Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.7.1.0
November 2019

ORACLE

Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.7.1.0
November 2019

Part Number: E83847-01

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190

Part Number: E83847-01
First Edition (November 2019)

Trademarks
Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
Other names may be trademarks of their respective owners.

Oracle Financial Services Software, Inc.
1900 Oracle Way
Reston, VA 20190
Phone: 703-478-9000
Fax: 703-318-6240
Internet: www.oracle.com/financialservices

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

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

Enterprise Case Management (ECM) supports the investigation and resolution of Anti-Money Laundering (AML), Know Your Customer (KYC), Customer Screening (CS), Studio (STDO), 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 designing workflows using the Processing Modelling Framework. *Figure 1* depicts the ECM workflow.

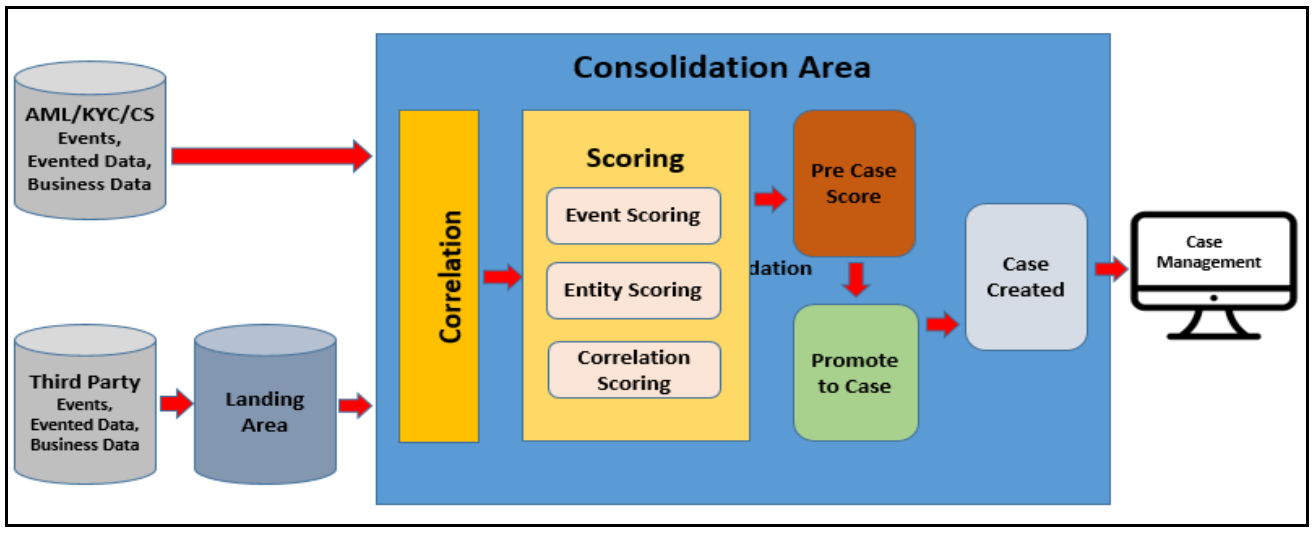


Figure 1. ECM Workflow

Administration and Configuration Activities

This section covers the following topics:

Loading Data

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 the 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 Action Settings

Case Action configuration allows the Administrator to add 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 instructions to log in to the OFS ECM application and manages the different features of the Oracle Financial Services Analytical Applications (OFSAA) application page.

The following sections are covered in this chapter:

System Requirements

The following applications are required to run the OFS ECM 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 OFS ECM Application

Access to the Oracle Financial Services Enterprise Case Management (OFS ECM) application depends on the Internet or Intranet environment. Oracle Financial Services Enterprise Case Management (OFS ECM) is accessed through Microsoft Internet Explorer (IE) or 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 purposes, you can change the password. For more information, see *Change Password* section.

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

To access OFS ECM Application, follow these steps:

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

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

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

   The OFSAA login page is displayed.

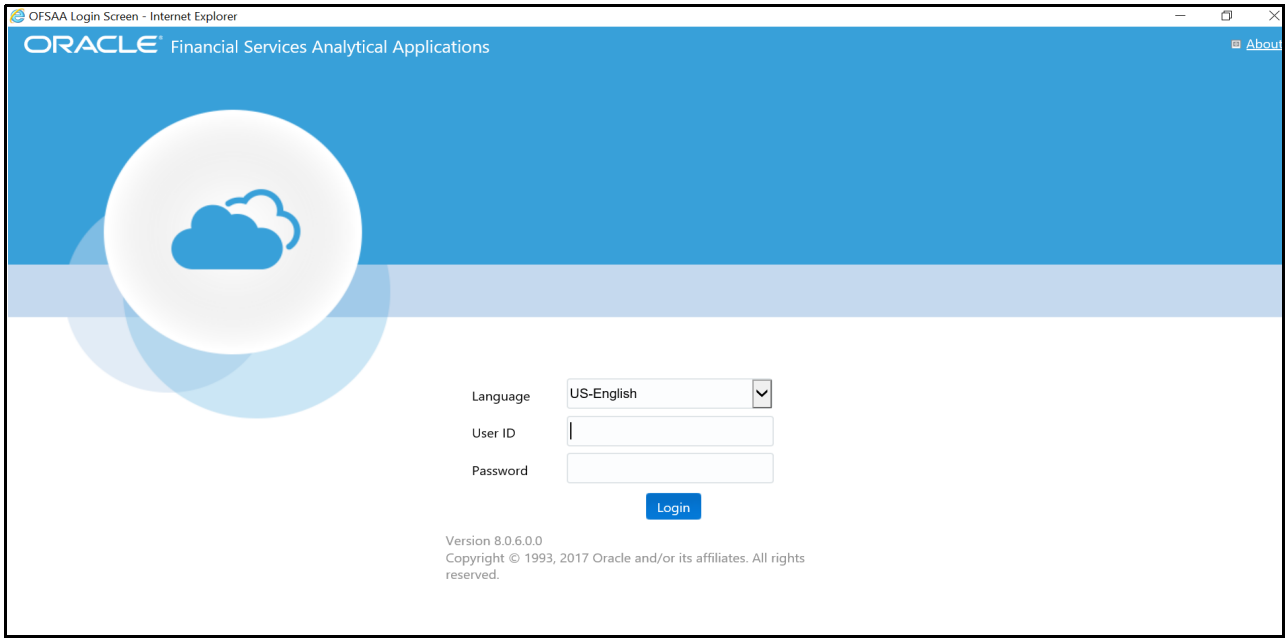


Figure 2. OFSAA Login Page

2. Select the Language from the Language drop-down list.
3. Enter your User ID and Password.
4. Click **Login**. The OFS ECM Application landing page is displayed.

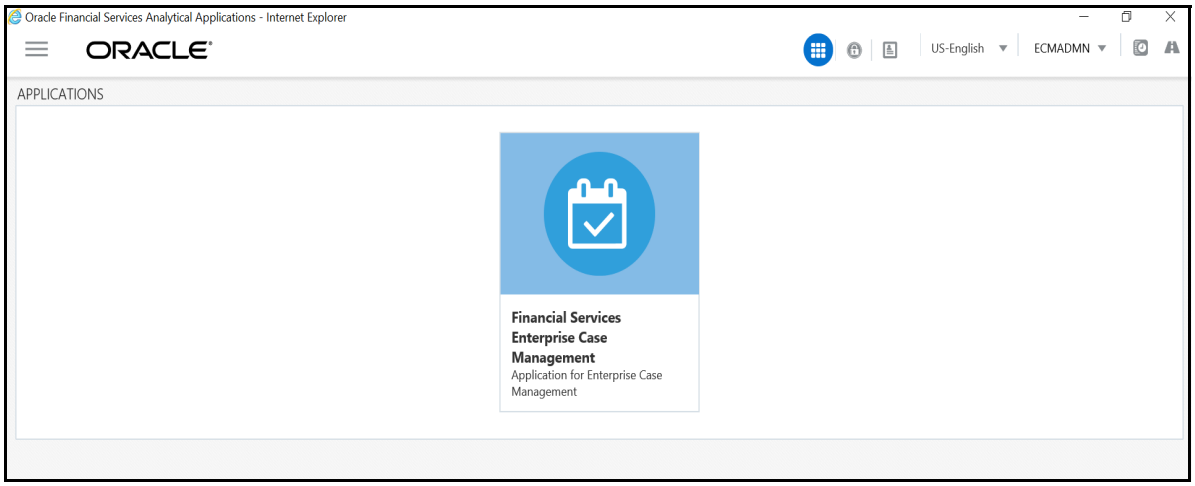


Figure 3. Enterprise Case Management Page

Masthead

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

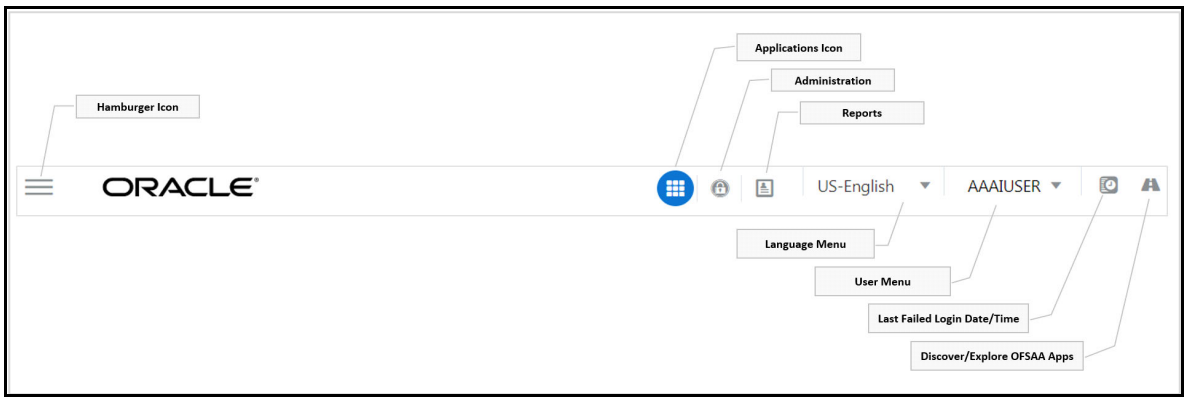


Figure 4. Masthead

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  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  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 purposes, you can change the password. This section explains how to change the password.

To change the password, follow these steps:

1. Navigate to OFSAA Applications page.

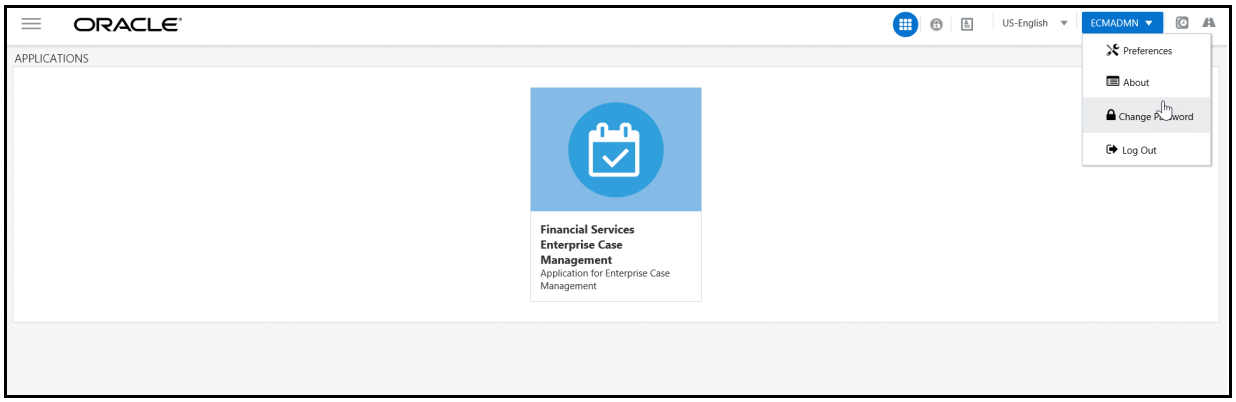


Figure 5. Change Password

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

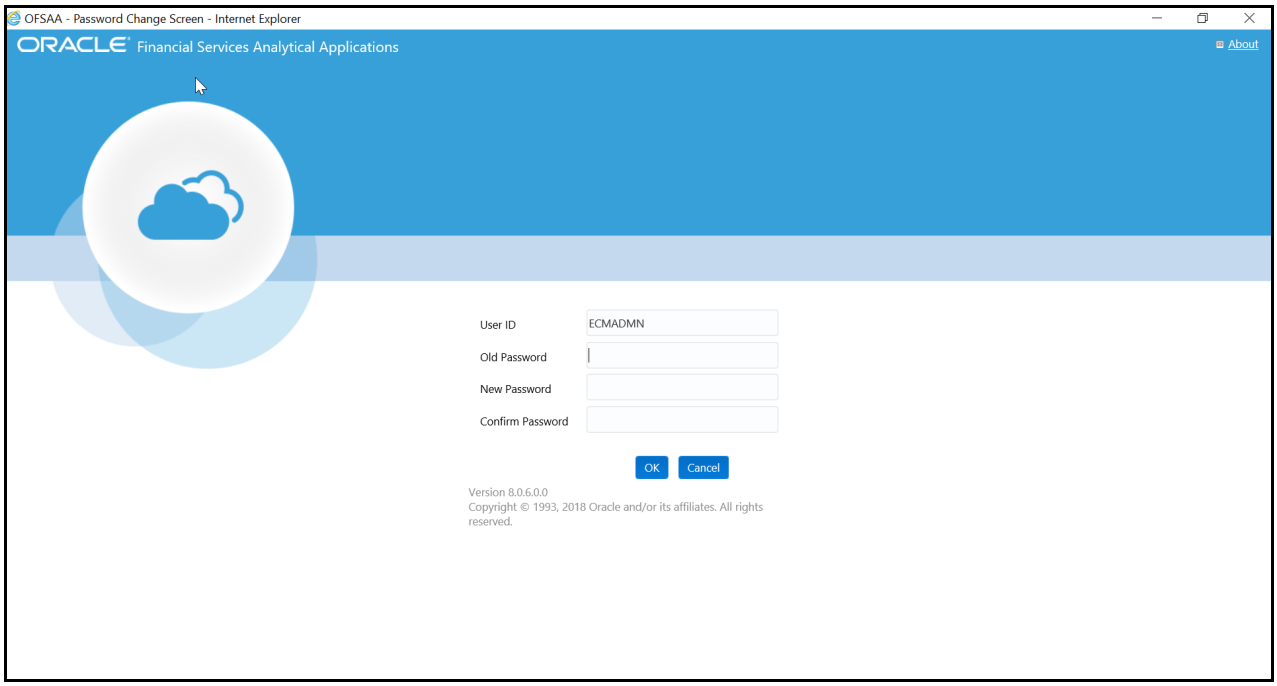


Figure 6. Change Password

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 log in 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.

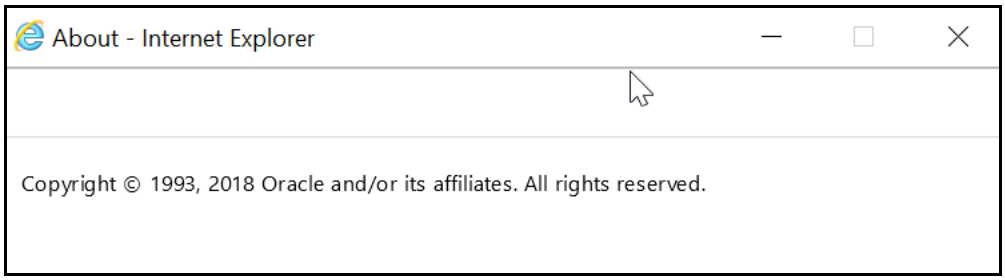
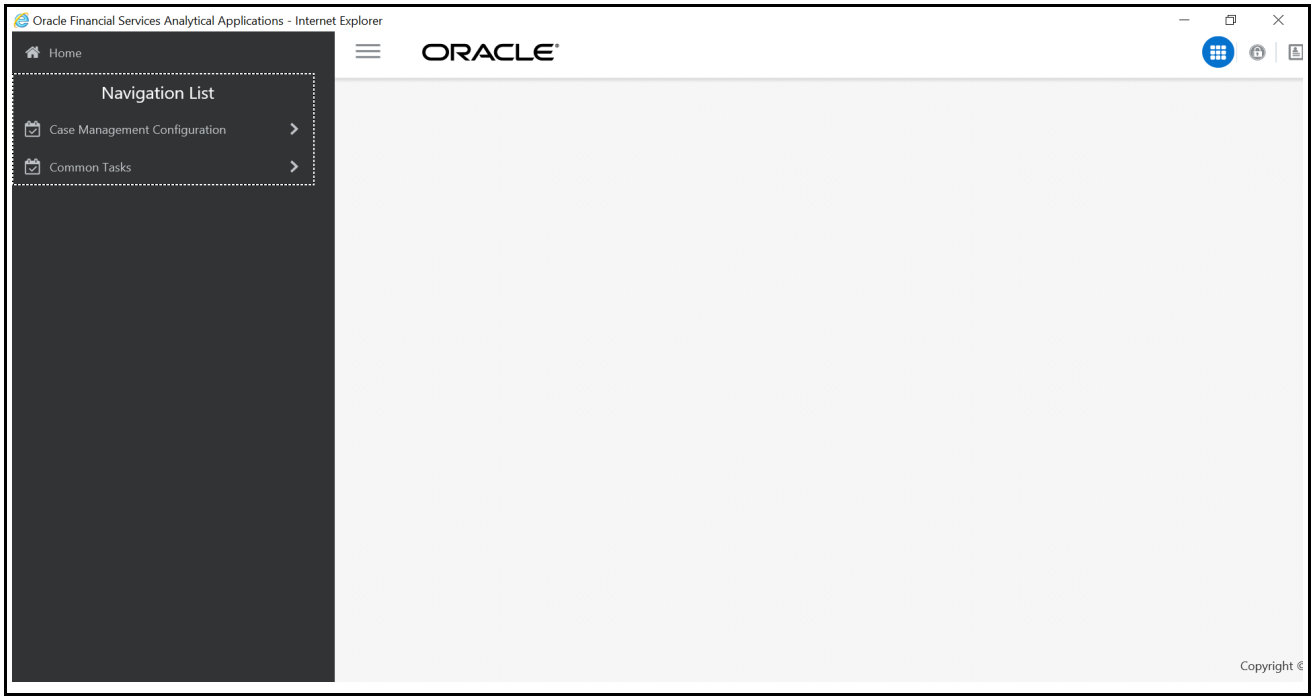


Figure 7. Copyright Information

Selecting Applications

This section explains how to access the 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.

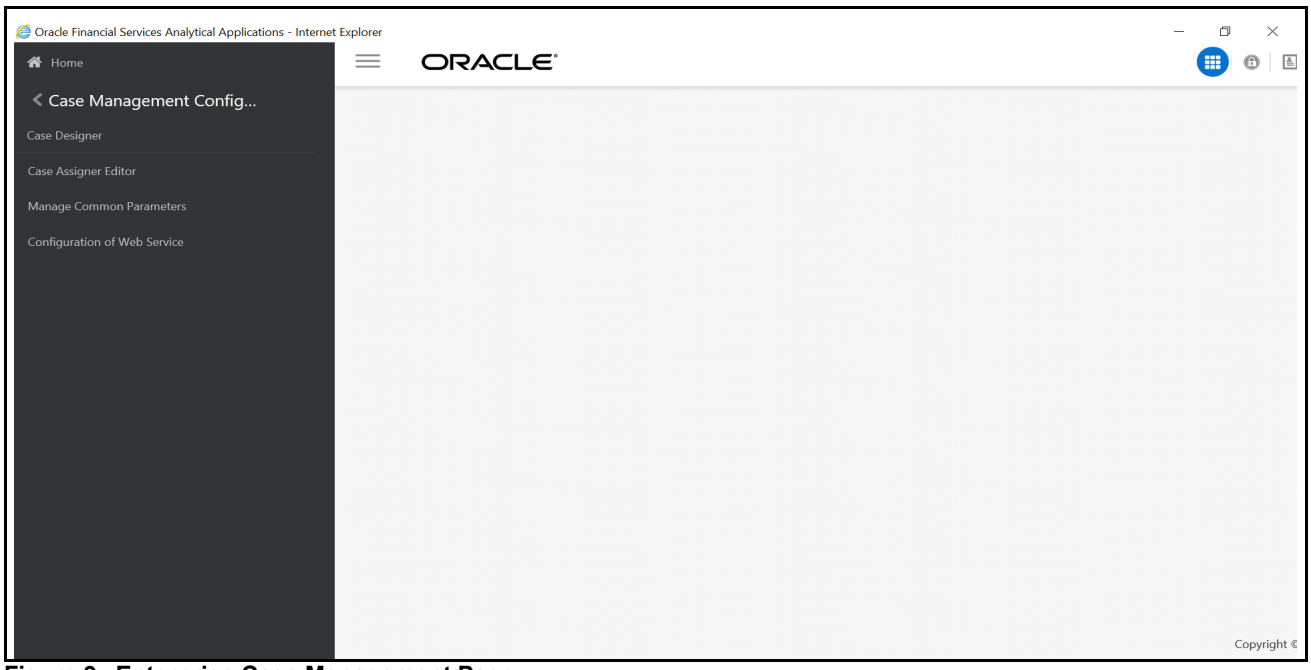


Figure 9. Enterprise Case Management Page

Managing OFSAA Administration Page

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

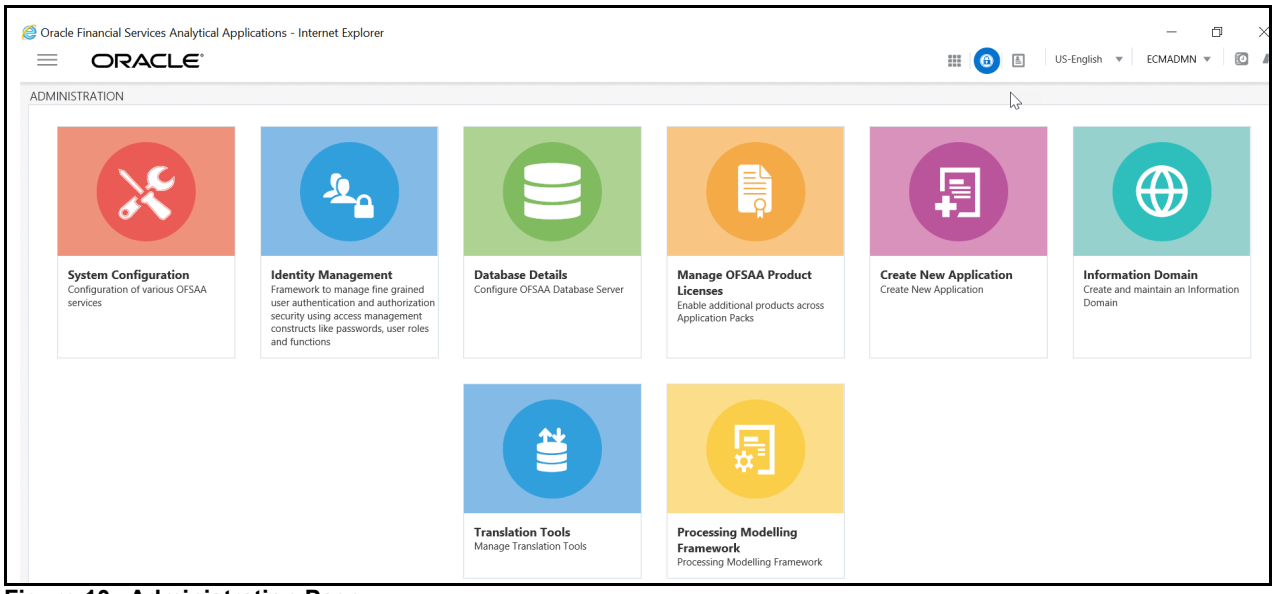


Figure 10. Administration Page

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 the following topics:

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.

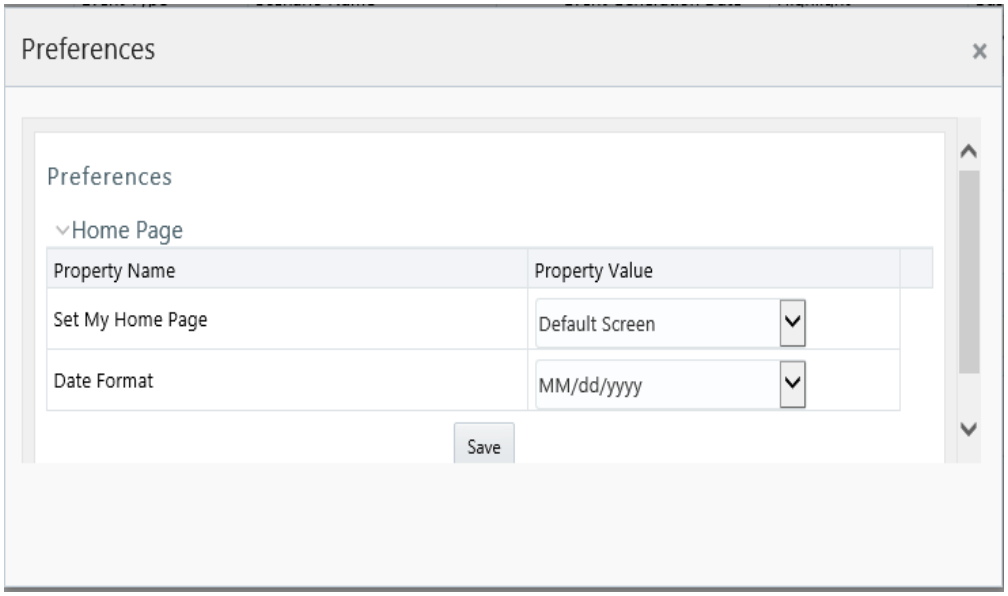


Figure 11. Preference screen.

2. In the Property Value drop-down list, select the application which you want to set as the Home Page.
3. Define the date format. The default date format is **MM/dd/yyyy**. You can change this to **dd/MM/yyyy** format.

   Note: Whenever a new application is installed, the related value for that application is found in the drop-down list.
4. Click **Save** to save your preference.

Note: : In ECM Application, for `DEFAULT_DATEFORMAT_REQ`, `PARAMVALUE` should be set to 'TRUE' in the `CONFIGURATION` table. Run the below update Query in CONFIG Schema and restart the servers, if the parameter is not set to TRUE.

```
update CONFIGURATION t  set t.PARAMVALUE = 'TRUE'  where t.paramname =
'DEFAULT_DATEFORMAT_REQ';
```

CHAPTER 3

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

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

An ECM administrator has following access permissions:

- User Security Administration
- Excel Upload
- Web Service Configuration
- Common Web Service
- Preferences
- User Administration
- Security Management System
- Security Attribute Administration
- Manage Common Parameters
- Case Management Configuration

- Unified Metadata Manager
- Processing Modelling Framework
- Case Designer

User Provisioning Process Flow

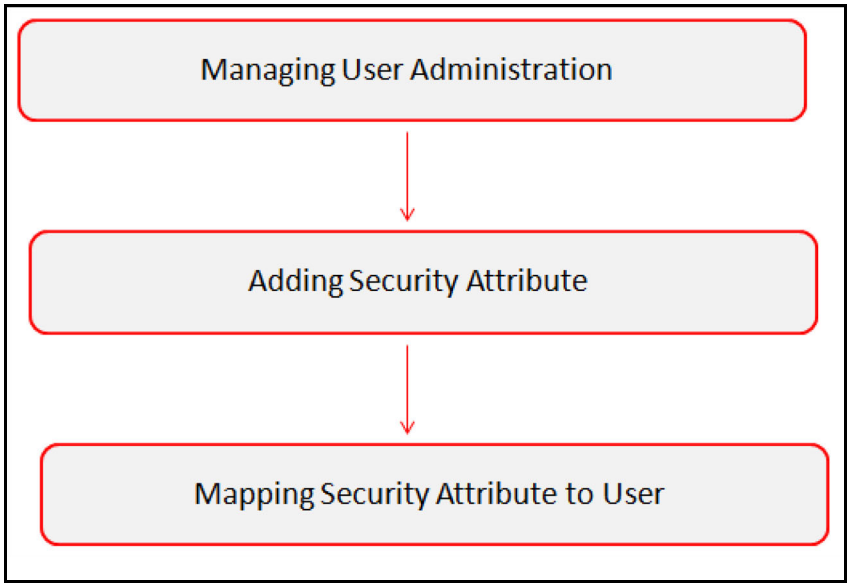


Figure 12. User Provisioning Process Flow

Table 2 lists the various actions and associated descriptions of the user administration process flow.

Table 2. 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 3. 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.

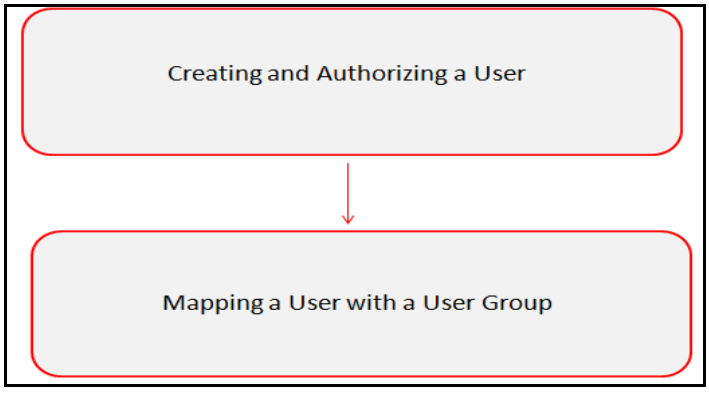


Figure 13. Managing Identity and Authorization Process Flow

Table 4 lists the various actions and associated descriptions of the user administration process flow:

Table 4. 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.

Note: Make sure the same User ID should not already exist as an organization in the KDD_ORG table.

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, 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 to 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 the 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, the Type defined is 0 (Textbox). You can provide it as 1 (Dropdown) if required and re-upload the Sheet using the Config Schema Upload.

   After updating the fields, click **Save**.

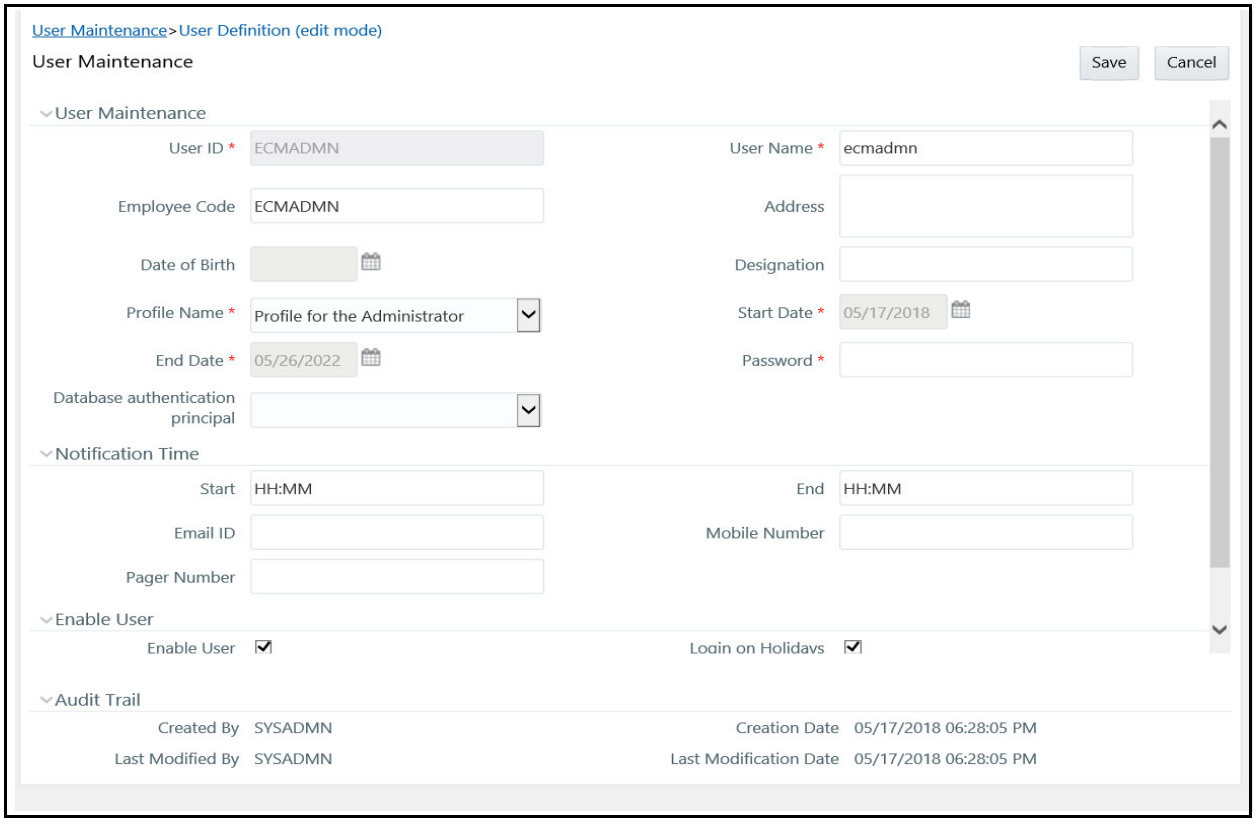


Figure 14. User Maintenance

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 5 describes the Case Management User Roles and corresponding User Groups.

Table 5. Case Management Roles and User Groups

User 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
RFIUSRROLE	RFI Questionnaire Response Access Group	RFIUSRGROUP
CMSECROLE	Refer Note[1]	Refer Note[1]

Note:

- If a user logs in with multiple roles, then system will the display actions on the Case List and Case Details page based on the highest role. In Take Action pop up window, if Supervisor and Analyst both roles are mapped to a user, then Analyst actions will be suppressed provided below notation is followed:
  - **Supervisor Actions:** Action code should be suffixed with S.
  - **Analyst Actions:** Action code should be suffixed with A.
- Do not assign Admin roles and Investigation roles (Supervisor, Analyst, Viewer roles) together for a user.
- **RFIUSRGROUP** user group code can be associated with any user for getting access to the RFI Questionnaire Response UI.
- **CMSECROLE**[1] role can be used for mapping to user groups, which are created only for security Attribute Mapping purpose. Usergroups mapped to this role will appear in the Mapper Maintenance Screen, along with the OOB User Groups.

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

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

Table 6. 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 a Single-character code that represents a business domain (for example, a, b, or c).		VARCHAR2(50)	No
V_ATTRIBUTE_PRIORITY	The 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 the 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 cases associated with jurisdictions to which they have access. You can use jurisdiction to divide data into 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 the use of this data attribute to define separate threshold sets based on jurisdictions. The list of jurisdictions in the system resides 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 versus 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 the 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 topmost definition through which a case is created. Case Type provides a 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 that 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 it.

Security attributes are loaded through Excel using the following templates:

Table 7. 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. Log in 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 the 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 8*.

Table 8. 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 the 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 *Table 9*.

Table 9. 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 the 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 10*.

Table 10. 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 to 1`, which is SYSTEM value 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

Security attributes can be mapped to User groups using Security mapper. This is done using the Mapper Maintenance window. Attributes mapped to User groups in the mapper, are mapped against each user in that user group, after running the Security batch. .

The following are members of 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

You 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, the 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 the KDD_INSTALL_PARAM table.

Note: Update the column ATTR_3_VALUE_TX for PARAM_ID=7 with the RRS URL in the 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 the Save Metadata screen.

Hierarchy Re-save

1. Log in as an 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

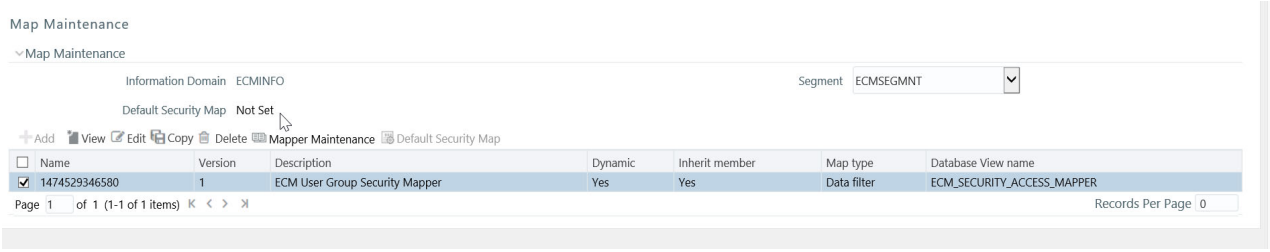
Load the User configuration data into CSSMS_ATTRIB_MAST table using Excel Upload if not done during before User creation. For more information, see the *Oracle Financial Services Analytical Applications Infrastructure User Guide*.

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

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**.

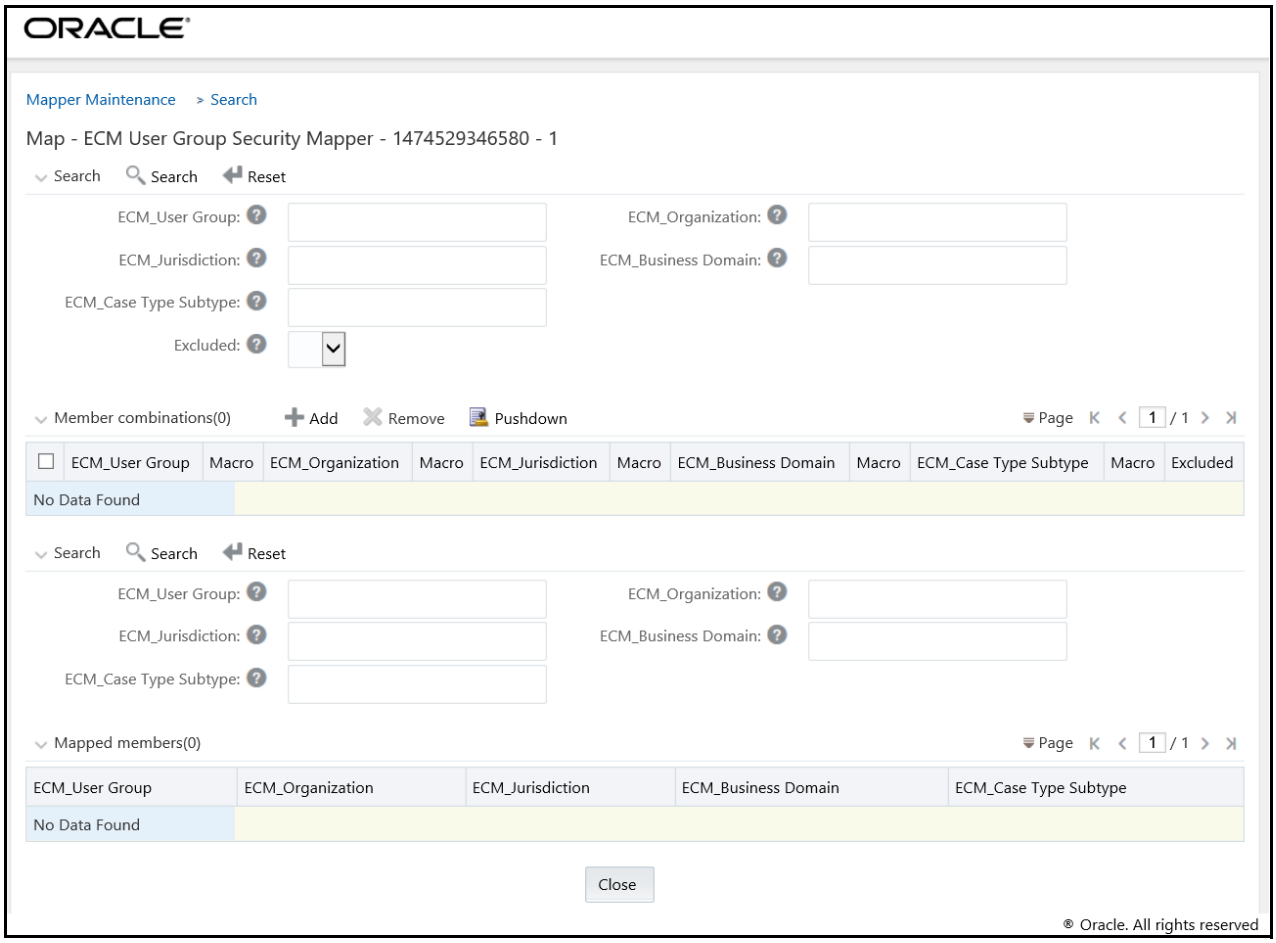


Figure 15. User Group Security Mapper window

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 Organizations 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 the 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 hierarchy and click **Go**. Click **Save**.
8. Click **Save**. You are directed to the previous screen, where the Member combinations can be viewed. All the changes get 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 the KDD_REVIEW_OWNER table and other control access mapping tables, you need to run the ECM Security Batch.

Note: If you are creating a new user, then perform the security mapping for that user and again execute the ECM_SECURITY_BATCH.

- 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 the 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 an 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 the 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.

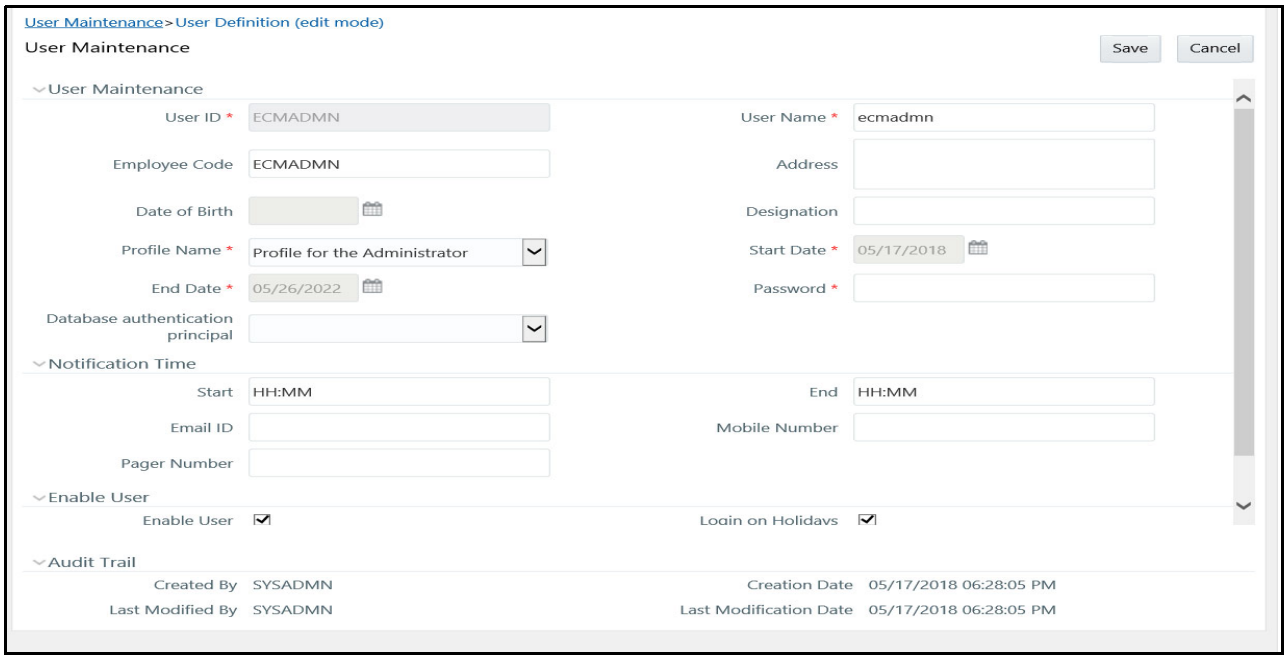


Figure 16. Batch Execution

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 on 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 the 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.

Mapping Read-Only Case type

If you need Read-Only access to certain Case types, then add an entry in KDD_REVIEW_OWNER_CSETYP_RDONLY table against the Case type.

CHAPTER 4 Pre-batch Execution Configuration

This chapter provides the details of pre-batch configuration activities.

Configure the following before executing a batch:

Step 1: Configuring Processing Group

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 SOURCE or MAN. For example, E2E BATCH ALL SOURCE and MAN are the group names provide in the table FCC_PROCESSING_GROUP. N_GROUP_ID should be the next greater numeric value.

Table 11. 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 the 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 the Start Batch run is executed, it loads the data into the FCC_BATCH_RUN table.

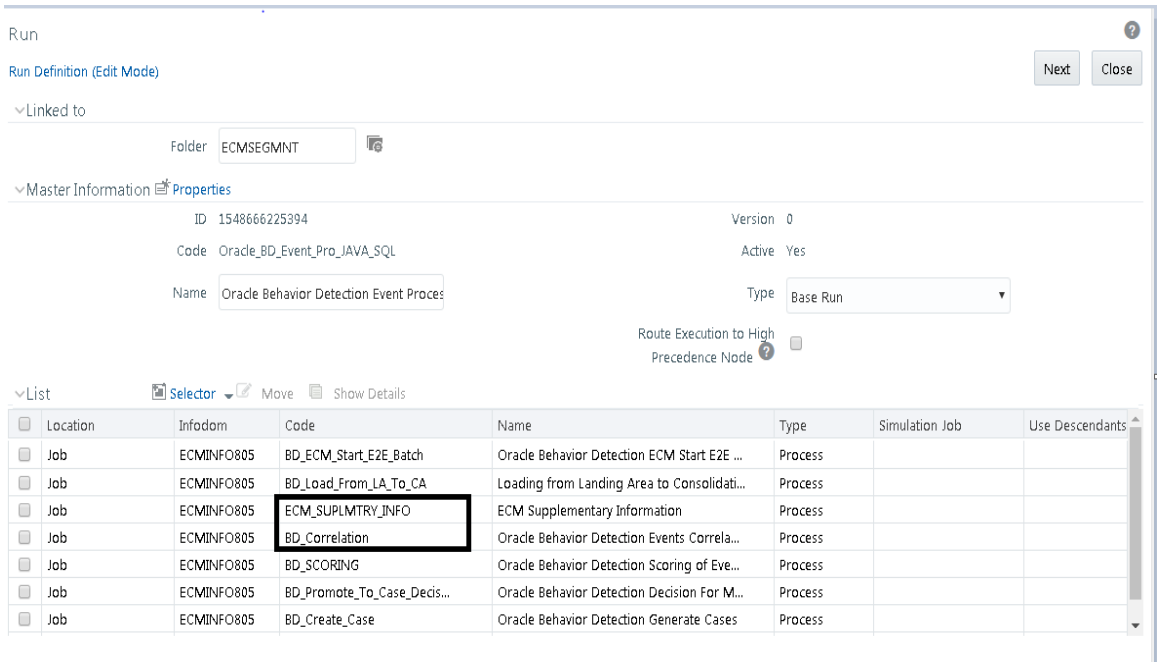
Step 2: Configuring Correlation

Note: From ECM 8.0.7.0.0 onwards, the default correlation is PGX.

PGX correlation does the same job as JAVA/SQL correlation (BD_Correlation) do, but further drill down approach. It helps us to identify all the relationships between the entities and present it in a graph.

If you want to use **BD_Correlation** process, then follow the below steps:

1. Remove the PGX Process.
2. Add the **BD_Correlation** process. Refer to below screenshot.
3. Trigger the batch.



1. **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:

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

2. **Configuring Correlation Rules**

After events are correlated to business entities, the event-to-business entity relationships are 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 12. 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	Yes
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	No
F_LOOKBACK_PROCESS_IND		NUMBER	Yes
V_CASE_TITTLE_RULE		VARCHAR2	Yes

- N_CORRELATION_RULE_SKEY *(required)*: This is the correlation rule unique Identification number.
- V_RULE_NAME *(required)*: Defines the name of the 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._CT > 2. The set of supported comparison operators are: =, !=, <, >, <=, >=, IN, and NOT IN.
- 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 the 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 lookback period.
- Do not use a unitless 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 the case. If this is set to Y, then multiple events are linked if they have a common business entity and promoted to the 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 the processing date is picked. If this is set to 0, then the 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.

