the precedence number the stronger the relationship. Events are not considered for the correlation unless the precedence number associated with the business entity-to-event is less than or equal to (<=) the value defined.

- `V_EVENT_FILTER_OPERATIONS` and `V_EVENT_LINK_OPERATIONS` *(optional)*: Defines operations used to further constrain the events to be used for correlation. An operation consists of an event attribute compared to a numerical value , such as *from event* and *to event* which can be correlated if they both have `SCORE_CT >= 0`, represented by `CORR.SCORE_CT >= 0`, or a *from event* and *to event* which can be

correlated if CORR.ALERT_CT > 2. The set of supported comparison operators are: =, !=, <, >, <=, >=, IN, and NOT IN.

> **Note:** Because the SCNRO_ID attribute of both events and correlations can potentially have multiple values, only the IN and NOT IN operators should be used in expressions involving SCNRO_ID. The rest of the operators can only support single value operands. Also, there should be no space in the scenario ID list specified. For example, BOTH.SCNRO_ID IN (115600002,114690101).

Multiple operations can be joined together by logical AND and OR operators and operation precedence can be defined with parentheses.

● N_LOOKBACK_VALUE (*optional*): The *number* attribute indicates the number of days to look back from the current date/time to create a time window to consider events for correlation. This is a create timestamp of the event.

Note: If lookback value is defined, then lookback unit is also required.

● V_LOOKBACK_UNIT *(required)***:** The *unit* attribute identifies the unit of the look back number. Possible values are D and CM for days and current month, respectively. All of these require a valid number value except for CM, which essentially makes the look back the first of the current month , such as if the current date is October 14, we will look back to October 1 if the CM unit is selected. The create timestamp of the event is used to determine whether or not an event falls within the look back period.

Note: Do not use a unit less granular than a day in rules intended for batch events.

● F_EXTEND_FLAG(*required*): Defines the conditions for extending existing correlations. When a new correlation is discovered, it is possible that it is a superset (with only the triggering event not already included in the existing correlation) of a correlation that is previously identified. F_EXTEND_FLAG defines whether this correlation rule can result in extending an existing correlation. If this is set to FALSE (do not extend) then a new correlation is created when this condition is identified. If F_EXTEND_FLAG is set to TRUE then the existing correlation is added to unless it is already promoted to a case that has a status identified in the V_CASE_STATUS tags of NonExtendableCaseStatuses.

● F_CORRELATION_REQUIRED_FLAG*(required):* Defines the conditions for correlation required. You can set this as Y or N. If this is set to N, then every event is self linked and promoted to case. If this is set to Y, then multiple events are linked if they have common business entity and promoted to case.

● F_LOOKBACK_PROCESS_IND*(required)*: Indicates if the date of look back is event processing date or sysdate. If this is set to 1, then processing date is picked. If this is set to 0, then event created date is picked.

● V_STATUS*(required)*: Defines the status of correlation rule. By default, the correlation rule is *Active*.

   ■ To deactivate a correlation rule, modify the V_STATUS value to INACT.

   ■ To activate a correlation rule, modify the V_STATUS value to ACT.
Changes made to the metadata are effective immediately and are utilized the next time correlation is run.

Correlation Case Type Mapping

Define the Case Type mapping before executing the batch. This is performed using
`FCC_CORRELATION_CASE_TYPE_MAP` table.

Column Name	Primary Key	Column Type	Nullable
N_CORRELATION_RULE_SKEY	Y	NUMBER(10)	No
V_CASE_TYPE		VARCHAR2	No

- `N_CORRELATION_RULE_SKEY:` This is the correlation rule unique Identification number.
- `V_CASE_TYPE:` This is the type of case. The entry should be same as mentioned in KDD_CASE_TYPE_SUBTYPE table. For more information, see the *Case Type* section.

To perform this activity, follow these steps:

Add a new entry in `FCC_CORRELATION_CASE_TYPE_MAP` table. For example,
N_CORRELATION_RULE_SKEY can be 1, 2, 3 and **V_CASE_TYPE** can be CS_SAN, AML_SURV, CS_EDD.

Note: The value of `N_CORRELATION_RULE_SKEY` column (rule number) should be same as defined in FCC_CORRELATION_RULE table.

Case Priority

The scale defined in FCC_CASE_PRIORITY table should match with the rating values defined for case priority in table KDD_CODE_SET_TRNLN.

Note: If the entry is not present for a case type in table FCC_CASE_PRIORITY, then set the Case Priority as 'High'.

Case Domain and Jurisdiction

Values must be defined for jurisdiction and domain FCC_SECURITY_ATTRIBUTES table before running correlation.

Populating Country ID

Populate the KDD_COUNTRY table using the below query to select the data from STG_COUNTRY_MASTER and insert into KDD_COUNTRY table:

```
insert into kdd_country

(COUNTRY_ID, COUNTRY_CD, COUNTRY_NM, COUNTRY_DESC)

SELECT v_country_id country_id,

v_iso_country_cd country_cd,

v_country_name country_nm,
```

```
v_country_desc country_desc

FROM stg_country_master
```

Ending a Batch

Before ending a batch, configure the parameters in Process UI (under components). For example, configure the following parameters in Process UI (under components):

```
"","","ALL","END",""
```

For more information, see the *Ending a Batch Run* section.

CHAPTER 5 — *Performing Batch Run*

This chapter provides the details of ECM batch run. This chapter includes the following sections:

- About Batch Run
- Starting a Batch Run
- Ending a Batch Run
- Executing a Batch Run

About Batch Run

The ECM application batch run comprises of the following processes:

- Start ECM batch
- Load events, evented, and business data to Consolidation area
- Correlation
- Scoring
- Promote to case
- Create a case
- End ECM batch

Starting a Batch Run

Note: For executing a batch, you cannot start two batches simultaneously for same processing group.

This section explains how to start the batch run.

To start the batch run, follow these steps:

1. Navigate to Enterprise Case Management Application.
2. Go to the Common task section. Select the **Run Rule Framework**.
3. Click **Run**. The Run window is displayed with the available Processes.
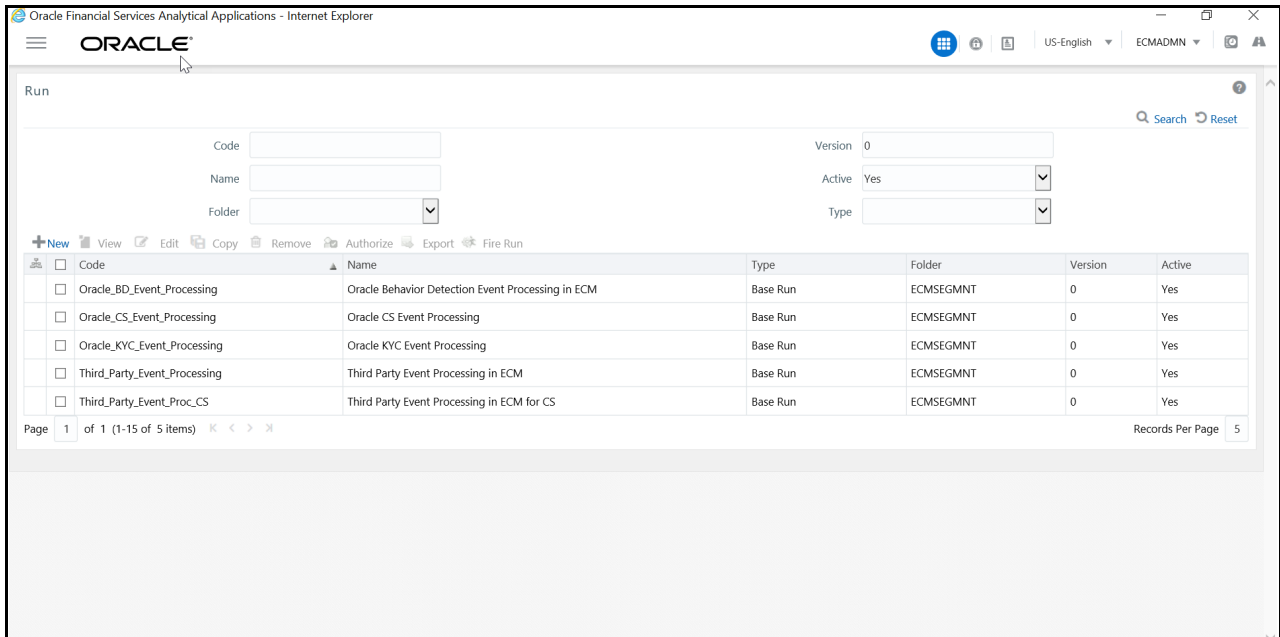
Figure 17. Application List

4. Go to the List section. Select an application for example (`Oracle_BD_Event_Processing`). The list of processes for selected application is displayed.
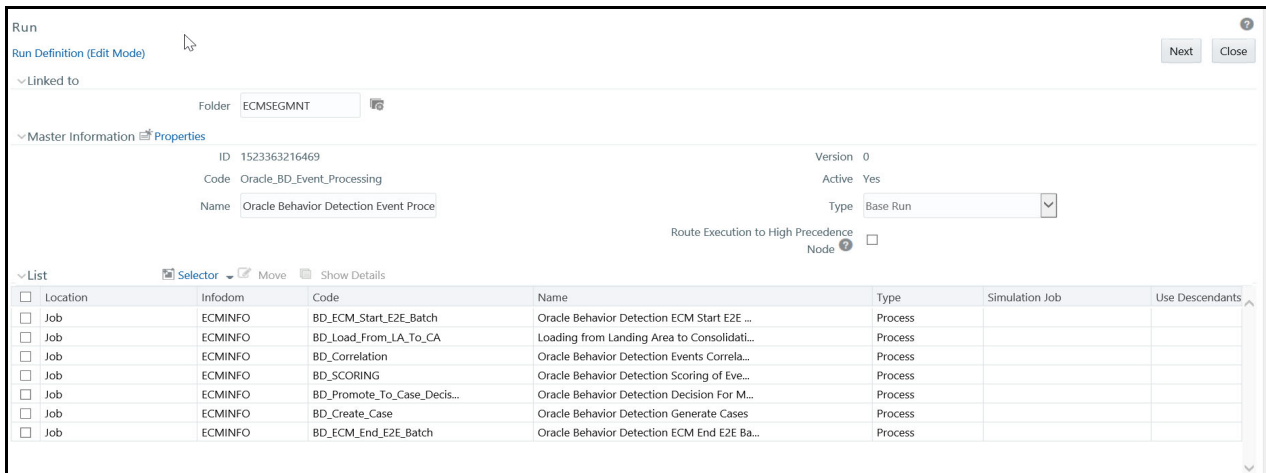
Figure 18. List of Processes

5. Navigate to Process Summary Page and search for **BD_ECM_Start_E2E_Batch**.

6. Select the batch **BD_ECM_Start_E2E_Batch** and click **Edit.**
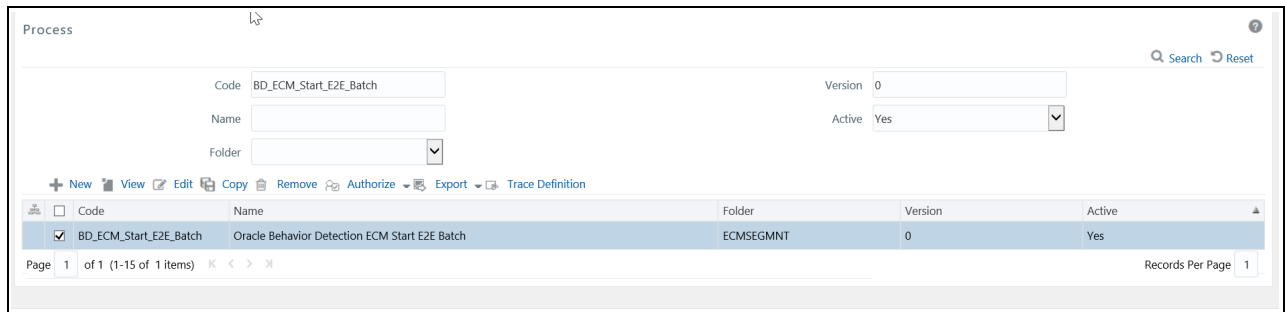
The Process Definition page is displayed.
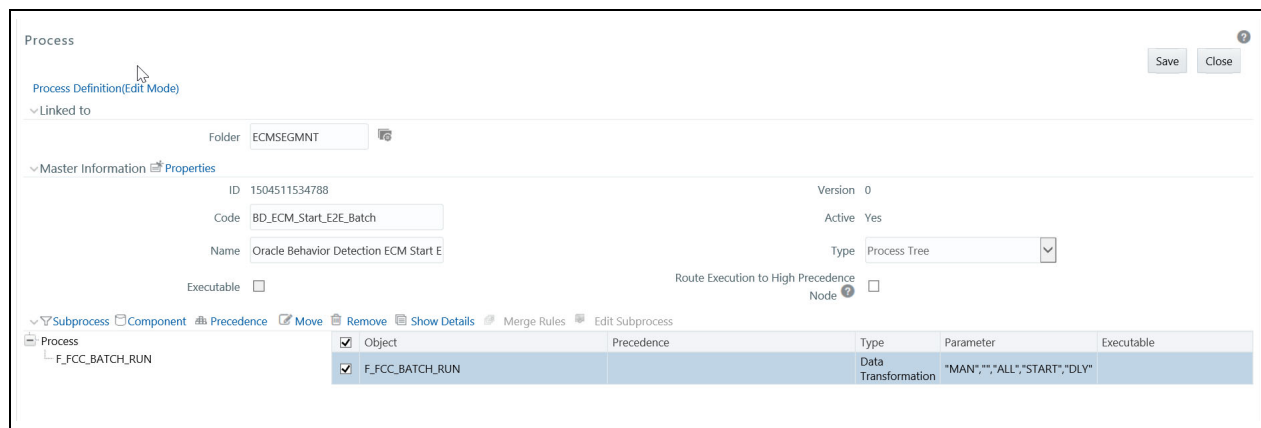
7. Click **Component.** The Component Selector window is displayed.

8. Click **Parameters** option. The Parameters window is displayed.
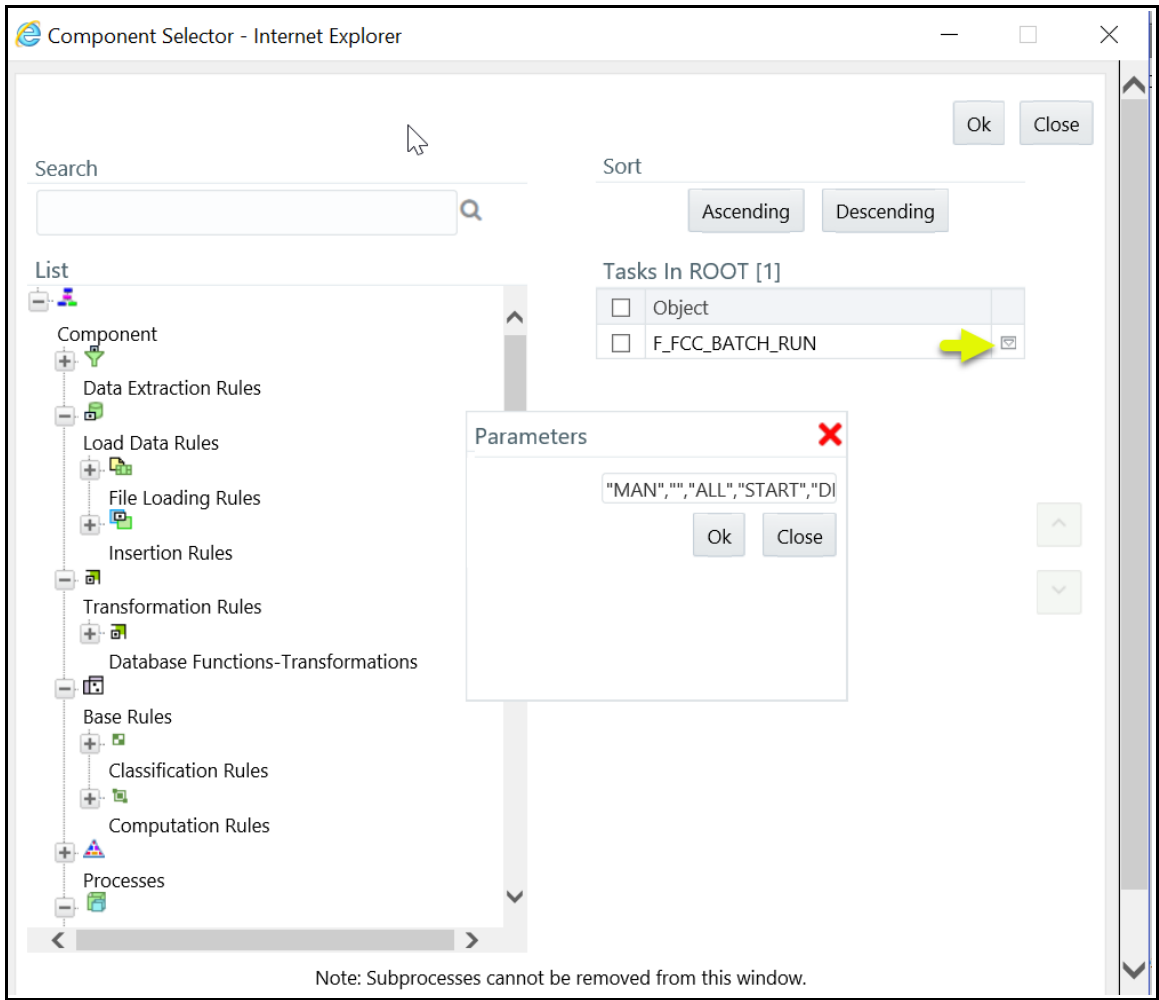
Figure 19. Parameters

The following are default parameters:

`"MAN","","ALL","START","DLY"`

- **MAN**: is group name. Modify the name of group as mentioned in `FCC_PROCESSING_GROUP` table. For example, `E2E BATCH ALL SOURCE`

- **""** Source Batch for Correlation

- **ALL**: is component that can be modified if required

- **START**: is used to start the batch

- **DLY**: is Data Origin

The following is an example of parameter

`"E2E BATCH ALL SOURCE","","ALL","START","IND"`

9. Modify the parameters and click **OK**.

Ending a Batch Run

This section explains how to end the batch run.

To end the batch run, follow these steps:

1. Navigate to Process Summary page and search for End Batch, for example `BD_ECM_End_E2E`.
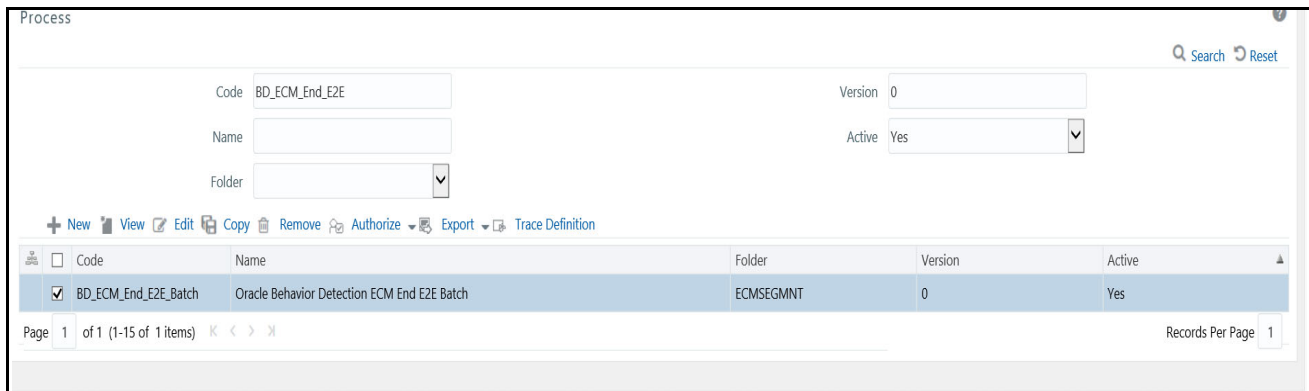
Figure 20. Application Batch List

2. Click **Edit**. The Process Definition page is displayed.

3. Click **Component.** The Component Selector window is displayed.

4. Click Parameters option. The Parameters window is displayed. Following are default parameters:

   The following are default parameters:

   `"","","ALL","END",""`

   ■   Source Batch for Correlation

   ■   **ALL**: is component. Modify the component if required

   ■   **END**: is used to end the batch

5. Modify the parameters and click **OK**.

Executing a Batch Run

This section explains how to execute the batch run.

To access and execute the batch run, follow these steps:

1. Navigate to Enterprise Case Management Application.

2. Go to the Common task section. Select the **Run Rule Framework**.

3. Click **Run**. The Run window is displayed with the available Processes.

4. Select the Application process from the Run definition page list that is to be executed and click **Fire Run**. The Fire Run window is displayed.
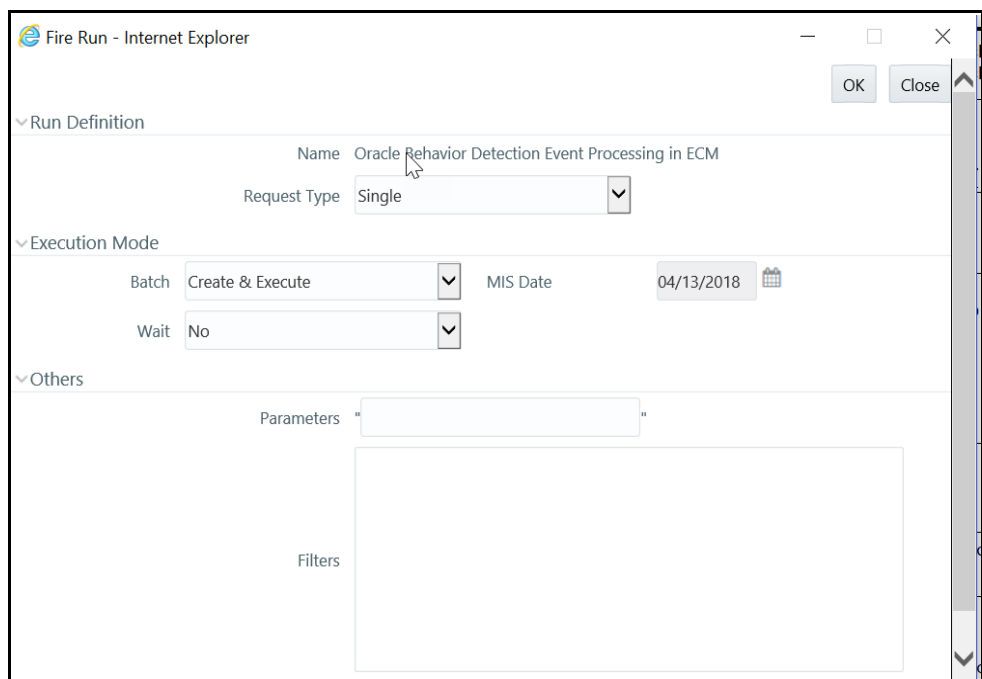
Figure 21. Fire Run

5. Enter the following details:

Table 14. Adding Fire Run Details

Fields	Description
Request Type	Select Request Type based on the following options: ● Single: If the batch must be executed once. ● Multiple: If the batch must be executed multiple times at different intervals.
Batch	Select Batch. It has the following options: ● Create ● Create & Execute From these options, select Create & Execute

Table 14. Adding Fire Run Details

Wait	Select Wait. It has the following options: ● Yes: This executes the batch after a certain duration. Enter the duration as required. ● No: This executes the batch immediately.
Filters	Enter the filter details. **Note:** $MISDATE option can be used to execute the run for that particular day. The format for it to enter in the filter details is: `to_date(<ACTIVITY_TABLE_NAME>.<ACTIVITY_DT_COL>)=$MISDATE` **Note:** For $MISDATE option: ● For either Date or Timestamp datatypes, to_date is mandatory for the filter. ● Activity Table Name and Activity Column Name should be in capital.

6. Click **OK** to run the batch. The following message is displayed: *Batch Execution is in progress.*

Note: If batch execution fails, then see the batch details in Batch Monitor. For more information on Batch Monitor, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide.*

7. Once the batch is triggered, following processes get executed:

   a. Start ECM batch, select required process code. For example, BD_ECM_Start_E2E_Batch. For more information on starting the batch, see *Starting a Batch Run*.

   b. Load events, evented, and business data to Consolidation area, select required process code. For example, BD_Load_From_LA_To_CA. For more information on using this connector, see *Loading Data*

   c. Perform correlation on loaded events and select required process code. For example, BD_Correlation. For more information on using correlation, see *Configuring Correlation*.

   d. Perform scoring on correlated events and select required process code. For example, BD_SCORING. For more information on using scoring, see *Scoring Rules*.

   e. Determine to promote correlated events to a case and select required process code. For example, BD_Promote_To_Case_Decision. For more information on using promote to case, see *Promoting to Case*.

   f. Create a case event and select required process code. For example, BD_Create_Case.

   g. End ECM batch and select required process code. For example, BD_ECM_End_E2E_Batch. For more information on running the batch, see *Ending a Batch Run*.

The following table provides you the complete details of Applications and related processes.

Table 15. Application Run processes

Process	Applications and Process Name			
	OBD	**OCS**	**OKYC**	**Third Party**
Start ECM batch	BD_ECM_Start_E2E_Batch	ECM_Start_E2E_Batch_For_CS	ECM Start E2E Batch For KYC	ECM Start E2E Batch
To load events, evented, and business data to Consolidation area	BD_Load_From_LA_To_CA	Load_From_CS_To_CA	Load_From_OKYC_To_CA	Load_From_LA_To_CA

Process	Applications and Process Name			
	OBD	**OCS**	**OKYC**	**Third Party**
Perform correlation on loaded events	BD_Correlation	Correlation	Correlation	Correlation
Perform scoring on correlated events	BD_SCORING	Scoring_OCS	Scoring_OKYC	Scoring
Decision to promote correlated events to a case	BD_Promote_To_Case_Decision	Promote_To_Case_Decision_OCS	Promote_To_Case_Decision_OKYC	Promote_To_Case_Decision
Create a case	BD_Create_Case	Create_Case	Create_Case	Create_Case
End ECM batch	BD_ECM_End_E2E_Batch	ECM_End_E2E_Batch_For_CS	ECM_End_E2E_Batch_For_KYC	ECM_End_E2E_Batch

CHAPTER 6 — *Loading Data*

This chapter provides the details of loading the data from different sources in the ECM. The following sections are covered in this chapter:

- About Loading Data
- Using Connectors
- Data Movement (DM) Utility
- Configuring Data Movement from LA to CA

About Loading Data

Data is loaded from landing area to consolidated area in the ECM using processors and they are called connectors. The connector processes are used to bring the data from different sources such as Oracle Behavior Detection (OBD), Oracle Know Your Customer (OKYC), Oracle Customer Screening (OCS), and third party application to the ECM. These connectors are used for event processing.

> **Note:** ECM does not support Multi-Match alerts.

Types of Connectors

The following are the sample connector types available in the ECM:

- OBD
- OKYC
- OCS
- Third Party

Using Connectors

This section describes how to use connector processes for different applications in the ECM. The following sections are covered in this topic:

- Accessing Connector Processes
- Using OBD Connector Process
- Loading OCS Data
- Using KYC Connector Process
- Loading Third Party Connector Data

Accessing Connector Processes

This section explains how to access different application connectors list in the Run window.

To access connectors, follow these steps:

1. Navigate to Enterprise Case Management Application.

2. Go to the Common task section. Select the **Run Rule Framework**.

3. Click **Run**. The Run window is displayed.

Loading OBD Data

The OBD connectors are used to load data from the BD application to the ECM.

To load data from the OBD to the ECM, follow these steps:

1. Navigate to the Run window.

2. Go to the List section. Select **Oracle_BD_Event_Processing**. The list of processes for OBD is displayed.
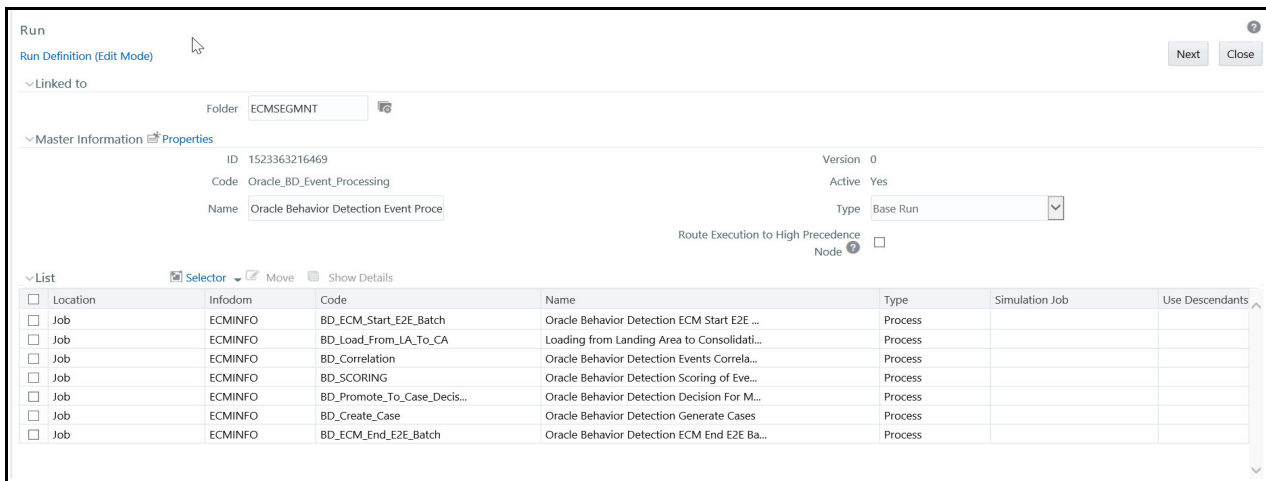
Figure 22. BD Processes

3. Select **BD_Load_From_LA_To_CA** (connector) process from the list. This has the following four sub processes:

   ■ Loading BD Events

   ■ Entity Surrogate Key Generation for BD

   ■ Oracle Behavior Detection Evented Data Load

   ■ Oracle Behavior Detection Business Data Load

For more information on processes and tasks, see the *Appendix A, List of Processes and Tasks*.

For more information on Configuring Data Movement from LA to CA, see the *Configuring Data Movement from LA to CA* .

Loading OCS Data

The OCS connectors are used to load data from the CS application to the ECM.

To load data from the OCS to the ECM, follow these steps:

1. Navigate to the Run window.

2. Go to the List section. Select **Oracle_CS_Event_Processing**. The list of processes for OCS is displayed.
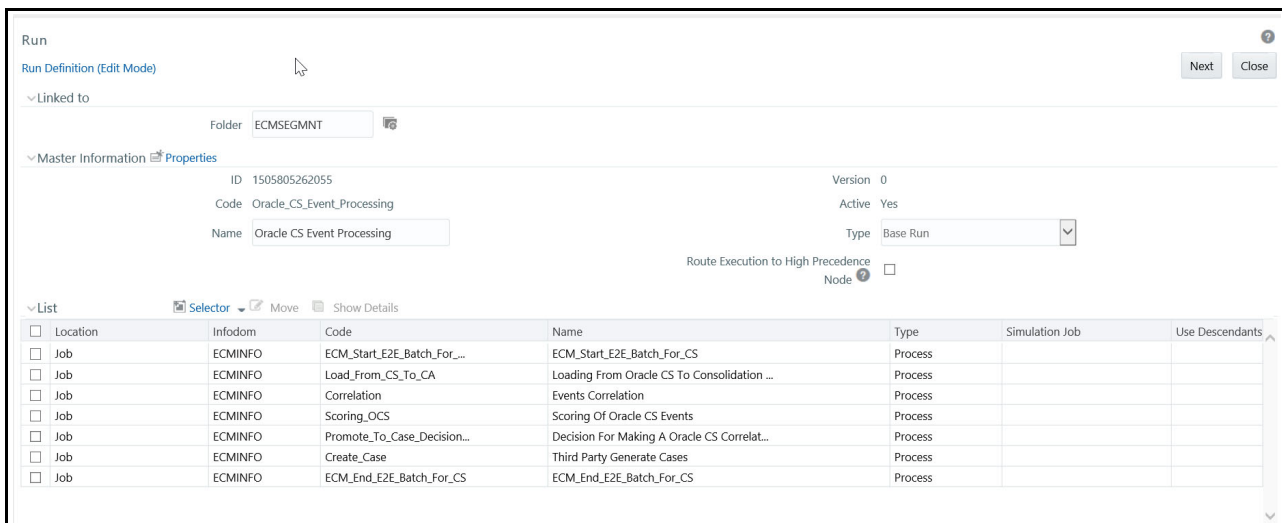
Figure 23. OCS Connector

3. Select **Load_From_CS_To_CA** (connector) process from the list. This has the following four sub processes:

   - Loading Oracle CS Event

   - Entity Surrogate Key Generation For Oracle CS

   - Evented Data Load for CS

   - Business Data Load for CS

For more information on processes and tasks, see the *Appendix A, List of Processes and Tasks*.

