

Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.5.0.0

November 2017



Administration & Configuration Guide

Oracle Financial Services

Enterprise Case Management

Release 8.0.5.0.0

November 2017

Part Number: E83847-01

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

Part Number: E83847-01
First Edition (November 2017)

Copyright © 2017, Oracle and/or its affiliates. All rights reserved.

Printed in U.S.A. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise without the prior written permission.

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 11

Who Should Use this Guide	11
How this Guide is Organized	11
Where to Find More Information.....	13
Conventions Used in This Guide.....	13

CHAPTER 1 About Oracle Financial Services Enterprise Case Management 1

Introduction	1
Administration and Configuration Activities	2
Loading Data	2
Correlation	2
Scoring	2
Promoted to Case.....	2
Processing Modelling Framework	2
Case Designer	3
Case Assigner Editor	3
Case Action Settings	3

CHAPTER 2 Getting Started..... 5

System Requirements	5
Accessing OFSAA Applications	6
Selecting Applications	7
Managing OFSAA Application Page.....	8
Applications Tab	8
Object Administration Tab.....	8
System Configuration and Identity Management Tab.....	9
Change Password	10
Copyright Information	11
Troubleshooting Your Display	12
Enabling JavaScript.....	12
Enabling Cookies	12
Enabling Temporary Internet Files	12
Enabling File Downloads	13
Setting Printing Options	13
Enabling Pop-up Blocker	13
Setting Preferences.....	14

CHAPTER 3 Managing User Administration and Security Configuration..... 15

About User Administration	15
Administrator User Privileges.....	15
User Provisioning Process Flow	16
Requirements to Access ECM Application	17
Managing User Administration	17
Managing Identity and Authorization.....	17
<i>Managing Identity and Authorization Process Flow.....</i>	17
<i>Creating and Authorizing a User.....</i>	18
<i>Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload.....</i>	18
<i>Creating or Editing User.....</i>	19
<i>Mapping a User with a User Group.....</i>	19
Adding Security Attributes	20
About Security Attributes	20
<i>Types of Security Attributes.....</i>	20
<i>Jurisdiction.....</i>	20
<i>Business Domain</i>	21
<i>Case Type.....</i>	21
<i>Organization</i>	21
Loading Security Attributes.....	22
<i>For more information on loading Case type, see the Managing Case Designer section.....</i>	22
<i>Loading Security Attributes through Excel.....</i>	22
<i>Uploading Excel</i>	22
<i>Loading Security Attributes through SQL Scripts.....</i>	23
<i>Loading Jurisdictions</i>	23
<i>Loading Business Domains</i>	23
<i>Loading Organizations</i>	24
Mapping Security Attributes to	Organizations and Users24
Introduction	25
Prerequisites for Mapper Maintenance.....	25
<i>Loading Security Attributes Data</i>	25
<i>Configuring Function.....</i>	25
<i>Resaving Metadata.....</i>	26
<i>Hierarchy Re-save.....</i>	26
<i>Derived Entity Re-save</i>	26
<i>Loading User Configuration Data.....</i>	26
Using Mapper Maintenance.....	27
<i>Updating Control Access tables from Mapper.....</i>	28
<i>Changing ICC Batch Ownership to ECM Admin from SYSADMN user.....</i>	29
<i>Batch Maintenance</i>	29
<i>Batch Execution</i>	30
<i>Batch Monitor/Checking the Execution Status</i>	31
CHAPTER 4	Pre Batch Execution Configuration
	35
Start a Batch.....	35
Correlation	35
<i>Initiating Correlation.....</i>	36
<i>Configuring Correlation Rules</i>	36
Correlation Case Type Mapping	38

Ending a Batch	38
CHAPTER 5 Performing Batch Run	39
About Batch Run	39
Starting a Batch Run	39
Ending a Batch Run	42
.....	42
Executing a Batch Run	43
CHAPTER 6 Loading Data	47
About Loading Data	47
Types of Connectors	47
Using Connectors	47
Accessing Connector Processes	48
Loading OBD Data	48
Loading OCS Data	49
Loading KYC Data	49
Loading Third Party Connector Data	50
Data Movement (DM) Utility	51
<i>DM Metadata Tables</i>	52
<i>DM Audit and Error Details Tables</i>	55
Configuring Data Movement from LA to CA	55
About Data Movement	55
Sample Processes	55
Using Precedence	57
Designing Processes	57
CHAPTER 7 Configuring Correlation	61
About Correlation	61
Using Business Entity Paths	61
Correlation Business Path	61
Correlation Business Entity Configuration	62
Executing Correlation Rules	63
Performing Jobs	63
Sample Correlation Rules	63
CHAPTER 8 Scoring	65
About Scoring	65
Initial Scoring	65
<i>Day - 1</i>	66
<i>Day - 2</i>	66
<i>Day - 3</i>	66

Adjustment Scoring	66
<i>Days - 1</i>	67
<i>2nd Month</i>	67
<i>3rd Month</i>	68
Types of Scoring	68
Event Scoring	68
Entity Scoring	68
Correlation Scoring	68
Pre case Scoring.....	68
Configuring Scoring Rules	69
Configuring AML Event Initial Scoring.....	69
Scoring Samples	76
Event.....	76
<i>Scenario</i>	76
<i>Total Transaction Amount and Risk Score</i>	77
<i>Aging</i>	77
Entity.....	78
<i>Watch List Screening</i>	78
<i>Effective Risk</i>	78
Correlation	79
<i>Number of events</i>	79
<i>Combination of Scenarios</i>	80
<i>Total Transaction Amount</i>	80
<i>Repeated Scenario Events</i>	80
CHAPTER 9 Promoting to Case	83
About Promoting to Case (PTC)	83
Configuring PTC	83
CHAPTER 10 Configuring Processing Modelling Framework (PMF)	85
About PMF.....	85
..... ECM Workflow Development Life Cycle	85
ECM Workflows	85
Pre-configuration Activities	86
Configuring Status.....	86
Configuring Action	86
Configuring Attributes	86
Accessing Process Modeller.....	88
Configuring an ECM Workflow.....	89
Creating Workflow.....	89
Defining Datafields.....	91
..... Defining Application Rules	91
Using Process Modeller Editor.....	92
<i>Starting a Process</i>	92

<i>Implementing a Process</i>	93
<i>Adding Transition</i>	93
<i>Adding an Activity</i>	93
<i>Implementing an Activity</i>	94
<i>Adding Transition</i>	95
Editing of an ECM Workflow	97
Deleting an ECM Workflow	98
 CHAPTER 11 <i>Managing Case Designer</i>	101
About Case Designer	101
Accessing Case Designer	101
Case Designer Home page	102
Defining Case Class	103
About Case Class	103
Adding Case Class	103
Editing Case Class	103
Defining Case Type	104
About Case Type	104
Adding Case Type	104
<i>Configuring Optional Definitions in CaseType</i>	106
<i>About Optional Definitions</i>	106
<i>Defining Attributes</i>	106
About Attributes	106
Adding Optional Attributes to the Case Type	106
Deleting Attributes	107
<i>Defining Entities</i>	108
About Entities	108
Adding Optional Entities to the Case Type	108
Deleting Entities	109
<i>Defining Workflow</i>	110
About Workflows	110
Adding Workflow	110
Deleting Workflow	111
Editing Case Type	112
.....	112
 CHAPTER 12 <i>General Configuration</i>	113
Configuring the Client Logo Image	113
Logo Specification	113
Placing a new Client Logo	113
Removing a Client Logo	114
Configuring the Base Time Zone	114
Accessing Manage Parameters	114
Modifying Time Zone	114
Configuring the Default Currency Code	115
Configuring Lock Time Period for Case Actions	116

Configuring E-mail.....	118
Configuring Organization Type	119
Configuring View All Organization.....	119
Configuring the Display of Value in By Field Name/ID.....	120
Configuring the Default Due Date Calculation	121
Configuring File Size.....	121
Configuring Views.....	122
Adding Views.....	122
Modifying Views	122
Removing Views.....	123
Configuring ECM Security Function.....	123
Managing Additional Configurations	124
Configuring File Type Extensions.....	124
 CHAPTER 13 Configuring Administration Tools.....	 125
Configuring Administration Tools.....	125
Configuring Application Server.....	126
 CHAPTER 14 Managing Case Assigner Editor.....	 127
About Case Assigner Editor	127
Accessing Case Assigner Editor.....	128
Case Assigner Screen Elements.....	128
Case Assigner Editor	129
<i>Assignment Rule List for Cases</i>	<i>129</i>
<i>Role Based Assignment Limits Editor</i>	<i>130</i>
Assignment Rule Editor.....	131
Using Case Assigner Editor	133
Adding a New Rule.....	133
Modifying a Rule	133
Deleting a Rule	134
Adding a Role Based Assignment Limit.....	134
Adding an Exception to a Role Based Assignment Limit	134
Modifying an Exception.....	135
Deleting an Exception.....	135
 CHAPTER 15 Configuring Actions	 137
Working with Case Action Settings	137
Understanding Case Workflows	137
Adding New Case Statuses	137
Configuring Case Action Data.....	138
<i>Adding a New Action Category</i>	<i>138</i>
<i>Adding a New Action</i>	<i>138</i>
<i>Mapping New Action to User Role</i>	<i>139</i>

<i>Mapping the New Action to Status</i>	140
<i>Map the New Action to the Case Type</i>	140
Configuring Standard Comment Data	140
Configuring Mandatory Action Attributes	140
Making Comments Mandatory	141
Making Reassignment Mandatory	141
Making a Due-Date for an Action Mandatory	141
CHAPTER 16 Configuring Web Application	143
Configuring the Session Timeout Setting	143
Configuring the Session Timeout Setting	143
Configuring the Session Timeout Setting for Admin Tools	143
APPENDIX A List of Processes and Tasks	145
OBD Application Process	145
Start Batch	145
Load Data from BD to ECM	145
Correlation	145
Scoring	145
Promote to Case	146
Create Case	146
End Batch	148
OCS Application Process	148
Start Batch	149
Load Data from CS to ECM	149
Correlation	149
Scoring	149
Promote to Case	149
Create Case	149
End Batch	149
OKYC Application Process	150
Start Batch	150
Load Data from KYC to ECM	150
Correlation	150
Scoring	150
Promote to Case	151
Create Case	151
Update Case ID	151
End Batch	151
Third party Application Process	151
Start Batch	151
Load Data from Third Party to ECM	151
Correlation	152
Scoring	152

Promote to Case.....	152
Create Case.....	152
<i>Create_Case is used to create a case if a Third Party event is promote to case.</i>	152
End Batch.....	152
APPENDIX B	
Configuring Parallel Graph AnalytiX (PGX) Correlation	153
Overview.....	153
Configuring Parallel Graph AnalytiX (PGX) Correlation.....	153
APPENDIX C	
Managing Batch Processing Utilities	155
About Batch Processing Utilities	155
Prerequisites for an Administrator User.....	157
Managing Common Resources for Batch Processing Utilities.....	158
Install.cfg File.....	158
<i>Categories.cfg File</i>	171
<i>Configuring Console Output</i>	174
Managing Annual Activities	174
Loading Holidays	174
Loading Non-business Days	176
Managing Alert and Case Purge Utility	177
Directory Structure	177
Logs.....	178
Precautions.....	178
Using the Alert and Case Purge Utility.....	178
<i>Configuring the Alert and Case Purge Utility</i>	179
<i>Executing the Alert and Case Purge Utility</i>	187
<i>Processing for Purging</i>	187
<i>Automatic Restart Capability</i>	188
Sample Alert And Case Purge Processes.....	188
<i>Example 1</i>	188
<i>Example 2</i>	189
Managing Batch Control Utility	190
Batches in Behavior Detection	190
Directory Structure	191
Logs.....	191
Using the Batch Control Utility	191
<i>Configuring the Batch Control Utility</i>	192
<i>Setting Up Batches</i>	192
<i>Single Batch</i>	193
<i>Single Site Intra-day Processing</i>	193
<i>Multiple Countries</i>	193
<i>Starting a Batch Process Manually</i>	194
<i>Processing for Batch Start</i>	194
<i>Ending a Batch Process</i>	195
<i>Processing for End Batch</i>	195
<i>Identifying a Running Batch Process</i>	196

To Obtain a Batch Name	196
<i>Obtaining a Batch Name</i>	<i>196</i>
Managing Calendar Manager Utility	197
Directory Structure	197
Logs	197
Calendar Information	198
Using the Calendar Manager Utility	198
<i>Configuring the Calendar Manager Utility.....</i>	<i>198</i>
<i>Executing the Calendar Manager Utility.....</i>	<i>199</i>
Starting the Utility Manually	199
<i>Updating the KDD_CAL Table.....</i>	<i>199</i>
Managing Data Retention Manager	201
Directory Structure	202
Logs	202
Processing Flow	203
Using the Data Retention Manager	203
<i>Configuring the Data Retention Manager.....</i>	<i>204</i>
<i>Executing the Data Retention Manager</i>	<i>205</i>
Running the Data Retention Manager.....	206
<i>Creating Partitions.....</i>	<i>207</i>
<i>Maintaining Partitions.....</i>	<i>207</i>
Managing Daily Partitioning Alternative	208
Partition Structures	208
Recommended Partition Maintenance.....	208
Managing Alternative Monthly Partition	209
Adding a Monthly Database Partition	209
Dropping a Monthly Database Partition	209
<i>Maintaining Indexes</i>	<i>209</i>
Utility Work Tables.....	209
<i>KDD_DR_MAINT_OPRTN Table</i>	<i>209</i>
<i>KDD_DR_JOB Table</i>	<i>210</i>
<i>KDD_DR_RUN Table</i>	<i>211</i>
Database Statistics Management	211
Logs	211
Using Database Statistics Management	211
Managing Flag Duplicate Alerts Utility	212
Using Flag Duplicate Alerts Utility.....	213
Executing Flag Duplicate Alerts Utility.....	213
.....	213
Managing Notification	213
<i>Event Based.....</i>	<i>213</i>
<i>Batch Based</i>	<i>214</i>
Managing Push E-mail Notifications	214
Using Push E-mail Notification.....	215
Configuring Push E-mail Notification.....	215
<i>Configuring General Notification Properties.....</i>	<i>216</i>
<i>Configuring Notifications.....</i>	<i>217</i>
<i>Configuring Notification Queries</i>	<i>219</i>

Logs	221
Refreshing Temporary Tables	222
Logs	222
Using Refreshing Temporary Tables	222
Populating Temporary Tables for Scenarios.....	222
<i>IML-HiddenRelationships-dINST</i>	222
<i>ML-NetworkOfAcEn-fAC</i>	223
<i>FR-NetworkOfAcEn-fAC</i>	224
<i>CST-Losses</i>	225
<i>CST-UncvrdLongSales-dRBPC</i>	225
Managing Truncate Manager	225
Logs.....	225
Using the Truncate Manager	225
Managing ETL Process for Threshold Analyzer Utility.....	225
Running Threshold Analyzer	226
Managing Deactivate Expired Alert Suppression Rules	227
 APPENDIX D FAQ	 229

About this Guide

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

This section focuses on the following topics:

- [Who Should Use this Guide](#)
- [How this Guide is Organized](#)
- [Where to Find More Information](#)
- [Conventions Used in This Guide](#)

Who Should Use this Guide

This *Administration and Configuration Guide* is designed for use by the Administrators. This user configures, maintains, and adjusts the system. The Administrator is usually an employee of a specific Oracle customer, who maintains user accounts and roles, assigns cases to users, manages case 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, Managing Case Assigner Editor*, provides details about ownership assignment of cases to various users.
- *Chapter 15, Configuring Actions*, provides procedures to configure the list of available actions.
- *Chapter 16, Configuring Web Application*, provides customization features available in the Web Application UI. This chapter contains information to configure session time out.
- *Appendix A, List of Processes and Tasks*, provides the details of batch processes and tasks.

Where to Find More Information

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

- *Oracle Financial Services Enterprise Case Management Application Release Notes or ReadMe*
- *Oracle Financial Services Enterprise Case Management Application User Guide*
- *Oracle Financial Services Enterprise Case Management Application Installation Guide*
- *Oracle Financial Services Data Model (FSDM) Guide*

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

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

Conventions Used in This Guide

This table lists the conventions used in this guide.

Table 1. Conventions Used in This Guide

Convention	Description
<i>Italics</i>	<ul style="list-style-type: none">● Names of books, chapters, and sections as references● Emphasis
Bold	<ul style="list-style-type: none">● 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	<ul style="list-style-type: none">● 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>	<ul style="list-style-type: none">● Substitute input value

About Oracle Financial Services Enterprise Case Management

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

The following sections are covered in this chapter:

- [Introduction](#)
- [Administration and Configuration Activities](#)

Introduction

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

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

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

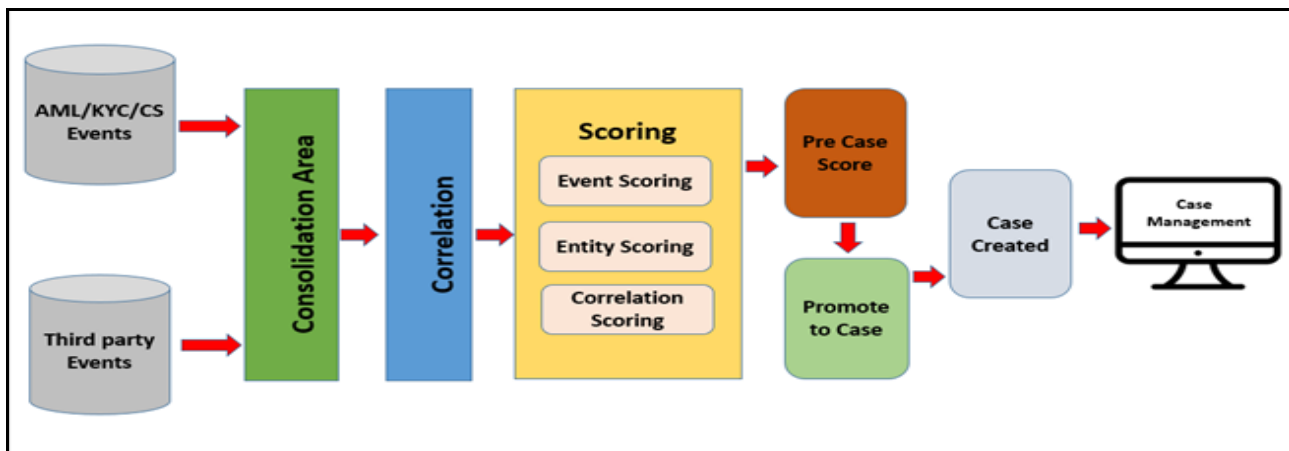


Figure 1. ECM Workflow

Administration and Configuration Activities

This section covers the following topics:

- [Loading Data](#)
- [Correlation](#)
- [Scoring](#)
- [Promoted to Case](#)
- [Processing Modelling Framework](#)
- [Case Designer](#)
- [Case Assigner Editor](#)
- [Case Action Settings](#)

Loading Data

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

Correlation

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

Scoring

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

Promoted to Case

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

Processing Modelling Framework

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

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

Case Designer

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

Case Assigner Editor

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

Case Action Settings

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

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

The following sections are covered in this chapter:

- [System Requirements](#)
- [Accessing OFSAA Applications](#)
- [Managing OFSAA Application Page](#)
- [Troubleshooting Your Display](#)

System Requirements

The following applications are required to run the 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 OFSAA Applications

Access to the Oracle Financial Services Case Management application depends on the Internet or Intranet environment. Oracle Financial Services Case Management is accessed through Microsoft Internet Explorer (IE). 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 more information, see [Change Password](#) section.

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

To access OFSAA Applications, follow these steps:

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

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

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

The OFSAA login page is displayed.