- V_CASE_TITTLE_RULE: This is used for defining the title of the case.

Step 3: Configuring Ending Batch Process

1. 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 the ECM batch run. This chapter includes the following sections:

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

Note: Users should configure their own batches and default OOB should not be run as it is a sample run.

Starting a Batch Run

Note: For executing a batch, you cannot start two batches simultaneously for the 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.

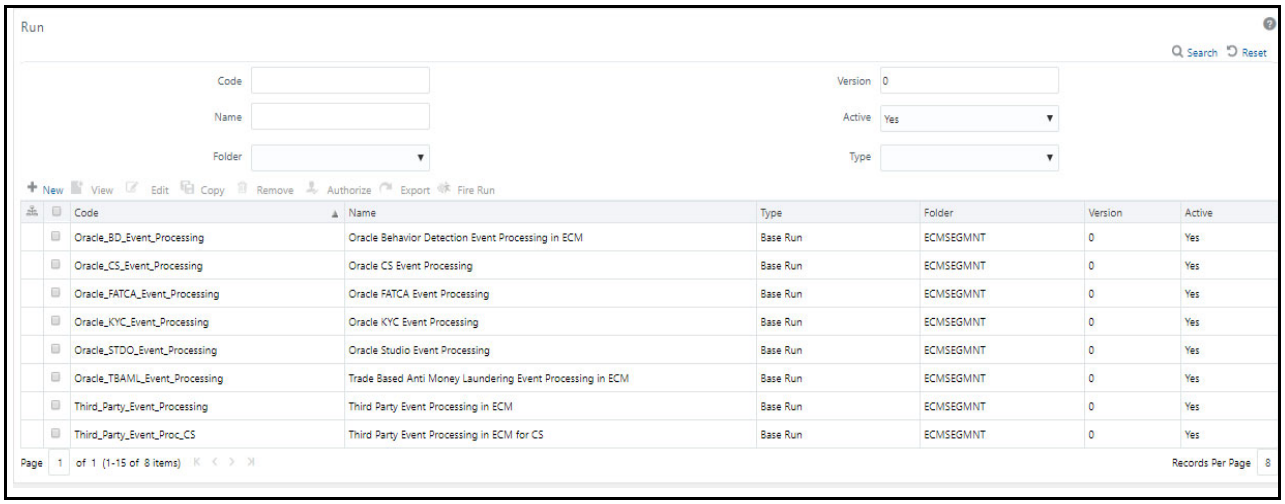


Figure 17. Application List

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

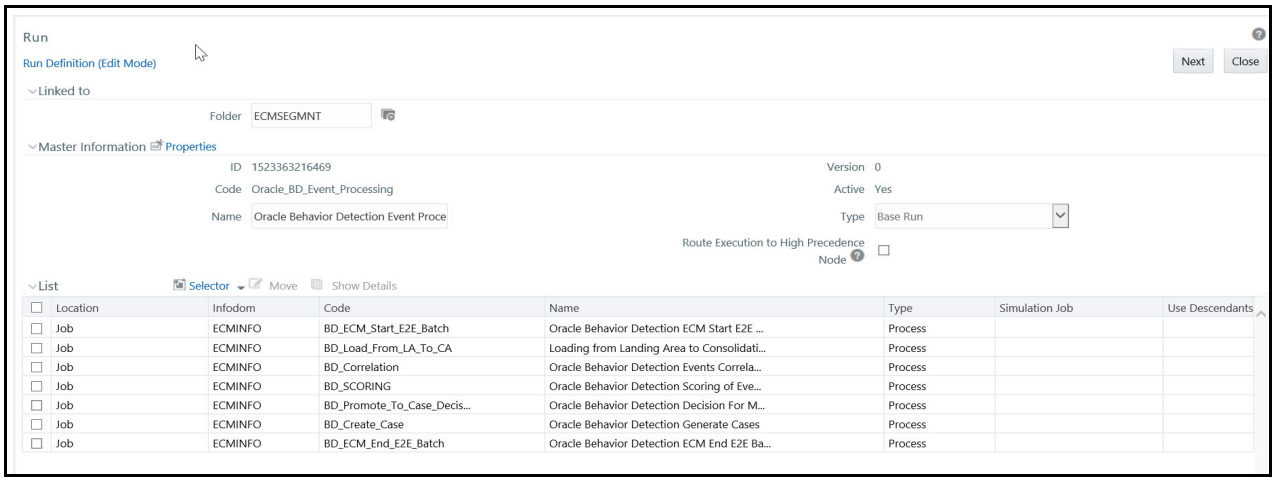
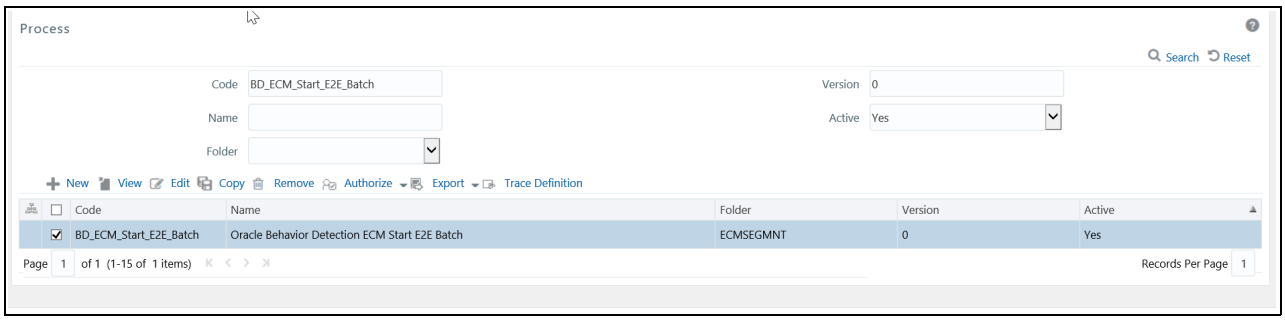
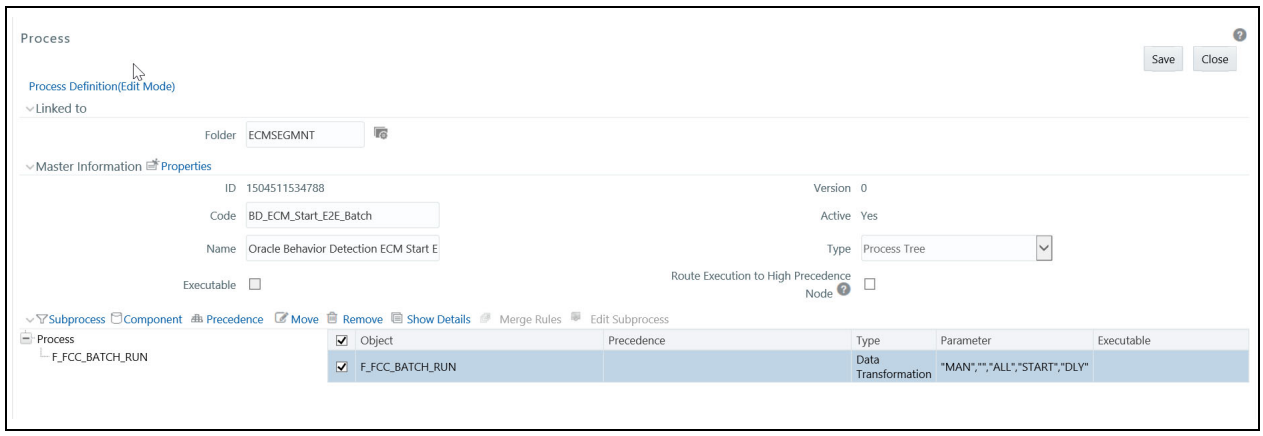


Figure 18. List of Processes

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.**



7. The Process Definition page is displayed.



8. Click **Component.** The Component Selector window is displayed.
9. Click **Parameters** option. The Parameters window is displayed.

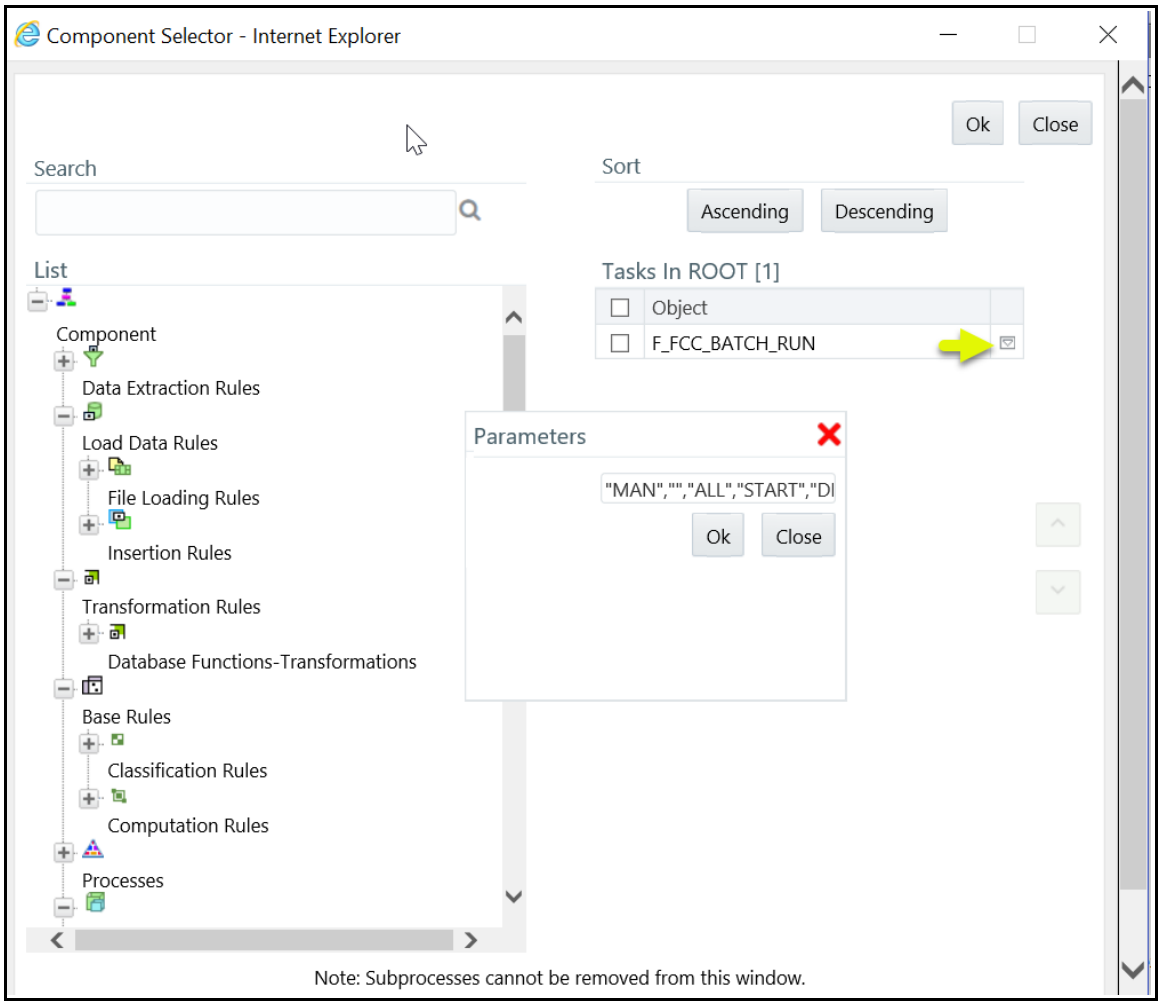


Figure 19. Parameters

The following are default parameters:

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

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

10. 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`.

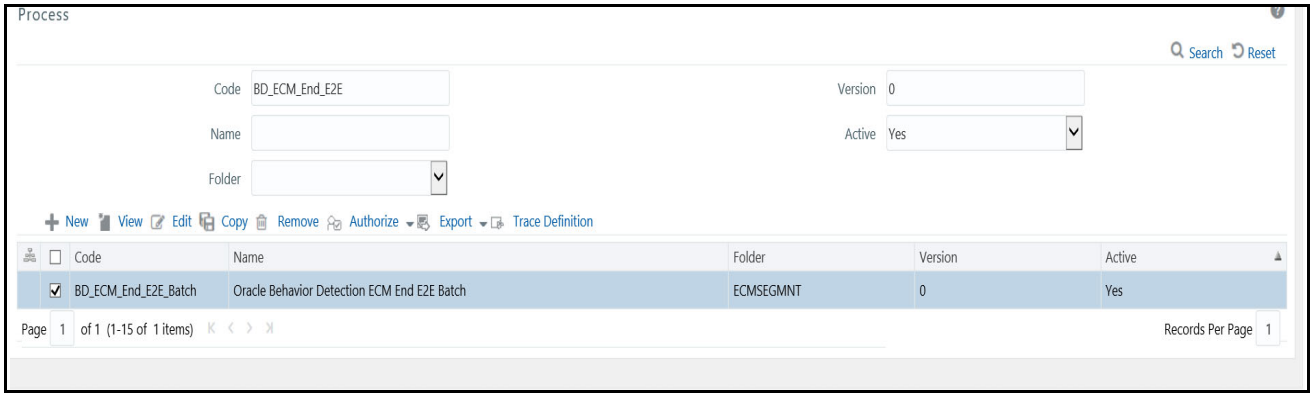


Figure 20. Application Batch List

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.

Note: If you have 10 days of data, then the ECM batch has to be executed from day-01 onwards.

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.

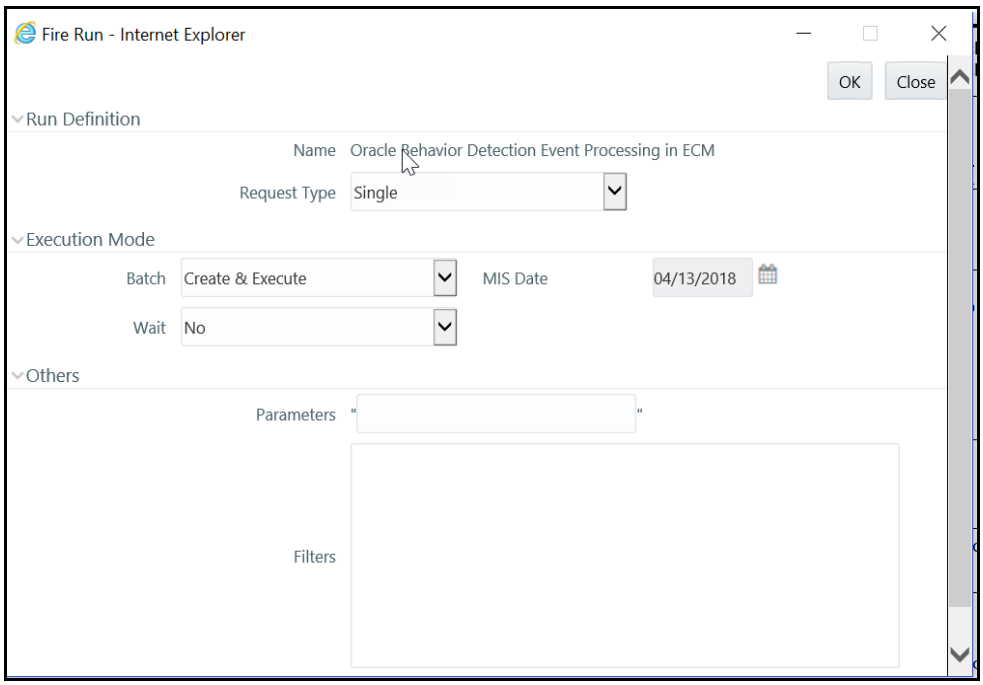


Figure 21. Fire Run

5. Enter the following details:

Table 13. 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
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:** $MISDATE option can be used to execute the run for that particular day. The format for it to enter the filter details is: `to_date(<ACTIVITY_TABLE_NAME>.<ACTIVITY_DT_COL>)=$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 the 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 the 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 the required process code. For example, BD_Correlation. For more information on using correlation, see *Configuring Correlation*.
   d. Perform scoring on correlated events and select the 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 the 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 the required process code. For example, BD_Create_Case.
   g. End ECM batch and select the 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 14. Application Run processes

Process	Applications and Process Name						
	OBD	**OCS**	**OFATCA**	**OKYC**	**OTBAML**	**OSTDO**	**Third-party**
Start ECM batch	BD_ECM_Start_E2E_Batch	ECM_Start_E2E_Batch_For_CS	ECM_Start_E2E_Batch_For_FATCA	ECM Start E2E Batch For KYC	TBAML_ECM_Start_E2E_Batch	STDO_ECM_Start_E2E_Batch	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_FATCA_To_CA	Load_From_OKYC_To_CA	TBAML_Load_From_LA_To_CA	STDO_Load_From_LA_To_CA	Load_From_LA_To_CA
Perform correlation on loaded events	BD_Correlation	Correlation	Correlation	Correlation	TBAML_Correlation	STDO_Correlation	Correlation
Perform scoring on correlated events	BD_SCORING	Scoring_OCS	Scoring_FATCA	Scoring_OKYC	TBAML_SCORING	STDO_SCORING	Scoring
Decision to promote correlated events to a case	BD_Promote_To_Case_Decision	Promote_To_Case_Decision_OCS	Promote_To_Case_Decision_FATCA	Promote_To_Case_Decision_OKYC	TBAML_Promote_To_Case_Decision	STDO_Promote_To_Case_Decision	Promote_To_Case_Decision
Create a case	BD_Create_Case	Create_Case	FATCA_Create_Case	Create_Case	TBAML_Create_Case	STDO_Create_Case	Create_Case
End ECM batch	BD_ECM_End_E2E_Batch	ECM_End_E2E_Batch_For_CS	ECM_End_E2E_Batch_For_FATCA	ECM_End_E2E_Batch_For_KYC	TBAML_ECM_End_E2E_Batch	STDO_ECM_End_E2E_Batch	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

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
- OSTDO
- Third-party
- FATCA
- TBAML

Using Connectors

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

- Loading OCS Data
- Loading FATCA Data
- Loading KYC Data
- Loading Studio Data
- 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.

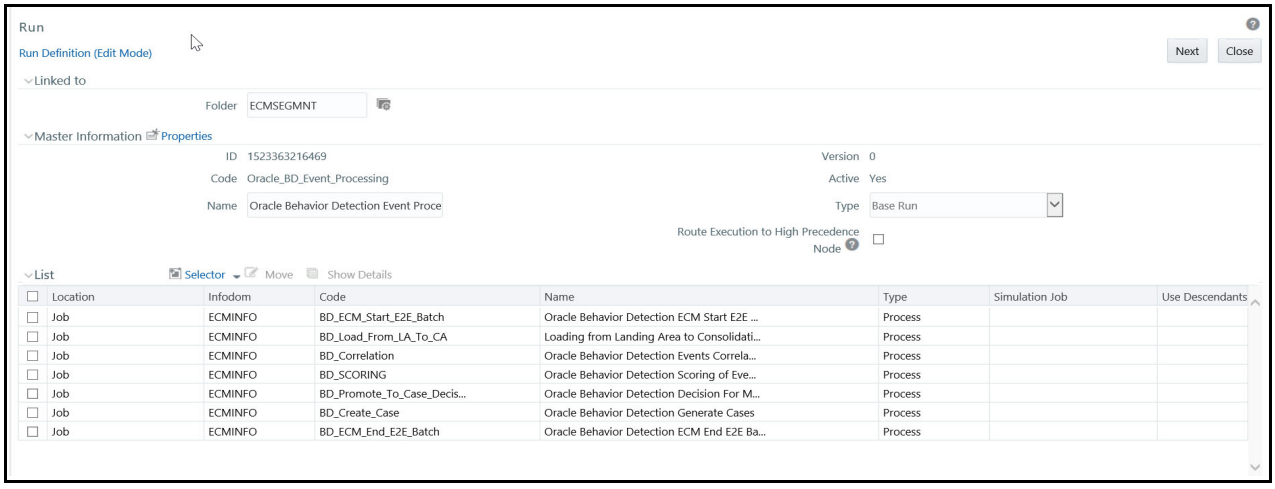


Figure 22. BD Processes

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 *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.

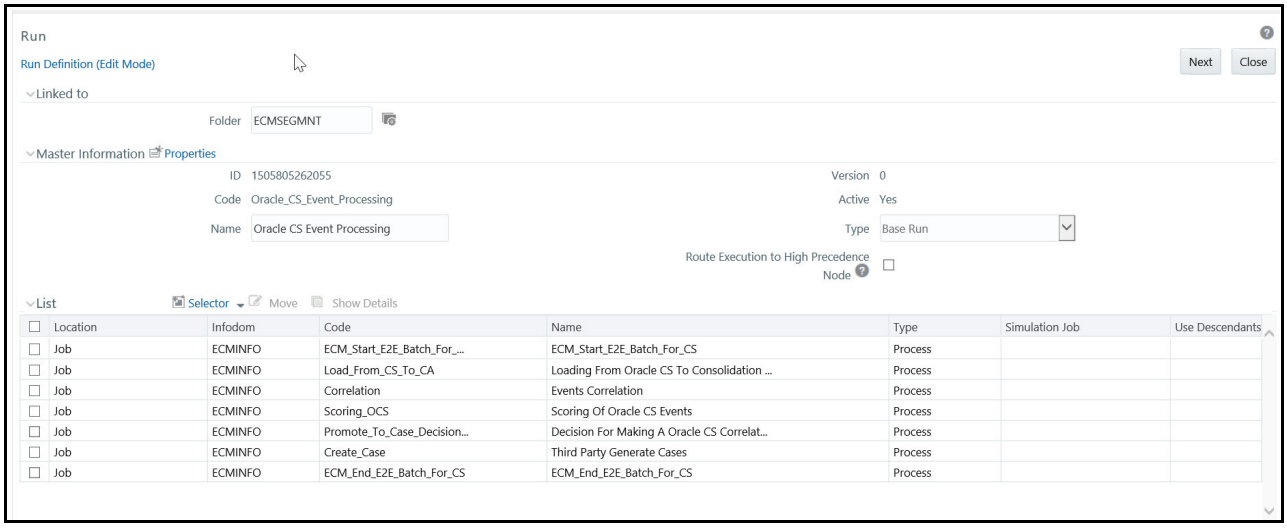


Figure 23. OCS Connector

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 *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 FATCA Data

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

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

1. Navigate to the Run window.
2. Go to the List section. Select **Oracle_FATCA_Event_Processing**. The list of processes for FATCA is displayed.

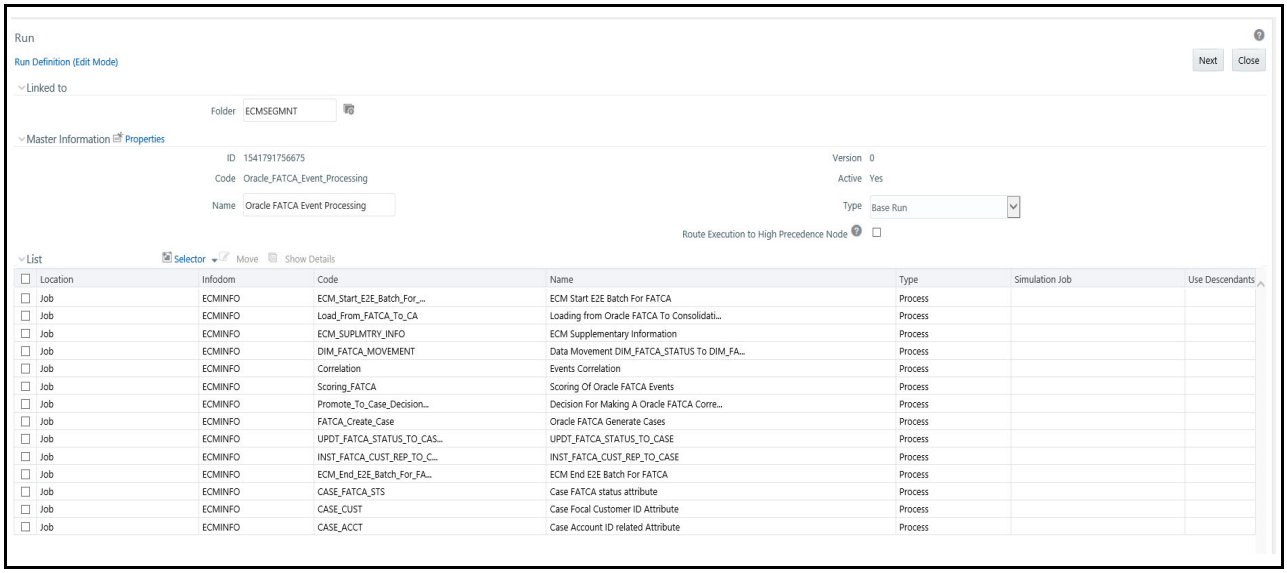


Figure 24. FATCA Connector

3. Select **Load_From_FATCA_To_CA** (connector) process from the list. This has the following four sub-processes:
   - Loading Oracle FATCA Events to Consolidation area
   - Entity Surrogate Key Generation For Oracle FATCA (to be executed after Loading Oracle FATCA Events sub-process.)
   - Evented Data Load for FATCA
   - Business Data Load for FATCA

For more information on processes and tasks, see *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.

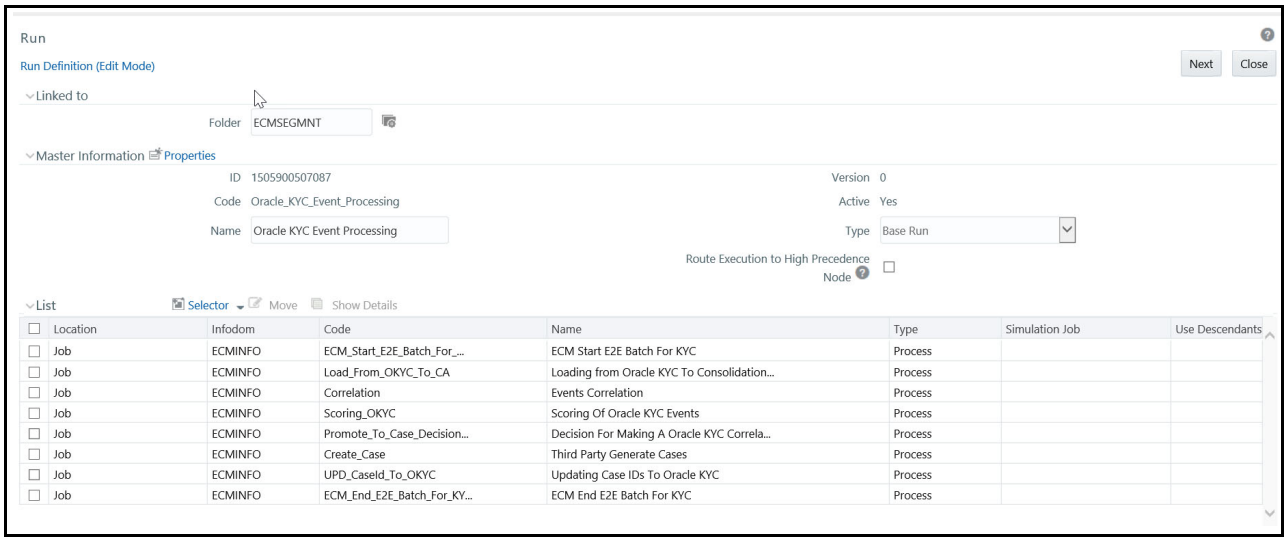


Figure 25. OKYC Connector

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 *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 TBAML Data

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

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

1. Navigate to the Run window.
2. Go to the List section. Select **Oracle_TBAML_Event_Processing**. The list of processes for TBAML is displayed.

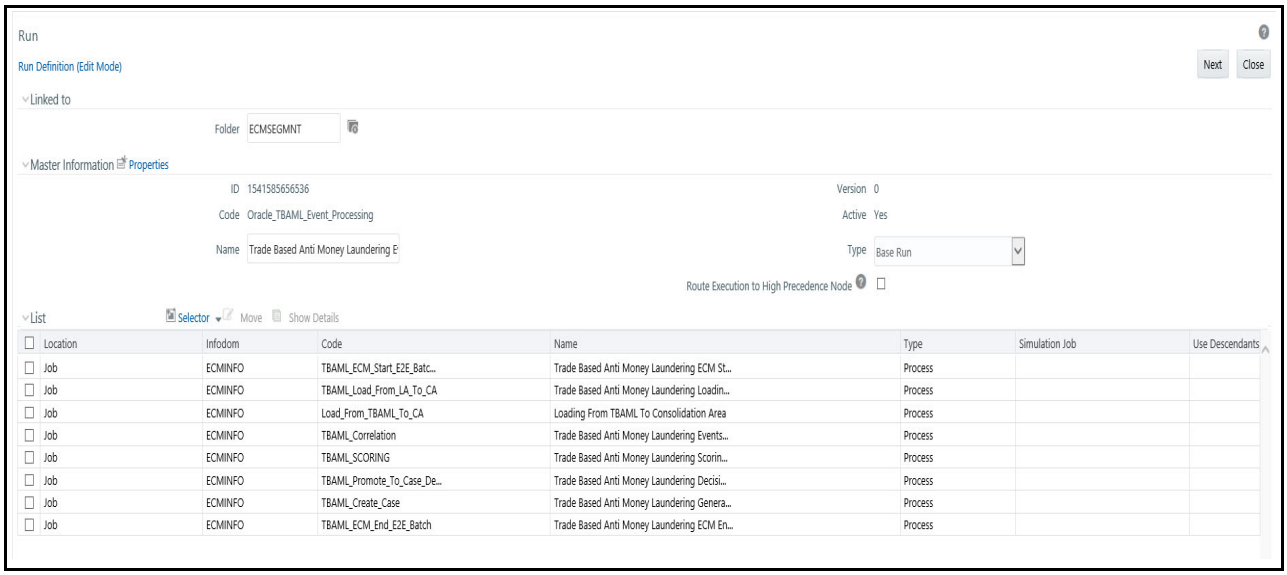


Figure 26. TBAML Connector

3. Select **Load_From_TBAML_To_CA** (connector) process from the list. This has the following four sub-processes:
   - Loading Oracle TBAML Events to Consolidation area
   - Entity Surrogate Key Generation For Oracle TBAML (to be executed after Loading Oracle TBAML Events sub-process.)
   - Evented Data Load for TBAML

For more information on processes and tasks, see *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 Studio Data

The STDO connectors are used to load data from the Studio application to the ECM.

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

1. Navigate to the Run window.
2. Go to the List section. Select **Oracle_STDO_Event_Processing**. The list of processes for Studio is displayed.

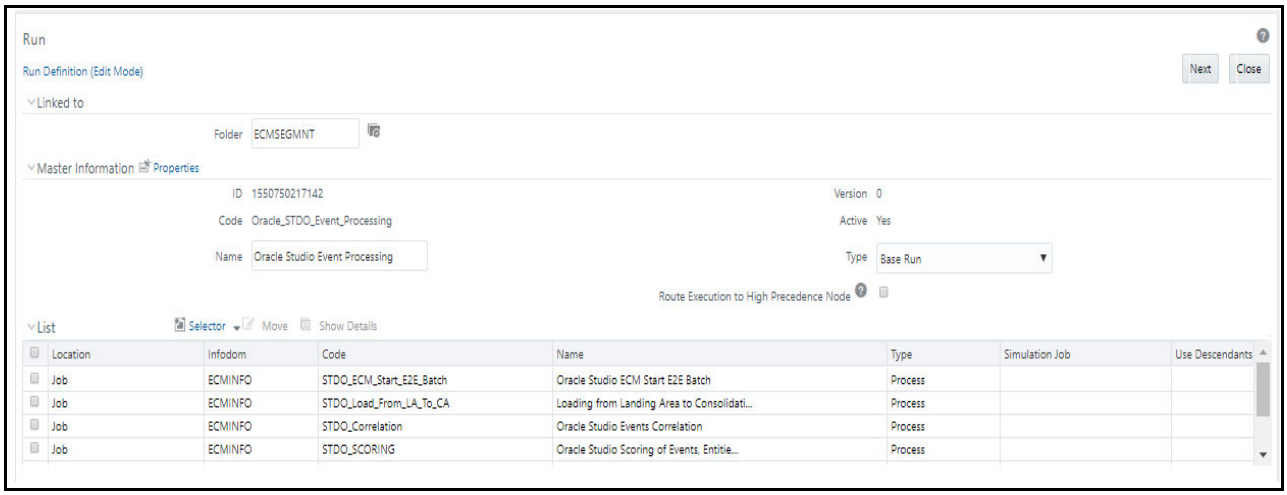


Figure 27. Studio Connector

3. Select **STDO_Load_From_LA_To_CA** (connector) process from the list. This has the following four sub-processes:
    - Loading Studio Events
    - Entity Surrogate Key Generation for Studio
    - Oracle Studio Business Data Load
    - Studio Supplementary Information
    - Oracle Studio Evented Data Load

Loading Third-party Connector Data

Third-party connectors are used to load data from the third-party application to the ECM.

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 processes for Third-party is displayed.

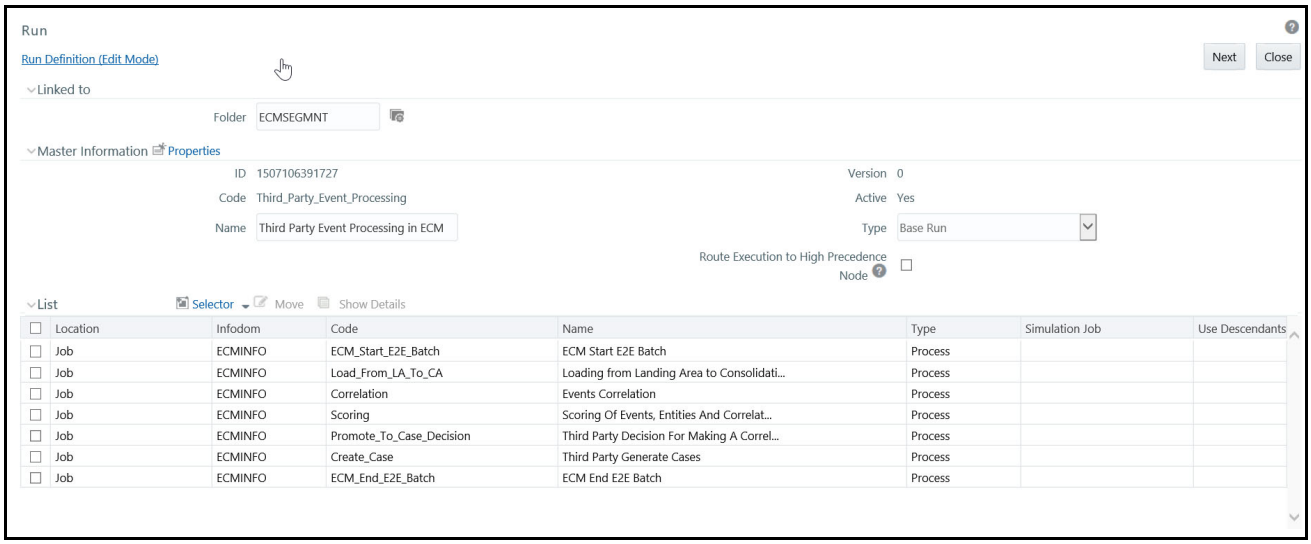


Figure 28. Third-party Connector

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 *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. This utility can be used for moving the data from landing area to the consolidation area. And, then consolidation area to UI (KDD Case tables, example KDD_CASE_CUSTOMER, KDD_CASE_ACCOUNT and so on.

- 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_DEFINITION and FCC_DM_MAPPING tables. Data is removed from the target is based on its PK/UK. Then the data is moved into the source table.
- **IS**: In this mode, Utility inserts the data from the 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 the source database

The structure of the DM definition table is as follows:

Table 15. 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 the Source table. It can contain the join conditions with multiple source tables and conditions associated with it. All source tables must be put under the 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 the source to target table.

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

Table 16. 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

Column Name	Primary Key	Column Type	Nullable
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
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 the 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
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 that occurred in the source or target database.

Configuring Data Movement from LA to CA

This section covers the following topics:

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, OFATCA, OTBAML, and Third-party. In the OOB process, you can run the

processes in parallel as well as in sequence. However, you can configure these processes based on your requirements.

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 the Business data movement. These OOB sample processes can be used only for reference purposes.

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 can be run in both parallel and 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 17. Sample Processes

Process Name	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 Summary, ● 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

Table 17. Sample Processes

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 Summary ● Oracle Behavior Detection to CA Account Email Address, and so on
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:

- The above process names are used for reference purpose.
- Process 1, 2, and 3 are designed based on similar entity bucketed into one process.
- Process 4, 5, 6, and 7 are designed based on the distribution of volume of data. For example, if Process4 has a huge volume of data compare to Process5, 6, and 7. You can design the process (business data movement) in such a way that the Process4 runs in parallel with Process5, internally, Process5, 6, and 7 can run in sequence.

Using the above sample processes, you can design entrie 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: 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.

Oracle Behavior Detection Sub-Processes

Sub Process (SP)	Description
SP1	Oracle Behavior Detection to CA Account
SP2	Oracle Behavior Detection to CA Account Address
SP3	Oracle Behavior Detection to CA Account Balance Position Summery
SP4	Oracle Behavior Detection to CA Account Email Address

Sub Process (SP)	Description
SP5	Oracle Behavior Detection to CA Customers
SP6	Oracle Behavior Detection to CA Customers Account
SP7	Oracle Behavior Detection to CA Customers Address
SP8	Oracle Behavior Detection to CA Customers Email Address

Sub Process (SP)	Description
SP9	Oracle Behavior Detection to CA Employee
SP10	Oracle Behavior Detection to CA Employee Address
SP11	Oracle Behavior Detection to CA Employee Email Address
SP12	Oracle Behavior Detection to CA Employee Phone

Figure 29. Oracle Behavior Detection processes

The following figure illustrates the Processes (1 to 9) designed using sub-processes (SP).

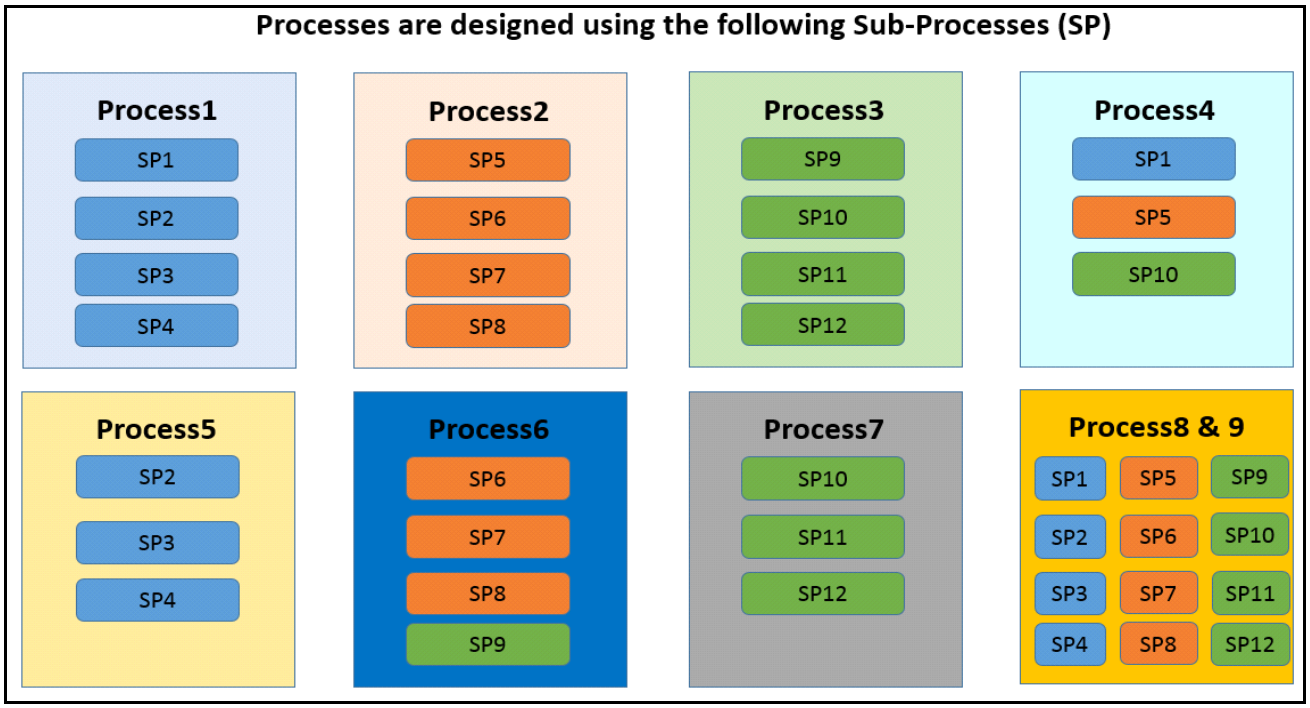


Figure 30. Oracle Behavior Detection Sub - processes

You can run Processes using the list of options shown in the following figure.

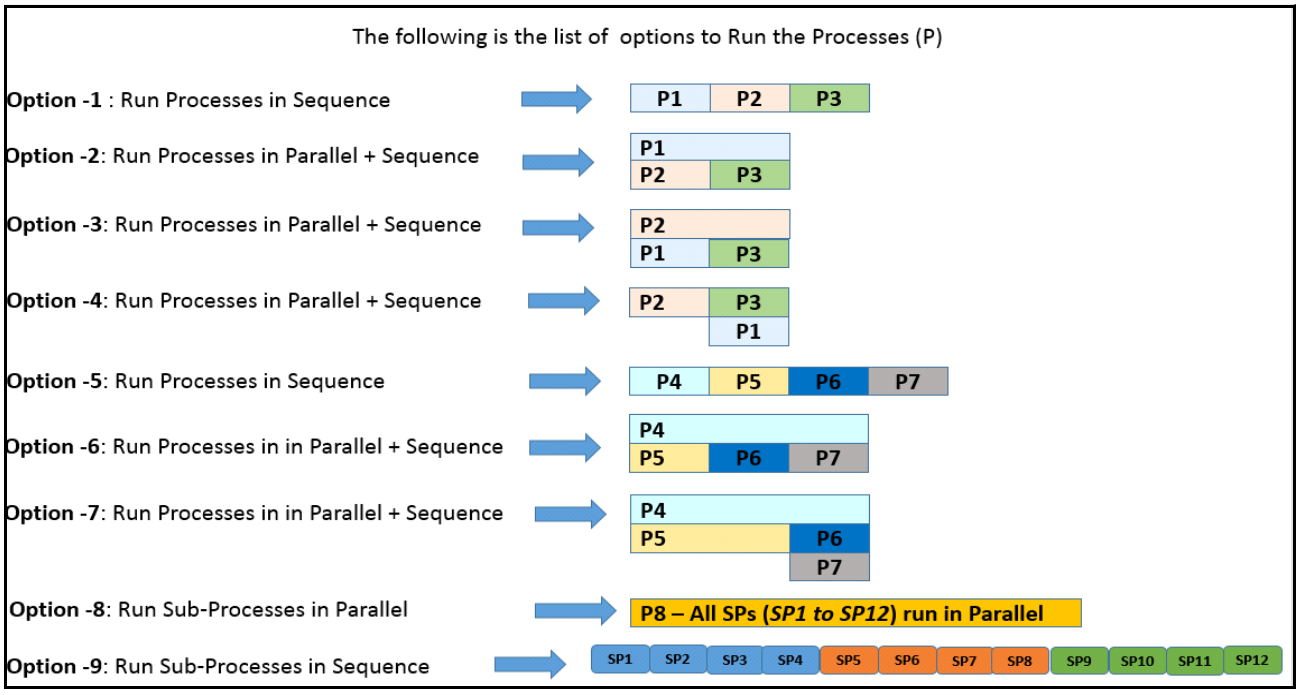


Figure 31. Options- processes

The following table provides a complete description of each options.

Table 18. 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.
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).

- The 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*.

CHAPTER 7 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, OFATCA, OTBAML, OSTDO 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 is identified for correlation-based on business entries in an application (BD, KYC, CS, FATCA, TBAML, OSTDO or Third-party).

Correlation can be performed for both manual events and real-time events.

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 of adding to it. The structure of the table is as follows:

Table 19. 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
_FOCUS_ID		NUMBER(10)	Yes

Table 19. FCC_CORR_BUS_ENTITY_PATH **(Metadata Table) (Continued)**

Column Name	Primary Key	Column Type	Nullable
V_ENTITY_TYPE		VARCHAR2(50)	Yes
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 the 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 _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 20. 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 the 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 s 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 is populated, this path configuration is considered for the case 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 case.

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 cases 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 that identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.
- **FATCA Correlation**: FATCA Groups events created in the past month based on a common correlated business entity. FATCA 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 that identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.
- **TBAML Correlation**: TBAML Groups events created in the past month based on a common correlated business entity. TBAML 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 that 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 that 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 that 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 that 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.

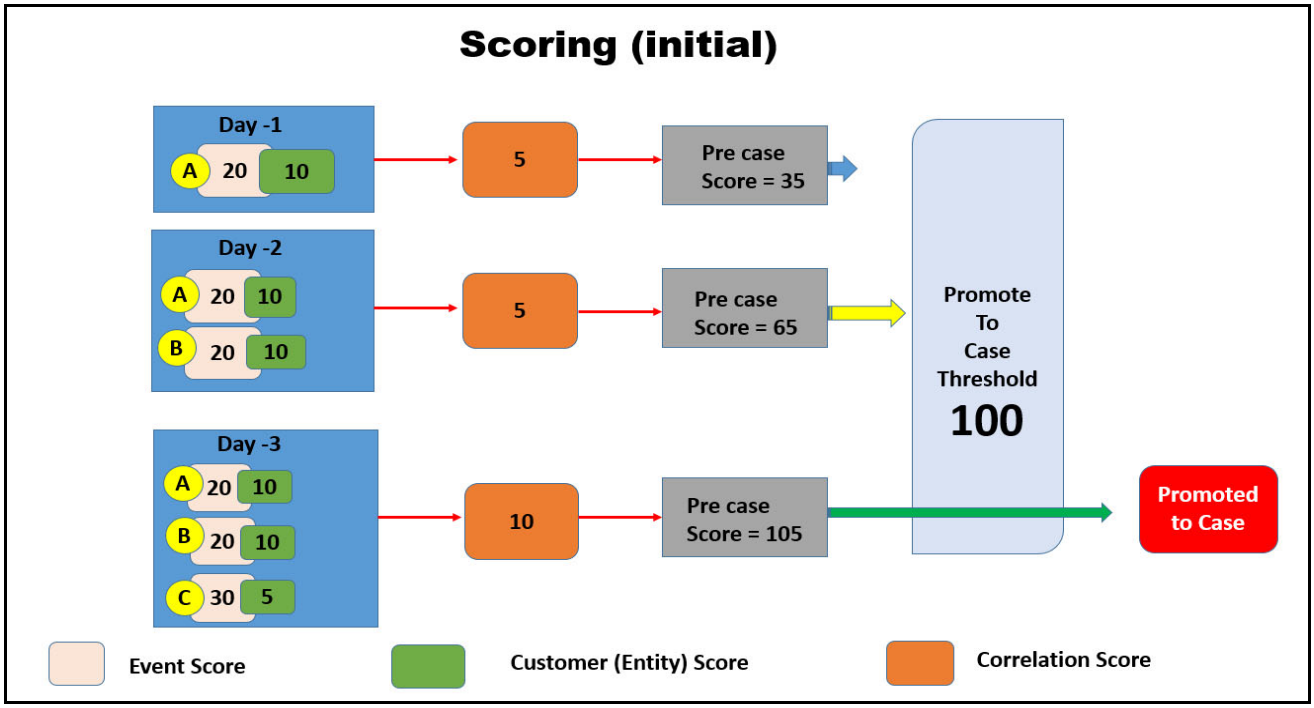


Figure 32. Initial Scoring

Table 21. 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 is 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 the case.

Adjustment Scoring

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

The following figure depicts the adjustment scoring process.