For more information on Configuring Data Movement from LA to CA, see the *Configuring Data Movement from LA to CA* .

Loading KYC Data

The OKYC connectors are used to load data from the KYC application to the ECM.

To load data from the OKYC to the ECM, follow these steps:

1. Navigate to the Run window.

2. Go to the List section. Select **Oracle_KYC_Event_Processing**. The list of processes for OKYC is displayed.
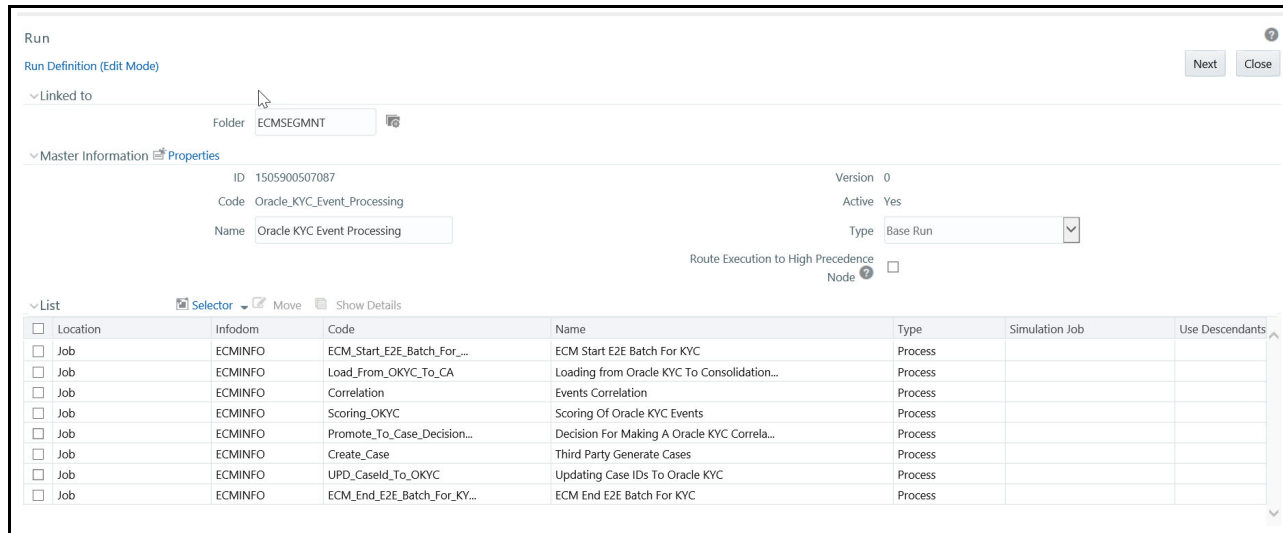
Figure 24. OKYC Connector

3. Select **Load_From_OKYC_To_CA** (connector) process from the list. This has the following four sub processes:

- Loading Oracle KYC Events to Consolidation area

- Entity Surrogate Key Generation For Oracle KYC (to be executed after Loading Oracle KYC Events sub process.)

- Evented Data Load for KYC

- Business Data Load for KYC

For more information on processes and tasks, see the *Appendix A, List of Processes and Tasks*.

For more information on Configuring Data Movement from LA to CA, see the *Configuring Data Movement from LA to CA*

Loading Third Party Connector Data

Third Party connectors are used to load data from the Third Party application to the ECM. Before loading the data from Third Party application to Landing area, it is moved to staging area.

To load data from the Third Party to the ECM, follow these steps:

1. Navigate to the Run window.

2. Go to the List section. Select **Third_Party_Event_Processing**. The list of process for Third Party is displayed.
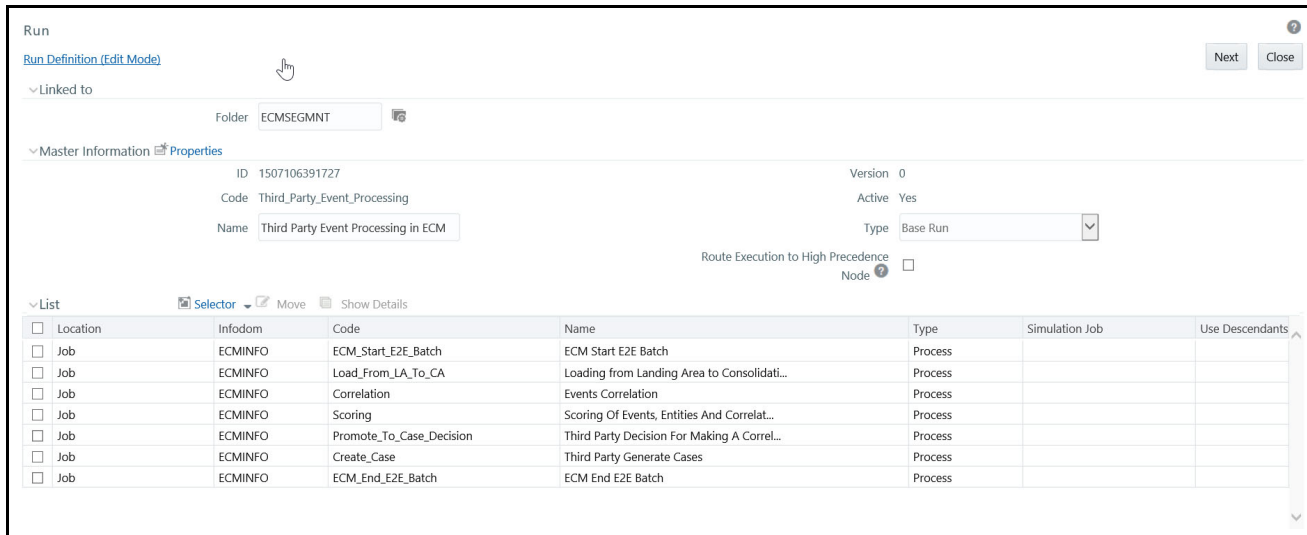
Figure 25. Third Party Connector

3. Select **Load_From_LA_To_CA** (connector) process from the list. This has the following four sub processes.

- Loading Events to Consolidation area

- Entity Surrogate Key Generation (to be executed after Loading Events sub process.)

- Evented Data Load

- Business Data Load

- Derive Wire, Cash and MI Transaction

For more information on processes and tasks, see the *Appendix A, List of Processes and Tasks*.

For more information on Configuring Data Movement from LA to CA, see the *Configuring Data Movement from LA to CA*

Data Movement (DM) Utility

It is used to transfer data from one Oracle data source to another Oracle data source.

- Data movement across source and target tables residing in two different databases. For example: source table on database1 and target table on database2.

- Data movement across source and target tables residing in two different schema in the same database. For example: source table on schema1.table1 and target table on schema2.table2.

- Data movement across source and target tables residing in the schema in the same database. For example: source table on schema1.table1 and target table on schema1.table2.

The following Data transfer modes are available:

- **DI**: In this mode, the Utility fetches the data from the source table/s based on the metadata available in the `FCC_DM_DEFINATION` and `FCC_DM_MAPPING` tables. Data is removed from the target is based its PK/UK. Then the data is moved into the source table.

- **IS**: In this mode, Utility inserts the data from selected table of source to target.

- **MI**: In this mode, Utility performs insert or update operations. If data is not available in the target table, then Insert operation is performed. If data is available in the target table, then Update operation is performed.

DM Metadata Tables

- `FCC_DM_DEFINITION`: Stores the definition of SQL conditions that is used to fetch the data from source database

The structure of the DM definition table is as follows:

Table 16. FCC_DM_DEFINITION (Metadata Table)

Column Name	Primary Key	Column Type	Nullable
DM_GROUP_ID	*	NUMBER(10)	No
DM_ID		NUMBER(10)	No
DM_CODE		VARCHAR2(100)	Yes
DM_DESCRIPTION		VARCHAR2(4000)	Yes
V_SOURCE_DATASET		CLOB	Yes
V_TARGET		VARCHAR2(30)	Yes
V_SRC_FILTER		VARCHAR2(4000)	Yes
V_TARG_FILTER		VARCHAR2(4000)	Yes
V_TARGET_DATASET		CLOB	Yes
V_SELECT_HINT		VARCHAR2(500)	Yes
V_PARALLEL_DEGREE		VARCHAR2(3)	Yes

- DM_GROUP_ID: Grouping code of DM definition. DM definitions can be grouped to pull the data together.

- DM_ID: Unique identification ID of DM definition.

- DM_CODE: Unique name of DM definition.

- DM_DESCRIPTION: Description of DM definition.

- V_SOURCE_DATASET: Name of Source table. It can contain the join conditions with multiple source tables and conditions associated with it. All source table must be put under curly bracket '{'. For example: {EMP_PHON}

- V_TARGET: Name of Target table.

- V_SRC_FILTER: Source filter that contains the filter condition for source database.

  For example,

  EMP_PHON.DATA_DUMP_DT = $MISDATE AND EMP_PHON.PRCSNG_BATCH_NM IN (SELECT FCC_BATCH_DATAORIGIN.V_DATA_ORIGIN FROM FCC_BATCH_DATAORIGIN WHERE FCC_BATCH_DATAORIGIN.N_RUN_SKEY = $RUNSKEY)

- V_TARG_FILTER: Filter condition in target database.

● V_TARGET_DATASET: Contains the join condition with multiple target tables and filter condition associated with it.

For example,

INNER JOIN FCC_EMPLOYEE_LOOKUP ON FCC_EMPLOYEE_LOOKUP.EMP_INTRL_ID = [EMP_PHON].EMP_INTRL_ID

The following is the example:

DM_GROUP_ID	DM_ID	DM_CODE	DM_DESCRIPTION	V_SOURCE_DATASET	V_TARGET	V_SRC_FILTER	V_TARG_FILTER	V_TARGET_DATASET
1	1	BD_EMP_PHON	T2T_FCCM_PROD_EMP_PHON	{EMP_PHON}		EMP_PHON.DATA_DUMP_DT = $MISDATE AND EMP_PHON.PRCSNG_BATCH_NM IN (SELECT FCC_BATCH_DATAORIGIN.V_DATA_ORIGIN FROM FCC_BATCH_DATAORIGIN WHERE FCC_BATCH_DATAORIGIN.N_RUN_SKEY = $RUNSKEY)		INNER JOIN FCC_EMPLOYEE_LOOKUP ON FCC_EMPLOYEE_LOOKUP.EMP_INTRL_ID = [EMP_PHON].EMP_INTRL_ID

● FCC_DM_FIELD_MAPPING: Stores the field-to-field mapping details of data from source to target table.

The structure of the DM field mapping table is as follows:

Table 17. FCC_DM_Field_Mapping (Metadata table)

Column Name	Primary Key	Column Type	Nullable
DM_ID	*	NUMBER(10)	No
V_ENTITY_NAME		VARCHAR2(50)	Yes
V_FIELD_NAME		VARCHAR2(50)	Yes
V_SRC_DATA_TYPE		VARCHAR2(50)	Yes
V_FIELD_FORMAT		VARCHAR2(50)	Yes
F_IS_NULL_ALLOWED		CHAR(1)	Yes
V_SQL_EXPRESSION		VARCHAR2(4000)	Yes
V_TARGET_ENTITY_NAME		VARCHAR2(30)	Yes
V_TARGET_FIELD_NAME		VARCHAR2(50)	Yes
V_SQL_FUNCTION		VARCHAR2(500)	Yes
V_NULL_IF		VARCHAR2(50)	Yes

Column Name	Primary Key	Column Type	Nullable
V_DEFAULT_IF		VARCHAR2(50)	Yes
V_TARG_DATA_TYPE		VARCHAR2(50)	Yes
V_EXECUTION_SPACE		VARCHAR2(5)	Yes

- DM_ID: DM ID from FCC_DM_DEFINITION table.
- V_ENTITY_NAME: Name of Source table.

Note: It can contain expression and target table, if source value is populating from any SQL expression or a particular column from target table.

Example: EXPRESSION, CM_EMP_SEQ.NEXTVAL

- V_FIELD_NAME: Name of Source field.

Note: It can contain target filed name if the value is coming from target table.

- V_SRC_DATA_TYPE: Data type of Source field.
- V_FIELD_FORMAT: Data type format of source field.
  Example: mm-dd-yyyy
- F_IS_NULL_ALLOWED: Set this flag as yes if is Null allowed.
- V_SQL_EXPRESSION: Type of SQL expression.
  For example: Case statement, Sequences and so on. It can contain direct variable from application interface for example, $MISDATE (MIS date passed from external interface for source filter)
- V_TARGET_ENTITY_NAME: Name of Target table
- V_TARGET_FIELD_NAME: Name of Target field.
- V_TARG_DATA_TYPE: Data type of target field.

The following is the example:

DM_ID	V_ENTITY_NAME	V_FIELD_NAME	V_SRC_DATA_TYPE	V_FIELD_FORMAT	F_IS_NULL_ALLOWED	V_SQL_EXPRESSION	V_TARGET_ENTITY_NAME	V_TARGET_FIELD_NAME	V_SQL_FUNCTION	V_NULL_IF	V_DEFAULT_IF	V_TARG_DATA_TYPE	V_EXECUTION_SPACE
1	EXPRESSION	DATA_DUMP_DT	DATE		Y	$MISDATE	FCC_EMP_PHON	MIS_DATE				DATE	Trg
1	EMP_PHON	EMP_INTRL_ID	VARCHAR2(200)		Y		FCC_EMP_PHON	EMP_INTRL_ID				VARCHAR2(200)	Src

DM_ID	V_ENTITY_NAME	V_FIELD_NAME	V_SRC_DATA_TYPE	V_FIELD_FORMAT	F_IS_NULL_ALLOWED	V_SQL_EXPRESSION	V_TARGET_ENTITY_NAME	V_TARGET_FIELD_NAME	V_SQL_FUNCTION	V_NULL_IF	V_DEFAULT_IF	V_TARG_DATA_TYPE	V_EXECUTION_SPACE
1	EXPRESSION	EMP_PHON_SEQ_ID	NUMBER(22,0)		Y	CM_EMP_PHON_SEQ.NEXTVAL	FCC_EMP_PHON	EMP_PHON_SEQ_ID				NUMBER(22,0)	Trg
1	EMP_PHON	PHON_EXT_NB	VARCHAR2(20)		Y		FCC_EMP_PHON	PHON_EXT_NB				VARCHAR2(20)	Src
1	EXPRESSION	PHONE_TYPE	VARCHAR2(20)		Y	'Business'	FCC_EMP_PHON	PHONE_TYPE				VARCHAR2(20)	Src

DM Audit and Error Details Tables

- FCC_DM_AUDIT: Stores the execution order of each run and SQL execution in source and target.
- FCC_DM_ERROR_DETAILS: Stores all the errors occurred in source or target database.

Configuring Data Movement from LA to CA

This section covers the following topics:

- About Data Movement
- Sample Processes
- Using Precedence
- Designing Processes

About Data Movement

This section explains configuring the data movement form Landing Area (LA) to Consolidation Area (CA). This is applicable for OBD, OKYC, OCS, and Third party. In OOB process, you can run the processes in parallel as well as in sequence. However, you can configure these processes based on your requirement.

For example, you can configure processes based on entity and related data such as account, customer, employee, institution and so on. The following are OOB processes as part of Business data movement.

Sample Processes

These sample processes are designed using OOB Oracle Behavior Detection Business data processes (Oracle Behavior Detection to CA Account Address, Oracle Behavior Detection to CA Customer, Oracle Behavior Detection to CA Employee Email Address, and so on).

The sub –processes used to create a process, from process1 to Process9 are part of OOB Business Data Movement processes. In the out of box batch run, these sub processes run in parallel and in sequence.

You can create processes based on clients' requirement. The processes are created using sub-processes considering various parameters such as scenario, focus and associated business data, the volume of records, hardware configuration, and so on.

The following is the list of sample processes (Oracle Behavior Detection Business data from LA to CA) which has sub processes attached to it.

Table 18. Sample Processes

Process	Description
Process1	This process is designed using the following sub-processes (OBD to CA Account): ● Oracle Behavior Detection to CA Account, ● Oracle Behavior Detection to CA Account Address, ● Oracle Behavior Detection to CA Account Balance Position Summery, ● Oracle Behavior Detection to CA Email Address, and so on
Process2	This process is designed using the following sub-processes (OBD to CA Customer): ● Oracle Behavior Detection to CA Customers, ● Oracle Behavior Detection to CA Customers Account, ● Oracle Behavior Detection to CA Customers Address, ● Oracle Behavior Detection to CA Customers Email Address, ● Oracle Behavior Detection to CA Customers IMP License, and so on
Process3	This process is designed using the following sub-processes (OBD to CA Employee): ● Oracle Behavior Detection to CA Employee, ● Oracle Behavior Detection to CA Employee Address, ● Oracle Behavior Detection to CA Employee Email Address, ● Oracle Behavior Detection to CA Employee Phone, ● Oracle Behavior Detection to CA Employee to Account, and so on
Process4	This process is designed using the following sub-processes: ● Oracle Behavior Detection to CA account, ● Oracle Behavior Detection to CA Employee, ● Oracle Behavior Detection to CA Customers, and so on
Process5	This process is designed using the following sub-processes: ● Oracle Behavior Detection to CA Account Address ● Oracle Behavior Detection to CA Account Balance Position Summery ● Oracle Behavior Detection to CA Account Email Address, and so on

Table 18. Sample Processes

Process6	This process is designed using the following sub-processes:
	● Oracle Behavior Detection to CA Customers Account
	● Oracle Behavior Detection to CA Customers Address
	● Oracle Behavior Detection to CA Customers Email Address
	● Oracle Behavior Detection to CA Employee
Process7	This process is designed using the following sub-processes:
	● Oracle Behavior Detection to CA Employee Address,
	● Oracle Behavior Detection to CA Employee Email Address,
	● Oracle Behavior Detection to CA Employee Phone,
	● Oracle Behavior Detection to CA Employee to Account, and so on
Process8 & 9	These processes are designed using all sub-processes.

Note:

■ Process1, 2, and 3 are designed based on similar entity bucketed into to one process.

■ Process4, 5, 6, and 7 are designed based on the distribution of volume of data. For example, if Process4 has huge volume of data compare to Process5, 6, and 7. You can design the process (business data movement) in such way that the Process4 runs in parallel with Process5, internally, Process5, 6, and 7 can run in sequence.

Using above sample processes, you can design entire Landing Area to Consolidation Area data movement based on client's requirement.

Using Precedence

Follow the sequence of precedence while moving the data.

1. Event lookup should be populated

2. Event related tables should be populated and the sub-processes can run in parallel.

3. Surrogate key should be populated for all entities (lookup table, for example, account lookup, customer lookup). The sub-processes can run in parallel.

4. Evented data movement processes and business data movement processes can run in parallel.

   Note: Note: make sure precedence is set for data movement.

Designing Processes

You can design processes using sub-processes. This section is explained using Oracle Behavior Detection processes and sub- processes as an example. For more information on Sample Processes, see the section *Load Data from BD to ECM* of *Appendix A, "List of Processes and Tasks,"*

The following figure depicts sub-processes in Oracle Behavior Detection processes.

Figure 26. Oracle Behavior Detection processes

The following figure illustrates the Processes (1 to 9) designed using sub-processes (SP).
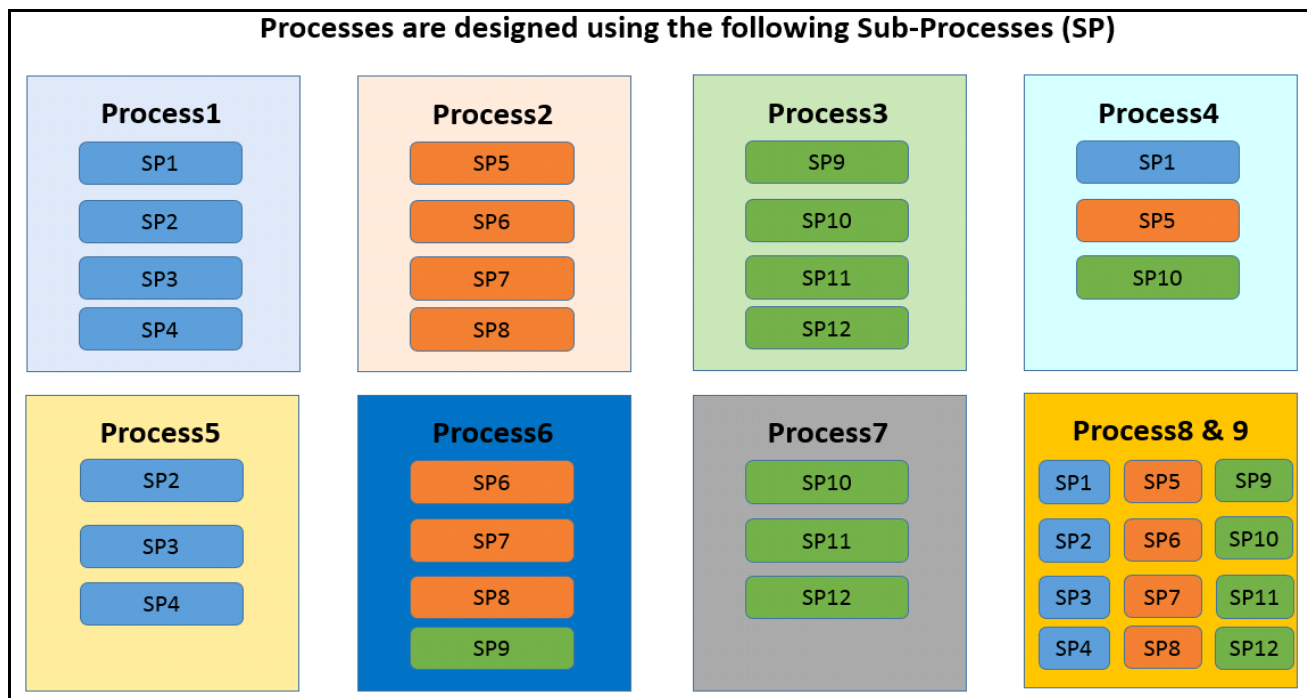
Figure 27. Oracle Behavior Detection Sub - processes

You can run Processes using the list of options shown in the following figure.
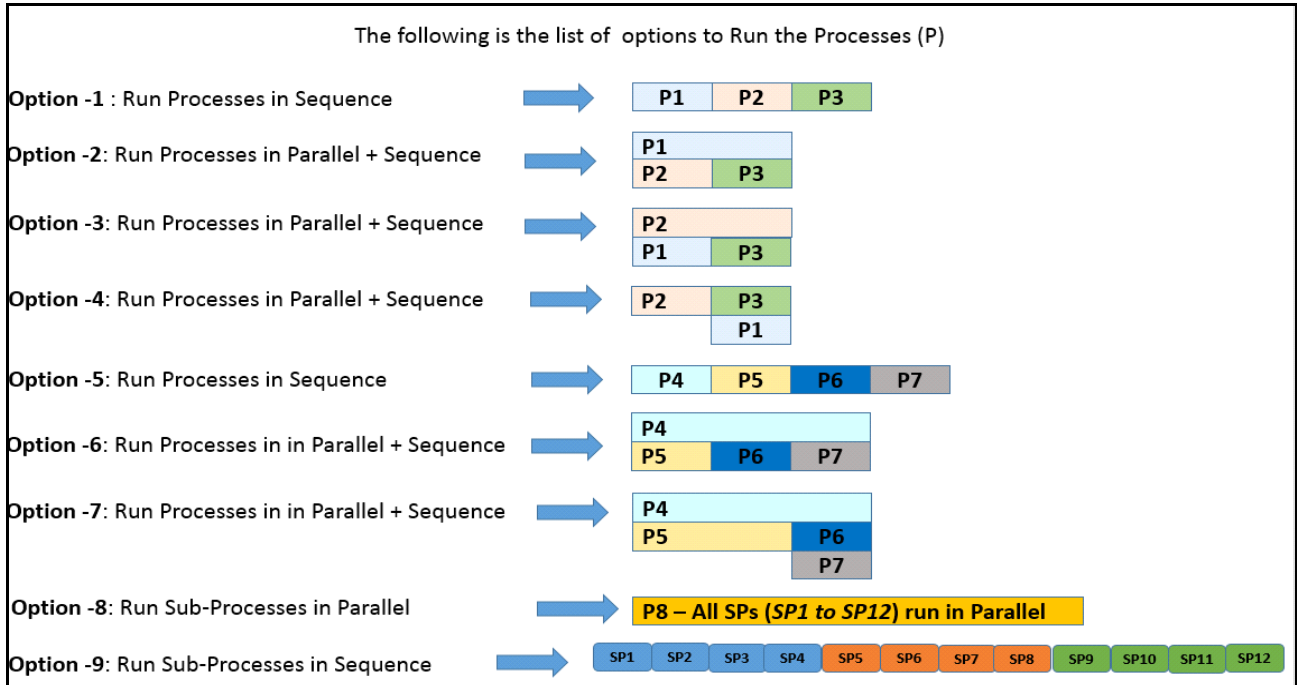
Figure 28. Options- processes

The following table provides the complete description of each options.

Table 19. Options

Option	Description
1	P1, P2, and P3 processes are configured in sequence. ● In P1, sub processes - SP1, SP2, SP3, and SP4 will run in parallel. ● Once the P1 is completed, P2 will start and sub processes SP5, SP6, SP7, and SP8 will run in parallel. ● Once P2 is completed, P3 will start and sub processes SP9, SP10, SP11, and SP12 will run in parallel.
2	P1 and P2 will start in parallel and P3 will start only after P2 is completed, irrespective of P1 is completed or not. ● In P1, sub processes - SP1, SP2, SP3, and SP4; in P2, sub processes- SP5, SP6, SP7, and SP8 will run in parallel. ● Once the P2 is completed, P3 will start and sub processes SP9, SP10, SP11, and SP12 will run in parallel.
3	P2 and P1 will start in parallel and P3 will start only after P1 is completed, irrespective of P2 is completed or not. ● In P2, sub processes - SP5, SP6, SP7, and SP8; in P1, sub processes- SP1, SP2, SP3, and SP4 will run in parallel. ● Once the P1 is completed, P3 will start and sub processes SP9, SP10, SP11, and SP12 will run in parallel.
4	Only after completion of P2, P3 and P1 will start in parallel. ● In P2, sub processes - SP5, SP6, SP7, and SP8 run in parallel. ● P3 - SP9, SP10, SP11, and SP12, and P1 - SP1, SP2, SP3, and SP4 sub process will run in parallel only after completion of all sub processes of P2.

Table 19. Options

5	P4, P5, P6, and P7 processes are configured in sequence. P4 - SP1, SP5, and SP10 will run in parallel. ● Once the P4 is completed, P5- SP2, SP3, and SP4 will start in parallel. ● Once the P5 is completed, P6- SP6, SP7, SP8, PS9 will start in parallel. ● Once the P6 is completed, P7- SP10, SP11, and SP12 will start in parallel.
6	P4 and P5 will start in parallel and P6 will start only after P5 is completed, and followed by P7 irrespective of P4 is completed or not. ● In P4, sub processes – SP1, SP5, and SP10; in P5, sub processes- SP2, SP3, and SP4 will run in parallel. ● Once the P5 is completed, P6 will start and sub processes SP6, SP7, SP8, and SP9 will run in parallel. ● Once the P6 is completed, P7 will start and sub processes SP10, SP11, and SP12 will run in parallel.
7	P4 and P5 will start in parallel. P6 and P7 will start in parallel only after P5 is completed, irrespective of P4 is completed or not. ● In P4, sub processes - SP1, SP5, and SP10; in P5, sub processes- SP2, SP3, and SP4 will run in parallel. ● P6 - SP6, SP7, SP8, and SP9, and P7 - SP10, SP11, and SP12 sub process will run in parallel only after completion of all sub processes of P5.
8	Once P8 starts, all sub processes from SP1 to SP12 will run in parallel.
9	All sub processes will run in sequence from SP1 to SP12.

Note:

■   Same sub processes should not be part of two processes. For example, you should add P1 and P4 in the same run as they have similar sub process (SP1).

■   Above options are used as samples, you can configure your own options based on the requirement.

To design the above process, see the *OFS AAI User Guide*.

Configuring Correlation

This chapter provides the concept and usage of correlation. The following sections are covered in this chapter:

- About Correlation
- Using Business Entity Paths
- Executing Correlation Rules
- Sample Correlation Rules

About Correlation

After the event data is loaded from OBD, OKYC, OCS, or third party applications into ECM, you can correlate event to business entities and event to event based on business entities using configurable rule sets. This functionality is performed by the Event Correlation process. The group of events are identified for correlation based on business entries in an application (BD, KYC, CS or Third Party).

Using Business Entity Paths

Following two tables are used for configuring business entity paths:

- Correlation Business Path
- Correlation Business Entity Configuration

Correlation Business Path

The business entity paths are managed through manual interaction with the FCC_CORR_BUS_ENTITY_PATH table in the ECM. This table is populated with a comprehensive set of sample data paths. The following information assists in modifying the path or adding to it. The structure of the table is as follows:

Table 20. FCC_CORR_BUS_ENTITY_PATH **(Metadata Table)**

Column Name	Primary Key	Column Type	Nullable
N_BUS_ENTITY_PATH_SKEY	Y	NUMBER(10)	No
D_MIS_DATE			
V_BUSINESS_ENTITY_PATH_NAME		VARCHAR2(50)	No
V_QUERY_DEFINITION_NAME		VARCHAR2(50)	Yes
N_BUSINESS_ENTITY_ID		NUMBER(10)	Yes
ALERT_FOCUS_ID		NUMBER(10)	Yes
V_ENTITY_TYPE		VARCHAR2(50)	Yes

Table 20. FCC_CORR_BUS_ENTITY_PATH **(Metadata Table) (Continued)**

Column Name	Primary Key	Column Type	Nullable
V_QUERY_DEFINITION_NAME		VARCHAR2(50)	Yes
N_QUERY_DEFINITION_SKEY		NUMBER(10)	Yes

To correlate events to business entities, follow these steps:

1. Define paths using above table to perform the Event Correlation algorithm.

2. Define whether the origin of the path should be the focus of an event or a matched record, by populating either.

3. Establish either populating the ALERT_FOCUS_ID column (indicating that the origin should be the focus of the event), or the V_QUERY_DEFINITION_NAME column (indicating that the origin should be a matched record of the event).

4. The destination of the path (the business entity you are trying to correlate to by executing this path) is defined by the N_BUSINESS_ENTITY_ID column.

Correlation Business Entity Configuration

The structure of the Business Entity path configuration table is as follows:

Table 21. **FCC_CORRELATION_BUS_ENTITY_CFG (Metadata Table)**

Column Name	Primary Key	Column Type	Nullable
N_BUS_ENTITY_PATH_CFG_SKEY	*	NUMBER(10)	No
N_BUS_ENTITY_PATH_SKEY		NUMBER(10)	No
N_SCENARIO_MASTER_SKEY		NUMBER(10)	Yes
V_SCENARIO_CLASS_CD		VARCHAR2(3)	Yes
N_PATH_PRECEDENCE		NUMBER(10)	Yes
V_EVENT_TYPE		VARCHAR2(3)	

To configure Business Entity path, follow these steps:

1. Select to apply the path identified by the N_BUS_ENTITY_PATH_CFG_SKEY in this table for alerts of a certain scenario or scenario group.

2. Populate the N_SCENARIO_MASTER_SKEY or the V_SCENARIO_CLASS_CD column to establish respectively.

Note: If neither of these columns are populated, this path configuration is considered for an alert of any scenario or scenario group. The "importance" or "strength" of a correlation determined by this path can vary depending on the scenario or scenario group of the alert.

This is defined by the N_PATH_PRECEDENCE (the lower the number, the higher the precedence). A NULL N_PATH_PRECEDENCE indicates not to apply this N_BUS_ENTITY_PATH_CFG_SKEY to any alerts of this SCNRO_ID or V_SCENARIO_CLASS_CD.

By default, For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY and V_SCENARIO_CLASS_CD is NULL and N_PATH_PRECEDENCE = 10 then the PATH_SKEY = 1004 will be considered for execution for all the scenario class except the below mentioned cases

1. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY is NULL and V_SCENARIO_CLASS_CD = 'FR' and N_PATH_PRECEDENCE = 15 then the PATH_SKEY = 1004 will be executed for 'FR' related scenarios

2. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD is NULL and N_PATH_PRECEDENCE is NULL then the PATH_SKEY = 1004 will not be considered for execution

3. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD = 'ML' and N_PATH_PRECEDENCE is NULL then the PATH_SKEY = 1004 will not be considered for execution.

4. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD = 'IML' and N_PATH_PRECEDENCE = 13 then the PATH_SKEY = 1004 will be considered for execution only for the above mentioned '114697025' and 'IML'

Executing Correlation Rules

You can execute the correlation using two methods:

- Using Run Rule Framework
- Performing Jobs

Using Run Rule Framework

You can run a correlation using the Run Rule Framework. For more information, refer to *Performing Batch Run* section.

Performing Jobs

If the correlation execution fails from the Run Rule Framework, then execute it using the following steps:

Note: Run the Event Correlation process to execute only those correlation rules that are designated as Active. Rules that are designated as Inactive is ignored and not executed.

1. Navigate to `$FIC_HOME/ficdb/bin/ficdb/bin`.

2. Execute the following script:

   ./correlation.sh ECMINFO_1509116374374_20091226_1 a b 20091226 c

   ECMINFO_1509116374374_20091226_1 is V_BATCH_RUN_ID from FCC_BATCH_RUN

   D_MIS_DATE is date from FCC_BATCH_RUN

Sample Correlation Rules

OFS ECM delivers the following four sample correlation rules:

- **KYC Correlation**: KYC Groups events created in the past month based on a common correlated business entity. KYC Groups events created in the past seven days that are generated on one or more specified scenarios where the events share a common correlated business entity. Specified scenarios are those scenarios which identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.

- **AML Correlation**: AML Groups events created in the past month based on a common correlated business entity. AML Groups events created in the past seven days that are generated on one or more specified scenarios where the events share a common correlated business entity. Specified scenarios are those scenarios which identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.

- **Customer Screening Correlation**: CS Groups events created in the past month based on a common correlated business entity. CS Groups events created in the past seven days that are generated on one or more specified scenarios where the events share a common correlated business entity. Specified scenarios are those scenarios which identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.

- **Third Party**: Third Party Groups events created in the past month based on a common correlated business entity. Third Party Groups events created in the past seven days that are generated on one or more specified scenarios where the events share a common correlated business entity. Specified scenarios are those scenarios which identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.

CHAPTER 8

Scoring ·

This chapter provides the concept behind scoring in the ECM. The following sections are covered in this chapter:

- About Scoring
- Types of Scoring
- Configuring Scoring Rules
- Scoring Samples

About Scoring

Scoring is a methodology to score events, correlation, and entity (customer or account).

The following are the methods of scoring:

- Initial Scoring
- Adjustment Scoring

Initial Scoring

The following figure depicts the initial scoring process.
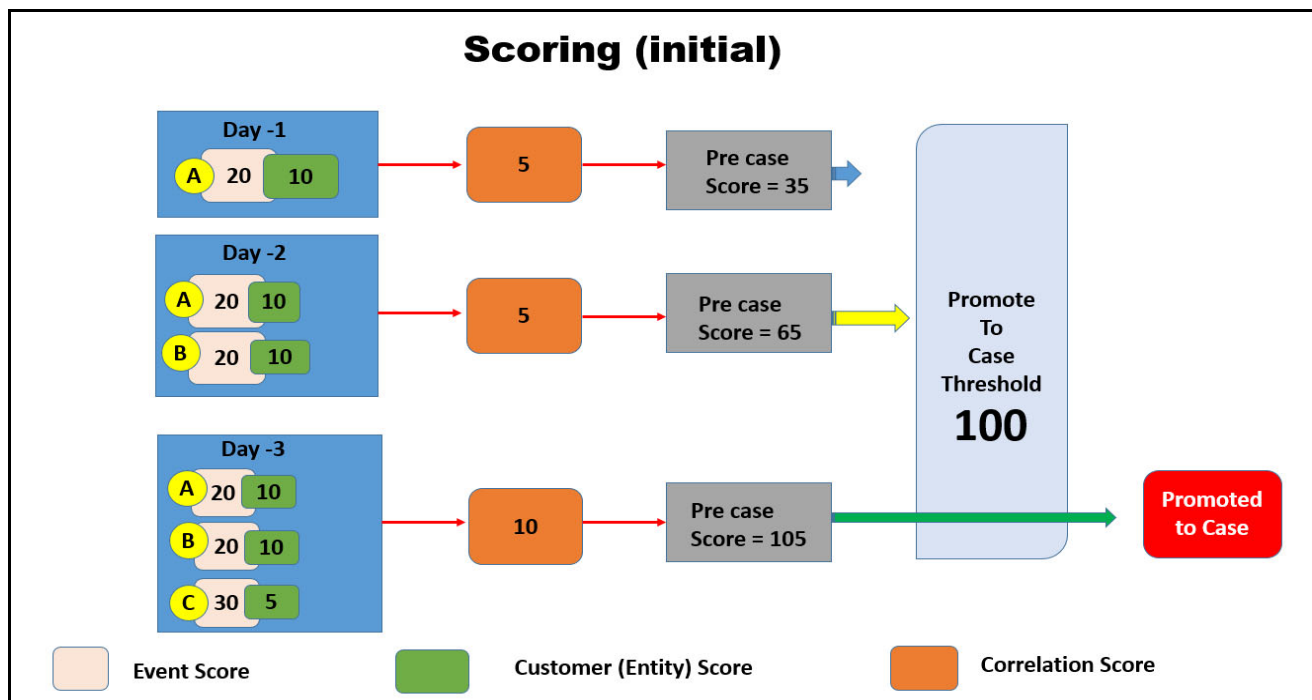
Figure 29. Initial Scoring

Table 22. Initial Scoring

Day	Event - A Score	Event - B Score	Event - C Score	Customer Score	Correlation Score	Pre case Score	PTC Threshold	PTC (Yes/No)
Day - 1	20			10	5	35	100	No
Day - 2	20	20		20	5	65	100	No
Day - 3	20	20	30	25	10	105	100	Yes

Day - 1

- A newly generated event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).

- The pre case score is 35. It is the sum of event + customer + correlation = pre case score. That is, 20 + 10 +5 = 35.

- As it could not cross the threshold, hence, it remained as a pre case.

Day - 2

- Another event (event B) is generated, along with event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).

- The pre case score is 65. It is the sum of event A + event B + customer + correlation = pre case score. That is, 20 + 20 + 10 +5 = 65.

- As it could not cross the threshold, hence, it remained as a pre case.

Day - 3

- Another event (event C) is generated along with event (event B), event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).

- The pre case score is 65. It is the sum of event A + event B + event C + customer + correlation = pre case score. That is, 20 + 20 + 30 + 10 +10 = 105.

- A pre case is promoted to case.

Adjustment Scoring

An Adjustment Scoring happens everyday for all events which are not part of PTC (Promote to case). That is, event is scored every day till it is promoted to case. This is negative scoring of an event.

The following figure depicts the adjustment scoring process.
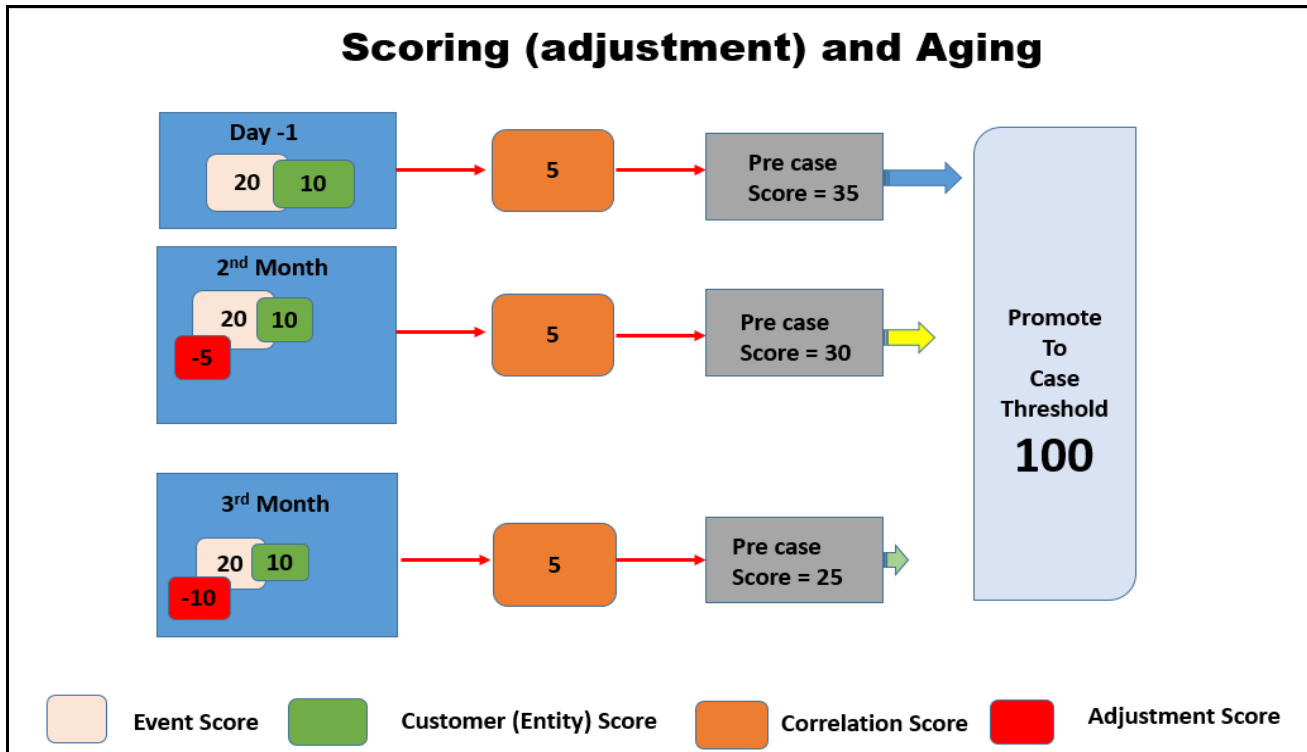
Figure 30. Adjustment Scoring

.

Table 23. Adjustment Scoring

Period	Event - A Score	Event adjustment Score	Customer Score	Correlation Score	Pre case Score	PTC Threshold	PTC (Yes/No)
Day - 1	20		10	5	35	100	No
2nd Month	20	-5	10	5	30	100	No
3rd Month	20	-10	10	5	25	100	No

Days - 1

- A newly generated event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).

- The pre case score is 35. It is the sum of event + customer + correlation = pre case score. That is, 20 + 10 +5 = 35.

- As it could not cross the threshold, hence, it remained as a pre case.

2nd Month

- If the event (A), associated entity (customer), and correlation are not promoted, an adjustment score is applied. That is, event score is reduced (-5).

- The pre case score is 30. It is the sum of event + customer + correlation - event adjustment score = pre case score. That is, 20 + 10 + 5 -5 = 30.

3rd Month

- If the event (A), associated entity (customer), and correlation are not promoted, an adjustment score is applied further. That is, event score is reduced (-10).

- The pre case score is 30. It is the sum of event + customer + correlation - event adjustment score = pre case score. That is, 20 + 10 + 5 -10 = 25.

Types of Scoring

The following is the list scoring types:

- Event Scoring
- Entity Scoring
- Correlation Scoring
- Pre case Scoring

Event Scoring

Every event that is generated is scored. Event scoring is performed on events of AML and Third Party.

- **Event Scoring in AML**: both initial and adjustment scoring are performed.
- **Event Scoring in Third party**: both initial and adjustment scoring are performed. The Initial scoring on third party events is performed by event scoring rules created by IPE.

Entity Scoring

Entity scoring is performed on AML and third party entities. Every entity that is associated with the entity is scored. Here, Customer is the only entity. The Entity scoring is performed by entity rules defined in the IPE. User can perform the entity scoring on different attributes of an entity such as effective risk of the entity, business domain, jurisdiction and so on. Entity scoring happens daily till they are promoted to case.

Correlation Scoring

This scoring is performed on correlation on same day. The score generated by correlation scoring contributes to pre-case score. Correlation scoring happens daily till they are promoted to case.

Pre case Scoring

An event is promoted to case based on Pre-case scoring. The pre case score is the sum of event A + event B + event C + customer + correlation score. If the pre case score does not cross the promote to case threshold, it remains as pre case only.

Configuring Scoring Rules

The following seeded scoring rules are used for scoring:

- Aging Event Scoring

- Correlation Scoring

- Customer Scoring

- Initial Event Scoring

For more information configuring scores, see the *Inline Processing Engine User Guide*.

Configuring AML Event Initial Scoring

This section explains how to configure the initial scoring of AML Event.

To configure the AML Event initial scoring, follow these steps:

1. Navigate to Enterprise Case Management Application.

2. Go to the Common task section. Select the **Run Rule Framework**.

3. Click **Process**. The Process Summary window is displayed with the available Processes.

	Code	Name	Folder	Version	Active
	BD_ACCOUNTATMDAILY_LOOKUP	Oracle Behavior Detection to CA Account ATM Daily Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNTDLY_LOOKUP	Oracle Behavior Detection to CA Account Daily Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNTTRADEDLY_LOOKUP	Oracle Behavior Detection to CA Account Trade Daily Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNTTRXNDLY_LOOKUP	Oracle Behavior Detection to CA Account Transaction Daily Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNT_GROUP_LOOKUP	Oracle Behavior Detection to CA Account Group Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNT_GROUP_LOOKUP1	BD_New	ECMSEGMNT	0	Yes
	BD_ACCOUNT_LOOKUP	Oracle Behavior Detection to CA Account Lookup	ECMSEGMNT	0	Yes
	BD_ACCOUNT_PEERGROUP_LOOKUP	Oracle Behavior Detection to CA Account PeerGroup Lookup	ECMSEGMNT	0	Yes
	BD_ACCT	Oracle Behavior Detection to CA Account	ECMSEGMNT	0	Yes
	BD_ACCT_ACCT_ADDR_EVNT	Oracle Behavior Detection to CA Evented Account Address	ECMSEGMNT	0	Yes
	BD_ACCT_ADDR	Oracle Behavior Detection to CA Account Address	ECMSEGMNT	0	Yes
	BD_ACCT_ATM_SMRY_DAILY	Oracle Behavior Detection to CA Account ATM summary Daily	ECMSEGMNT	0	Yes
	BD_ACCT_ATM_SMRY_DAILY_EVNT	Oracle Behavior Detection to CA Evented Account ATM summary Daily	ECMSEGMNT	0	Yes

Figure 31. Process Summary Window

4. Search for BD Scoring code, for example BD_Event_Scoring.

Figure 32. BD_Event_Scoring

5. Click **Edit** after selecting the BD Event processing. The list of tasks is displayed.
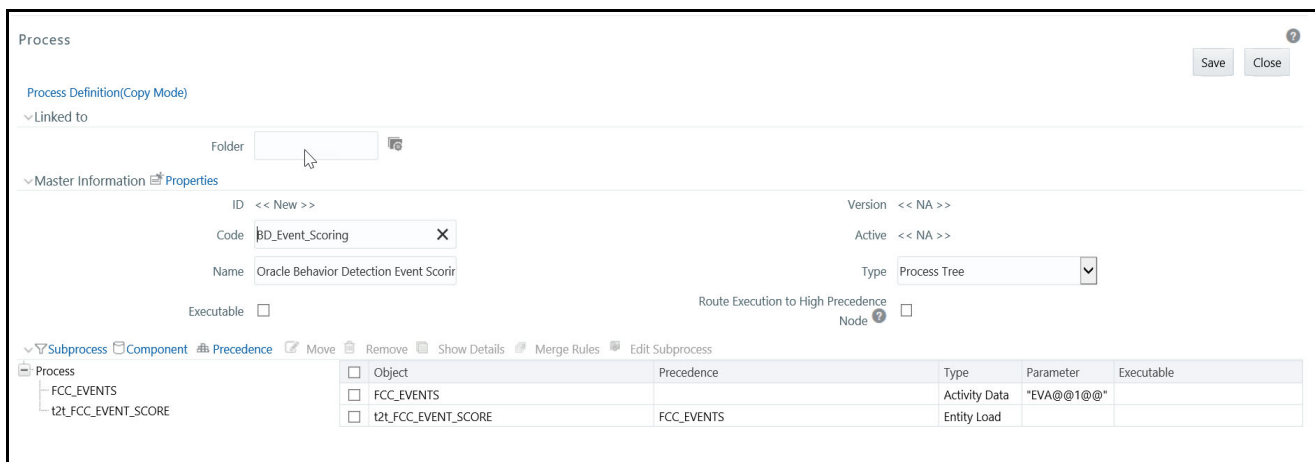
Figure 33. List of Tasks

6. Click **Components**.
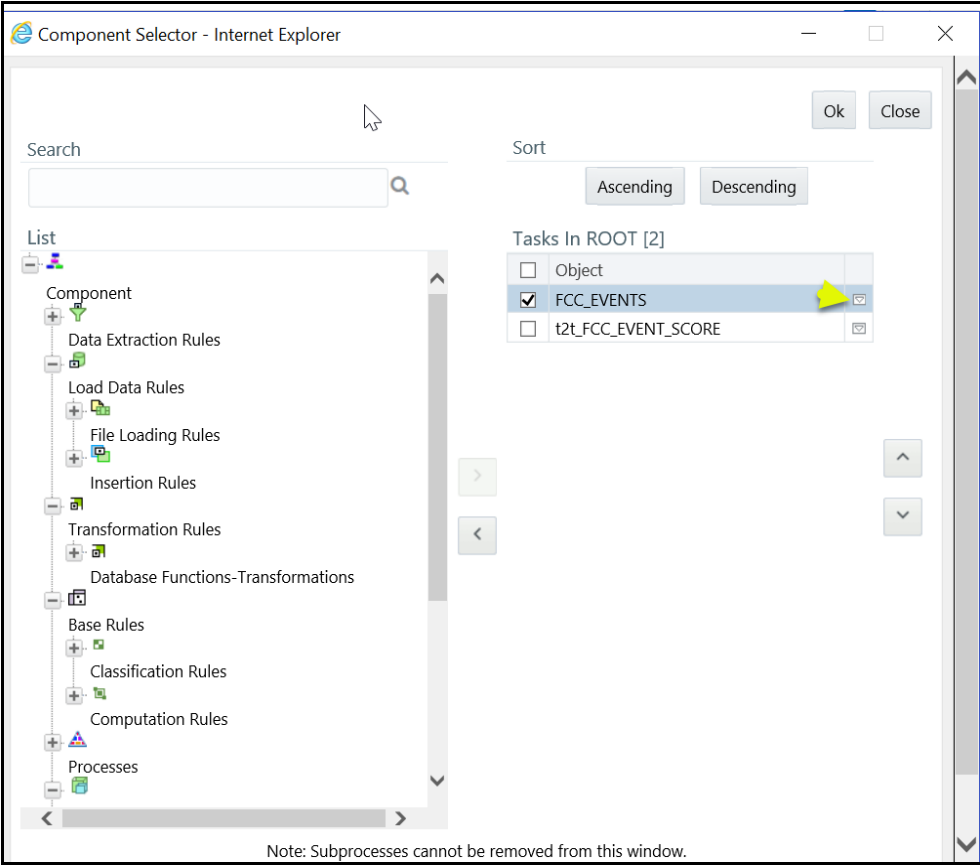
Figure 34. Components

7. Delete all the parameters of FCC_Events task and click **Ok**.
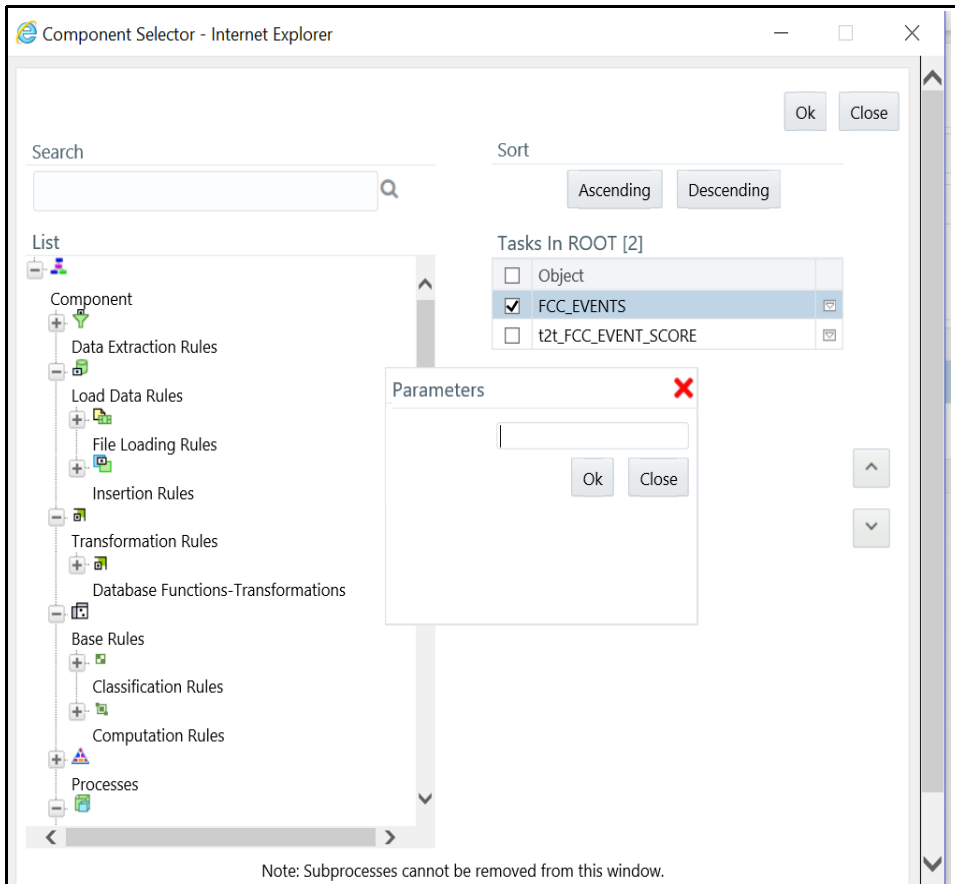
Figure 35. Parameters

8. Navigate to Process Summary window and search **BD_Entity_Surrogate_Key_Gen**.
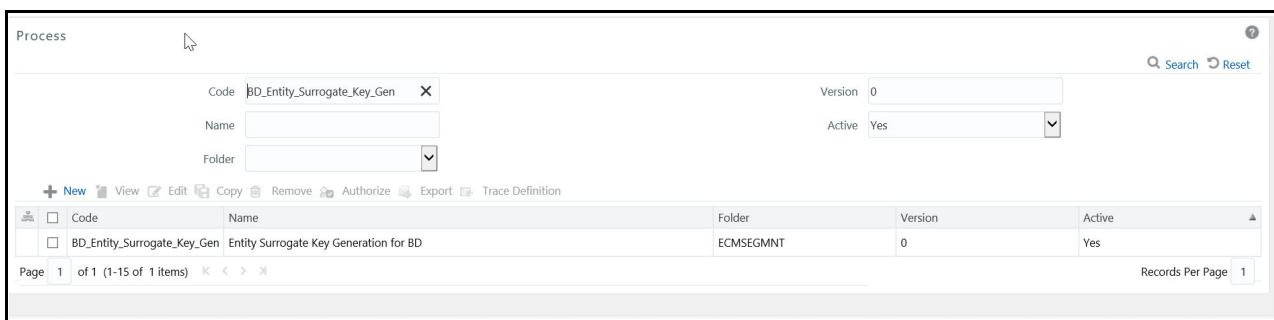
9. The list of tasks is displayed. Click **Component.**
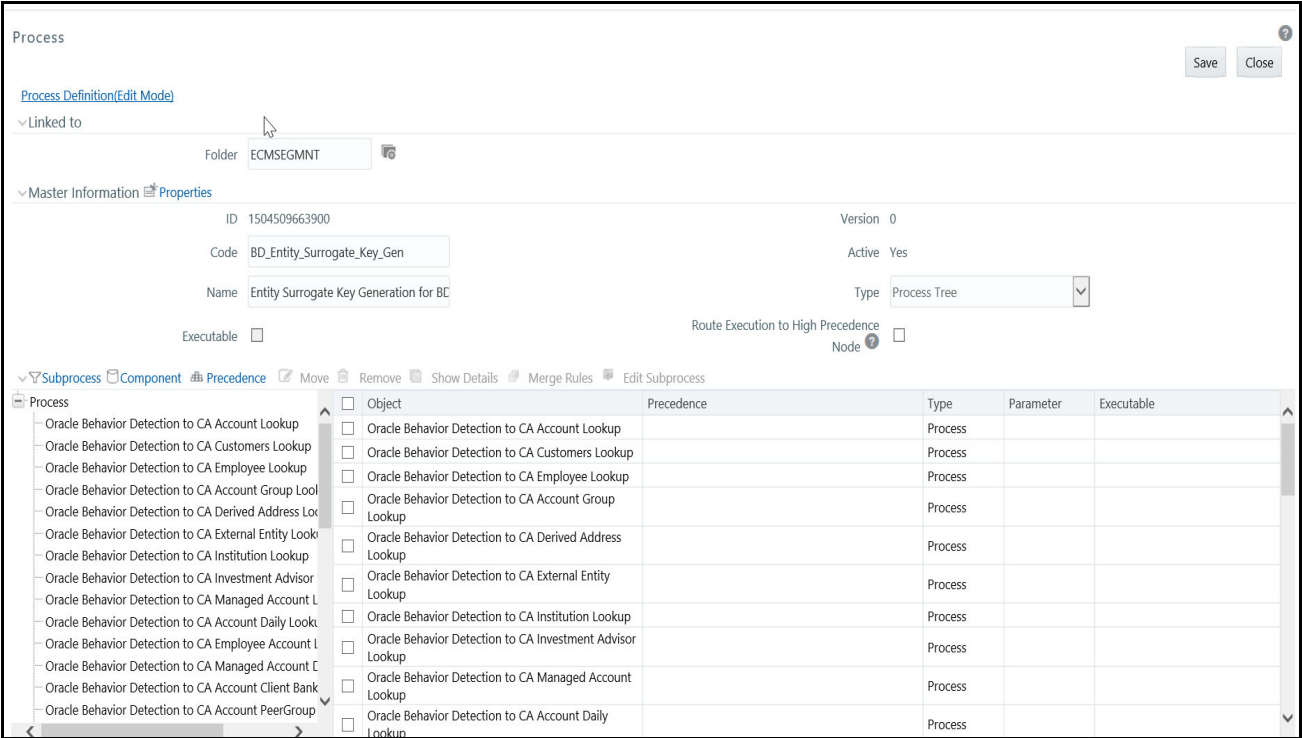
Figure 36. List of Tasks

10. Select **Oracle Behavior Detection to CA Event Scoring** and click OK.
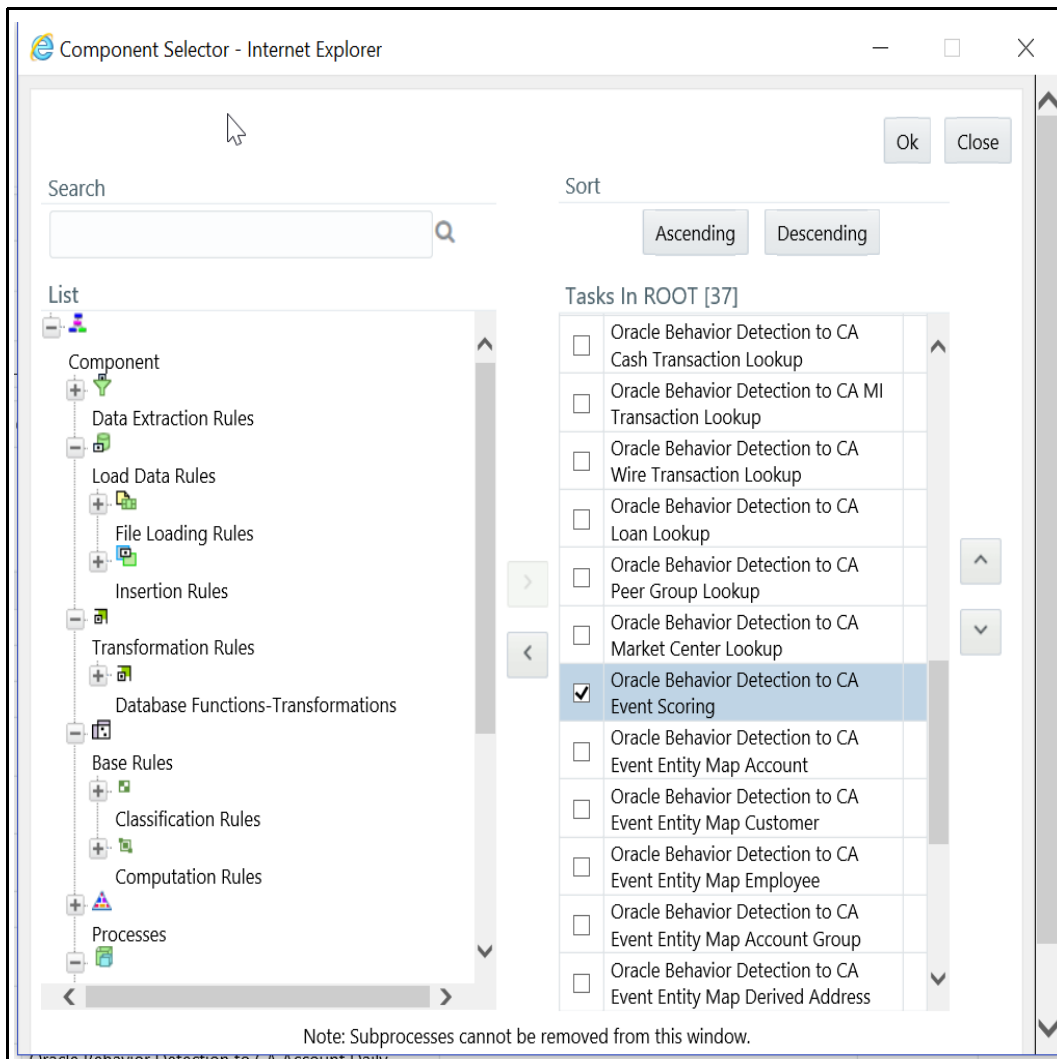
Figure 37. Deselecting of Oracle Behavior Detection to CA Event Scoring Process

11. Save the Process.

Scoring Samples

This section covers the following scoring samples:

- Event

- Entity

- Correlation

Event

This scoring rule defines various scoring criteria to be followed focusing on the event attributes. The Event Scoring is performed on the following event attributes:

- Scenario
- Total Transaction Amount and Risk Score
- Aging

Scenario

- Provide default scoring for each scenario. The total of events scored contributes to pre-case score. The following are the default score for different scenarios:
    - ML – 10
    - Fraud – 5
    - Transaction/Sanctions Filtering – 30
    - KYC – 20
- If a correlation is formed for three events (A, B and C) by ML, TF and KYC. The following is the pre-case score for correlation.
    - Event A – ML (Rapid Movement of Funds – All Activity (CU focus)) – 10
    - Event B – TF – 30
    - Event C – KYC – 30
    - Total pre-case score – 70.
- If a correlation is formed for 3 events (A, B and C) all ML scenarios. The following is the pre-case score for correlation.
    - Event A – ML (Rapid Movement of Funds – All Activity (CU focus)) – 10
    - Event B – ML (CIB - Previous Average Activity (AC focus)) – 10
    - Event C – ML (HR Trans – Focal HRE (CU focus)) – 10
    - Total pre-case score – 30.

Total Transaction Amount and Risk Score

In this attribute, each event is scored. The total of the events scored contributes to pre-case score.

- When event has total transaction amount >= <Configurable amount> and risk score >= <configurable risk score>, give X score to event. Risk scores for amounts can be segregated into 3 buckets. For dollar amounts transactions between 50K and 100K should be given score of 20, 100K to 500K should be given as 30 and anything above 500K should be 50.

- Correlation is created for 2 events A and B by an ML and TF. Transaction amounts between 0 and 50000.99 get 10 points; Trxn amounts between 50001 and 100000 get 20 points; Trxn amounts > 100000 get 30 points. Pre-case score should be calculated as below:

  - Event A – (Total amount of transactions - $ 80K) - 20

  - Event B – (Total transaction amount - $ 300K) - 30

  - Total pre-case score is 50 (A(20) + B(30) = 50)

Aging

Scores of the events in the correlation is decreased if the correlation is not consolidated to a case after some time. After certain duration event is completely dropped from the correlation and shall be archived. The score reduction is configurable by country, jurisdiction, scenario and time period.

In this attribute, each event is scored. The total of the events scored contributes to pre-case score.

The following is the scaling for ageing events that are members of un-promoted correlations. Age scaling must be configurable and can be changed from following sample:

- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 3 months reduce the event score by 3

- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 6 months reduce the event score by another 3

- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 9 months reduce the event score by another 3

- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 12 reduce the event score to equal 0

- Drop and archive any event of correlation age more than year.