Figure 2. OFSAA Login Page

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

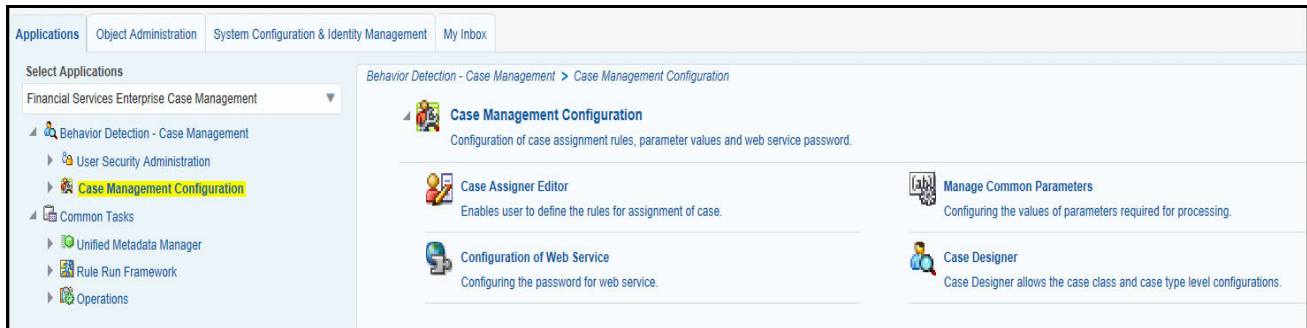


Figure 3. OFSAA Application Page

The OFSAA Application page is a common landing page for all users until a preferred application page is set. For more information about how to set your preferred application page, see [Setting Preferences](#). You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

Selecting Applications

This section explains how to access required applications.

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

This page is divided into two panes:

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

To access ECM applications, follow these steps:

1. Navigate to OFSAA Applications page.
2. Select **Financial Services Enterprise Case Management**. The Enterprise Case Management page is displayed.

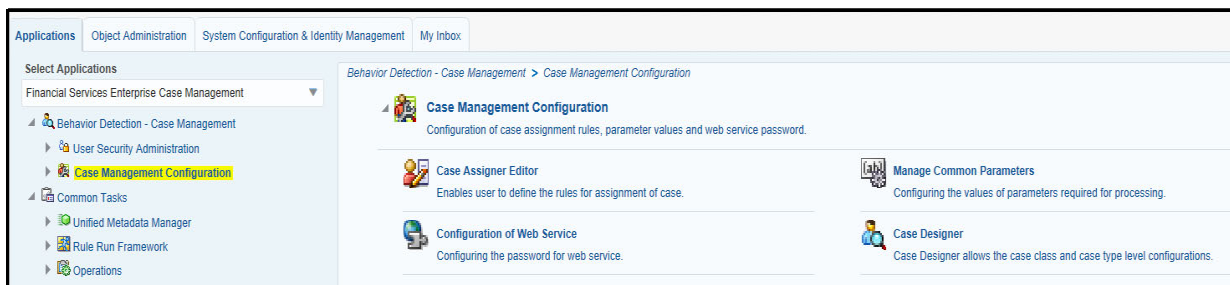


Figure 4. Enterprise Case Management Page

Managing OFSAA Application Page

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

The OFSAA Application page has the following tabs:

- [Applications Tab](#)
- [Object Administration Tab](#)
- [System Configuration and Identity Management Tab](#)
- [Change Password](#)
- [Copyright Information](#)

Applications Tab

The Applications tab lists the OFSAA Applications that are installed in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups).

To access the OFSAA Applications, select the required Application from Select Applications drop-down list. For Case Management, select **Financial Services Case Management**. Based on your selection, the page refreshes the menus and links across the panes.

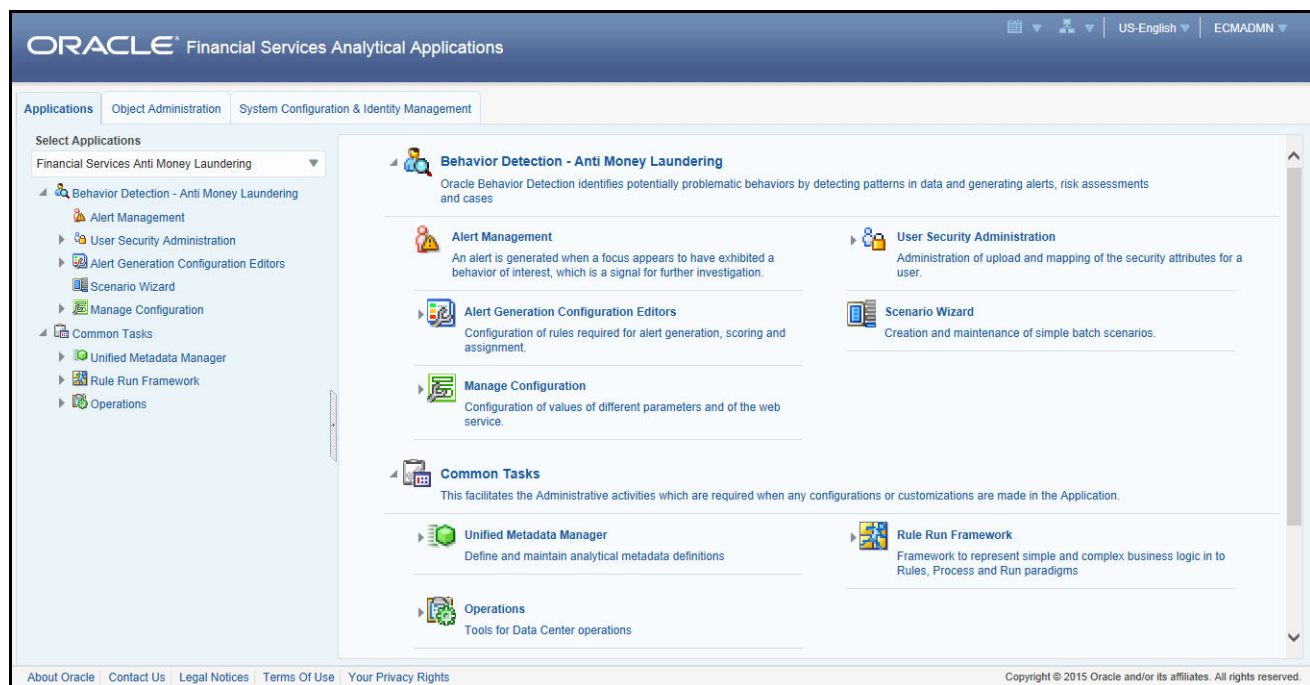


Figure 5. Applications Tab

Object Administration Tab

Object Administration is an integral part of the Infrastructure system and allows system administrators to define the security framework with the capacity to restrict access to the data and metadata in the warehouse, based on a flexible, fine-grained access control mechanism. These activities are mainly done at the initial stage, and then as required.

This tab includes information related to the workflow of the Infrastructure Administration process with related procedures to assist, configure, and manage administrative tasks.

The Object Administration tab lists the OFSAA Information Domains created in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups.

To define or maintain access for an Information Domain, select the required Information Domain from the Select Information Domain drop-down list. Based on your selection, the page refreshes the menus and links across the panes.

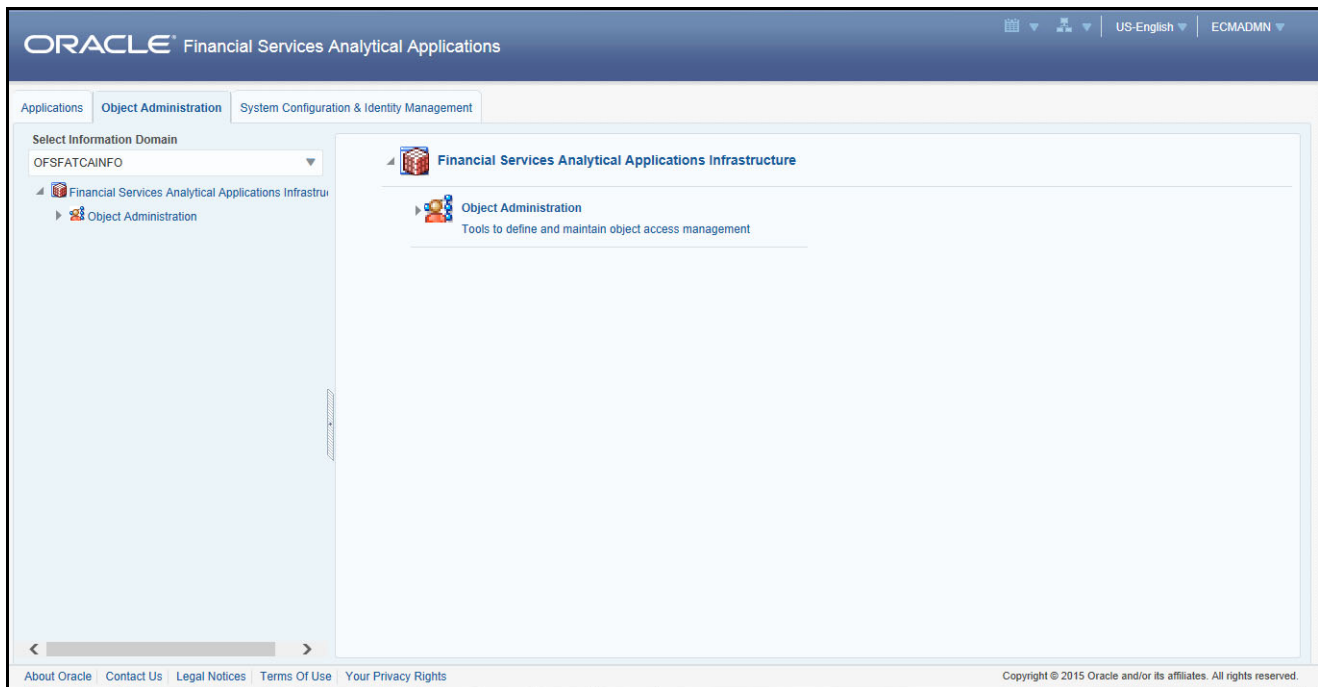


Figure 6. Object Administration Tab

System Configuration and Identity Management Tab

System Configuration and Identity Management is an integral part of the Infrastructure administration process. This tab helps System Administrators to provide security and operational framework required for the Infrastructure.

System Administrators can configure Server, Database, OLAP, and Information Domains, along with other configuration processes such as segment and metadata mapping, segments to securities mapping, and rules setup. The System Configuration is a one-time activity, which helps the System Administrator make the Infrastructure system operational.

The System Configuration and Identity Management tab lists the OFSAA Infrastructure System Configuration and Identity Management modules. These modules work across Applications and Information Domains, so there is no Application or Information Domain drop-down list in this tab.

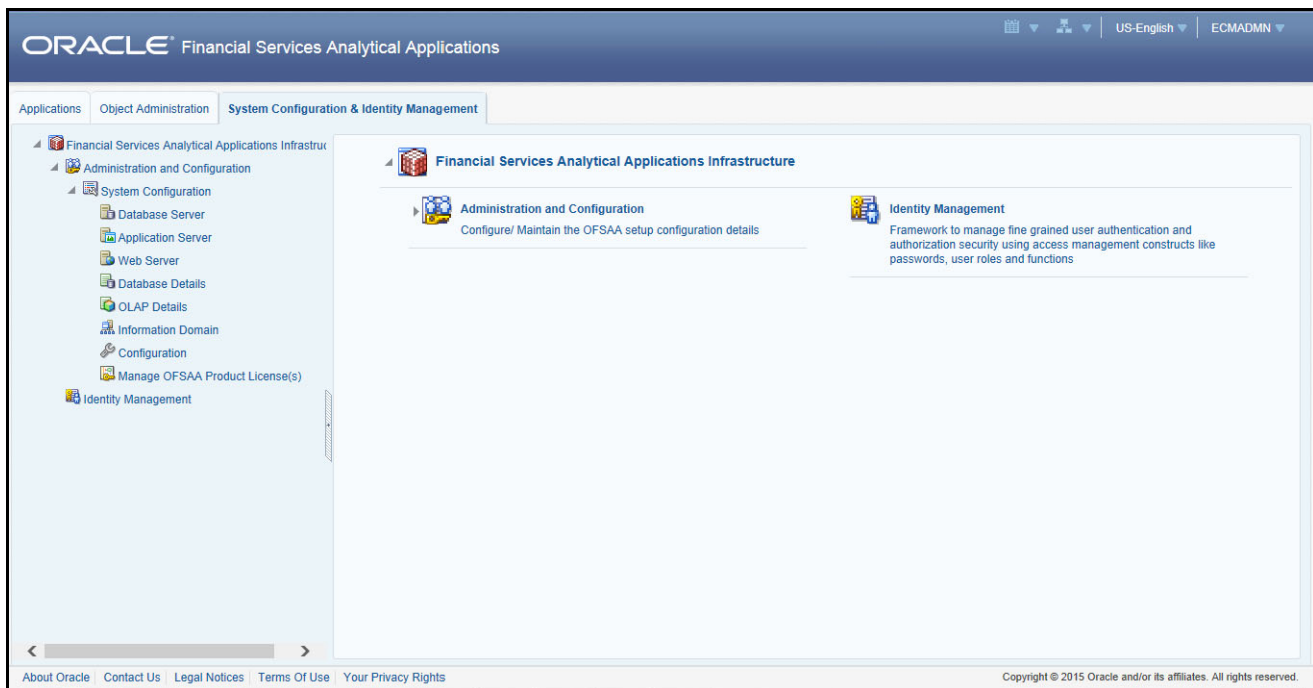


Figure 7. System Configuration and Identity Management Tab

Selecting Identity Management allows System Administrators to manage Users, User Groups, and the functions each User or User Group can access. For more information about managing Users and User Groups, see [Administration Guide](#).

Change Password

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

To change the password, follow these steps:

1. Navigate to OFSAA Applications page.

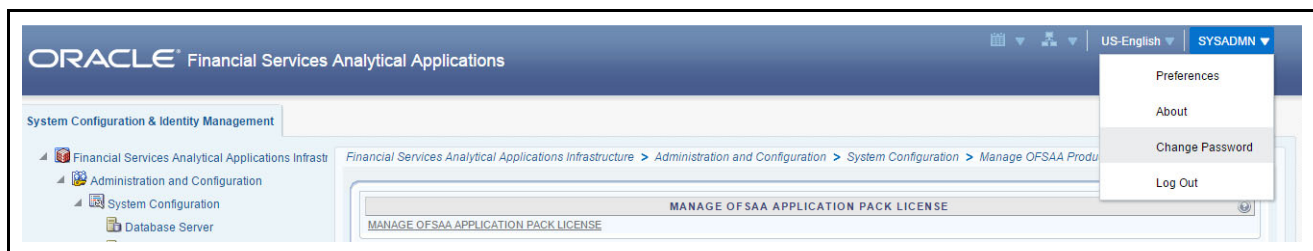


Figure 8. Change Password

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



Figure 9. Change Password

3. Enter your old and new password in the respective fields.
4. Click **OK**. Your password is changed successfully. The application navigates back to the Login page where you can login with the new password.

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

Copyright Information

To access copyright information, click the User drop-down list and select **About** in OFSAA login page. The Copyright text displays in a new window.

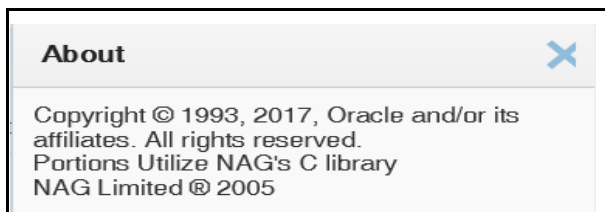


Figure 10. Copyright Information

Troubleshooting Your Display

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

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

This section covers following topics:

- [Enabling JavaScript](#)
- [Enabling Cookies](#)
- [Enabling Temporary Internet Files](#)
- [Enabling File Downloads](#)
- [Setting Printing Options](#)
- [Enabling Pop-up Blocker](#)
- [Setting Preferences](#)

Enabling JavaScript

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

1. From the Tools menu, click **Internet Options**.
The Internet Options dialog box displays.
2. Click the **Security** tab.
3. Click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**.

The Security Setting - Local Intranet Zone dialog box displays.

5. In the Settings list and under the Scripting setting, ensure that Enable is selected for all options.
6. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

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

Enabling Temporary Internet Files

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

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

The Internet Options dialog box displays.

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

The Website Data Settings dialog box displays.

3. Select the **Every time I visit the webpage** option.
4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

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

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

The Internet Options dialog box displays.

2. Click the **Security** tab.
3. Click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**.

The Security Setting - Local Intranet Zone dialog box displays.

5. Under the Downloads section, ensure that **Enable** is selected for all options.
6. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

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

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

The Internet Options dialog box displays.

2. Click the **Advanced** tab.
3. In the Settings list, under the Printing setting, click **Print background colors and images**.
4. Click **OK** to exit the Internet Options dialog box.

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

Enabling Pop-up Blocker

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

To enable Pop-up Blocker, follow these steps:

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

The Internet Options dialog box displays.

2. Click the **Privacy** tab.
3. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option.

The **Settings** is enabled.

4. Click **Settings** to open the Pop-up Blocker Settings dialog box.
5. In the Pop-up Blocker Settings dialog box, enter the URL of the application in Address of website to allow.
6. Click **Add**.

The URL appears in the Allowed sites list.

7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

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

To access this section, follow these steps:

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

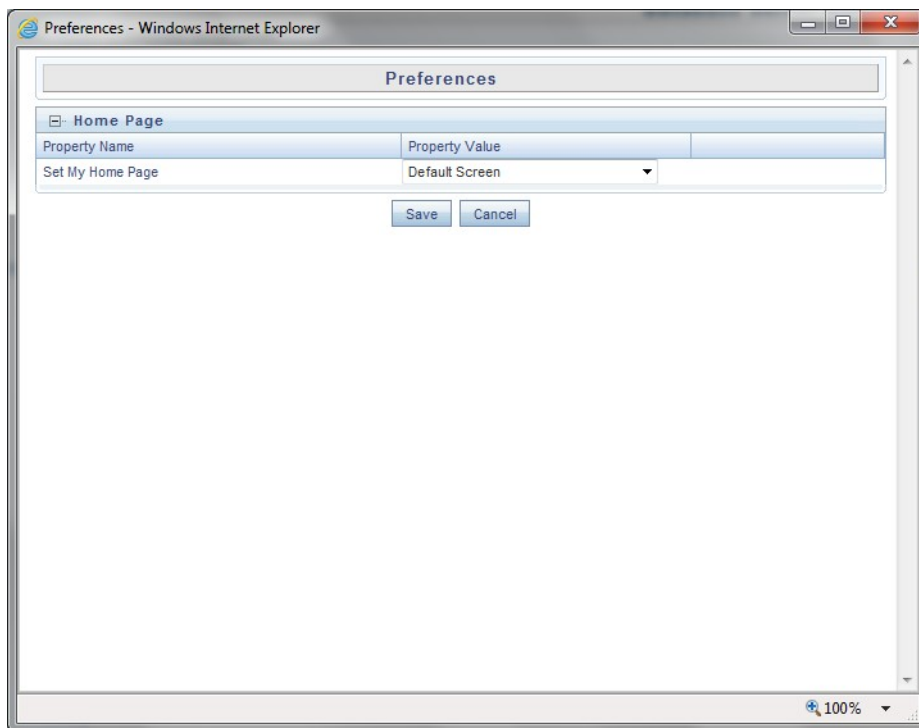


Figure 11. Preference screen.

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

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

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

Managing User Administration and Security Configuration

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

The following sections are covered in this chapter:

- [About User Administration](#)
- [Administrator User Privileges](#)
- [User Provisioning Process Flow](#)
- [Managing User Administration](#)
- [Adding Security Attributes](#)
- [Mapping Security Attributes to Organizations and Users](#)

About User Administration

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

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

Administrator User Privileges

[Table 2](#) lists the access permissions of the ECM administrator.