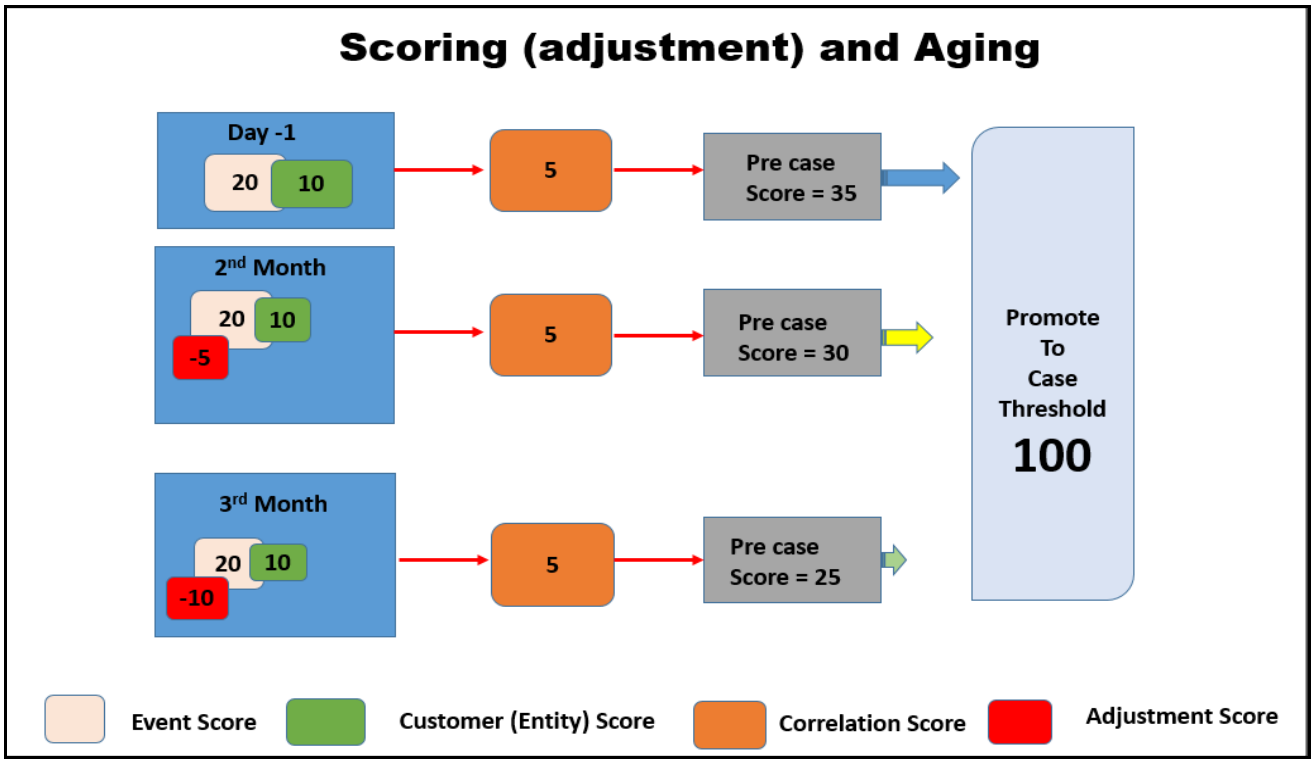


Figure 33. Adjustment Scoring

.

Table 22. 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, the 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, the 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, the Customer is the only entity. The Entity scoring is performed by entity rules defined in the IPE. You 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 the case.

Correlation Scoring

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

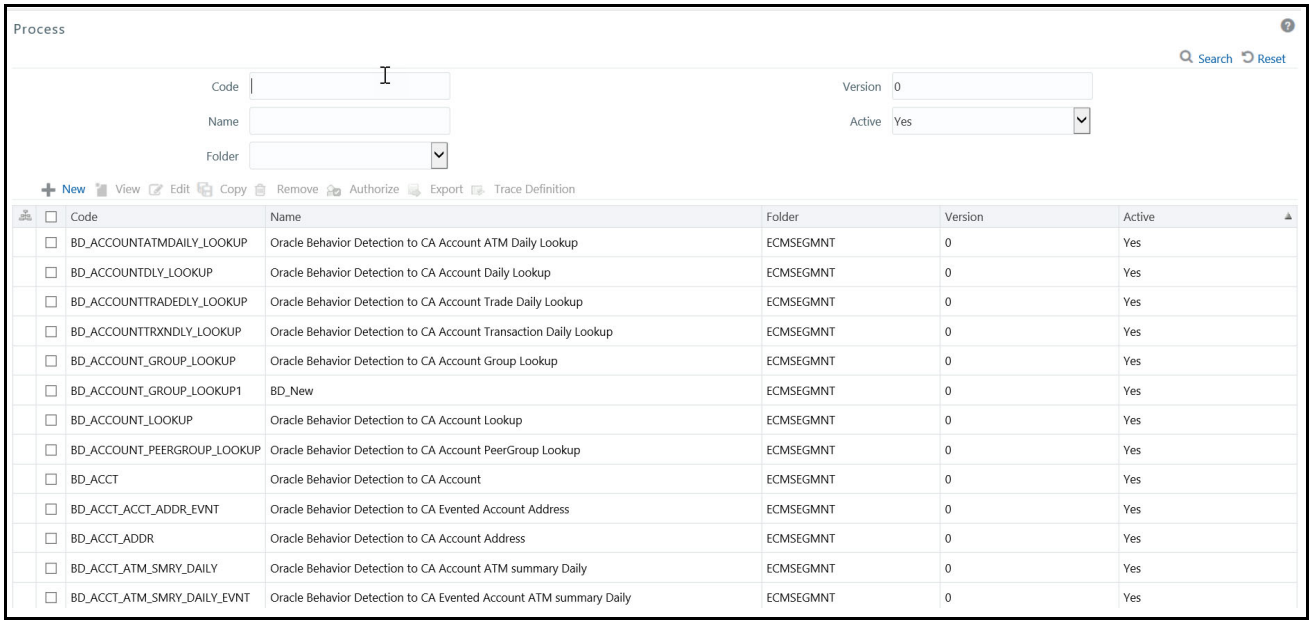
For more information configuring scores, see the *Inline Processing Engine User Guide*.

Configuring AML Event Initial Scoring

This section explains how to configure the initial scoring of the 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 34. Process Summary Window

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

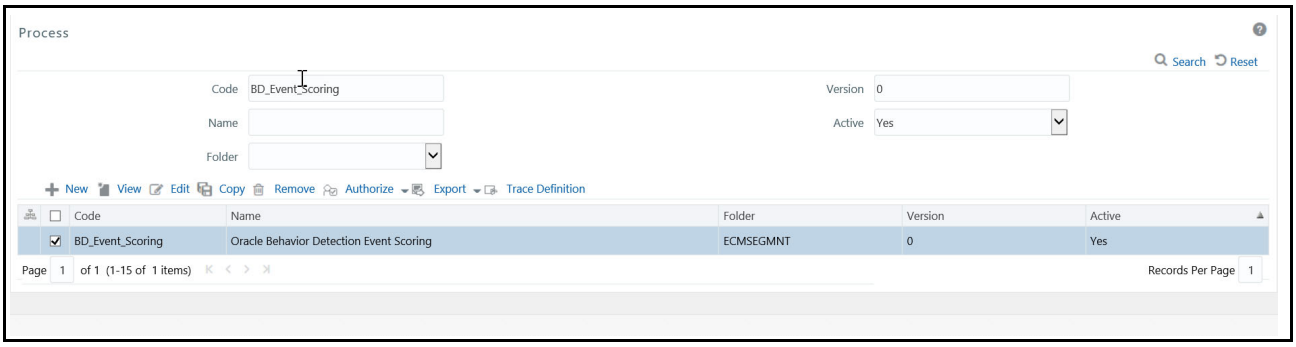


Figure 35. BD_Event_Scoring

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

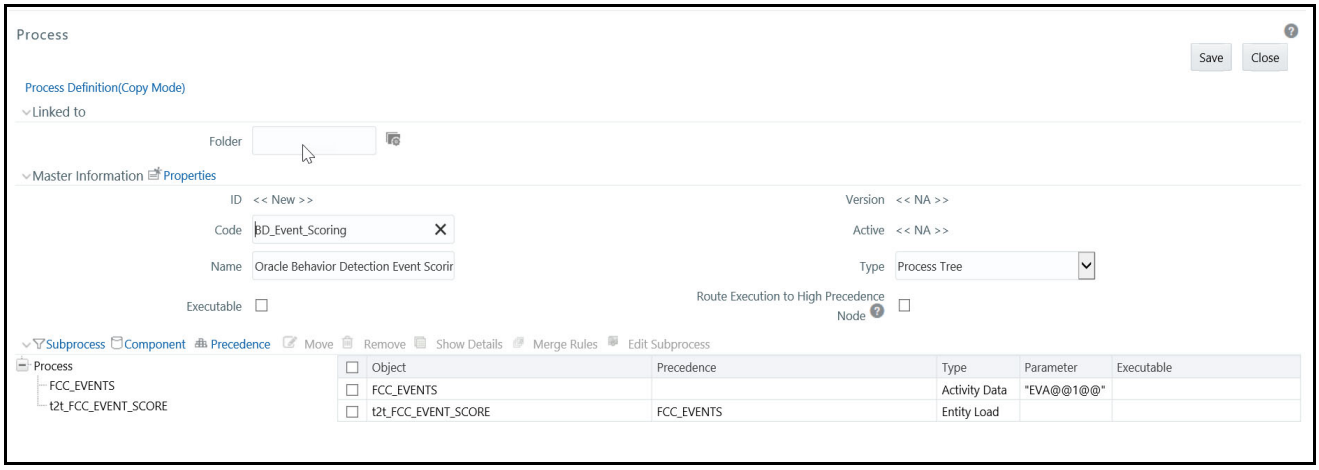


Figure 36. List of Tasks

6. Click **Components**.

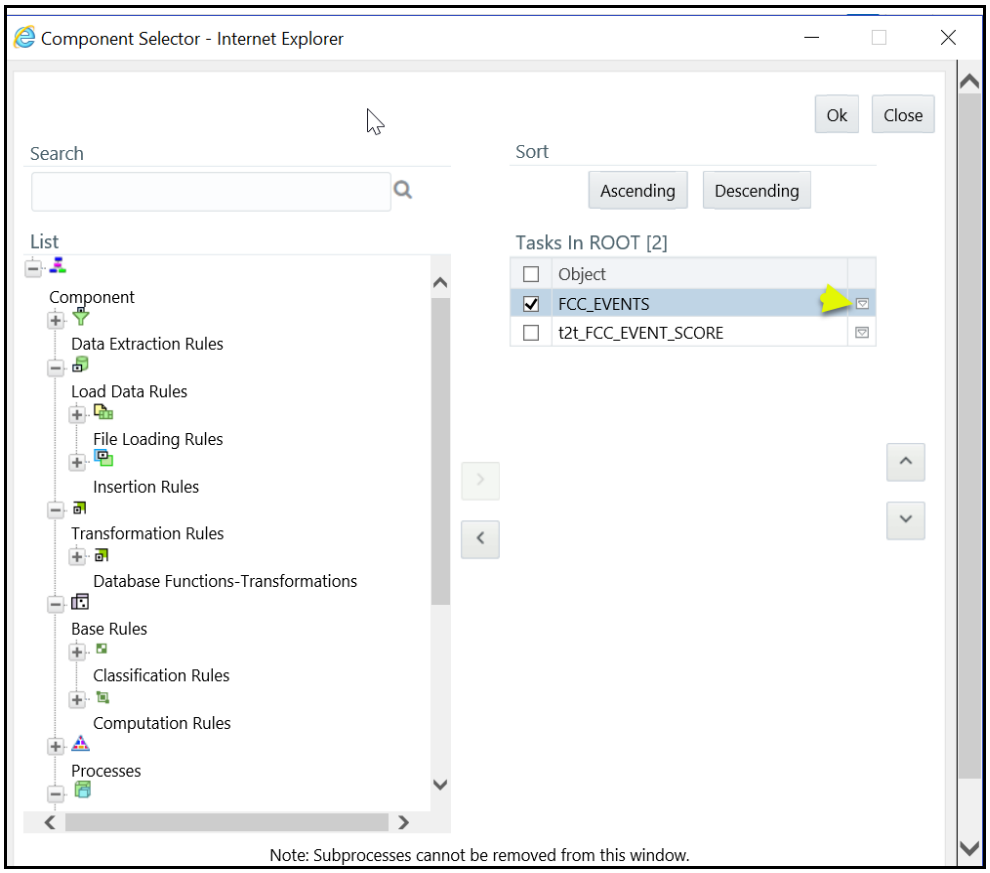


Figure 37. Components

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

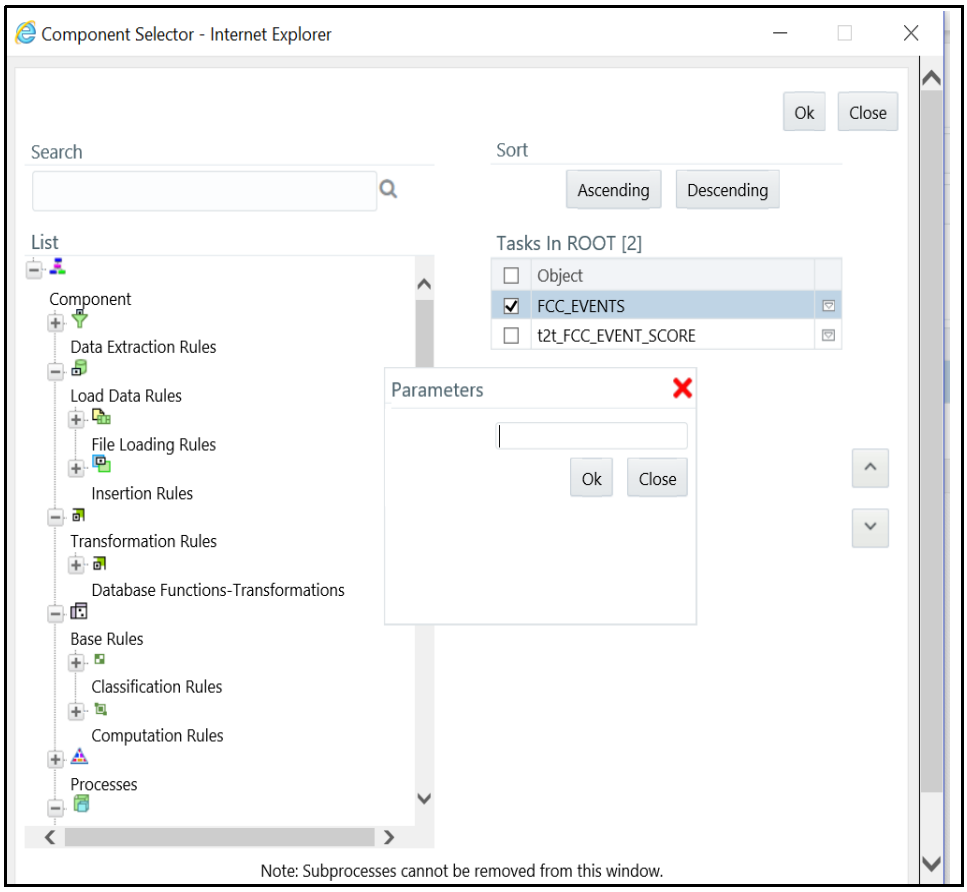
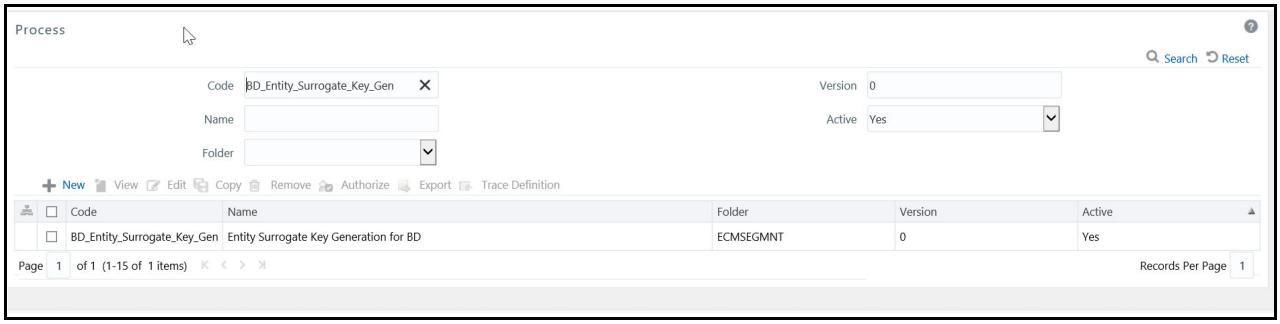


Figure 38. Parameters

8. Navigate to Process Summary window and search **BD_Entity_Surrogate_Key_Gen**.



9. The list of tasks is displayed. Click **Component.**

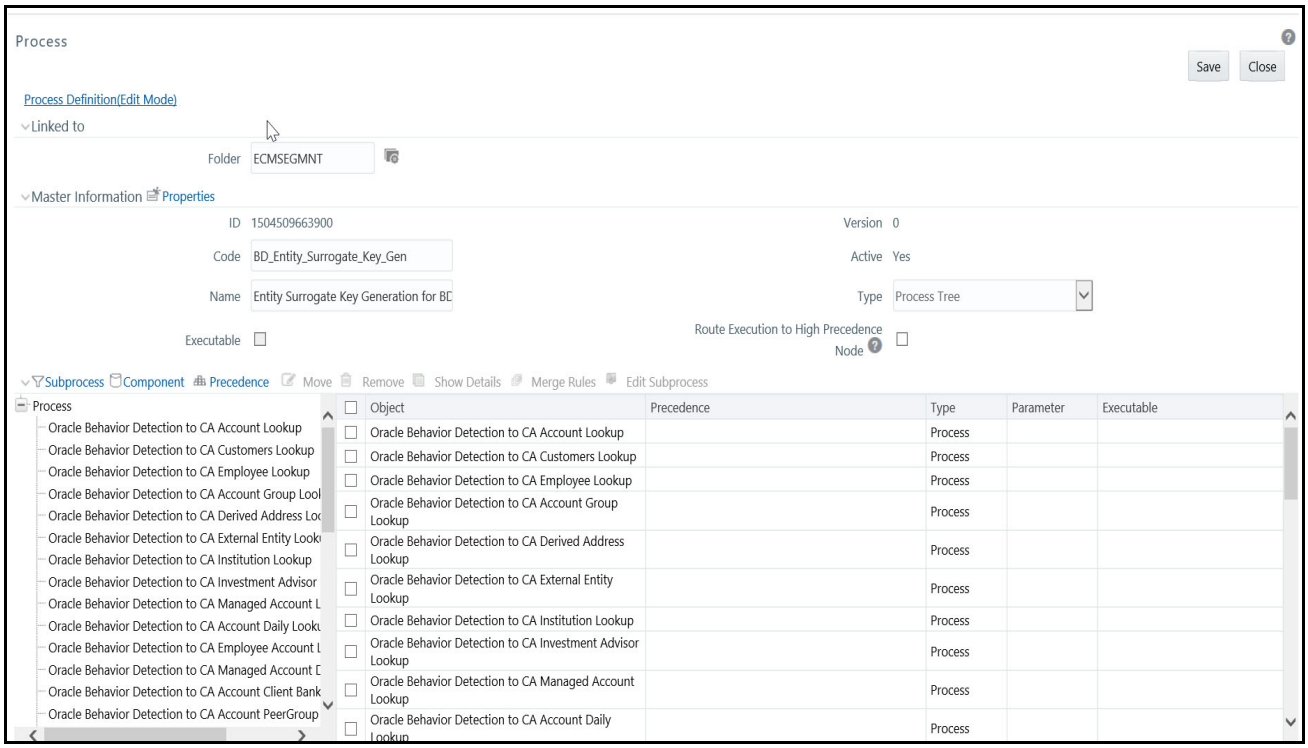


Figure 39. List of Tasks

10. Select **Oracle Behavior Detection to CA Event Scoring** and click OK.

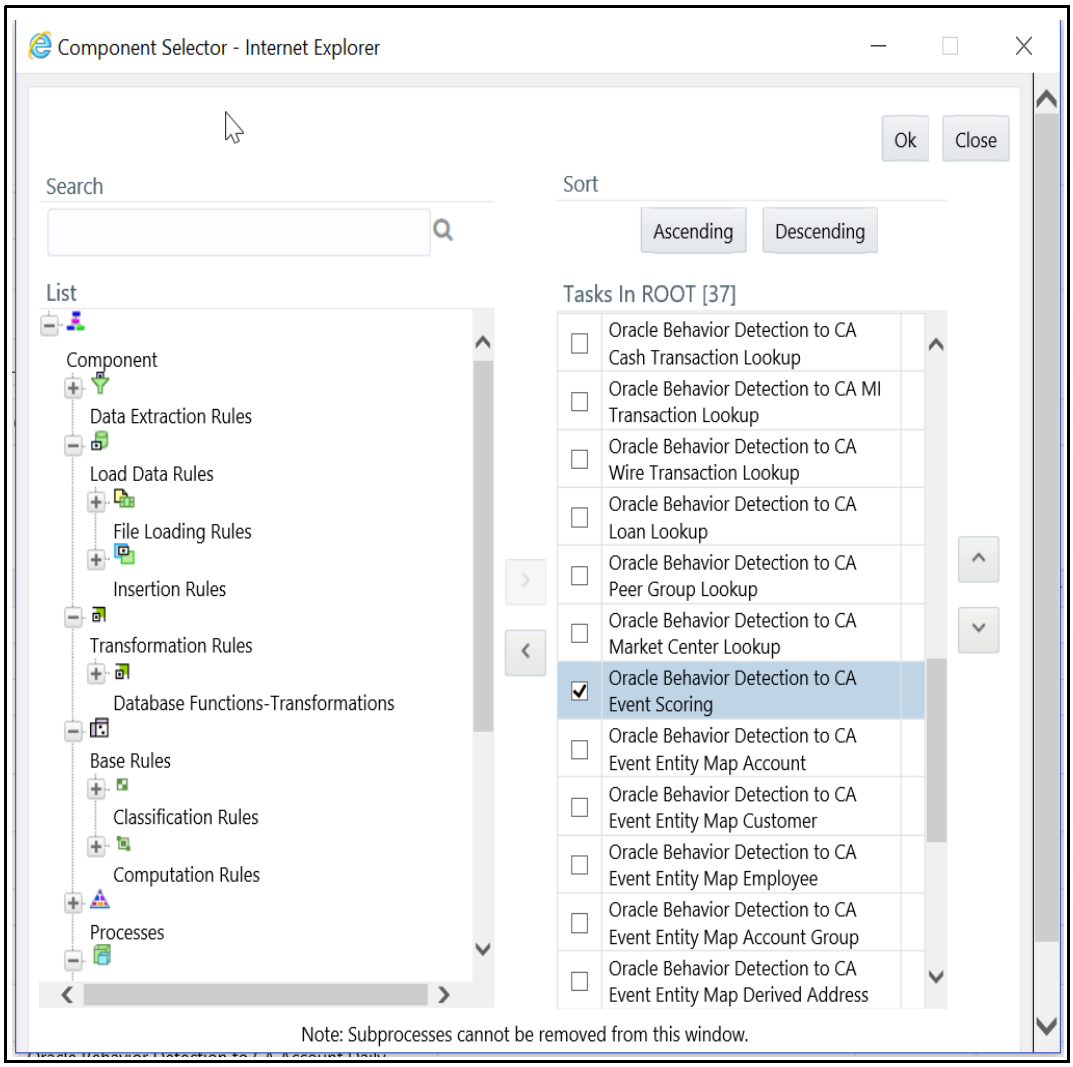


Figure 40. Deselecting of Oracle Behavior Detection to CA Event Scoring Process

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 the 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 the 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 a 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. The 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 a 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 the 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 a 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 the 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 the 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 the 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 the 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 the 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. The Score will be dropped to 0. And Event A will be closed and completely dropped from correlation. Event B is the only event in correlation and total pre-case score will be now 1.
- On 2nd Feb 2017 event B age is now 12 months. The 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. The scale should be configurable by effective risk and jurisdiction.

The total customer score contributes to pre-case.

For example,

- Set up the rule to find the KDD__CORR_LINK.BUS_NTITY_KEY_ID and KDD__CORR_LINK.BUS_NTITY_ID for an 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 creating 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 the 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 the 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

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

Combination of Scenarios

- When correlation contains events from scenario X and Scenario Y at the same time consider correlation to add a 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, the total of transactions across all correlated events is between 50K and 100K should give a 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 the total trxn amount (configurable to use a functional currency total trxn amount is scenario configured for it).
- The total 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 the 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 the same entity/same scenario within look back period. The number of events and lookback are configurable.
  - Increase score by 50 if 3 or more events created for the same entity/same scenario within look back period. The 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, the 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 the 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 is identified for correlation-based on business entries in an application, for example BD, CS, KYC, FATCA, TBAML, STDO, Third-party. This is performed based on the configurable set of rules. Once the correlation is defined, every entity will have event scoring, the entity will have entity scoring. Also, correlation scoring is performed. After scoring, an event can be promoted to the case if it crosses the defined 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 the case:

- BD
- CS
- KYC
- FATCA
- TBAML
- STDO
- Third-party

Once an event is promoted, an Administrator takes the decision for Pre-case to the 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 the 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 the **Business Processor.** The Business Processor page is displayed.
3. Click **Edit**. The Business Processor page is displayed.

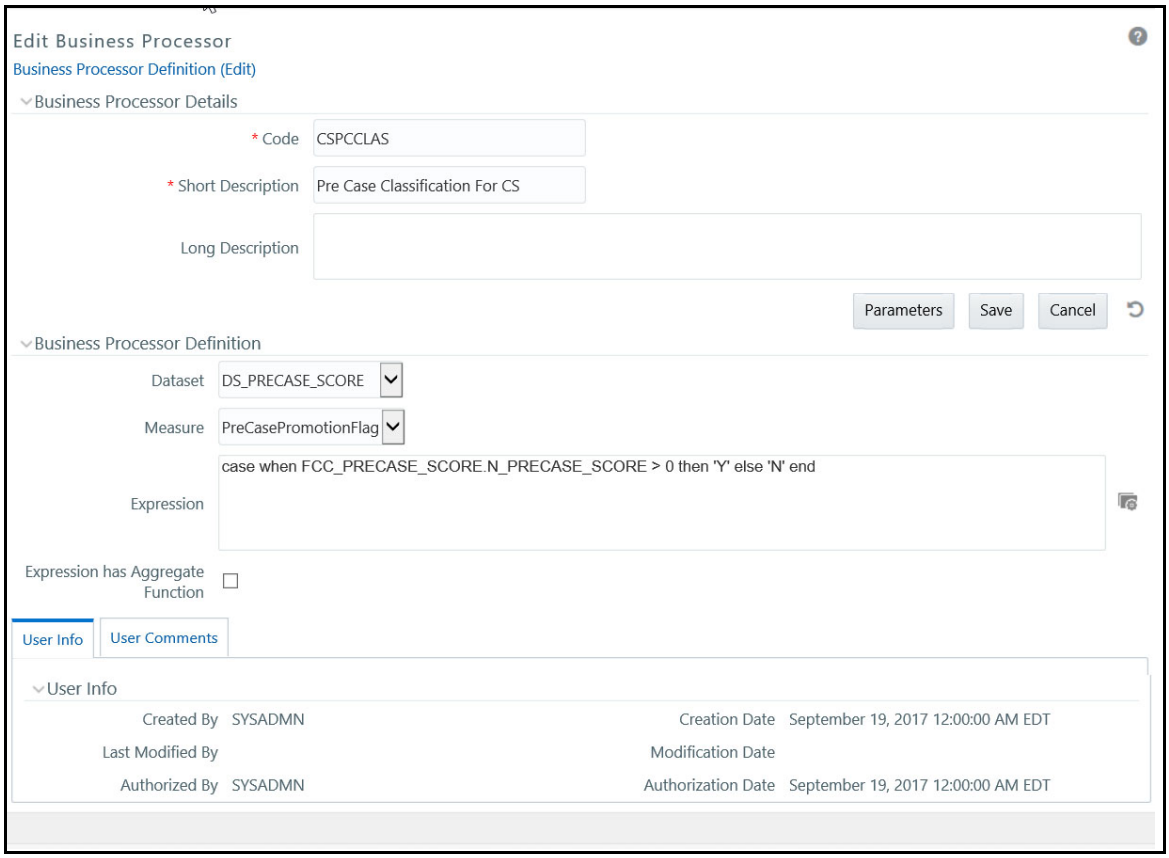


Figure 41. Adding Business Process

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

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 the 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

The ECM workflow follows various stages in the development lifecycle:

- **Modelling**: 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
- FATCA
- TBAML
- KYCOB

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 the 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 23. 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 the 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 24. 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 classpath is invoked to get the attribute values in this case.

2. Define the query for the attribute in V_ATTRIBUTE_VALUE1 column.

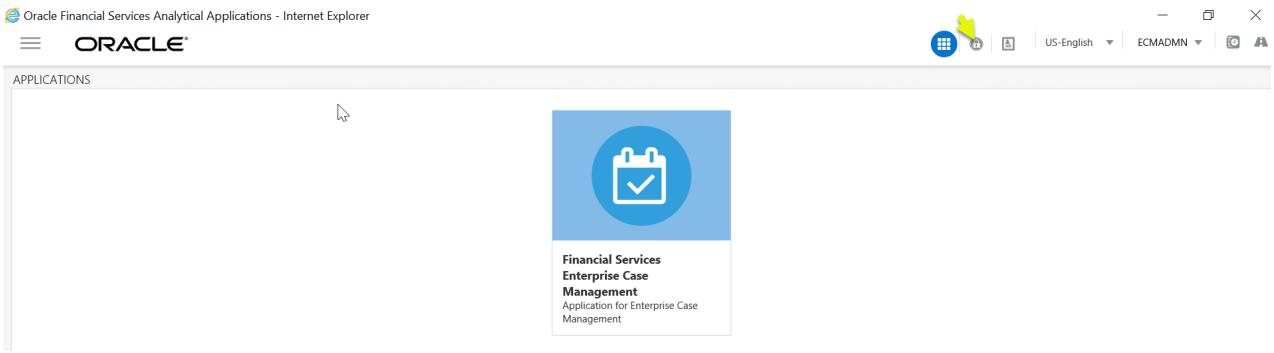
After the attribute is defined, you can access this using Application Rule "Attribute Expression". For more information, see the *Defining Application Rules* section.

Accessing Process Modeller

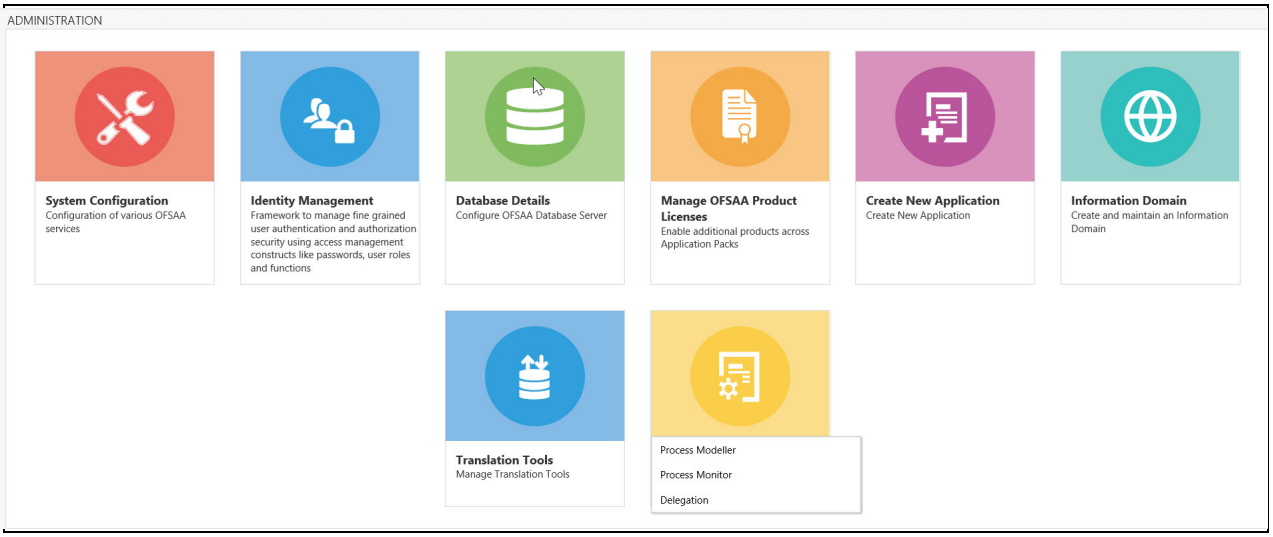
This section explains how to access the Process Modeller page.

To access the Process Modeller page, follow these steps:

1. Click Administration icon.



2. The Administration page is displayed. Click the **Process Modeller** option from **Process Modelling Framework**.



3. The Process Modeller window is displayed.

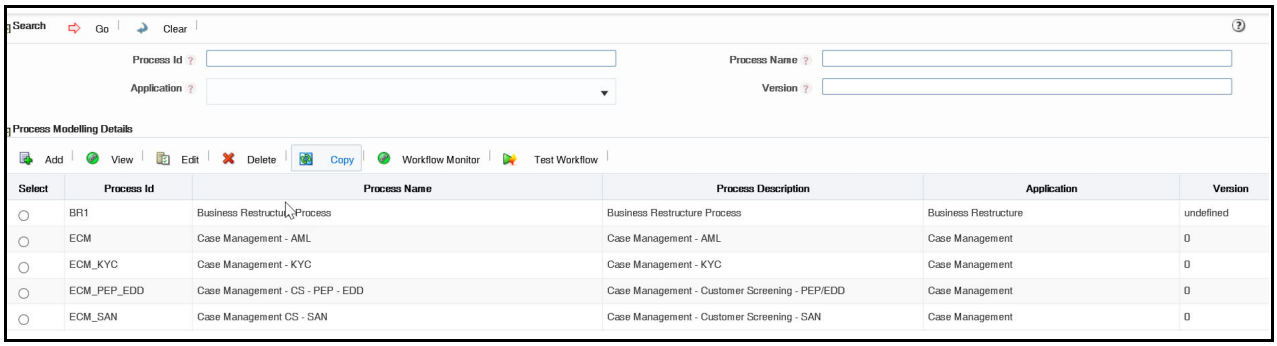


Figure 42. Process Modelling

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.

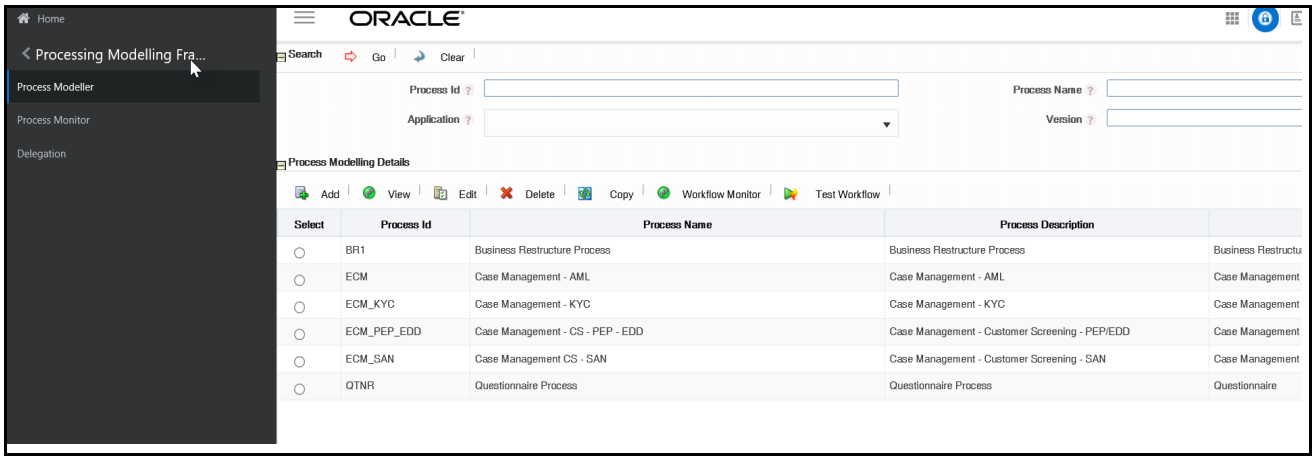


Figure 43. Process Modeller Window

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

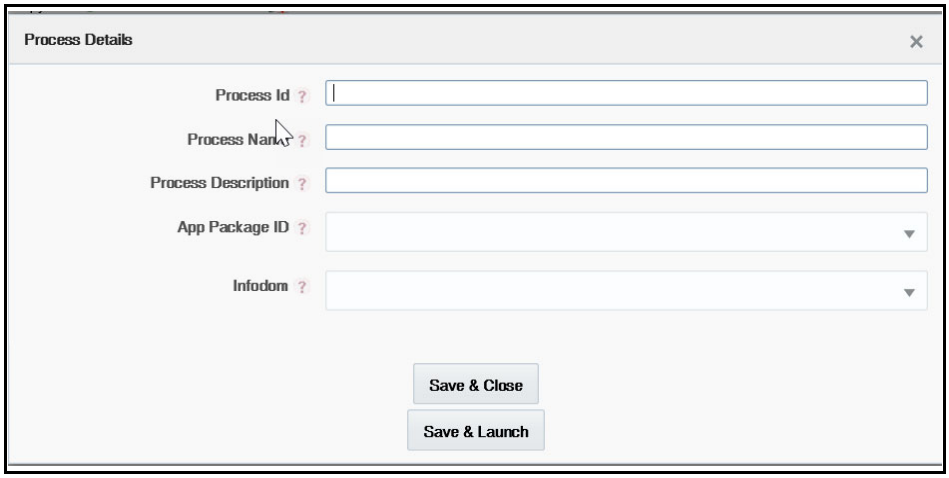


Figure 44. Process Details

3. Enter the following details in Process Details window:

Table 25. 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.

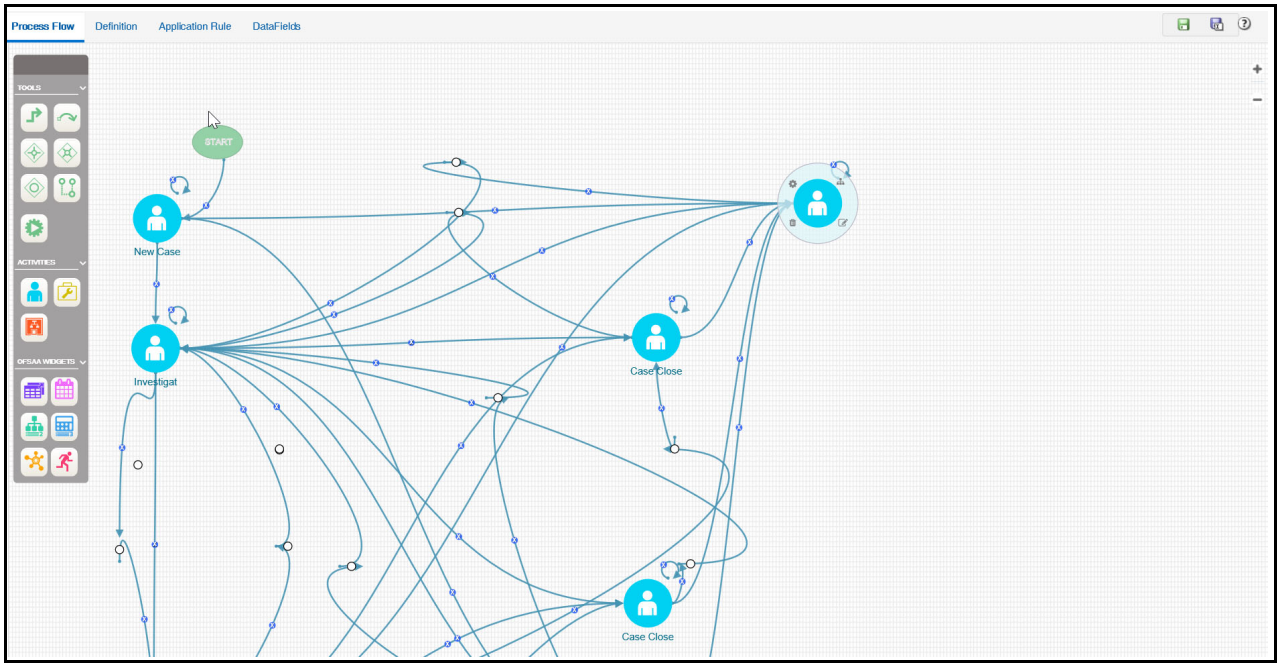


Figure 45. Process Modeller Editor window

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 the 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:

- Adding a Transition
- 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.

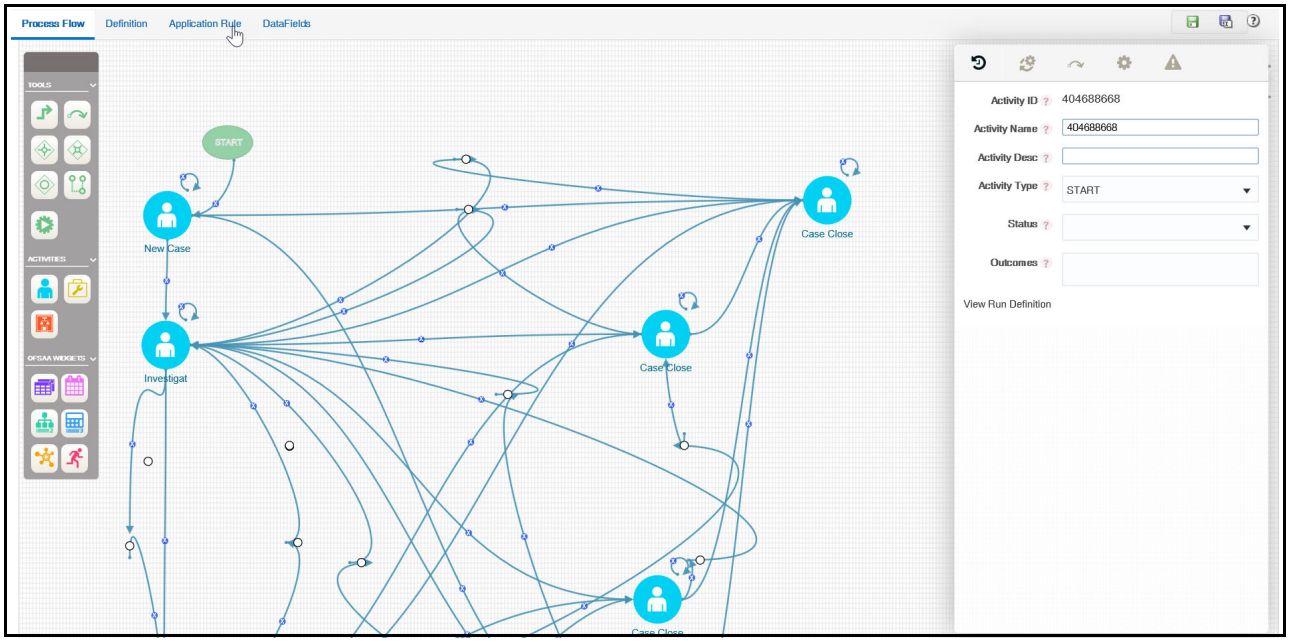


Figure 46. Starting Process

3. Enter the following information in the respective fields:

Table 26. Process

Field Name	Description
Activity ID	Displays the automatically generated Activity ID.
Activity Name	The activity name is displayed automatically the 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 the transition to the newly created process. For more information, see the *Adding Transition*.

Adding an Activity

To add an 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 27. 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 the 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, MultiChoice, 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

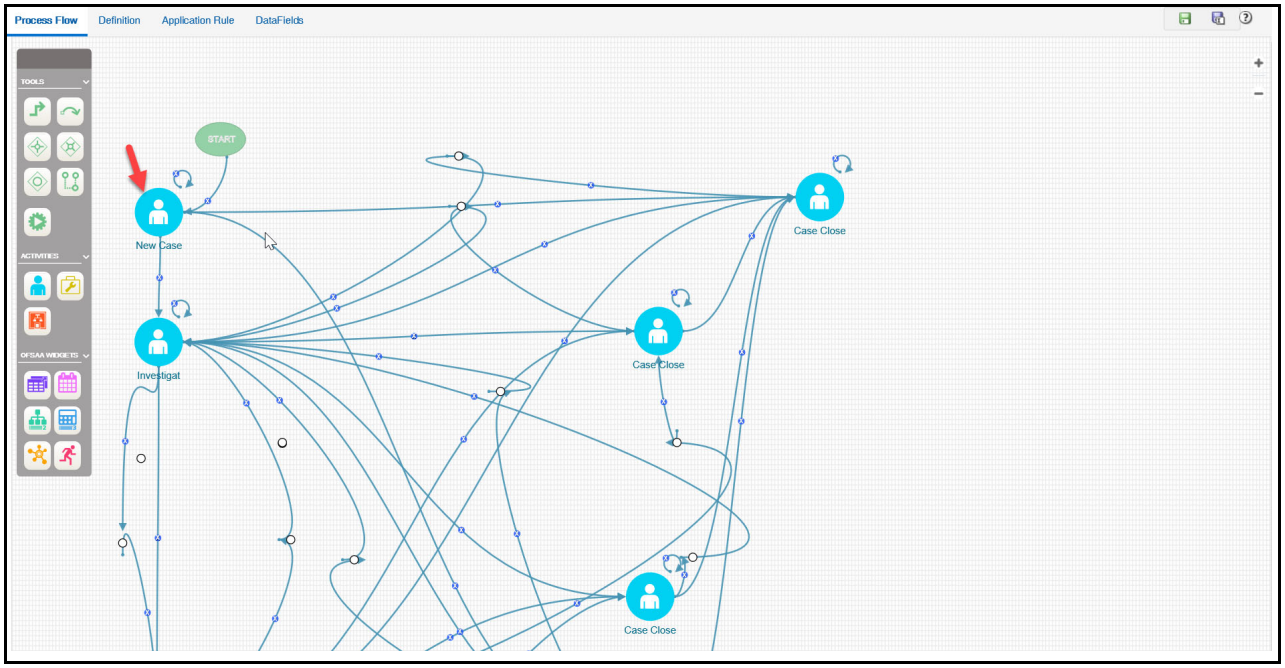


Figure 47. Adding Activity

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 the **Implementation** tab. The Implementation details are displayed.

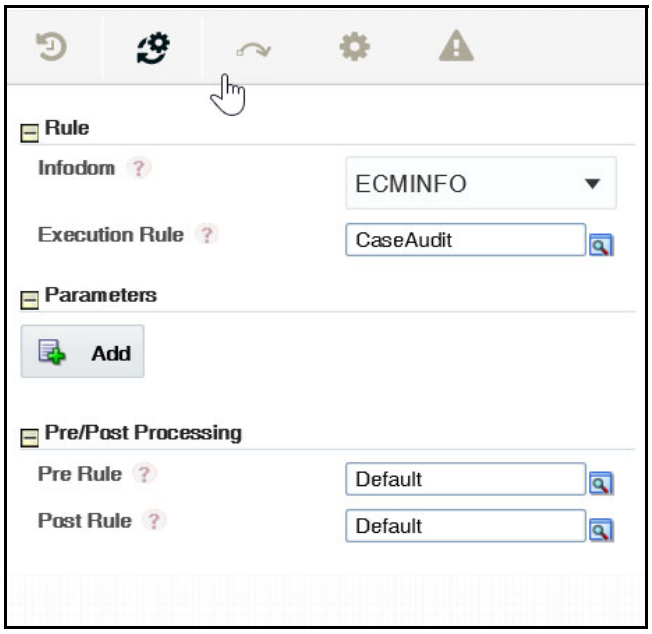


Figure 48. Implementing Activity

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 a 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.