Note: need to determine the process that would remove the event with a score of 0 from the correlation and close it with a specific reason.

Correlation is created for event A by (ML) Rapid Movement of Funds All Activity CU.

- Correlation creation date is 1st Jan 2016 and Event A with event creation date 1st Jan 2016 has an initial score of 10. So pre-case score is 10.

- On 1st of February event B by (ML) Rapid Movement of Funds All Activity CU with creation date 1st February 2016 is added to correlation. Event B score is 10 and total pre-case score now is 20. A(10)+ B(10) = 20

- On 1st April, event A age is now 3 months. Event A score will be reduced by 3 points to 7 and total pre-case score is now 17. A(7) + B(10) = 17

- On 1st May, event B age is now 3 months. Event B score will be reduced by 3 points to 7 and total pre-case score is now 14. A(7) + B(7) = 14

- On 1st July, event A age is now 6 months. Event A score will be reduced by 3 points to 4 and now total pre-case score will be 11. A(4) + B(7) = 11

- On 1st Aug, event B age is now 6 months. Event B score will be reduced by 3 points to 4 and now total pre-case score will be 8. A(4) +B(4) = 8.

- On 1st Oct, event A age is now 9 months. Event A score will be reduced by 3 points to 1 and now total pre-case score will be 5. A(1) + B(4) = 5

- On 1st Nov, event B age is now 9 months. Event B score will be reduced by 3 points to 1 and now total pre-case score will be 2. A(1) +B(1) = 2.

- On 2nd Jan 2017 event A age is now 12 months. Score will be dropped to 0. And Event A will be closed and completely dropped from correlation. Event B is only event in correlation and total pre-case score will be now 1.

- On 2nd Feb 2017 event B age is now 12 months. Score will be dropped to 0. And Event B will be closed and completely dropped from correlation.

Entity

This scoring rule defines various scoring criteria to be followed focusing on the entity attributes. The Entity scoring is performed on following entity attributes:

- Watch List Screening
- Effective Risk

Watch List Screening

If correlated entity is matched against screening specified watchlist, give the distinct customer a score. The total of the customer score contributes to pre-case score.

For example,

Entity A (10 for ML event) and B (10 for ML event) are part of correlation. The total pre-case score is 20. After some time Event C is added to the correlation. Event C involves entity C and entity C is matched to a specific WL (configurable). Matches to that WL receive a score of 60. The Event score for Event C is 10 for ML event. The correlation also now has an entity score of 60 for Entity C.

Pre-case score = A(10) + B(10) + C(10) + Entity C (60) = 90

Effective Risk

If correlated entity, effective risk >= Y then increase customer score. Scale should be configurable by effective risk and jurisdiction.

The total customer score contributes to pre-case.

For example,

- Set up rule to find the KDD_ALERT_CORR_LINK.BUS_NTITY_KEY_ID and KDD_ALERT_CORR_LINK.BUS_NTITY_ID for an alert in the correlation. Look at the respective business table (based on the BUS_NTITY_ID type) to find the Effective Risk.

- Event A Rapid Movement of Funds All Activity CU focus – scenario score of 10; Customer XXX has CUST. CUST_EFCTV_RISK_NB = 8

- Event B Rapid Movement of Funds All Activity CU focus - scenario score of 10; Same customer XXX has CUST. CUST_EFCTV_RISK_NB = 8

- Customer Effective Risk >= 7 add 10 points

- Pre-case score = A(10) + B(10) + Cust XXX(10) = 30. Dev Note – this is on distinct customer in correlation

Correlation

This scoring rule defines various scoring criteria to be followed while treating an entire correlation. The score generated by correlation scoring contributes to pre-case score. This is performed on the following criteria:

- Number of events

- Combination of Scenarios

- Total Transaction Amount

- Repeated Scenario Events

Number of events

- If the number of events in the correlation is more than X, increase correlation score.

- Scaling of correlation by number of events should be as below (scaling should be configurable by no. of events):

  - Number of events greater than 3 and less than or equal to 5 should be given a correlation score of 30.

  - Number of events between 6 and less than or equal to 10 will be given 40.

  - Correlation with more than 10 events will be given 50.

- The additional score has to be added to pre-case score.

  For example,

  A correlation has 4 events A, B, C and D by ML. Event scores for 4 events are as follow.

  - A – 10

  - B – 20

  - C – 10

  - D – 30

  Pre-case score will be now 70 but an additional 30 correlation score will be added to pre-case score as number of events in the correlation are 4. And correlation is promoted to case.

Combination of Scenarios

- When correlation contains events from scenario X and Scenario Y at the same time consider correlation to add score.

- The total of the correlation score contributes to the pre-case score.

  For example,

Event A Rapid Movement of Funds All Activity CU focus and Event B Deposit Withdrawal Same or Similar Amount AC focus are correlated in same correlation add 50 points

- Event A – 10

- Event B – 10

- Correlation – 50

- Pre-case score = 70

Total Transaction Amount

- If the total amount of transaction of the correlated events is greater than X amount, consider adding score to correlation. Risk scores for amounts can be segregated into 3 buckets (configurable). For dollar amounts, total of transactions across all correlated events is between 50K and 100K should give score of 20, 100K to 500K should be given as 30 and anything above 500K should be 50. Transaction amount should be based off of the matched binding for total trxn amount (configurable to use a functional currency total trxn amount is scenario configured for it).

- The total of the correlation score contributes to pre-case score.

  For example,

  - Event A ML scenario – total base transaction amount = 15000

  - Event B ML scenario – total base transaction amount = 40000

  - Event C ML scenario – total base transaction amount = 45000

  - Total correlation transaction amount = 100000

  - Score is A(10 for ML) + B(10 for ML) + C(10 for ML) + Correlation(30) = 60 for pre-case score

Repeated Scenario Events

- Increase score of the correlation if events are generated for same customer/entity within a configurable time period.

- Scaling for correlation by repeated scenario events should be as below:

  - Increase score by 30 if 2 events are created for same entity/same scenario within look back period. Number of events and lookback are configurable.

  - Increase score by 50 if 3 or more events created for same entity/same scenario within look back period. Number of events and lookback are configurable.

  For example,

  Assume customer CU1 had an event A on Rapid Movement of Funds (RMF) on 1st July 2016 and which had a score of 50 to start with.

  On 28th July 2016 the customer had another RMF event B with an Event score of 30. But since this a repeat event for the same scenario on the customer within a (Repeated scenario event lookback) 31 days, correlation score could be increased by say 20 points. So overall the pre case would tip over to 100 which is the score required to convert the pre-case to case.

- The total correlation score contributes to pre-case score.

CHAPTER 9 — *Promoting to Case*

The chapter focuses on the following topics:

- About Promoting to Case (PTC)
- Configuring PTC

About Promoting to Case (PTC)

The group of events are identified for correlation based on business entries in an application for example BD, CS, KYC, Third Party. This is performed based on configurable set of rules. Once the correlation is defined, every entity will have event scoring, entity will have entity scoring. Also, correlation scoring is performed. After scoring, an event can be promoted to case if it crosses the defied threshold. This is decided based on pre-scoring. Pre-scoring is performed on event scoring, entity scoring, and correlation scoring.

The following event types are promoted to case:

- BD
- CS
- KYC
- Third Party

Once an event is promoted, Administrator takes the decision for Pre-case to promotion and creates a case.

Configuring PTC

The scoring for PTC is performed in the Inline Processing Engine (IPE). For more information on scoring, see the *Scoring* section.

You can define the threshold to promote an event to case using Business Processor. A Business Processor encapsulates a business logic for assigning a value to a measure as a function of observed values for other measures.

To configure PTC, follow these steps:

1. Navigate to the ECM Home Page and select **Common Tasks** and select **Unified Metadata Manager**.

2. Click **Business Metadata Management** and select **Business Processor.** The Business Processor page is displayed.

3. Click **Edit**. The Business Processor page is displayed.

Figure 38. Adding Business Process

4. Enter the required details and click **Save**. For more information, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

5. The new threshold limit is defined.

CHAPTER 10

Configuring Processing Modelling Framework (PMF)

This chapter includes the following topics:

- About PMF
- Pre-configuration Activities
- Accessing Process Modeller
- Configuring an ECM Workflow
- Editing of an ECM Workflow
- Deleting an ECM Workflow

About PMF

The Enterprise Case Management Processing Modelling Framework (PMF) facilitates built-in tooling for orchestration of human and automatic workflow interfaces. This enables Administrator to create process-based ECM. It also enables Administrator to model business processes and workflows.

Workflows those are created using PMF are available in the Case Designer for the administrator to associate for any Case Type.

For more information on Key Features, Architecture, and Components, see the latest Processing Modelling Framework section of *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

This section covers the following topics:

- ECM Workflow Development Life Cycle
- ECM Workflows

ECM Workflow Development Life Cycle

The ECM workflow follows various stages in the development lifecycle:

- **Modeling**: The CM Administrator models the workflow in line with the ECM requirement.
- **Implementing**: The CM Administrator implements the required service and the ECM resources.
- **Deploying**: The CM Administrator integrates the Process with the ECM and deploys for execution.
- **Monitoring**: The CM Administrator monitors the current state of the Process after it is executed.

ECM Workflows

The following are default workflows available in the ECM:

- KYC

- AML

- CS-SAN

- CS-PEP & EDD

Note: You can also create new process workflow using the **Add** option. For more information, see the *Configuring an ECM Workflow* section.

Pre-configuration Activities

Before creating a workflow, the appropriate action and status should be present in the system. To perform this, you must add the entries in respective application tables.

Configuring Status

The following are the pre-configuration activities for status:

- Add a new status if the required status is not seeded.

  - To add a new status, add the entries in AAI_WF_STATUS_B and AAI_WF_STATUS_TL tables of the Config Schema.

  - The package ID should be OFS_NGECM.

- Add the same entries in KDD_STATUS table of the Atomic Schema.

Configuring Action

Add a new action if required action is not seeded. For more information on configuring action, see the *Configuring Actions*.

Note: If you want to configure a new report type, you must add a new PMF action to the KDD_RRS_ACTN table. If the report type is based on the CRR framework, set the FRAMEWORK_ENABLE_FL parameter to Y. For example:

```
insert into kdd_rrs_actn (ACTN_CD, ACTN_DESC_TX, ACTN_ERR_CD, SUPPL_RPT_FL, CRCTD_RPT_FL,
ACTN_DT, RPT_TYPE_CD, FRAMEWORK_ENABLE_FL) values ('CA945S', null, 'CA264', 'N', 'N', null,
'SAR', null);
```

Configuring Attributes

You can define a new attribute which is used in the Attribute Expression Application Rule. These attributes are used for status changing actions in the Attribute Expression. Each attribute is identified with an ID APP_COMP_ATTR_MAP_ID, based on which the values for attributes can be fetched. To perform this, you must add the entries in AAI_AOM_APP_COMP_ATTR_MAPPING table. The following is the format of this table:

Table 24. Configuring Attributes

Column Name	Description	Example
APP_COMP_ATTR_MAP_ID	App ID of the attribute	1
N_ATTRIBUTE_ID	ID of the attribute	1
V_ATTR_CODE	Name of the attribute	Action, status, or Role
N_ATTR_TYPE_ID	ID of the attribute type. The values of the attributes are fetched based on attribute type. 1001- Static 1002- Query 1003- JavaAPI For more information, see the *Attribute Types*.	1002
V_ATTRIBUTE_VALUE1 V_ATTRIBUTE_VALUE2	Values to be fetched for the attribute. Based on the attribute type, you need to pass the values.	If Attribute Type is 1002, then below are example of query: Select `t.action_cd,t.action_nm` from kdd_action t where `t.action_category_code` is not null and `t.action_category_code` not in ('ENT','PR','EXP','AS','DD','EML', 'OBS') **or** Select `t.status_cd,t.status_nm` from kdd_status t **or** Select `s.v_role_code,s.v_role_code` from cssms_role_function_map s where `s.v_function_code = 'CMACCESS'`
N_APP_ID	Application code for which the current attribute is configured.	OFS_NGECM
N_COMP_ID	Component code for which the attribute is configured.	-1
V_UDP_CODE	Special property used by applications (user defined). For example, 'GET_STATUS' –to get the status for the workflow.	

1. Add the values in `N_ATTRIBUTE_ID` and `V_ATTR_CODE` columns. Here, the values of attributes are fetched based on the attribute types. Following are the attribute types with their IDs:

Table 25. Attribute Types

Attribute Type ID	Attribute Type Name	Description
1001	Static	Store attribute values in the AAI_AOM_STATIC table as V_STATIC_ID and V_STATIC_VAL.
1002	Query	Enter the SQL query in V_ATTRIBUTE_VALUE1 in the AAI_AOM_APP_COMP_ATTR_MAPPING table, which has to be fired to fetch the attribute values.
1003	JavaAPI	Enter the method that is configured for V_ATTRIBUTE_VALUE1 for the required attribute. The configured method in the class path is invoked to get the attribute values in this case.

2. Define the query for attribute in V_ATTRIBUTE_VALUE1 column.

After the attribute is defined, you can access this using Application Rule "Attribute Expression". For more information, see the *Defining Application Rules* section.

Accessing Process Modeller

This section explains how to access the Process Modeller page.

To access the Process Modeller page, follow these steps:

1. Click Administration icon.
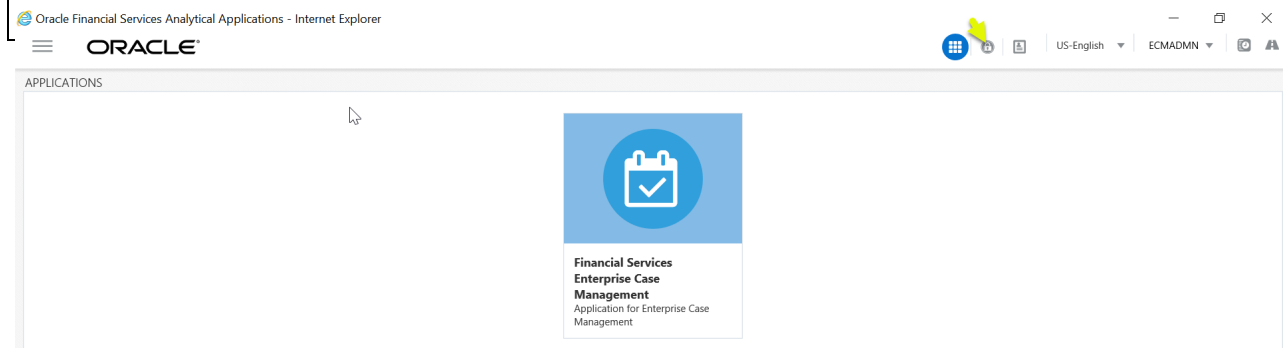
2. Administration page is displayed. Click the **Process Modeller** option from **Process Modelling Framework**.
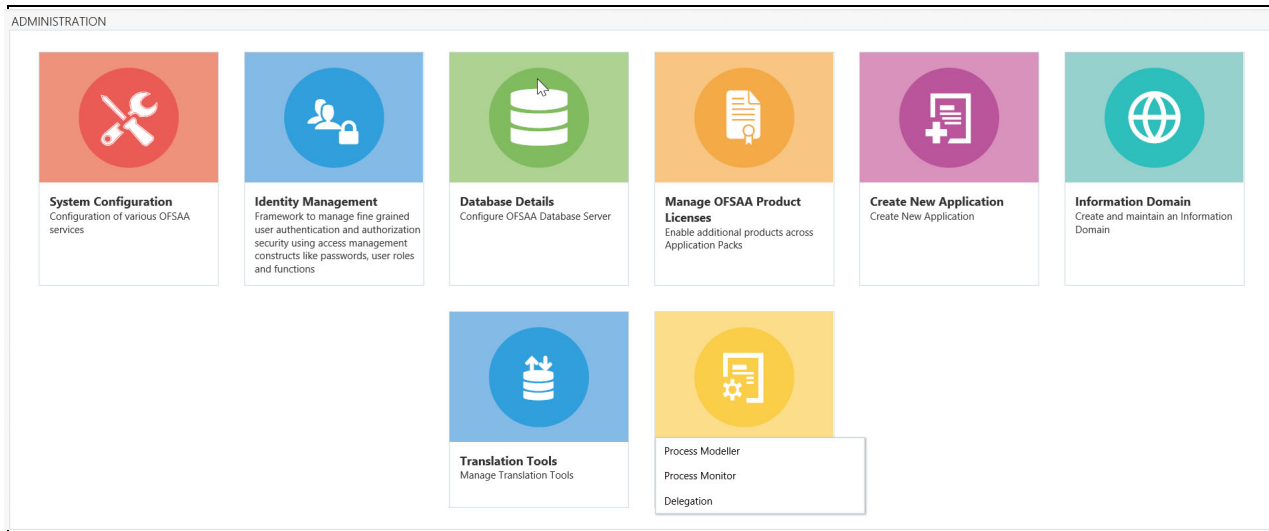
3. The Process Modeller window is displayed.
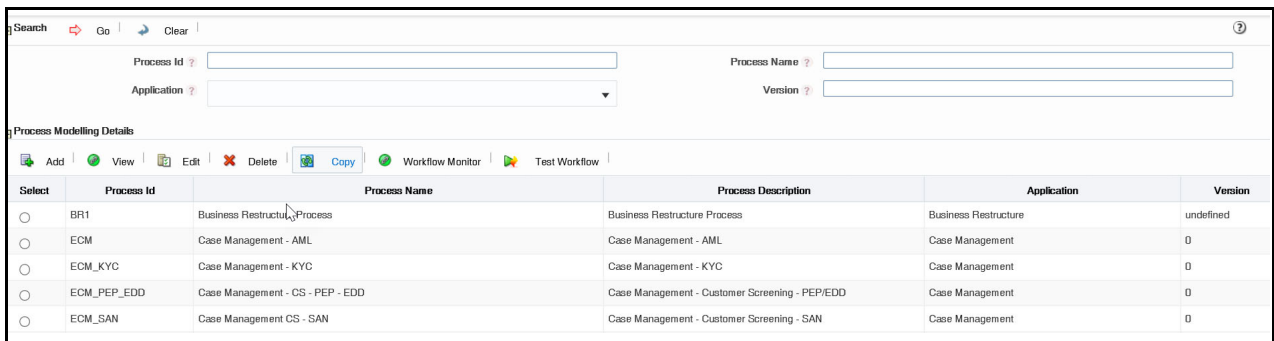
Figure 39. Process Modelling

The Process Modeller window displays the existing Processes with the details such as Process ID, Process Name, Process Description, Application, and Version. This window allows you to add a new Process, modify and delete the existing Processes, and monitor the workflow of the Processes. You can also export the Process definition.

Using the Search grid, you can search for a specific Process based on the Process ID, Process Name, Application or Version.

Configuring an ECM Workflow

The following is a sample workflow (AML) used to demonstrate how to configure the workflows in the ECM using PMF.

The following sections are covered in this topic:

*   Creating Workflow

- Defining Datafields
- Defining Application Rules
- Using Process Modeller Editor

Creating Workflow

This section explains how to create a new ECM workflow.

To create a workflow, follow these steps:

1. Navigate to Process Modeller window under Processing Modelling Framework.
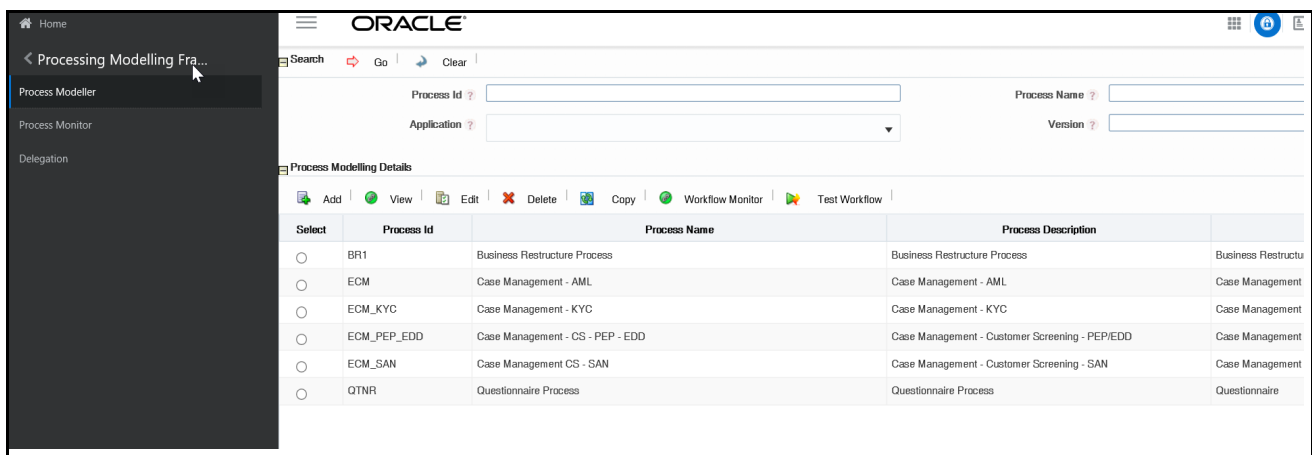
Figure 40. Process Modeller Window

2. Go to Process Modelling Details section. Click **Add**. The Process Details window is displayed.
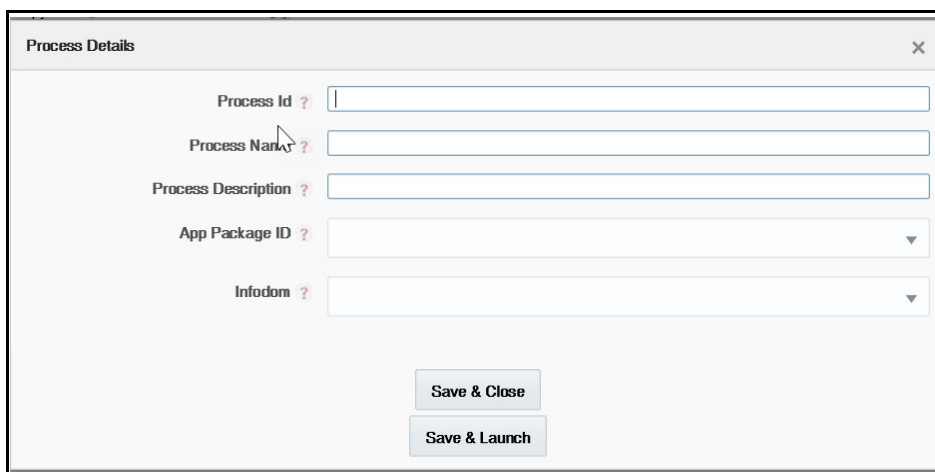
Figure 41. Process Details

3. Enter the following details in Process Details window:

Table 26. Process Details

Field Name	Description
Process ID	Enter the new ECM workflow Process ID.
Process Name	Enter the Process name for ECM workflow.
Process Description	Enter a brief description of the Process.
App Package ID	Select the *Case Management* form the App Package ID drop-down list.
Infodom	Select the ECMINFO from the Infodom drop-down list. This is the default Infodom. You can configure your own Infodom. It is the information domain in which you want to create the business process.

4. Click **Save & Close** to save the definition and go back to Process Modeller Summary window or **Save & Launch** to save the definition and open the Process Modeller Editor window.
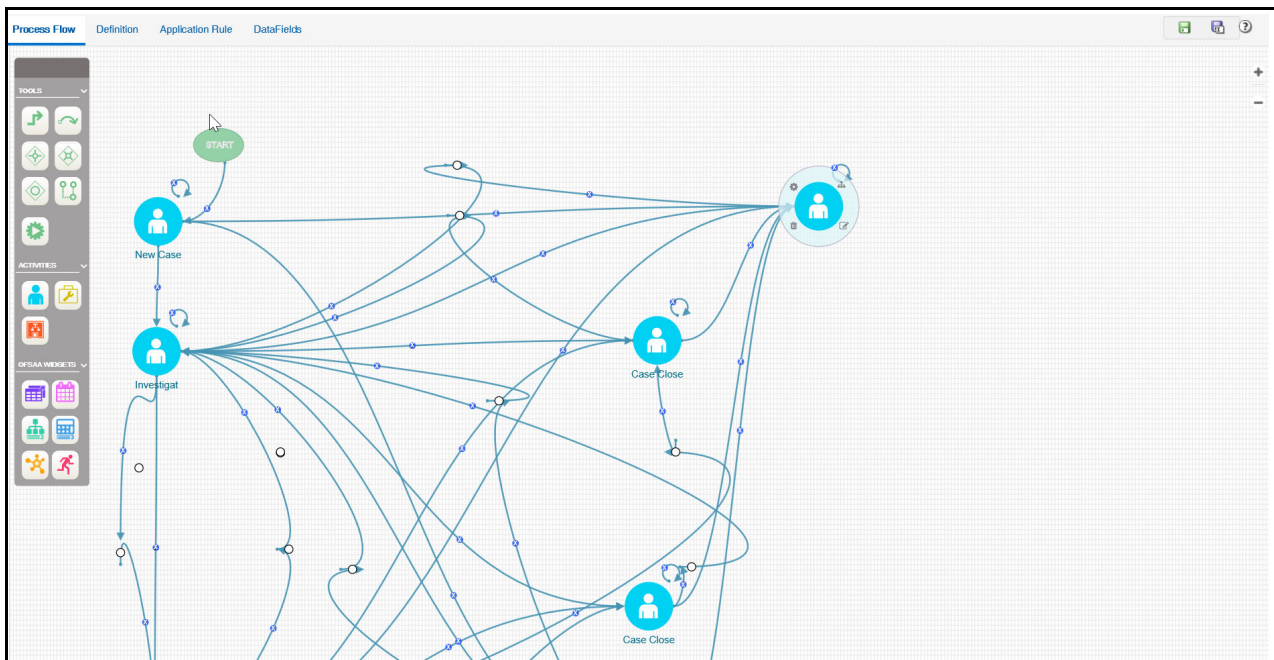
Figure 42. Process Modeller Editor window

Defining Datafields

Data Fields are Process variables which hold the data information required to be passed between ECM and Process Engine.

Data Field which is also known as Process Variable helps Processes to access and store information from outside the application. Often the process flow is based on the value of this information. In other cases, this information is the result of running the tasks in the process. This tab helps to view, add, edit, and delete Data Fields associated with the Process.

The defined Datafield is populated and used when you are defining a new Application Rule (Stored Procedure, Function, Java External API). It is used in Input Parameter field.

For more information, see the *Defining Application Rules* section.

For more information on Datafields, see the Processing Modelling Framework section of *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Defining Application Rules

Application Rules is the interface through which Process Engine executes the Application Business Logic and other Conditional logic. This tab helps to add, edit, and delete Application Rules associated with the Process.

The Application or API Rule is the interface between the process engine and the application, including any parameters to be passed.

Based on their usage these are categorized into three types.

- Execution Rule: These are Business Logic executed as Task by an Activity.

- Decision Rule: This rule returns Boolean value "True/False", used in decision making during split/branching of transition.

- Selection Rule: This rule fetches some value, useful to get value dynamically from a table or other source.

For example, select v_created_by from fct_expenses where id=101

Following are the supported Application Rule Types:

- SQL, JAVA

- Stored Procedure

- Function

- Java External API

- Webservices

- Outcome Rules

- Expression

- Attribute Expressions

For more information, see the Processing Modelling Framework section of *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

Using Process Modeller Editor

Using the Process Modeller Editor window you can perform the following tasks:

- Starting a Process

- Adding an Activity

- Adding a Transition

Starting a Process

Using this component you can start a new ECM workflow.

To start a process, follow these steps:

1. Navigate to the Process Flow tab, click **Start** from the toolbar and then click the canvas where you want to draw the activity. The new Start icon is displayed. This Start activity indicates the first activity to be executed in the Process.

2. Double-click the **Start** icon.
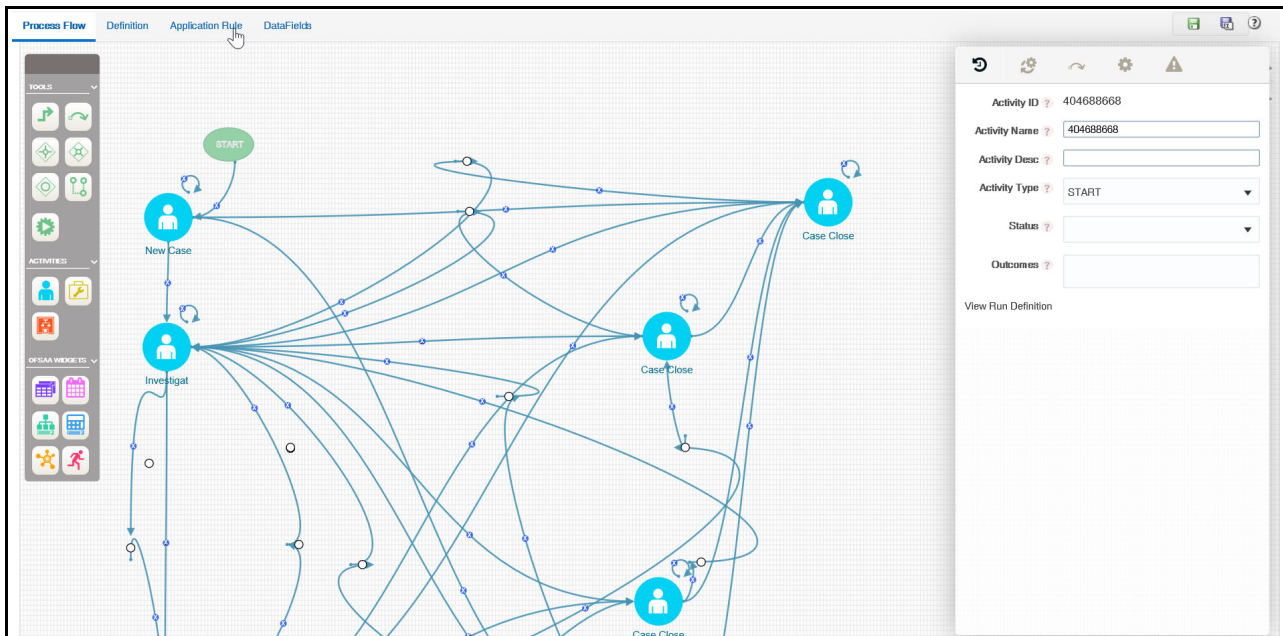
Figure 43. Starting Process

3. Enter the following information in the respective fields:

Table 27. Process

Field Name	Description
Activity ID	Displays the automatically generated Activity ID.
Activity Name	The activity name is displayed automatically same as the Activity ID. Modify the activity name if required.
Activity Desc	Enter the description of the Activity.
Activity Type	By default, the activity type of the selected activity is displayed. To change the activity type, select the required activity type from the drop-down list. The options are Manual, Automatic, Start, Parallel, Sequential, Connector, Run Task, Multi-choice, and Sub Process.
Status	Select the status of the activity from the drop-down list. For example, Closed-SAR, New, Investigation. **Note:** This is not applicable if the Activity is a Run Task.

Field Name	Description
Outcomes	Select the required Outcomes from the drop-down list. For example, Approve, Reject, or, Submit. **Note:** This is not applicable if the Activity is a Service Task or Run Task.
File Upload	Click Attachment and browse to select the file you want to upload. The progress of file upload is shown. The following message is displayed: *Your file has been uploaded* after successful upload of the file. Only a single file can be uploaded. If you upload a new file, the existing file is replaced with the new one. Click Attachment icon adjacent to the file name to remove the file. If a file is attached, Attachment icon is displayed. Click Attachment icon to view or save the file.

Implementing a Process

This section explains how to implement the newly created process. For more information, see the *Implementing a Process* section.

Adding Transition

This section explains how to add transition to the newly created process. For more information, see the *Adding Transition*.

Adding an Activity

To add activity, follow these steps:

1. Click an activity under Activities toolbar in the left panel and then click the canvas where you want to draw the activity. The options are Human Task, Service Task, Run Task and Sub Process.

2. Double-click the icon. On the Right Panel, the Activity tab is displayed.

3. Enter the following information in the respective fields:

Table 28. Adding Activity

Field Name	Description
Activity ID	Displays the automatically generated Activity ID. For example, Job_1504159648899.
Activity Name	The activity name is displayed automatically same as the Activity ID. Modify the activity name if required. For example, New Case.
Activity Desc	Enter the description of the Activity.
Activity Type	By default, the activity type of the selected activity is displayed. Select activity type as Manual from the drop-down list. To change the activity type, you can select the required activity type from the drop-down list. The options are Manual, Automatic, Start, Parallel, Sequential, Connector, Run Task, Multi Choice, and Sub Process.
Status	Select the status of the activity from the drop-down list as New. The list displays the seeded values in the AAI_WF_STATUS_B table.