Table 2. Access Permissions for Administrators

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

Table 2. Access Permissions for Administrators

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

User Provisioning Process Flow

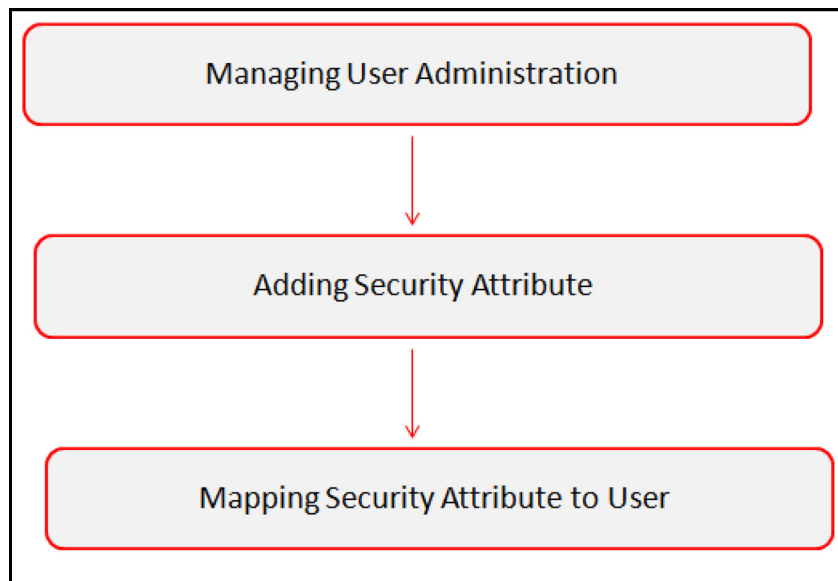


Figure 12. User Provisioning Process Flow

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

Table 3. User Provisioning Process Flow

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

Requirements to Access ECM Application

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

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

Table 4. Requirements

Applications	Conditions
Case Management	<ul style="list-style-type: none">● Set of policies that associate functional roles with access to specific system functions● Access to one or more case types● One or more associated organizational affiliations that control the user's access to cases● Access to one or more jurisdictions● Access to one or more business domains
Administration Tools	Set of policies that associate the admin functional role with access to specific system functions

Managing User Administration

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

Managing Identity and Authorization

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

This section covers the following topics:

- [Managing Identity and Authorization Process Flow](#)
- [Creating and Authorizing a User](#)
- [Mapping a User with a User Group](#)

Managing Identity and Authorization Process Flow

Figure 13 shows the process flow of identity management and authorization.

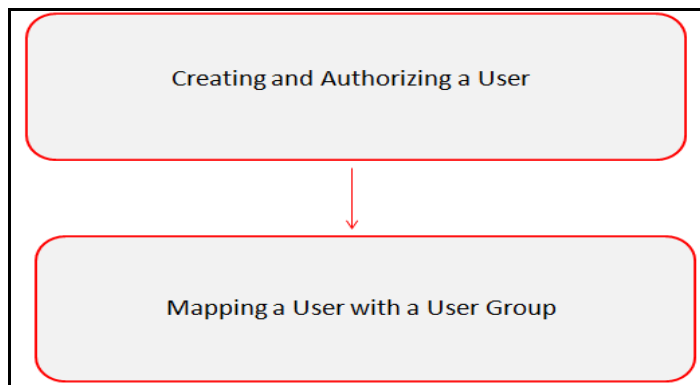


Figure 13. Managing Identity and Authorization Process Flow

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

Table 5. Administration Process Flow

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

Creating and Authorizing a User

The SYSADMN and SYSAUTH roles can be provided to users in the ECM application. User and role associations are established using Security Management System (SMS) and are stored in the Config Schema. User security attribute associations are defined using Security Attribute Administration.

For more information on creating and authorizing a user, see *Chapter 9*, in [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload

To load user configuration data, follow these steps:

1. Navigate to Financial Services Enterprise Case Management, go to Common Tasks.
2. Select **Unified Metadata Manager**. Click **Data Entry Forms and Queries**.
3. Click **Upload**. Select **Config Schema Upload**.
4. Select the CSSMS_ATTRIB_MAST table in the **Select the table** drop-down list.
5. In **Select the File to Upload** field, click **Browse**. In **Choose File to Upload** window, specify the path of the data file (Microsoft Excel 2003/2007) which you want to upload. The CSSMS_ATTRIB_MAST.xlsx will be available in the /STAGE/ExcelUpload/TEMPLATE path inside the ftpshare folder.
6. Click **Select the Sheet** button, the Sheet Selector pop-up window is displayed. Select the required sheet from the drop-down list and click OK. If the excel contains multiple sheets, select the sheet from which data is to be uploaded. Else, by default the first sheet data is selected for upload.
7. In the Upload Type options, select one of the following:
 - **Incremental**: In this type of upload, the data in Excel sheet is inserted / appended to the target database object. The upload operation is successful only when all the data in the selected Excel Sheet is uploaded. In case of an error, the uploaded data will be rolled back.
 - **Complete**: In this type of upload, the data present in the selected database object is overwritten with the data selected Excel sheet. In case of an error, data in the selected database object will be reverted back to its original state.
8. Select Upload. If you have selected Complete upload type, you must need confirm to overwrite data in the confirmation dialog.

Creating or Editing User

To create or edit user, follow these steps:

1. Create or Edit the user for which you must map the Security Attributes.

After loading the User configuration data into `CSSMS_ATTRIB_MAST`, a new section is displayed in User creation screen – User Attributes. This contains the following two fields. The Type of the Field is defined by the Type column in `CSSMS_ATTRIB_MAST.xlsx` file.

- **Case Own Flag:** The Own Case flag is required for taking ownership of the cases. Allowed Values are **Yes** and **No**.
- **Line Organization:** In the OOB `CSSMS_ATTRIB_MAST.xlsx` file, Type defined is 0 (Text box). User can provide it as 1 (Dropdown) if required and re-upload the Sheet using the Config Schema Upload. After updating the fields, click **Save**.

User Maintenance
 User Maintenance > User Definition (add mode)

» **User Maintenance**

User ID *	<input type="text"/>	User Name *	<input type="text"/>
Employee Code	<input type="text"/>	Address	<input type="text"/>
Date of Birth	<input type="text"/>	Designation	<input type="text"/>
Profile Name *	Profile for the Administrator ▼	Start Date *	<input type="text"/>
End Date *	<input type="text"/>	Password *	<input type="text"/>
Database authentication principal	<input type="text"/>		

» **Notification Time**

Start	HH:MM <input type="text"/>	End	HH:MM <input type="text"/>
Email ID	<input type="text"/>	Mobile Number	<input type="text"/>
Pager Number	<input type="text"/>		

» **Enable User**

Enable User	<input type="checkbox"/>	Login on Holidays	<input type="checkbox"/>
Enable Proxy	<input type="checkbox"/>	Proxy User name	<input type="text"/>

» **User Attributes**

Case Own Flag	<input type="text"/>	Line Organization	<input type="text"/>
---------------	----------------------	-------------------	----------------------

Figure 14. User Maintenance

Mapping a User with a User Group

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

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

Table 6. Case Management Roles and User Groups

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

Adding Security Attributes

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

This section covers the following topics:

- [About Security Attributes](#)
- [Loading Security Attributes](#)

About Security Attributes

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

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

Types of Security Attributes

The following are the security attributes:

- [Jurisdiction](#)
- [Business Domain](#)
- [Case Type](#)
- [Organization](#)

Jurisdiction

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

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

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

Business Domain

Business domains are used for data access controls similar to jurisdiction, but have a different objective. The business domain can be used to identify records of different business types such as Private Client 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 business domain **a** or **b**, the user can view the record. You can use this concept to protect special classes of data, such as data about executives of the firm. For example, you can define a business domain as *e: Executives*. You can assign this business domain to the employee, account and customer records that belong to executives. Thus, only specific users of the system have access to these records. If the executive's account is identified in the Private Client business domain, any user who can view Private Client data can view the executive's record. Hence, it is important not to apply many domains to one record.

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

Case Type

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

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

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

Organization

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

Loading Security Attributes

This section covers the following topics:

- [Loading Security Attributes through Excel](#)
- [Loading Security Attributes through SQL Scripts](#)

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

Loading Security Attributes through Excel

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

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

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

Security attributes are loaded through Excel using the following templates:

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

Loading Security Attributes through SQL Scripts

This section covers the following topics:

- [Loading Jurisdictions](#)
- [Loading Business Domains](#)
- [Loading Organizations](#)

Loading Jurisdictions

To load jurisdictions in the database, follow these steps:

1. Add the appropriate record to the KDD_JRSDCN database table as mentioned in [Table 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 name of the jurisdiction such as North or South.
JRSDCN_DESC_TX	Description of the jurisdiction such as Northern US or Southern US.

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

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

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

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

Loading Business Domains

To load a business domain, follow these steps:

1. Add the appropriate user record to the KDD_BUS_DMN database table as mentioned in the [Table 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 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,
MANTAS_DMN_FL) VALUES ('a', 'Compliance Employees', 'COMP', 'N');
```

```
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX, BUS_DMN_DSPLY_NM,  
MANTAS_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 1, which is SYSTEM, if another suitable ID is not available.
COMMENT_TX	Additional remarks added by the user.

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

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

Mapping Security Attributes to Organizations and Users

This section covers the following topics:

- [Introduction](#)
- [Prerequisites for Mapper Maintenance](#)
- [Using Mapper Maintenance](#)

Introduction

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

The following are members in the Mapper:

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

Prerequisites for Mapper Maintenance

The following are the prerequisites for Mapper Maintenance:

- [Loading Security Attributes Data](#)
- [Configuring Function](#)
- [Resaving Metadata](#)
- [Loading User Configuration Data](#)

Loading Security Attributes Data

To load security attribute data, follow these steps:

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

Security Attribute	Table Name
Organization	KDD_ORG
Jurisdiction	KDD_JRSDCN
Business Domain	KDD_BUS_DMN

For more information, see the [Loading Data](#).

Configuring Function

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

1. Provide the Function code in the KDD_INSTALL_PARAM table for param_name='ECM Security Function'. By default, CMAccess function is provided.
2. All the User Groups mapped to that Function are displayed in the Mapper.

For more information, see the [Configuring Administration Tools](#).

Resaving Metadata

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

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

Hierarchy Re-save

1. Login as a ECM Admin user.
2. Navigate to Financial Services Enterprise Case Management and select Common Tasks.
3. Select Utilities and click **Save Metadata**.
4. Select Hierarchy and select the below mentioned Hierarchies. To select them, use >> button and click **Save**.
 - ECM_User Group
 - ECM_Organization
 - ECM_Jurisdiction
 - ECM_Business Domain
 - ECM_Case Type

Derived Entity Re-save

1. Login as a ECM Admin user.
2. Navigate to Financial Services Enterprise Case Management and select Common Tasks.
3. Select Utilities and click **Save Metadata**
4. Select Derived Entity and select the below mentioned Derived Entities. To select them, use >> button and click **Save**.
 - DE_GRPMAST
 - DE_GROUP
 - DE_ROLE
 - DE_ROLE_FUNCTION_MAP
 - Derived Entity on Usergroup Dataset

Loading User Configuration Data

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

Create or Edit the user for which you must map the Security Attributes. For more information, see the [Managing Identity and Authorization](#).

Using Mapper Maintenance

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

1. Login as an ECM Admin user.
2. Navigate to Financial Services Enterprise Case Management and go to Common Tasks.
3. Select Unified Metadata Manager and click Business Metadata Management, and click **Map Maintenance**.
4. Select ECM User Group Security Mapper from the Mapper List. Click Map Maintenance. The User Group Security mapper window is displayed.
5. User Group Security mapper window is displayed. Click **Add**.

The screenshot displays the 'Oracle OFSAAI Map' interface for the 'ECM User Group Security Mapper'. The window title is 'Map - ECM User Group Security Mapper - 1474529346580 - 1'. It features a search section with filters for 'ECM_User Group', 'ECM_Organization', 'ECM_Jurisdiction', 'ECM_Business Domain', and 'ECM_Case Type Subtype'. Below the search filters is a table titled 'Member combinations(0)' with columns: ECM_User Group, Macro, ECM_Organization, Macro, ECM_Jurisdiction, Macro, ECM_Business Domain, Macro, ECM_Case Type Subtype, Macro, and Excluded. The table shows 'No Data Found'. Below this is another search section with the same filters. At the bottom is a table titled 'Mapped members(0)' with columns: ECM_User Group, ECM_Organization, ECM_Jurisdiction, ECM_Business Domain, and ECM_Case Type Subtype. This table also shows 'No Data Found'. A 'Close' button is located at the bottom right of the window.

Figure 15. User Group Security Mapper window

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

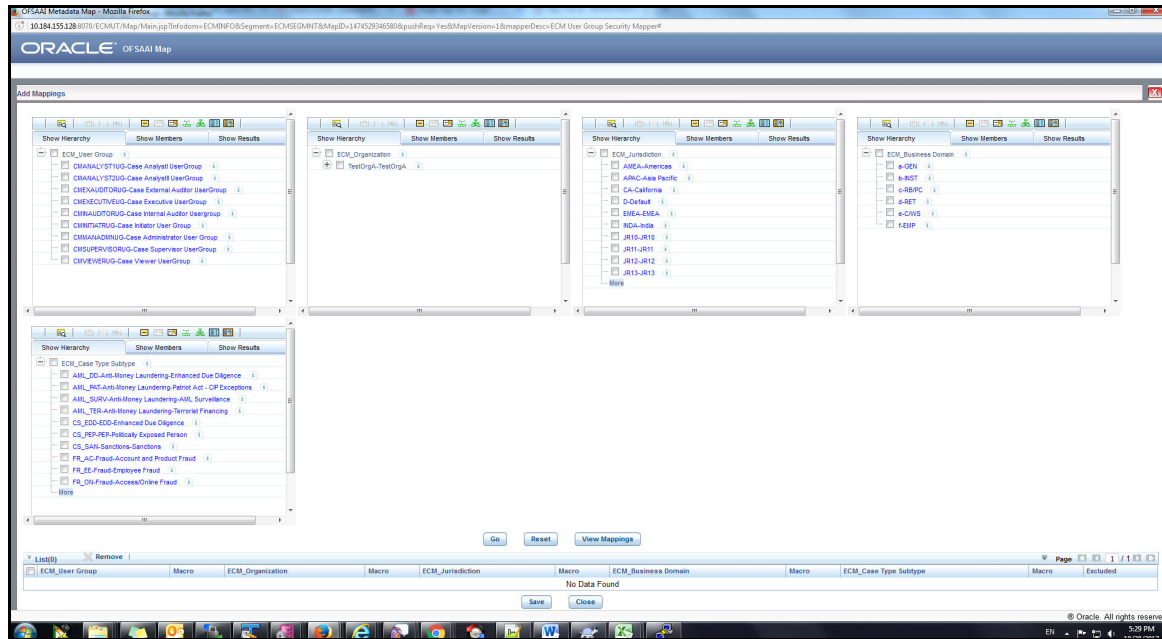


Figure 16. Add Mappings

- Usergroups of the users for the Security Attributes are mapped. Lists all User groups which are mapped to the Function code mentioned in KDD_INSTALL_PARAM.
- Organization: A User or Organization's access to other Organization depends on the selection(s) made for this organization parameter. For example, if a user is mapped to Org1 and Org2, then user can access these two organizations, but other security attributes are also should match.
- Jurisdiction: Mapping of one or more jurisdictions to a usergroup, gives the privilege of accessing cases that belong to the mapped jurisdiction.
- Business Domain: Mapping of one or more business domains to a usergroup gives privilege of accessing cases that belong to the mapped business domains.
- Case Type: Mapping of one or more Case Types to a usergroup gives them the privilege of accessing cases that belong to the mapped Case Type.

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

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

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

Updating Control Access tables from Mapper

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

- [Batch Maintenance](#)

- [Batch Execution](#)
- [Batch Monitor/Checking the Execution Status](#)

Changing ICC Batch Ownership to ECM Admin from SYSADMN user

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

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

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

Syntax:

```
begin
```

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

```
end;
```

OR

```
begin
```

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

Here,

- **fromUser** indicates the user who currently owns the batch
- **toUser** indicated the user to which the ownership has to be transferred
- Infodom is optional parameter, if specified the ownership of batches pertaining to that Infodom will be changed.

For example:

```
begin
```

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

```
end;
```

Batch Maintenance

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

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

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

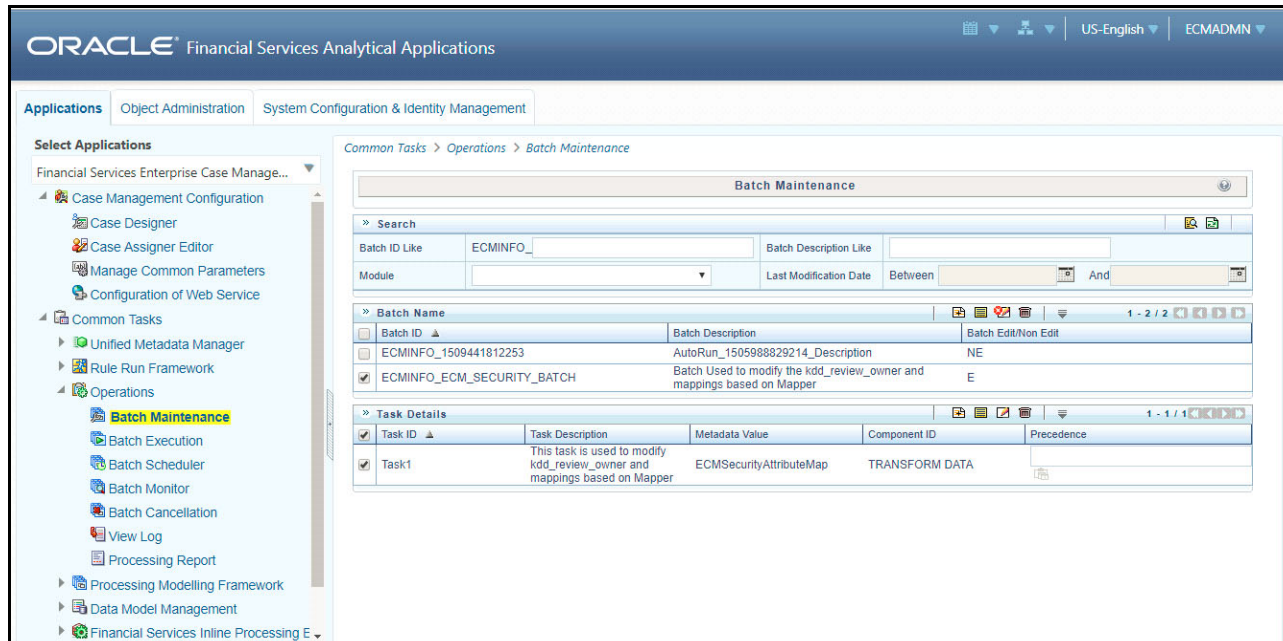


Figure 17. Batch Maintenance

2. Select the <Infodom>_ECM_SECURITY_BATCH and select the Task1. Click **Edit** from the Task Details section.
3. Modify the **Parameter List**. Seeded values are p_create_id.
4. For the Parameter List-Syntax is 'p_create_id','p_user_id'.

- op_create_id: Current Admin User who is going to execute the Batch.
- op_user_id: User(s) for which the Security Attribute Mapping changed through the Security Mapper.

This can be changed in following two ways:

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

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

Batch Execution

The seeded Batches are executed from the Batch Execution operation.