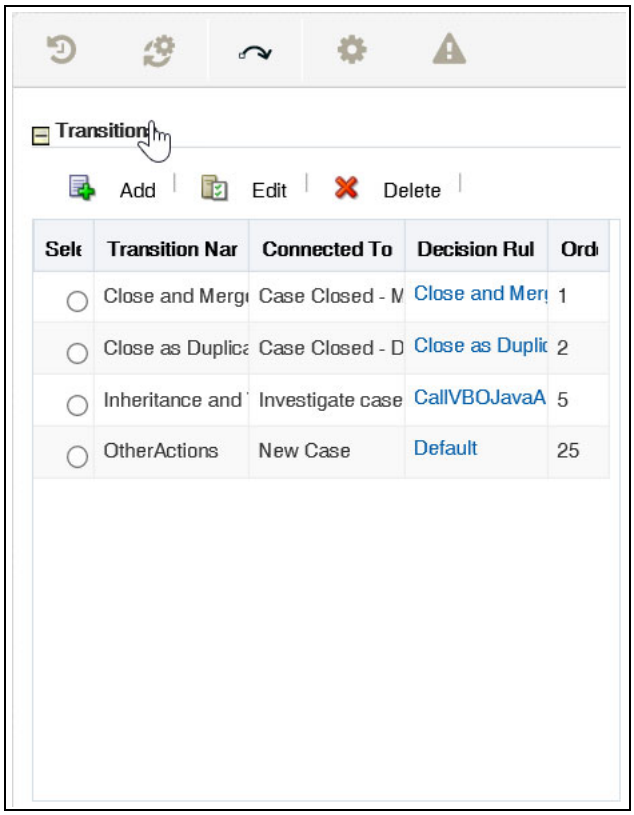


Figure 49. Add Transition

4. Enter the following information in the respective fields:

Table 28. 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 the *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.

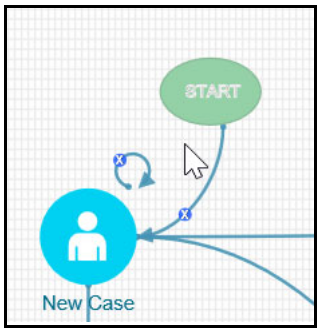


Figure 50. Adding Transition

Editing of an ECM Workflow

To edit an ECM workflow, follow these steps:

1. Navigate to Process Modeller window.

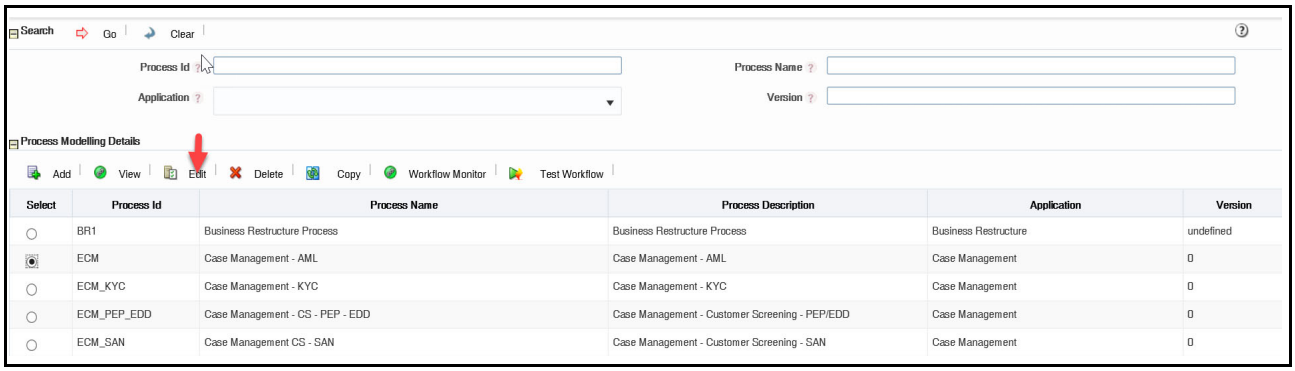


Figure 51. Process Modeller window

2. Select the workflow using the corresponding radio button.
3. Click Edit. The Process Modeller window is displayed for editing.

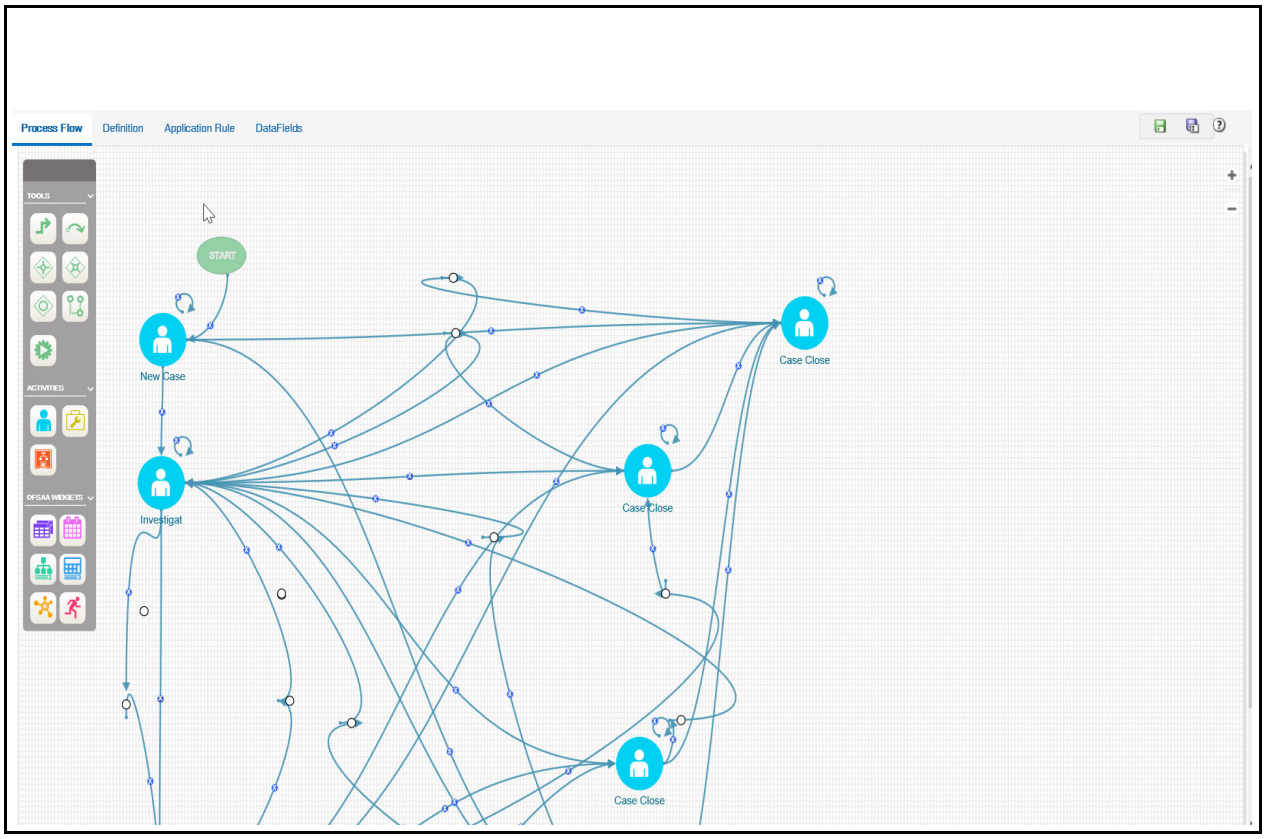


Figure 52. Editing Workflow

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**.

Implementing the ECM PMF Workflow

PMF provides many features that can be used to create various types of case investigation workflows. This section provides guidance about the basic steps that are required to create a new workflow in PMF. For more details, refer to the AAI user guide.

Defining Metadata

Define the following metadata before creating a workflow in PMF:

1. Define ALL actions (status changing and non-status changing) in KDD_ACTION table as follows. Note: You will see status changing actions in this table which are leftover from earlier versions. These will be cleaned up over time. The status changing actions will have the OBS category so they will not appear on the UI.

Column Name	Description	Is column applicable to status-changing action?	Is column applicable to non-status-changing action?
ACTION_ID	Unique identifier of the action which can be performed on a case.	X	X
ACTION_CATEGORY_CODE	Category within which this action is displayed on the Take Action window. E.g. OOB the action “Send Email” is displayed within a category called “Email”. Action category is just a way to segment actions into logical groups for easy reading on the UI. This does not impact the action in any way. This field references the KDD_ACTION_CAT_CD column in the ACTION_CAT_CD table.	X	X
ACTION_CD	Unique code that identifies the action. E.g. CA123. This code is not displayed on the UI.	X	X
ACTION_DESC	Action name that is displayed on audit history tab.	X	X
ACTION_NM	Action name that is displayed on the UI except the audit history tab.	X	X
ACTION_ORDER	Order used to display status and non-status changing actions on Take Action window.		X
DFLT_DUE_DT_LM	Enter number of days. When this action is saved on the case, system will automatically assign a due date to case = System Date + Number of days defined here.	X	X
REQ_DUE_DATE_FL	With the introduction of Validation Framework, this column is no longer required and need not be populated.		
LAST_ASSIGN_REQ	Flag used to assign the case back to last assignee. E.g. if a user recommended a closing action but the action was rejected, the case may need to be reassigned to the user who recommended closure. This column is not used OOB post 805. Use the STATUS_CD from KDD_STATUS		
NEXT_REVIEW_STATUS_CD	This column is used to record the resulting status of this action. Even though we now define the resulting status of a status changing action in PMF, this data should still be populated because ECM needs it for processing information other than just the case workflow. It is recommended that the resulting status defined here should be the same that is defined in PMF.	X	

REG_TYPE_CD	Unique identifier for the regulatory report type associated with an action (where applicable).	Only for CRR actions	Only for CRR actions
RESOLUTION_ACTION_FL	This value is required to mark which actions are resolution actions. Based on that we store some information in KDD_CASES table.	X	
REQ_CMNT_FL	With the introduction of Validation Framework, this column is no longer required and need not be populated.		
REQ_REASN_FL	With the introduction of Validation Framework, this column is no longer required and need not be populated.		
REQ_REASN_OWNER_FK	With the introduction of Validation Framework, this column is no longer required and need not be populated.		
EXPORT_DIR_REF	Directory path on the server where the Export to XML file is stored. Since we don't have that action anymore, this column is no longer required and need not be populated.		
LAST_UPDATED_BY	User ID of the person who last updated this action. Not required but good to provide for auditing purposes	X	X
LAST_UPDATED_DT	Date on which this action was last updated. Not required but good to provide for auditing purposes	X	X
CMMNT_TX	Comments added while adding this action. Not required but good to provide for auditing purposes	X	X

2. Define ALL statuses in KDD_STATUS table as follows:

Column Name	Description	Is column applicable to status-changing action?	Is column applicable to non-status-changing action?
STATUS_CD	Unique code for this status. This code is not displayed on the UI.	X	
STATUS_NM	Status name displayed on the UI.	X	
CLOSED_STATUS_FL	Indicator of whether this status is considered a "closed" status.	X	
CAN_NHRIT_FL	In previous releases, this column was used to indicate whether a case could be inherited when it is in this status. This is now handled by VBO in PMF. It is recommended that this value should be populated in sync with what's defined in PMF.	X	
VIEWD_BY_OWNER_ACTVY_TYPE_CD	In previous releases, this column was used to record the action code for the VBO action. This action would be recorded on a case with this status when the case was viewed by a user with privileges to own the case. This information is now defined in PMF. However, it is recommended that this value should be populated in sync with what's defined in PMF.	X	
VIEWD_RESULT_STATUS_CD	In previous releases, this column was used to record the resulting status of the VBO action. This information is now defined in PMF. However, it is recommended that this value should be populated in sync with what's defined in PMF.	X	

3. Define which non-status changing action will be available for which user role in KDD_ROLE_ACTION_MAP table as follows:

Column Name	Description	Is column applicable to status-changing action?	Iscolumn applicable to non-status-changing action?
CASE_ROLE_ACTION_MAP_SEQ	Unique Sequence Identifier for this record.		X
ROLE_CD	Unique code assigned to this user role. This field references the V_ROLE_CODE column in the CSSMS_ROLE_MAST table.		X
ACTION_CD	Unique code that identifies the action. This field references the ACTION_CD column in the KDD_ACTION table.		X

4. Define which non-status changing action will be available in which case status in KDD_STATUS_ACTION_MAP table as follows:

Column Name	Description	Is column applicable to status-changing action?	Is column applicable to non-status-changing action?
CASE_STATUS_ACTION_MAP_SEQ	Unique Sequence Identifier for this record.		X
STATUS_CD	Unique code for this status. This field references the STATUS_CD column in the KDD_STATUS table.		X
ACTION_CD	Unique code that identifies the action. This field references the ACTION_CD column in the KDD_ACTION table.		X

5. Define which non-status changing actions will be available for which case type in KDD_CASETYPE_ACTION_MAP table as follows:

Column Name	Description	Is column applicable to status-changing action?	the column applicable to non-status-changing action?
CASE_CASETYPE_ACTION_MAP_SEQ	Unique Sequence Identifier for this record.		X
CASE_TYPE_SUBTYPE_CD	Case Type Identifier. This field references the KDD_CASE_TYPE_SUBTYPE column in the CASE_TYPE_SUBTYPE_CD table.		X
ACTION_CD	Unique code that identifies the action. This field references the ACTION_CD column in the KDD_ACTION table.		X

6. Add all statuses to AAI_WF_STATUS_B and AAI_WF_STATUS_TL tables in the Config schema
   - AAI_WF_STATUS_B table:
     1. Contains the status code and package map
     2. In STATUS_ID enter the status code used in KDD_STATUS.STATUS_CD
     3. The package ID should be OFS_NGECM if this workflow is for use with ECM
   - AAI_WF_STATUS_TL:

1. Contains the status name and package map
2. Enter the Status ID, Status Name and Status Description as you entered them in KDD_STATUS. (The Description should be the same as the Name)
3. The package ID should be OFS_NGECM if this workflow is for use with ECM

Updating the New Statuses and Masking

If new statuses were added to KDD_STATUS in step #2 additional updates need to be made to masking tables so UI functions will be visible when the case in one of the new statuses. This enables

1. Execute below query in the Config schema and update V_ATTRIBUTE_VALUE1 with the new Status code. It's a query and modify the same to pick the new statuses:
   SELECT T.* FROM AAI_AOM_APP_COMP_ATTR_MAPPING T WHERE T.V_ATTR_CODE='MSTATUS';

   Note: There is currently an AAI limit on the V_ATTRIBUTE_VALUE1 field to 300 characters. This may not support all statuses. You can use the following update query to get around this:

   UPDATE AAI_AOM_APP_COMP_ATTR_MAPPING T SET T.V_ATTRIBUTE_VALUE1 =

   'SELECT T.STATUS_CD,T.STATUS_NM FROM KDD_STATUS T WHERE T.VIEWD_RESULT_STATUS_CD IS NULL OR T.VIEWD_RESULT_STATUS_CD <> 'OBS"WHERE T.V_ATTR_CODE = 'MSTATUS'
2. Execute below query in the Config schema and update V_ATTRIBUTE_VALUE1 to include new statuses. Note that you don't have to include closed statuses everywhere. Look at the OOB entries and you can see where necessary
   SELECT t.* FROM AAI_OJFF_MASKING_ATTR_VAL_MAP t;
3. Execute the below query and update RULE_ATTRBT_VAL in table FCC_UI_RULE_CONF
   SELECT T.*, T.ROWID FROM FCC_UI_RULE_CONF T WHERE T.RULE_ATTRBT = 'MSTATUS'
4. In order to allowing linking of cases from Relationship tab, update KDD_STATUS_LINKTYPE_MAP with the new statuses. Entries for open statuses and close statuses are different. The below query can be used as a reference. For open statuses, refer entries for INV and for close statuses, refer entries for CCNSAR.
   SELECT T.*, T.ROWID FROM KDD_STATUS_LINKTYPE_MAP T WHERE T.STATUS_CD IN ('INV','CCNSAR')
5. After this doing these updates, restart the servers.

Creating the workflow in PMF

1. **Add a new workflow** from the Process Modeler landing page. This creates a blank workflow and system will navigate the user to a Process Modeler page. This page contains several tabs (Process Flow, Definition, Application Rules etc.) that will be used to create the workflow. Below are some of the basic things you will need to define to create a workflow in PMF.
2. Define the "Application Rules"
   - An "application rule" is a rule that is executed in relation to an activity or a transition.

- There are several rules that can be created in PMF (Stored Procedure, Attribute Expression, Java API etc.) - all these rules need to be categorized as one of the three main types of rules:
  - **Execution Rule –** this is the business logic executed by the activity. For example, the OOB AML workflow includes an execution rule called "Case Audit". This rule is used by all activities where the action leading to that activity is going to be recorded on the case audit history.
  - **Decision Rule -** This rule returns a "True/False" value that is used in decision making during a transition.
    - For actions that will be displayed on the Take Action window, an "Attribute Expression" decision rule should to be created. This is how PMF will know which action should be displayed on the Take Action window for which user role and in which case status. **To create an attribute expression** on the Application Rule tab:
      a) Click on the "Add" button (on the top-left side of the tab) to open a menu. Select "Attribute Expression" from this list. "Rule Details" window is displayed.
      b) On the Rule Details window, enter the name of this attribute expression.
      c) Select "Action" in the Attribute drop down and click Add. This will add a record in the Attributes Values section. In Attributes Values section, the "Value" drop-down shows all the actions defined in KDD_ACTION. Select the action(s) you want to associate with this rule.
      d) Select "Status" in the Attribute drop-down and click Add. This will add another record in the Attributes Values section. The Value drop-down displays all the statuses defined in KDD_STATUS. Select the status(es) you want to associate with this rule.
      e) Now select "Role" in the Attribute drop-down and click Add. This will add another record in the Attributes Values section. The Value drop-down shows you all the roles defined for ECM. Select the role(s) you want to associate with this rule.
      f) Click Save.

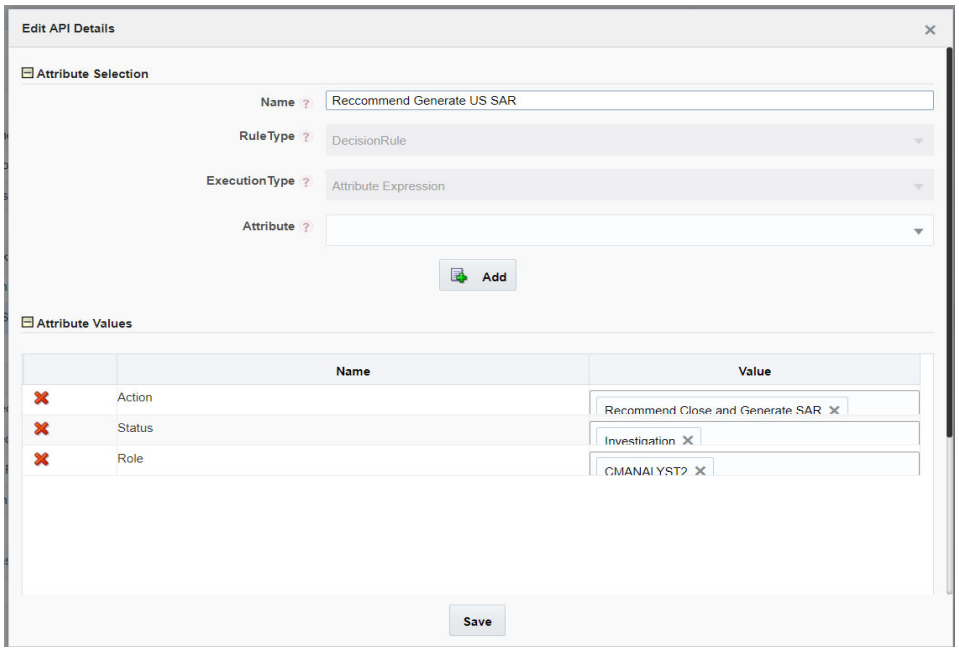


Figure 53. Attribute Expression details window:

- ECM uses the "attribute expression" decisions rules to determine which actions to display on the Take Action window. If an action is associated with an attribute expression, that action will be displayed on the Take Action window. Any status changing action that is not displayed on the take action window (e.g. Close and Merge from the Relationship tab) should be associated with an "Expression" decision rule instead of an attribute expression rule. Expression rules are simple rules like "If action code = X, move the case to the next status". If there is a need to show this type of action only for specific user roles, use masking to achieve that.

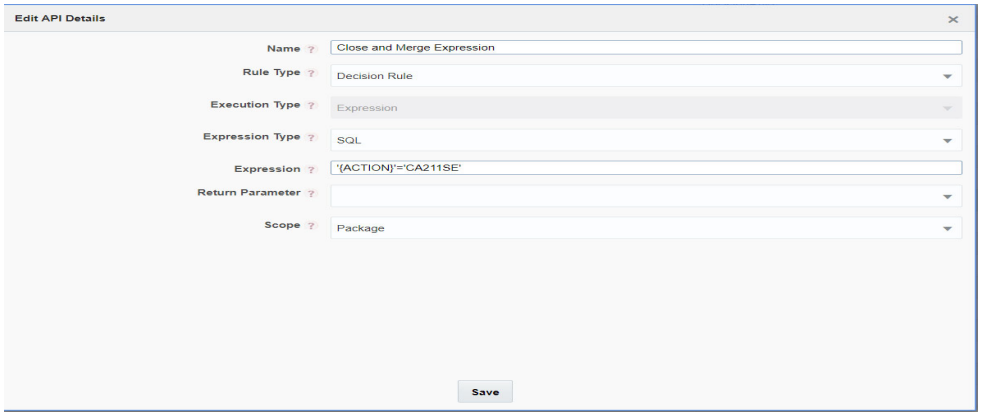


Figure 54. Expression Details

- **Selection Rule -** This rule fetches some value, useful to get value dynamically from a table or other source. OOB ECM does not use selection rules.

- Define application rules on the "Application Rules" tab within Process Modeler **prior** to drawing activities and transitions on the Process Flow tab.
- Workflow logic determines which types of rules need to be created. OOB ECM only uses execution and decision rules.
- For more information about application rules refer to the AAI user guide

3. **Draw the "activities"** (i.e. case statuses) on the "Process Flow" tab:
   - An "activity" means a case status. From the Left-Hand-Side menu, add the applicable type of "activity" to the canvas.
     - Select a "Human Task" if human action is required to move the case to the next status. This is what will be used most of the time as almost all case workflows require a user to take any action that moves the case to the next status.
     - Select a "Service Task" if an automatic activity is going to move the case to the next status.
     - Select a "Sub Process" if you want to call another Process/ Workflow from your current workflow.
   - After selecting an activity and adding it to the canvas, double click on the activity to open a window (that has many tabs) to enter details about this activity.
   - On the first tab of this window, enter "Activity Details" as follows:
     - **Activity Name** = name of status. This name is just for use in PMF – ECM UI displays the status name defined in KDD_STATUS.
     - **Activity Description** = description of this status for use in PMF.
     - **Activity Type** = pre-populated based on the type of activity selected from the left-hand-side menu (human, service etc.) but can be changed as needed.
     - **Status** = associate this activity with a status defined in the database. This drop-down list displays the values in the AAI_WF_STATUS_B table.
     - **Outcomes** = OOB workflows do not use this setting. For more details about this setting, refer to the AAI user guide

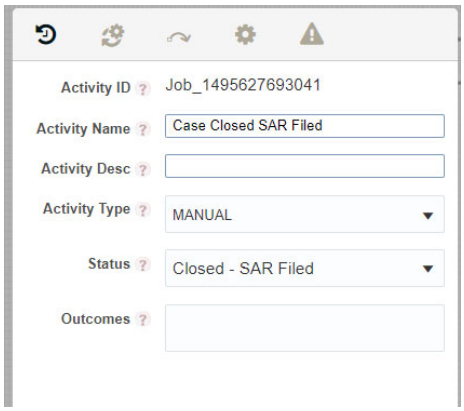


Figure 55. Activity Details tab

- After defining "Activity Details", **define rules on the second tab (IMPL)** and as follows:
  - **Execution Rule** = this is the business logic executed by the activity. For example, the OOB AML workflow includes an execution rule called "Case Audit". This rule is used by all activities where the action leading to that activity is going to be recorded on the case audit history.
  - **Pre-rule and Post-rule =** select the API rule that needs to be run before reaching the activity (pre-rule) or while exiting that activity (post rule). "Exiting that activity" means that when you move out of this status this rule will be called. As an example: the OOB AML workflow uses an Execution Rule called "CallRRSJavaAPI" to call the RRS API for the "Close and Generate SAR" action.
  - To view/edit the OOB rules OR define a new rule, navigate to the "Application Rule" tab in Process Modeler.

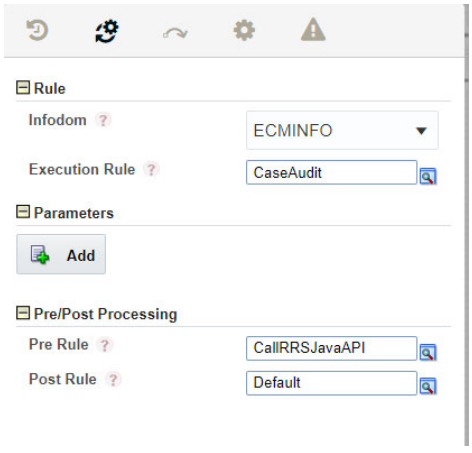


Figure 56. IMPL tab

- On the same window where users can enter activity details and execution rules, there are three more tabs with settings that can be defined for activities but we have not needed those for OOB workflows. For more information about these settings, refer to the AAI user guide

  Note: That even though transitions leading out of that status can be defined on the "Transitions" tab of this window, it is better to draw them directly on the canvas.

4. **Draw the "transitions"** (i.e. case actions) on the "Process Flow" tab within Process Modeler:
   - After adding activities to the canvas, add "transitions" between these activities.
   - A "transition" is an action that takes the case from one activity to another (that is, from one status to another).
   - From the left-hand-side menu on Process Flow tab, add the applicable type of "transition" to the canvas.
   - Double click on the transition to open the "Edit Transaction" window and enter transaction details as follows:
     - **Transition name**: name of transition. This name is just for use in PMF; ECM UI displays the action name defined in KDD_ACTION.
     - **Decision Rule:** every transition should be linked to a decision rule.
       - For actions that will be displayed on the Take Action window, select an "Attribute Expression" rule from this drop-down list.
       - For actions that will not be displayed on the Take Action window (e.g. Close and Merge on Relationship tab), an "Expression" decision rule should be created.
       - Details of how to define decision rules expression are included.
     - **Order**: If there are multiple transitions that have to run sequentially between 2 activities, this is the order in which the Decision rules for these transition will be executed. Note: The order in which actions are displayed on the Take Action window is defined in KDD_ACTION table, not in PMF.
     - **Stroke:** this is the style in which the transition will be displayed on the Canvas (Process Flow tab). That is, users may choose to display some transition lines as "dotted" lines and some as "dashed" lines to make it easier to read the workflow diagram.

Note: Use a Connector when making multiple transitions between statuses. It makes the workflow diagram easier to read. Also, draw a circular transition on every status. Create a transition that circles back on the same status and name it "Other Actions". Associated this transition with a "default" decision rule and give it a high order number. When ECM calls the PMF workflow, if there is no transition available for that Case, PMF considers the workflow completed for that case and the status will not change any further. If the circular transition is defined, it takes that path and waits for the next action.

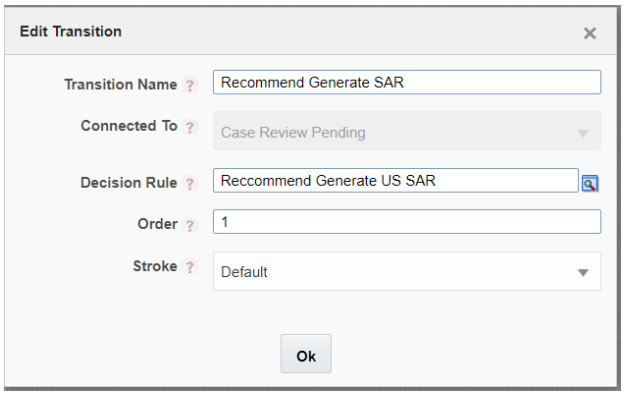


Figure 57. Edit Transition window

5. Data Fields
   - Data Fields allow PMF to access and store information from the ECM application. Data Fields are passed from the ECM UI to PMF as part of an action and are used in application rules. E.g. when a user takes an action that moves the case to "Investigation" status, if an application rule has been defined that requires a specific transaction amount to be greater than a specific value before a case can be moved to that status; ECM will need to send that transaction amount as a Data Field to PMF. The application rule will use this data field to conduct the calculation and move the case to the next status only if the application rule returns True.
   - For more information about Data Fields refer to the AAI user guide.

Note: Creating new data fields is possible in PMF but passing the value from ECM to PMF required a code change.

6. Save the workflow:
   - Following two buttons on the Process Flow tab to save the workflow:
     - **Save** button – use this form of saving if you are creating a brand new workflow OR editing an existing workflow and do not need to maintain the previous version of that workflow. This button over-writes the workflow being edited. As a result, all cases (in-flight and closed) using that workflow will follow the modified workflow as soon as the changes are saved in PMF. New cases (of the Case Type(s) using this workflow) will also use this modified workflow.
     - **Save as New Version** button – use this form of saving if you are editing an existing workflow and do not want to change the version which you selected to edit. This button saves the modifications as a

new version of the workflow and leaves the previous version unchanged. The version number assigned to this new version = parent workflow's version number + 1. For example: If the parent workflow had a version number 4, this new version will have a version number 5. But just saving a new version of a workflow does not have any impact on any case unless this new version is mapped to a Case Type in Case Designer. When the Case Type-Workflow mapping is updated in Case Designer, all cases of that Case Type created after the update will use the latest workflow mapped to the Case Type. All older cases of that Case Type continue on the version they were using previously. The moment a case type is mapped to a different workflow, new cases will start using the new workflow (but old cases will not be impacted). Note: In Case Designer you can associate any version of a workflow with a Case Type. Case Designer does not have any restrictions around which version of a workflow can be linked to a Case Type.

Mapping of Workflow to a Case Type(s) in Case Designer

1. For ECM to use a workflow, that workflow must be linked to one Case Type.
2. One workflow may be linked to more than one case type.
3. Case Designer provides the ability to link Case Types to PMF workflows as a part of case type definition.

Steps to customize the "Checklist" functionality in ECM

1. Use case: A checklist has to be completed when a case has reached a pre-closing status (e.g. Decision Preparation). Only after a user has selected all items on the checklist can the case move to a different status.
2. Steps to accomplish:
   - Define each "item" on the checklist as a non-status changing action in KDD_ACTION.
   - Since the checklist actions are non-status changing actions, a user is expected to save all the checklist actions before taking a status changing action that closes the case.
   - Define this status-changing action (in KDD_ACTION) that the user will save AFTER the checklist actions have been saved on the case.
   - Define metadata for these actions so that ECM knows when to display these actions and add the status changing action to the PMF workflow.
   - Define a validation in the validation framework for this status-changing action to check if all the checklist actions have been recorded on the case. If they have, the system will allow the user to save the status-changing action and close the case. If not, the system will not allow the user to close the case.

Configuring CRR Workflows in PMF

You can configure CRR workflows for various STRs.

1. Navigate to Process Modeller window.

2. Go to Case Management-AML. A new window with workflow will open.
3. To create a new rule, click the **Application Rule tab**. Click Add and select Attribute Expression from drop-down.
4. Enter the following details in Attribute expression:
   - Name: User specific details such as **generate GO AML** and so on.
   - Attribute: Select Action from Attribute drop-down and click Add. Select user-specific action such as Generate GO STR, Generate CA STR and so on.
   - Attribute: Select Role from Attribute drop-down and click Add. Select CMSUPRVISR
   - Attribute: Select Status from Attribute drop-down and click Add. Select status that you want to be posted such as new, Investigation and so on.
5. Click Ok to save.
6. Go to Process Flow. Select the pipeline coming from 'Investigate case' to 'Case closed SAR Filed' and double click on it.
7. Edit Transition window will display. In Edit Transition, provide Transition name of STR such as **generate GO AML**. Select the rule that was created in step 3 from Decision Rule.
8. Click Ok.
9. Click Save.

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

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.

- **Case Class:** Create a case class or use an existing one. A Case Class is a grouping definition (AML, Fraud, and KYC). Case Type is where the case is actually defined. Each Type is associated with a Class and a Class can have multiple Case Types.
- **Case Type:** In the case type, the majority of the case definition is made. Here, you can define the various attributes associated with the case as well as the business entity tabs and the workflows that all cases of this type will follow.
- **Case Attributes:** Case attributes are specific data fields that can be associated with a case. Many of these are required and come pre-selected out of the box. These attributes are applicable to all cases regardless of type. Other attributes can be added to the individual case Type and custom attributes can also be created. For each case type parameters can be set to control how that attribute behaves.
- **Case Entities:** Case Entities are the tabs that are seen when viewing a case. Entities are related to two types: business data and operational. Business data entities are items like customer, account and correspondent bank. After selecting one of these entities, it will be displayed when viewing a case. Operational Entities are mandatory for a case type. These are types, like Audit Trail, Narrative and Evidence which are necessary to disposition a case.
- **Case Workflow:** The case type's workflow is first defined in AAI's Process Modeling Framework application. Once it is created there it can be selected for a specific case type. Each case type can only have one workflow.

Below is a list of features:

- Create and modify Case Class and Case Type definitions.
- Case Class is the topmost definition through which a case is created.

- Case Type provides a 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 in 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.

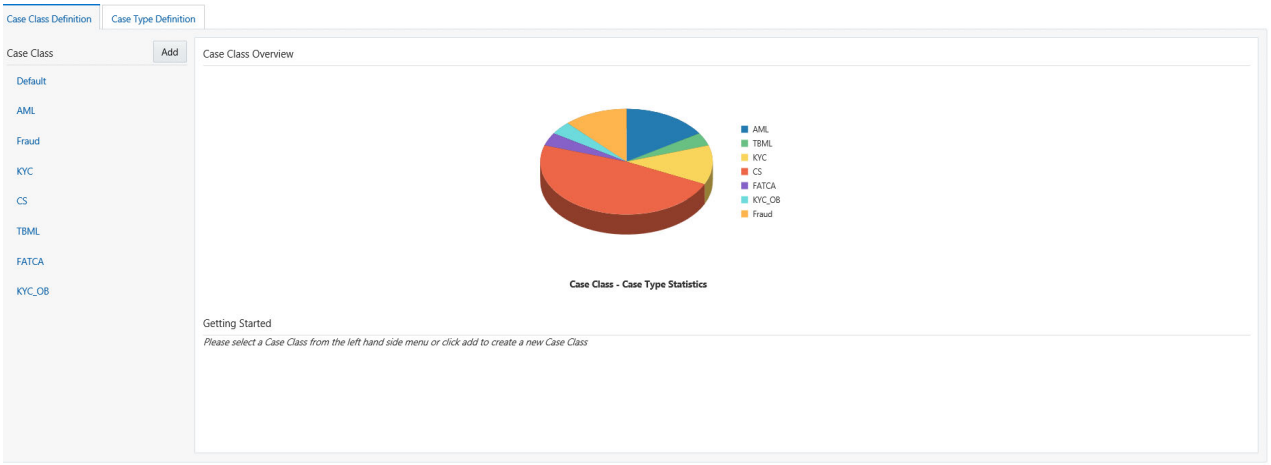


Figure 58. Case Designer Home Page

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 the **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 is 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 topmost definition through which a case is created.
- Used for grouping case types.
- Add and modify the 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 the **Case Class Definition** tab.
3. Click **Add**. The Case Class Definition page is displayed.

4. Enter the following information in the respective fields.

Table 29. 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 the case class is reflected in 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 the **Case Class Definition** tab.
3. Select the existing case class in the LHS menu. The case class details are displayed in the RHS panel.
4. Modify the necessary information in the required fields. For more information on the fields, see *Table 29*.
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

- 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.

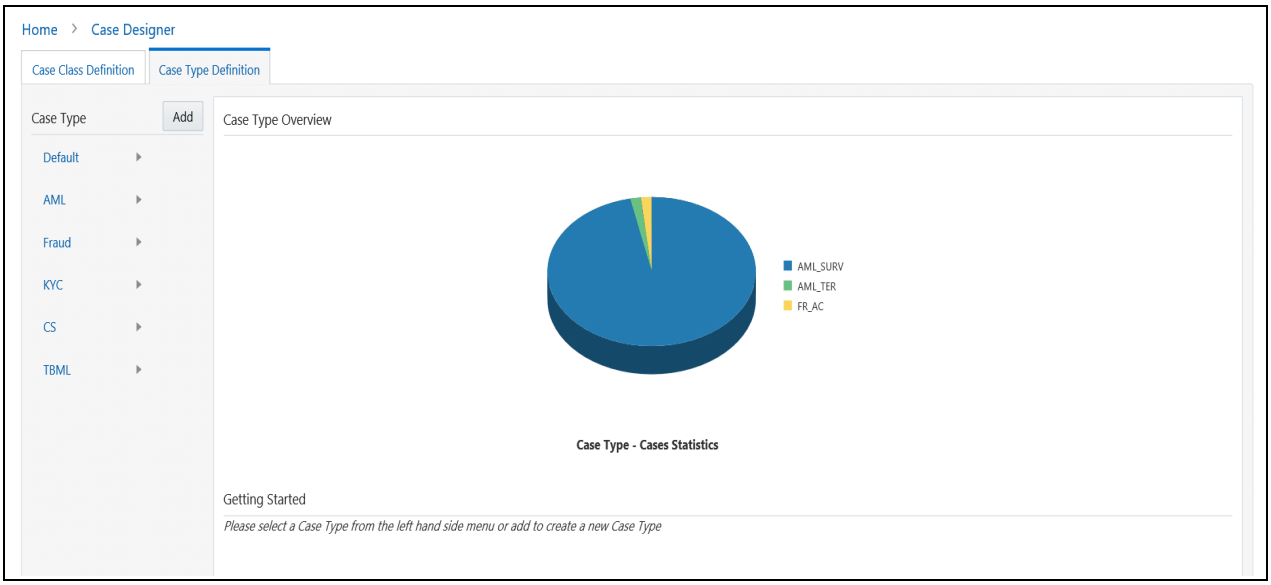
Note: The data displayed on the tab is not controlled by case type.

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 the **Case Type Definition** tab.



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

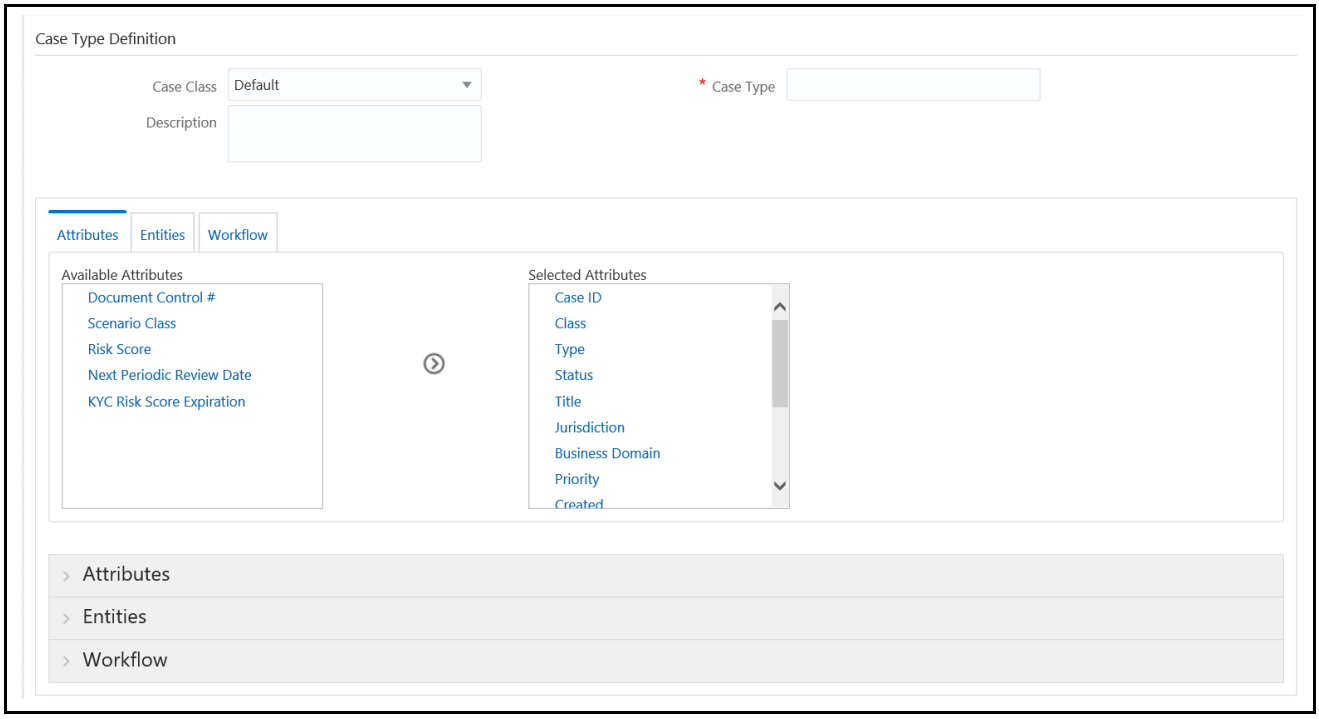


Figure 59. Case Type Definition Page

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 30. 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 the 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 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, the 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 the 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 the **Attributes** tab. The optional attributes are displayed in the *Available Attributes* menu.

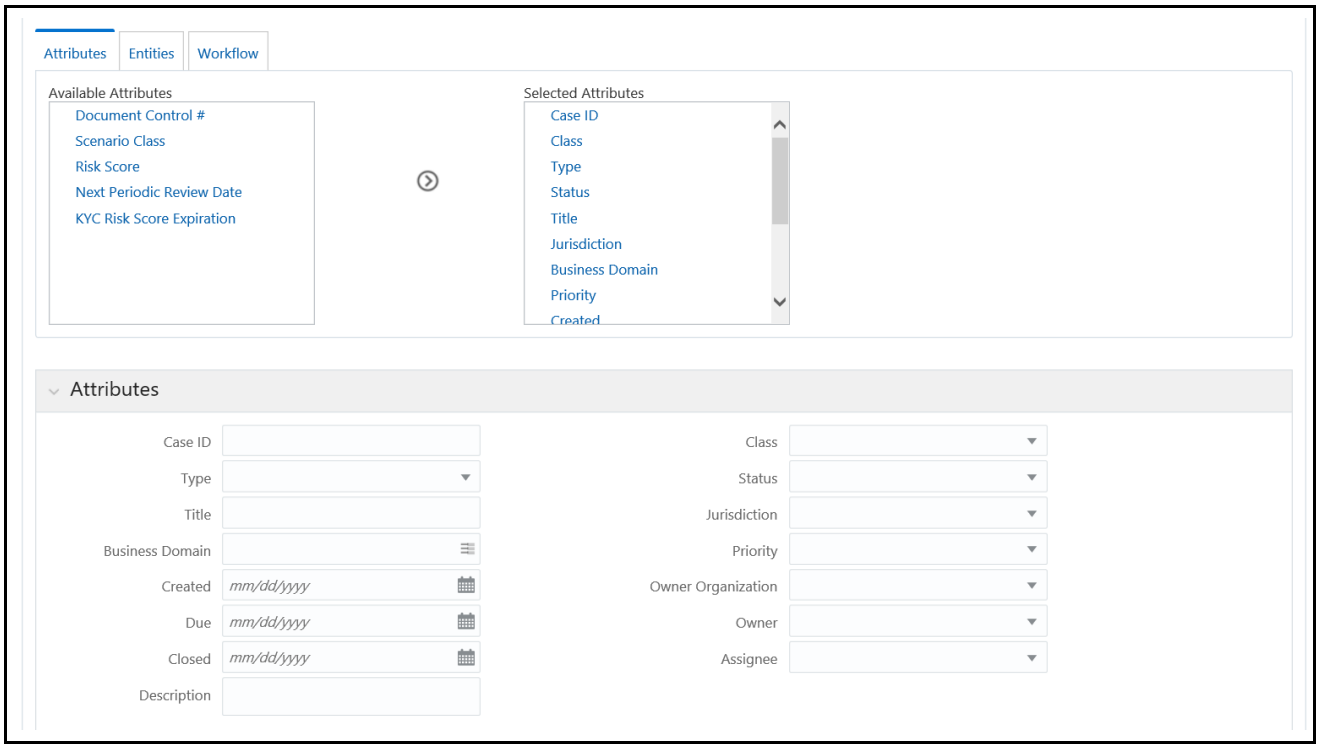


Figure 60. Attributes Page

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 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 the required Case Type. Go to the Attribute section.
3. Click 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 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 following:
  - Mandatory Entities – These entities are by default associated to the case type at the time of creation. These entities cannot be disassociated from the case type.
  - Optional-Default Entities - These entities are by default associated to the case type at the time of creation. These entities can be associated/disassociated to/from the case type using Case Designer. Evidence, Relationship, Audit History are the Optional-Default entities provided out of the box.

- Optional Entities - These entities are not by default associated with the case type at the time of creation. These entities can be associated/disassociated to/from the case type using Case Designer. Event Details, Narrative, Correlation, Account, Customer, Employee, Household, Investment Advisor, External Entity, Correspondent Bank, Transactions, Financials, Involved Party, Network Analysis, Customer Screening, KYC Risk Score, External Entity Screening, Trade Finance, Real-Time Screening are the Optional entities provided out of the box.

- Case Summary section of ECM UI display entities (tabs) even there is no data is associated with the entity.
- Add or remove only optional and optional-default entities.
- Ordering of entities can be configured.
- Whenever changes happen to entities those changes are reflected on the 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 the Selected Entities menu. All entities that are in the 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 the **Entities** tab. The optional entities are displayed in the *Available Entities* menu.

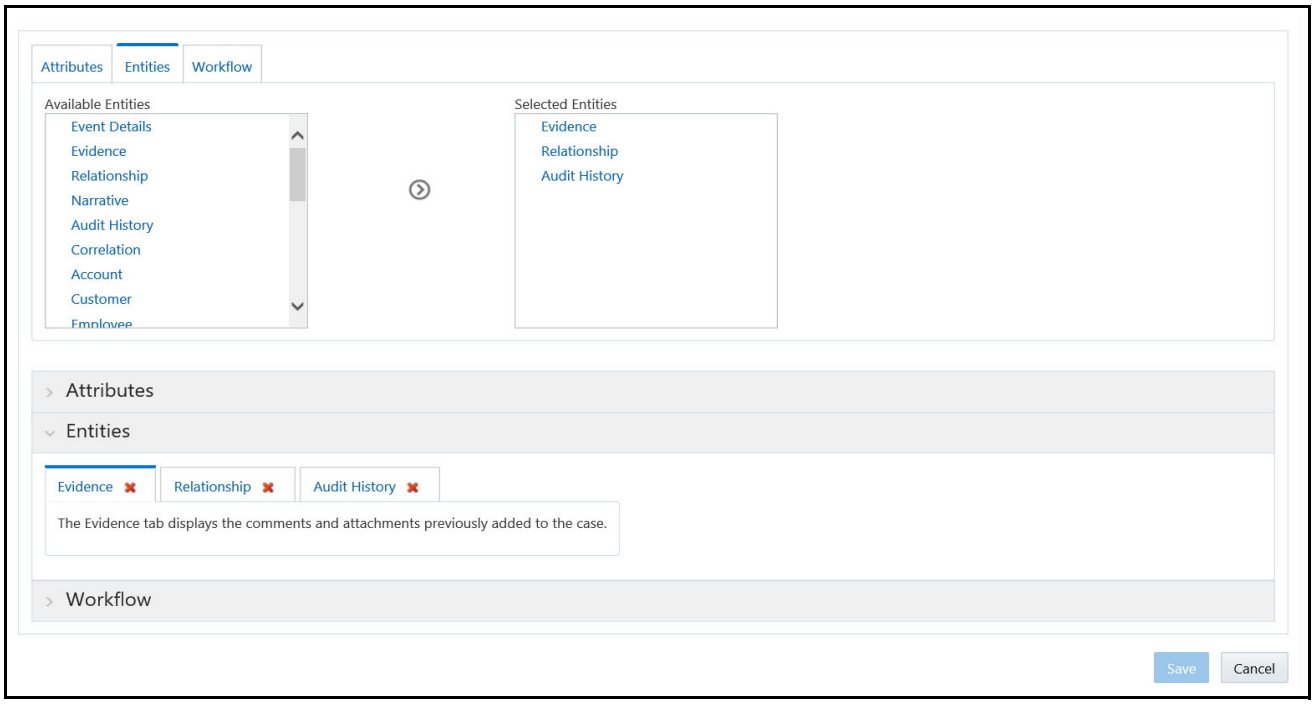


Figure 61. Entities Page

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 requirements.
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 the required Case Type. Go to the Entities section.
3. Click against required entities to remove from the 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 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 the 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 a 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 the **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 the **Workflow** tab. The defined workflows are displayed in the **Available Workflows** menu with following format:
   Process Name (ProcessID) - v#

   Here,

   Process Name is the name of the workflow.