Field Name	Description
Outcomes	Select the required Outcomes from the drop-down list. The list displays the seeded values in the AAI_WF_OUTCOMES_B table. **Note:** This is not applicable if the Activity is a Service Task or Run Task
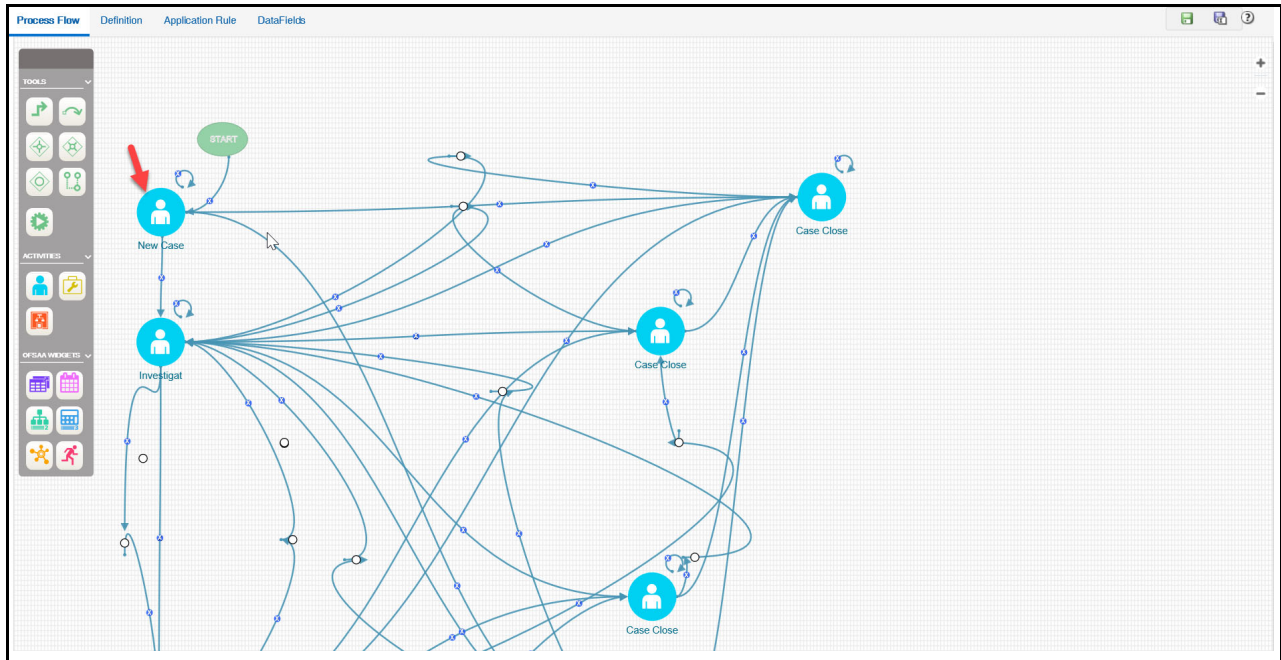
Figure 44. Adding Activity

Implementing an Activity

This section explains how to implement the New Case as an activity.

To implement the newly created activity, follow these steps:

1. Select Implementation tab. The Implementation details are displayed.
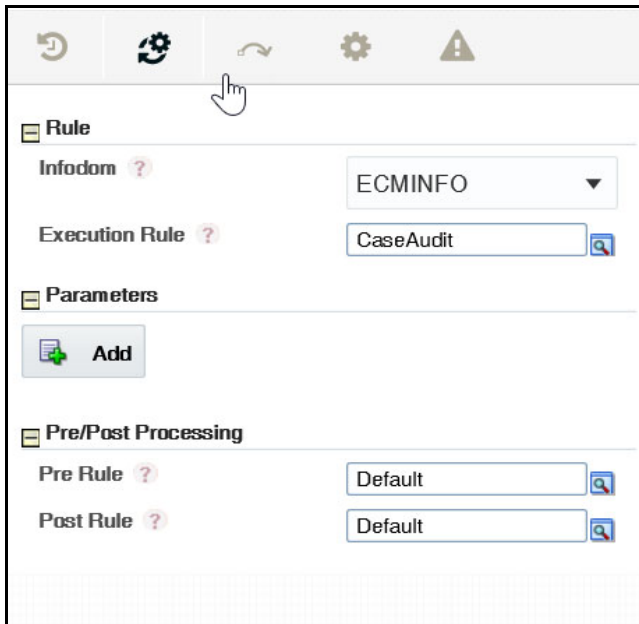
Figure 45. Implementing Activity

2. Go to Rule section. Select ECMINFO as the information domain from the Infodom drop-down list.

3. Select the execution rule which must be executed for this activity. For example: Case Audit. Or, you can search for the execution rules using the **Search** icon.

4. For Run Task: Click **Search**. The Run Component Details window is displayed. Expand Base Run or Simulation Run and select the required Run definition from the Segment. Click **OK**.

Adding Transition

Using this component you can add transition to New Case.

To add transition, follow these steps:

1. Go to the Process Flow tab, click **Transition** from Tools.

2. Click the activity from which you want to start the transition.

3. Again, click the activity to which you want to connect the transition.

    Double-click the Transition and enter the required details in the Edit Transition window.

Or Double-click the Activity for which you want to add a transition. On the Right panel, click Transitions icon and click **Add**. The Add New Transition window is displayed.
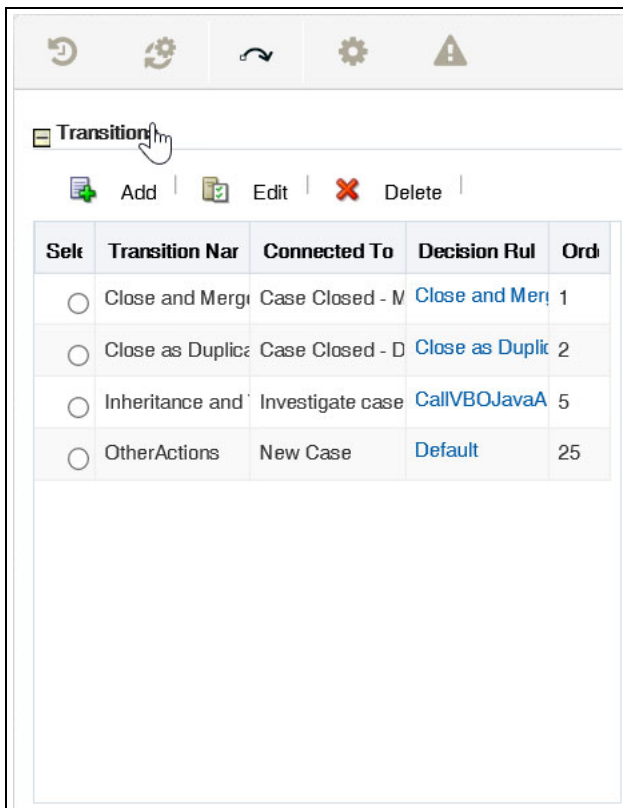
Figure 46. Add Transition

4. Enter the following information in the respective fields:

Table 29. Transition

Field Name	Description
Transition Name	Enter the Transition Name. For example, 404688668_Job_1495627226471
Connected To	Select the activity (as New Case) to which you want to connect the current activity, from the Connected To drop-down list. All defined activities in the current Business Process are displayed.
Decision Rule	Select the appropriate Decision Rule by clicking Search icon. This rule is validated during Process execution. If the output value is TRUE which indicates Success, the process has to flow through this transition to go the next activity. If the output value is FALSE which indicates Failure, the current transition is ignored and the next transition is taken for evaluation if available. If all the transition rules fail (that is evaluated to value FALSE), then the Process remains in the current State. For more information, see th *Defining Application Rules* section.
Order	Enter the Precedence value based on which the transition Decision rules must be executed for multiple transitions, in the Order field. This has effect for transitions from a Sequential gateway only.

5. Click **OK**. The transition has linked two activities. That is Start and New Case.
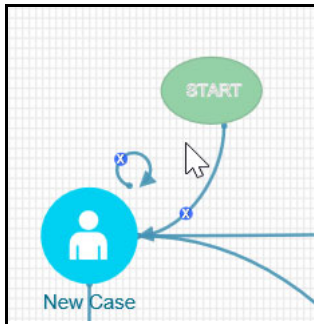
Figure 47. Adding Transition

Editing of an ECM Workflow

To edit an ECM workflow, follow these steps:

1. Navigate to Process Modeller window.
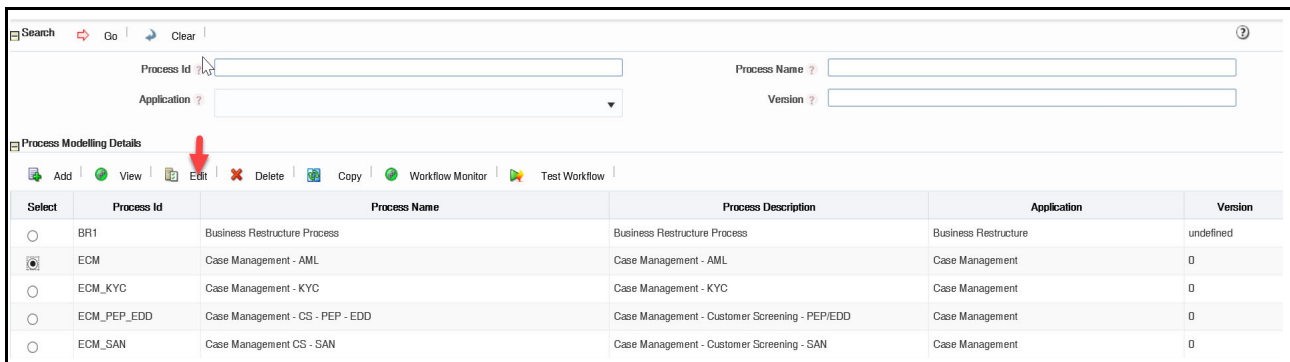
Figure 48. Process Modeller window

2. Select the workflow using the corresponding radio button.

3. Click Edit. The Process Modeller window is displayed for editing.
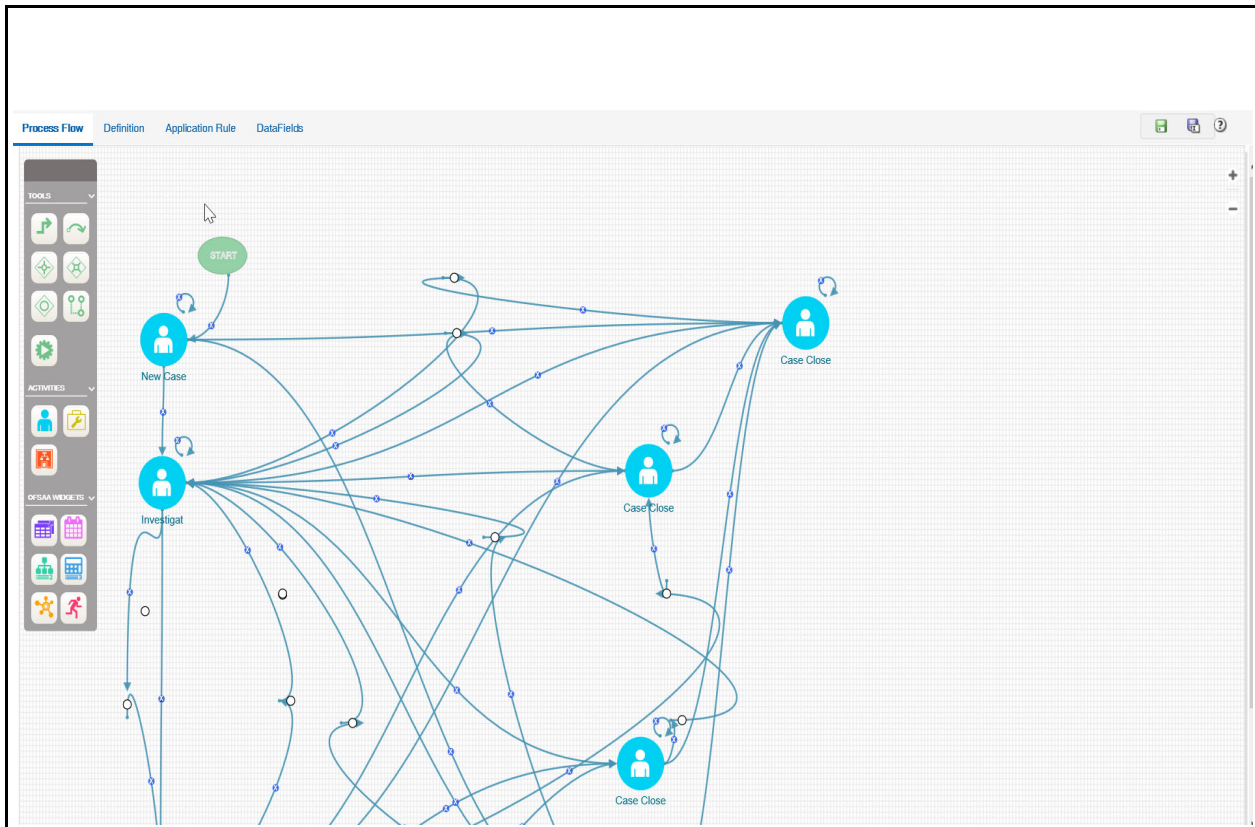
Figure 49. Editing Workflow

    4. Make the required changes and click **OK**.

Deleting an ECM Workflow

To delete a workflow, follow these steps:

1. Navigate to Process Modeller page under Processing Modelling Framework.

2. Select the workflow using the corresponding radio button.

3. Click **Delete**. A confirmation message is displayed.

4. Click **OK**.

CHAPTER 11 · *Managing Case Designer*

This chapter explains the concept behind Case Designer and configuring a case using the Case Designer UI by the Administrator user.

The following topics are covered in this chapter:

- About Case Designer
- Accessing Case Designer
- Case Designer Home page
- Defining Case Class
- Defining Case Type

About Case Designer

Case Designer allows to configure Case Class, Case Type, and associated definitions. Based on the configuration, definitions are dynamically rendered in the Case Management application to investigate cases and take appropriate actions on them for case resolution.

- Create and modify Case Class and Case Type definitions.
- Case Class is the top most definition through which a case is created.
- Case Type provides detailed classification of a case. For example, you can create a Case Class as *AML* and Case Type as *AML Surveillance* and related Attributes (*Jurisdiction, Business domain*, and so on), Entities (*Narrative, Evidence*, and so on), and Workflow (*Case Management*)
- Define related attributes, entities, and workflow in the Case Type.
- Case Type definitions control the display of tabs and fields on the Case Management UI.
- Changes to Case Class and Case Type definitions are automatically reflected on the Case Management UI.

Accessing Case Designer

This section explains how to access the Case Designer page.

To access the Case Designer page, follow these steps:

1. Navigate to the Case Management Configuration page. For more information on how to navigate to the Case Management Configuration page, see *Chapter 2, Getting Started.*

2. Click **Case Designer**. The Case Designer page is displayed.

Case Designer Home page

This section displays the list of previously added Case Classes or Case Types and overview in a 3D Pie chart. This also allows you to add a new Case Class or Case Type.
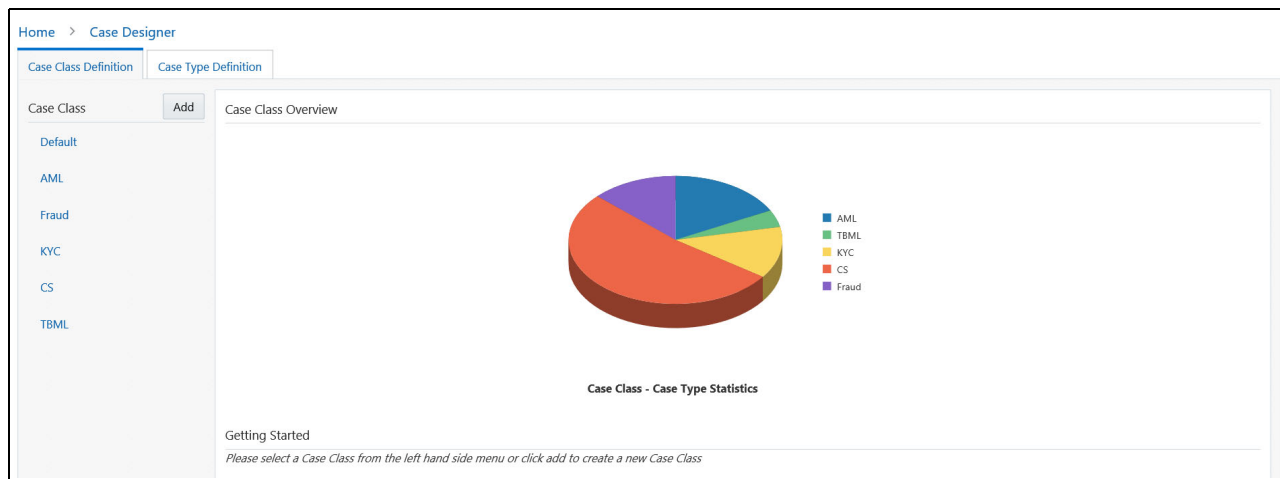
Figure 50. Case Designer Home Page

To view Case Designer Home page, follow these steps:

1. Navigate to the Case Designer page.

2. Click the **Case Class Definition** or **Case Type Definition** tab. The previously added Case Class or Case Type list is displayed in the Left Hand Side (LHS) menu.

3. Select **Case Class Definition** tab and go to the **Case Class Overview** section. Hover over the Statistics pie chart. The number of case types created under a particular case class is displayed.

   Or, select **Case Type Definition** tab and go to the **Case Type Overview** section. Hover over the Statistics pie chart. The number of cases created under a particular case type are displayed.

   Using the Case Designer Home page, you can also add a new Case Class or Case Type. For more information, see *Adding Case Class* or *Adding Case Type* sections.

Defining Case Class

This section explains key features and how to define a Case Class.

The following topics are covered in this section:

- About Case Class
- Adding Case Class
- Editing Case Class

About Case Class

- A Case Class is the top most definition through which a case is created.

- Used for grouping case types.

- Add and modify case class.

- Does not impact directly on the ECM workflows.

- Updated even if cases are linked to case type.

- Cannot remove existing case classes.

Adding Case Class

This section explains how to add a new case class. For example, AML and Fraud.

To add a new case class, follow these steps:

1. Navigate to the Case Designer page.

2. Click **Case Class Definition** tab.

3. Click **Add**. The Case Class Definition page is displayed.

4. Enter the following information in the respective fields.

Table 30. Case Class Definition

Fields	Description
Case Class	Enter the unique case class name. For example, AML or Fraud.
Description	Enter details about the case class.

5. Click **Save**. The following message is displayed: *Case Class is created successfully*.

6. Click **OK**. The Case Class is added to the Left Hand Side (LHS) menu.

Editing Case Class

This section allows you to modify the existing case classes. Any change to case class is reflected on the ECM UI.

Note: A Case Class is updated even if cases are linked to the case type.

To modify a case class, follow these steps:

1. Navigate to the Case Designer page.
2. Click **Case Class Definition** tab.
3. Select the existing case class in LHS menu. The case class details are displayed in Right Hand Side (RHS) pane.
4. Modify the necessary information in the required fields. For more information on the fields, see *Table 30*.
5. Click **Save**. The following message is displayed: *Case Class is updated successfully*.
6. Click **OK**. The Case Class is updated in the LHS menu.

Defining Case Type

This section explains key features and how to define a Case Type in the Case Designer.

This section covers the following topics:

- About Case Type
- Adding Case Type
- Editing Case Type

About Case Type

- A Case Type is the second level definition after Case Class through which cases are created.
- Provides more detailed classification of a case. For example, If Class is *AML*, Type can be *AML Surveillance*.
- Add new case types and modify the existing case types.
- Define related attributes, entities, and workflow.
- Controls the display and behavior of fields on the Case Search, Case Context, Create Case page.
- Determines the display of tabs in the Case Summary page, and drives the case action workflow.
- Must associate one Workflow to the Case Type.

Note: The data displayed on the tab is not controlled by case type.

Adding Case Type

This section how to add a new case type to the existing case class along with related attributes, entities, and workflow.

To add a new case type, follow these steps:

1. Navigate to the Case Designer page.

2. Click **Case Type Definition** tab.
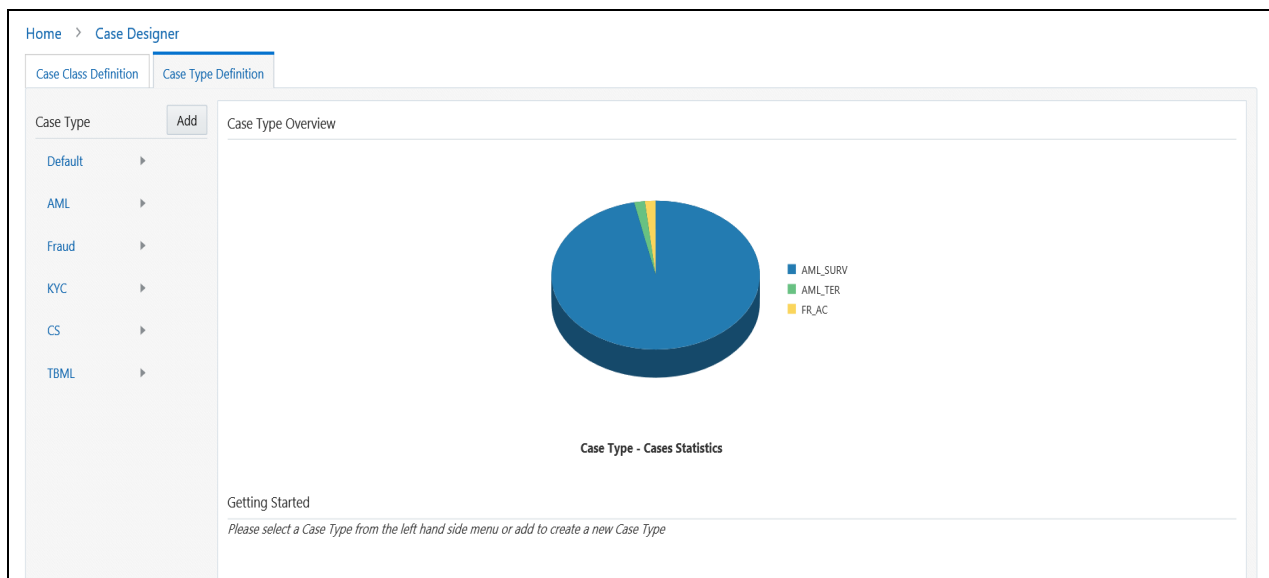
3. Click **Add**. The Case Type Definition page is displayed.

Figure 51. Case Type Definition Page

4. Enter the following information in the respective fields.

Note: The fields marked with * (Asterisk) are mandatory. The Save button is disabled till you enter mandatory fields. You must associate one Workflow to the CaseType. For more information on associating a workflow, see *Defining Workflow* section.

Table 31. Case Type Definition

Fields	Description
Case Class	Select a case class from the Case Class drop-down list. For example, AML or Fraud.
Name	Enter the unique name for the case type.
Description	Enter details about the case type.

5. If you want to create a case type with only default fields, click **Save**. The following message is displayed: *Case Type is created successfully.*

Note: When you modify case type definitions, you cannot edit Case Type name.

The Case Type is created with the default attributes, entities, and workflow. The newly created Case Type is added in the LHS menu under the respective Case Class.

Or, if you want to add optional definitions to Attributes, Entities, or Workflow sections of newly created case type, then continue with *Configuring Optional Definitions in CaseType* section.

Configuring Optional Definitions in CaseType

This section explains about optional definitions and how to manage them in Case Designer.

This section covers the following topics:

About Optional Definitions

- Additional attributes and entities are defined as optional definitions.

- If any optional definitions are removed from the Case Type, then it is not shown in the Case Summary. This impact is generic irrespective of the status.

Defining Attributes

This section describes about additional attributes definitions and how to configure them in the Case Type.

The following sections are covered in this topic:

- About Attributes
- Adding Optional Attributes to the Case Type
- Deleting Attributes

About Attributes

- Attributes are fields that display on the Case Search, Case Context, and Create Case page of ECM UI.

- Classified into mandatory and optional definitions.

- Mandatory Attributes - Case ID, Class, Type, Status, Title, Jurisdiction, Business Domain, Priority, Created, Owner Organization, Due, Owner, Closed, Assignee, Description.

- Optional Attributes - Document Control, Scenario Class, and Risk Score.

- Configure Attributes definitions to show or hide them on ECM UI.

- By default, all mandatory attributes are shown in the Attributes section.

- Can add or remove only optional attributes using Case Designer.

- Dynamic rendering of the attributes based on its behavior across the different case pages. For example, Case ID attribute is hidden on the Create Case page but it is disabled on the Case Context page.

- Whenever changes happen to attributes those changes are reflected on all case related pages based on its behavior in the Enterprise Case Management UI.

Adding Optional Attributes to the Case Type

This section explains how to add optional attributes to a case type. By default, optional attributes are displayed in the Available Attributes box. The mandatory attributes are displayed in the Selected Attributes box. You can select optional attributes and move them to Selected Attributes box. All attributes that are in Selected Attributes box appear as fields in the case related pages of ECM UI based on its behavior.

To add optional attributes, follow these steps:

1. Navigate to the Case Type Definition page.

2. Click **Attributes** tab. The optional attributes are displayed in the *Available Attributes* menu.
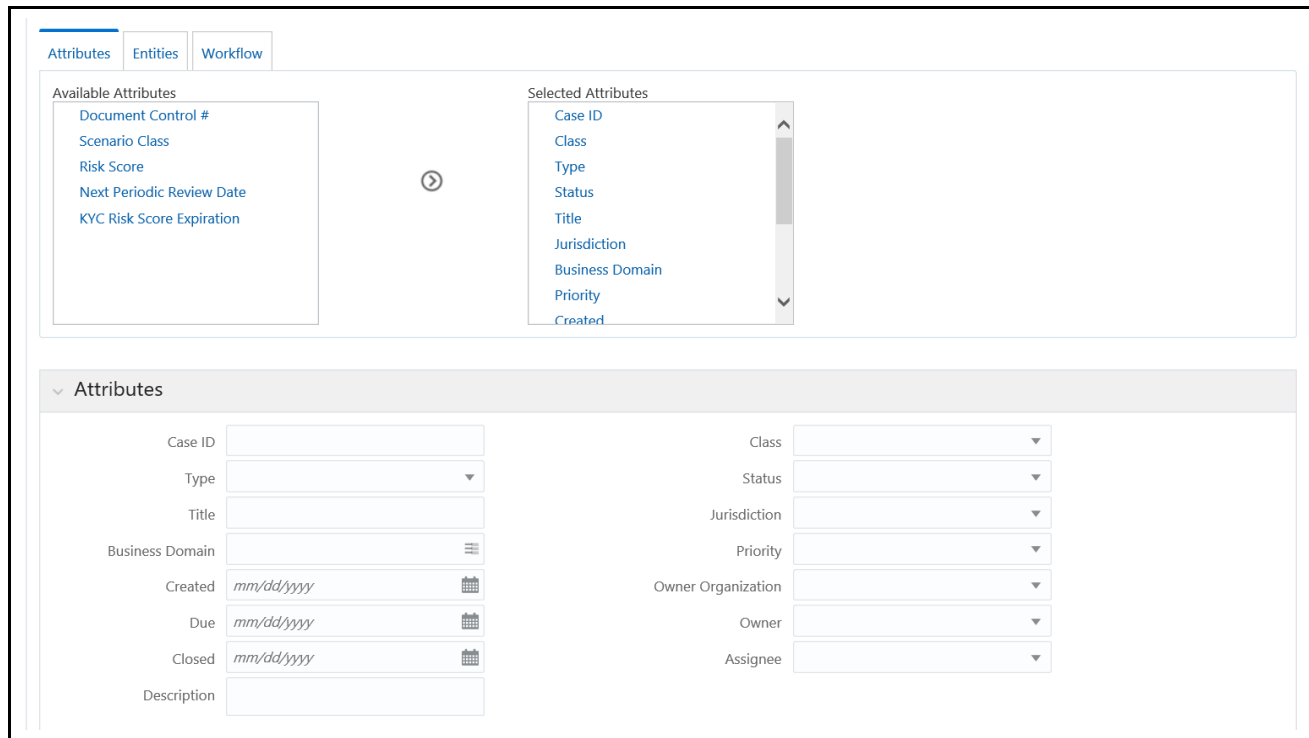
Figure 52. Attributes Page

3. Select the required attributes from the **Available Attributes** menu and click [>] button. The selected optional attributes are moved to the **Selected Attributes** menu and these are displayed in Attributes sections.

   Note: The newly added attributes are marked with [X] icon.

4. Click **Save**. The following message is displayed: *Case Type is created successfully.*

   Note: If you modify existing Case Type attributes, the following message is displayed: *Case Type is updated successfully.*

5. Click **OK**. The Case Type is updated with optional attributes.

Deleting Attributes

This section explains how to remove optional attributes from the Case Type.

To remove optional attributes, follow these steps:

1. Navigate to the Case Type Definition tab.

2. Select required Case Type. Go to the Attribute section.

3. Click [X] against the required attributes to remove from Attributes section. The deleted attributes are moved back to the Available Attributes box.

4. Click **Save**. The Attribute section is updated.

   Note: The deleted attributes are not displayed on the case related pages in the Enterprise Case Management UI.

Defining Entities

This section describes about an Entity and how to configure in the Case Type.

The following sections are covered in this topic:

- About Entities

- Adding Optional Entities to the Case Type

- Deleting Entities

About Entities

- Entities are tabs that display on the Case Summary section of ECM UI after you define them in Case Designer.

- Defines entities to show or hide them on the Case Summary.

- Entities are classified into mandatory and optional.

- Mandatory Entities – Event Details, Evidence, Relationship, Narrative, Audit History.

- Optional Entities - Correlation, Account, Customer, Employee, Household, Investment Advisor, External Entity, Correspondent Bank, Transactions, FATCA Assessment, Financials, Involved Party, Network Analysis, Enhanced Due Diligence, and Risk Assessment.

- Case Summary section of ECM UI display entities (tabs) even there is no data is associated with the entity.

- Add or remove only optional entities.

- Ordering of entities can be configured.

- Whenever changes happen to entities those changes are reflected on Case Summary section for that Case Type in Enterprise Case Management UI.

Adding Optional Entities to the Case Type

This section explains how to add optional entities to a case type. By default, optional entities are displayed in the Available Entities menu. The mandatory entities are displayed in the Selected Entities menu. You can select optional entities and move them to Selected Entities menu. All entities that are in Selected Entities menu appear as tabs on the Case Summary page of ECM UI.

To add optional entities, follow these steps:

1. Navigate to the Case Type Definition page.

2. Click **Entities** tab. The optional entities are displayed in the *Available Entities* menu.
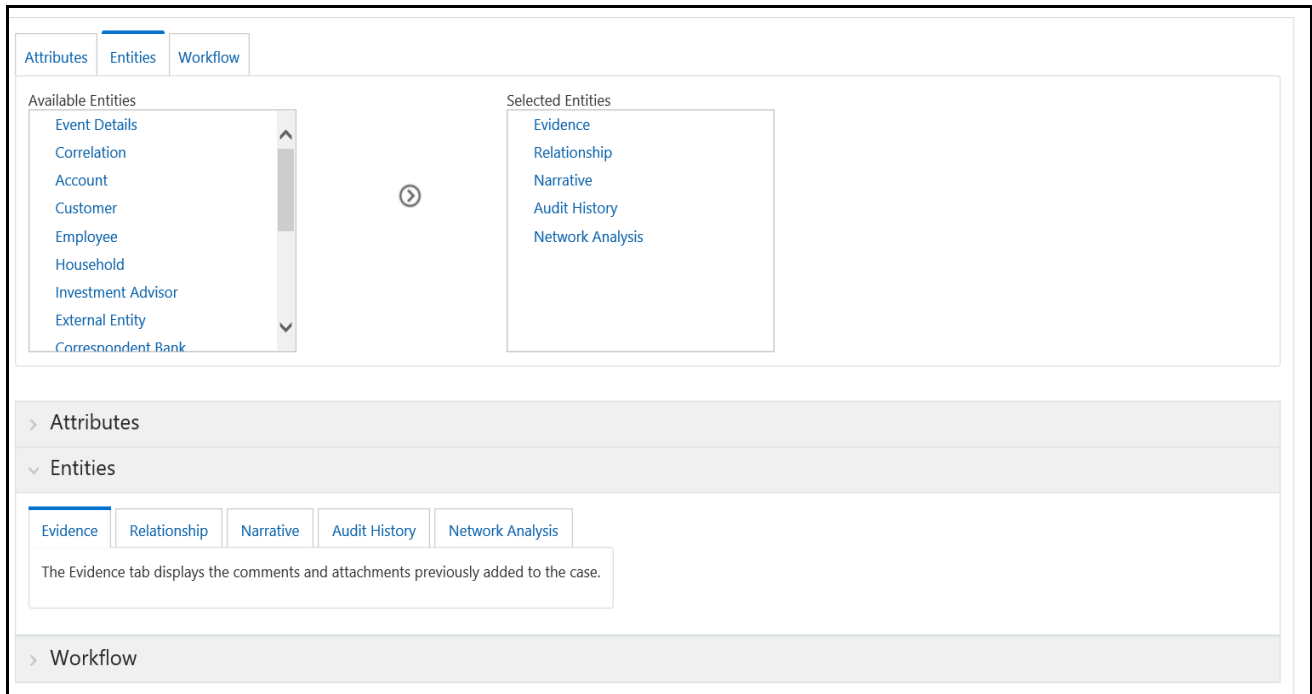
Figure 53. Entities Page

3. Select the required entities from the **Available Entities** menu and click ⏵ button. The selected optional entities are added to the **Selected Entities** menu and these options are displayed in Entities sections as tabs.