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

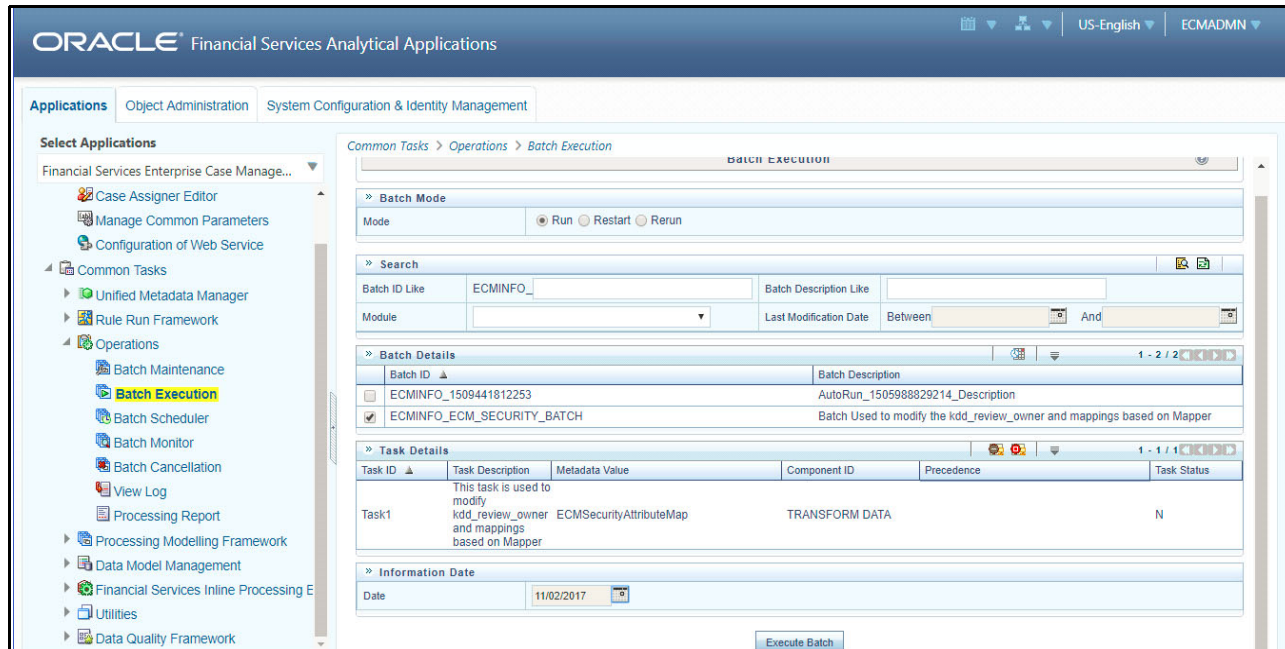


Figure 18. Batch Execution

2. Before executing a Batch, check if the following services are running on the application server:
 - ICCserver
 - Router
 - AM Server
 - Message Server

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

3. The seeded batch (<Infodom>_ECM_SECURITY_BATCH) must be executed for the required MIS Date in this screen.
4. Select <Infodom>_ECM_SECURITY_BATCH and provide the Current Date in the Information Date section.
5. Click **Execute Batch**.

Batch Monitor/Checking the Execution Status

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

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

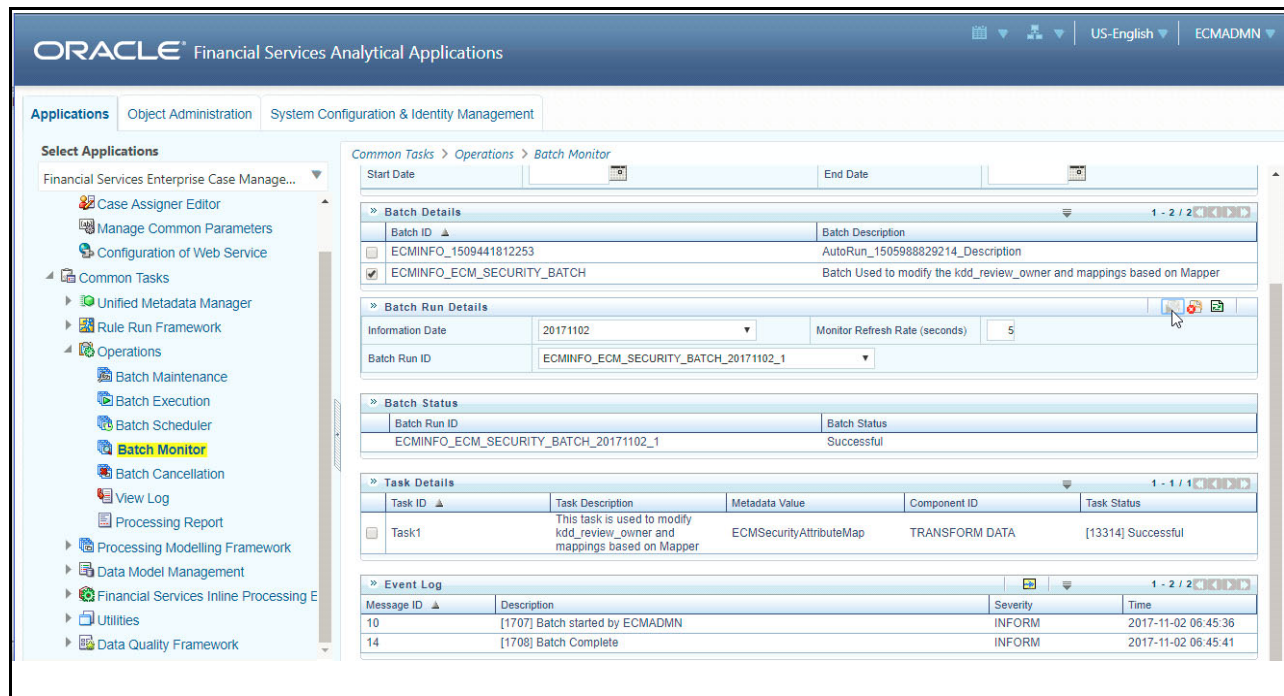


Figure 19. Batch Monitor

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

2. Following are the status messages in Batch Monitor:

- N: Not Started
- O: On Going
- F: Failure
- S: Success

3. The execution log is accessed on the application server from the following directory:

\$FIC_DB_HOME/log/date.

The file name has the batch execution ID. After the Batch is successful, the mappings for the User(s) is reflected in KDD_REVIEW_OWNER and its mapping tables. The Audit is recorded in the respective Audit Tables.

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

Configure the following activities before executing a batch:

- [Start a Batch](#)
- [Correlation](#)
- [Correlation Case Type Mapping](#)
- [Ending a Batch](#)

Start a Batch

Perform the following activities before starting a batch:

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

Table 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 FCC_PROCESSING_GROUP table. For example:
"MAN", "", "ALL", "START", "IND"

For more information, see the [Start Batch Run](#) section.

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

Correlation

Perform the following activities before defining correlation:

- [Initiating Correlation](#)
- [Configuring Correlation Rules](#)
- [Activating or Deactivating the Correlation Rules](#)

Initiating Correlation

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

To initiate the correlation, follow these steps:

1. Navigate to `$FIC_HOME/ficdb/bin`.
2. Execute `initiateCorrelation.sh`. This populates the data in business entity path tables (`FCC_CORR_BUS_ENTITY_PATH` and `FCC_CORRELATION_BUS_ENTITY_CFG`). For more information, see the [Using Business Entity Paths](#) section.

Configuring Correlation Rules

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

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

Table 12. `FCC_CORRELATION_RULE`

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

- `N_CORRELATION_RULE_SKEY` (*required*): This is the correlation rule unique Identification number.
- `V_RULE_NAME` (*required*): Defines the name of correlation rule.
- `N_PATH_PRECEDENCE` (*required*): Number indicating the maximum precedence value that a business entity shared between events must have to be considered a correlation by this rule. The lower the precedence number the stronger the relationship. Events are not considered for the correlation unless the precedence number associated with the business entity-to-event is less than or equal to (\leq) the value defined.
- `V_EVENT_FILTER_OPERATIONS` and `V_EVENT_LINK_OPERATIONS` (*optional*): Defines operations used to further constrain the events to be used for correlation. An operation consists of an event attribute compared to a numerical value, such as *from event* and *to event* which can be correlated if they both have `SCORE_CT >= 0`, represented by `CORR.SCORE_CT >= 0`, or a *from event* and *to event* which can be

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

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

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

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

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

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

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

- `F_EXTEND_FLAG` (*required*): Defines the conditions for extending existing correlations. When a new correlation is discovered, it is possible that it is a superset (with only the triggering event not already included in the existing correlation) of a correlation that is previously identified. `F_EXTEND_FLAG` defines whether this correlation rule can result in extending an existing correlation. If this is set to `FALSE` (do not extend) then a new correlation is created when this condition is identified. If `F_EXTEND_FLAG` is set to `TRUE` then the existing correlation is added to unless it is already promoted to a case that has a status identified in the `V_CASE_STATUS` tags of `NonExtendableCaseStatuses`.
- `F_CORRELATION_REQUIRED_FLAG` (*required*): Defines the conditions for correlation required. You can set this as `Y` or `N`. If this is set to `N`, then every event is self linked and promoted to case. If this is set to `Y`, then multiple events are linked if they have common business entity and promoted to case.
- `F_LOOKBACK_PROCESS_IND` (*required*): Indicates if the date of look back is event processing date or sysdate. If this is set to 1, then processing date is picked. If this is set to 0, then event created date is picked.
- `V_STATUS` (*required*): Defines the status of correlation rule. By default, the correlation rule is *Active*.
 - To deactivate a correlation rule, modify the `V_STATUS` value to `INACT`.
 - To activate a correlation rule, modify the `V_STATUS` value to `ACT`.

Changes made to the metadata are effective immediately and are utilized the next time correlation is run.

Correlation Case Type Mapping

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

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

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

To perform this activity, follow these steps:

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

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

Ending a Batch

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

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

For more information, see the [Ending a Batch Run](#) section.

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

- [About Batch Run](#)
- [Starting a Batch Run](#)
- [Ending a Batch Run](#)
- [Executing a Batch Run](#)

About Batch Run

The ECM application batch run comprises of the following processes:

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

Starting a Batch Run

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

This section explains how to start the batch run.

To start the batch run, follow these steps:

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

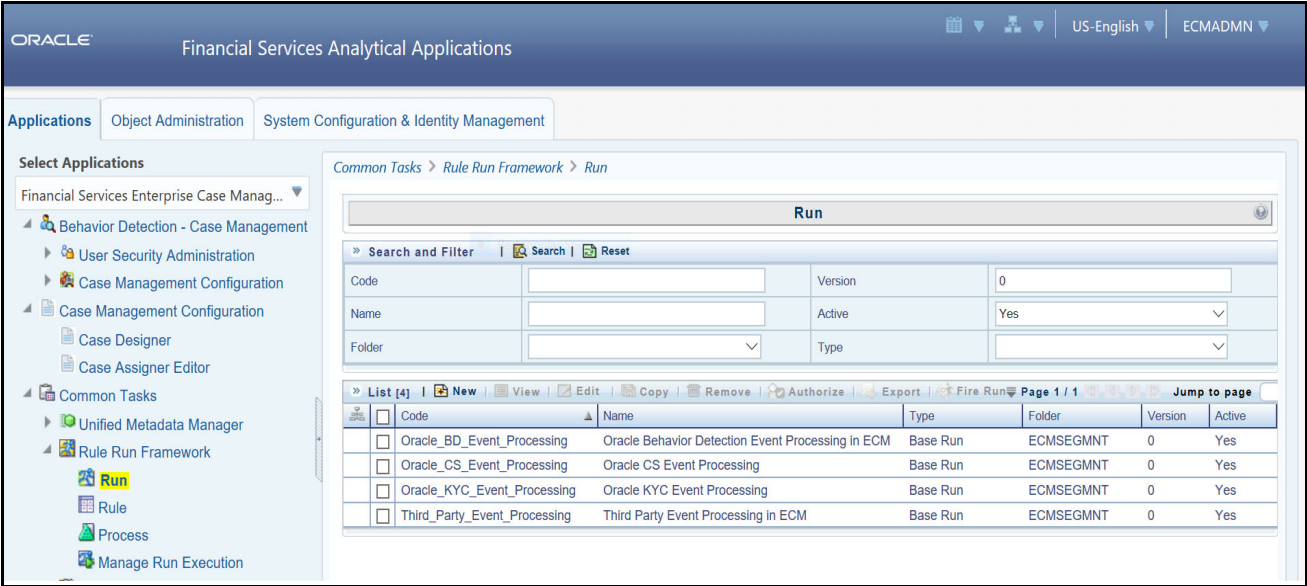


Figure 20. Application List

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

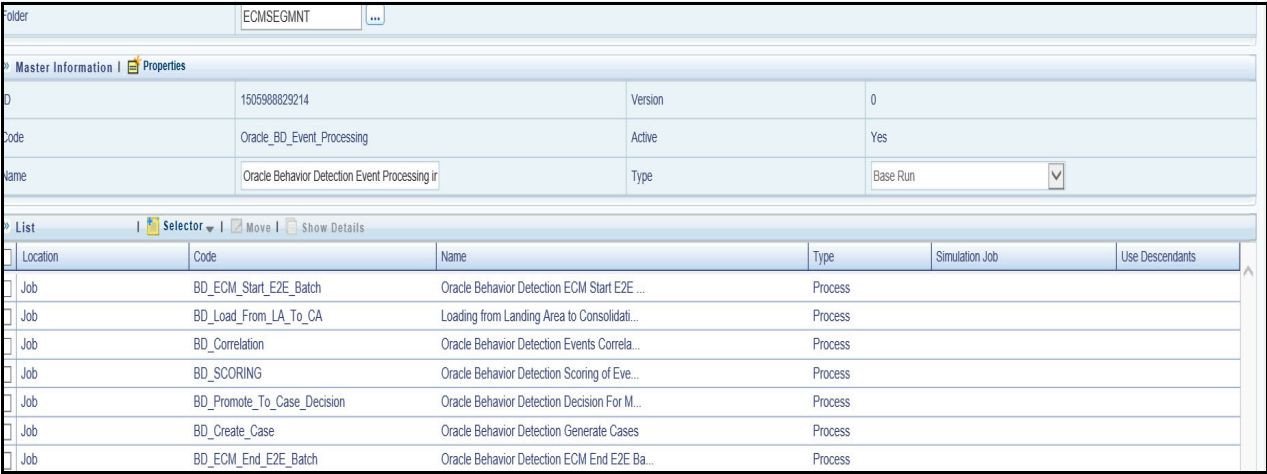


Figure 21. List of Processes

- Select start batch. For example, BD_ECM_Start_E2E_Batch.
- Click **Edit**. The Process Definition page is displayed.
- Click **Component**. The Component Selector window is displayed.
- Click **Parameters** option. The Parameters window is displayed.

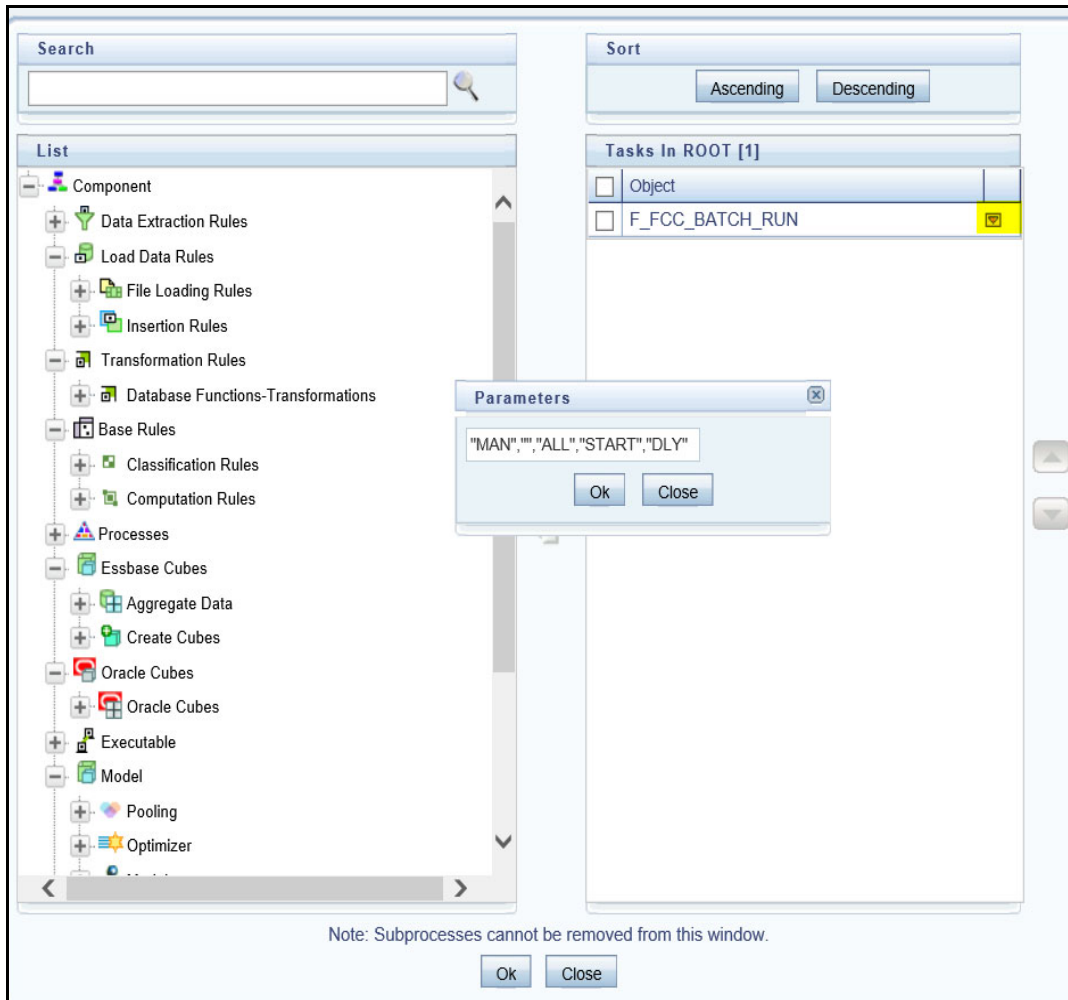


Figure 22. Parameters

The following are default parameters:

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

- **MAN:** is group name. Modify the name of group as mentioned in FCC_PROCESSING_GROUP table. For example, E2E BATCH ALL SOURCE
- **""** Source Batch for Correlation
- **ALL:** is component that can be modified if required
- **START:** is used to start the batch
- **DLY:** is Data Origin

The following is an example of parameter

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

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

Ending a Batch Run

This section explains how to end the batch run.

To end the batch run, follow these steps:

1. Navigate to Process Summary page and search for End Batch, for example BD_ECM_End_E2E.

The screenshot shows a web application interface for managing processes. At the top, there's a breadcrumb trail: 'Common Tasks > Rule Run Framework > Process'. Below this is a header bar labeled 'Process'. The main area contains a search and filter section with fields for 'Code' (containing 'BD_ECM_End_E2E'), 'Version' (containing '0'), 'Name', 'Active' (a dropdown menu set to 'Yes'), and 'Folder'. Below the search section is a toolbar with icons for 'List [1]', 'New', 'View', 'Edit', 'Copy', 'Remove', 'Authorize', 'Export', and 'Trace Definition'. The bottom part of the screenshot shows a table with the following data:

Code	Name	Folder	Version	Active
BD_ECM_End_E2...	Oracle Behavior Detection ECM End E2E Batch	ECMSEGMNT	0	Yes

Figure 23. Application Batch List

2. Click **Edit**. The Process Definition page is displayed.
3. Click **Component**. The Component Selector window is displayed.
4. Click Parameters option. The Parameters window is displayed. Following are default parameters:

The following are default parameters:

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

- Source Batch for Correlation
- **ALL**: is component. Modify the component if required
- **END**: is used to end the batch

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

Executing a Batch Run

This section explains how to execute the batch run.

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

1. Navigate to Enterprise Case Management Application.
2. Go to the Common task section. Select the **Run Rule Framework**.
3. Click **Run**. The Run window is displayed with the available Processes.
4. Select the Application process from the Run definition page list that is to be executed and click **Fire Run**. The Fire Run window is displayed.

The screenshot shows a 'Fire Run' dialog box with the following details:

- Run Definition:**
 - Name: Oracle Behavior Detection Event Processing in ECM
 - Request Type: Single (dropdown)
- Execution Mode:**
 - Batch: Create & Execute (dropdown)
 - MIS Date: 11/01/2017 (calendar icon)
 - Wait: No (dropdown)
- Others:**
 - Parameters: (empty text area)
 - Filters: (empty list area)

Buttons: OK, Close

Figure 24. 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: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● Create ● Create & Execute From these options, select Create & Execute

Table 13. Adding Fire Run Details

Wait	<p>Select Wait. It has the following options:</p> <ul style="list-style-type: none"> ● Yes: This executes the batch after a certain duration. Enter the duration as required. ● No: This executes the batch immediately.
Filters	<p>Enter the filter details.</p> <p>Note: \$MISDATE option can be used to execute the run for that particular day. The format for it to enter in the filter details is:</p> <p><code>to_date(<ACTIVITY_TABLE_NAME>.<ACTIVITY_DT_COL>)=\$MISDATE</code></p> <p>Note: For \$MISDATE option:</p> <ul style="list-style-type: none"> ● For either Date or Timestamp datatypes, to_date is mandatory for the filter. ● Activity Table Name and Activity Column Name should be in capital.