   ProcessID is the unique identifier assigned to this workflow.

   v indicates that a version number is going to follow.

   # is the actual version number assigned to this workflow.

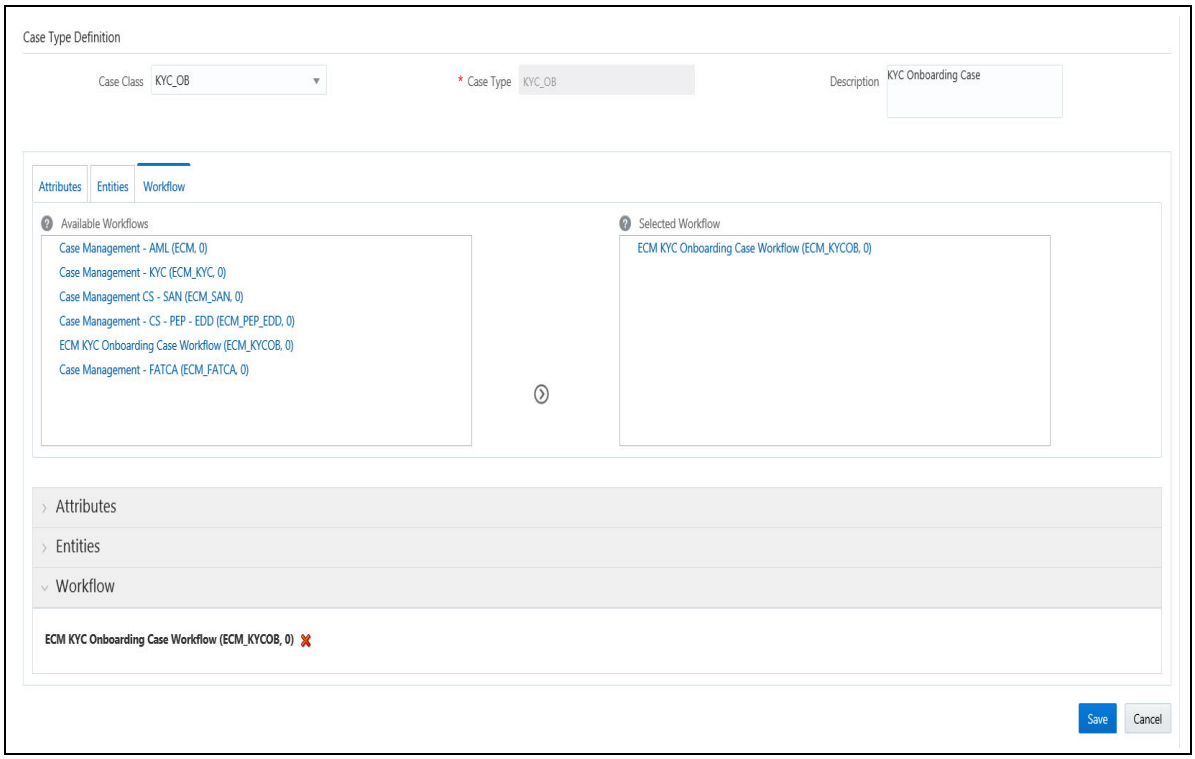


Figure 62. Workflow Page

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 the required Case Type. Go to the Workflow section.
3. Click  against the required workflow to remove from the 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 the **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 29*.

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 Attribute or Entity 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

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 App server'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 App server's work folder.

Accessing Manage Parameters

To access the Manage Parameters, follow these steps:

1. Navigate to the 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 the 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 63 illustrates the modified currency code as EUR.

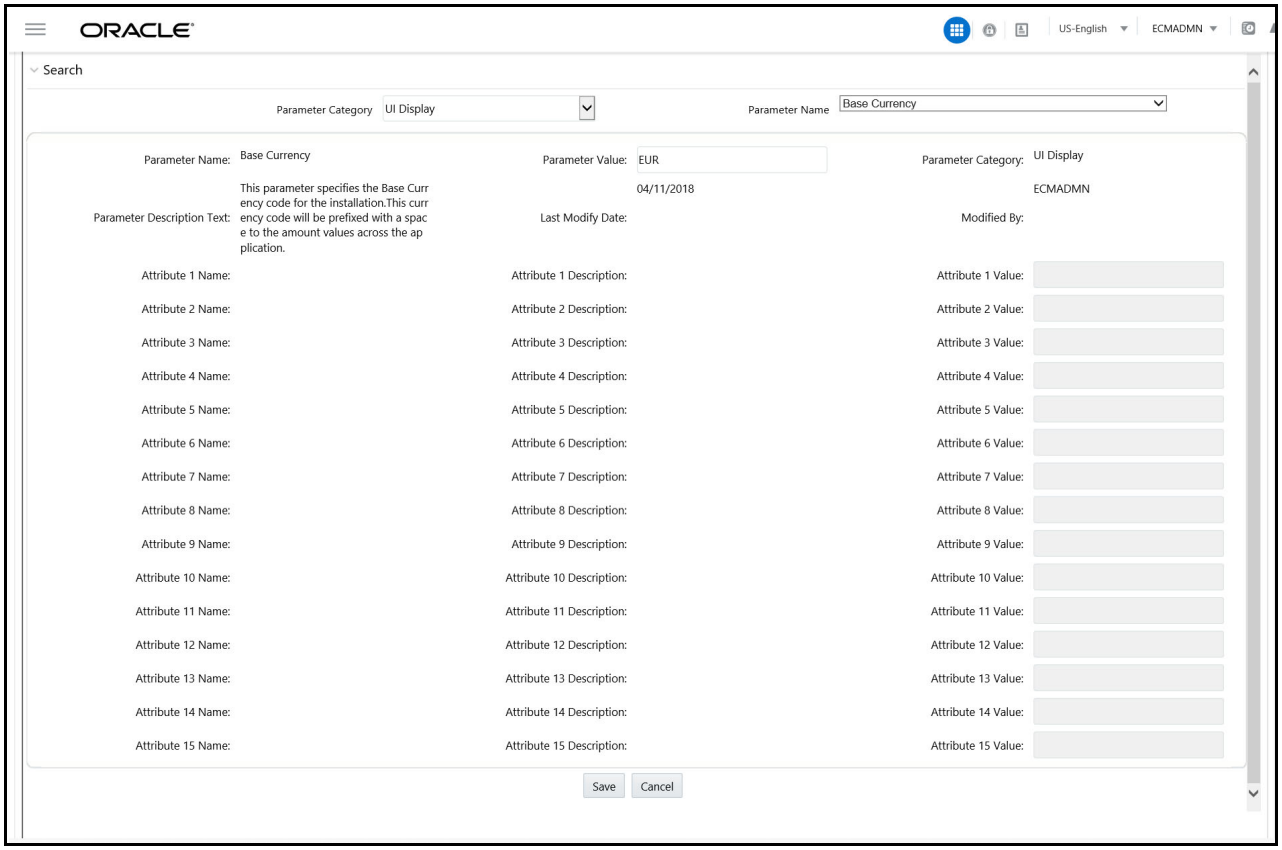


Figure 63. Financials Tab—with Modified Currency Format

Perform the following steps from the back end:

1. Take the backup of the AAI_FF_CONTROL_PROPERTIES table.
2. Execute below query in config schema:

   UPDATE AAI_FF_CONTROL_PROPERTIES SET V_CONTROL_SPECIFIC_11 = '**MMK**' WHERE V_CONTROL_SPECIFIC_12 ='code' and V_CONTROL_SPECIFIC_11='**USD**';
3. Restart the servers and test the UI.

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.

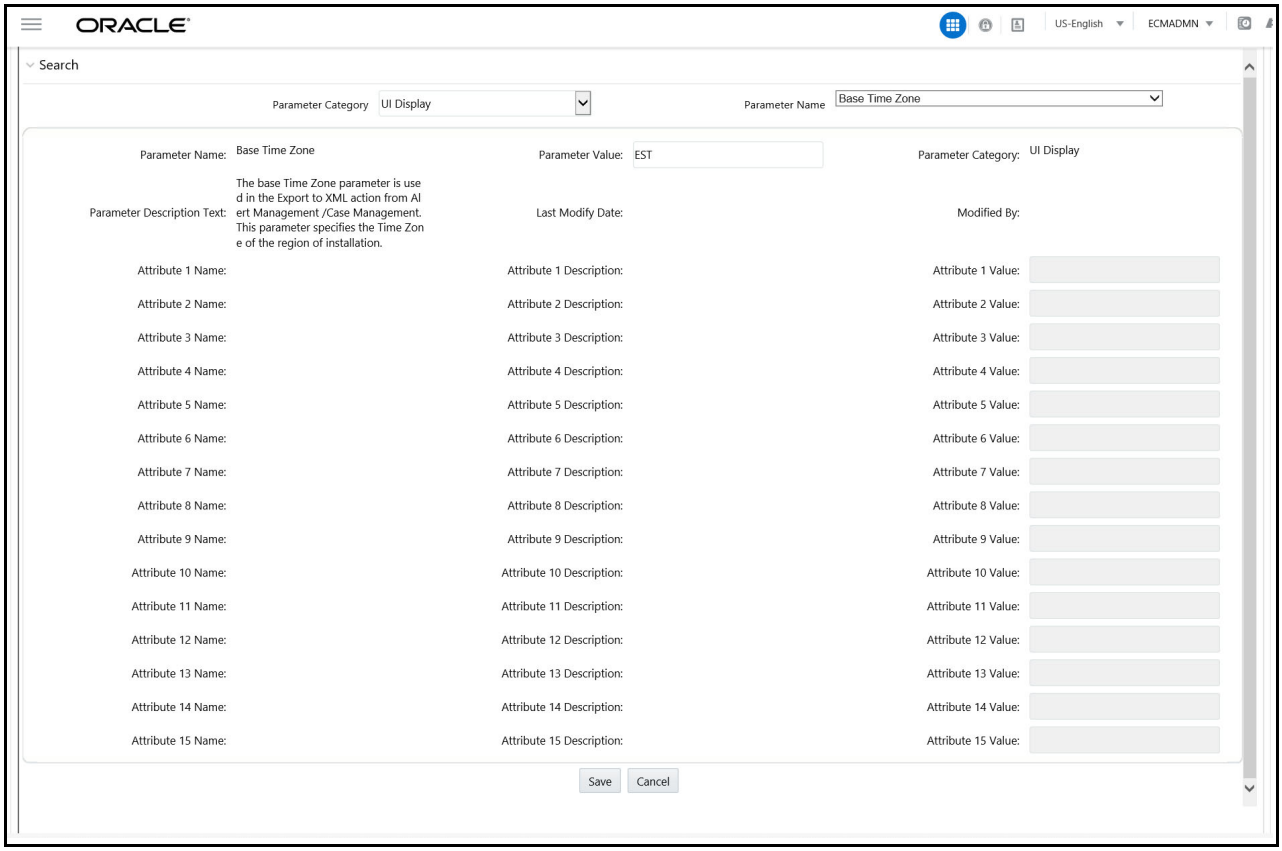


Figure 64. Configuring Base Time Zone

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 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.

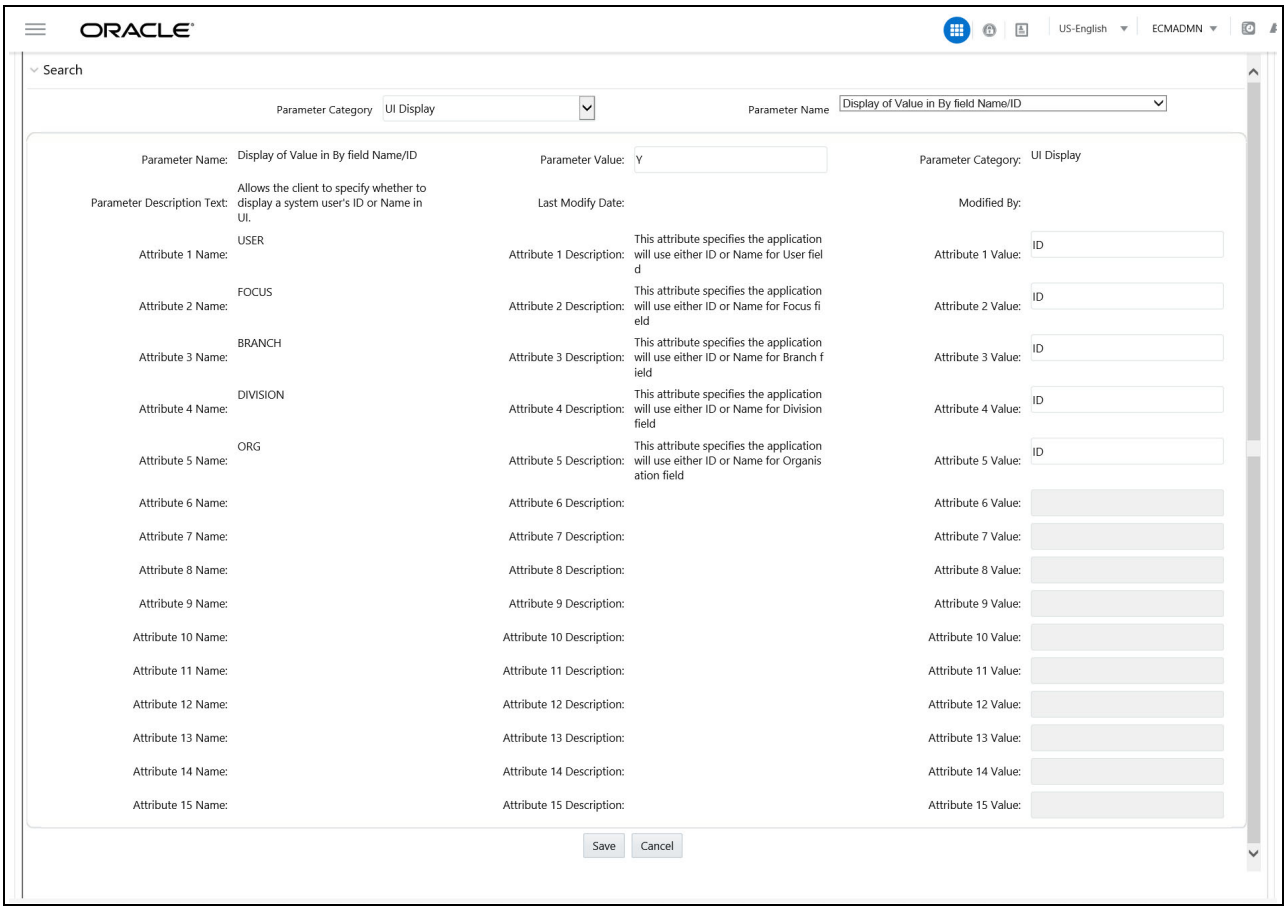
Configuring the Display of Value in By Field Name/ID

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 31. Configuring Display of Value in By Field Name/ID Attributes

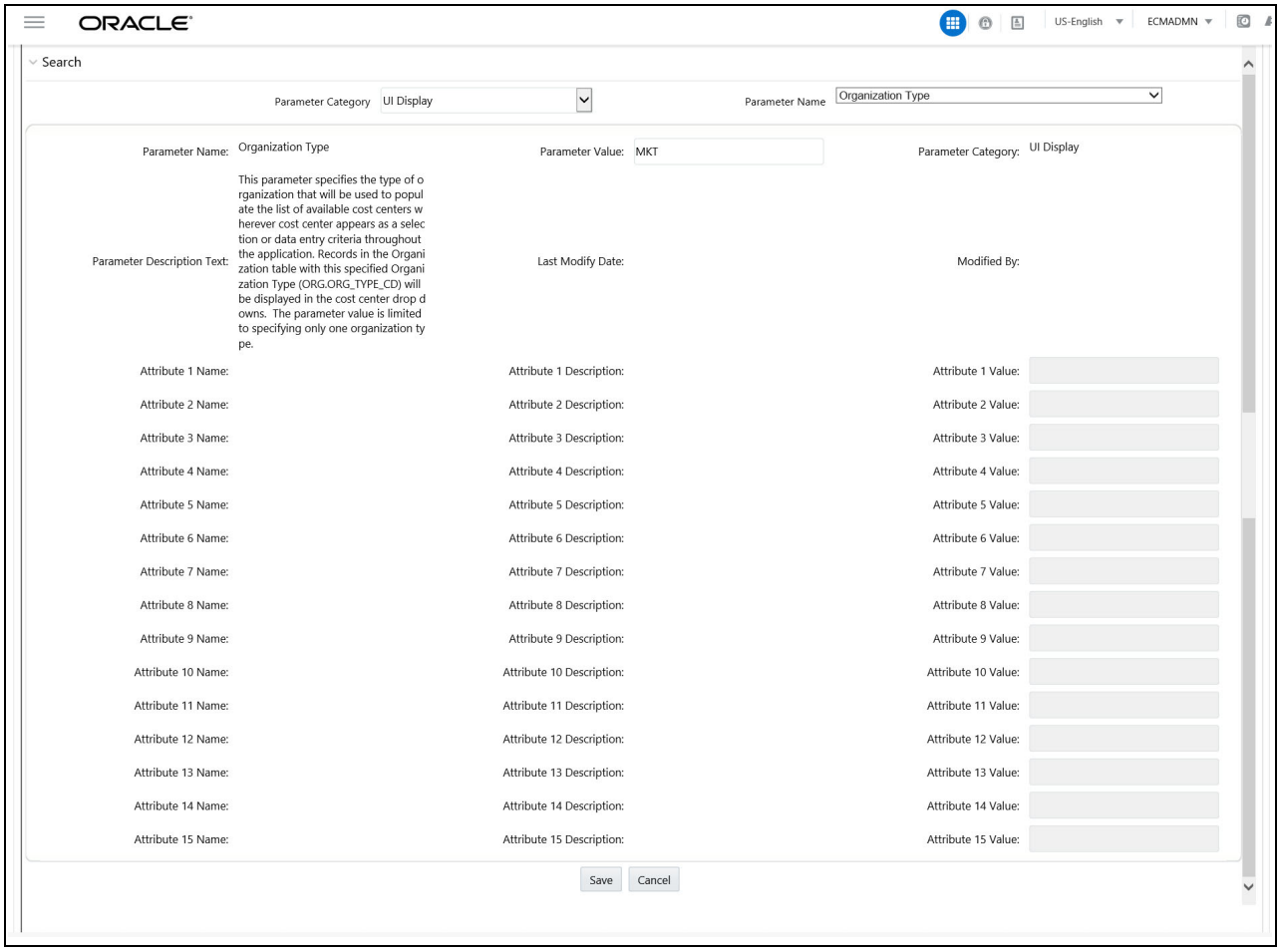
Attribute	Description
User	ID or Name for User field.
Focus	ID or Name for Focus field.
Branch	ID or Name for Branch field.
Division	ID or Name for Division field.
Org	ID or Name for Org field.

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 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 32 describes the attributes to be configured for setting the application server.

Table 32. 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.

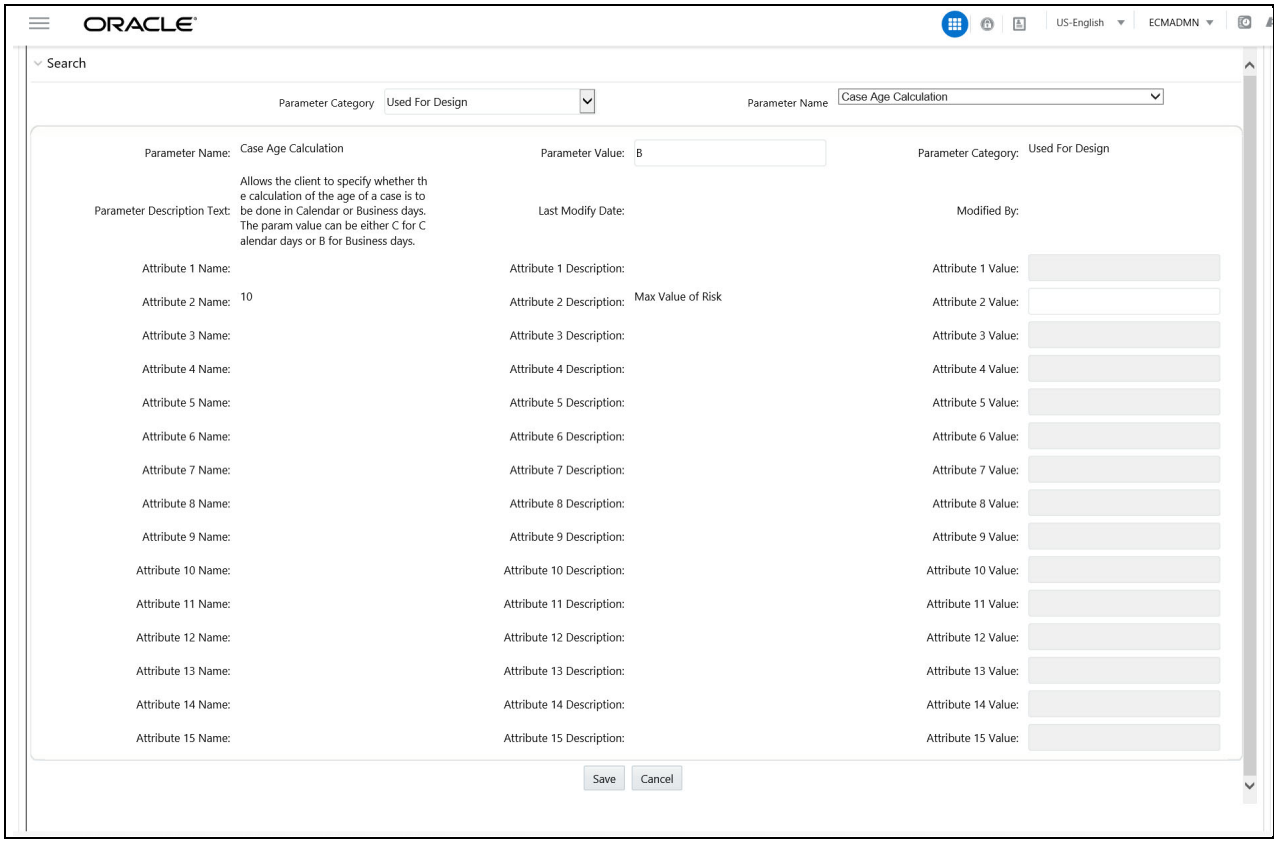
Configuring Case Age Calculation

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.

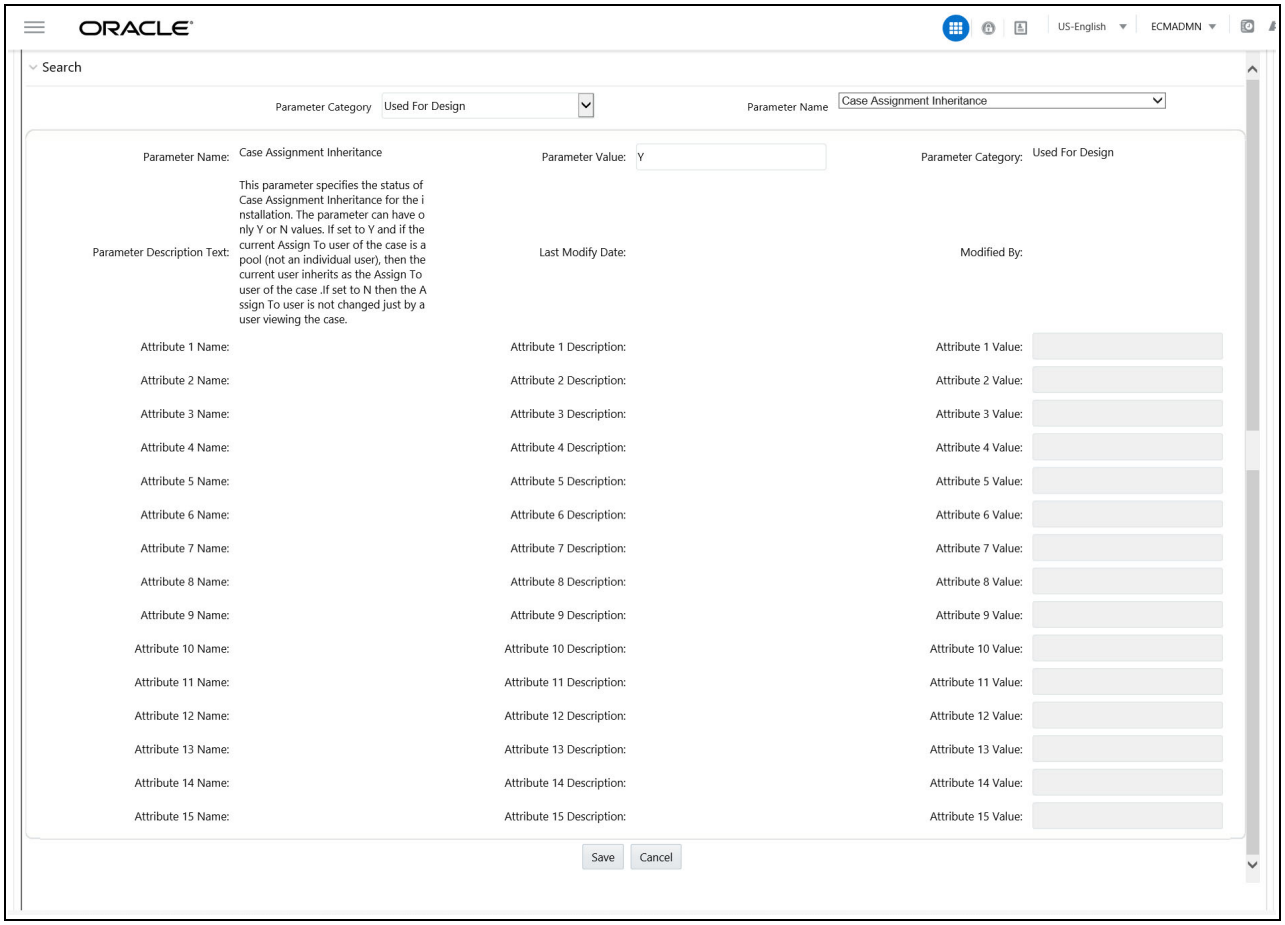
Configuring Case Assignment Inheritance

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 a 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 a 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 33. 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 s 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 risk value, follow these steps:

1. Open the Manage Common Parameters screen.
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 34. 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 the promotion of an alert or manual creation will be assigned to. This allows for the 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 a 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.

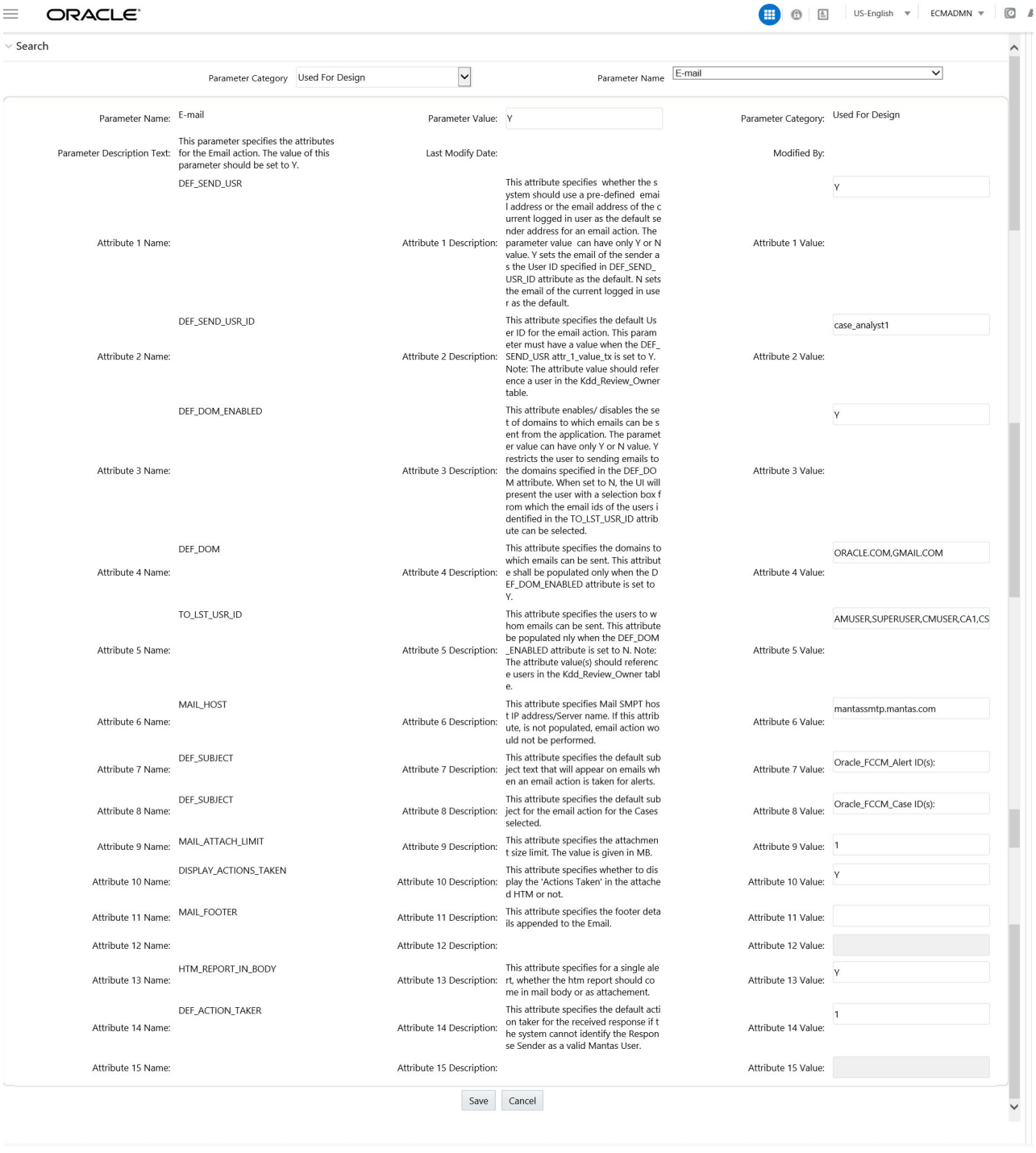
Table 35. Configuring Case Owner

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 36 describes the attributes which need to be configured for E-mail parameters.

Table 36. 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 the mail body or as an 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.

Note: ECM supports default port (25) of the SMTP server only. Also, it doesn't support any authentication mechanism or any user credential integrations.

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.

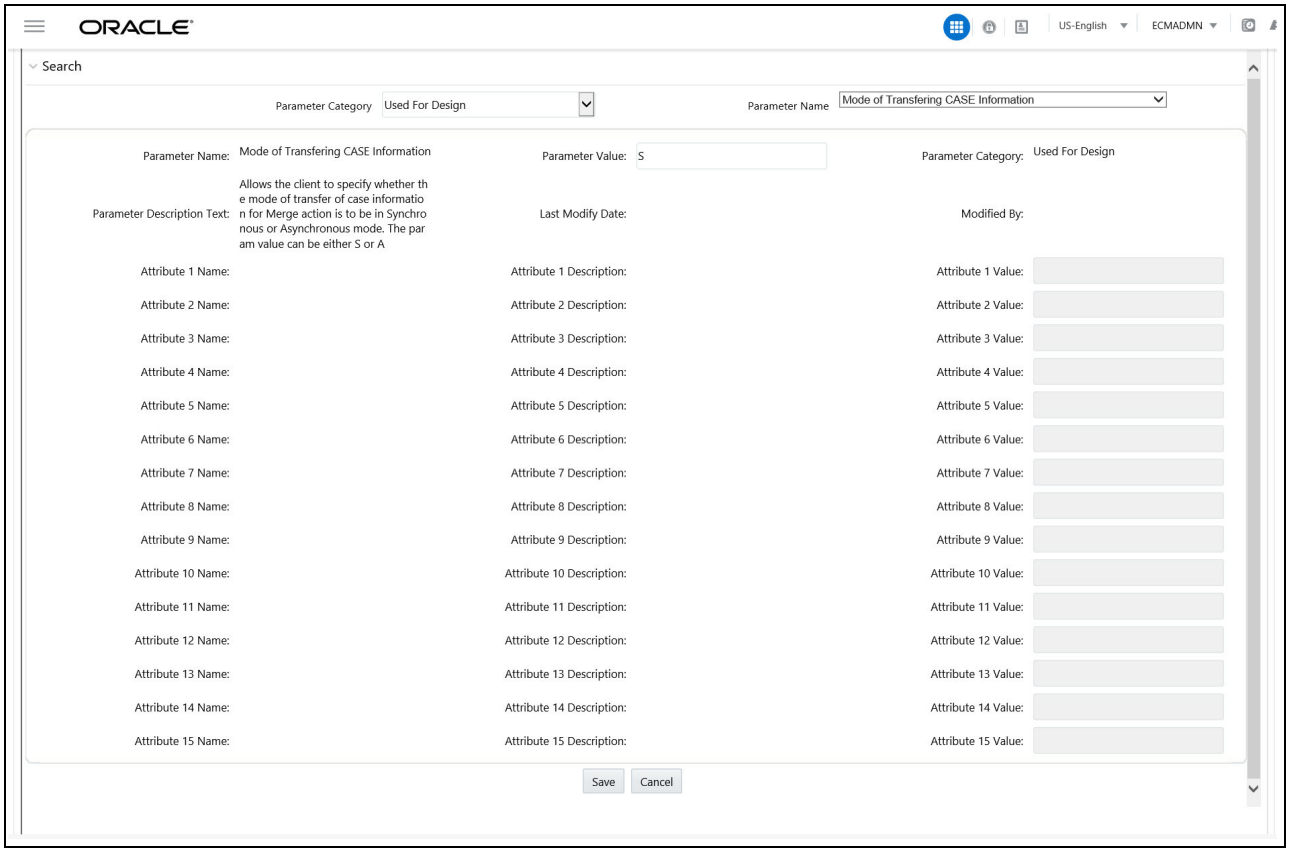
Configuring Mode of Transferring Case Information

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 case until the data transfer action is complete. An Asynchronous allows the user to continue to work on the 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 maybe 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 37. 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 views.

QUEUE_SEQ_ID	ATTRBT_ID	ATTRBT_VAL_TX
Unique sequence ID	Unique Attribute ID. ATTRBT_ID will be referred from KDD_CASEATTRBT_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 the 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 the filter. Date filter requires the 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 38. 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 the 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 the KDD_QUEUE_MASTER.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.

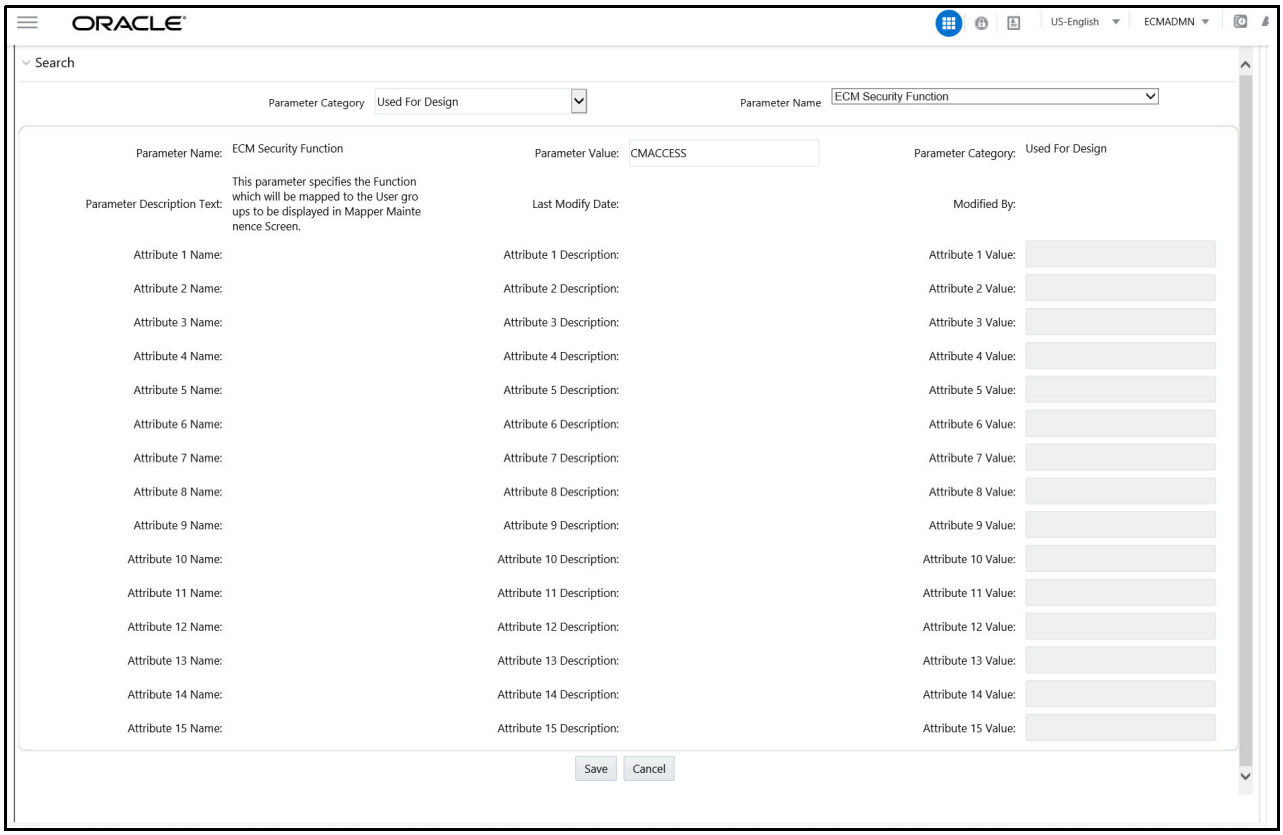


Figure 65. Configuring ECM Security Function

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.

Configuring Default Created Date Range

To configure the default Created To and Created From dates, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used For Design** from the Parameter Category drop-down list.
3. Select **Created Date Range** from the Parameter Name drop-down list.

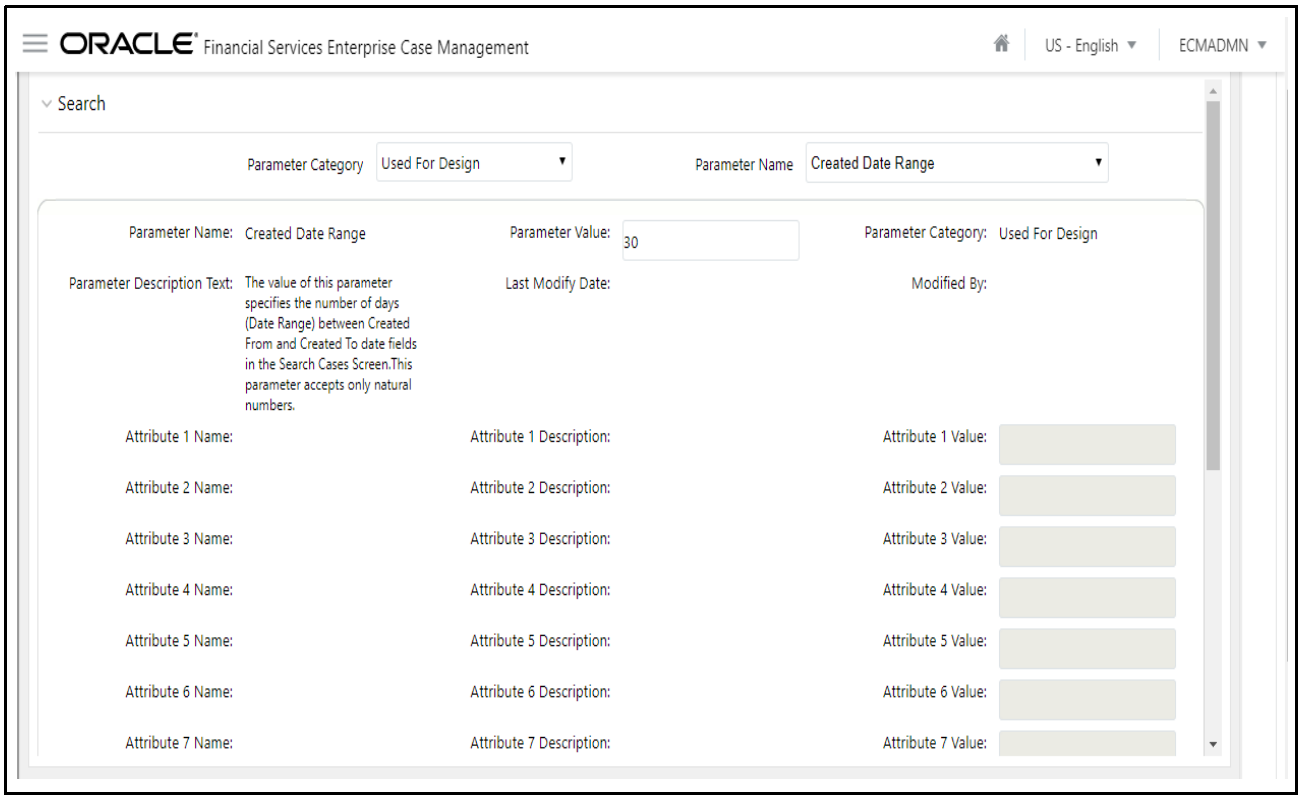


Figure 66. Configuring Created Date Range

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. This defined date range will be displayed on Search Cases page.

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`.

Managing KYC Configurations

Perform the below configurations when ECM integration with KYC is done:

- Configuring KYC Close Service Parameters (KYC Batch case)
- Configuring KYC Customer Dashboard Parameters (KYC Batch Case)
- Configuring CommonGatewayService Parameters
- Configuring createJSONService Parameters
- Configuring KYC Risk Score UI Service Parameters (Onboarding KYC Case)
- Configuring KYC Close Service Parameters (Onboarding KYC Case)

Configuring KYC Close Service Parameters (KYC Batch case)

Refer section **Updating the URL for the KYC Close Service** under Configurations in the ECM UI in *KYC Admin guide*.

Configuring KYC Customer Dashboard Parameters (KYC Batch Case)

Refer section **Updating the BD Application URL for the KYC Customer Dashboard** under Configurations in the ECM UI in *KYC Admin guide*.

Configuring CommonGatewayService Parameters

Refer section **Updating the User Name and Password for the Common Gateway Service** under Configurations in the ECM UI in *KYC Admin guide*.

Configuring createJSONService Parameters

Refer section **Updating the User Name and Password for the Create JSON Service** under Configurations in the ECM UI in *KYC Admin guide*.

Configuring KYC Risk Score UI Service Parameters (Onboarding KYC Case)

Refer section **Updating the User Name and Password for the KYC Risk Score UI Service** under Configurations in the ECM UI in *KYC Admin guide*.

Configuring KYC Close Service Parameters (Onboarding KYC Case)

Refer section **Updating the User Name and Password for the JSON To Table Service** under Configurations in the ECM UI in *KYC Admin guide*.

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

This parameter specifies the web application context and URL of the admin tools application.

Follow these steps if 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 39 describes the attributes which should be configured for enabling and using the administration tools.

Table 39. Configuring Administration Tools

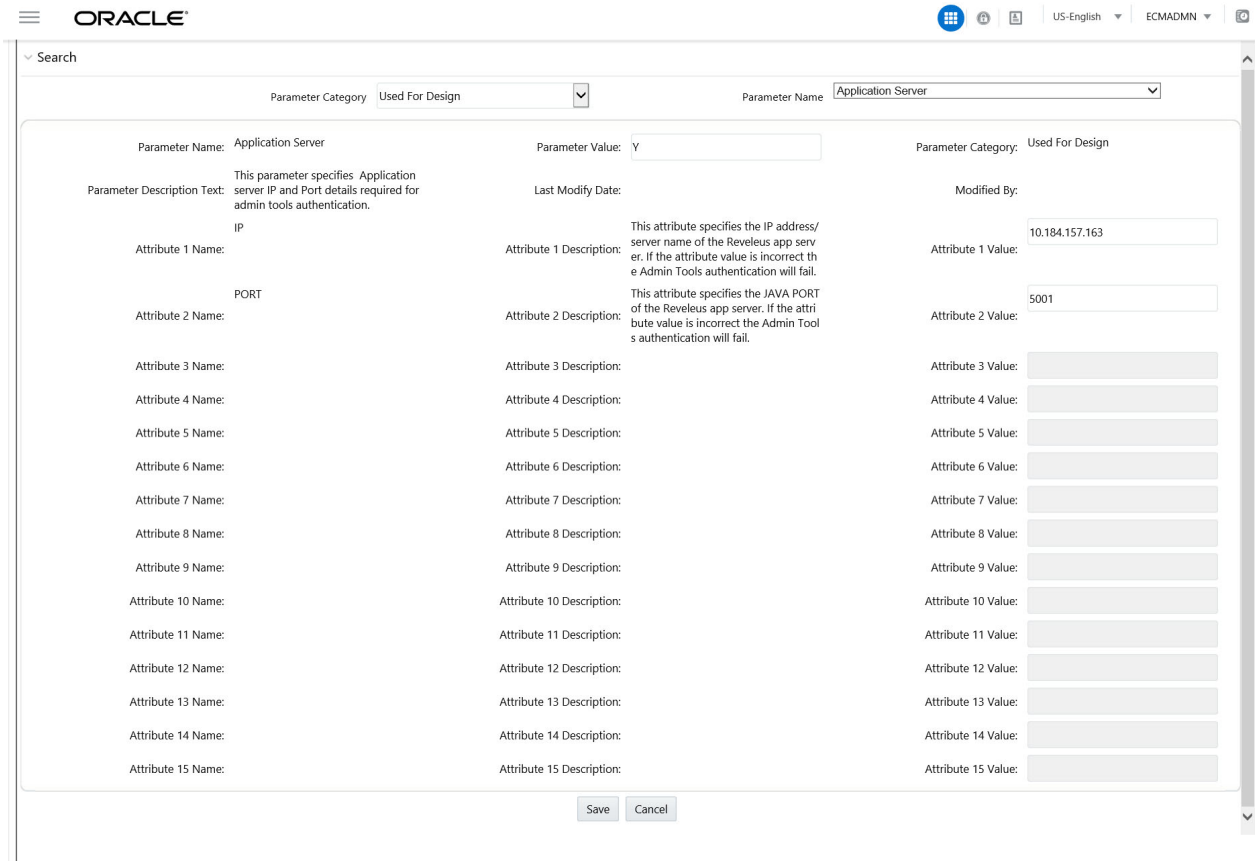
Attribute	Description
APPLICATION_CONTEXT	This parameter specifies the context name of the admin tools application.
ADMINISTRATION_TOOLS_APPLICATION_URL	This parameter specified the URL of the admin tools application.

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 40 describes the attributes to be configured for setting the application server.

Table 40. 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.

CHAPTER 14 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 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.