    Note: The newly added entities are marked with ❎ icon.

4. Select the required tab. Hold it and move to position it according to your requirement.

5. Click **Save**. The following message is displayed: *Case Type is created successfully.*

    Note: If you modify existing Case Type Entities, the following message is displayed: *Case Type is updated successfully.*

6. Click **OK**. The Case Type is updated with optional entities.

Deleting Entities

This section explains how to remove optional entities from the case type.

To remove optional entities, follow these steps:

1. Navigate to the Case Type Definition tab.

2. Select required Case Type. Go to the Entities section.

3. Click ❎ against required entities to remove from Entities section. The deleted entities are moved back to the Available Entities menu.

4. Click **Save**. The Entities section is updated.

Note: The deleted entities (tabs) do not display on the Case Summary section in the Enterprise Case Management UI.

Defining Workflow

This section describes about the workflow and its usage in case type.

The following sections are covered in this topic:

- About Workflows
- Adding Workflow
- Deleting Workflow

About Workflows

- Workflows are tabs that display on the Case Summary section of ECM UI after you define them in Process Modelling Framework (PMF). For more information, see the Process Modelling Framework section.
- Only one workflow selection at a time

Adding Workflow

This section explains how to add workflow to a case type. The workflow selection is optional for a case.

By default, the list of defined workflows will be displayed in the **Available Workflows** box. You can select the workflow and move them to **Selected Workflows** box. The workflow that is in **Selected Workflows** box appear as fields in the case related pages of ECM UI based on its behavior.

To add a workflow, follow these steps:

1. Navigate to the Case Type Definition page.
2. Click **Workflow** tab. The defined workflows are displayed in the **Available Workflows** menu.

Figure 54. Workflow Page

3. Select the required workflow from the **Available Workflows** menu and click ⏩ button. The selected workflow is moved to the **Selected Workflows** menu and these are displayed in Workflow sections.

   Note: The newly added workflow is marked with ❌ icon.

4. Click **Save**. The following message is displayed: *Case Type is created successfully.*

   Note: If you modify existing Case Type attributes, the following message is displayed: *Case Type is updated successfully.*

Deleting Workflow

This section explains how to remove the workflow from the Case Type.

To remove the workflow, follow these steps:

1. Navigate to the Case Type Definition tab.

2. Select required Case Type. Go to the Workflow section.

3. Click ❌ against the required workflow to remove from Workflow section. The deleted workflow is moved back to the **Available Workflows** box.

4. Click **Save**. The Workflow section is updated.

Editing Case Type

This section describes how to modify existing Case Type definitions.

To modify a case type, follow these steps:

1. Navigate to the Case Designer page.

2. Click **Case Type Definition** tab.

3. Select an existing case type in LHS menu. The Case Type Definition page is displayed.

4. Modify the necessary details in the Case Class and Description fields. For more information on the fields, see *Table 30*.

Note: Case Type is not editable.

5. Click **Save**. The Case Type Definition section is updated.

Note: The modified Case Type definitions are updated in the Enterprise Case Management UI.

To modify or delete Attributes or Entities definitions, see *Defining Attributes* and *Defining Entities* respectively.

CHAPTER 12　*General Configuration*

This chapter provides instructions for configuring parameters for case management. This chapter includes the following topics:

- Configuring the Client Logo Image
- Accessing Manage Parameters
- Configuring the Default Currency Code
- Configuring the Base Time Zone
- Modifying Case Highlight Status
- Configuring a Visual Cue for Cases Nearing Due Date
- Configuring Case Own Flag Consideration
- Configuring Case Prefix
- Configuring the Display of Value in By Field Name/ID
- Configuring Organization Type
- Configuring the Default Due Date Calculation
- Configuring Administration Tools
- Configuring Application Server
- Configuring Case Age Calculation
- Configuring Case Assignment Inheritance
- Configuring Case Correlation Owner
- Configuring Case Inheritance
- Configuring Case Risk Values
- Configuring Default Case Owner
- Configuring E-mail
- Configuring Mode of Transferring Alert Information
- Configuring Mode of Transferring Case Information
- Configuring Lock Time Period for Case Actions
- Configuring OBIEE
- Configuring View All Organization
- Configuring File Size
- Configuring Views
- Configuring ECM Security Function
- Managing Additional Configurations

Configuring the Client Logo Image

The client logo has a default blank image included in all Mantas JSPs. You need to replace the blank image for both your Oracle Financial Services product and the Administration Tools with a `.gif` file that contains your firm's name and logo.

Logo Specification

The following lists the client logo specification:

- The logo name should be `client_logo.gif`

- Dimensions: Height: 40 pixels; Width: Constrain Proportions

- File format: GIF

Placing a new Client Logo

To place a new client logo, follow these steps:

1. Make a backup of existing `client_logo.gif` from the location: `<AAI deployed area>/images` (for example, `/OFSAAI/images/`).

2. Place the customer logo from location: `<AAI deployed area>/images` (for example, `/OFSAAI/images/`).

3. After placing the image in the web server, refresh the IE browser.

4. Refresh the Appserver's work folder.

Removing a Client Logo

To remove a custom client logo, follow these steps:

1. Replace `client_logo.gif` from the backup location.

2. After placing the image in the web server, refresh the IE browser.

3. Refresh the Appserver's work folder.

Accessing Manage Parameters

To access the Manage Parameters, follow these steps:

1. Navigate to Administration tab and select Manage Parameters option.

2. Select Manage Common Parameters to access the Manage Common Parameters window.

Configuring the Default Currency Code

You can modify the default currency settings that display throughout the UI. The following section provides detailed instructions to modify the currency code, which is highlighted in below figure.

To modify the default currency code, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Base Currency** from the Parameter Name drop-down list.

4. Edit the parameter. Figure 55 illustrates the modified currency code as EUR.
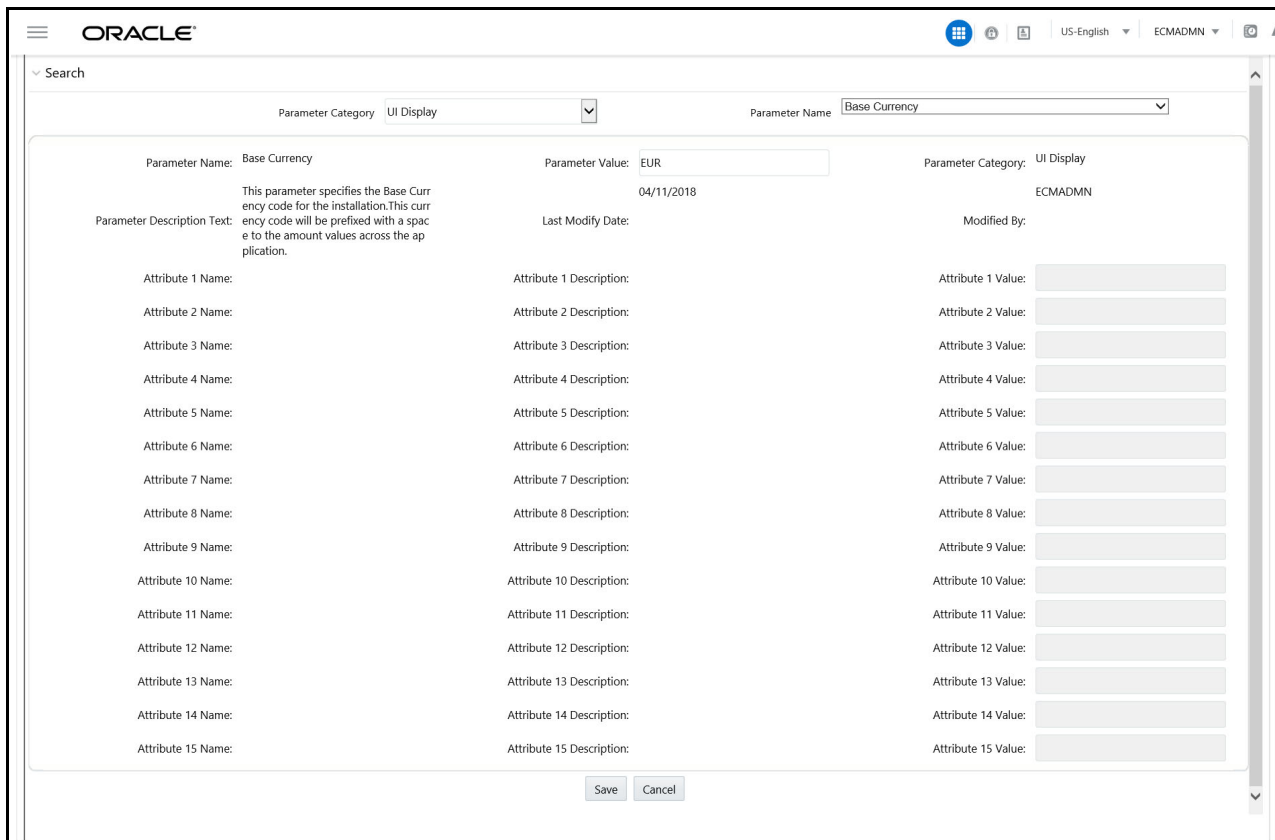
Figure 55. Financials Tab—with Modified Currency Format

To modify the default currency code, from the back end, follow these steps:

1. Locate the CFG_Env.xml file in the following directory:

   <MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config

2. Save a copy of the original CFG_Env.xml file in the custom directory that contains backup files:

   <MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config/custom/backup

3. Open the original CFG_Env.xml in an editor.

4. Locate the default currency code that you want to modify, that is similar to the following:

   ```
   <I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCur-
   rency="USD" pdfFont="ArialUnicodeMS"/>
   ```

5. Modify the currency code.

In the following example, the modified currency code is EUR (Euro):

```
<I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCur-
rency="EUR" pdfFont="ArialUnicodeMS"/>
```

6. Save the file to the original directory and exit the editor.

Note: The currency for highlights is configured in the `<OFSECM Installed Directory>/database/dbtools/mantas_cfg` directory where you run the `run_highlights.ksh` script.

Configuring the Base Time Zone

The Base Time Zone parameter is used in the Export to XML action from Case Management. You can modify the default Base Time Zone through the Manage Common Parameters screen (Figure 41).

Modifying Time Zone

To modify the base time zone, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Base Time Zone** from the Parameter Name drop-down list.
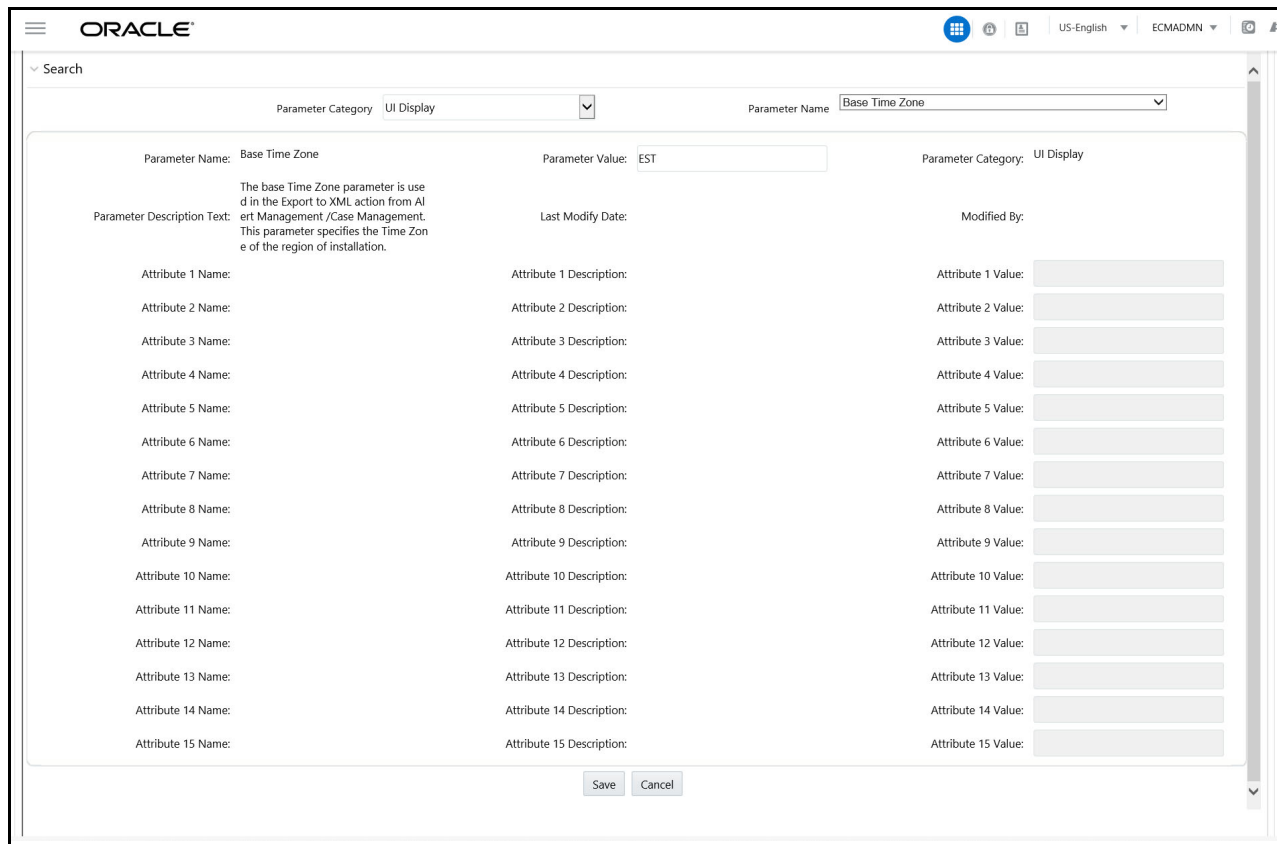
Figure 56. Configuring Base Time Zone

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

7.

Modifying Case Highlight Status

This parameter specifies the list of Case statuses to be highlighted in **bold** font when displayed in the UI. Making bold font for certain statuses ensures that alerts cases with the corresponding statuses are more easily identified when in a list with other cases.

To modify the case highlight status, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Case Highlight Status** from the Parameter Name drop-down list.

Figure 57. Configuring Base Time Zone

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring a Visual Cue for Cases Nearing Due Date

You can configure a time period for cases that signals when they are approaching their due date. When the specified time period is reached or passed, the due date column (Due) displays the dates in highlighted red.

To configure a time period that signals when a case is approaching its due date, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Case Near Due Date** from the Parameter Name drop-down list.s

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 32. Configuring a Visual Cue for Cases Nearing Due Date

Attribute	Description
CM_Near	This attribute specifies the number of days to be considered before the due date of a case in order to color code the case as a near due case in the UI.

Configuring Case Own Flag Consideration

This parameter specifies if a user should be checked for their case owning eligibility before they are assigned the case. The parameter should have only Y or N values. If the value is set to Y, then only those users who have access privileges to the case and are also eligible to own a case are displayed in the Assign To fields. If set to N, then all users who have access privileges to the case, regardless of their eligibility to own a case, are displayed in the Assigned to fields.

Note: The default value is Y.

To disable the Case Own Flag Consideration, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Case Own Flag Consideration** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Prefix

This parameter specifies the non numeric value to be prefixed before the Case ID while displaying the Case ID in the UI.

To modify the Case Prefix parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **UI display** from the Parameter category drop-down list.

3. Select **Case Prefix** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring the Display of Value in By Field Name/ID

This configuration allows you to see either the ID or Name field for the User, Focus, Branch, Division and Organization in the UI. This parameter specifies the client to specify the Name or ID value in the By field.

To modify the Display of Value in the By Field Name/ID, follow these steps:

1. Navigate to **Applications** and click **Manage Configuration**.

2. Open the Manage Common Parameters screen.

3. Select **UI Display** from the Parameter Category drop-down list.

4. Select **Display of Value in By Field Name/ID** from the Parameter Name drop-down list.

5. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

6. Click **OK**. A confirmation dialog box appears with the message: *Update Operation Successful.*

7. Click **OK**. The Manage Common Parameters page is displayed.

Table 5 describes the attributes which should be configured for Display of Value in By Field Name/ID.

Table 33. Configuring Display of Value in By Field Name/ID Attributes

Attribute	Description
User	ID or Name for User field.
Focus	ID or Name for Focus field.
Branch	ID or Name for Branch field.
Division	ID or Name for Division field.
Org	ID or Name for Org field.

Configuring Organization Type

This parameter specifies the type of organization that is used to populate the list of available cost centers wherever cost center appears as a selection or data entry criteria throughout the application. Records in the Organization table with this specified Organization Type (ORG.ORG_TYPE_CD) is displayed in the cost center drop-downs. The parameter value is limited to specifying only one organization type.

To modify the Organization Type, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Organization Type** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring the Default Due Date Calculation

This parameter allows the client to specify the use of Business days versus Calendar days. Here you can specify **C** for Calendar days and **B** for Business days.

Note: The default value is Calendar days (C).

To modify the Default Due Date Calculation, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Default Due Date Calculation** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Administration Tools

This parameter specifies the web application context and URL of the admin tools application.

Follow these steps in Case admin tools deployed web application context and URL were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Admin Tool** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

32 describes the attributes which should be configured for enabling and using the administration tools.

Table 34. Configuring Administration Tools

Attribute	Description
APPLICATION_CONTEXT	This parameter specifies the context name of admin tools application.
ADMINISTRATION_TOOLS_APPLICATION_URL	This parameter specified the URL of admin tools application.

Configuring Application Server

This parameter specifies the OFSAAI Application Server IP Address and Java Port.

Follow these steps if in case the values were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Application Server** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 35 describes the attributes to be configured for setting the application server.

Table 35. Configuring Application Server

Attribute	Description
Application Server IP	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server IP address/server name details required for admin tools.
Application Server Port	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server port details required for admin tools.

Configuring Case Age Calculation

This parameter allows the client to specify whether the calculation of the age of a case is to be done in Calendar or Business days. The param value can be either C or B.

Note: The default value is Business (B).

To modify the Case Age Calculation parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Case Age Calculation** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Assignment Inheritance

This parameter specifies the status of Case Assignment Inheritance for the installation. The parameter can have only Y or N values. If set to Y and if the current Assign To user of the case is a pool (not an individual user), then the current user inherits as the Assign To user of the case. If set to N, then the Assign To user is not changed just by a user viewing the case.

Note: The default value is Y.

To modify the Case Assignment Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Case Assignment Inheritance** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Correlation Owner

This parameter specifies the users or user pools who should be assigned as the *Owner* and *Assign To* users for cases created through correlation promotion. The users or user pools that need to be assigned as the *Owner* and *Assign To* users are identified from other attributes of this parameter based on the case type. Here every attribute specifies an owner for a Case Type Sub Type. Some of the Case Type Sub Type will be prepackaged.

Client can specify new case type sub type and default owner for the case type subtype. To add new case type sub type, follow these steps:

1. If the Case Correlation Owner parameter has used up to attribute 4, then use the following query:

   ```
   update kdd_install_param set kdd_install_param.attr_5_cd='<Case Type Sub Type>'
   ,kdd_install_param.attr_5_value_tx='<Owner>'
   ```

   ```
   where kdd_install_param.param_id=30 and kdd_install_param.param_nm='Case Correlation
   Owner 1'
   ```

2. If all the attributes have been filled then add one more case correlation owner Parameter. To add another Correlation parameter, follow these steps:

   a. Get maximum param ID of `kdd_install_param` table by running the following query.
      ```
      select max (param_id) from kdd_install_param.
      ```

   b. Insert into `kdd_install_param (param_id, param_nm, param_value_tx,` `param_cat_cd,param_desc_tx`) values

      ```
      (< Max Param id > +1,'Case Correlation Owner 2','Y','Used for Design',
      ```

      This parameter specifies the users or user pools who should be assigned as the *Owner* and *Assign To* users for cases created through correlation promotion. The parameter value by default is kept as Y but can also be changed and the same is not validated. The users or user pools who need to be assigned as the Owner and Assign To users are identified from other attributes of this parameter based on the case type.

   c. To add new case type sub type and owner use the query mentioned in step 1 after replacing the filter clause with the new param ID and name.

To modify the Case Correlation Owner for an existing Case Type Sub Type, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Case Correlation Owner** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 36. Configuring Case Correlation Owner

Attribute	Description
DEF_OWNER	This attribute specifies the default Case owner. **Note:** The attribute value can have only one user ID ● Should be the same as of 　　KDD_REVIEW_OWNER.OWNER_ID ● Should have Case role and ● Have access to all the security attributes defined in the Security Attribute Administration User Interface, if not the alerts would not be assigned to any user.

Configuring Case Inheritance

This parameter specifies the status of Case Inheritance for the installation. The parameter can have only Y or N values.

If set to Y, the case ownership changes for cases when in New or Reopened statuses based on the rules defined for case inheritance. If set to N, then ownership does not change when a user accesses the case.

If set to Y the system automatically assigns ownership of a case owned by pools (as long as not in a closed status) to the user who has selected to view the case. If set to N, case ownership is not inherited by a user just by viewing the case.

To modify the Case Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Case Inheritance** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Case Risk Values

This parameter allows deployment level configuration of the minimum and maximum range of risk values during add and edit feature in Case related business tabs.

To modify the Case Age Calculation parameter, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Case Risk Values** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 37. Configuring Case Risk Values

Attribute	Description
Min Risk Value	Will define the minimum value of all the types of risks; will have a default value of -2.
Max Risk Value	Will define the maximum value of all the types of risks; will have a default value of 10.

Configuring Default Case Owner

This parameter allows the client to specify the default user or user pool to which cases created through promotion of an alert or manual creation will be assigned to. This allows for specification of default *Owner* and *Assign To* users. Some of the Case Type Sub Type will be prepackaged.

Client can specify a new case type sub type and default owner for the case type subtype. To add new case type sub type, follow these steps:

1. If the Default Case Owner parameter has used up to attribute 4 then use following query:

   ```
   update kdd_install_param set kdd_install_param.attr_5_cd='<Case Type Sub Type>'
   ,kdd_install_param.attr_5_value_tx='<Owner>'
   ```
   ```
   where kdd_install_param.param_id=33 and kdd_install_param.param_nm= 'Default Case Owner
   1'
   ```

2. If all the attributes have been filled then add one more case correlation owner Parameter. To add another Correlation parameter, follow these steps:

   a. Get the maximum param ID of `kdd_install_param` table by running the following query:

      select max(`param_id`) from `kdd_install_param`

   b. Insert into kdd_install_param (`param_id, param_nm, param_value_tx, param_cat_cd, param_desc_tx`) values

      `(< Max Param id > +1, ' Default Case Owner 2','Y', 'Used for Design',`

      This attribute specifies the default user or user pool who should be assigned as the Owner and Assigned To user for correlated cases for case types that are not mentioned in other attributes of this parameter).

   c. To add new case type sub type and owner, use the query mentioned in step 1 after replacing the filter clause with the new param ID and name.

To modify the Default Case Owner for existing Case Type Sub Type, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Default Case Owner** from the Parameter Name drop-down list.

   Note: If you are configuring for the first time after installation, populate the owner field for all case types and subtypes displayed in the configuration screen.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 38. Configuring Case Owner

Attribute	Description
DEF_OWNER	This attribute specifies the default Case owner. **Note:** The attribute value can have only one user id • Should be the same as of KDD_REVIEW_OWNER.OWNER_ID • Should have Case role and • Have access to all the security attributes defined in the Security Attribute Administration User Interface, if not the alerts would not be assigned to any user.

Configuring E-mail

This parameter specifies the attributes for the E-mail action. The value of this parameter should be set to Y.

To modify E-mail parameters, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **E-Mail** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 39 describes the attributes which need to be configured for E-mail parameters.

Table 39. Configuring E-mail Attributes

Attribute	Description
DEF_SEND_USR	This attribute specifies whether the system should use a pre-defined E-mail address or the E-mail address of the current logged in user as the default sender address. The parameter value can have only Y or N value. Y sets the E-mail of the sender as the User ID specified in DEF_SEND_USR_ID attribute as the default. N sets the E-mail of the current logged in user as the default.
DEF_SEND_USR_ID	This attribute specifies the default user ID for the E-mail action. This parameter must have a value when the DEF_SEND_USR is set to Y. **Note:** The attribute value should reference a user in the KDD_REVIEW_OWNER table.
DEF_DOM_ENABLED	This attribute enables/disables the set of domains where E-mails can be sent. The parameter value can have only Y or N value. Y restricts the user from sending E-mails to the domains specified in the DEF_DOM attribute. When it is set to N, the UI presents the user with a selection box from which the E-mail IDs of the users identified in TO_LST_USR_ID attribute can be selected.
DEF_DOM	This attribute specifies the domains to which the E-mails can be sent. This attribute should be populated only when the DEF_DOM_ENABLED attribute is set to Y.
TO_LST_USR_ID	This attribute specifies the users to whom the E-mails can be sent. This attribute should be populated only when the DEF_DOM_ENABLED attribute is set to N. **Note:** The attribute values) should reference users in the KDD_REVIEW_OWNER table.
MAIL_HOST	This attribute specifies Mail SMTP host IP address/Server name. If this attribute is not populated, E-mail actions cannot be performed.
DEF_SUBJECT	This attribute specifies the default subject text that appears on E-mails when an E-mail action is taken for cases.
MAIL_FOOTER	This attribute specifies optional footer details which can be appended to the E-mail.
MAIL_ATTACH_LIMIT	This attribute specifies the attachment size limit. The value is given in MB.
DISPLAY_ACTIONS_TAKEN	This attribute specifies whether to display the 'Actions Taken' in the attached HTML or not.
HTML_REPORT_IN_BODY	This attribute specifies for a single case, whether the HTML report should come in mail body or as attachment.
DEF_ACTION_TAKER	This attribute specifies the default action taker for the received response if the system cannot identify the Response Sender as a valid User.

Configuring Mode of Transferring Alert Information

This parameter specifies the mode in which business data from an alert to a case is transferred during Promote to Case or Link actions. The parameter value can have only S or A value. Synchronous (S) restricts the user from working on the alert or case until the data transfer action is complete. Asynchronous (A) allows the user to continue to work on the alert or case, while the data transfer is being carried out in the background.

Note: The default value is synchronous (S).

To modify the Mode of Transferring Alert Information, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for design** from the Parameter Category drop-down list.

3. Select **Mode of Transferring Alert Information** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Mode of Transferring Case Information

This parameter specifies the mode in which case information is transferred during Merge Action and is applicable for implementations which have installed Oracle Financial Services Enterprise Case Management. The parameter value can have only S or A value. S (Synchronous) restricts the user from working on the alert or case until the data transfer action is complete. A (Asynchronous) allows the user to continue to work on the alert or case, while the data transfer is being carried out in the background.

Note: The default value is synchronous (S).

To modify the Mode of Transferring Case Information, follow these steps:

1. Open the Manage Common Parameters screen (Figure 1).

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Mode of Transferring Case Information** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message: *Would you like to Save these actions?*

5. Click **OK**. A dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring Lock Time Period for Case Actions

Cases are locked when you are taking actions on them, however, the lock is opened when you complete the action. If you close the browser window while the lock is still active, then the lock remains active until it expires. This prevents other users from acting on the locked case.

By default, the system retains the lock for 30 minutes. This parameter applies for Case Management implementations. If you want to change the time period for this lock, then follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **UI Lockout Time** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

   Note: UI Lock Out Time should be mentioned in minutes. That is, `param_value_tx` value should be in minutes.

Configuring View All Organization

This parameter, along with other access permissions defined for the user, determines the cases that can be viewed by a user in the Related Cases matrices of the Relationship tab for Case Management implementations. The parameter value can have only Y or N value. Y enables the current user to view cases as related events and- related cases respectively, even if the user does not have viewing rights for the case's primary organization, which is defined based on the organization associated with the owning user. N restricts the user from viewing, as related, events or cases whose primary organizations the user does not have access to view.

For example, User Joe Smith may be not be allowed to see the details of cases owned by users (or a pool) who have Employee Compliance as their primary organization. However, if this parameter is set to Y, Joe Smith would be able to see cases associated with the organization of Employee Compliance in a list of related cases, as long as they have a relationship to the current case being viewed. If this parameter is set to N, Joe Smith would have no ability to see the above mentioned cases, even as related.

To disable View All Organization, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **View All Organization** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring OBIEE

This parameter specifies the OBIEE Server Application context and URL parameters.

To configure OBIEE, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **OBIEE** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring File Size

By default the size supported by attachment is 1 MB. If you want to attach files greater than 1 MB size using the Save and Attach button, follow these steps:

1. Open file `$FIC_HOME/EXEWebService/<WebSphere or Weblogic or Tomcat>/ROOT/conf/DynamicWSConfig.xml`

2. Update from:

   `<PROPERTY NAME="MAXFILESIZE" VALUE="1024000"/>`

   to:

   `<PROPERTY NAME="MAXFILESIZE" VALUE="<desired value in bytes up to 10MB>"/>`

3. Recreate the `ExeWebservices ear` file and redeploy it.

4. Restart the web application server.

The size that is allowed to be attached while performing document attachment action should be configured in Configuration table of OFSSAAI configuration schema in its `PARAMVALUE` column where `PARAMNAME` is `DOCUMENT_MAX_SIZE`.

Configuring Views

Views help you to quickly view search results based on pre-defined search queries.

Adding Views

To add views, follow these steps:

1. Make entry in the KDD_QUEUE_MASTER table.

Table 40. KDD_QUEUE_MASTER table

QUEUE_SEQ_ID	QUEUE_CD	QUEUE_DISPLAY_NM	QUEUE_TYPE
Unique sequence ID	Unique Queue Code	The name of the view that will be displayed in the UI	**ECM** : If the view is related to Cases

2. Make the entries in the KDD_QUEUE_FILTER table for each filter for respective view.

QUEUE_SEQ_ID	ATTRBT_ID	ATTRBT_VAL_TX
Unique sequence ID	Unique Attribute ID. ATTRBT_ID will be referred from KDD_CASEATT RBT_MASTER	This Attribute value is the actual value used for the attribute of filter. In this, you can give hardcoded values (for example, put a filter condition on status attribute for the cases which are in New status). The possible value for this is NW. You can also specify session attributes for your filter. The session attributes are enclosed in curly brackets {}. For example: {userSeqId}, {userPool} You can define SYSDATE value for filter. Date filter requires following two inputs: ● From Date ● To Date For example: #NS#, #SYSDATE# You should specify the date values in enclosed # Use #NS# to mention the date filter as blank.

3. Map Queue in the KDD_QUEUE_ROLE_MAP table.

Table 41. KDD_QUEUE_ROLE_MAP table

QUEUE_SEQ_ID	ROLE_CD
Queue sequence id as given in the above table	Role code

Modifying Views

Following are the various modifications for views:

1. **Modify An Existing View Query**

In order to modify the underlying filters for a view, changes are to be done in the `KDD_QUEUE_FILTER` table column.

2. **Modifying View-Role Mapping**

   In order to make a view available for an existing role, the mapping has to be done in `KDD_QUEUE_ROLE_MAP` table.

3. **Modifying the Display Name of the View**

   In order to change the display name for a particular view, changes have to be done in `KDD_QUEUE_MAS-TER.QUEUE_DISPLAY_NM` column.