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

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

7. Once the batch is triggered, following processes get executed:
 - a. Start ECM batch, select required process code. For example, BD_ECM_Start_E2E_Batch. For more information on starting the batch, see [Starting a Batch Run](#).
 - b. Load events, evented, and business data to Consolidation area, select required process code. For example, BD_Load_From_LA_To_CA. For more information on using this connector, see [Loading Data](#).
 - c. Perform correlation on loaded events and select required process code. For example, BD_Correlation. For more information on using correlation, see [Configuring Correlation](#).
 - d. Perform scoring on correlated events and select required process code. For example, BD_SCORING. For more information on using scoring, see [Scoring Rules](#).
 - e. Determine to promote correlated events to a case and select required process code. For example, BD_Promote_To_Case_Decision. For more information on using promote to case, see [Promoting to Case](#).
 - f. Create a case event and select required process code. For example, BD_Create_Case.
 - g. End ECM batch and select required process code. For example, BD_ECM_End_E2E_Batch. For more information on running the batch, see [Ending a Batch Run](#).

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

Table 14. Application Run processes

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

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

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

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

About Loading Data

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

Note: ECM does not support Multi-Match alerts.

Types of Connectors

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

- OBD
- OKYC
- OCS
- Third Party

Using Connectors

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

- [Accessing Connector Processes](#)
- [Using OBD Connector Process](#)
- [Loading OCS Data](#)
- [Using KYC Connector Process](#)
- [Loading Third Party Connector Data](#)

Accessing Connector Processes

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

To access connectors, follow these steps:

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

Loading OBD Data

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

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

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

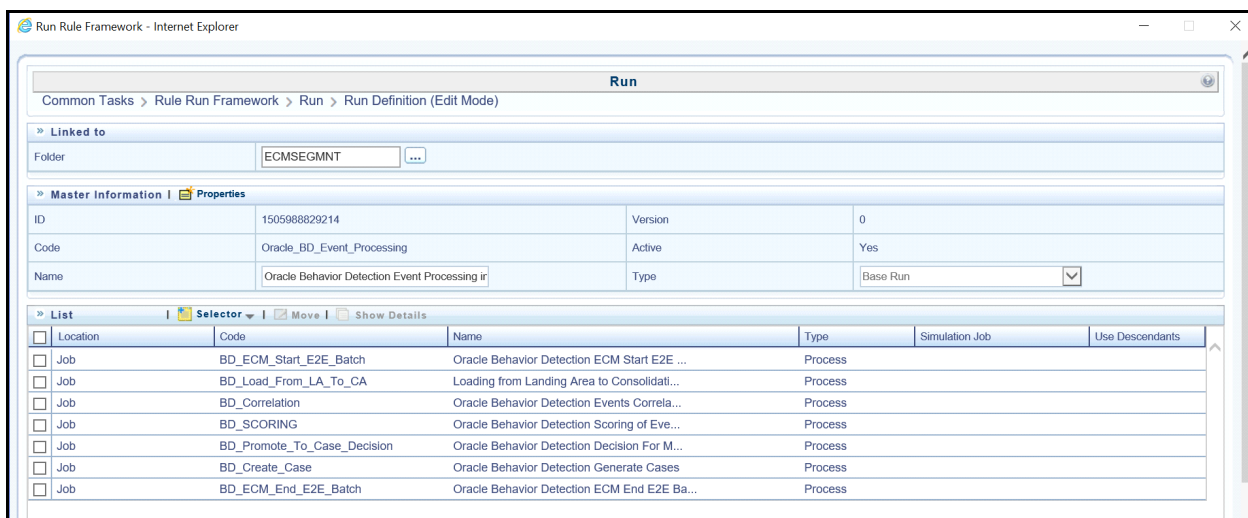


Figure 25. BD Processes

3. Select **BD_Load_From_LA_To_CA** (connector) process from the list. This has the following four sub processes:
 - Loading BD Events
 - Entity Surrogate Key Generation for BD
 - Oracle Behavior Detection Evented Data Load
 - Oracle Behavior Detection Business Data Load

For more information on processes and tasks, see the [Appendix A, List of Processes and Tasks](#).

For more information on Configuring Data Movement from LA to CA, see the [Configuring Data Movement from LA to CA](#).

Loading OCS Data

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

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

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

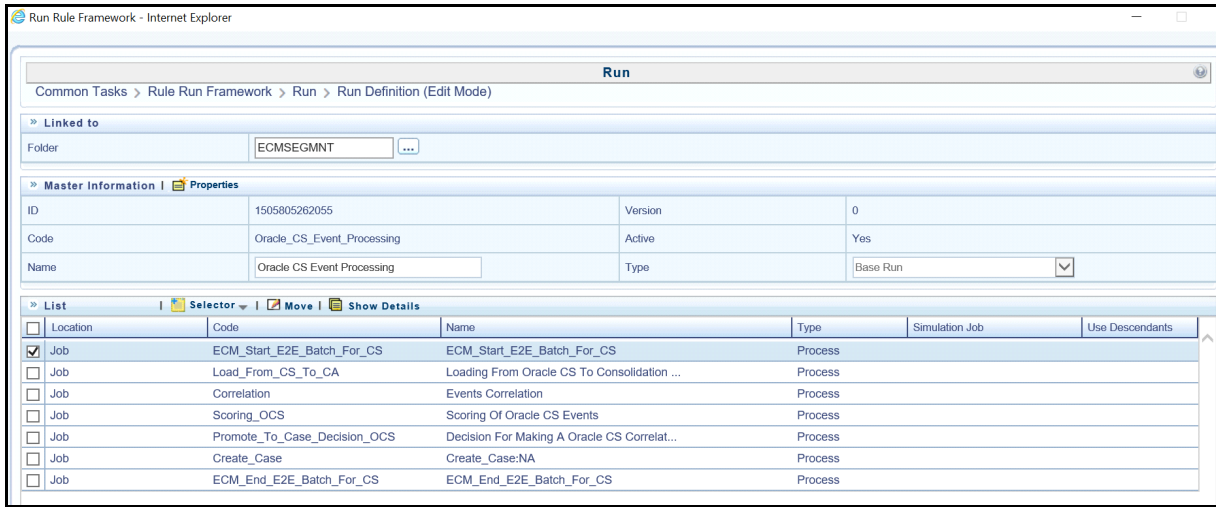


Figure 26. OCS Connector

3. Select **Load_From_CS_To_CA** (connector) process from the list. This has the following four sub processes:
 - Loading Oracle CS Event
 - Entity Surrogate Key Generation For Oracle CS
 - Evented Data Load for CS
 - Business Data Load for CS

For more information on processes and tasks, see the [Appendix A, List of Processes and Tasks](#).

For more information on Configuring Data Movement from LA to CA, see the [Configuring Data Movement from LA to CA](#).

Loading KYC Data

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

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

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

Location	Code	Name	Type	Simulation Job	Use Descendants
<input type="checkbox"/> Job	ECM_Start_E2E_Batch_For_KYC	ECM Start E2E Batch For KYC	Process		
<input type="checkbox"/> Job	Load_From_OKYC_To_CA	Loading from Oracle KYC To Consolidation...	Process		
<input type="checkbox"/> Job	Correlation	Events Correlation	Process		
<input type="checkbox"/> Job	Scoring_OKYC	Scoring Of Oracle KYC Events	Process		
<input type="checkbox"/> Job	Promote_To_Case_Decision_OKYC	Decision For Making A Oracle KYC Correla...	Process		
<input type="checkbox"/> Job	Create_Case	Create_Case:NA	Process		
<input type="checkbox"/> Job	UPD_CaseId_To_OKYC	Updating Case IDs To Oracle KYC	Process		
<input type="checkbox"/> Job	ECM_End_E2E_Batch_For_KYC	ECM End E2E Batch For KYC	Process		

Figure 27. OKYC Connector

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

- Loading Oracle KYC Events to Consolidation area
- Entity Surrogate Key Generation For Oracle KYC (to be executed after Loading Oracle KYC Events sub process.)
- Evented Data Load for KYC
- Business Data Load for KYC

For more information on processes and tasks, see the [Appendix A, List of Processes and Tasks](#).

For more information on Configuring Data Movement from LA to CA, see the [Configuring Data Movement from LA to CA](#)

Loading Third Party Connector Data

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

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

1. Navigate to the Run window.
2. Go to the List section. Select **Third_Party_Event_Processing**. The list of process for Third Party is displayed.

The screenshot shows the 'Data Movement (DM) Utility' interface. At the top, there's a 'Linked to' section with a 'Folder' dropdown set to 'ECMSEGMNT'. Below this is the 'Master Information' tab, which displays the following details:

ID	1505826053869	Version	0
Code	Third_Party_Event_Processing	Active	Yes
Name	Third Party Event Processing in ECM	Type	Base Run

Below the master information is the 'List' tab, which shows a table of jobs. The 'Load_From_LA_To_CA' job is selected.

Location	Code	Name	Type	Simulation Job	Use Descendants
<input type="checkbox"/> Job	ECM_Start_E2E_Batch	ECM Start E2E Batch	Process		
<input type="checkbox"/> Job	Load_From_LA_To_CA	Loading from Landing Area to Consolidati...	Process		
<input type="checkbox"/> Job	Correlation	Events Correlation	Process		
<input type="checkbox"/> Job	Scoring	Scoring Of Events, Entities And Correlat...	Process		
<input type="checkbox"/> Job	Promote_To_Case_Decision	Promote_To_Case_Decision:NA	Process		
<input type="checkbox"/> Job	Create_Case	Create_Case:NA	Process		
<input type="checkbox"/> Job	ECM_End_E2E_Batch	ECM End E2E Batch	Process		

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 the [Appendix A, List of Processes and Tasks](#).

For more information on Configuring Data Movement from LA to CA, see the [Configuring Data Movement from LA to CA](#)

Data Movement (DM) Utility

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

- Data movement across source and target tables residing in two different databases. For example: source table on database1 and target table on database2.
- Data movement across source and target tables residing in two different schema in the same database. For example: source table on schema1.table1 and target table on schema2.table2.
- Data movement across source and target tables residing in the schema in the same database. For example: source table on schema1.table1 and target table on schema1.table2.

The following Data transfer modes are available:

- **DI:** In this mode, the Utility fetches the data from the source table/s based on the metadata available in the FCC_DM_DEFINITION and FCC_DM_MAPPING tables. Data is removed from the target is based its PK/UK. Then the data is moved into the source table.
- **IS:** In this mode, Utility inserts the data from selected table of source to target.
- **MI:** In this mode, Utility performs insert or update operations. If data is not available in the target table, then Insert operation is performed. If data is available in the target table, then Update operation is performed.

DM Metadata Tables

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

The structure of the DM definition table is as follows:

Table 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 Source table. It can contain the join conditions with multiple source tables and conditions associated with it. All source table must be put under curly bracket '{'. For example: {EMP_PHON}
- **V_TARGET**: Name of Target table.
- **V_SRC_FILTER**: Source filter that contains the filter condition for source database.

For example,

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

- **V_TARG_FILTER**: Filter condition in target database.
- **V_TARGET_DATASET**: Contains the join condition with multiple target tables and filter condition associated with it.

For example,

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

The following is the example:

DM_GROUP_ID	DM_ID	DM_CODE	DM_DESCRIPTION	V_SOURCE_DATASET	V_TARGET	V_SRC_FILTER	V_TARGET_FILTER	V_TARGET_DATASET
1	1	BD_EMP_PHON	T2T_FC CM_PROD_EMP_PHON	{EMP_PHON}		EMP_PHON.DATA_DUMP_DT = \$MISDATE AND EMP_PHON.PRCNG_BATCH_NM IN (SELECT FCC_BATCH_DATAORIGIN.V_DATA_ORIGIN FROM FCC_BATCH_DATAORIGIN WHERE FCC_BATCH_DATAORIGIN.N_RUN_KEY = \$RUNSKEY)		INNER JOIN FCC_EMPLOYEE_LOOKUP ON FCC_EMPLOYEE_LOOKUP.EMP_INTRL_ID = [EMP_PHON].EMP_INTRL_ID

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

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

Table 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
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

Column Name	Primary Key	Column Type	Nullable
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 field name if the value is coming from target table.

- V_SRC_DATA_TYPE: Data type of Source field.
- V_FIELD_FORMAT: Data type format of source field.

Example: mm-dd-yyyy

- F_IS_NULL_ALLOWED: Set this flag as yes if is Null allowed.
- V_SQL_EXPRESSION: Type of SQL expression.

For example: Case statement, Sequences and so on. It can contain direct variable from application interface for example, \$MISDATE (MIS date passed from external interface for source filter)

- V_TARGET_ENTITY_NAME: Name of Target table
- V_TARGET_FIELD_NAME: Name of Target field.
- V_TARG_DATA_TYPE: Data type of target field.

The following is the example:

DM_ID	V_ENTITY_NAME	V_FIELD_NAME	V_SRC_DATA_TYPE	V_FIELD_FORMAT	F_IS_NULL_ALLOWED	V_SQL_EXPRESSION	V_TARGET_ENTITY_NAME	V_TARGET_FIELD_NAME	V_SQL_FUNCTION	V_NULL_IF	V_DEFAULT_IF	V_TARGET_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

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_TARGET_DATA_TYPE	V_EXECUTION_SPACE
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_PHONE_TYPE	PHONE_TYPE				VARCHAR2(20)	Src

DM Audit and Error Details Tables

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

Configuring Data Movement from LA to CA

This section covers the following topics:

- [About Data Movement](#)
- [Sample Processes](#)
- [Using Precedence](#)
- [Designing Processes](#)

About Data Movement

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

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

Sample Processes

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

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

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

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

Table 17. Sample Processes

Process	Description
Process1	This process is designed using the following sub-processes (OBD to CA Account): <ul style="list-style-type: none"> ● Oracle Behavior Detection to CA Account, ● Oracle Behavior Detection to CA Account Address, ● Oracle Behavior Detection to CA Account Balance Position Summery, ● Oracle Behavior Detection to CA Email Address, and so on
Process2	This process is designed using the following sub-processes (OBD to CA Customer): <ul style="list-style-type: none"> ● 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): <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● Oracle Behavior Detection to CA account, ● Oracle Behavior Detection to CA Employee, ● Oracle Behavior Detection to CA Customers, and so on
Process5	This process is designed using the following sub-processes: <ul style="list-style-type: none"> ● Oracle Behavior Detection to CA Account Address ● Oracle Behavior Detection to CA Account Balance Position Summery ● Oracle Behavior Detection to CA Account Email Address, and so on
Process6	This process is designed using the following sub-processes: <ul style="list-style-type: none"> ● 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: <ul style="list-style-type: none"> ● Oracle Behavior Detection to CA Employee Address, ● Oracle Behavior Detection to CA Employee Email Address, ● Oracle Behavior Detection to CA Employee Phone, ● Oracle Behavior Detection to CA Employee to Account, and so on
Process8 & 9	These processes are designed using all sub-processes.

Note:

- Process1, 2, and 3 are designed based on similar entity bucketed into to one process.
- Process4, 5, 6, and 7 are designed based on the distribution of volume of data. For example, if Process4 has huge volume of data compare to Process5, 6, and 7. You can design the process (business data movement) in such way that the Process4 runs in parallel with Process5, internally, Process5, 6, and 7 can run in sequence.

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

Using Precedence

Follow the sequence of precedence while moving the data.

1. Event lookup should be populated
2. Event related tables should be populated and the sub-processes can run in parallel.
3. Surrogate key should be populated for all entities (lookup table, for example, account lookup, customer lookup). The sub-processes can run in parallel.
4. Evented data movement processes and business data movement processes can run in parallel.

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

Designing Processes

You can design processes using sub-processes. This section is explained using Oracle Behavior Detection processes and sub- processes as an example.

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

Oracle Behavior Detection Sub-Processes					
Sub Process (SP)	Description	Sub Process (SP)	Description	Sub Process (SP)	Description
SP1	Oracle Behavior Detection to CA Account	SP5	Oracle Behavior Detection to CA Customers	SP9	Oracle Behavior Detection to CA Employee
SP2	Oracle Behavior Detection to CA Account Address	SP6	Oracle Behavior Detection to CA Customers Account	SP10	Oracle Behavior Detection to CA Employee Address
SP3	Oracle Behavior Detection to CA Account Balance Position Summary	SP7	Oracle Behavior Detection to CA Customers Address	SP11	Oracle Behavior Detection to CA Employee Email Address
SP4	Oracle Behavior Detection to CA Account Email Address	SP8	Oracle Behavior Detection to CA Customers 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).

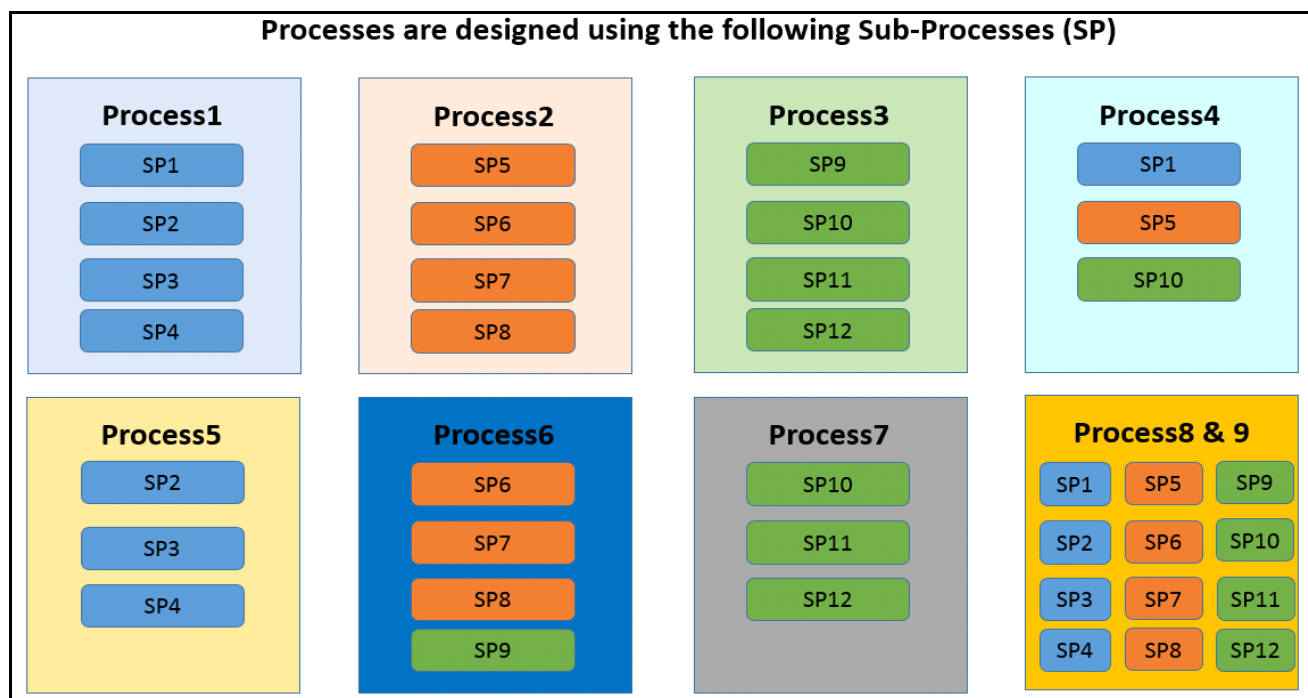


Figure 30. Oracle Behavior Detection Sub - processes

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

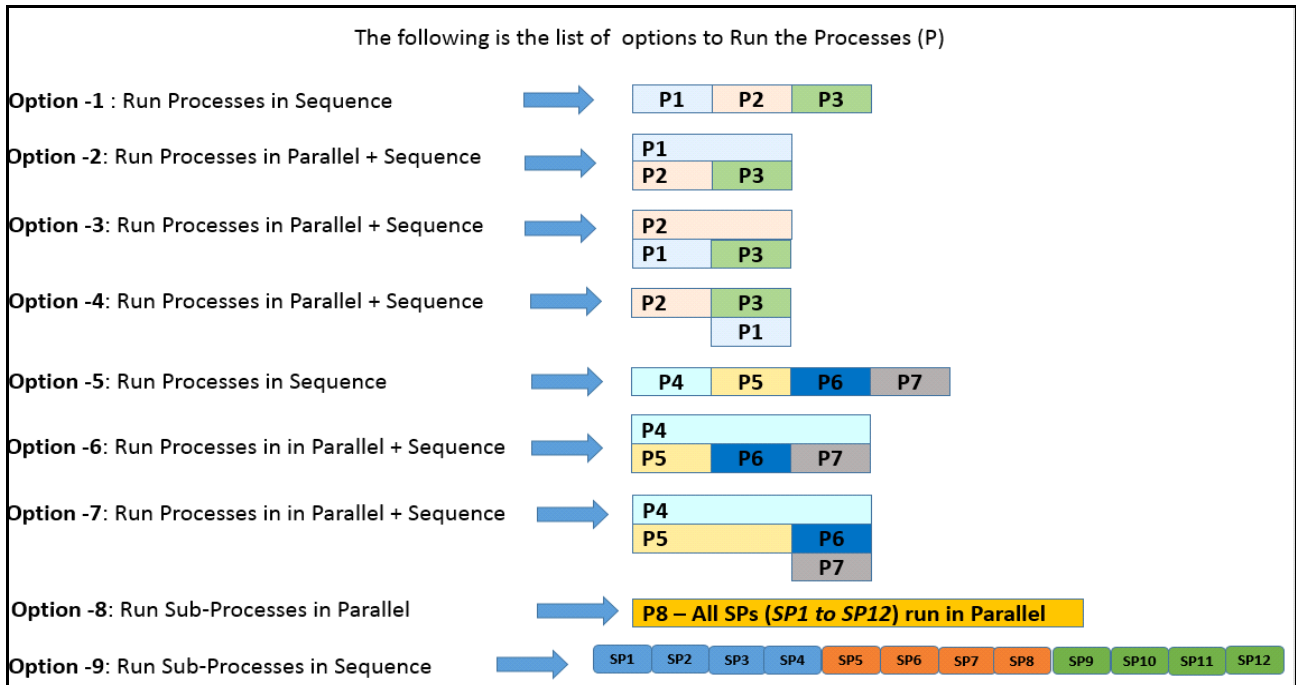


Figure 31. Options- processes

The following table provides the complete description of each options.