Note: Define standard comments that is available in the workflow. For more information, see Configuring Standard Comment Data. 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 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'. The parameter will look like '&mStatus=INV'.

You can update **KDD_STATUS.VIEWD_RESULT_STATUS_CD** to **OBS,** if you do not want to display this status in application UI.

Configuring Case Status in CRR

To configure the case status in CRR, follow the below 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
('CCASTR','N',null,null,'Y''Closed - CA STR Filed')
```

   Here, you can replace the Status ID (CCASTR) with your respective STR.

2. In Config schema, add an entry to the AAI_WF_STATUS_B table, as follows:

```
insert into AAI_WF_STATUS_B (V_STATUS_ID,V_APP_PACKAGE_ID) values
('CCASTR','OFS_NGECM')
```

   Here,

   - Status ID (CCASTR) should be the same as provided in KDD_STATUS table.
   - The default package name is **OFS_NGECM.** Do not change this package name.

3. In Config schema, add an entry to the AAI_WF_STATUS_TL table, as follows:

```
insert into AAI_WF_STATUS_TL (V_STATUS_ID, V_STATUS_NAME, V_STATUS_DESC, V_LO-
CALE_CODE, V_APP_PACKAGE_ID) values
('CCASTR', 'Closed - CA STR Filed', 'Closed - CA STR Filed', 'en_US', 'OFS_NGECM')
```

   Here,

   - **Status ID** (CCASTR) should be the same as provided in KDD_STATUS table.
   - **Status Name (`Closed - CA STR Filed`)** should be the same as provided in KDD_STATUS table.
   - The default package name is **OFS_NGECM.** Do not change this package name.

Restricting Case Status

If you need restriction in viewing the cases in a certain Status, then add the entry in KDD_ROLE_STATUS_MAP against Status code. After configuring this, you will be able to see only cases in that Status.

Masking for New Statuses

If you are adding a new status, then perform the following steps:

1. Execute the following query in the Config schema and update V_ATTRIBUTE_VALUE1. This query modifies V_ATTRIBUTE_VALUE1 to pick the new statuses

   SELECT t.*, t.rowid FROM AAI_AOM_APP_COMP_ATTR_MAPPING t where t.v_attr_code='mStatus';

2. Execute the following query in the Config schema and update V_ATTRIBUTE_VALUE1 to include the new statuses.

   SELECT t.*, t.rowid FROM AAI_OJFF_MASKING_ATTR_VAL_MAP t;

Note: You cannot include Closed status everywhere. Investigator and Admin roles should not be mapped to the same users.

3. Execute the below query and update RULE_ATTRBT_VAL in table FCC_UI_RULE_CONF for RULE_ATTRBT = ‘mStatus’ .

   select t.*, t.rowid from fcc_ui_rule_conf t where t.rule_attrbt = 'mStatus'

4. For allowing linking of cases from the Relationship tab, you have to update KDD_STATUS_LINKTYPE_MAP with the new statuses. Entries for open statuses and close statuses are different. The below query can be used as a reference for the same. For open statuses, refer entries for INV and for close statuses, refer entries for CCNSAR

   select t.*, t.rowid from kdd_status_linktype_map t where t.status_cd in ('INV','CCNSAR')

5. Restart the servers to verify the updates.

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 this 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 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 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 recommendation 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 prevented 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)
CA939	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

Column Name	Primary Key	Column Type	Nullable
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 need 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 need 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 a 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 searchedPreviousValue=[];
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 a 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 a 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 15 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

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 an 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 an 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>
   ```

CHAPTER 16 Additional Configuration

This chapter provides the details of additional configuration activities. For more information, see the *Performing Batch 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 the 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 the N_CORRELATION_RULE_SKEY column (rule number) should be the same as defined in the 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
```

Adding Relationship Type values for Involved Parties

You can add or edit the Relationship Type values in Relationship Type drop-down for Involved Parties.

For example, if you have two relationship types as Primary Suspect and Secondary Suspect, then add the following entries for InvolvedPrtyRelType and RelationshipType-InvParty in KDD_CODE_SET_TRNLN table (Atomic Schema) as shown below:

CODE_SET	CODE_VAL	SRC_SYS_CD	CODE_DISP_TX	CODE_SET_DSP
InvolvedPrtyRelType	PS1		Primary Suspect	
InvolvedPrtyRelType	SS1		Secondary Suspect	
RelationshipType-InvParty	PS1		Primary Suspect	
RelationshipType-InvParty	SS1		Secondary Suspect	

The newly added values will reflect in Relationship Type drop-down on Involved Parties UI. This can be viewed in Account, Customer, External Entity and Involved Party tabs.

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 the N_CORRELATION_RULE_SKEY column (rule number) should be the same as defined in the FCC_CORRELATION_RULE table.

Configuring Case Allocation

The Case Allocation feature automatically assigns the new and existing cases to individuals or pools at any point during the case investigation process based on a defined allocation rule. This automation feature saves the time of managers/administrators who otherwise manually go through each case and assign them team members based on select criteria.

You can use this feature by the configuring following tables:

- FCC_ASSGN_RULE_DEFN is used for defining the rules.
- FCC_ASSGN_RULE_USER_MAP is used for mapping the rules to a user/pool.

The allocation task runs along with the correlation batch. But, if you want to run it multiple times in a day, then it can be configured to run independently by scheduling task accordingly in a run-rule framework.

Administrators or Allocation Team Lead can create the Allocation Rules.

Administrators can add multiple filter conditions for a single rule by adding multiple rows with the same Rule ID.

Below is the sample rule that defines an assignment rule by case age greater than 30 days, case type of 'Trade Finance' and of Jurisdiction 'IN-CIC'. To configure this, follow the below steps:

1. To define the rule, add entries in the FCC_ASSGN_RULE_DEFN table. Case allocation rules are defined in table FCC_ASSGN_RULE_DEFN.

V_RULE_NAME	N_RULE_ID	V_FILTER_NM	V_FILTER_OPERATOR	V_FILTER_VAL
TF Cases Older than 30 Days	1	AGE	>	30
TF Cases Older than 30 Days	1	CASE_TYPE_CD	=	'Trade Finance'
TF Cases Older than 30 Days	1	JRSDCN_CD	=	'IN-CIC'

   - V_RULE_NAME: The name used to define the rule.
   - V_RULE_ID: A unique rule ID for the rule.
   - V_FILTER_NM: The column name of the case attribute which is being filtered. Filter names should be the same as the column name in KDD_CASES tale. For example, if the rule is for filtering cases by case score, then the filter name will be 'SCORE_CT".
   - V_FILTER_OPERATOR: A filter operator applicable for the attribute. The framework supports filter operators <, >, >=, <=, =, IN and BETWEEN.
   - V_FILTER_VAL: The filter values for the defined attribute. For example, if the filter is to allocate based on status, then the values would be 'OPEN', 'REVIEW' and so on. These must be values that are defined in the PMF workflow associated with this type of case (as defined with a filter name for that rule)

2. An individual user/pool is mapped to a rule in table FCC_ASSGN_RULE_USER_MAP. When these rules run they make the individual/pool the assignee and the owner of the case. A single user/pool can be mapped to multiple rules if necessary and a single rule can be mapped to multiple individuals/pools. In the below example, a user is mapped to three different rules, so the user will get three different flavors of cases. User capacity is calculated by the cases assigned by each rule but not by aggregated capacity of all the rules mapped to him. Add the following entries in FCC_ASSGN_RULE_USER_MAP table:

V_USER_NAME	V_RULE_NAME	V_ACTIVE	N_USER_ID	N_USER_CAP	N_RULE_ID	N_CURR_CAP
Bob Smith	TF Cases Older than 30 Days	Active	1234	30	1	
Bob Smith	AML Complex Cases	Active	1234	30	2	
Bob Smith	AML Easy Cases	Active	1234	30	3	

   - V_RULE_NAME: The Rule Name to be mapped for the user/group as defined in table FCC_ASSGN_RULE_DEFN.

- N_RULE_ID: The Rule ID of the rule defined in table FCC_ASSGN_RULE_DEFN.
- V_USER_NAME: The name of the user/pool.
- N_USER_ID: The exact User/Pool ID as defined in the KDD_REVIEW_OWNER table.
- V_ACTIVE: The status of the rule. For any value other than 'ACTIVE' the system considers the rule inactive and doesn't allocate cases as per the rule to a user.
- N_USER_CAP: The maximum number of cases that can be allocated to this user for that rule. The system will not allocate cases beyond that number.

Here, N_USER_ID should be same as given in the KDD_REVIEW_OWNER table.

The following query is required to fetch the cases by particular scenario type (SCENARIO_SKEY):

```
(Select t.case_intrl_id
          from kdd_cases t
         inner join fcc_precase_case_map pcm on pcm.v_case_id =
t.case_intrl_id
         inner join fcc_correlation_event_map cor on
cor.n_event_correlation_skey = pcm.n_event_correlation_skey
                              inner join fcc_event_details s on
s.n_event_skey = cor.n_event_skey
         where s.N_SCENARIO_SKEY in (279,403));
```

In the above query, 279,403 represents the scenarios which can be used in this attribute. These are obtained from the N_SCENARIO_SKEY field in the FCC_SCENARIO_MASTER table.

Load Balancing Cases to Users

Cases are allocated by a **Load Balancing** algorithm. The system will filter cases by the first rule and check the users/pools whose capacity is below 50%. Then, it fills that user's bucket up to 50% and moves to the next user and fills their bucket to 50% till all the users are at the same level. If any cases are left over after bringing all users to their 50% capacity, the system will circle back and fill to 75% until all users have the same capacity. After this, if still any cases are left then the system will circle back to the first user and completely fill the bucket. The algorithm then performs the same allocation for the second rule if there are more than one rule mapped to users.

In the below example, the same rule is mapped to two different users. Let's assume, the rule has filtered 125 available cases for assignment and Bob and Sue's buckets are empty. The system will allocate 50 cases to Bob and then 50 cases to Sue. Then, it would circle back and give Bob 25 and Sue zero.

V_USER_NAME	V_RULE_NAME	V_ACTIVE	N_USER_ID	N_USER_CAP	N_RULE_ID	N_CURR_CAP
Bob Smith	TF Cases Older than 30 Days	Active	1234	100	1	
Sue Green	TF Cases Older than 30 Days	Active	1234	100	1	

If after another batch run, there are another 300 cases available for allocation and Bob and Sue's buckets are unchanged after the previous allocation, then the system first fills Bob with 25 cases to bring him to his max and then bring Sue to her max. The remaining 225 will wait until the next run and if the users have the capacity it will assign to them.

The following seeded attributes are available for rule creation. All of these columns are defined in the KDD_CASES table:

Attribute	Function
STATUS_CD	Status
JRSDCN_CD	Jurisdiction
PRIORITY_CD	Case Priority
BUS_DMN_ST	Business Domain
SCORE_CT	Case Score
CASE_TYPE_CD	Case Type
AGE	Case Age

Custom Rule Attributes

If you want to define a rule for an attribute that is not seeded, then you can use SQL script to define an attribute and insert that as the V_FILTER_VAL in the FCC_ASSGN_RULE_DEFN table.

Below is an example of how you can define and insert **Event Scenario** as a rule attribute.

Note: A case can have multiple scenarios as a case can have multiple events and in turn these events can be generated for different queries. So, insert below query to filter scenario through a rule:

```
insert into FCC_ASSGN_RULE_DEFN (V_RULE_NAME, N_RULE_ID, V_FILTER_NM,
V_FILTER_OPERATOR, V_FILTER_VAL)
values ('rule1', 1, 'case_intrl_id', 'in ',('(Select t.case_intrl_id
from kdd_cases t
inner join fcc_precase_case_map pcm on pcm.v_case_id = t.case_intrl_id
inner join fcc_correlation_event_map cor on cor.n_event_correlation_skey =
pcm.n_event_correlation_skey
inner join fcc_event_details s on s.n_event_skey = cor.n_event_skey
where s.N_SCENARIO_SKEY in (XXX,XXX))'));
```

Note: In the above, XXX,XXX represents the scenarios that can be used in this attribute. These is obtained from the N_SCENARIO_SKEY field in the FCC_SCENARIO_MASTER table.

Configuring Case Age

Case age can be calculated based on Business Days or Calendar Days by updating the configurable parameter set in the Installation Parameter table, from the Manage Parameters screen. (For more information, see Configuring Case Age Calculation section).

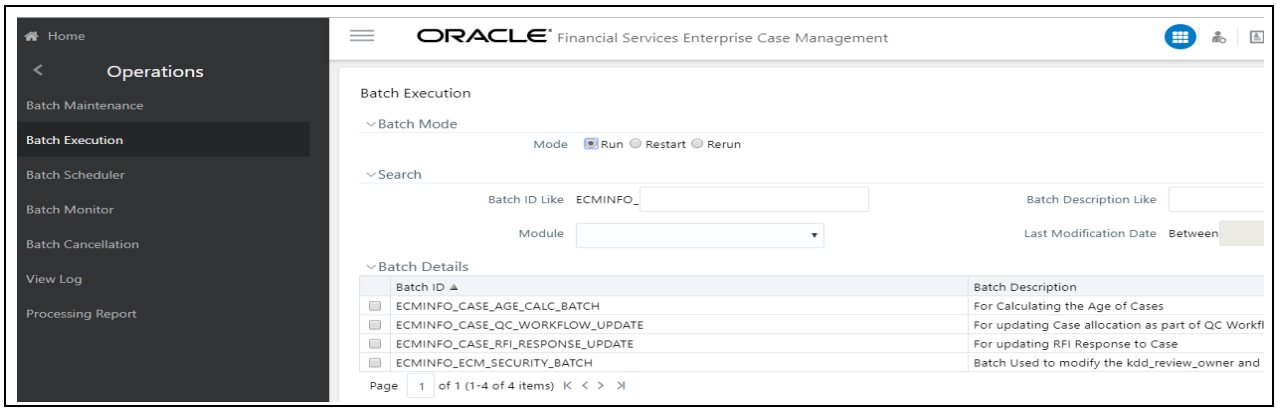
Calculation of Case Age is done by running the Batch <INFODOM>_CASE_AGE_CALC_BATCH. For more information, see Executing Case Age Calculation Batch section.

This will update the KDD_CASES_AGE column with age of the case, calculated in business days or calendar days based on the configuration made in the Installation Parameter table.

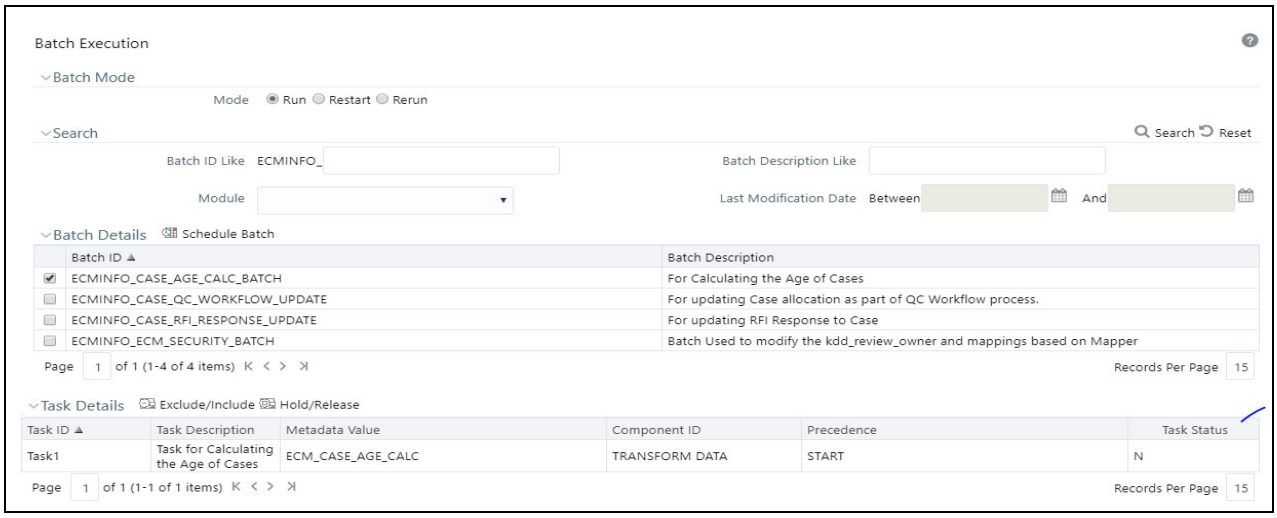
Executing Case Age Calculation Batch

To execute the Case Age Calculation batch <INFODOM>_CASE_AGE_CALC_BATCH, follow the below steps:

1. Login as ECM Administrator.
2. Navigate to the Common Tasks option.
3. Select Operations.
4. Click Batch Execution.



5. Search for <INFODOM>_CASE_AGE_CALC_BATCH (batch and enter the Information Date (MIS date) using Calendar. Click Execute Batch.



6. Click Ok on confirmation box. A batch execution triggered message is displayed.
7. To view the status of batch, navigate to **Batch Monitor** under **Operations**.

Configuring Tabs based on Role

You can control the access of a tab based on role. For example, if the **Account** tab is configured for **Analyst** role, then the only **Analyst** will be able to view the **Account** tab.

1. Identify the tab on which you want to provide the control access to the user (based on Role). Here, ##TAB_NAME## is the placeholder for tab Name.
2. Create an SMS function and map it to the User Role.

   Or

   Select the unique Function Code. ##FUNCTION_CODE## is the placeholder for Function Code.
3. Take a backup of following query results from Config schema:
   select * from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and v_container_name='##TAB_NAME##';

   select * from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='##TAB_NAME##')
4. Execute following queries in Config schema before replacing the ##placeholder## with correct values:
   update AAI_FF_FORMS_CONTAINERS_B t set t.v_view_mode=1, t.v_function_codes='##FUNCTION_CODE##' where t.v_form_code='CM_CASE_CONTEXTN' and v_container_name='##TAB_NAME##'

   delete from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='##TAB_NAME##')
5. Restart both application and web servers.

Example:

The following example will explain configuring the Account tab for a specific user role.

1. Create a function called "TEST".
2. Take a backup of following query from Config schema:
   select * from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and v_container_name='**Account**';

   select * from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='**Account**')
3. Execute following queries in Config schema before replacing the placeholders with correct values. That is, function code as **TEST** and tab name as **Account**.
   update AAI_FF_FORMS_CONTAINERS_B t set t.v_view_mode=1, t.v_function_codes='**TEST**' where t.v_form_code='CM_CASE_CONTEXTN' and v_container_name='**Account**'

   delete from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='**Account**')
4. Restart both application and web servers.

Adding Event Decision for Customer Screening

If you want to add new event decisions in Event Decision drop-down of Customer Screening UI, then update FCC_EVENT_STATUS_B, FCC_EVENT_STATUS_TL, FCC_CASETYPE_EVENT_STATUS_MAP tables. By default, True Positive and False Positive values are provided from the installer (Status ID 3 and 4).

To add a new status value, add the entries into FCC_EVENT_STATUS_B, FCC_EVENT_STATUS_TL, FCC_CASETYPE_EVENT_STATUS_MAP tables and make a corresponding entry into KDD_ACTION table describing the new status added and mapping has to be provided in KDD_INSTALL_PARAMS table:

PARAM_ID	PARAM_NM	PARAM_VALUE_TX
500	CS_EVENT_DECISION_ACTION_MAP	3:963,4:964,5:800

Status ID populates from FCC_EVENT_STATUS_B and Action ID comes from KDD_ACTION.

These changes will be recorded in the Audit History tab.

Adding Search Results Fields based on Case Type

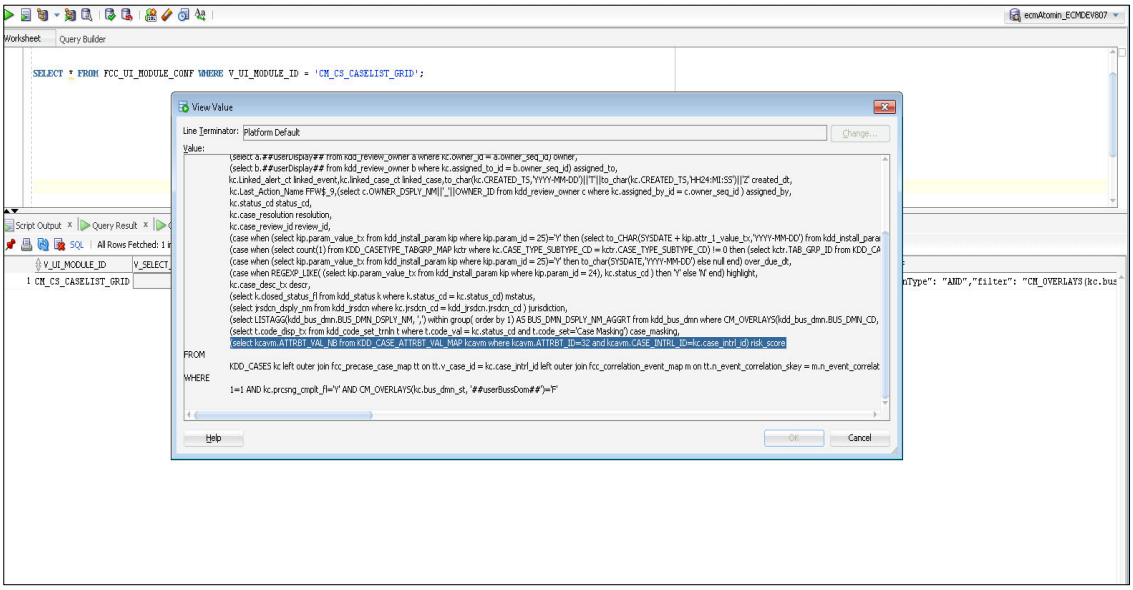
You can define which attributes should be displayed in the search results for each case type.

Example: for CS, you can add attributes like Customer Name, Watch List ID/Name and others that are specific to CS cases.

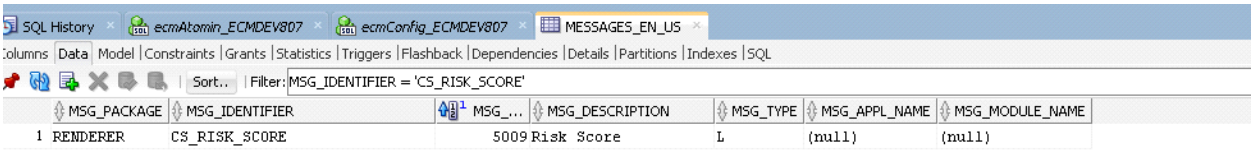
If you want to see a focus column in the case search results, then add this as an attribute. This shows the Focus and the Focus Name ('CU Bob Smith') of the focal entity associated with the case. This is an optional attribute since some cases will have more than one focus.

Below example shows how to add a new column 'Risk Score' to the existing case type:

1. Update the select query that defines all fields that are returned in the search results to include the new field. In table FCC_UI_MODULE_CONF where V_UI_MODULE_ID equals to CM_CS_CASELIST_GRID, update V_SELECT_QUERY field to include the new column in the select part of the query. In this example, we are adding 'risk_score'.



2. The header label for the above column (that is, 'risk_score') needs to be rendered from MESSAGES_EN_US table. If it is not already listed, then make an entry in the MESSAGES_EN_US table (with config schema) with the MSG_IDENTIFIER as 'CS_RISK_SCORE' and MSG_PACKAGE as 'RENDERER' as shown below.



3. Define column details. In table FCC_UI_MODULE_CONF where module ID equals to CM_CS_CASELIST_GRID, update V_MODULE_PROP field to include the column definition for the value added above. Each value has the following attributes:

   "key": "risk_score",

   "locale_code":"RENDERER.CS_RISK_SCORE",

   "align": "right",

   "headerAlign": "left",

   "width": "0.08",

   "dataType": "float",

   "displayType": "number",

"draggable":true,

"resizable":true,

"sortable":true,

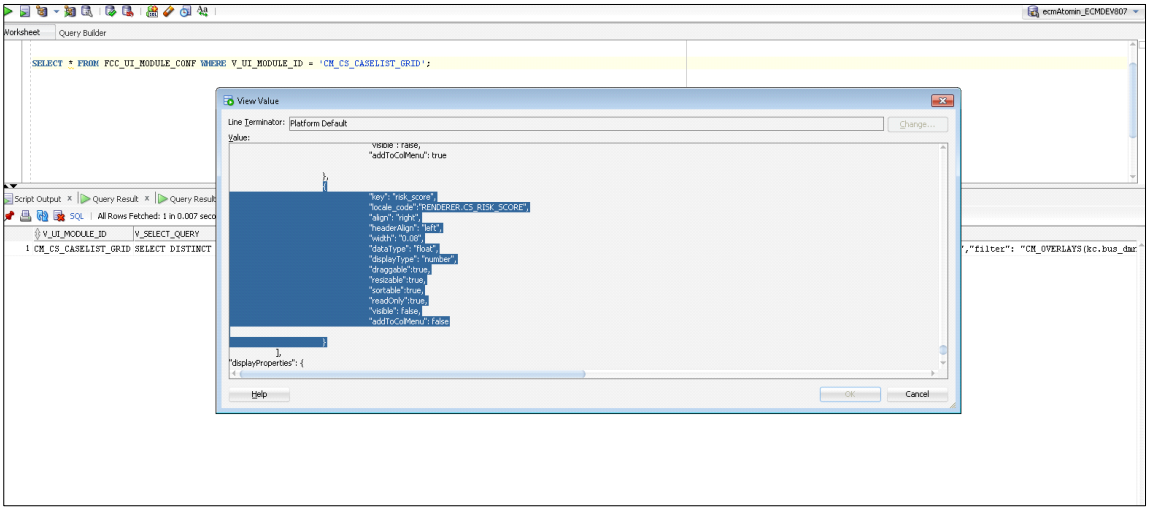
"readOnly":true,

"visible": false,

"addToColMenu": false

Note:

- 'key' property should match with the 'alias' name given in the query defined in Step 1.
- The 'locale_code' is the label for the column header and it is rendered from the MESSAGES_EN_US table as explained in Step 2. It follows the convention [MSG_PACKAGE].[MSG_IDENTIFIER] from the MESSAGES_EN_US table.
- For the new column, 'visible' property should be set to False.
- For the new column, 'addToColMenu' property should be set to False.
- The other variables define the column's functionality.
- If multiple case types are selected to be searched on that have conflicting search results a default set of fields are displayed, then set the "visible" and "addToColMenu" to True to show this field in that default setting.



4. Define the new field in table KDD_CASEATTRBT_MASTER and then enter it in table KDD_CASEATTRBT_COLMNID_MAP.

KDD_CASEATTRBT_COLMNID_MAP

Columns | Data | Model | Constraints | Grants | Statistics | Triggers | Flash

Sort.. | Filter:

	ATTRBT_ID	COLMN_ID
1	1	case_id
2	3	case_type
3	4	status
4	5	case_title
5	6	jurisdiction
6	7	bus_domain
7	15	priority
8	18	created_dt
9	21	due_dt
10	23	owner
11	25	assigned_to
12	26	linked_event
13	27	linked_case
14	29	descr
15	32	risk_score

5. Assign the new column ID to the applicable case types and define the order. Define the visible as default, if required. Map all the required column IDs to the selected case type in the KDD_CASETYPE_COLMNID_MAP table.

KDD_CASETYPE_COLMNID_MAP

Columns | Data | Model | Constraints | Grants | Statistics | Triggers | Flashback | Dependencies | Details | Partitions | Indexes | SQL

Sort.. | Filter: CASE_TYPE_SUBTYPE_CD='KYC_CORP'

	CASE_TYPE_SUBTYPE_CD	COLMN_ID	DPLY_ORDR	DFLT_VISIBLE_FL
1	KYC_CORP	case_id	1	Y
2	KYC_CORP	case_type	2	Y
3	KYC_CORP	status	3	Y
4	KYC_CORP	case_title	4	Y
5	KYC_CORP	jurisdiction	5	N
6	KYC_CORP	bus_domain	6	N
7	KYC_CORP	priority	7	Y
8	KYC_CORP	created_dt	8	Y
9	KYC_CORP	due_dt	9	Y
10	KYC_CORP	owner	10	N
11	KYC_CORP	assigned_to	11	N
12	KYC_CORP	linked_event	12	N
13	KYC_CORP	linked_case	13	N
14	KYC_CORP	descr	14	N
15	KYC_CORP	risk_score	15	Y

6. After adding these columns for a new Case Type, create the new Case Type. If the new Case Type is created already or adding columns for an existing Case Type, then re-load the Case Designer screen and edit. Again save the Case Type.

Note: From the case designer, edit the description if required. For example, enter a space at the end of the description and then remove the space and click Save.

7. Verify the configuration in the Search Case page.

Adding and Configuring Case Type Attribute

You can create and configure a case attribute which can be used in Case Type Designer. You can define the attribute in the Case Attribute Master table (KDD_CASEATTRBT_MASTER). Here, you define the attribute name and the type of attribute.

1. Define the type of attribute in the ATTRBT_TYPE_CD column. The following types are available:
   - Text box: Allows for string values
   - Hierarchy: The field brings the data from another table. The table it pulls from is defined in Case Attribute Value (KDD_CASEATTRBT_VAL). In this table, the following should be defined for each hierarchy attribute. It is not possible at this time to have nested hierarchy drop-downs.
     - The first row defines the table where the values should be retrieved.
     - The second row is the ID attribute
     - The third row defines which column to show in the drop-down list
     - The fourth row is a Yes/No values to define if the multiple select option should be shown for the drop-down.
     - The fifth row is used to specify the filter ('Where' clause) for the table if any is needed.
     - The sixth row is used to specify the order by attribute. If not specified, it orders the values based on the description or shown column (third row value).
   - Drop-down: This is used for defining a finite set of values that do not come from a table. The Case Attribute Value table is also used to define the list. For each attribute, there should be one row for each value in the drop-down. The Drop-down will always be single select.
   - Date: The format of the date field is defined in the ATTRBT_DT_FRMT column of the table.
   - Textarea: Allows for text areas
   - Checkbox: Allows for any number of values to be check-box options. The Case Attribute Value table is also used to define the list. For each attribute, there should be one row for each value that needs a checkbox. Checkbox attributes are multi-select
   - Number: The number field automatically comes with the up/down arrows when displayed.
   - Derived: This type allows you to derive the attribute from information related to the case in the case. Derived Attributes are only visible in the Case Context Area of the case. They are not shown on the Manual Case Creation page or on the search page (even if configured as such). They are also read-only in format. Any value can be derived as long as it can be obtained from the Case ID.

Note: If the attribute is mandatory for all case types, then the ATTRBT_MNDTRY_FL column is set to Y for that attribute.

2. For Derived type attributes code, define the query that retrieves the value. Enter the query into the ATTRBT_VAL column of the **KDD_CASEATTRBT_VAL** table. Both request and session parameters are supported. You can specify them using the below notation:

   Request Parameter: @@ ParameterName@@

   Session Parameter: ## ParameterName##

3. Define the behavior of each attribute that is how it behaves in the UI need to be defined. Define this in Case Attribute Behavior table **KDD_CASEATTRBT_BHVR**. Define the following page codes in **PAGE_CD** column for every attribute:
   - Case Designer: Controls the attribute's behavior in Case Type Designer
   - Create: Controls the attribute's behavior in Manual Case Creation
   - Modify: Controls the attribute's behavior in the Case Context
   - Operator: If the attribute is a number field this controls if there is an operator in the search field for this attribute. Current available operators are Greater than Equal to, Less than Equal to and Equal To.
   - Search: Controls the attributes behavior in Case Search
4. Define the behavior of each page code in the **ATTRBT_MODE_NB** column:
   - 1: Editable
   - 2: Disabled
   - 3: Hidden
5. For derived type attributes, a record for each page code needs to be added to the **KDD_CASEATTRBT_BHVR** table. You can define the following modes:
   - CaseDesigner: 1
   - Create: 3
   - Modify: 2
   - Operator: 3
   - Search: 3

Adding and Configuring Search Attributes

You can customize new search attributes in ECM. Following types of Search Attributes available based on its visibility:

There are following two types of Search attributes:

- Generic Search Attribute
- Case Type Specific Search Attributes

Both Generic and Case Type Specific search attributes can search in two ways based on the tables in which the search is performed.

1. KDD_CASE_ATTRBT_VAL_MAP table (Pure Optional Attribute):
   - This type of search attribute performs the search only on the optional attributes present in KDD_CASE_ATTRBT_VAL_MAP. Example: Risk Score. For more information, see the *Adding and Configuring Search Attributes* section.
2. Searching on a field stored in any other table:
   - This type of search attribute performs the search on any table like KDD_CASES, KDD_CASE_ACTIONS or any other table which can be filtered based on join with KDD_CASES's CASE_INTRL_ID column.

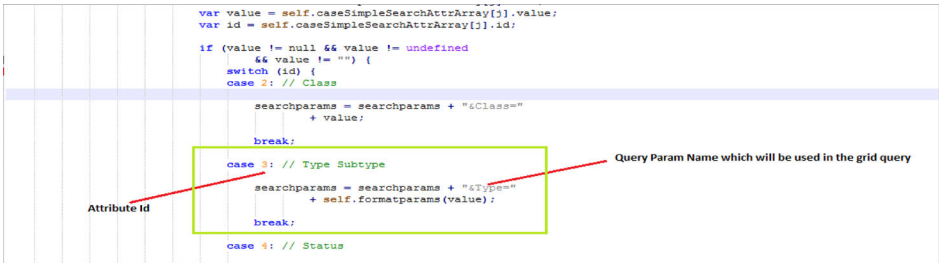
Generic Search Attribute

This type of search attribute implies to all Case Type. It will be available for all case types. It can be displayed in the Less Criteria Section/ More Criteria section. An example is Case Class or Case Created Date.

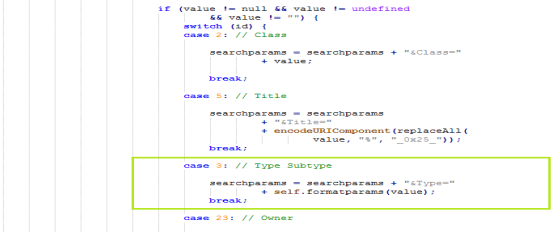
Perform below additional changes in <<deployedir>>/ ojff/js/viewModels/searchCase.js to customize the generic search attributes:

1. Add the Search Attribute in the **simpleSearchAtrArray** for respective Attribute ID. Enter the attribute ID in this array in the order you want it to appear.

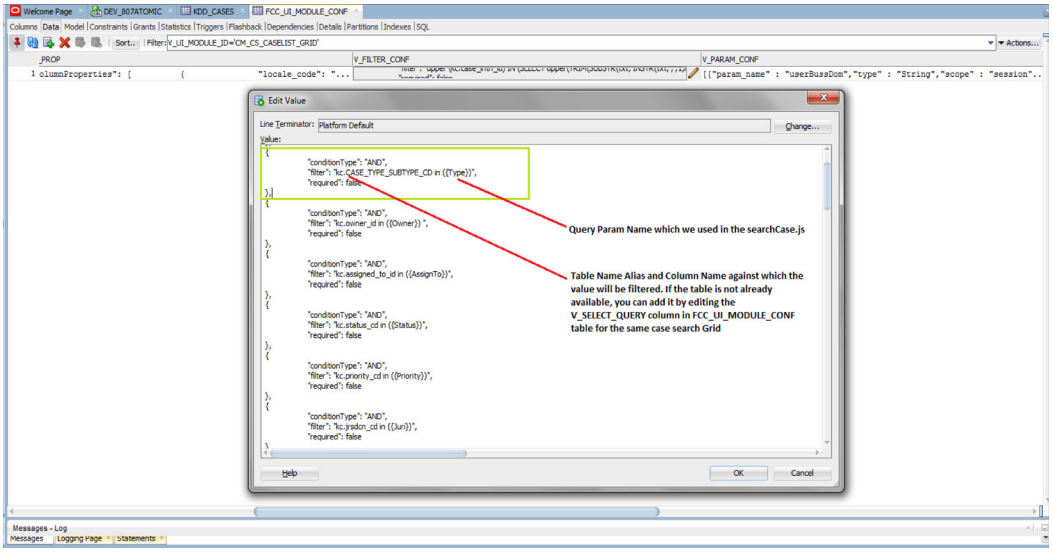
2. Add the search parameter passing code for respective Attribute ID under **self.buttonClickSimpleSearch** function.



3. Add the search parameter passing code for respective Attribute ID under **self.buttonClickSearch** function.



4. Configure the search parameter in the `FCC_UI_MODULE_CONF` table for `V_UI_MODULE_ID='CM_CS_CASELIST_GRID'`. To configure, the `V_FILTER_CONF` entry should be updated with the JSON object for the new search parameter.

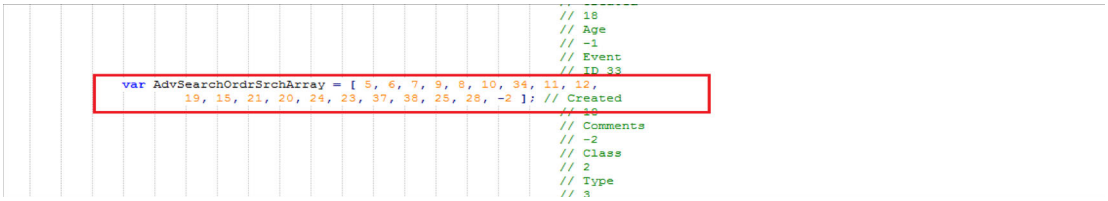


Case Type Specific Search Attributes

This type of search attribute applies only to the Case Type to which it is associated. It will be shown only in the Optional Attribute Area in More Criteria Section and only when the user selects a Case Type. An example is Risk Score which is displayed when the KYC Case Type is selected.

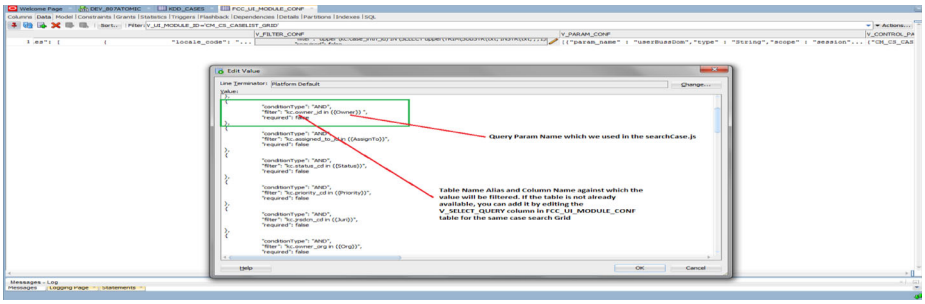
Perform below additional changes in `<<deployedir>>/ ojff/js/viewModels/searchCase.js` to customize the search attributes:

1. Add the Search Attribute in **AdvSearchOrdrSrchArray** for respective Attribute ID. Enter the attribute ID in this array in the order you want it to appear.



2. Add the search parameter passing code for respective **AttributeId** under **self.buttonClickSearch** function.

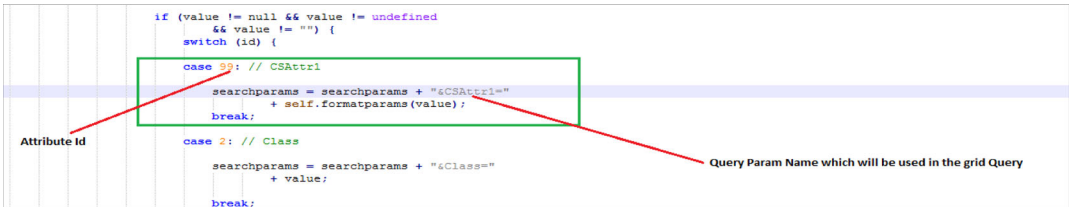
3. Configure the search param in the `FCC_UI_MODULE_CONF` table for `V_UI_MODULE_ID='CM_CS_CASELIST_GRID`. To configure, the `V_FILTER_CONF` entry should be updated with the JSON object for the new search parameter



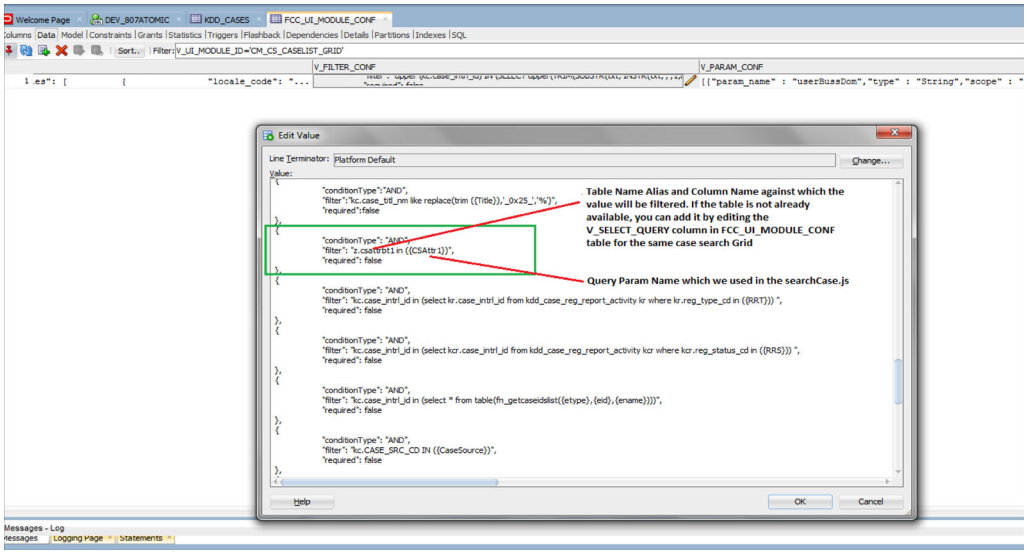
Note: Case type Specific Search Attribute whose search is based on the KDD_CASE_ATTRBT_VAL_MAP table, then no advanced configuration required.

Perform below additional changes in `<<deployedir>>/ ojff/js/viewModels/searchCase.js` to customize the Case Type Specific Search Attribute whose search is based on any other table:

1. Add the search param passing code for respective Attribute ID under **self.buttonClickSearch** function.



2. Configure the search param in the FCC_UI_MODULE_CONF table for V_UI_MODULE_ID='CM_CS_CASELIST_GRID. To configure, the V_FILTER_CONF entry should be updated with the JSON object for the new search param.



Adding and Configuring Derived Attribute

You can define the attribute type as "Derived" which will display in the context area of Case Summary UI.

You can add attributes like Show Case Age, Last Action Taken, Case Created By, Last Updated Date, Last System Added Event Date, Scenario to specific to Case context.

For example, if you want to see a Case Age in the case context, then add this as a derived attribute.

1. Define the basic attribute details in KDD_CASEATTRBT_MASTER with type as "Derived".

ATTRB...	ATTRBT_NM	ATTRBT_DESC_TX	ATTRBT_DT_FRMT	ATTRBT_TYPE_CD	ATTRBT_MNDTRY_FL
39	Case Reopen Count	Displays the number of time the case was reopened	(null)	Derived	N

2. Below is the request attribute passed as part of OOB to the getCaseDetails Service:
caseId (CaseId of the case whose details page is currently accessed)

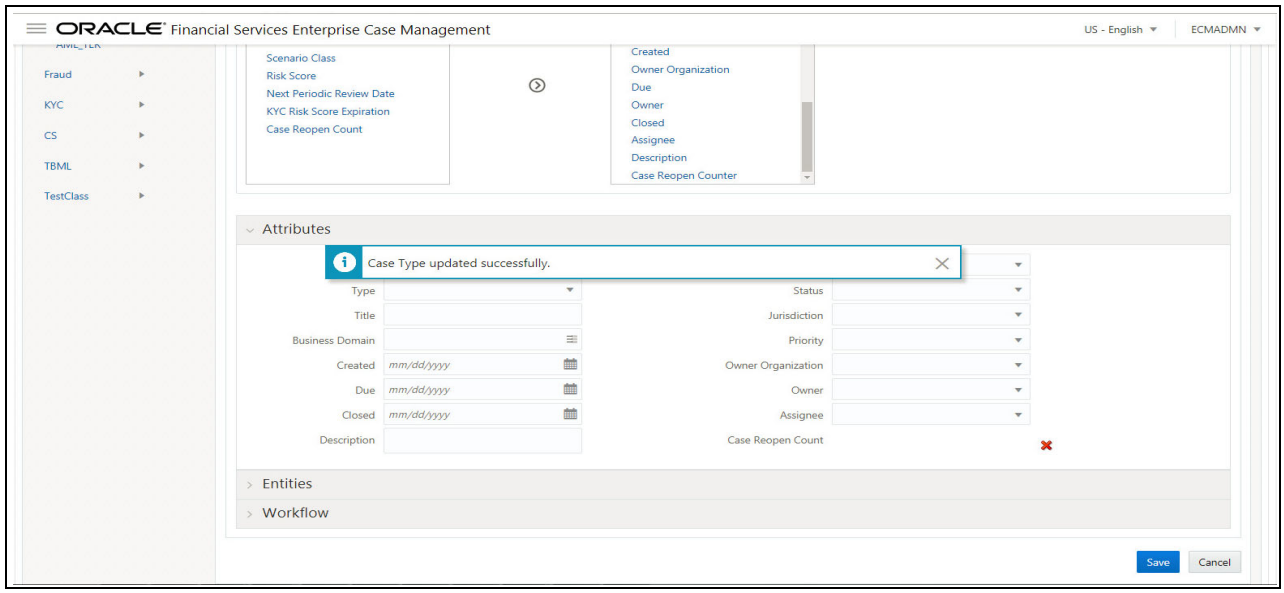
ATTRBT_ID	ATTRBT_SEQ_NB	ATTRBT_VAL
39	1	select count(*) from kdd_case_actions where CASE_INTRL_ID='@@caseId@@' and ACTION_ID=207

3. Define the behavior of the attribute in KDD_CASEATTRBT_BHVR table:

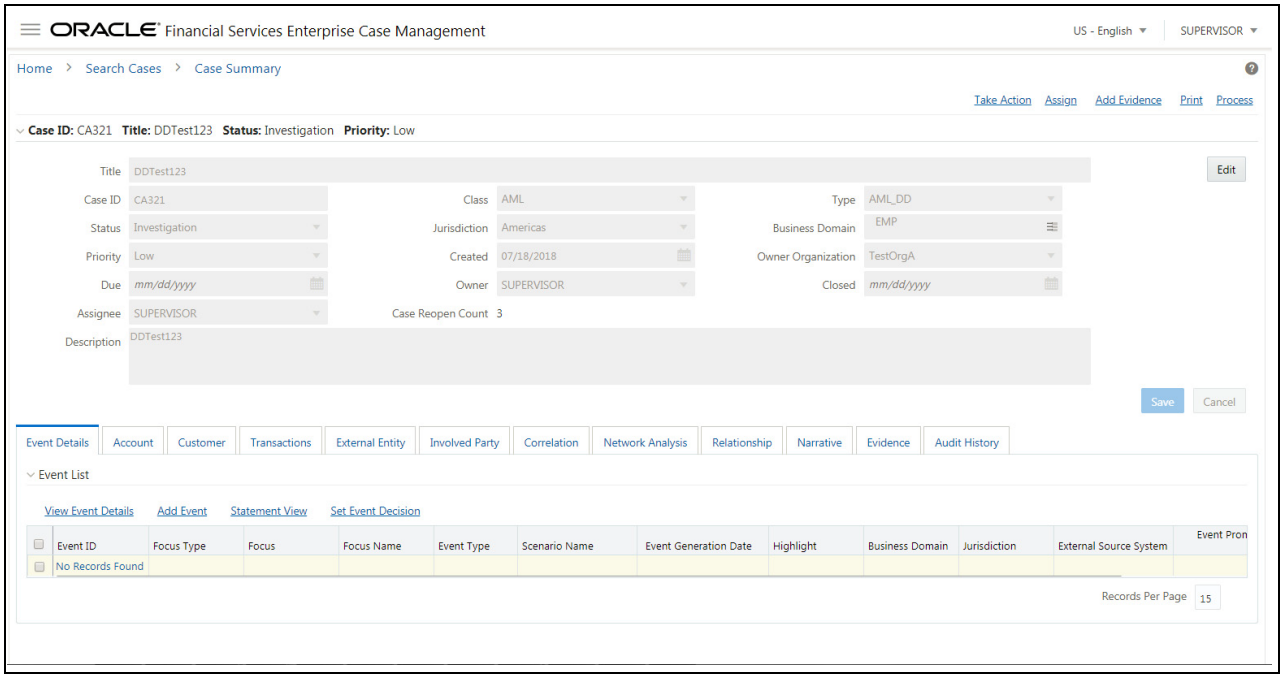
ATTRBT_ID	PAGE_CD	ATTRBT_MODE_NB
39	CaseDesigner	1
39	Create	3
39	Modify	2
39	Operator	3
39	Search	3

Note that the derived attribute is supported only in Case Designer (for associating/Disassociating) the derived attributes to case types and in Case Details Page (Modify Page) for showing the derived attribute value. Derived Attributes are not displayed on the **Create/Search** page even if configured as visible in the KDD_CASEATTRBT_BHVR table. Also, Derived attributes will be displayed in a read-only format.

4. Associate the newly created attribute to the required case type using Case Designer UI.



5. Login as a supervisor and check the Case details of the respective case type for which you have added the derived attribute.



Configuring the Case Title

During the Batch execution, all the cases will be updated with the common Case title (correlation rule name). It will be difficult to identify the case. To resolve this, you can update the values in the V_CASE_TITLE_RULE field of FCC_CORRELATION_RULE and add a task manually before batch execution.

The value defined in this field will be populated on UI after batch execution.

To configure the case tittle, follow the below steps:

1. Update the values in the V_CASE_TITLE_RULE field of FCC_CORRELATION_RULE. For example, customerName, eventType. For more information on FCC_CORRELATION_RULE table, see *Configuring Correlation Rules* section.
   For AML case type, the following attributes can be defined:

   AML:focusType,focusEntityName

   Example, ACCOUNT-YUV : CUSTOMER-RICKY NAME GIBSON : ACCOUNT-SAPNA GOBA: ACCOUNT-SMITH

   For CS case type, the following attributes can be defined:

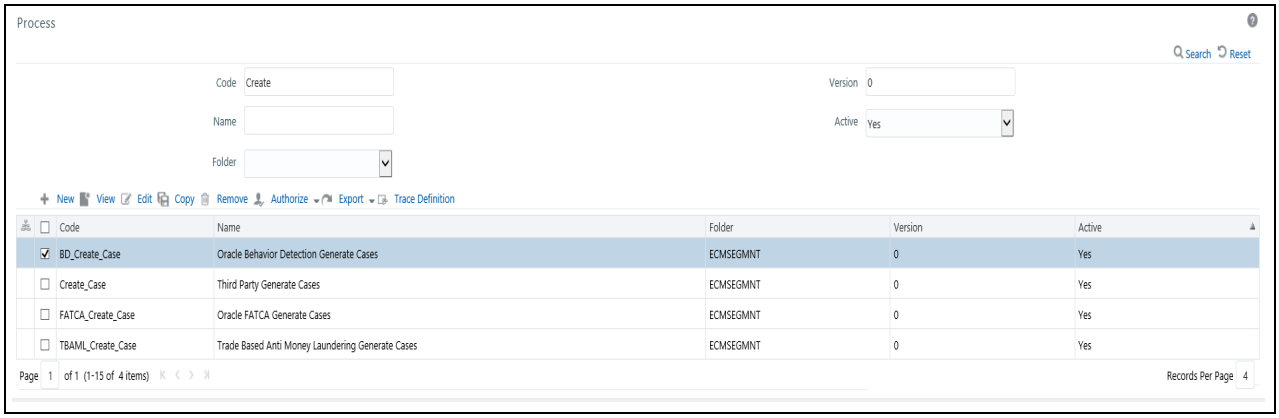
   CS: customerName, eventType

   For KYC case type, the following attributes can be defined:

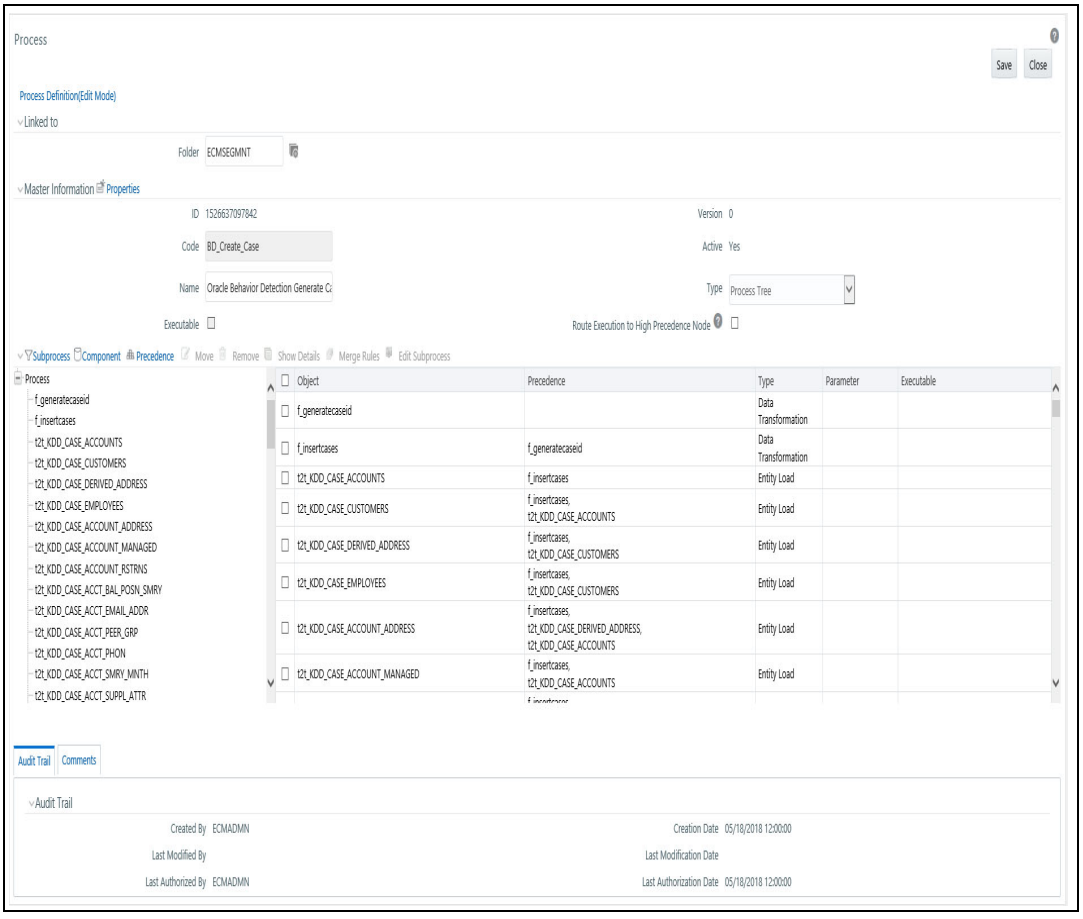
   KYC: customerName, kycRiskScore, jurisdiction, businessDomain

2. Create a task casetittle under BD_Create_Case/Create_Case process manually before batch execution.
   1. Navigate to Enterprise Case Management Application.
   2. Go to the Common task section. Select the **Run Rule Framework**.

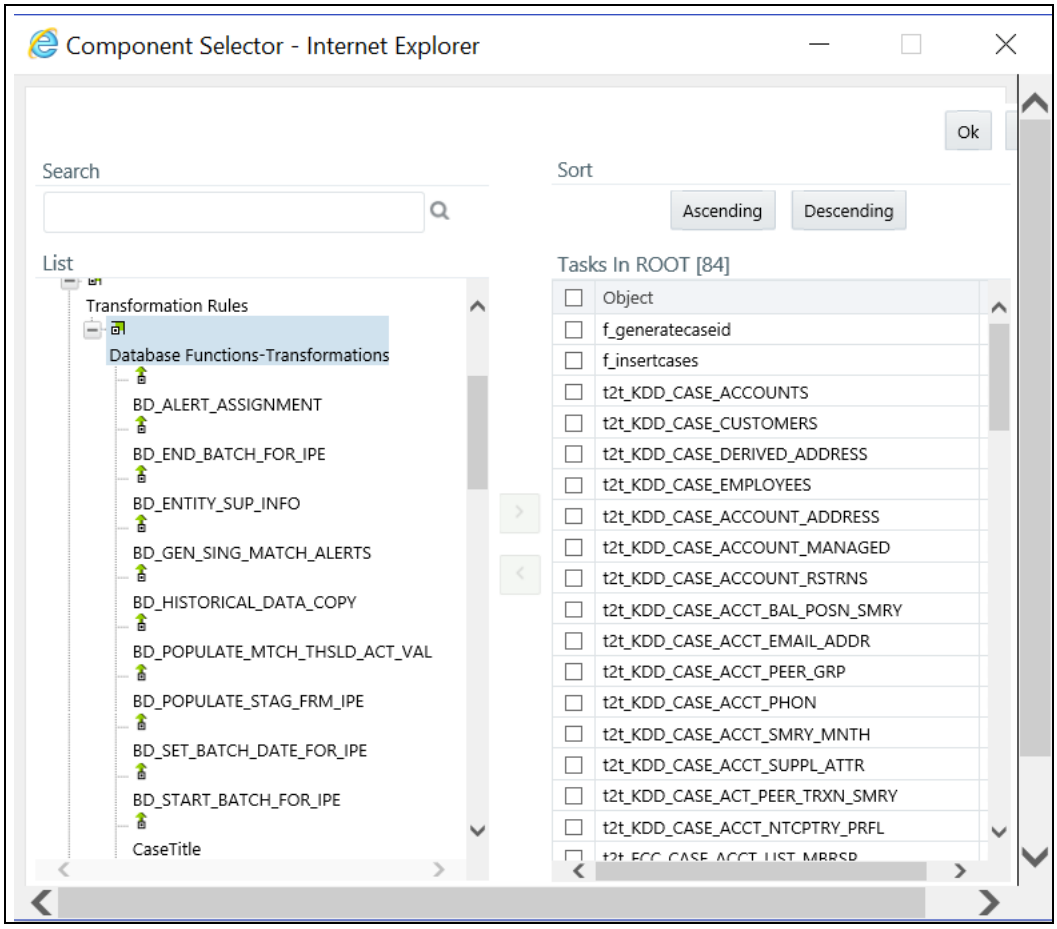
3. Click **Process**. The Process window is displayed with the available Processes. Search for 'Create process'. The list of processes will be displayed.



4. Select the BD_Create_Case and click **Edit**.



5. Click **Component.** The Component Selector window is displayed. Under **Transformation Rules**, select CaseTittle and move it to the task list.



6. Set the precedence of the task after f_insertcases.

Configuring a Case as Read Only

An Administrator can define the full access to some case types to the specific user and make some case types to read-only.

For example, if a user has access to case types AML, FR, and KYC, then Administrator can define the view and take the action access to AML case and read-only access to KYC and FR cases for that user. You can only view the case in read-only access but cannot edit the case.

To configure the case as read-only, follow the below steps:

1. Define the Owner Sequence ID (OWNER_SEQ_ID) and Case type (CASE_TYPE_ID) in KDD_REVIEW_OWNER_CSETYP_RDONLY table.

   Here, Owner Sequence ID value should be the same as defined in the KDD_REVIEW_OWNER table. Case type value should be the same as the KDD_REVIEW_OWNER_CASE_TYPE table.

2. Log-in ECM UI as supervisor (or any other user).

Adding a New Scenario

User can define their own scenarios in the FCC_SCENARIO_MASTER table

Column Name	Primary Key	Column Type
N_SCENARIO_SKEY	Y	NUMBER(22)
V_SCENARIO_NAME		VARCHAR2(250 CHAR)
V_SCENARIO_DESCRIPTION		VARCHAR2(4000 CHAR)
V_SCENARIO_CLASS_CD		VARCHAR2(250 CHAR)
V_SCENARIO_DISPLAY_NAME		VARCHAR2(250 CHAR)
V_SCENARIO_CATALOG_ID		VARCHAR2(250 CHAR)
V_SCENARIO_FOCUS_ENTITY_CD		VARCHAR2(250 CHAR)
N_SCENARIO_SCORE		NUMBER(22)
ORIG_SCENARIO_SKEY		NUMBER(22)

- N_SCENARIO_SKEY – Unique Sequence ID
- V_SCENARIO_NAME – Name of the Scenario
- V_SCENARIO_DESCRIPTION – Description of the Scenario
- V_SCENARIO_CLASS_CD – Class of scenario
- V_SCENARIO_DISPLAY_NAME – Display name of scenario
- V_SCENARIO_CATALOG_ID – Catalog ID of scenario
- V_SCENARIO_FOCUS_ENTITY_CD – Focus entity code of scenario
- N_SCENARIO_SCORE – Scenario score. This column can be Null.
- ORIG_SCENARIO_SKEY – Scenario ID from the Source system

Configuring Quality Control (QC) Sampling Rules

You can define one or many sampling rules, based on which cases will move in the workflow for quality analysis.

To add a QC sampling rule:

1. Add the entries in KDD_QC_RULE_MASTER table. This table used to define the overall structure of the sampling rules.

.

Column Name	Primary Key	Column Type	Nullable
RULE_ID	Y	NUMBER(10)	
RULE_NM		VARCHAR2(1000 CHAR)	Y

RULE_DESC		VARCHAR2(4000 CHAR)	Y
SAMPLE_QNTITY_TYPE		VARCHAR2(300 CHAR)	Y
SAMPLE_QNTITY		NUMBER(10)	Y
DS_ID		NUMBER(10)	Y
ACTIVE_FL		VARCHAR2(1 CHAR)	Y
LAST_UPDATED_DT		DATE	Y
LAST_UPDATED_BY		VARCHAR2(20 CHAR)	Y
COMMENTS		VARCHAR2(4000 CHAR)	Y
PRIORITY_CD		NUMBER(10)	Y
ACTION_CD		VARCHAR2(20 CHAR)	Y

- **RULE_ID:** Unique identifier of the rule.
- **RULE_NM:** Name of the rule. This should be unique name.
- **RULE_DESC:** Description of the rule.
- **SAMPLE_QNTITY_TYPE:** Define the quality type as PERCENTAGE or COUNT.
  - Enter PERCENTAGE if the system has to select a percentage of cases for QC from the candidate superset.
  - Enter COUNT if the system has to select a specific count of cases for QC from the candidate superset.
- **SAMPLE_QNTITY:** Enter the sampling quality value in numerals. For example,
  - If SAMPLE_QNTITY = 10 and SAMPLE_QNTITY_TYPE = PERCENTAGE, then system will take 10% of the candidate cases for QC.
  - If SAMPLE_QNTITY =10 and SAMPLE_QNTITY_TYPE = COUNT, then the system will select 10 candidate cases for QC.
- **DS_ID:** Unique identifier of the dataset that is associated with the rule. The dataset contains the sampling logic (SQL) for this rule. This field references the DS_ID column in KDD_QC_DATASET_MASTER and KDD_QC_DATASET_VALUES tables.
- **ACTIVE_FL:** This flag indicates whether the rule can be used during the QC batch.
  - If this is set to "Y", then the system will run this rule during the QC batch.
  - If this is set to "N", then the system will ignore this rule when the QC batch is executed.
- **LAST_UPDATED_DT:** Date when the record was last updated.
- **LAST_UPDATED_BY:** User name who last updated the record
- **COMMENTS:** Enter the comments
- **PRIORITY_CD:** Define the priority of the rule.
- **ACTION_CD:** This action code is used to identify the resulting status of a case that is selected for QC as a result of this sampling rule. This should be the same as ACTION_CD column of the KDD_ACTION table.

2. Add the dataset entries in the KDD_QC_DATASET_MASTER table. This table is used to define the dataset associated with each rule.

Column Name	Primary Key	Column Type	Nullable
DS_ID	Y	NUMBER(10)	
DS_NM		VARCHAR2(1000 CHAR)	Y
DS_DESC		VARCHAR2(4000 CHAR)	Y
LAST_UPDATED_DT		DATE	Y
LAST_UPDATED_BY		VARCHAR2(20 CHAR)	Y
COMMENTS		VARCHAR2(4000 CHAR)	Y

- **DS_ID:** Unique identifier of the dataset that is associated with the rule. The dataset contains the sampling logic (SQL query) for the rule. This field references the DS_ID column in KDD_QC_RULE_MASTER and KDD_QC_DATASET_VALUES tables.
- **DS_NM:** Name of the dataset. This should be unique name.
- **DS_DESC:** Description of dataset
- **ACTIVE_FL:** This flag indicates whether or not this dataset can be used during the QC batch. If set to "Y", system will run this rule during the QC batch. If set to "N", the system will ignore this rule when the QC batch is executed. Ideally, you should make sure that if the ACTIVE_FL on a rule is set to Yes, the ACTIVE_FL on the dataset associated with that rule should also be set to Yes.
- **LAST_UPDATED_DT:** Date when this record was last updated.
- **LAST_UPDATED_BY:** User name who last updated this record.
- **COMMENTS:** Enter the comments

3. Define the dataset values in KDD_QC_DATASET_VALUES table. This table is used to define the actual SQL logic for each dataset.

Column Name	Primary Key	Column Type	Nullable
DS_ID		NUMBER(10)	
DS_VALUE_TYPE		VARCHAR2(1000 CHAR)	Y
DS_VALUE		CLOB	

- **DS_ID:** Unique identifier of the dataset that is associated with the rule. The dataset contains the sampling logic (SQL query) for the rule. This field references the DS_ID column in KDD_QC_RULE_MASTER and KDD_QC_DATASET_MASTER tables.
- **DS_VALUE_TYPE:** Define the type of dataset value
- **DS_VALUE:** Define the value of the dataset.
  - If DS_VALUE_TYPE = USEDTABLES, then this should be the PDM name of the table that will be used in the rule.
  - If DS_VALUE_TYPE = "ANSIJOIN", then this should be the JOIN relationship.
  - If DS_VALUE_TYPE = "WHERECLAUSE", then this should be the WHERE condition.

- If DS_VALUE_TYPE = "ORDERBY"

4. The entries will be updated in the KDD_QC_RULE_XCUTN_AUDIT table.

Column Name	Primary Key	Column Type	Nullable
RULE_ID		NUMBER(10)	Y
RULE_QUERY		CLOB	Y
EXECUTION_DT		DATE	Y
EXECUTION_BY		VARCHAR2(20 CHAR)	Y
BATCH_ID		VARCHAR2(1000 CHAR)	Y

- `RULE_ID:` Enter the Rule ID
- `RULE_QUERY:` Define the SQL query for the rule
- `EXECUTION_DT:` Date of batch execution
- `EXECUTION_BY:` User name who executed the batch
- `BATCH_ID:` ID of batch

A seeded batch CASE_QC_WORKFLOW_UPDATE is used to trigger the QC process. This batch can be scheduled through the Batch Scheduler like all other batches. When this batch runs, ECM compares every case in the database with every QC sampling rule defined in the system to identify candidate cases for QC. Candidate cases form the superset of cases from which a random set of cases will be selected for QC. Each sampling rule will gather its own superset of candidate cases.

Based on the logic defined for each sampling rule, the system randomly will select a percentage (or number) of cases from the superset to QC.

When the Quality Controlled cases are identified, the system will use Case Allocation rules to determine the case owner and assignee.

Note: Currently, the ECM system assigns the same user as the case owner and the assignee.

Here, the system also uses the action code defined on the sampling rule to call PMF and assign a resulting (QC) status to the case. These workflows need to be defined in PMF. For more information on PMF, see the Configuring Processing Modelling Framework (PMF) chapter. In out of the box workflows, the QC process is not configured. Also, clients can create new roles for the QC process, if required. Out of the box doesn't include any specific QC roles.

Audit History tab is also updated with Owner name, Assignee name, and Action (on the sampling rule) that moved the case into the QC process.

Event Purge

Sometimes, events are ingested multiple times or generated by poor data quality during the processing. In these instances, you can clear the ingested data for better correlations and investigations. This is applicable to both cases and pre-cases. When event purge is performed for the case, the linked events and entities will be deleted. If an entity is linked to both valid and purged events, then the entity will not be removed.

There are two types of purge:

- Individual Event Purge: Individual events that are identified with bad data. Provide `n_event_skey` generated in the consolidation layer and relevant comments to purge the event.
- Batch Purge: Enter the purge type as "BATCH" in `v_purge_type` column and run skey in `n_run_skey` column of `FCC_PURGE_INPUT` table if you want to purge a complete batch. When a batch is purged, the events linked to that batch will be purged.

Below is the list of features:

- Supports purging individual and batch events.
- Removing purged events and related entities from the case
- Capturing the audit log of the purged events related to the case.
- Purging case(in 'New' status) if all the events in the case are purged.

Note:

- Events Purged before promoting to case: If the event is part of an un-promoted correlation, then drop the event and associated entities from the correlation. The events which are purged will not take part in future correlation process. If the events in correlation after purging are disconnected, then re-run correlation for these events.
- Events Purged after promoting to Case: If any event is part of case, then drop the event and associated business entities from the case. If the associated business entities (for example, customer) of the purged event(s) are associated with other events in the case, then those will remain in the business tab. By default, only events which are part of the case in status 'New' can be purged. The events which are purged will not take part in the future correlation process.

Event Purging using Tables

Perform the following steps to purge events using table updates:

1. Configure the parameters in table `FCC_PURGE_INPUT`.

Note:

In this table, data with event skey column can be added. For this, follow the below steps:

1. Locate `EventPurge.cfg` (path: `<installed area>/ficdb/conf`)
2. Look at the existing table `FCC_EVENTS`. In table `FCC_PURGE_INPUT`, event skey should be the same as mentioned in table `FCC_EVENTS`.

Column Name	Primary Key	Column Type	Nullable
n_err_seq_id		NUMBER	
n_event_skey	Y	NUMBER(22)	No
n_run_skey		NUMBER(22)	No
v_user_comments		VARCHAR2(4000 CHAR)	
f_purge_success_flag		CHAR(1 CHAR)	
d_requested_date		DATE	
d_fic_mis_date		DATE	
v_user_id		VARCHAR2(50 CHAR)	

Column Name	Primary Key	Column Type	Nullable
v_data_origin		VARCHAR2(30 CHAR)	
d_prcsng_batch_date		DATE	
v_purge_type		VARCHAR2(20 CHAR)	

- n_err_seq_id: Enter the sequence ID. This field accepts only numeric values.
- n_event_skey: Enter the skey of the event which you want to purge. This is a mandatory field.
- n_run_skey: Enter the run skey of the batch if you want to purge a complete batch.
- v_user_comments: User comments if required
- f_purge_success_flag: Defines the purge success flag. If the purge is failed, then this flag will be displayed as E. By default, it has to be set to Null or N. This flag turns to Y if purge is successful. If purge fails (flag = E), then check and correct it, and update this entry as Null or N and again execute the purge.
- d_requested_date: Date of individual event purge request
- d_fic_mis_date: Date of BATCH. This is applicable only if n_run_skey is defined.
- v_user_id: User ID who is performing the purge.
- v_data_origin: Define the data region, like US, IND and so on. This is applicable only for the batch purge. For example, a batch can have data for multiple data origins and if you want delete data only for India region, then define the region in this field.
- d_prcsng_batch_date: Date on which the purge process request is completed.
- v_purge_type: Define the type of purge. It can be a BATCH or EVENT.

3. Execute the following script:
   EventPurge.sh

Event Expiry

ECM Engine accepts the events generated from various transaction monitoring applications (CS, KYC, and so on) and process these for correlation. After scoring each event, the engine will promote these correlations which have score more than a threshold score. But, some events in the back end are not used because associated attributes of these events didn't yield enough score. So these events/correlations are not promoted to a case. A few events scores may also drop to '0' or below by increase in age. ECM engine identifies such events and removes them from the correlation process.

Engine will not only remove these events but also remove the evented data related to events. Following are the conditions by which events are identified for expiry:

- Events with age greater than the specified time period. For more information, see the Identifying Events by Age section.
- Events score <= 0. For more information, see the Identifying Events by Score section.

Identifying Events by Age

The ageing rules are defined in IPE to identify the events by age for expiry. This IPE rule is configurable by

- Age
- Event Type
- Jurisdiction
- Domain

This rule runs post correlation batch and identifies the events that needs to be archived, which is move to expiry events table.

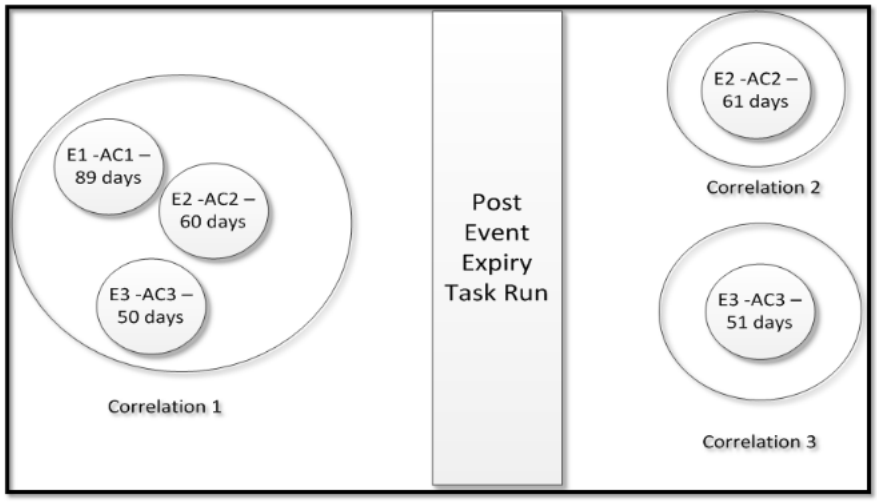
Identifying Events by Score

Events which need to be expired can be identified through event score.

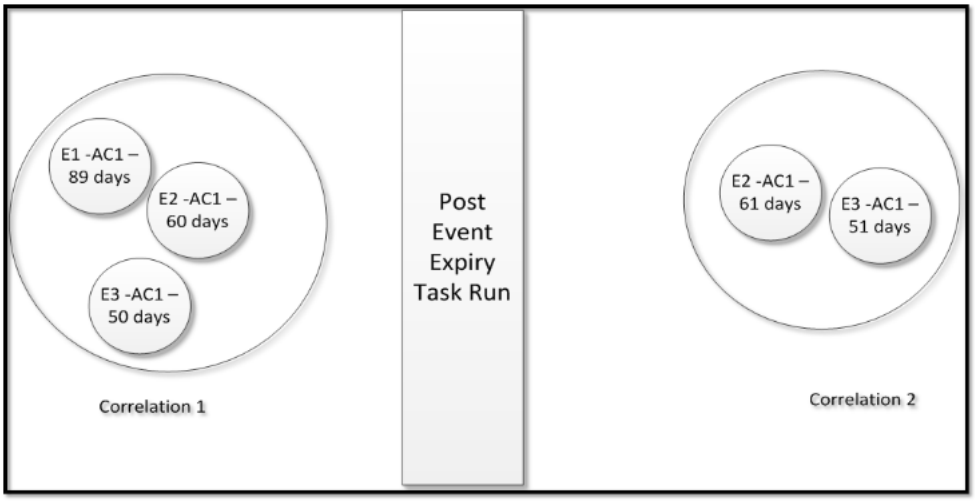
Examples

Following is the list of examples:

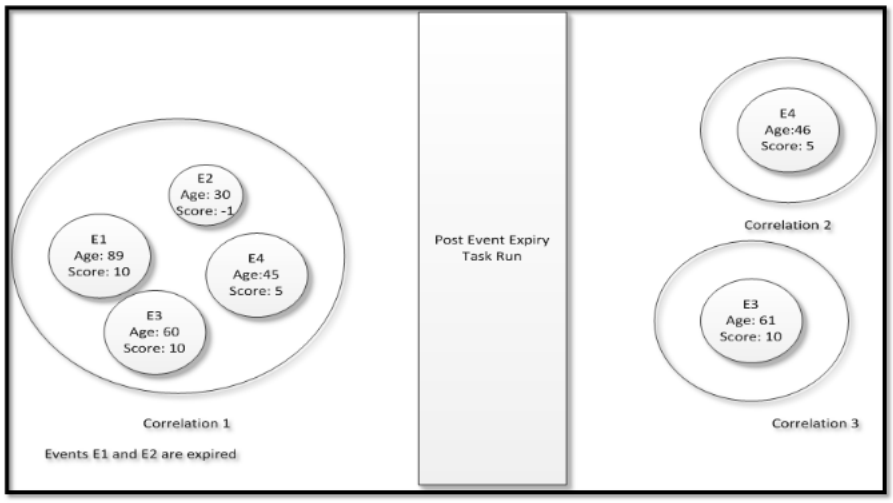
1. In the below example, Event E1, E2, and E3 are correlated in Correlation 1. When the task for Event expiry is executed, Event E1 will be out of the case correlation based on defined IPE rule. Event E2 and Event E3 will be correlated to Correlation 2 and Correlation 3 respectively.



2. In the below example, Event E1, E2, and E3 are correlated in Correlation 1. When the task for Event expiry is executed, Event E2 will not be promoted to case based on defined IPE rule. Event E1 and Event E3 will be correlated together in Correlation 2.



3. In the below example, Event E1, E2, E3, and E4 are correlated in Correlation 1. When the task for Event expiry is executed, Event E1 and Event E2 will not be promoted to case based on defined scoring. Event E3 and Event E4 will be correlated to Correlation 2 and Correlation 3 respectively.

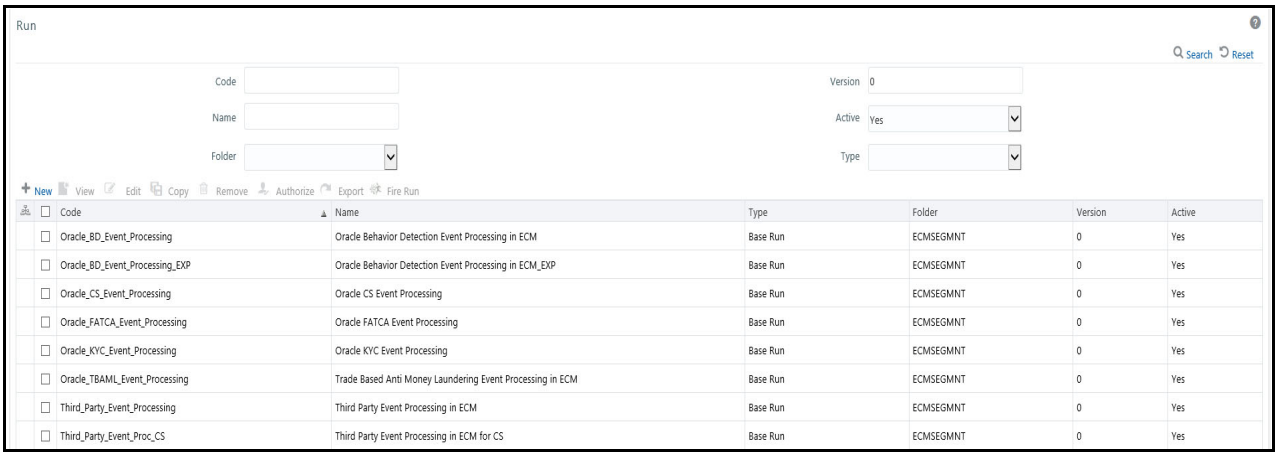


Configuring Event Expiry

This section explains how to configure the event expiry.

To configure the event expiry, follow these steps:

1. Create an IPE rule for event expiry. For more information, see the *IPE User Guide* on OHC.
2. Navigate to Enterprise Case Management Application.
3. Go to the Common task section. Select the **Run Rule Framework**.
4. Click **Run**. The Run Summary window is displayed with the available Processes.



5. Go to the List section. Select **Oracle_BD_Event_Processing**. The list of processes for OBD is displayed. Select the **BD_Scoring** code and **Job** option from **Selector**.

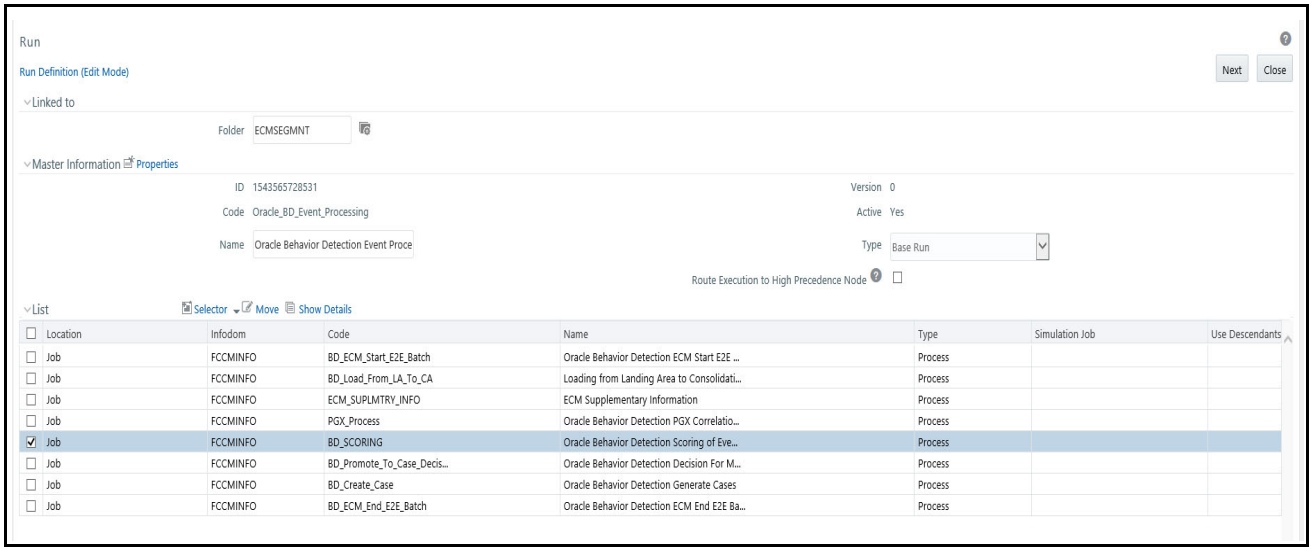
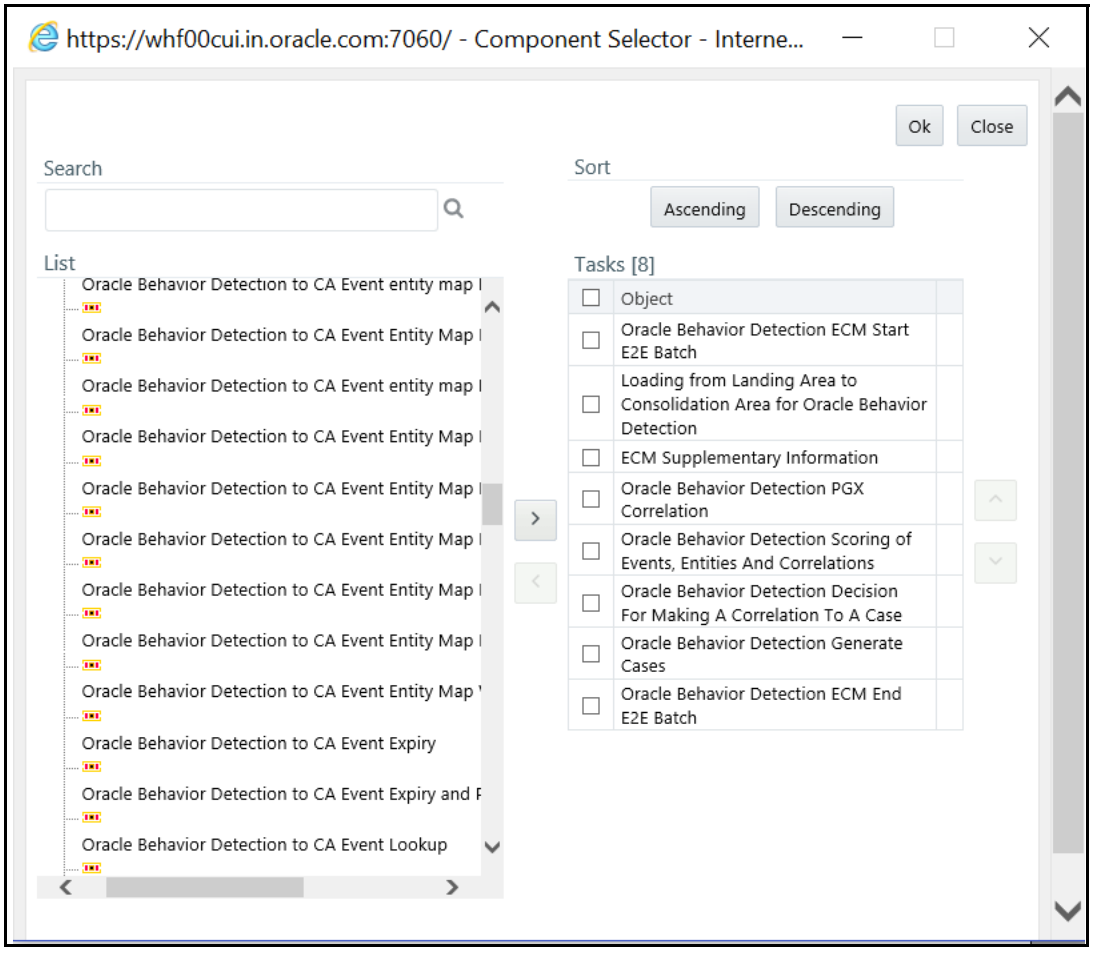


Figure 67. Run Summary Window

6. The **Component Selector** window is displayed. Select **Oracle Behavior Detection to CA Event Expiry and Prege** process from the list and move it to **Task** list.

   This process has following two sub-processes:

   - Oracle Behavior Detection to CA Event Expiry
   - Oracle Behavior Detection to CA Orphaned Event Purge



7. Select the precedence of **Oracle Behavior Detection to CA Event Expiry and Prege** process after the **Oracle Behavior Detection Scoring of Events, Entities And Correlations**. Click **Ok**.

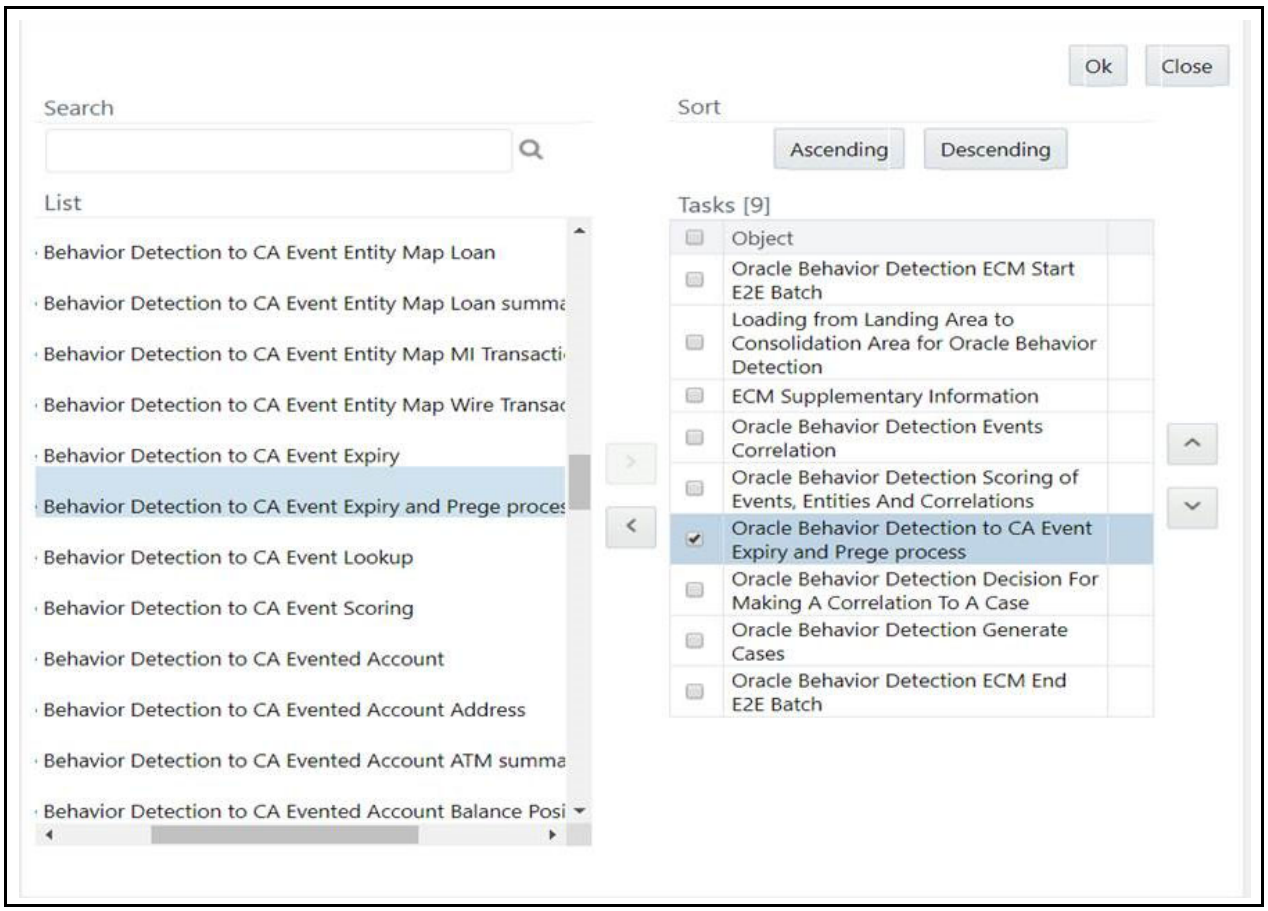


Figure 68. Components

8. Modify the configuration table FCC_EVENT_EXPIRY_CONF.

Column Name	Primary Key	Column Type	Nullable
N_CONF_ID	Y	NUMBER	
N_GROUP_ID		NUMBER	
F_IS_ASSMNT_ENABLED		VARCHAR2	
N_ASSESSMENT_ID		NUMBER	
F_IS_EVENT_SCORE_ENABLED		VARCHAR2	
N_SCORE_THRESHOLD		NUMBER	

- **N_CONF_ID:** This is the sequence ID of the event. This should be a numeric value. For example, 1 and so on.
- **N_GROUP_ID:** Provide the ECM Processing Group ID

- **F_IS_ASSMNT_ENABLED:** Set this flag to Y if you want to enable the event assessment. If this value is set to Y, then provide the assessment ID in the **N_ASSESSMENT_ID** field.
- **N_ASSESSMENT_ID:** Provide the assessment ID if **F_IS_ASSMNT_ENABLED** field is set to Y. This assessment ID should be valid IPE rule number.
- **F_IS_EVENT_SCORE_ENABLED:** Set this flag to Y if you want to enable the event score. Enable this flag before defining the threshold score in the **N_SCORE_THRESHOLD** field.
- **N_SCORE_THRESHOLD:** Define the threshold score value.

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

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 the 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 a 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**).

Correlation

Correlation is used to perform correlation on loaded BD events. This has following two tasks:

- PGX_CORRELATION
- BD_CORRELATION

Scoring

BD_SCORING is used to perform the 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 an OBD correlation can be promoted to a case. This is based on the defined threshold limit. This has following task. The task type of this is the Computation Rule.

- Pre Case Promotion Rule

Create Case

BD_Create_Case process is used for case creation if an OBD event is promoted to case.

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table 43*)
- CASE_COMPLETION_FLAG

Here, Level 1, Level 2, Level 2, Level 2, Level 3, Level 4, Level 5, Level 6, and Level 7 should run in sequence. Sub-processes within any level (for example, level3) can be executed in any order in parallel (depending upon the hardware specification) or sequentially.

Table 41. Level Details

Level	Process Name
Level 1	Oracle Behavior Detection to CA Event Lookup
Level 2	Oracle Behavior Detection to CA Event
Level 2	Oracle Behavior Detection to CA Event Binding
Level 2	Oracle Behavior Detection to CA Event Details
Level 3	CA Lookup
Level 4	CA Event Entity Map
Level 5	CA Business
Level 6	Additional Information
Level 7	CA Evented

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_LOOKUP BD_ACCOUNT_LOOKUP BD_CUSTOMER_LOOKUP BD_DERIVED_ADDRESS_LOOKUP BD_EMPLOYEE_LOOKUP BD_EVENT_LOOKUP BD_EXTERNAL_ENTITY_LOOKUP BD_INSTITUTION_LOOKUP BD_INVESTMENT_ADVISOR_LOOKUP BD_LOAN_LOOKUP BD_MARKET_CENTER_LOOKUP BD_PEER_GROUP_LOOKUP	BD_EVENT_ENTITY_MAP_AC BD_EVENT_ENTITY_MAP_AG BD_EVENT_ENTITY_MAP_BOT BD_EVENT_ENTITY_MAP_CT BD_EVENT_ENTITY_MAP_CUST BD_EVENT_ENTITY_MAP_DA BD_EVENT_ENTITY_MAP_EE BD_EVENT_ENTITY_MAP_EMPL BD_EVENT_ENTITY_MAP_IA BD_EVENT_ENTITY_MAP_IM BD_EVENT_ENTITY_MAP_MIT BD_EVENT_ENTITY_MAP_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_EVNT 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_EVNT BD_CASH_TRXN_EVNT BD_CB_PR_TXN_SM_MNT_EVNT 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_EVNT BD_INSTL_ACCT_SMRY_MNTH_EVNT BD_INSTN_MASTER_EVNT BD_INSURANCE_POLICY_EVNT BD_INSURANCE_PRODUCT_EVNT 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 the business data population (see the Business Metadata Movement).	

Table 42. Sub-processes

CA Area	Process Name	Process Parameter
CA Event	Oracle Behavior Detection to CA Event	BD_EVENT
CA Event	Oracle Behavior Detection to CA Event Binding	BD_EVENT_BINDING
CA Event	Oracle Behavior Detection to CA Event Details	BD_EVENT_DETAILS
CA Area	**Process Name**	**Data Movement Code**
CA Lookup	Oracle Behavior Detection to CA Account ATM Daily Lookup	BD_ACCOUNTATMDAILY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account ATM Daily Lookup	BD_CustomerBalance_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Balance Summary Lookup	BD_ACCT_SMRY_MNTH_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Client Bank Lookup	BD_ACCT_CLIENTBANK_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Daily Lookup	BD_ACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Group Lookup	BD_ACCOUNT_GROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Lookup	BD_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account PeerGroup Lookup	BD_ACCOUNT_PEERGROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Trade Daily Lookup	BD_ACCOUNTTRADEDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Transaction Daily Lookup	BD_ACCOUNTTRXNDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Anticipatory Profile Lookup	BD_ANTICIPATORYPRFL_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Back Office Transaction Lookup	BD_BACK_OFFICE_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Cash Transaction Lookup	BD_CASH_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank Peer Transaction Summary Lookup	BD_CBPEERTRXNSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank PeerGroup Lookup	BD_CLIENTBANK_PEERGRP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank Summary Lookup	BD_CLINETBANKBSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA ClientBank Transaction Summary Lookup	BD_ACCT_PR_TRXN_SMR_MN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Account Lookup	BD_CUSTOMER_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Customer Lookup	BD_CUSTOMER_CUSTOMER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Daily Lookup	BD_CUSTOMERDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer MarketServed Lookup	BD_CUSTOMER_MRKTSRV_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Product Lookup	BD_CUSTOMER_PRODUCT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Summary Lookup	BD_CUSTOMERSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customers Lookup	BD_CUSTOMER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Derived Address Lookup	BD_DERIVED_ADDRESS_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Employee Account Lookup	BD_EMPLOYEE_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Employee Lookup	BD_EMPLOYEE_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Event Lookup	BD_EVENT_LOOKUP