Removing Views

To remove a view, entries for that view must be deleted from the `KDD_QUEUE_MASTER`, `KDD_QUEUE_FILTER` and `KDD_QUEUE_ROLE_MAP` tables

```
Delete KDD_QUEUE_MASTER where QUEUE_SEQ_ID = <View Sequence Id>; Delete KDD_QUEUE_ROLE_MAP
 where QUEUE_SEQ_ID = <View Sequence Id>; COMMIT;


Delete KDD_QUEUE_FILTER where QUEUE_SEQ_ID = <View Sequence Id>; Delete KDD_QUEUE_ROLE_MAP
 where QUEUE_SEQ_ID = <View Sequence Id>; COMMIT;
```

Configuring ECM Security Function

To configure the ECM Security Function, follow these steps:

1. Open the Manage Common Parameters screen.

2. Select **Used For Design** from the Parameter Category drop-down list.

3. Select **ECM Security Function** from the Parameter Name drop-down list.
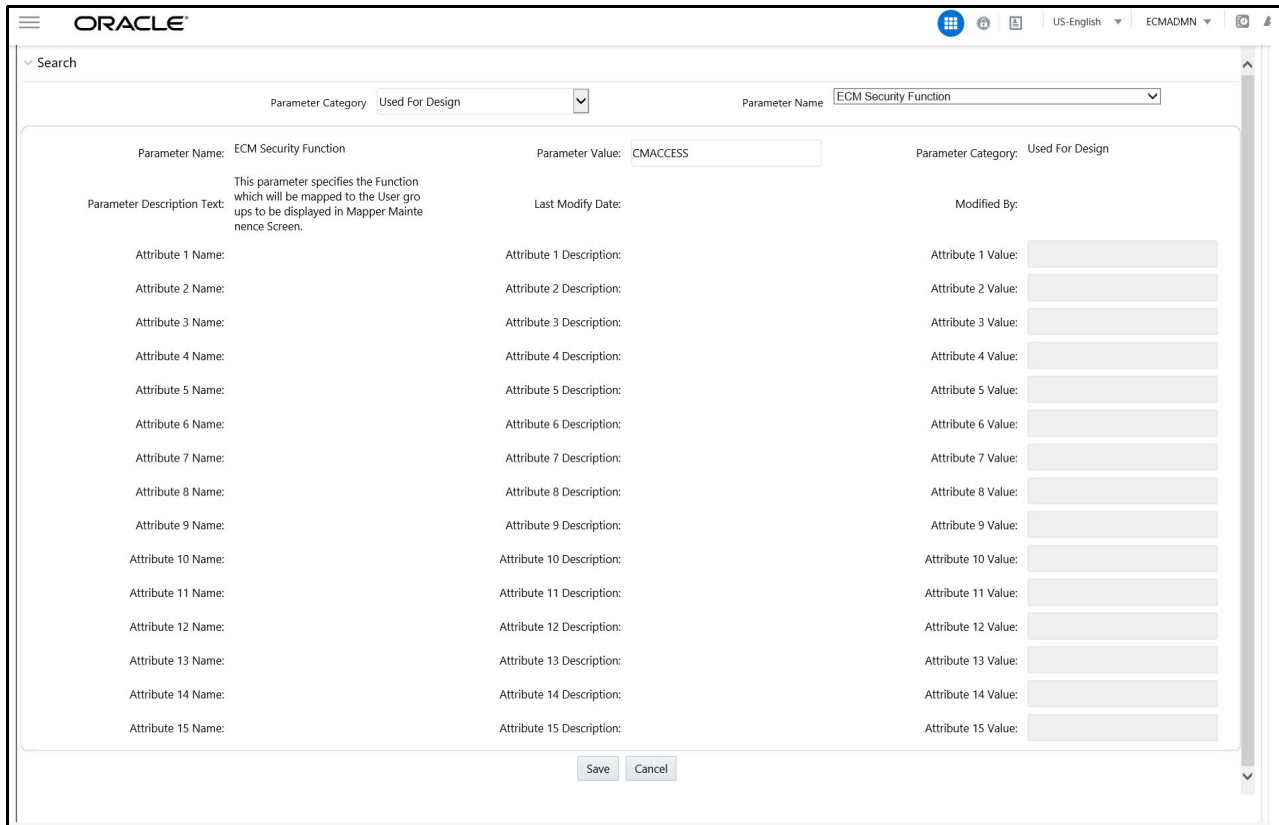
Figure 58. Configuring ECM Security Function

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Managing Additional Configurations

The section describes the additional configurations that need to be carried out by the system administrator.

This section covers the following topics:

- Configuring File Type Extensions

Configuring File Type Extensions

The list of file type extensions that are allowed to be attached while performing document attachment action should be configured as comma separated values in the CONFIGURATION table of the OFSSAAI configuration schema in its PARAMVALUE column where PARAMNAME is DOCUMENT_ALLOWED_EXTENSION.

CHAPTER 13   *Configuring Administration Tools*

This chapter provides instructions for configuring parameters specific to administration tools.

This chapter covers the following topics:

- Configuring Administration Tools
- Configuring Application Server

Configuring Administration Tools

This parameter specifies the web application context and URL of the admin tools application.

Follow these steps incase admin tools deployed web application context and URL were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Admin Tool** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 42 describes the attributes which should be configured for enabling and using the administration tools.

Table 42. Configuring Administration Tools

Attribute	Description
APPLICATION_CONTEXT	This parameter specifies the context name of admin tools application.
ADMINISTRATION_TOOLS_APPLICATION_ URL	This parameter specified the URL of admin tools application.

Configuring Application Server

This parameter specifies the OFSAAI Application Server IP Address and Java Port.

Follow these steps if in case the values were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen.

2. Select **Used for Design** from the Parameter Category drop-down list.

3. Select **Application Server** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*

5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful.*

6. Click **OK**. The Manage Common Parameters page is displayed.

Table 43 describes the attributes to be configured for setting the application server.

Table 43. Configuring Application Server

Attribute	Description
Application Server IP	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server IP address/server name details required for admin tools.
Application Server Port	This parameter specifies Oracle Financial Services Analytical Applications Infrastructure Application server port details required for admin tools.

Managing Case Assigner Editor

This chapter describes how you can assign ownership of cases, and covers the following topics:

- About Case Assigner Editor
- Case Assigner Screen Elements
- Using Case Assigner Editor

About Case Assigner Editor

The Case Assigner Editor allows the application Administrator to view and modify the rules used to assign ownership of cases. The Case Assigner Editor allows you to perform the following tasks:

- Create, modify, or delete a rule
- Define Role-Based Assignment Limits

Each case generated within the application is assigned an initial owner before it is available for analysis. The application automatically determines an appropriate owner (a user or group of users) for each case based on the initial assignment logic you configured or configured for your firm. Initial assignment logic is composed in a set of operations that evaluate various attributes of the case. For example, scenario, score, or related entities. Case assignment rules apply only to those cases created automatically as a result of promotion of a event Correlation to a case. They do not impact cases created directly by a user.

You can add, modify, or delete assignment rules. The following elements are combined to form a set of logic against which the cases are evaluated:

- Each assignment rule is defined as an attribute of a case, an operator, and a value.

Table 44 shows a sample of a case assignment rule.

Table 44. Sample of a Case Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
1	Case Type	- Cases with case type AML Surveillance are assigned to the AML Compliance Pool. - Cases with case type Fraud - Online Fraud are assigned to the FR Risk Pool.

Table 44. Sample of a Case Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
2	Case Type and Jurisdiction	● Cases with case type AML Surveillance AND with a Jurisdiction of High Wealth Customer are assigned to the AML Compliance - Wealth Management Pool. ● Cases with case type AML Surveillance AND with Jurisdiction of Eastern Region Retail are assigned to the AML Compliance - Eastern Region Pool.
3	Default	● All cases that do not meet other rules are assigned to the AML & Fraud Risk Management pool.

● Each assignment rule consists of an operation set that identifies a grouping of rules of which it is a member.

● Operations are logical expressions that can be used to evaluate cases (for example, score > 50). A set of operations based on the same attribute (for example, score) are grouped into an operation set.

● All operations within an operation set must be mutually exclusive and should collectively cover the entire spectrum of values for a given attribute.

● Each operation specifies the next step that is applied to cases that satisfy the operation. This next step is either an owner for the case, or the next operation set, or branch, to further evaluate the cases.

● Each case is evaluated against the operations within operation set one (1). Each case then branches out based upon the next operation set specified for the operation within Operation Set one (1) that they satisfy. Each case continues through a chain of operation sets until it satisfies an operation for which an owner has been specified. Cases that do not reach an operation that they satisfy and for which an owner has been specified, are assigned to the Default Owner that has been specified through initial configuration using installation parameters.

Note: Manually posted cases, generated by the event correlation process, are not assigned to the default owner that is specified through the assignment editor.

Accessing Case Assigner Editor

To access Case Assigner Editor, follow these steps:

1. Navigate to the Administration menu and select **Case Management Configuration**.

2. Select the **Case Assigner Editor** option. The Case Assigner Editor page is displayed.

Case Assigner Screen Elements

The following pages are associated with the Case Assigner Editor:

● **Case Assigner Editor:** This is the first page displayed when accessing the Case Assigner Editor. You can delete a rule from this page or navigate to the Assignment Rule Editor to add a new rule or modify an existing rule. See the *Case Assigner Editor* for more information.

● **Assignment Rule List for Cases:** This page enables you to create a new rule or modify an existing rule. See the *Assignment Rule List for Cases* for more information.

- **Role Based Assignment Rule Editor:** This page allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. See the *Assignment Rule Editor* for more information.

Case Assigner Editor

The Case Assigner Editor displays the assignment rules associated to cases.
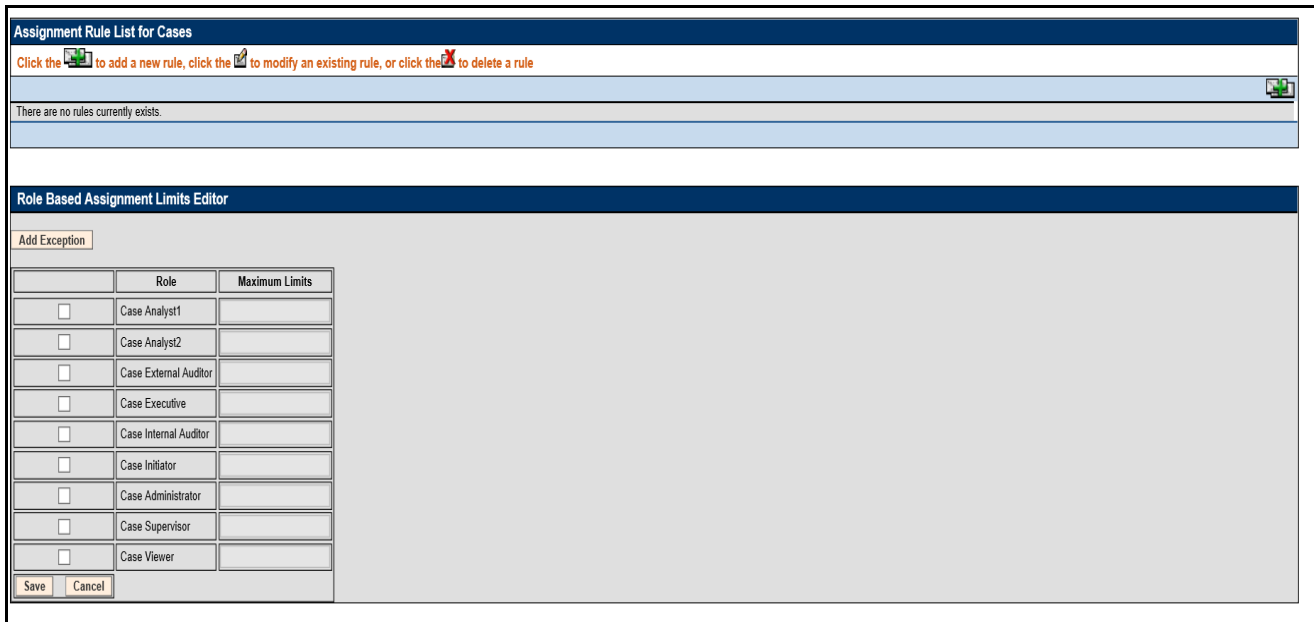
Figure 59. Case Assigner Editor

The components of the Case Assigner Editor include the following:

- Assignment Rule List for Cases
- Role Based Assignment Limits Editor

Assignment Rule List for Cases

The assignment rule list displays in the Case Assigner Editor. The rules in the list are sorted in ascending order by operation set number (*Figure 60*).
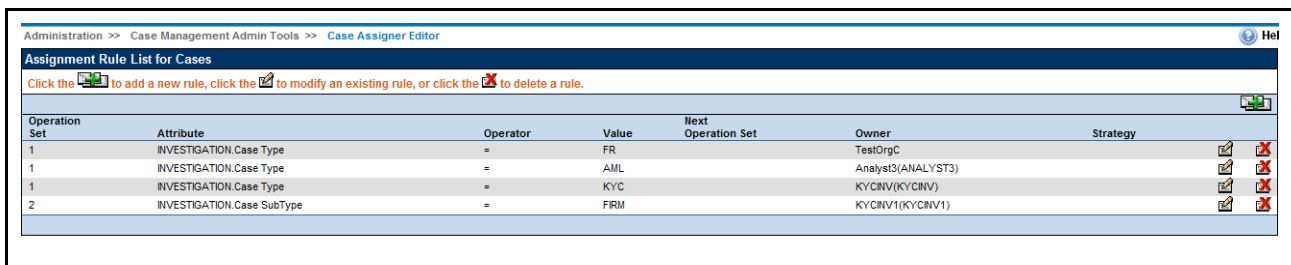
Figure 60. Assignment Rule List for Cases

The Assignment Rule List for Cases includes the following components:

- **Add button**: Navigates you to the Assignment Rule Editor.

- **Update button**: Navigates you to the Assignment Rule Editor.

- **Delete button**: Deletes the assignment rule.

- **Assignment Rule List for Cases** page displays the column headings: Operation Set, Attribute, Operator, Value, Next Operation Set, and Owner. See *Assignment Rule Editor* for more information.

Role Based Assignment Limits Editor

The Role Based Assignment Limits Editor allows you to limit the number of cases that can be assigned to members of a pool based on user role. For example, if a member pool contains 25 investigators, you can limit junior investigators to have a maximum of 10 cases assigned to them, and assign a senior investigator no cap.

Cases are assigned based on the available assignment rules until members reach their caps, then cases are assigned only to members who have not reached their caps. If all members have reached their limit, cases are assigned to the pool, and can be accessed by using the Auto-Assignment option.

Figure 61. Role Based Assignment Limits Editor

The Role Based Assignment Limits Editor includes the following components:

- **User Role grid**: When a user role is selected, you can edit the maximum limit. A *Null* value indicates there is no limit for the assignment of cases.

- **Add Exception button**: Allows you to enter exceptions to the limit assigned to the user role. See *Adding an Exception to a Role Based Assignment Limit* for more information.

- **Save button**: Saves all modifications to the database.

- **Cancel button**: Redisplays the Assignment Editor. The New Maximum Limits value is not saved.

Assignment Rule Editor

The Assignment Rule Editor displays after you click **Add** or **Update** (*Figure 62*). This editor allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. The decision trees are used to determine the owner (an individual or group of users) of each case generated by the system.

Figure 62. Assignment Rule Editor

The components of the Assignment Rule Editor include the following:

- **Operation Set**: Specifies a grouping of mutually exclusive rules based on an attribute.

  - If you select **Add**, the **Operation Set** text box displays as blank.

  - If you select **Update**, the **Operation Set** text box field is populated with the current data for the selected rule.

  - You must create rules within Operation Set 1 before creating any additional rules. Any condition not covered by Operation Set 1 is assigned to the default assignment owner, as are all other operation sets when cases are added to them.

- **Investigation Attribute**: Populates alphabetically with values for each attribute of the case. For example, Jurisdiction, Business Domain, Case Type, Linked Events, Linked Cases, and Priority, off which to base the rule.

  - If you select **Add**, the **Investigation Attribute** drop-down list displays a blank value (" ") (the default).

  - If you select **Update**, the **Investigation Attribute** drop-down list displays the current value of the selected rule.

- **Operator** drop-down list: Contains the following values =, !=, >, <, <=, >=, in, contains, blanks (" "), and else.

  - If you select **Add**, the **Operator** drop-down list displays a blank value (" ") (the default).

  - If you select **Update**, the **Operator** drop-down list displays the current value of the selected rule.

  - If you base your rule on an investigation attribute for which an enumerated list of values has been defined, only the values = and != are available in the **Operator** drop-down list.

  - If you have a list of values and you want to check if the database field is one of the values in the list, select the *in* operator in the **Operator** drop-down list.

  - If you want to check a database field that contains a comma-delimited list of values for a specific value, select the **contains** operator in the **Operator** drop-down list.

Note: The selection between the *in* and *contains* operators depends on the type of search you want to perform. Using the *contains* operator allows you to check if a database field containing a comma-delimited list of values contains a specific value. For example, checking if the Business Domain contains a particular business domain. The *contains* operator is similar to the *in* operator, but it reverses the comparison. With the *in* operator, the single value is in the field in the database, and a list of values is provided as the argument. With the *contains* operator, the list is in the database, and the single value is provided as an argument.

- ■ If you select the *else* operator, the *value* must be NULL; followed by a subsequent operation or case owner recipient specification. The system evaluates the *else* operation after evaluating all other operations.

- ● **Value** text box or drop-down: Within the rule, the value of the investigation is compared to the **Value** field. If you have selected an attribute in the **Investigation Attribute** drop-down list with defined values (Jurisdiction, Business Domain, Case Type, Linked Events, Linked Cases, and Priority), the **Value** drop-down list will contains those values. The **Value** field displays as a text box for all other attributes (for example, score or account balance).

    - ■ If you select **Add** , the **Value** text box displays a blank value (" ").

    - ■ If you select **Update**, the **Value** text box displays the current value of the selected rule.

    - ■ If you enter multiple values in the **Value** text box after having selected *IN* as the operator, separate the values with pipe (|).

    - ■ If you select the *else* operator, the **Value** must be NULL therefore, the system disables the Value text box or drop-down list.

- ● **Next Operation Set** text box: The number of the next operation set, or branch, to further evaluate the case or assign to an owner.

    - ■ If you select **Add**, the **Next Operation Set** text box displays a blank value (" ") (the default).

    - ■ If you select **Update**, the **Next Operation Set** text box displays the current value of the selected rule.

    - ■ If the result of your rule is to continue to the next operation set, you must not select an owner to assign the or case.

- ● **Owner** drop-down list: Displays available owners for both cases.

    - ■ If you select **Add**, the **Owner** drop-down list displays a blank value (" ") (the default).

    - ■ If you select **Update**, the **Owner** drop-down list displays the current value of the selected rule.

    - ■ If the result of your rule is to assign case, you must not select to continue to the next operation set.

- ● **Strategy** drop-down list (*Optional:*): Displays available strategies for the assignment rule. This drop-down list is disabled unless an owner is selected and that owner is a pool and not an individual user.

    - ■ If you select **Round Robin**, cases are assigned to the members of a pool in a circular order until all the cases have been assigned.

    - ■ If you select **Load Leveling**, the pool member's current load is taken into consideration when assigning cases.

    - ■ If a strategy is selected and then an individual user is selected in the **Owner** drop-down list, then the value in the Strategy drop-down list is made blank.

Using Case Assigner Editor

This section explains the following functions of the Assignment Editor:

- Adding a New Rule

- Modifying a Rule

- Deleting a Rule

- Adding a Role Based Assignment Limit

- Adding an Exception to a Role Based Assignment Limit

Adding a New Rule

To add a new rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Click **Add**. The Assignment Rule Editor displays.

2. Type an operation set number in the **Operation Set** text box.

   You can add to an existing operation set based on the same attribute by entering the same number as the other rules in that set or you can start a new set by entering the next sequential number.

3. Select either an investigation attribute on which to base the rule in the **Investigation Attribute** drop-down list.

   This attribute must be the same for any other rules within the same operation set.

4. Select an operator in the **Operator** drop-down list. If you select the *else* operation, skip to Step #6 since no value is required for this operand.

5. Type a value in the **Value** text box.

   Depending on the attribute, this value can be a numeric or a text string.

6. Select either the next operation set to attach additional rules to this rule in the **Next Operation Set** text box, or select an owner to assign cases to in the **Owner** drop-down list.

    Note: Ensure that the new owner has permission to view cases with the attributes specified in the rule.

7. If you selected a pool in the **Owner** drop-down list, select a strategy for case assignment from the **Strategy** drop-down list.

8. Click **Save**.

   The system creates the new rule and redisplays the Case Assigner Editor with the new rule.

Modifying a Rule

To modify the rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Click **Update** for the desired rule.

   The Assignment Rule Editor displays.

2. Do one or more of the following:

   - Modify the operation set number in the **Operation Set** text box.

   - Modify the investigation attribute on which to base the rule from the **Investigation Attribute** drop-down list.

   This attribute must be the same for any other rules within the same operation set.

   - Modify the operator in the **Operator** drop-down list.

   - Modify the value in the **Value** text box.

   Depending on the attribute, this value can be a numeric or a text string.

   - Modify the next operation set to attach additional rules to this rule in the **Next Operation Set** text box, or select an owner to assign cases to in the **Owner** drop-down list.

   - Modify the strategy selected to assign cases to the pool in the **Strategy** drop-down list.

3. Click **Save**.

   The system updates the rule and redisplays the Case Assigner Editor with the rule's updates.

Deleting a Rule

To delete an existing Assignment Rule for a case from the Assignment Rule Editor, follow these steps:

1. Click **Delete** for the associated rule.

   The Confirmation dialog box displays the message: *Are you sure you want to delete the selected Assignment Rule?*

2. Click **OK** to delete the rule.

   The system removes the rule and redisplays the Case Assigner Editor.

Adding a Role Based Assignment Limit

To add an assignment limit for a user role, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Enter the Maximum Limit for this user role.

3. Click **Save**.

   The Confirmation dialog box displays the message: *Are you sure you want to modify the limits of this user role?*

4. Click **OK** to set the assignment limit.

   The system sets the limit and redisplays the Case Assigner Editor.

Adding an Exception to a Role Based Assignment Limit

To add an exception for a use role based assignment limit, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Click **Add Exception**.

3. Select the user you want to add the exception for from the dropdown list.

4. Enter the Maximum Limit.

5. Click **Save**.

   The Confirmation dialog box displays the message: *Are you sure you want to add the user with the mentioned limits?*

6. Click **OK** to set the assignment limit.

   The system sets the limit and redisplays the Case Assigner Editor.

Modifying an Exception

To modify the rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Click **Add Exception**.

3. Select the user you want to modify the exception for from the drop-down list.

4. Click **Edit**.

5. Modify the limits.

6. Click **Save**.

   The system updates the rule and redisplays the Case Assigner Editor with the rule's updates.

Deleting an Exception

To delete an existing exception for a case from the Assignment Rule Editor, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Click **Add Exception**.

3. Select the user you want to modify the exception for from the drop-down list.

4. Click **Delete**.

   The Confirmation dialog box displays the message: *Are you sure you want to delete the selected exception?*

5. Click **OK** to delete the rule.

   The system removes the exception and redisplays the Case Assigner Editor.

Configuring Actions

This chapter provides procedures for configuring the list of available actions. Configuration of actions requires database privileges. Using actions pop-ups, you can document your analysis and close cases. You can take action on a selected case, such as, closing it, taking a follow-up action on it, or assigning it to other users. The following sections are detailed in this chapter:

- Working with Case Action Settings
- Action Validation Framework

Working with Case Action Settings

The following sections defines how to configure case workflows:

- Understanding Case Workflows
- Adding New Case Statuses
- Configuring Case Action Data
- Configuring Standard Comment Data

Understanding Case Workflows

In general, Case workflows consist of a series of steps and actions. The actions that are available at each step of the workflow determine the next step (or status) in the workflow. With each action, the case can change its status to advance through the workflow.

Defining a Case workflow consists primarily of the following tasks:

1. Create case types, see the *Managing Case Designer*, for more information.

2. Define case statuses that represent steps in the workflow. For more information, see Adding New Case Statuses.

3. Define actions to be used in the workflow. For more information, see Configuring Case Action Data.

4. Define standard comments that is available in the workflow. For more information, see Configuring Standard Comment Data.

Note: When defining workflows, you specify individual actions or comments available at each step.

Adding New Case Statuses

You can add a new case status by following these steps:

1. Add an entry to the KDD_STATUS table, as follows:

```
insert into KDD_STATUS (STATUS_CD,CAN_NHRIT_FL,VIEWD_BY_OWNER_ACTVY_TYPE_CD,
VIEWD_RESULT_STATUS_CD,CLOSED_STATUS_FL,STATUS_NM) values
('CZZZ','N',null,null,'Y','Closed - Loss Recovered')
```

2. Add an entry to the `KDD_CODE_SET_TRNLN` table, as follows:

```
insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL, SRC_SYS_CD, CODE_DISP_TX) values
('CaseStatus', 'CZZZ',null, 'Closed - Loss Recovered')
```

Note: Status is a one of the masking parameter. Populate 'Open' status value as a parameter in `AAI_MENU_B` and `cssms_start_page_master`. Here, we are passing parameter value as INV (code for the Investigation Status). If INV is a valid status code in the application, then do not change anything.

In `AAI_MENU_B`, menu ID is 'OFS_NGECM_SRCH', and in `cssms_start_page_master` , start_page_id is 'ECM'. Parameter will look like '&mStatus=INV'.

Configuring Case Action Data

This section defines how to configure case action. The configured actions will display in UI. You can configure case actions as described in the following subsections:

- Adding a New Action Category
- Adding a New Action
- Mapping New Action to User Role
- Mapping the New Action to Status
- Map the New Action to the Case Type

Note: Sections *Mapping New Action to User Role*, *Mapping the New Action to Status*, *Map the New Action to the Case Type* applicable only for Non-status changing actions. Use PMF for Status changing actions. You can configure these Status changing actions using **Attribute Builder** in PMF. For more information, see the *Configuring Processing Modelling Framework (PMF)*.

Adding a New Action Category

To add a new case action item, follow these steps:

1. Create a new action category by adding a new record in the `KDD_ACTION_CAT_CD` as follows:

```
 insert into KDD_ACTION_CAT_CD (ACTION_CAT_CD,DISPL_NM,DISPL_ORDER_NB, MANTAS_ACTVY_-
CAT_FL) values ('REV','Research & Review',40, 'Y')
```

Adding a New Action

To add a new record code, follow these steps:

1. Create a new action code by adding a new record in the `KDD_ACTION` table as follows:

```
insert into KDD_ACTION (ACTION_ID, ACTION_CATEGORY_CODE, ACTION_NM, ACTION_CD, ACTION_-
DESC, LAST_UPDATED_DT, LAST_UPDATED_BY, COMMENTS, ACTION_ORDER, REQ_CMMNT_FL, DFLT_-
DUE_DT_LM, REQ_REASN_FL, REQ_DUE_DATE_FL, NEXT_REVIEW_STATUS_CD, REG_TYPE_CD,
REQ_REASN_OWNER_FL, LAST_ASSIGN_REQ, RESOLUTION_ACTION_FL, EXPORT_DIR_REF) values (73,
'REV', 'Reviewed with Account Manager', 'CA73A', 'Reviewed with Account Manager', null,
null, null, 90, 'Y', null, 'N', 'N', 'INV', null, 'N', 'N', null, , null)
```

While adding a new action, the set of supplemental values to be associated with the action should be decided based on the following criteria:

a. `ACTION_CATEGORY_CODE` - Category code that identifies the classification of an action. If you want to change the category of an action, you need to change this column accordingly.

b. `ACTION_ORDER` - Integer that represents the order in which action is performed by the system in the scenario of multiple actions take together. The larger the number the higher the precedence. This allows for multiple actions with differing resulting statuses to be taken at the same time and enforcing that the action with the highest action order will be the one to affect the resulting status. For example, action with resulting status *Followup* has action order 10. It is taken at the same time as action with resulting status Closed that has action order 20. Both actions will be applied and visible in the Audit. But the resulting status will be Closed.

   Note: The action order of client-created actions should be less than the action order of system-initiated actions for Re-assignment (CA202A) and Ownership Change (CA103S).

c. `NEXT_REVIEW_STATUS_CD` – Resulting status code to be set when this action type is performed on an investigation record.

d. `REQ_REASN_FL` - Indicator of whether this action type requires reassignment of an investigation record.

e. `REQ_DUE_DATE_FL` - Indicator of whether this action type requires the user to enter a due date on a case.

   Note: Unless superseded by another action being taken on the investigation record that has a Closed status as the resulting status based on the lowest order precedence established in the Investigation Status table the provided due date will be applied on the investigation record.

f. `REQ_CMMNT_FL` - Indicator of whether a comment, either the standard or free-text comment, is required for this action type.

g. `REQ_REASN_OWNER_FL` Indicator of whether this action type requires reassignment of ownership of a case investigation record.

h. `LAST_ASSIGN_REQ` – Used by the system to determine the last user who performed this action in the situation where the this recommendation or escalation action is rejected and the case would need to be reassigned back to the last user who took the action. "Y" means that when this action appears on a case previous to a rejection action by another user the user who took this action would become the owner. "N" means this is not a recommend for approval or escalation type action or is not an action that would be used by the system to determine reassignment.

i. `RESOLUTION_ACTION_FL` - Indicator of whether this action is a resolution action.

Note: If you are adding new actions, then start the action sequence number with a higher number like 30000. If any of the OOB actions not required, then change the category of that action to OBS. This is prevent to that action to appear in the Search screens.

Mapping New Action to User Role

Create a new action Role mapping by adding a new record in the `KDD_ROLE_ACTION_MAP` table as follows: where the `CASE_ROLE_ACTION_MAP_SEQ` represents the next sequential number for a record in this table:

```
insert into KDD_ROLE_ACTION_MAP (CASE_ROLE_ACTION_MAP_SEQ, ROLE_CD, ACTION_CD) values (22, 'CMANALYST1', 'CA73A')
```

Each record in the Case Role to Action Map table represents the mapping between user roles and the actions that a particular user role is allowed to perform. Each Action can be mapped to multiple roles.

Note: If you are adding new records, then start the CASE_ROLE_ACTION_MAP_SEQ with a higher number like 30000.

Mapping the New Action to Status

Create a new action Role mapping by adding a new record in the `KDD_STATUS_ACTION_MAP` table as follows: where the `CASE_STATUS_ACTION_MAP_SEQ` represents the next sequential number for a record in this table:

insert into `KDD_STATUS_ACTION_MAP` (CASE_STATUS_ACTION_MAP_SEQ, STATUS_CD, ACTION_CD) values (26, 'RO', 'CA73A')

Each record in the Case Status to Action table captures the actions that will be available for a case based on the case's current status.

Note: If you are adding new records, then start the CASE_STATUS_ACTION_MAP_SEQ with a higher number like 30000.

Map the New Action to the Case Type

Create a new Case Type Action mapping by adding a new record in the `KDD_CASETYPE_ACTION_MAP` table as follows, where the `CASE_CASETYPE_ACTION_MAP_SEQ` represents the next sequential number for a record in this table:

insert into `KDD_CASETYPE_ACTION_MAP` (CASE_CASETYPE_ACTION_MAP_SEQ, ACTION_CD, CASE_TYPE_-SUBTYPE_CD) values (80, 'CA73S', 'AML_SURV')

Note: If you are adding new records, then start the CASE_CASETYPE_ACTION_MAP_SEQ with a higher number like 30000.

Records in the Case Type to Action table represent actions that are available for a case based on the case type combination of the case.

Configuring Standard Comment Data

Configuring standard comments and standard comment categories is similar to configuring them for the Case Actions pop-up. The comments are created in the `KDD_CMMNT` table, and the categories are in the `KDD_CMMNT_CAT_CD` table.

Mapping of Standard Comment and case type is made by entering a record in the `KDD_CASE_TYPE_CMMNT` table in Case Management schema.

For adding a new record in the `KDD_CASE_TYPE_CMMNT` table, follow the script:

insert into KDD_CASE_TYPE_CMMNT (CASE_TYPE_CD, CMMNT_ID) values ('AML_SURV', 8090)

Action Validation Framework

The action validator framework allows you to perform the validation based on the configuration made in the table KDD_ACTION_VLDTN.

Examples:

1. If you want to set a validation rule where you want to exclude the comments action(CA8) when Send Email Action is taken , then for "Send Email Action"(CA921), set the below configuration entries in KDD_ACTION_VLDTN table:

ACTION_CD	VLDTN_TYPE	VLDTN_CONFIG_DATA	VLDTN_FLD_MSG	VLDTN_ORDER	ACTV_FL
CA921	EXCLUDE	CA8	(null)	(null)	Y

When this validation rule is executed, an error message will display.

2. If you want to a set a validation rule where Case Owner and Case Assignee values should not be same, then for "Set Case Owner" (CA938) and "Set Case Assignee" (CA939), set below JAVASCRIPT validator in KDD_ACTION_VLDTN table:

ACTION_CD	VLDTN_TYPE	VLDTN_CONFIG_DATA	VLDTN_FLD_MSG	VLDTN_ORDER	ACTV_FL
CA938	JAVASCRIPT	validateOwnerAssignee	RENDERE.CM_TA_OWNRASSGN_NTSM	1	(null)
CA938	JAVASCRIPT	validateOwnerAssignee	RENDERE.CM_TA_OWNRASSGN_NTSM	1	(null)

When this validation rule is executed, an error message will display.