Table 18. Options

Option	Description
1	<p>P1, P2, and P3 processes are configured in sequence.</p> <ul style="list-style-type: none"> ● 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	<p>P1 and P2 will start in parallel and P3 will start only after P2 is completed, irrespective of P1 is completed or not.</p> <ul style="list-style-type: none"> ● 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	<p>P2 and P1 will start in parallel and P3 will start only after P1 is completed, irrespective of P2 is completed or not.</p> <ul style="list-style-type: none"> ● 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	<p>Only after completion of P2, P3 and P1 will start in parallel.</p> <ul style="list-style-type: none"> ● In P2, sub processes - SP5, SP6, SP7, and SP8 run in parallel. ● P3 - SP9, SP10, SP11, and SP12, and P1 - SP1, SP2, SP3, and SP4 sub process will run in parallel only after completion of all sub processes of P2.

Table 18. Options

5	<p>P4, P5, P6, and P7 processes are configured in sequence. P4 - SP1, SP5, and SP10 will run in parallel.</p> <ul style="list-style-type: none">● 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	<p>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.</p> <ul style="list-style-type: none">● 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	<p>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.</p> <ul style="list-style-type: none">● 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	<p>Once P8 starts, all sub processes from SP1 to SP12 will run in parallel.</p>
9	<p>All sub processes will run in sequence from SP1 to SP12.</p>

Note:

- Same sub processes should not be part of two processes. For example, you should add P1 and P4 in the same run as they have similar sub process (SP1).
- Above options are used as samples, you can configure your own options based on the requirement.

To design the above process, see the [OFS AAI User Guide](#).

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

- [About Correlation](#)
- [Using Business Entity Paths](#)
- [Executing Correlation Rules](#)
- [Sample Correlation Rules](#)

About Correlation

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

Using Business Entity Paths

Following two tables are used for configuring business entity paths:

- [Correlation Business Path](#)
- [Correlation Business Entity Configuration](#)

Correlation Business Path

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

Table 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
ALERT_FOCUS_ID		NUMBER(10)	Yes
V_ENTITY_TYPE		VARCHAR2(50)	Yes

Table 19. FCC_CORR_BUS_ENTITY_PATH (Metadata Table) (Continued)

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

To correlate events to business entities, follow these steps:

1. Define paths using above table to perform the Event Correlation algorithm.
2. Define whether the origin of the path should be the focus of an event or a matched record, by populating either.
3. Establish either populating the ALERT_FOCUS_ID column (indicating that the origin should be the focus of the event), or the V_QUERY_DEFINITION_NAME column (indicating that the origin should be a matched record of the event).
4. The destination of the path (the business entity you are trying to correlate to by executing this path) is defined by the N_BUSINESS_ENTITY_ID column.

Correlation Business Entity Configuration

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

Table 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 Business Entity path, follow these steps:

1. Select to apply the path identified by the N_BUS_ENTITY_PATH_CFG_SKEY in this table for alerts of a certain scenario or scenario group.
2. Populate the N_SCENARIO_MASTER_SKEY or the V_SCENARIO_CLASS_CD column to establish respectively.

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

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

Executing Correlation Rules

You can execute the correlation using two methods:

- Using Run Rule Framework
- Performing Jobs

Using Run Rule Framework

You can run a correlation using the Run Rule Framework. For more information, refer to [Performing Batch Run](#) section.

Performing Jobs

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

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

1. Navigate to `$FIC_HOME/ficdb/bin/ficdb/bin`.
2. Execute the following script:

```
./correlation.sh ECMINFO_1509116374374_20091226_1 a b 20091226 c  
ECMINFO_1509116374374_20091226_1 is V_BATCH_RUN_ID from FCC_BATCH_RUN  
D_MIS_DATE is date from FCC_BATCH_RUN
```

Sample Correlation Rules

OFS ECM delivers the following four sample correlation rules:

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

scenarios where the events share a common correlated business entity. Specified scenarios are those scenarios which identify behaviors that, in isolation or when considered as a whole, can be indicative of identity theft.

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.

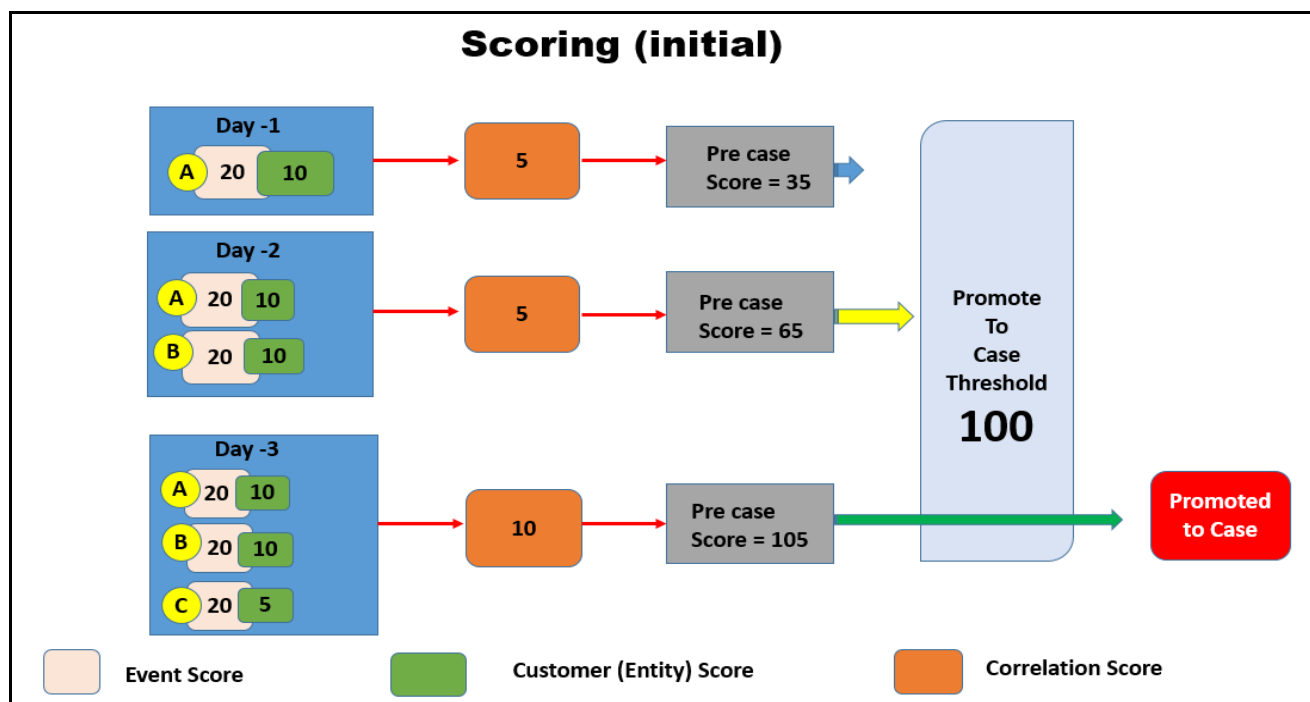


Figure 32. Initial Scoring

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		10	5	65	100	No
Day - 3	20	20	20	10	10	105	100	Yes

Day - 1

- A newly generated event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).
- The pre case score is 35. It is the sum of event + customer + correlation = pre case score. That is, $20 + 10 + 5 = 35$.
- As it could not cross the threshold, hence, it remained as a pre case.

Day - 2

- Another event (event B) is generated, along with event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).
- The pre case score is 65. It is the sum of event A + event B + customer + correlation = pre case score. That is, $20 + 20 + 10 + 5 = 65$.
- As it could not cross the threshold, hence, it remained as a pre case.

Day - 3

- Another event (event C) is generated along with event (event B), event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).
- The pre case score is 105. It is the sum of event A + event B + event C + customer + correlation = pre case score. That is, $20 + 20 + 20 + 10 + 10 = 105$.
- A pre case is promoted to case.

Adjustment Scoring

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

The following figure depicts the adjustment scoring process.

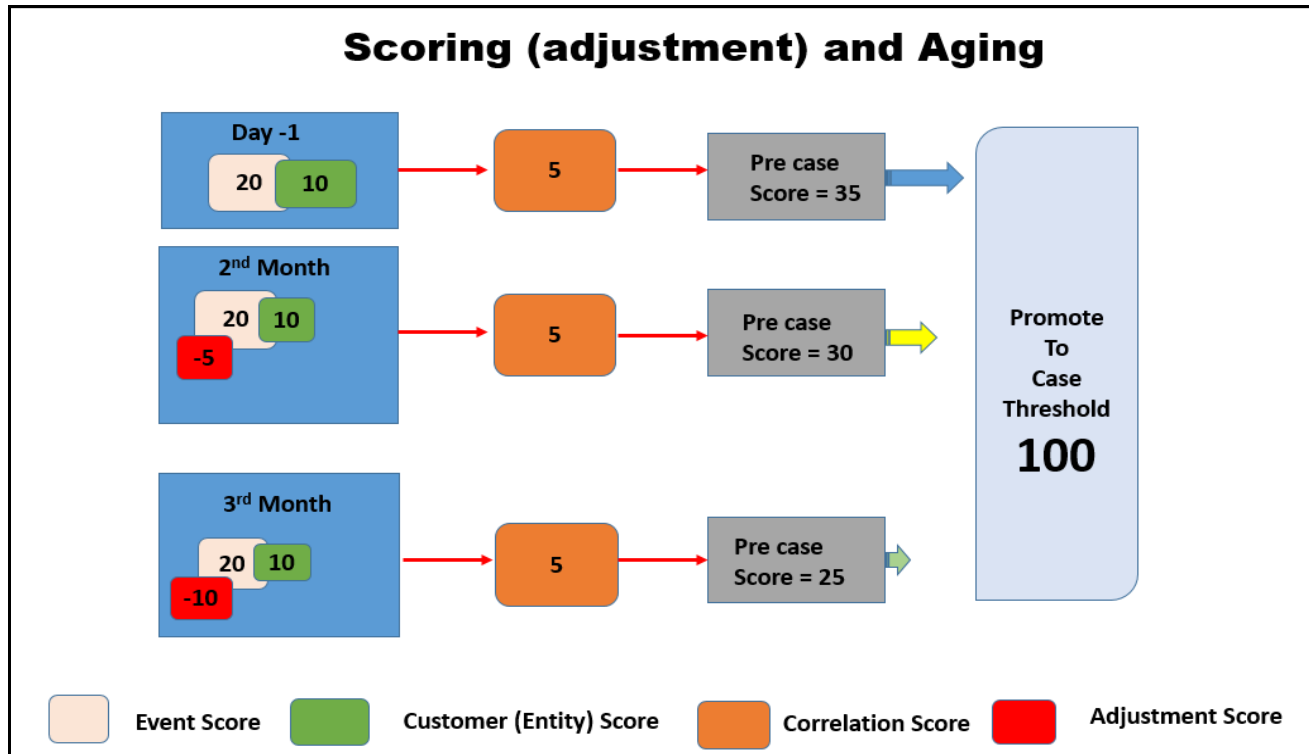


Figure 33. Adjustment Scoring

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
2 nd Month	20	-5	10	5	30	100	No
3 rd Month	20	-10	10	5	25	100	No

Days - 1

- A newly generated event (A), associated entity (customer), and correlation are scored. A case to get promoted, the pre case should cross the threshold score (100).
- The pre case score is 35. It is the sum of event + customer + correlation = pre case score. That is, 20 + 10 + 5 = 35.
- As it could not cross the threshold, hence, it remained as a pre case.

2nd Month

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

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

3rd Month

- If the event (A), associated entity (customer), and correlation are not promoted, an adjustment score is applied further. That is, event score is reduced (-10).
- The pre case score is 30. It is the sum of event + customer + correlation - event adjustment score = pre case score. That is, $20 + 10 + 5 - 10 = 25$.

Types of Scoring

The following is the list scoring types:

- [Event Scoring](#)
- [Entity Scoring](#)
- [Correlation Scoring](#)
- [Pre case Scoring](#)

Event Scoring

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

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

Entity Scoring

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

Correlation Scoring

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

Pre case Scoring

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

Configuring Scoring Rules

The following seeded scoring rules are used for scoring:

- Aging Event Scoring
- Correlation Scoring
- Customer Scoring
- Initial Event Scoring

For more information configuring scores, see the [Inline Processing Engine User Guide](#).

Configuring AML Event Initial Scoring

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

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

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

Common Tasks > Rule Run Framework > Process

Process				
» Search and Filter Search Reset				
Code	Name	Folder	Version	Active
BD_ACCOUNT_G...	Oracle Behavior Detection to CA Account Group Lookup	ECMSEGMNT	0	Yes
BD_ACCOUNT_G...	BD_New	ECMSEGMNT	0	Yes
BD_ACCOUNT_L...	Oracle Behavior Detection to CA Account Lookup	ECMSEGMNT	0	Yes
BD_ACCT	Oracle Behavior Detection to CA Account	ECMSEGMNT	0	Yes
BD_ACCT_ACCT...	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_BAL_P...	Oracle Behavior Detection to CA Account Balance Position Summary	ECMSEGMNT	0	Yes
BD_ACCT_BAL_P...	Oracle Behavior Detection to CA Evented Account Balance Position...	ECMSEGMNT	0	Yes
BD_ACCT_EMAIL...	Oracle Behavior Detection to CA Account Email Address	ECMSEGMNT	0	Yes
BD_ACCT_EVENT	Oracle Behavior Detection to CA Evented Account	ECMSEGMNT	0	Yes
BD_ACCT_GRP	Oracle Behavior Detection to CA Account Group	ECMSEGMNT	0	Yes
BD_ACCT_GRP E...	Oracle Behavior Detection to CA Evented Account Group	ECMSEGMNT	0	Yes

Figure 34. Process Summary Window

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

Common Tasks > Rule Run Framework > Process

Process

> Search and Filter | Search | Reset

Code	BD_Event_Scoring	Version	0
Name		Active	Yes
Folder			

> List [1] | New | View | Edit | Copy | Remove | Authorize | Export | Trace Definition | Page 1 / 1 | Jump to page

<input checked="" type="checkbox"/>	Code	Name	Folder	Version	Active
<input checked="" type="checkbox"/>	BD_Event_Scoring	Oracle Behavior Detection Event Scoring	ECMSEGMNT	0	Yes

Figure 35. BD_Event_Scoring

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

Common Tasks > Rule Run Framework > Process > Process Definition(Edit Mode)

Process

> Linked to

Folder: ECMSEGMNT

> Master Information | Properties

ID	1510036290419	Version	0
Code	BD_Event_Scoring	Active	Yes
Name	Oracle Behavior Detection Event Scoring	Type	Process Tree
Executable	<input type="checkbox"/>		

> Subprocess | Component | Precedence | Move | Remove | Show Details | Merge Rules | Edit Subprocess

Process	Object	Precedence	Type	Parameter	Executable
-FCC_EVENTS	<input type="checkbox"/> FCC_EVENTS		Activity Data		
-t2t_FCC_EVENT_SCORE	<input type="checkbox"/> t2t_FCC_EVENT_SCORE	FCC_EVENTS	Entity Load		
-FCC_EVENTS_SCORE_UPD	<input type="checkbox"/> FCC_EVENTS_SCORE_UPD	FCC_EVENTS, t2t_FCC_EVENT_SCORE	Data Transformation		

Figure 36. List of Tasks

- Click **Components**.