Table 42. Sub-processes

CA Lookup	Oracle Behavior Detection to CA External Entity Daily Lookup	BD_EXTERNALENTITYDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA External Entity Lookup	BD_EXTERNAL_ENTITY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA House Hold Summary Lookup	BD_HOUSEHOLDSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Household Balance Lookup	BD_HOUSEHOLDBALDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Account Daily Lookup	BD_INSTLACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Account Summary Lookup	BD_INSTACCOUNTSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Lookup	BD_INSTITUTION_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Insurance Policy Balance Lookup	BD_INSURANCEPOLICYBAL_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Insurance Policy Daily Lookup	BD_INSURANCEPOLICYDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA InsurancePolicy Customer Lookup	BD_INSURPOLICY_CUST_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Lookup	BD_INVESTMENT_ADVISOR_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Lookup	BD_INVESTMENTADVISORLOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Summary Lookup	BD_INVESTMENTSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA LinkAnalysis Lookup	BD_LINKANALYSIS_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Loan Lookup	BD_LOAN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Loan Summary Lookup	BD_LOANSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA MI Transaction Lookup	BD_MI_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Managed Account Daily Lookup	BD_MANAGEDACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Managed Account Lookup	BD_MANAGEDACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Market Center Lookup	BD_MARKET_CENTER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA NetworkLogon Lookup	BD_NETWORKLOGON_LOOKUP
CA Lookup	Oracle Behavior Detection to CA NetworkUser Account Lookup	BD_NTWKUSER_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Online Account Lookup	BD_ONLINEACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA OnlineAccount Account Lookup	BD_ONLINEACCT_ACCT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Peer Group Lookup	BD_PEER_GROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Trade Lookup	BD_TRADE_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Wire Transaction Lookup	BD_WIRE_TRXN_LOOKUP
CA Area	**Process Name**	**Process Parameter**
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account	BD_EVENT_ENTITY_MAP_AC
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Balance Position Summary	BD_EVENT_ENTITY_MAP_ABPS
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Group	BD_EVENT_ENTITY_MAP_AG
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Summary Month	BD_EVENT_ENTITY_MAP_ASM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Back Office Transaction	BD_EVENT_ENTITY_MAP_BOT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Cash Transaction	BD_EVENT_ENTITY_MAP_CT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Client Bank Summary Month	BD_EVENT_ENTITY_MAP_CBSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Customer	BD_EVENT_ENTITY_MAP_CUST
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Customer Summary Month	BD_EVENT_ENTITY_MAP_CSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Derived Address	BD_EVENT_ENTITY_MAP_DA
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Employee	BD_EVENT_ENTITY_MAP_EMPL
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map External Entity	BD_EVENT_ENTITY_MAP_EE

Table 42. Sub-processes

CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Institution Master	BD_EVENT_ENTITY_MAP_IM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Investment Advisor	BD_EVENT_ENTITY_MAP_IA
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Loan	BD_EVENT_ENTITY_MAP_LOAN
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Loan summary month	BD_EVENT_ENTITY_MAP_LSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map MI Transaction	BD_EVENT_ENTITY_MAP_MIT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Trade	BD_EVENT_ENTITY_MAP_TRADE
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Wire Transaction	BD_EVENT_ENTITY_MAP_WT
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Account ATM summary daily	BD_EVENT_ENTITY_MAP_AASD
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Anticipatory Profile	BD_EVENT_ENTITY_MAP_NP
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Employee Account	BD_EVENT_ENTITY_MAP_EA
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Household Balance position summary	BD_EVENT_ENTITY_MAP_HBPS
CA Event Entity Map	Oracle Behavior Detection to CA Event Scoring	BD_EVENT_SCORE
CA Area	**Process Name**	**Process Parameter**
CA Business	Oracle Behavior Detection to CA Account	BD_ACCT
CA Business	Oracle Behavior Detection to CA Account ATM summary Daily	BD_ACCT_ATM_SMRY_DAILY
CA Business	Oracle Behavior Detection to CA Account Address	BD_ACCT_ADDR
CA Business	Oracle Behavior Detection to CA Account Balance Position Summary	BD_ACCT_BAL_POSN_SMRY
CA Business	Oracle Behavior Detection to CA Account Email Address	BD_ACCT_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Account Group	BD_ACCT_GRP
CA Business	Oracle Behavior Detection to CA Account Institution mapping	BD_ACCT_ID_INSTN_ID_MAP
CA Business	Oracle Behavior Detection to CA Account List Membership	BD_ACCT_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Account Peer Group	BD_ACCT_PEER_GRP
CA Business	Oracle Behavior Detection to CA Account Peer Transaction Summary Month	BD_ACCT_PEER_TRXN_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Account Phone	BD_ACCT_PHON
CA Business	Oracle Behavior Detection to CA Account Restriction	BD_ACCT_RSTRN
CA Business	Oracle Behavior Detection to CA Account Summary Month	BD_ACCT_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Account Supplemental Attribute	BD_ACCT_SUPPLEMENTAL_ATR
CA Business	Oracle Behavior Detection to CA Anticipatory Profile	BD_NTCPTRY_PRFL
CA Business	Oracle Behavior Detection to CA Back Office Transaction	BD_BACK_OFFICE_TRXN
CA Business	Oracle Behavior Detection to CA Cash Transaction	BD_CASH_TRXN
CA Business	Oracle Behavior Detection to CA Client Bank	BD_CLIENT_BANK
CA Business	Oracle Behavior Detection to CA Client Bank List Membership	BD_CB_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Client Bank Peer Group	BD_CLIENT_BANK_PEER_GRP
CA Business	Oracle Behavior Detection to CA Client Bank Peer Transaction Summary Month	BD_CB_PR_TRXN_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Client Bank Summary Month	BD_CLIENT_BANK_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Customer Account Role	BD_CUST_ACCT_ROLE
CA Business	Oracle Behavior Detection to CA Customer to Customer	BD_CUST_CUST
CA Business	Oracle Behavior Detection to CA Customers	BD_CUST
CA Business	Oracle Behavior Detection to CA Customers Account	BD_CUST_ACCT
CA Business	Oracle Behavior Detection to CA Customers Address	BD_CUST_ADDR

Table 42. Sub-processes

CA Business	Oracle Behavior Detection to CA Customers Email Address	BD_CUST_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Customers IMP License	BD_CUST_IMP_LICENSE
CA Business	Oracle Behavior Detection to CA Customers IMP License Good	BD_CUST_IMP_LICENSE_GOOD
CA Business	Oracle Behavior Detection to CA Customers List Membership	BD_CUST_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Customers Phone	BD_CUST_PHON
CA Business	Oracle Behavior Detection to CA Customers Summary Months	BD_CUST_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Customers Supplemental Attribute	BD_CUST_SUPPLEMENTAL_ATR
CA Business	Oracle Behavior Detection to CA Derived Address	BD_DERIVED_ADDRESS
CA Business	Oracle Behavior Detection to CA Employee	BD_EMP
CA Business	Oracle Behavior Detection to CA Employee Address	BD_EMP_ADDR
CA Business	Oracle Behavior Detection to CA Employee Email Address	BD_EMP_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Employee Phone	BD_EMP_PHON
CA Business	Oracle Behavior Detection to CA Employee to Account	BD_EMP_ACCT
CA Business	Oracle Behavior Detection to CA External Entity	BD_EXTERNAL_ENTITY
CA Business	Oracle Behavior Detection to CA External Entity Address	BD_EXTERNAL_ENTITY_ADDR
CA Business	Oracle Behavior Detection to CA External Entity Link	BD_FCC_EXTERNAL_ENTITY_LINK
CA Business	Oracle Behavior Detection to CA External Entity Membership	BD_EXTRNAL_NTTY_MMBRSHP
CA Business	Oracle Behavior Detection to CA House Hold Summary Month	BD_EVENT_ENTITY_MAP_HSM
CA Business	Oracle Behavior Detection to CA HouseHold Balance Position Summary	BD_HH_BAL_POSN_SMRY
CA Business	Oracle Behavior Detection to CA Household summary Month	BD_HH_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Institution Master	BD_INSTN_MASTER
CA Business	Oracle Behavior Detection to CA Institutional Account Summary Month	BD_INSTL_ACCT_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Insurance Policy	BD_INSURANCE_POLICY
CA Business	Oracle Behavior Detection to CA Insurance Policy Customer	BD_INSURANCE_POLICY_CUST
CA Business	Oracle Behavior Detection to CA Insurance Product	BD_INSURANCE_PRODUCT
CA Business	Oracle Behavior Detection to CA Investment Manager	BD_NVSMT_MGR
CA Business	Oracle Behavior Detection to CA Investment Manager Summary Month	BD_NVSMT_MGR_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA LinkAnalysis Link	BD_LINKANALYSIS_LINK
CA Business	Oracle Behavior Detection to CA LinkAnalysis LinkSummary	BD_LINKANALYSIS_LINKSUMMARY
CA Business	Oracle Behavior Detection to CA LinkAnalysis Network	BD_LINKANALYSIS_NETWORK
CA Business	Oracle Behavior Detection to CA LinkAnalysis Node	BD_LINKANALYSIS_NODE
CA Business	Oracle Behavior Detection to CA LinkAnalysis TypeSummary	BD_LINKANALYSIS_TYPESUMMARY
CA Business	Oracle Behavior Detection to CA Loan	BD_LOAN
CA Business	Oracle Behavior Detection to CA Loan Summary Month	BD_LOAN_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA MI Transaction	BD_MI_TRXN
CA Business	Oracle Behavior Detection to CA Managed Account	BD_MANGD_ACCT
CA Business	Oracle Behavior Detection to CA Online Account	BD_ONLINE_ACCT
CA Business	Oracle Behavior Detection to CA Online Account	BD_ONLINE_ACCT_ACCT
CA Business	Oracle Behavior Detection to CA Peer Group	BD_PEER_GRP
CA Business	Oracle Behavior Detection to CA Trade	BD_TRADE

Table 42. Sub-processes

CA Business	Oracle Behavior Detection to CA TransactionPartyCrossReference BOT	BD_TRXN_PARTY_XREF_BOT
CA Business	Oracle Behavior Detection to CA TransactionPartyCrossReference FOT	BD_TRXN_PARTY_XREF_FOT
CA Business	Oracle Behavior Detection to CA Wire Transaction	BD_WIRE_TRXN
CA Area	**Process Name**	**Data Movement Code**
Additional Information	BD_ENTITY_SUP_INFO This sub-process code has to be executed after business data population (see the Business Metadata Movement)	BD_ENTITY_SUP_INFO
CA Area	**Process Name**	**Data Movement Code**
CA Evented	Oracle Behavior Detection to CA Evented Account	BD_ACCT_EVENT
CA Evented	Oracle Behavior Detection to CA Evented Account ATM summary Daily	BD_ACCT_ATM_SMRY_DAILY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Address	BD_ACCT_ACCT_ADDR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Balance Position Summary	BD_ACCT_BAL_POSN_SMRY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Group	BD_ACCT_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Peer Group	BD_ACCT_PEER_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Peer Transaction Summary Month	BD_ACCT_PR_TXN_SMRY_MN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Restriction	BD_ACCT_RSTRN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Summary Month	BD_ACCT_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Supplemental Attribute	BD_ACCT_SUPPLEMENTAL_ATR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Anticipatory Profile	BD_NTCPTRY_PRFL_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Back Office Transaction	BD_BACK_OFFICE_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Cash Transaction	BD_CASH_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank	BD_CLIENT_BANK_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Peer Group	BD_CLINT_BNK_PR_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Peer Transaction Summary Month	BD_CB_PR_TXN_SM_MNT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Summary Month	BD_CLNT_BNK_SM_MNT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customer Balance Position Summary	BD_CUST_BAL_POSN_SMRY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers	BD_CUST_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers IMP License	BD_CUST_IMP_LICENSE_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers IMP License Good	BD_CUST_IMP_LIC_GOD_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers Summary Months	BD_CUST_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers Supplemental Attribute	BD_CUST_SUPPL_ATR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Derived Address	BD_DERIVED_ADDRESS_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee	BD_EMP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee Address	BD_EMP_ADDR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee Email Address	BD_EMP_EMAIL_ADDR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee Phone	BD_EMP_PHON_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee to Account	BD_EMP_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Entity	BD_EXTERNAL_ENTITY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Entity Address	BD_XTRNL_ENTY_ADR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Org	BD_EXTRL_ORG_EVNT
CA Evented	Oracle Behavior Detection to CA Evented HouseHold Balance Position Summary	BD_HH_BAL_POSN_SMRY_EVNT

Table 42. Sub-processes

CA Evented	Oracle Behavior Detection to CA Evented Household summary Month	BD_HH_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Institution Master	BD_INSTN_MASTER_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Policy	BD_INSURANCE_POLICY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Policy Customer	BD_INS_PLCY_CUST_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Product	BD_INSURANCE_PRODUCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Investment Manager	BD_NVSMT_MGR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Investment Manager Summary Month	BD_NVSMT_MGR_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Loan	BD_LOAN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Loan Summary Month	BD_LOAN_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented MI Transaction	BD_MI_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Managed Account	BD_MANGD_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Online Account	BD_ONLINE_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Peer Group	BD_PEER_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Trade	BD_TRADE_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Wire Transaction	BD_WIRE_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Institutional Account Summary Month	BD_INSTL_ACCT_SMRY_MNTH_EVNT

Following processes are related to network building block:

- BD_LINKANALYSIS_LOOKUP (Oracle Behavior Detection to CA LinkAnalysis Lookup)
- BD_LINKANALYSIS_NETWORK (Oracle Behavior Detection to CA LinkAnalysis Network)
- BD_LINKANALYSIS_NODE (Oracle Behavior Detection to CA LinkAnalysis Node)
- BD_LINKANALYSIS_LINK (Oracle Behavior Detection to CA LinkAnalysis Link)
- BD_LINKANALYSIS_LINKSUMMARY (Oracle Behavior Detection to CA LinkAnalysis LinkSummary)
- BD_LINKANALYSIS_TYPESUMMARY (Oracle Behavior Detection to CA LinkAnalysis TypeSummary)

Table 43. 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_ACCOUNTS (Level 1) process has to be executed before the 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 the 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 the 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 the 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 the execution of KDD_CASE_LOAN_SMRY_MNTH.
- KDD_CASE_NVSMT_MGR (Level 1) process has to be executed before the 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

The following processes 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 the 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 the scoring of OCS events. This has the following sub-process:

- Pre-Case-Scoring For Oracle CS

Promote to Case

Promote_To_Case_Decision_OCS is used to make the decision if an OCS correlation can be promoted to a case. This is based on the defined threshold limit. This has the following sub-process:

- Pre Case Promotion Rule

Create Case

Create_Case is used to create a case if an OCS event is promoted to the case.
Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table*)
- CASE_COMPLETION_FLAG

End Batch

ECM_End_E2E_Batch_For_CS is used for ending the batch execution for CS.

OFATCA Application Process

The following process are used for this:

- Start Batch
- Load Data from FATCA to ECM
- Data Movement DIM_FATCA_STATUS To DIM_FATCA_STS
- Correlation
- Scoring
- Promote to Case
- Create Case
- Update FATCA Status to Case
- Insert Customer REP information
- Case FATCA Status Attribute
- Case Focal Customer ID Attribute
- Case Account ID related Attribute
- End Batch

Start Batch

ECM Start E2E Batch for FATCA process is used to start the batch execution to move the data from OFATCA to ECM.

Load Data from FATCA to ECM

Load_From_OFATCA_To_CA process loads OFATCA data from the Landing area to Consolidation area. This has following four sub-processes:

- Loading Oracle FATCA Events: loads the FATCA events to the Consolidation area
- Entity Surrogate Key Generation For Oracle FATCA: This should be executed after **Loading Oracle FATCA Events** sub-process.
- Evented Data Load for FATCA
- Business Data Load for FATCA

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
FATCA_FCC_EVENT_LOOKUP	FATCA_FCC_EVENTS	FATCA_FCC_CUSTOMER_LOOKUP	FATCA_FCC_EVENT_ENTITY_MAP_ACC	BD_ACCT	FATCA_FCC_CUST_EVNT

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
	FATCA_FCC_EVENT_DETAILS	FATCA_FCC_ACCOUNT_LOOKUP	FATCA_FCC_EVENT_ENTITY_MAP_CUS	BD_ACCT_ADDR	FATCA_FCC_ACCT_EVNT
	FATCA_FCC_FATCA_EVENT_DTLS	FATCA_CUSTOMER_ACCOUNT_LOOKUP	FATCA_FCC_EVENT_ENTITY_MAP_RULE	BD_ACCT_EMAIL_ADDR	FATCA_FCC_CUST_ACCT_EVNT
	FATCA_FCC_EVENT_BINDING	FATCA_CUSTOMER_CUSTOMER_LOOKUP	FATCA_FCC_EVENT_ENTITY_MAP_AC	BD_ACCT_PHON	FATCA_FCC_CUST_CUST_EVNT
				BD_ACCT_SMRY_MNTH	FATCA_FCC_FATCA_RULE_EVNT
				BD_CUST	
				BD_CUST_ACCT	
				BD_CUST_ADDR	
				BD_CUST_EMAIL_ADDR	
				BD_CUST_PHON	
				BD_CUST_SMRY_MNTH	
				BD_CUST_CUST	
				BD_CUST_ACCT_ROLE	
				FATCA_FCC_CUST_RPTNG_INFO	

Below is a list of DMs which are used for case search:

- CASE_FATCA_STS
- CASE_CUST
- CASE_ACCT

ECM Supplementary Information

BD_ENTITY_SUP_INFO process of ECM_SUPLMTRY_INFO is used to provide additional information on data.

Data Movement DIM_FATCA_STATUS To DIM_FATCA_STS

This process is used to move the FATCA data from DIM_FATCA_STATUS to the DIM_FATCA_STS table.

Below DM is used for DIM_FATCA_STATUS data movement to ECM:

DIM_FATCA_MOVEMENT

Correlation

This is used to perform a correlation on loaded FATCA events.

- DT_CORRELATION

Scoring

Scoring_OFATCA is used to perform the scoring of OFATCA events. This has following sub-process:

- Pre-Case Scoring For Oracle FATCA

Promote to Case

Promote_To_Case_Decision_OFATCA is used to make the decision if a OFATCA correlation can be promoted to a case. This is based on defined threshold limit. This has following sub-process:

- POPULATE_P2C_FL_OFATCA

Create Case

Create_Case is used to create a case if an OFATCA event is promoted to the case.
Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- t2t_KDD_CASE_ACCOUNTS
- t2t_KDD_CASE_CUSTOMERS
- t2t_KDD_CASE_ACCT_EMAIL_ADDR
- t2t_KDD_CASE_CUST_ACCT
- t2t_KDD_CASE_ACCT_PHON
- t2t_KDD_CASE_ACCT_SMRY_MNTH
- t2t_KDD_CASE_CUST_ADDR
- t2t_KDD_CASE_CUST_EMAIL_ADDRS
- t2t_KDD_CASE_CUST_PHONE
- t2t_KDD_CASE_CUST_SMRY_MNTH
- CASE_COMPLETION_FLAG
- CASE_ASSIGNMENT

Update FATCA Status to Case

UPDT_FATCA_STATUS_TO_CASE is used for updating the status of FATCA to case.

Insert Customer REP information

The INST_FATCA_CUST_REP_TO_CASE process is used to insert FATCA customer information.

Case FATCA Status Attribute

The CASE_FATCA_STS process is used to update the FATCA attribute status.

Case Focal Customer ID Attribute

The CASE_CUST process is used to update the Focal Customer ID of the case.

Case Account ID related Attribute

The CASE_ACCT process is used to update the Account ID of the case.

End Batch

ECM_End_E2E_Batch_For_FATCA is used for ending the batch execution for FATCA.

OKYC Application Process

The 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

Note: After applying patch ECM patch 29519580, follow the below steps to add the task for movement of data to `fcc_party_party_rlshp`:

1. Login as ECM ADMIN.
2. Navigate to **Rule Run Framework** and select **Process**.
3. In the **Name** field, type **Oracle Behavior Detection to CA Customer List**.
4. Click **Edit**.
5. In the popup, click **Component**.

6. From the List, click **Process** and select **ECMSEGMENT.**
7. Move BD_PARTY_PARTY_RLSHP_LOOKUP and BD_PARTY_PARTY_RLSHP to the right **TASKS IN ROOTS** section.
8. Move the BD_PARTY_PARTY_RLSHP_LOOKUP task prior to BD_PARTY_PARTY_RLSHP in the **TASKS IN ROOTS** section.
9. Save the changes.

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 the 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 a correlation on loaded KYC events.

- DT_CORRELATION

Scoring

Scoring_OKYC is used to perform the 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 the defined threshold limit. This has the following sub-process:

- POPULATE_P2C_FL_OKYC

Create Case

Create_Case is used to create a case if an OKYC event is promoted to the case.
Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table*)
- 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.

OTBAML Application Process

The following process are used for this:

- Start Batch
- Load Data from TBAML to ECM
- Loading Data from TBAML to Consolidation Area
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

Start Batch

TBAML_ECM Start E2E Batch process is used to start the batch execution to move the data from OTBAML to ECM.

Load Data from TBAML to ECM

TBAML_Load_From_LA_To_CA process loads OTBAML data from Landing area to Consolidation area. This has following four sub-processes:

- Trade Based Anti Money Laundering Loading Events
- Trade Based Anti Money Laundering Entity Surrogate Key Generation
- Trade Based Anti Money Laundering Oracle Business Data Load
- Trade Based Anti Money Laundering Oracle Evented Data Load

Below is the list of TBAML sub-process codes.

Here, Level 0 sub-process code execution is a prerequisite for Level 1 sub-process execution. Similarly, Level 1 sub-process code execution is a prerequisite for Level 2 sub-process execution and so on. Sub-process within a level can be executed in any order or it can be executed in parallel. There are two types of processes: Scenario-based (TBAML_EVENT_LOOKUP) and Screening based (TBAML_FCC_EVENT_LOOKUP).

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
TBAML_EVENT_LOOKUP	TBAML_EVENT	TBAML_TRADE_FIN_CNTRCT_LOOKUP	TBAML_EVENT_ENTITY_MAP_CUST	TBAML_TRADE_FIN_SWIFT_MSG	TBAML_CUST_IMP_LICENSE_EVNT
	TBAML_EVENT_BINDING	TBAML_EXTRL_INSUR_PLCY_LOOKUP	TBAML_EVENT_ENTITY_MAP_TFP	TBAML_TRADE_FIN_PARTY	TBAML_CUST_IMP_LIC_GOD_EVNT
	TBAML_EVENT_DETAILS	TBAML_TRADE_DOCMNTRY_LOOKUP	TBAML_EVENT_ENTITY_MAP_TFGS	TBAML_TRADE_FIN_GOOD_SRVC	TBAML_TRADE_FIN_CNTRCT_EVNT
		TBAML_DOC_COLL_MULTIT_LOOKUP	TBAML_EVENT_ENTITY_MAP_TFCE	TBAML_EXTRL_INSURANCE_POLICY	TBAML_TRADE_FIN_BRKG_DSTR_EVNT
		TBAML_TRD_FIN_GOD_SRVC_LOOKUP	TBAML_EVENT_ENTITY_MAP_TFC	TBAML_CUST_IMP_LICENSE_GOOD	TBAML_EXTRL_INSU_POLICY_EVNT
		TBAML_DOC_COLL_CNTRCT_LOOKUP	TBAML_EVENT_ENTITY_MAP_DCCE	TBAML_CUST_IMP_LICENSE	TBAML_TRADE_FIN_PARTY_EVNT
		TBAML_TRADE_FIN_DOC_LOOKUP	TBAML_EVENT_ENTITY_MAP_DCCEE	TBAML_TRADE_FIN_CNTRCTEVENT	TBAML_TRADE_FIN_ACCT_EVNT
		TBAML_TRADE_FIN_PARTY_LOOKUP	TBAML_EVENT_ENTITY_MAP_DCSD	TBAML_TRADE_FIN_BRKRGE_DSTR	TBAML_TRADE_FIN_DRAFT_EVNT
		TBAML_CUSTMERIMPRTLIC_LOOKUP		TBAML_TRADE_FIN_ACCT	TBAML_TRADE_FIN_GOOD_SRVC_EVNT
		TBAML_TRD_FIN_BRKRGE_LOOKUP		TBAML_DOCMNTRY_COLL_CNTRCT	TBAML_TRD_FIN_CTRCTEVENT_EVNT
		TBAML_TRD_FIN_ACCT_LOOKUP		TBAML_TRADE_FIN_DOC	TBAML_DOC_COLL_CNTRCT_EVNT
		TBAML_TRD_FIN_SWIFT_MSG_LOOKUP		TBAML_TRADE_FIN_DRAFT	TBAML_TRADE_FIN_SWIFT_MSG_EVNT
		TBAML_CUSTOMER_LOOKUP		TBAML_TRADE_FIN_BRKRGE	TBAML_TRADE_FIN_DOC_EVNT
		TBAML_TRADE_FIN_DRAFT_LOOKUP		TBAML_TRADE_FIN_CNTRCT	TBAML_CUST_EVNT
		TBAML_DOC_COL_CNTRT_EVT_LOOKUP		TBAML_CUST	TBAML_DOC_COLL_SHPMT_DTL_EVNT
				TBAML_CUST_ACCT	TBAML_DOC_COLL_CNTRCTE_EVENT
				TBAML_CUST_ADDR	
				TBAML_CUST_EMAIL_ADDR	
				TBAML_CUST_PHON	

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
				TBAML_CUST_LIST_MEMBERSHIP	
				TBAML_DOCMNTRY_COLL_CNTRCTE	
				TBAML_DOCMNTRY_COLL_SHPMT_DTL	
TBAML_FCC_EVENT_LOOKUP	TBAML_FCC_EVENTS	TBAML_FCC_TBAML_WATCHLIST_LKUP	TBAML_FCC_TBAML_WATCHLIST	TBAML_BD_DERIVED_ADDRESS	TBAML_FCC_CUST_EVNT
	TBAML_FCC_TBAML_EVENTS_OUTCOME	TBAML_FCC_CNTRCT_MSG_LOOKUP	TBAML_FCC_EVENT_ENTITY_MAP_Wlt	TBAML_FSI_RT_RAW_DATA	TBAML_FCC_TBAML_EVENT_MATCHES
	TBAML_FCC_EVENT_DETAILS		TBAML_FCC_EVENT_ENTITY_MAP_Cst		TBAML_FCC_TBAML_WATCHLIST_EVNT
			TBAML_FCC_EVENT_ENTITY_MAP_tcm		TBAML_FCC_TBAML_CNTRCT_MSG_EVE
			TBAML_FCC_EVENT_ENTITY_MAP_tfc		TBAML_TRADE_FIN_CNTRCT_EVNT_SC

Loading Data from TBAML to Consolidation Area

Load_From_TBAML_To_CA process loads data from TBAML to Consolidation area. This has following three sub-processes:

- Loading TBAML Events
- Entity Surrogate Key Generation For TBAML
- Evented Data Load For TBAML

Correlation

This is used to perform a correlation on loaded TBAML events.

- DT_CORRELATION

Scoring

Scoring_OTBAML is used to perform the scoring of OTBAML events. This has the following sub-process:

- Oracle Behavior Detection Event Scoring
- Oracle Behavior Detection Entity Scoring

- Oracle Behavior Detection Correlation Scoring
- Oracle Behavior Detection Pre-Case Scoring

Promote to Case

TBAML_Promote_To_Case_Decision is used to make the decision if an OTBAML correlation can be promoted to a case. This is based on the defined threshold limit. This has the following sub-process:

- Pre Case Promotion Rule

Create Case

Create_Case is used to create a case if an OTBAML event is promoted to the case.

- Oracle Behavior Detection Generate Cases

Here, Level 0 is the prerequisite for Level 1 execution. Similarly, Level 1 is a prerequisite for Level 2, and so on. Sub-processes within any level can be executed in any order or it can be executed in parallel.

Table 44. Promote_To_Case T2Ts

Level 0	Level 1	Level 2
KDD_CASES	KDD_CASE_TRD_FIN_CNTRCT	KDD_CASE_CUST_ADDRS
	KDD_CASE_TRD_FIN_CNTRCT_EVT	KDD_CASE_CUST_ACCT
	KDD_CASE_TRD_FIN_GOOD_SRVC	KDD_CASE_CUST_EMAILS
	KDD_CASE_TRD_FIN_PARTY	KDD_CASE_CUST_PHONS
	KDD_CASE_CUSTOMERS	KDD_CASE_CUST_LIST_MEMBERSHIPS
	KDD_CASE_DERIVED_ADDRESS	
	KDD_CASE_TRD_FIN_DOC	
	KDD_CASE_DOC_COL_MULTNR_DTL	
	KDD_CASE_DOC_COL_CNTRCT	
	KDD_CASE_DOC_COL_CNTRCT_EVT	
	KDD_CASE_DOC_COL_SHPMT_DTL	

Below is the list of few tasks, which are common for BD and TBAML applications. You can configure a common task list.

t2t_KDD_CASE_CUSTOMERS

t2t_KDD_CASE_CUST_ADDR

t2t_KDD_CASE_CUST_ACCT

t2t_KDD_CASE_CUST_EMAIL_ADDRS

t2t_KDD_CASE_CUST_PHONE

t2t_KDD_CASE_CUST_LIST_MEMBERSHIP

t2t_KDD_CASE_DERIVED_ADDRESS

End Batch

TBAML_ECM_End_E2E_Batch is used for ending the batch execution for TBAML.

OSTDO Application Process

The following process are used for this:

- Start Batch
- Load Data from STDO to Consolidation Area
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

Start Batch

STDO_ECM_Start_E2E_Batch process is used to start the batch execution to move the data from OSTDO to ECM.

Load Data from STDO to Consolidation Area

STDO_Load_From_LA_To_CA process loads OSTDO data from the Landing area to Consolidation area. This has the following sub-processes:

- STDO_Event_Load
- STDO_Entity_Surrogate_Key_Gen
- STDO_Business_Data_Load
- STDO_SUPLMTRY_INFO
- STDO_Evented_Data_Load

Here, Level 0 sub-process code execution is a prerequisite for Level 1 sub-process execution. Similarly, Level 1 sub-process code execution is a prerequisite for Level 2 sub-process execution and so on. Sub-process within a level can be executed in any order or it can be executed in parallel.

Level 0	Level 1	Level 2
STDO_Event_Load	STDO_EVENT_LOOKUP	
	STDO_EVENT	
	STDO_EVENT_BINDING	
	STDO_EVENT_DETAILS	
STDO_Entity_Surrogate_Key_Gen	BD_ACCOUNTATMDAILY_LOOKUP	STDO_EVENT_ENTITY_MAP
	BD_ACCOUNTDLY_LOOKUP	STDO_EVENT_ENTITY_MAPII
	BD_ACCOUNTTRADEDLY_LOOKUP	STDO_EVENT_ENTITY_MAPIII
	BD_ACCOUNTTRXNDLY_LOOKUP	STDO_EVENT_ENTITY_MAPIV
	BD_ACCOUNT_GROUP_LOOKUP	
	BD_ACCOUNT_PEERGROUP_LOOKUP	
	BD_ACCT_CLIENTBANK_LOOKUP	
	BD_ACCT_PR_TRXN_SMR_MN_LOOKUP	
	BD_ACCT_SMRY_MNTH_LOOKUP	
	BD_CBPEERTRXNSMRY_LOOKUP	
	BD_CLIENTBANK_PEERGRP_LOOKUP	
	BD_CLINETBANKBSMRY_LOOKUP	
	BD_CUSTOMERBALANCE_LOOKUP	
	BD_CUSTOMERDLY_LOOKUP	
	BD_CUSTOMERSMRY_LOOKUP	
	BD_CUSTOMER_ACCOUNT_LOOKUP	
	STDO_ACCOUNT_LOOKUP	
	STDO_CUSTOMER_LOOKUP	
	STDO_BACK_OFFICE_TRXN_LOOKUP	
	STDO_CASH_TRXN_LOOKUP	
	STDO_MI_TRXN_LOOKUP	
	STDO_WIRE_TRXN_LOOKUP	
	BD_CUSTOMER_PRODUCT_LOOKUP	
	BD_DERIVED_ADDRESS_LOOKUP	
	BD_EMPLOYEE_ACCOUNT_LOOKUP	

Level 0	Level 1	Level 2
	BD_EMPLOYEE_LOOKUP	
	BD_EXTERNALENTITYDLY_LOOKUP	
	BD_EXTERNAL_ENTITY_LOOKUP	
	BD_HOUSEHOLDBALDLY_LOOKUP	
	BD_HOUSEHOLDSMRY_LOOKUP	
	BD_INSTACCOUNTSMRY_LOOKUP	
	BD_INSTITUTION_LOOKUP	
	BD_INSTLACCOUNTDLY_LOOKUP	
	BD_INSURANCEPOLICYBAL_LOOKUP	
	BD_INSURANCEPOLICYDLY_LOOKUP	
	BD_INSURPOLICY_CUST_LOOKUP	
	BD_LOANSMRY_LOOKUP	
	BD_LOAN_LOOKUP	
	BD_MANAGEDACCOUNTDLY_LOOKUP	
	BD_MANAGEDACCOUNT_LOOKUP	
	BD_MARKET_CENTER_LOOKUP	
	BD_NETWORKLOGON_LOOKUP	
	BD_NTWKUSER_ACCOUNT_LOOKUP	
	BD_ONLINEACCOUNT_LOOKUP	
	BD_ONLINEACCT_ACCT_LOOKUP	
	BD_PEER_GROUP_LOOKUP	
STDO_Business_Data_Load	BD_ACCT_ATM_SMRY_DAILY	
	BD_ACCT_BAL_POSN_SMRY	
	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_SMRY_MNTH	

Level 0	Level 1	Level 2
	BD_ACCT_SUPPLEMENTAL_ATR	
	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_ONLINE_ACCT_ACCT	
	STDO_ACCT	
	STDO_ACCT_ADDR	
	STDO_ACCT_EMAIL_ADDR	
	STDO_ACCT_PHON	
	STDO_ACCT_RSTRN	
	STDO_ACCT_LIST_MEMBERSHIP	
	BD_CUST_ACCT	
	BD_CUST_ACCT_ROLE	
	BD_CUST_ADDR	
	BD_CUST_CUST	
	BD_CUST_EMAIL_ADDR	
	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	

Level 0	Level 1	Level 2
	BD_EMP_PHON	
	BD_EXTERNAL_ENTITY	
	BD_EXTERNAL_ENTITY_ADDR	
	BD_EXTRNAL_NTTY_MMBRSHP	
	BD_HH_BAL_POSN_SMRY	
	BD_HH_SMRY_MNTH	
	BD_HOUSE_HOLD	
	BD_INSTL_ACCT_SMRY_MNTH	
	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_ONLINE_ACCT	
	BD_WIRE_TRXN	
STDO_SUPLMTRY_INFO	Studio Supplementary Information	
STDO_Evented_Data_Load	STDO_ACCT_EVENT	
	STDO_CUST_EVENT	
	STDO_EMP_EMAIL_ADDR_EVNT	
	STDO_ACCT_PR_TXN_SMRY_MN_EVNT	
	STDO_ACCT_SMRY_MNTH_EVNT	
	STDO_MI_TRXN_EVNT	
	STDO_ACCT_BAL_POSN_SMRY_EVNT	

Level 0	Level 1	Level 2
	STDO_HH_BAL_POSN_SMRY_EVNT	
	STDO_INSTN_MASTER	
	STDO_BOT_EVNT	
	STDO_CASH_TRXN_EVNT	
	STDO_EMP_ACCT_EVNT	
	STDO_ACCT_PEER_GRP_EVNT	
	STDO_NTCPTRY_PRFL_EVNT	
	STDO_ACCT_SUPPLEMENTAL_ATR_EVN	
	STDO_WIRE_TRXN_EVNT	
	STDO_EMP_PHON_EVNT	
	STDO_ONLINE_ACCT_ACCT_EVNT	
	STDO_EMP_ADDR_EVNT	
	STDO_ACCT_ADDR_EVNT	
	STDO_CUST_SMRY_MNTH_EVNT	
	STDO_ONLINE_ACCT_EVNT	
	STDO_EMP_EVNT	
	STDO_ACCT_RSTRN_EVNT	
	STDO_CUST_SUPPL_ATR_EVNT	
	STDO_ACCT_GRP_EVNT	
	STDO_MANGD_ACCT_EVNT	
	STDO_HH_SMRY_MNTH_EVNT	
	STDO_CLIENT_BANK_EVNT	
	STDO_ACCT_ATM_SMRY_DAILY_EVNT	
	STDO_DERIVED_ADDRESS_EVNT	

Correlation

This is used to perform a correlation on loaded STDO events.

- DT_CORRELATION

Scoring

STDO_SCORING is used to perform the scoring of OSTDO events. This has the following sub-process:

- Oracle Behavior Detection Event Scoring
- Oracle Behavior Detection Entity Scoring
- Oracle Behavior Detection Correlation Scoring
- Oracle Behavior Detection Pre-Case Scoring

Promote to Case

STDO_Promote_To_Case_Decision is used to make the decision if an OSTDO correlation can be promoted to a case. This is based on the defined threshold limit. This has the following sub-process:

- Pre Case Promotion Rule

Create Case

STDO_Create_Case is used to create a case if an OSTDO event is promoted to the case.

Following is the list of Promote_To_Case T2Ts:

- Oracle Behavior Detection Generate Cases

Below is the list of T2T tasks for STDO application:

- f_generatecaseid
- f_insertcases
- t2t_KDD_CASE_ACCOUNTS
- t2t_KDD_CASE_CUSTOMERS
- t2t_KDD_CASE_DERIVED_ADDRESS
- t2t_KDD_CASE_EMPLOYEES
- t2t_KDD_CASE_ACCOUNT_ADDRESS
- t2t_KDD_CASE_ACCOUNT_MANAGED
- t2t_KDD_CASE_ACCOUNT_RSTRNS
- t2t_KDD_CASE_ACCT_BAL_POSN_SMRY
- t2t_KDD_CASE_ACCT_EMAIL_ADDR
- t2t_KDD_CASE_ACCT_PEER_GRP
- t2t_KDD_CASE_ACCT_PHON
- t2t_KDD_CASE_ACCT_SMRY_MNTH
- t2t_KDD_CASE_ACCT_SUPPL_ATTR
- t2t_KDD_CASE_ACT_PEER_TRXN_SMRY
- t2t_KDD_CASE_ACCT_NTCPTRY_PRFL
- t2t_FCC_CASE_ACCT_LIST_MBRSP
- t2t_KDD_CASE_CLIENT_BANK

- t2t_KDD_CASE_CLIENT_BANK_SMRY_MNTH
- t2t_KDD_CASE_CUST_ADDR
- t2t_KDD_CASE_CUST_EMAIL_ADDRS
- t2t_KDD_CASE_CUST_LIST_MEMBERSHIP
- t2t_KDD_CASE_CUST_PHONE
- t2t_KDD_CASE_CUST_SUPPL_ATTR
- t2t_KDD_CASE_CUST_SMRY_MNTH
- t2t_KDD_CASE_EMP_ACCT
- t2t_KDD_CASE_EMP_ADDR
- t2t_KDD_CASE_EMP_EMAIL_ADDR
- t2t_KDD_CASE_EMP_PHONE
- t2t_KDD_CASE_INSTL_ACCT_SMRY_MNTH
- t2t_KDD_CASE_INSTN_MASTER
- t2t_KDD_CASE_INSURANCE_POLICY
- t2t_KDD_CASE_INSURANCE_PRODUCT
- t2t_KDD_CASE_NTWK_USER_ACCT_MAP
- t2t_KDD_CASE_ONLINE_ACCT
- t2t_KDD_CASE_ONLINE_ACCT_ACCT
- t2t_KDD_CASE_PEER_GRP
- t2t_KDD_CASE_CB_LIST_MEMBERSHIP
- t2t_KDD_CASE_CB_PEER_TXN_SMRY_MNTH
- t2t_KDD_CASE_CLIENT_BANK_PEER_GRP
- t2t_KDD_CASE_EXTERNAL_ENTITY
- t2t_KDD_CASE_EXTERNAL_ENTITY_MEMBERSHIP
- t2t_KDD_CASE_HH_ACCT_BAL_SMRY
- t2t_KDD_CASE_HH_SMRY_MNTH
- t2t_KDD_CASE_INSURANCE_PLCY_CUST
- t2t_KDD_CASE_NVSMT_MGR_SMRY_MNTH
- t2t_KDD_CASE_NVSMT_MGR
- t2t_KDD_CASE_ACCT_ID_INSTN_ID_MAP
- t2t_KDD_CASE_ACCT_GRP
- t2t_KDD_CASE_WIRE_TRXN
- t2t_KDD_CASE_CASH_TRXN

- t2t_KDD_CASE_DERIVED_ADDRESS_CASH_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_MI_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_WIRE_TRXN
- t2t_KDD_CASE_BACK_OFFICE_TRXN
- t2t_KDD_CASE_CUST_IMP_LICENSE_GOODS
- t2t_KDD_CASE_CUST_IMP_LICENSE
- t2t_KDD_CASE_DOC_COLL_CNTRCT
- t2t_KDD_CASE_DOC_COLL_CNTRCT_EVENT
- t2t_KDD_CASE_DOC_COLL_DISCRP_DTL
- t2t_KDD_CASE_DOC_COLL_INVOICE
- t2t_KDD_CASE_DOC_COLL_MULTNR_DTL
- t2t_KDD_CASE_DOC_COLL_SHPMT_DTL
- t2t_KDD_CASE_EXTERNAL_INSURANCE_PLCY
- t2t_KDD_CASE_EXTERNAL_ORG
- t2t_KDD_CASE_TRADE_FIN_SWIFT_MSG
- t2t_KDD_CASE_TRADE_FIN_PARTY
- t2t_KDD_CASE_TRADE_FIN_GOOD_SRVC
- t2t_KDD_CASE_TRADE_FIN_DRAFT
- t2t_KDD_CASE_TRADE_FIN_DOC
- t2t_KDD_CASE_TRADE_FIN_CNTRCT
- t2t_KDD_CASE_TRADE_FIN_BRKRGE_DIST
- t2t_KDD_CASE_TRADE_FIN_BRKRGE
- t2t_KDD_CASE_TRADE_FIN_ACCT
- t2t_KDD_CASE_TRADE
- t2t_KDD_CASE_ORDER
- t2t_KDD_CASE_MI_TRXN
- t2t_KDD_CASE_LOAN_ACCOUNT
- t2t_KDD_CASE_LOAN
- t2t_KDD_CASE_LOAN_SMRY_MONTH
- t2t_KDD_CASE_INSTRUCTION
- CASE_COMPLETION_FLAG
- CASE_ASSIGNMENT

End Batch

STDO_ECM_End_E2E_Batch is used for ending the batch execution for Studio.

Third-party Application Process

The 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 the Landing area to Consolidation area. Here, the data will populate to the Landing area from the Staging area. This has following four sub-processes:

- Loading Events: See the Level 1 and 2 in *Table 45*
- Entity Surrogate Key Generation: See Level 3 and 4 in *Table 45*
- Evented Data Load: See the Level 5 in *Table 45*
- Derive Wire, Cash and MI Transaction: See the Level 6 in *Table 45*

Table 45 contains 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 a 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 the business data population (see the **Business Metadata Movement**).

Table 45. Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
t2t_LOOKUP_EVENT	t2t_EVENTS t2t_FCC_EVENT_BINDING t2t_FCC_EVENT_DETAILS	t2t_LOOKUP_ACCOUNT t2t_LOOKUP_CUSTOMER t2t_LOOKUP_EMPLOYEE t2t_LOOKUP_EXTERNAL_ENTITY t2t_LOOKUP_INSTITUTION_CB t2t_LOOKUP_ACCOUNT_GROUP t2t_LOOKUP_BOT t2t_LOOKUP_FOT	t2t_FCC_EVENT_ENTITY_MAP_ACCOUNT t2t_FCC_EVENT_ENTITY_MAP_CUSTOMER t2t_FCC_EVENT_ENTITY_MAP_EMPLOYEE t2t_FCC_EVENT_ENTITY_MAP_EXTERNAL_ENTITY t2t_FCC_EVENT_ENTITY_MAP_CLIENT_BANK t2t_FCC_EVENT_ENTITY_MAP_ACCOUNT_GROUP t2t_FCC_EVENT_ENTITY_MAP_FOTWIRE t2t_FCC_EVENT_ENTITY_MAP_FOTCASH t2t_FCC_EVENT_ENTITY_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_ADDR t2t_EVENTED_NTCPTRY_PRFL_ACCT t2t_EVENTED_NTCPTRY_PRFL_CUST t2t_EVENTED_ACCT_BAL_POSN_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_SUPPLEMENTAL_ATTR t2t_EVENTED_DERIVED_ADDRESS t2t_EVENTED_EMP_PHON t2t_EVENTED_EXTERNAL_ENTITY 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_BNK2BNK_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 Phone 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 the business data population (see the Business Metadata Movement). This sub-process code has to be executed after the business data population.	

Correlation

Correlation is used to perform correlation on loaded BD events. This has following two tasks:

- PGX_CORRELATION
- BD_CORRELATION

Scoring

This is used to perform the scoring of third-party events, entities and correlation. This has the 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 the defined threshold limit.

Create Case

Create_Case is used to create a case if a third-party event is promoted to the case.

Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts (see the *Table*)
- 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

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.

Note: PGX based correlation is not supported on AIX and Solaris SPARC OS. You can use Java-SQL correlation, which is a functionally equivalent module to PGX based correlation.

Pre-requisites

Below is the list of pre-requisites:

1. Java 8 is mandatory as PGX is the default.
2. `Initiatecorrelation.sh` should be triggered once before calling batch. This configures correlation module. This instruction already there as part of the old correlation module.
3. `<installed path>/ficdb/lib_PGX/ pgxConfig.cfg` where k hop should be configured by the user between 2 and 10. The default value is 5.

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 the 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 the batch needs a rerun?

Remove all the CA tables data for the MISDATE and Data Origin. Start a new batch again.

There can be cases where source schema is different but data resides in the same instance. In this case, `Grant select to all user tables` need 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 a few wrong records into a 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.

How can I create new attributes?

To understand how to create new attributes, see the ECM Case Type Attributes section.

How do I manage the parameters of attributes?

Setting the parameters for attributes is completed in the database. The parameters available are:

- Manual create case page
- Case search page
- Case Search results page
- Display page of Case Context
- Editable page of Case Context

To understand how to modify these parameters, see the ECM Case Type Attributes section.

Can I set the order of the tabs to define how the as seen in a case?

Yes. In Case Type Designer you can drag and drop the entities tabs to the order you desire and that will be replicated in the individual case. At this time individual users are not allowed to re-order the tab.

How do I define the tab a user lands on when entering the case details?

Whichever entity you have defined as the furthest to the left in the Case Entities section of that Case Type will be the tab a user lands on when the access the Case Details.

What is the Event Details tab?

The Event Details tab displays all the events associated with the case. Unless specified otherwise these would be the s created in FCCM Behavior Detection or external events ingested into the ECM landing area. Other products have similar tabs which are labeled accordingly in the Case Entities section for each Case Type. It is recommended that these tabs be the default landing tab for users when they access the case details.

Can I deactivate a case type or case class?

Not available in the current version.

Can I rename tabs?

Currently, individual users cannot rename their tabs. However, it is possible to change the name of the tab or make it different from what is Case Designer. Case Designer tab names pull from KDD_CASEENTITY_MASTER. The Case UI pulls from AAI_FF_FORMS_CONTAINERS_TL

Can the business entities that I see in a case be dependent on the types of events associated with the case and not explicitly defined in the Case Type?

The business entities displayed are only those defined in the case type definition. In previous versions of ECM, some tabs were displayed dynamically based on if the focus of an event contains those entities. This feature will be reserved for future releases.

What happens if I change the attribute and entity configuration of a case type for a case type which is currently active?

The updated case type will apply to all cases of that type. Both those currently active and all new cases.

What happens if I change the underlying PMF workflow definition for a case type which is currently active?

Refer to PMF section for this type of information