KDD_ACTION_VLDTN table

Column Name	Primary Key	Column Type	Nullable
ACTION_CD	Y	VARCHAR2 (20 CHAR)	No
VLDTN_TYPE	Y	VARCHAR2 (50 CHAR)	No
VLDTN_CONFIG_DATA	Y	VARCHAR2 (4000 CHAR)	No
VLDTN_FLD_MSG		VARCHAR2 (1000 CHAR)	Yes
VLDTN_ORDER		NUMBER(10)	Yes
ACTV_FL		VARCHAR2 (1 CHAR)	Yes

- **ACTION_CD:** This is the Action code for which validation will be performed.

- **VLDTN_TYPE:** Indicates the Validation Type. Below are the possible values

  ■ EXCLUDE: Exclude Action validator

  ■ INCLUDE: Include Mandatory Action validator

  ■ QUERY: Query based validator

  ■ JAVASCRIPT: JavaScript based client side validator

- **VLDTN_CONFIG_DATA:** Indicates the configuration for the validator.

  ■ For Exclude Type:
  Action codes which are mutually exclusive for this action must be provided. Multiple action codes needs to be provided in separate rows with type as EXCLUDE.

  ■ For Include Type:
  Action codes which are mandatorily inclusive for this action must be provided. Multiple action codes needs to be provided in separate rows with type as INCLUDE.

  ■ For Query Type:
  Query needs to be provided in VLDTN_CONFIG_DATA column. The query should be such that in case of failure should return false and in case of success should return true. Both request and session attributes are supported. You can specify them using the below notation:
  Request Attributes: @@AttributeName@@
  Session Attributes: ##AttributeName##
  Below is list of seeded parameters to Query Validator:

    ■ actionCode (Action Code for which the validation is been performed)

    ■ ReviewId (Case ID on which the action is performed)

    ■ setDDActnVal (Set Due Date Value)

    ■ clearDDActnVal (Clear Due Date Value)

    ■ setCAActnVal (Case Assignee Value)

    ■ setCOActnVal (Case Owner Value)

    ■ autoAssgnActnVal (Auto Assignment value)

    ■ emailFromIdActnVal (Email From Value)

    ■ emailSubjTextActnVal (Email Subject Value)

    ■ emailToIdActnVal (Email To Value)

    ■ emailBodyTextActnVal (Email Body Value)

    ■ commentsStdActnVal (Standard Comments value under Comments Action)

    ■ addlnCommentsActnVal (Textual Comments value under Comments Action)

    ■ attachCommentsStdActnVal (Standard Comments value under Attachment Action)

    ■ attachAddlnCommentsActnVal (Textual Comments value under Attachment Action)

    ■ attachFileNameActnVal (File Name under Attachment Action)

    ■ closedCasesAvail (Indicates if any of the selected cases are in a closed status)

- pmfActionsAvail (Indicates if any PMF action is selected or not)

- For JAVASCRIPT Type:

  JavaScript method name should be provided in VLDTN_CONFIG_DATA column. The method can be defined in any custom **JS** file. Follow the steps mentioned in Adding custom JS file in ECM.

  This method should have two inputs one is the actionCode for which this validator is defined and another input is the userEnteredValueMap which contains below attributes that holds user entered values on the Take Action page:

  - setDDActnVal (Set Due Date Value)

  - clearDDActnVal (Clear Due Date)

  - setCAActnVal (Case Assignee Value)

  - setCOActnVal (Case Owner Value)

  - autoAssgnActnVal (Auto Assignment Value)

  - emailFromIdActnVal (Email From Value)

  - emailSubjTextActnVal (Email Subject Value)

  - emailToIdActnVal (Email To Value)

  - emailBodyTextActnVal (Email Body Value)

  - commentsStdActnVal (Standard Comments value under Comments Action)

  - addlnCommentsActnVal (Textual Comments value under Comments Action)

  - attachCommentsStdActnVal (Standard Comments value under Attachment Action)

  - attachAddlnCommentsActnVal (Textual Comments value under Attachment Action)

  - attachFileNameActnVal (File Name under Attachment Action)

The method should return true if the validation is successful or false if the validation fails.

Adding custom JS file in ECM:

1. Copy the custom JS file to <<deployedarea>>/ojff/js/appCommon

2. Go to <<deployedarea>>/ojff/js/appCommon/viewModels/aai-ecm.js. In aai-ecm.js add entry for your js file in the define block. For example, if your custom JS file name is customValidator.js, then add as shown below

```
var viewLoad=false;
var lastSearchedData=null;
var searchedPreviouseValue=[];
var selectedViewSeqID=null;
var searchTrack=false;

define([
        'knockout',
        'ojs/ojcore',
        'knockoutmapping',
        'EventDispatcher',
        'appCommon/cmSolution',
        'appCommon/cmCommon',
        'appCommon/cmLayout',
        'appCommon/customValidator'
    ],

        function (
        ko,
        oj,
        komapping,
        EventDispatcher
    )
    {
        function ECMPageViewModel(params) {

            var self = this;
            var routerConfigArray = getRouterConfigArray();
            self.form = routerConfigArray.lastLoadedModule;
            self.queryString = routerConfigArray.lastQueryString;

        }
        return ECMPageViewModel;
    });
```

- **VLDTN_FLD_MSG:** This is used to specify particular message constant to be shown in case of validation failure. If no message is configured default message will be shown. Default Messages are as below:

  Exclude Validator:

  <ACTION NAME1> is not permitted along with <ACTION_NAME2>

  Include Validator:

  <ACTION NAME1> must be mandatorily taken along with <ACTION_NAME2>

  Query Validator:

  Query validation failed for <ACTION NAME1>

  JavaScript Validator:

  Validation failed for <METHOD_NAME>

- **VLDTN_ORDER:** Numeric Sequence indicating the order of the validator within particular action code.

- **ACTV_FL:** Flag to identify whether the mentioned action validator is active or not.

Note: After making the changes in the table, restart the server.

CHAPTER 16 *Configuring Web Application*

As an Oracle Financial Services Administrator you can customize features in the Web Application UI. This chapter contains information about configuring session time out.

Configuring the Session Timeout Setting

This section describes the following topics:

- Configuring the Session Timeout Setting
- Configuring the Session Timeout Setting for Admin Tools

Configuring the Session Timeout Setting

As an Oracle Financial Services Administrator, you can set the inactive web application users to automatically log off by setting the number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

For more information on how to set the duration before logout for inactive sessions, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide.*

Configuring the Session Timeout Setting for Admin Tools

As Oracle Financial Services Administrator, you can optionally log off inactive Web Application users by establishing a set number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

To modify the idle session timeout for idle or inactive users, follow these steps:

1. Open the web.xml file associated with the WebLogic or WebSphere application.

   You can find this file in the WEB-INF directory under each Web application in the Oracle Financial Services installation.

2. Modify the XML code within the file that contains `<session-config>` in its `<session-descriptor>` entry.

   Do this by setting the `<session-timeout>` part of the entry so that the number of minutes equals the current quantity of minutes of inactivity that result in a logoff.

3. Save the changes.

   After setting the parameter to 30 minutes, the edited XML code should look similar to the following:

   ```
   <session-config>
   <session-timeout>30</session-timeout>
   </session-config>
   ```

APPENDIX A *List of Processes and Tasks*

This appendix describes the list of Processes and Tasks used in various application batches.

OBD Application Process

- Start Batch
- Load Data from BD to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

Start Batch

To start a batch, follow these steps:

1. Log in as **ECM ADMIN** and navigate to **Enterprise Case Management** Application.

2. Go to the **Common Tasks** section and select the **Rule Run Framework**.

3. Click **Run**. The **Run** window is displayed with the available Processes.

4. Go to the **List** section, select **Oracle_BD_Event_Processing**, and click **Edit**.

5. Add the **BD_POPULATE_ENTITY_RELATION** Data Transformation task after the **BD_Create_Task** Data Transformation task and click **Save**. This task populates data in the KDD_CASE_NTITY_REL_EVNT and KDD_CASE_NTITY_REL_CASE tables.

6. Run the **Oracle_BD_Event_Processing** batch.

Load Data from BD to ECM

BD_Load_From_LA_To_CA process is used for load data from Landing area to Consolidation area for OBD. This has following four sub processes:

- Loading BD Events
- Entity Surrogate Key Generation for BD
- Oracle Behavior Detection Evented Data Load
- Oracle Behavior Detection Business Data Load

Below is the list of BD sub-process codes. These sub-processes can be used by OCS, and OKYC applications along with their application specific processes.

Here, Level 1 sub process code execution is a prerequisite for Level 2 sub process execution. Similarly, Level 2 sub process code execution is prerequisite for Level 3 sub process execution and so on. Sub-process within a level can be executed in any order or it can be executed in parallel.

Note: BD_ENTITY_SUP_INFO sub process code has to be executed after business data population (see the **Business Metadata Movement**).

Table 45. BD Sub-process Codes (Run chart)

Correlation

BD_Correlation is used to perform correlation on loaded BD events.This has following two tasks:

- DT_Correlation
- BD_Entity_Sup_Info

Scoring

BD_SCORING is used to perform scoring of OBD events. This has following four sub processes:

- Oracle Behavior Detection Event Scoring
- Oracle Behavior Detection Entity Scoring
- Oracle Behavior Detection Correlation Scoring
- Oracle Behavior Detection Pre-Case Scoring

Promote to Case

BD_Promote_To_Case_Decision is used to make the decision if a OBD correlation can be promoted to a case. This is based on defined threshold limit. This has following task. The task type of this is Computation Rule.

- Pre Case Promotion Rule

Create Case

BD_Create_Case process is used for case creation if a OBD event is promoted to case.

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table 46*)
- CASE_COMPLETION_FLAG

Following is the list of Promote_To_Case T2Ts

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
BD_EVENT _LOOKUP	BD_EVENT BD_EVENT _BINDING BD_EVENT _DETAILS	BD_ACCOUNT_ GROUP_LOOKU P BD_ACCOUNT_ LOOKUP BD_CUSTOMER _LOOKUP BD_DERIVED_A DDRESS_LOOK UP BD_EMPLOYEE _LOOKUP BD_EVENT_LO OKUP BD_EXTERNAL_ ENTITY_LOOKU P BD_INSTITUTIO N_LOOKUP BD_INVESTMEN T_ADVISOR_LO OKUP BD_LOAN_LOO KUP BD_MARKET_C ENTER_LOOKU P BD_PEER_GRO UP_LOOKUP	BD_EVENT_ENTITY_M AP_AC BD_EVENT_ENTITY_M AP_AG BD_EVENT_ENTITY_M AP_BOT BD_EVENT_ENTITY_M AP_CT BD_EVENT_ENTITY_M AP_CUST BD_EVENT_ENTITY_M AP_DA BD_EVENT_ENTITY_M AP_EE BD_EVENT_ENTITY_M AP_EMPL BD_EVENT_ENTITY_M AP_IA BD_EVENT_ENTITY_M AP_IM BD_EVENT_ENTITY_M AP_MIT BD_EVENT_ENTITY_M AP_WT	**Business Metadata Movement** BD_ACCT BD_ACCT_ADDR BD_ACCT_BAL_POSN_SMRY BD_ACCT_EMAIL_ADDR BD_ACCT_GRP BD_ACCT_ID_INSTN_ID_MAP BD_ACCT_LIST_MEMBERSHIP BD_ACCT_PEER_GRP BD_ACCT_PEER_TRXN_SMRY_MNTH BD_ACCT_PHON BD_ACCT_RSTRN BD_ACCT_SMRY_MNTH BD_BACK_OFFICE_TRXN BD_CASH_TRXN BD_CB_LIST_MEMBERSHIP BD_CB_PR_TRXN_SMRY_MNTH BD_CLIENT_BANK BD_CLIENT_BANK_PEER_GRP BD_CLIENT_BANK_SMRY_MNTH BD_CUST BD_CUST_ACCT BD_CUST_ADDR BD_CUST_EMAIL_ADDR BD_CUST_IMP_LICENSE BD_CUST_IMP_LICENSE_GOOD BD_CUST_LIST_MEMBERSHIP BD_CUST_PHON BD_CUST_SMRY_MNTH BD_CUST_SUPPLEMENTAL_ATR BD_DERIVED_ADDRESS BD_EMP BD_EMP_ACCT BD_EMP_ADDR BD_EMP_EMAIL_ADDR BD_EMP_PHON BD_EVENT_SCORE BD_EXTERNAL_ENTITY BD_EXTERNAL_ENTITY_ADDR BD_EXTRNAL_NTTY_MMBRSHP BD_FCC_EXTERNAL_ENTITY_LINK BD_HH_BAL_POSN_SMRY BD_INSTN_MASTER BD_INSURANCE_POLICY BD_INSURANCE_POLICY_CUST BD_INSURANCE_PRODUCT BD_LOAN BD_LOAN_SMRY_MNTH BD_MANGD_ACCT BD_MI_TRXN BD_NTCPTRY_PRFL BD_NVSMT_MGR BD_NVSMT_MGR_SMRY_MNTH BD_PEER_GRP BD_WIRE_TRXN	**Evented Data Movement** BD_ACCT_EVENT BD_ACCT_ACCT_ADDR_EVNT BD_ACCT_BAL_POSN_SMRY_E VNT BD_ACCT_GRP_EVNT BD_ACCT_PEER_GRP_EVNT BD_ACCT_PR_TXN_SMRY_MN_ EVNT BD_ACCT_RSTRN_EVNT BD_ACCT_SMRY_MNTH_EVNT BD_BACK_OFFICE_TRXN_EVN T BD_CASH_TRXN_EVNT BD_CB_PR_TXN_SM_MNT_EVN T BD_CLIENT_BANK_EVNT BD_CLINT_BNK_PR_GRP_EVNT BD_CLNT_BNK_SM_MNT_EVNT BD_CUST_EVNT BD_CUST_IMP_LICENSE_EVNT BD_CUST_IMP_LIC_GOD_EVNT BD_CUST_SMRY_MNTH_EVNT BD_CUST_SUPPL_ATR_EVNT BD_DERIVED_ADDRESS_EVNT BD_EMP_ACCT_EVNT BD_EMP_ADDR_EVNT BD_EMP_EMAIL_ADDR_EVNT BD_EMP_EVNT BD_EMP_PHON_EVNT BD_HH_BAL_POSN_SMRY_EVN T BD_INSTL_ACCT_SMRY_MNTH _EVNT BD_INSTN_MASTER_EVNT BD_INSURANCE_POLICY_EVNT BD_INSURANCE_PRODUCT_EV NT BD_INS_PLCY_CUST_EVNT BD_LOAN_EVNT BD_LOAN_SMRY_MNTH_EVNT BD_MANGD_ACCT_EVNT BD_MI_TRXN_EVNT BD_NTCPTRY_PRFL_EVNT BD_NVSMT_MGR_EVNT BD_NVSMT_MGR_SMRY_MNTH _EVNT BD_PEER_GRP_EVNT BD_WIRE_TRXN_EVNT BD_XTRNL_ENTY_ADR_EVNT

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				BD_ENTITY_SUP_INFO This sub process code has to be executed after business data population (see the Business Metadata Movement).	

Here, Level 0 is the prerequisite for Level 1 execution. Similarly, Level 1 is a prerequisite for Level 0, and so on. Sub-processes within any level can be executed in any order or it can be executed in parallel.

Table 46. Promote_To_Case T2Ts

LEVEL 0	LEVEL 1	LEVEL2	LEVEL 3
KDD_CASES	KDD_CASE_ACCOUNTS	KDD_CASE_ACCT_ADDRS	
	KDD_CASE_ACCT_ATM_SMRY_DAILY	KDD_CASE_ACCT_BAL_POSN_SMRY	
	KDD_CASE_ACCT_GRP	KDD_CASE_ACCT_LIST_MEMBERSHIPS	
	KDD_CASE_ACCT_ID_INSTN_ID_MAP	KDD_CASE_ACCT_RSTRNS	
	KDD_CASE_ACCT_PEER_GRP	KDD_CASE_ACCT_SMRY_MNTH	
	KDD_CASE_ACT_PEER_TXN_SMR_MNTH	KDD_CASE_ACCT_SUPPL_ATTR	
	KDD_CASE_ATTRBT_VAL_MAP	KDD_CASE_INSTL_ACCT_SMRY_MNTH	
	KDD_CASE_BACK_OFFICE_TRXN	KDD_CASE_MANGD_ACCT	
	KDD_CASE_CASH_TRXN	KDD_CASE_ACCT_EMAIL_ADDR	
	KDD_CASE_CB_PEER_TXN_SMRY_MNTH	KDD_CASE_ACCT_PHON	
	KDD_CASE_CUSTOMERS	KDD_CASE_HH_BAL_POSN_SMRY	
	KDD_CASE_CUST_ACCT	KDD_CASE_HH_SMRY_MNTH	
	KDD_CASE_CUST_CREDIT_RTNG	KDD_CASE_CUST_ADDRS	
	KDD_CASE_DERIVED_ADDRESS	KDD_CASE_CUST_EMAILS	
	KDD_CASE_EMP	KDD_CASE_CUST_LIST_MEMBERSHIPS	
	KDD_CASE_EMP_ACCT	KDD_CASE_CUST_PHONS	
	KDD_CASE_INSTN_MASTER	KDD_CASE_CUST_SMRY_MNTH	
	KDD_CASE_INSTRUCTION	KDD_CASE_CUST_SUPPL_ATTR	
	KDD_CASE_INVOLVED_PARTY_LINK	KDD_CASE_EMP_ADDR	
	KDD_CASE_LINKS	KDD_CASE_EMP_EMAIL_ADDR	
	KDD_CASE_LOAN	KDD_CASE_EMP_PHON	
	KDD_CASE_LOSS_RECOVERY	KDD_CASE_CB_LIST_MEMBERSHIP	KDD_CASE_EXTRNL_NTITY_ADDR KDD_CASE_EXTRNL_NTITY_MBRSHP KDD_CASE_EXTRL_NTITY_SMRY_MNTH
	KDD_CASE_LOSS_RECVRY_COST_CR	KDD_CASE_CLIENT_BANK	
	KDD_CASE_MI_TRXN	KDD_CASE_CLIENT_BANK_PEER_GRP	
	KDD_CASE_NARRATIVE	KDD_CASE_CLIENT_BANK_SMRY_MNTH	
	KDD_CASE_NTCPTRY_PRFL KDD_CASE_NTWK_USER_ACCT_MAP KDD_CASE_NVSMT_MGR	KDD_CASE_EXTERNAL_ENTITY	
		KDD_CASE_LOAN_SMRY_MNTH	
		KDD_CASE_NVSMT_MGR_SMRY_MNTH	
	KDD_CASE_ONLINE_ACCT		
	KDD_CASE_ONLINE_ACCT_ACCT		
	KDD_CASE_ORDR		
	KDD_CASE_PEER_GRP		

- KDD_CASE_ACCOUNTS (Level 1) process has to be executed before execution of KDD_CASE_ACCT_ADDRS, KDD_CASE_ACCT_BAL_POSN_SMRY, KDD_CASE_ACCT_LIST_MEMBERSHIPS, KDD_CASE_ACCT_RSTRNS, KDD_CASE_ACCT_SMRY_MNTH, KDD_CASE_ACCT_SUPPL_ATTR, KDD_CASE_INSTL_ACCT_SMRY_MNTH, KDD_CASE_MANGD_ACCT, KDD_CASE_ACCT_EMAIL_ADDR, and KDD_CASE_ACCT_PHON.

- KDD_CASE_ACCT_GRP (Level 1) process has to be executed before execution of KDD_CASE_HH_BAL_POSN_SMRY and KDD_CASE_HH_SMRY_MNTH.

- KDD_CASE_CUSTOMERS (Level 1) process has to be executed before execution of KDD_CASE_CUST_ADDRS, KDD_CASE_CUST_EMAILS, KDD_CASE_CUST_LIST_MEMBERSHIPS, KDD_CASE_CUST_PHONS, KDD_CASE_CUST_SMRY_MNTH, and KDD_CASE_CUST_SUPPL_ATTR.

- KDD_CASE_EMP (Level 1) process has to be executed before execution of KDD_CASE_EMP_ADDR, KDD_CASE_EMP_EMAIL_ADDR, and KDD_CASE_EMP_PHON.

- KDD_CASE_INSTN_MASTER (Level 1) process has to be executed before execution of KDD_CASE_CB_LIST_MEMBERSHIP, KDD_CASE_CLIENT_BANK, KDD_CASE_CLIENT_BANK_PEER_GRP, KDD_CASE_CLIENT_BANK_SMRY_MNTH, and KDD_CASE_EXTERNAL_ENTITY.

- KDD_CASE_LOAN (Level 1) process has to be executed before execution of KDD_CASE_LOAN_SMRY_MNTH.

- KDD_CASE_NVSMT_MGR (Level 1) process has to be executed before execution of KDD_CASE_NVSMT_MGR_SMRY_MNTH.

- KDD_CASE_EXTERNAL_ENTITY (Level 2) process has to be executed before execution of KDD_CASE_EXTRNL_NTITY_ADDR, KDD_CASE_EXTRNL_NTITY_MBRSHP, and KDD_CASE_EXTRL_NTITY_SMRY_MNTH.

End Batch

BD_ECM_End_E2E_Batch is used for ending the batch execution for BD.

OCS Application Process

Following process are used for this:

- Start Batch
- Load Data from CS to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case

- End Batch

Start Batch

ECM_Start_E2E_Batch_For_CS process is used to start the batch to move the data from OCS to ECM.

Load Data from CS to ECM

Load_From_CS_To_CA is used for loading the CS data from Landing area to Consolidation area. This has following four sub processes:

- Loading Oracle CS Events: loads the CS events to Consolidation area
- Entity Surrogate Key Generation For Oracle CS
- Evented Data Load for CS
- Business Data Load for CS

Correlation

This is used to perform correlation on loaded CS events.

- DT_CORRELATION

Scoring

Scoring_OCS is used to perform scoring of OCS events. This has following sub process:

- Pre-Case-Scoring For Oracle CS

Promote to Case

Promote_To_Case_Decision_OCS is used to make the decision if a OCS correlation can be promoted to a case. This is based on defined threshold limit. This has following sub process:

- Pre Case Promotion Rule

Create Case

Create_Case is used to create a case if a OCS event is promote to case.

Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table 46*)
- CASE_COMPLETION_FLAG

End Batch

ECM_End_E2E_Batch_For_CS is used for ending the batch execution for CS.

OKYC Application Process

Following process are used for this:

- Start Batch
- Load Data from KYC to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- Update Case ID
- End Batch

Start Batch

ECM Start E2E Batch For KYC process is used to start the batch execution to move the data from OKYC to ECM.

Load Data from KYC to ECM

Load_From_OKYC_To_CA process loads OKYC data from Landing area to Consolidation area. This has following four sub processes:

- Loading Oracle KYC Events: loads the KYC events to Consolidation area
- Entity Surrogate Key Generation For Oracle KYC: This should be executed after **Loading Oracle KYC Events** sub process.
- Evented Data Load for KYC
- Business Data Load for KYC

Correlation

This is used to perform correlation on loaded KYC events.

- DT_CORRELATION

Scoring

Scoring_OKYC is used to perform scoring of OKYC events. This has following sub process:

● Pre-Case Scoring For Oracle KYC

Promote to Case

Promote_To_Case_Decision_OKYC is used to make the decision if a OKYC correlation can be promoted to a case. This is based on defined threshold limit. This has following sub process:

● POPULATE_P2C_FL_OKYC

Create Case

Create_Case is used to create a case if a OKYC event is promote to case.

Following is the list of Promote_To_Case T2Ts:

● f_generatecaseid

● f_insertcases

● Promote_To_Case T2Ts (see the *Table 46*)

● CASE_COMPLETION_FLAG

Update Case ID

UPD_CaseId_To_OKYC is used for updating the Case IDs to OKYC.

End Batch

ECM_End_E2E_Batch_For_KYC is used for ending the batch execution for KYC.

Third party Application Process

Following process are used for this:

● Start Batch

● Load Data from Third Party to ECM

● Correlation

● Scoring

● Promote to Case

● Create Case

● End Batch

Start Batch

ECM Start E2E Batch process is used to start the batch execution to move the data from Third party application to ECM.

Load Data from Third Party to ECM

Load_From_LA_To_CA process loads the data from Landing area to Consolidation area. Here, the data will populate to Landing area from Staging area. This has following four sub processes:

- Loading Events: This has following tasks

- Entity Surrogate Key Generation: This has following tasks:

- Evented Data Load

- Derive Wire, Cash and MI Transaction

Below is the list of Third Party sub-process codes.

Here, Level 1 sub process code execution is a prerequisite for Level 2 sub process execution. Similarly, Level 2 sub process code execution is prerequisite for Level 3 sub process execution and so on. Sub-process within a level can be executed in any order or it can be executed in parallel.

Note: BD_ENTITY_SUP_INFO sub process code has to be executed after business data population (see the **Business Metadata Movement**).

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
t2t_LOOKU P_EVENT	t2t_EVENTS t2t_FCC_EVEN T_BINDING t2t_FCC_EVEN T_DETAILS	t2t_LOOKUP_ACCO UNT t2t_LOOKUP_CUST OMER t2t_LOOKUP_EMPL OYEE t2t_LOOKUP_EXTE RNAL_ENTITY t2t_LOOKUP_INSTI TUTION_CB t2t_LOOKUP_ACCO UNT_GROUP t2t_LOOKUP_BOT t2t_LOOKUP_FOT	t2t_FCC_EVENT_ENTI TY_MAP_ACCOUNT t2t_FCC_EVENT_ENTI TY_MAP_CUSTOMER t2t_FCC_EVENT_ENTI TY_MAP_EMPLOYEE t2t_FCC_EVENT_ENTI TY_MAP_EXTERNAL_ ENTITY t2t_FCC_EVENT_ENTI TY_MAP_CLIENT_BA NK t2t_FCC_EVENT_ENTI TY_MAP_ACCOUNT_ GROUP t2t_FCC_EVENT_ENTI TY_MAP_FOTWIRE t2t_FCC_EVENT_ENTI TY_MAP_FOTCASH t2t_FCC_EVENT_ENTI TY_MAP_FOTMI	t2t_EVENTED_ACCT t2t_EVENTED_ACCT_ADDR t2t_EVENTED_ACCT_RSTRN t2t_EVENTED_CUST t2t_EVENTED_CUST_CREDIT_ RTNG t2t_EVENTED_EMP t2t_EVENTED_EMP_ACCT t2t_EVENTED_EMP_ADDR t2t_EVENTED_EMP_EMAIL_AD DR t2t_EVENTED_NTCPTRY_PRF L_ACCT t2t_EVENTED_NTCPTRY_PRF L_CUST t2t_EVENTED_ACCT_BAL_PO SN_SMRY t2t_EVENTED_ACCT_GRP t2t_EVENTED_AUTO_QUOTE t2t_EVENTED_BACK_OFFICE_ TRXN t2t_EVENTED_CLIENT_BANK t2t_EVENTED_CORP_ACTN t2t_EVENTED_CUST_ADDR t2t_EVENTED_CUST_SUPPLE MENTAL_ATTR t2t_EVENTED_DERIVED_ADD RESS t2t_EVENTED_EMP_PHON t2t_EVENTED_EXTERNAL_EN TITY t2t_EVENTED_INSTN_MASTER t2t_EVENTED_MANGD_ACCT t2t_EVENTED_ONLINE_ACCT t2t_EVENTED_ONLINE_ACCT_ ACCT t2t_EVENTED_PEER_GRP	t2t_FCC_TRXN_PIVOT_ TRANSFORM_DS t2t_FCC_TRXN_BNK2BN K_FL_DS t2t_FCC_TRXN_PARTY_ XREF_BOT t2t_FCC_TRXN_PARTY_ XREF_BOT_OFFSET t2t_FCC_TRXN_PARTY_ XREF_FOT

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
		Stage to CA Customer Account Lookup Stage to CA Customer Customer Lookup Stage to CA Employee Account Lookup Stage to CA Account Daily Lookup		Stage to CA Account Stage to CA Account Address Email Address Stage to CA Account Address Email Phon Stage to CA Account Address Stage to CA Customer Stage to CA Customer Account Stage to CA Customer Address Stage to CA Customer Country Stage to CA Customer Email Address Stage to CA Customer Phone Stage to CA Customer Supplemental Attribute Stage to CA Customer to Customer Relation Stage to CA Correspondent Bank Stage to CA Back Office Transaction Stage to CA Derived Address Stage to CA Derived Entity Stage to CA Derived Entity Link Stage to CA Derived Entity to Derived Address Stage to CA FrontOffice Transaction Party Stage to CA Financial Institution Stage to CA Employee Stage to CA Employee Address Stage to CA Employee Email Address Stage to CA Employee Phone Stage to CA FrontOffice Transaction Stage to CA Employee Account	
				BD_ENTITY_SUP_INFO This sub process code has to be executed after business data population (see the Business Metadata Movement). This sub process code has to be executed after business data population.	

Correlation

This is used to perform correlation on loaded events.

- DT_CORRELATION

Scoring

This is used to perform scoring of Third Party events, entities and correlation. This has following sub process:

- Entity_Scoring

- Event_Scoring

- Correlation_Scoring

- Pre_Case_Scoring

Promote to Case

Promote_To_Case_Decision is used to make the decision if a Third Party correlation can be promoted to a case. This is based on defined threshold limit.

Create Case

Create_Case is used to create a case if a Third Party event is promote to case.

Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid

- f_insertcases

- Promote_To_Case T2Ts (see the *Table 46*)

- CASE_COMPLETION_FLAG

End Batch

ECM_End_E2E_Batch is used for ending the batch execution.

APPENDIX B

Configuring Parallel Graph AnalytiX (PGX) Correlation

This appendix describes the configuration activities for Parallel Graph AnalytiX (PGX) Correlation. This appendix covers following sections:

- Overview
- Configuring Parallel Graph AnalytiX (PGX) Correlation

Overview

PGX is a toolkit for graph analysis - both running algorithms such as PageRank against graphs, and performing SQL-like pattern-matching against graphs, using the results of algorithmic analysis. Algorithms are parallelized for extreme performance. The PGX toolkit includes both a single-node in-memory engine, and a distributed engine for extremely large graphs. Graphs can be loaded from a variety of sources including flat files, SQL and NoSQL databases and Apache Spark and Hadoop; incremental updates are supported.

Configuring Parallel Graph AnalytiX (PGX) Correlation

Perform the following steps to test the PGX configuration:

Note: Ensure that Java_HOME is pointing to Java 8.

1. Login as ECMADMN.

2. Navigate to Common Task. Select Unified Metadata Manager and click Data Integrator Framework.

3. Select Post Load Changes. A new screen is displayed.

4. Click DT_CORRELATION under transformation in the LHS.

5. Click Input Parameters in the RHS.

   In External Library Detail section, select External Library, update the value `./correlation.sh` to `./pgxCorrelation.sh`

APPENDIX C   *FAQ*

This section of the document consists of resolution to the frequently asked questions during the configuration.

What should be done if the batch fails during the initial task?

Check if V_GROUP_NAME has been passed correctly in the START batch and Backend servers are UP (such as, ICC as well as agent servers)

What should be done if the second/third task is struggling to start?

Login to Config Schema and execute the following query:

```
Select * from PR2_PROCESS_TASK_PARAMETER
```

Make sure that V_TASK_PARAMETER_VALUE column has correct SOURCENAME, and also LOADTYPE is correct.

What should be done if any process inside the batch fails?

Follow these steps:

1. Navigate to `$FIC_HOME/ficdb/log` and check the logs, and resolve the issues.
2. Once the issue is resolved, then navigate to Common Tasks UI and select Operations.
3. Select Batch execution and Restart the batch which is failed.

What should be done if batch needs a rerun?

Remove all the CA tables data for the MISDATE and Data Origin. Start a new batch again.

There can be the cases where source schema is different but data resides in the same instance. In this case, `Grant select to all user tables` needs to be provided to the ECM Atomic schema from the source schema.

What should be done if Correlation fails in first time run?

Make sure to run the `correlation.sh` file. For more information, see the *Pre Batch Execution Configuration*

Can I run the Batch again if data-loaded to CA went wrong?

- Yes, you can trigger a new batch. Before running the batch, you must clear all the data from all business, evented and event tables for that MIS Date and Data Origin.
- Yes, you can trigger a new batch. Before that you must remove the data from the Event tables. This will take more time than the above option.

What should I do, if I have loaded few wrong records into few business tables?

■   You can trigger a new batch. Before running the batch, you must clear all the data from all business, evented and event tables for that MIS Date and Data Origin

■   You can remove the data from the business tables for MIS Date and Data Origin, then run the batch only including the process for which you need to correct the data and then end this batch. This will take more time than the above option.