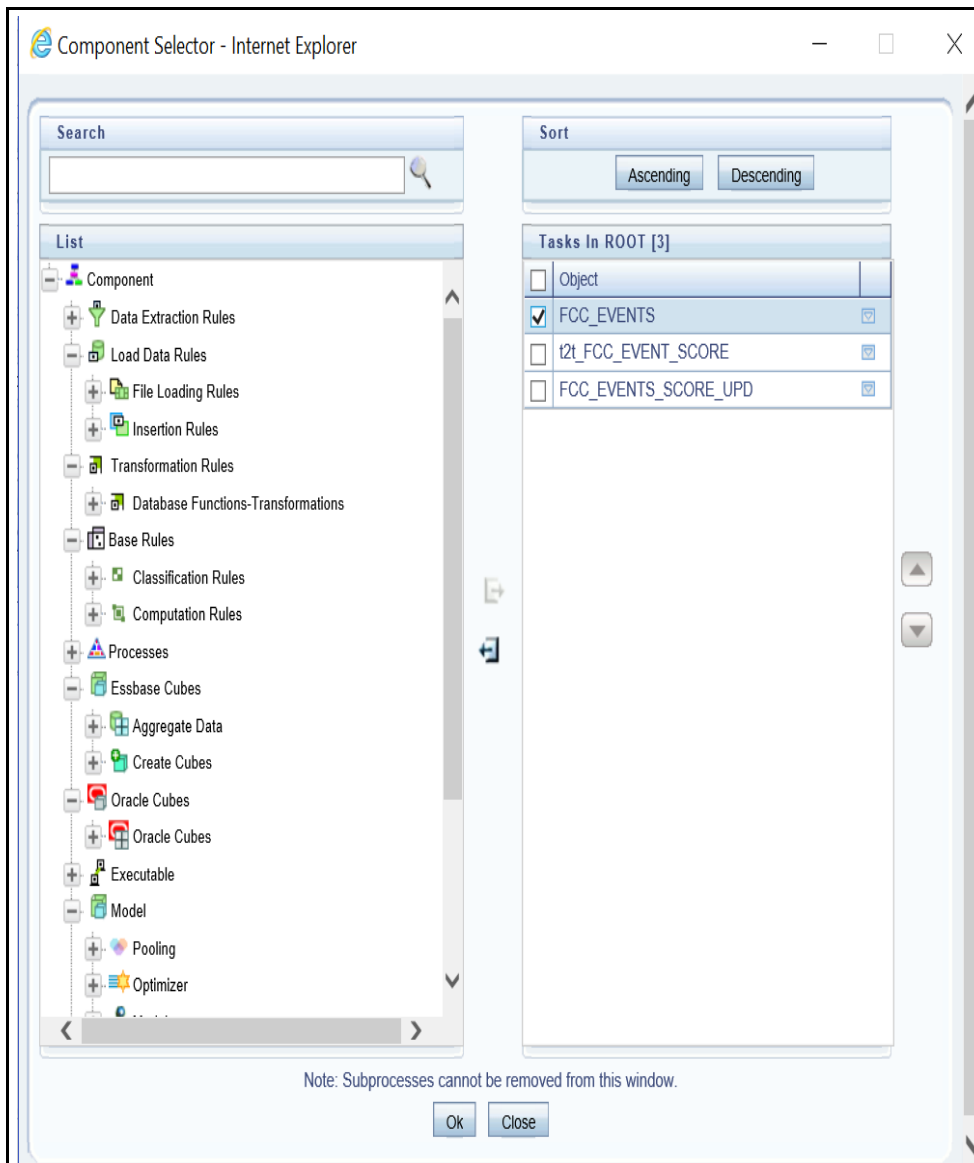


Figure 37. Components

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

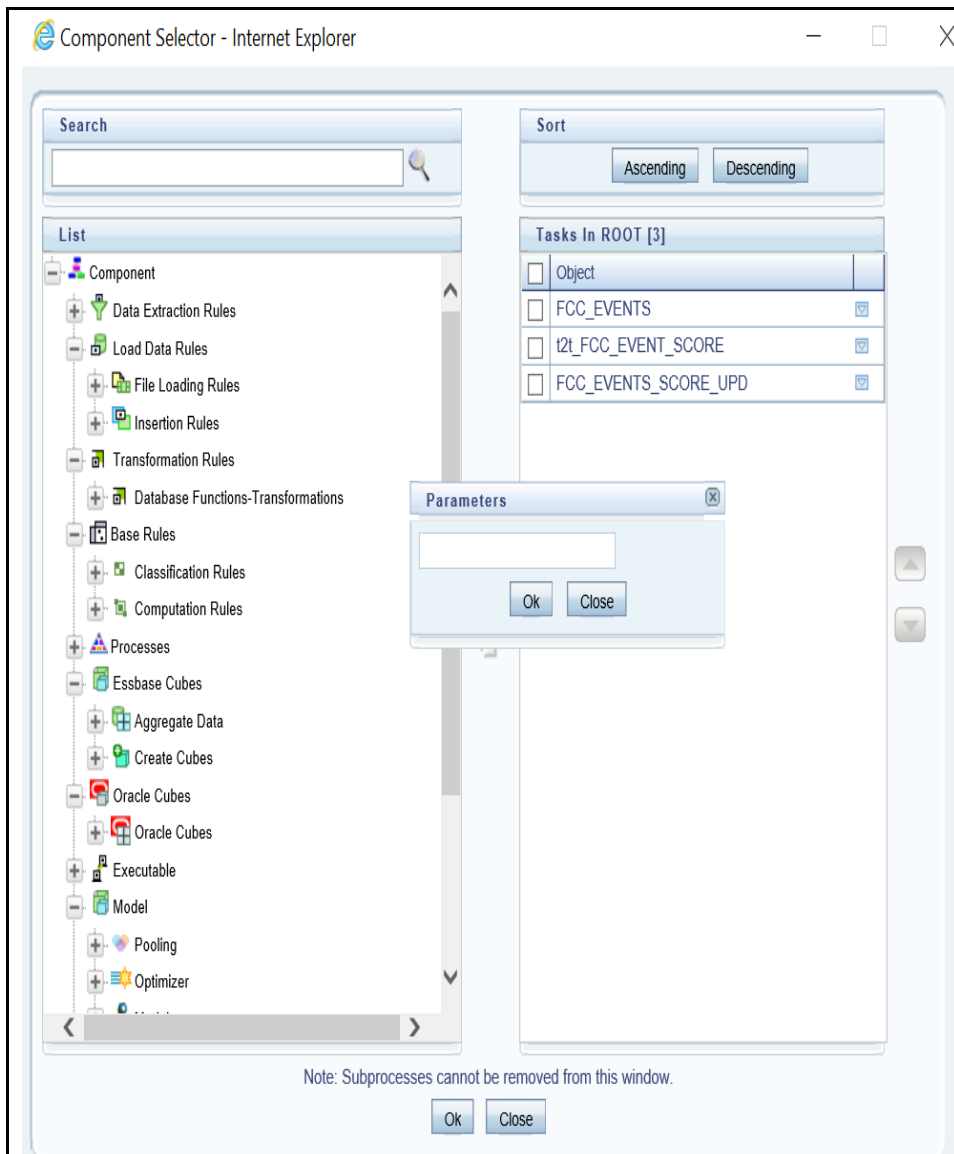


Figure 38. Parameters

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

Common Tasks > Rule Run Framework > Process

Process

» Search and Filter

Search

Reset

Code	<div>BD_Entity_Surrogate_Key_Gen</div>	Version	<div>0</div>
Name	<div></div>	Active	<div>Yes</div> <div>▼</div>
Folder	<div></div> <div>▼</div>		

» List [1]

New

View

Edit

Copy

Remove

Authorize

Export

Trace Definition

Page 1 / 1

Jump to page

<div><div></div><div>✓</div></div>	Code	Name	Folder	Version	Active
<div><div></div><div>✓</div></div>	BD_Entity_Surrogat...	Entity Surrogate Key Generation for BD	ECMSEGMNT	0	Yes

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

Process

Common Tasks > Rule Run Framework > Process > Process Definition(Edit Mode)

» Linked to

Folder

» Master Information | Properties

ID	1510036511417	Version	0
Code	BD_Entity_Surrogate_Key_Gen	Active	Yes
Name	Entity Surrogate Key Generation for BD	Type	Process Tree
Executable	<input type="checkbox"/>		

» Subprocess | Component | Precedence

Move | Remove | Show Details | Merge Rules | Edit Subprocess

Process

- Oracle Behavior Detection to CA Account Lookup
- Oracle Behavior Detection to CA Customers Lookup
- Oracle Behavior Detection to CA Employee Lookup
- Oracle Behavior Detection to CA Account Group Lookup
- Oracle Behavior Detection to CA Derived Address Lookup
- Oracle Behavior Detection to CA External Entity Lookup
- Oracle Behavior Detection to CA Institution Lookup
- Oracle Behavior Detection to CA Investment Advisor Lookup
- Oracle Behavior Detection to CA Loan Lookup
- Oracle Behavior Detection to CA Peer Group Lookup
- Oracle Behavior Detection to CA Market Center Lookup
- Oracle Behavior Detection to CA Event Entity Map Account
- Oracle Behavior Detection to CA Event Entity Map Customer
- Oracle Behavior Detection to CA Event Entity Map Employee

<input type="checkbox"/> Object	Precedence	Type	Parameter	Executable
<input type="checkbox"/> Oracle Behavior Detection to CA Account Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Customers Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Employee Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Account Group Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Derived Address Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA External Entity Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Institution Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Investment Advisor Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Loan Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Peer Group Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Market Center Lookup		Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Event Entity Map Account	Oracle Behavior Detection to CA Account Lookup	Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Event Entity Map Customer	Oracle Behavior Detection to CA Customers Lookup	Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Event Entity Map Employee	Oracle Behavior Detection to CA Employee Lookup	Process		
<input type="checkbox"/> Oracle Behavior Detection to CA Event Entity Map Account Group	Oracle Behavior Detection to CA Account Group Lookup	Process		

Save

Close

Figure 39. List of Tasks

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

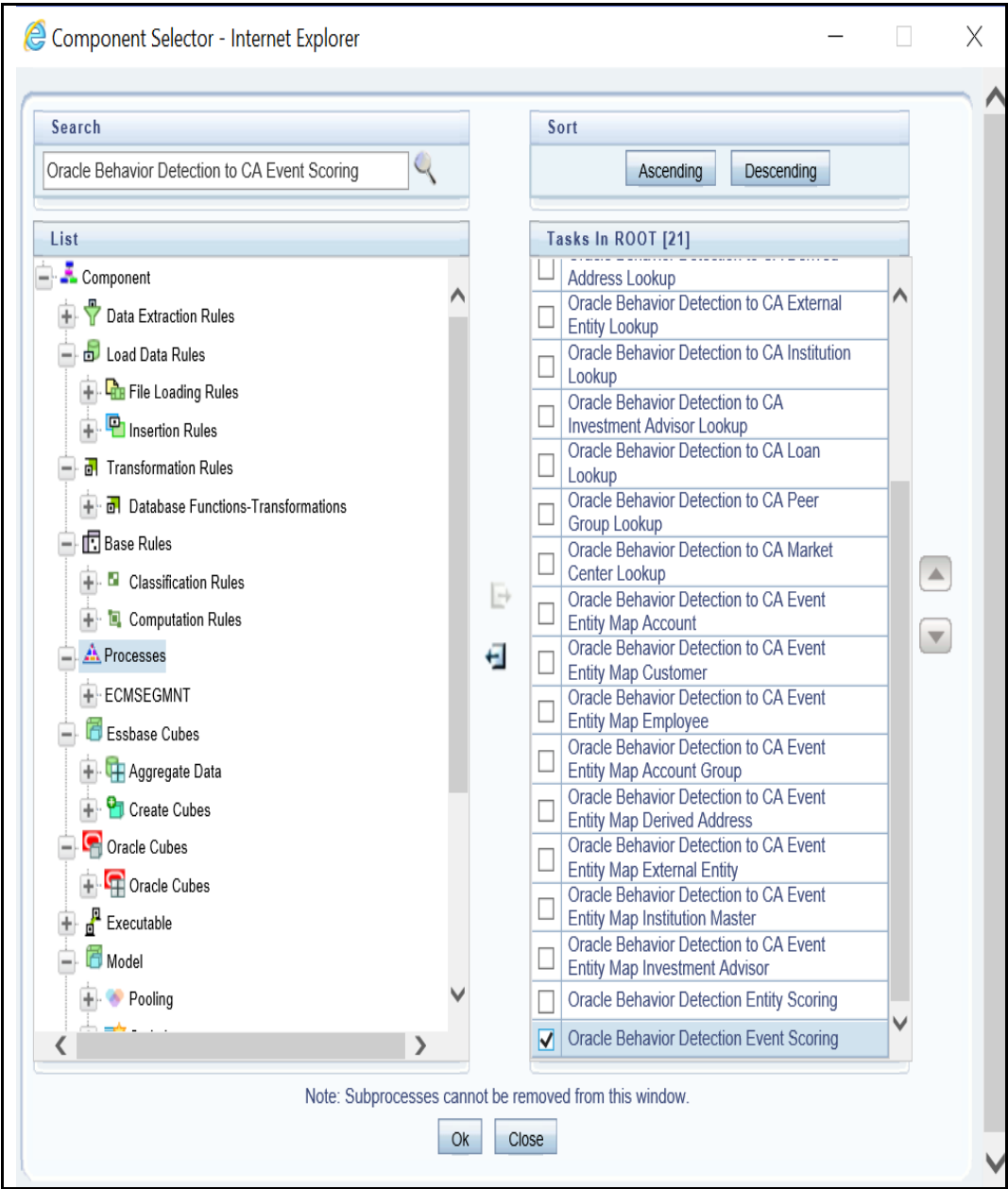


Figure 40. Deselecting of Oracle Behavior Detection to CA Event Scoring Process

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

Total Transaction Amount and Risk Score

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

- When event has total transaction amount \geq <Configurable amount> and risk score \geq <configurable risk score>, give X score to event. Risk scores for amounts can be segregated into 3 buckets. For dollar amounts transactions between 50K and 100K should be given score of 20, 100K to 500K should be given as 30 and anything above 500K should be 50.
- Correlation is created for 2 events A and B by an ML and TF. Transaction amounts between 0 and 50000.99 get 10 points; Trxn amounts between 50001 and 100000 get 20 points; Trxn amounts > 100000 get 30 points. Pre-case score should be calculated as below:
 - Event A – (Total amount of transactions - \$ 80K) - 20
 - Event B – (Total transaction amount - \$ 300K) - 30
 - Total pre-case score is 50 (A(20) + B(30) = 50)

Aging

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

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

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

- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 3 months reduce the event score by 3
- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 6 months reduce the event score by another 3
- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 9 months reduce the event score by another 3
- Scenario Rapid Movement of Funds All Activity (all focal types) - When an event age reaches 12 reduce the event score to equal 0
- Drop and archive any event of correlation age more than year.

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

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

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

- On 1st April, event A age is now 3 months. Event A score will be reduced by 3 points to 7 and total pre-case score is now 17. $A(7) + B(10) = 17$
- On 1st May, event B age is now 3 months. Event B score will be reduced by 3 points to 7 and total pre-case score is now 14. $A(7) + B(7) = 14$
- On 1st July, event A age is now 6 months. Event A score will be reduced by 3 points to 4 and now total pre-case score will be 11. $A(4) + B(7) = 11$
- On 1st Aug, event B age is now 6 months. Event B score will be reduced by 3 points to 4 and now total pre-case score will be 8. $A(4) + B(4) = 8$.
- On 1st Oct, event A age is now 9 months. Event A score will be reduced by 3 points to 1 and now total pre-case score will be 5. $A(1) + B(4) = 5$
- On 1st Nov, event B age is now 9 months. Event B score will be reduced by 3 points to 1 and now total pre-case score will be 2. $A(1) + B(1) = 2$.
- On 2nd Jan 2017 event A age is now 12 months. Score will be dropped to 0. And Event A will be closed and completely dropped from correlation. Event B is only event in correlation and total pre-case score will be now 1.
- On 2nd Feb 2017 event B age is now 12 months. Score will be dropped to 0. And Event B will be closed and completely dropped from correlation.

Entity

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

- [Watch List Screening](#)
- [Effective Risk](#)

Watch List Screening

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

For example,

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

Pre-case score = $A(10) + B(10) + C(10) + \text{Entity C (60)} = 90$

Effective Risk

If correlated entity, effective risk $\geq Y$ then increase customer score. Scale should be configurable by effective risk and jurisdiction.

The total customer score contributes to pre-case.

For example,

- Set up rule to find the KDD_ALERT_CORR_LINK.BUS_NTITY_KEY_ID and KDD_ALERT_CORR_LINK.BUS_NTITY_ID for an alert in the correlation. Look at the respective business table (based on the BUS_NTITY_ID type) to find the Effective Risk.
- Event A Rapid Movement of Funds All Activity CU focus – scenario score of 10; Customer XXX has CUST. CUST_EFCTV_RISK_NB = 8
- Event B Rapid Movement of Funds All Activity CU focus - scenario score of 10; Same customer XXX has CUST. CUST_EFCTV_RISK_NB = 8
- Customer Effective Risk ≥ 7 add 10 points
- Pre-case score = A(10) + B(10) + Cust XXX(10) = 30. Dev Note – this is on distinct customer in correlation

Correlation

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

- [Number of events](#)
- [Combination of Scenarios](#)
- [Total Transaction Amount](#)
- [Repeated Scenario Events](#)

Number of events

- If the number of events in the correlation is more than X, increase correlation score.
- Scaling of correlation by number of events should be as below (scaling should be configurable by no. of events):
 - Number of events greater than 3 and less than or equal to 5 should be given a correlation score of 30.
 - Number of events between 6 and less than or equal to 10 will be given 40.
 - Correlation with more than 10 events will be given 50.
- The additional score has to be added to pre-case score.

For example,

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

- A – 10
- B – 20
- C – 10
- D – 30

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

Combination of Scenarios

- When correlation contains events from scenario X and Scenario Y at the same time consider correlation to add score.
- The total of the correlation score contributes to the pre-case score.

For example,

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

- Event A – 10
- Event B – 10
- Correlation – 50
- Pre-case score = 70

Total Transaction Amount

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

For example,

- Event A ML scenario – total base transaction amount = 15000
- Event B ML scenario – total base transaction amount = 40000
- Event C ML scenario – total base transaction amount = 45000
- Total correlation transaction amount = 100000
- Score is A(10 for ML) + B(10 for ML) + C(10 for ML) + Correlation(30) = 60 for pre-case score

Repeated Scenario Events

- Increase score of the correlation if events are generated for same customer/entity within a configurable time period.
- Scaling for correlation by repeated scenario events should be as below:
 - Increase score by 30 if 2 events are created for same entity/same scenario within look back period. Number of events and lookback are configurable.
 - Increase score by 50 if 3 or more events created for same entity/same scenario within look back period. Number of events and lookback are configurable.

For example,

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

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

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

The chapter focuses on the following topics:

- [About Promoting to Case \(PTC\)](#)
- [Configuring PTC](#)

About Promoting to Case (PTC)

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

- BD
- CS
- KYC
- Third Party

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

Configuring PTC

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

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

To configure PTC, follow these steps:

1. Navigate to the ECM Home Page and select **Common Tasks** and select **Unified Metadata Manager**.
2. Click **Business Metadata Management** and select **Business Processor**. The Business Processor page is displayed.
3. Click **Edit**. The Business Processor page is displayed.

Edit Business Processor

Common Tasks > Unified Metadata Manager > Business Metadata Management > Business Processor > Business Processor Definition (Edit)

» Business Processor Details

Code *

CSPCCLAS

Short Description *

Pre Case Classification For CS

Long Description

» Business Processor Definition

Dataset

DS_PRECASE_SCORE

Measure

PreCasePromotionFlag

Expression

case when FCC_PRECASE_SCORE.N_PRECASE_SCORE > 0 then 'Y' else 'N' end

Expression has Aggregate Function

☐

Parameters

Save

Cancel

User Info

User Comments

» User Info

Created By

SYSADMN

Creation Date

September 19, 2017 12:00:00 AM IST

Last Modified By

Modification Date

Authorized By

SYSADMN

Authorization Date

September 19, 2017 12:00:00 AM IST

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.

Configuring Processing Modelling Framework (PMF)

This chapter includes the following topics:

- [About PMF](#)
- [Pre-configuration Activities](#)
- [Accessing Process Modeller](#)
- [Configuring an ECM Workflow](#)
- [Editing of an ECM Workflow](#)
- [Deleting an ECM Workflow](#)

About PMF

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

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

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

This section covers the following topics:

- [ECM Workflow Development Life Cycle](#)
- [ECM Workflows](#)

ECM Workflow Development Life Cycle

The ECM workflow follows various stages in the development lifecycle:

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

ECM Workflows

The following are default workflows available in the ECM:

- KYC

- AML
- CS-SAN
- CS-PEP & EDD

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

Pre-configuration Activities

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

Configuring Status

The following are the pre-configuration activities for status:

- Add a new status if the required status is not seeded.
 - To add a new status, add the entries in AAI_WF_STATUS_B and AAI_WF_STATUS_TL tables of the Config Schema.
 - The package ID should be OFS_NGECM.
- Add the same entries in KDD_STATUS table of the Atomic Schema.

Configuring Action

- Add a new action if required action is not seeded. For more information on configuring action, see the [Configuring Actions](#).

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

Column Name	Description	Example
N_ATTR_TYPE_ID	ID of the attribute type. The values of the attributes are fetched based on attribute type. 1001- Static 1002- Query 1003- JavaAPI For more information, see the Attribute Types .	1002
V_ATTRIBUTE_VALUE1 V_ATTRIBUTE_VALUE2	Values to be fetched for the attribute. Based on the attribute type, you need to pass the values.	If Attribute Type is 1002, then below are example of query: Select t.action_cd,t.action_nm from kdd_action t where t.action_category_code is not null and t.action_category_code not in ('ENT','PR','EXP','AS','DD','EML','OBS') or Select t.status_cd,t.status_nm from kdd_status t or Select s.v_role_code,s.v_role_code from cssms_role_function_map s where s.v_function_code = 'CMACCESS'
N_APP_ID	Application code for which the current attribute is configured.	OFS_NGECEM
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.

Attribute Type ID	Attribute Type Name	Description
1003	JavaAPI	Enter the method that is configured for V_ATTRIBUTE_VALUE1 for the required attribute. The configured method in the class path is invoked to get the attribute values in this case.

2. Define the query for attribute in V_ATTRIBUTE_VALUE1 column.

After the attribute is defined, you can access this using Application Rule “Attribute Expression”. For more information, see the [Defining Application Rules](#) section.

Accessing Process Modeller

This section explains how to access the Process Modeller page.

To access the Process Modeller page, follow these steps:

1. Navigate to the Systems Configuration & Identity Management tab and expand the Processing Modelling Framework link from the LHS menu.
2. Click the **Process Modeller**. The Process Modeller window is displayed.

The screenshot shows the 'Process Modeller' interface. At the top, there is a breadcrumb trail: 'Financial Services Analytical Applications Infrastructure > Processing Modelling Framework > Process Modeller'. Below this is a search bar with 'Search', 'Go', and 'Clear' buttons. There are four input fields for filtering: 'Process Id', 'Process Name', 'Application', and 'Version'. Below the search bar is a section titled 'Process Modelling Details' with a toolbar containing 'Add', 'Edit', 'Delete', 'Copy', 'Workflow Monitor', 'Process Modelling', and 'Export Definition' buttons. The main area contains a table with the following data:

Select	Process Id	Process Name	Process Description	Application	Version
<input type="radio"/>	BR1	Business Restructure Process	Business Restructure Process	Business Restructure	undefined
<input type="radio"/>	ECM	Case Management - AML	Case Management - AML	Case Management	0
<input type="radio"/>	ECM_KYC	Case Management - KYC	Case Management - KYC	Case Management	0
<input type="radio"/>	ECM_PEP_EDD	Case Management - CS - PEP - EDD	Case Management - Customer Screening - PEP/EDD	Case Management	0
<input type="radio"/>	ECM_SAN	Case Management CS - SAN	Case Management - Customer Screening - SAN	Case Management	0
<input type="radio"/>	MD_1	Model Deployment	Model Deployment	Platform	0

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.

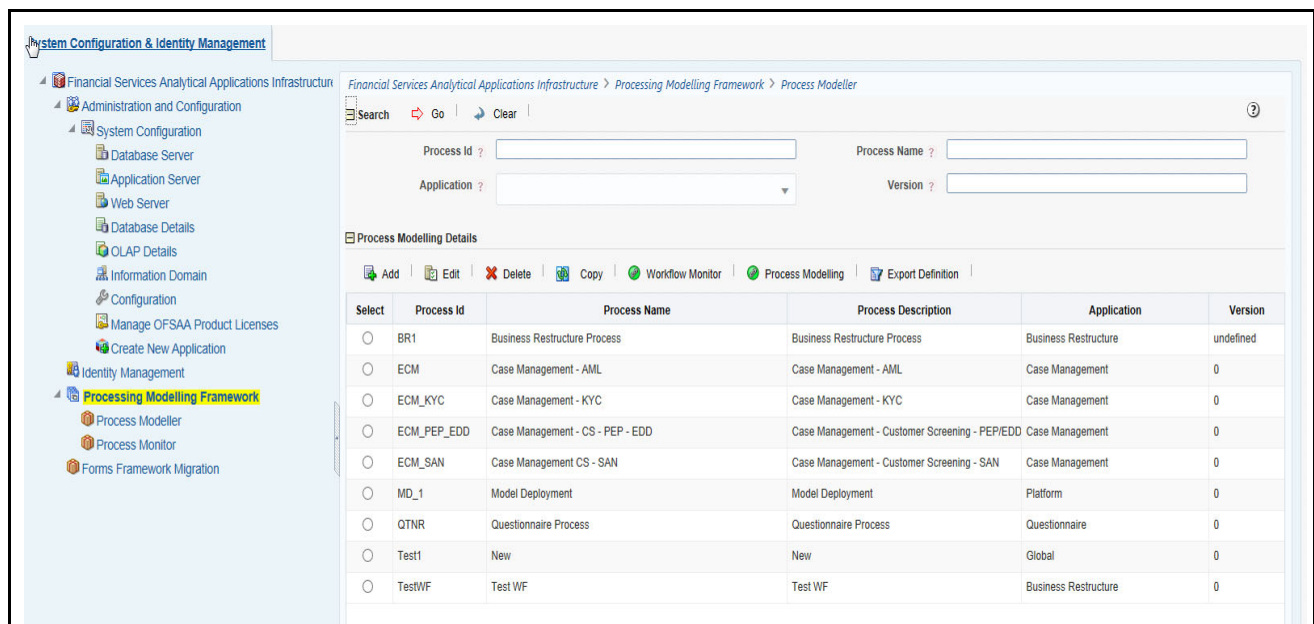
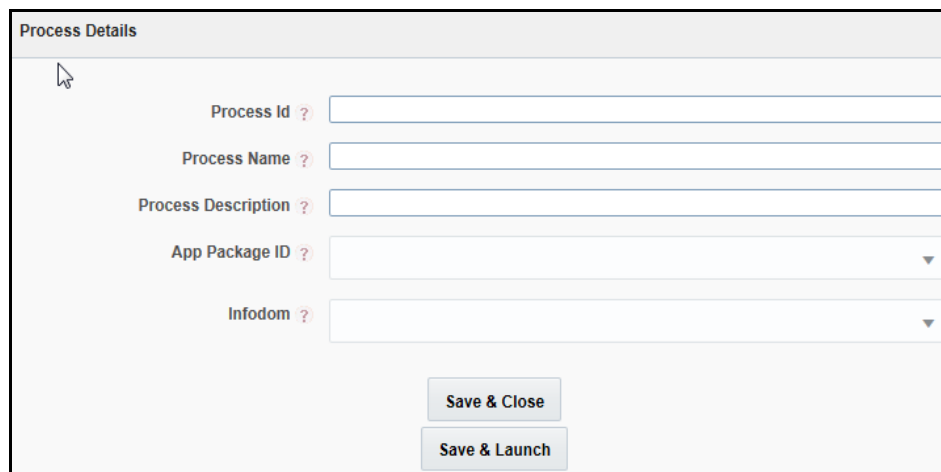


Figure 43. Process Modeller Window

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



The 'Process Details' form contains the following fields and buttons:

- Process Id ?**: Text input field
- Process Name ?**: Text input field
- Process Description ?**: Text input field
- App Package ID ?**: Drop-down menu
- Infodom ?**: Drop-down menu
- Save & Close**: Button
- Save & Launch**: Button

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 <i>Case Management</i> 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.



The 'Process Modeller Editor' window shows a canvas for building a process flow. On the left, there are two panels:

- TOOLS**: Contains icons and labels for Transition, Parallel Gateway, Sequential Gateway, Multi Choice Gateway, Start, and Connector.
- ACTIVITIES**: Contains icons and labels for Human Task, Service Task, Run Task, and SubProcess.

The main canvas is a large grid area for placing and connecting these elements.

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 Input Parameter field.

For more information, see the [Defining Application Rules](#) section.

For more information on Datafields, see the Processing Modelling Framework section of [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

Defining Application Rules

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

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

Based on their usage these are categorized into three types.

- Execution Rule: These are Business Logic executed as Task by an Activity.
- Decision Rule: This rule returns Boolean value “True/False”, used in decision making during split/branching of transition.
- Selection Rule: This rule fetches some value, useful to get value dynamically from a table or other source.

For example, select v_created_by from fct_expenses where id=101

Following are the supported Application Rule Types:

- SQL, JAVA
- Stored Procedure
- Function
- Java External API
- Webservices
- Outcome Rules
- Expression
- Attribute Expressions

For more information, see the Processing Modelling Framework section of [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

Using Process Modeller Editor

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

- [Starting a Process](#)
- [Adding an Activity](#)
- [Adding a Transition](#)

Starting a Process

Using this component you can start a new ECM workflow.

To start a process, follow these steps:

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

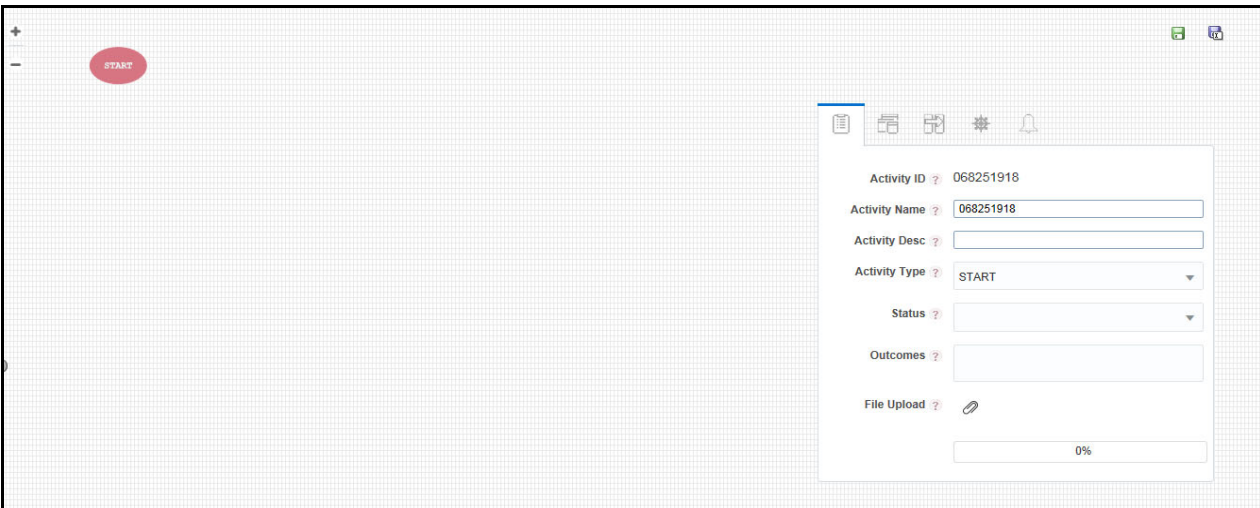


Figure 46. Starting Process

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 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.

Field Name	Description
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.
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: <i>Your file has been uploaded</i> after successful upload of the file. Only a single file can be uploaded. If you upload a new file, the existing file is replaced with the new one. Click Attachment icon adjacent to the file name to remove the file. If a file is attached, Attachment icon is displayed. Click Attachment icon to view or save the file.

Implementing a Process

This section explains how to implement the newly created process. For more information, see the [Implementing a Process](#) section.

Adding Transition

This section explains how to add transition to the newly created process. For more information, see the [Adding Transition](#).

Adding an Activity

To add activity, follow these steps:

1. Click an activity under Activities toolbar in the left panel and then click the canvas where you want to draw the activity. The options are Human Task, Service Task, Run Task and Sub Process.
2. Double-click the icon. On the Right Panel, the Activity tab is displayed.
3. Enter the following information in the respective fields:

Table 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 same as the Activity ID. Modify the activity name if required. For example, New Case.
Activity Desc	Enter the description of the Activity.
Activity Type	By default, the activity type of the selected activity is displayed. Select activity type as Manual from the drop-down list. To change the activity type, you can select the required activity type from the drop-down list. The options are Manual, Automatic, Start, Parallel, Sequential, Connector, Run Task, Multi Choice, and Sub Process.

Field Name	Description
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.
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

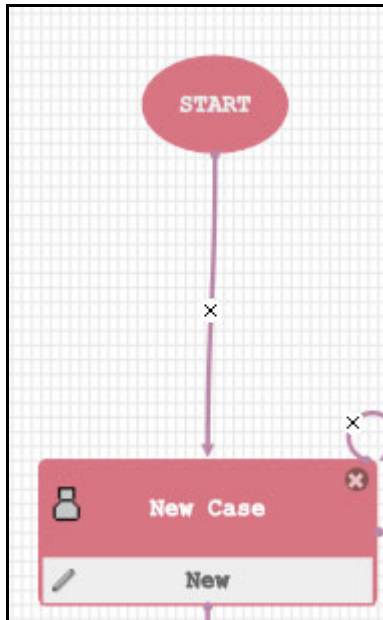


Figure 47. Adding Activity

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  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 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.

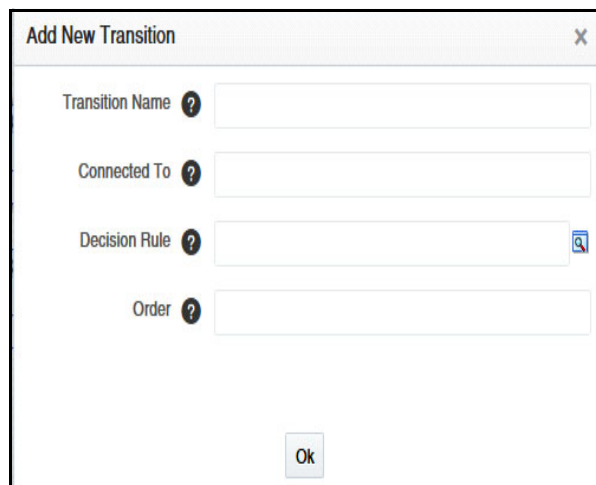
The image shows a window titled "Add New Transition" with a close button (X) in the top right corner. Inside the window, there are four input fields, each preceded by a question mark icon: "Transition Name", "Connected To", "Decision Rule", and "Order". The "Decision Rule" field has a small search icon (magnifying glass) to its right. At the bottom center of the window is an "Ok" button.

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 th Defining Application Rules section.
Order	Enter the Precedence value based on which the transition Decision rules must be executed for multiple transitions, in the Order field. This has effect for transitions from a Sequential gateway only.

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

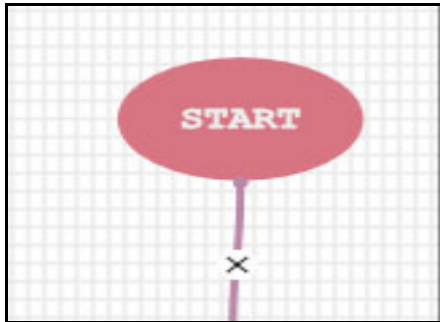


Figure 50. Adding Transition

Editing of an ECM Workflow

To edit an ECM workflow, follow these steps:

1. Navigate to Process Modeller window.

The screenshot shows the 'Process Modeller' window. At the top, there is a search bar with 'Search', 'Go', and 'Clear' buttons. Below this are input fields for 'Process Id', 'Process Name', 'Application', and 'Version'. The main section is titled 'Process Modelling Details' and contains a toolbar with icons for 'Add', 'Edit', 'Delete', 'Copy', 'Workflow Monitor', 'Process Modelling', and 'Export Definition'. Below the toolbar is a table with the following data:

Select	Process Id	Process Name	Process Description	Application	Version
<input type="radio"/>	BR1	Business Restructure Process	Business Restructure Process	Business Restructure	undefined
<input type="radio"/>	ECM	Case Management - AML	Case Management - AML	Case Management	0
<input type="radio"/>	ECM_KYC	Case Management - KYC	Case Management - KYC	Case Management	0
<input type="radio"/>	ECM_PEP_EDD	Case Management - CS - PEP - EDD	Case Management - Customer Screening - PEP/EDD	Case Management	0
<input type="radio"/>	ECM_SAN	Case Management CS - SAN	Case Management - Customer Screening - SAN	Case Management	0
<input type="radio"/>	MD_1	Model Deployment	Model Deployment	Platform	0

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.

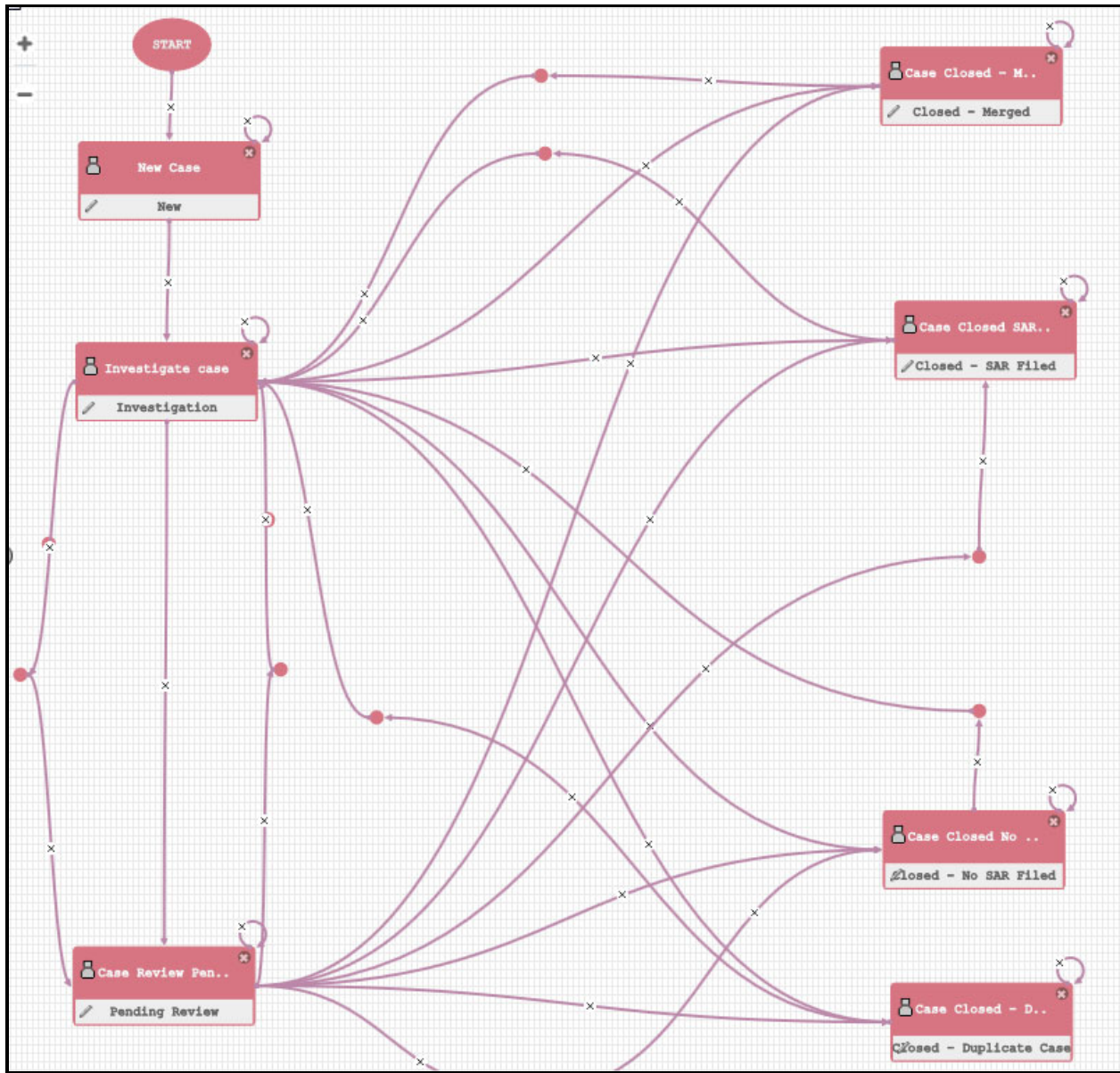


Figure 52. Editing Workflow

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**.

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

The following topics are covered in this chapter:

- [About Case Designer](#)
- [Accessing Case Designer](#)
- [Case Designer Home page](#)
- [Defining Case Class](#)
- [Defining Case Type](#)

About Case Designer

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

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

Accessing Case Designer

This section explains how to access the Case Designer page.

To access the Case Designer page, follow these steps:

1. Navigate to the Case Management Configuration page. For more information on how to navigate to the Case Management Configuration page, see [Chapter 2, Getting Started](#).
2. Click **Case Designer**. The Case Designer page is displayed.

Case Designer Home page

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



Figure 53. Case Designer Home Page

To view Case Designer Home page, follow these steps:

1. Navigate to the Case Designer page.
2. Click the **Case Class Definition** or **Case Type Definition** tab. The previously added Case Class or Case Type list is displayed in the Left Hand Side (LHS) menu.
3. Select **Case Class Definition** tab and go to the **Case Class Overview** section. Hover over the Statistics pie chart. The number of case types created under a particular case class is displayed.

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

Using the Case Designer Home page, you can also add a new Case Class or Case Type. For more information, see [Adding Case Class](#) or [Adding Case Type](#) sections.

Defining Case Class

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

The following topics are covered in this section:

- [About Case Class](#)
- [Adding Case Class](#)
- [Editing Case Class](#)

About Case Class

- A Case Class is the top most definition through which a case is created.
- Used for grouping case types.
- Add and modify case class.
- Does not impact directly on the ECM workflows.
- Updated even if cases are linked to case type.
- Cannot remove existing case classes.

Adding Case Class

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

To add a new case class, follow these steps:

1. Navigate to the Case Designer page.
2. Click **Case Class Definition** tab.
3. Click **Add**. The Case Class Definition page is displayed.
4. Enter the following information in the respective fields.

Table 29. Case Class Definition

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

5. Click **Save**. The following message is displayed: *Case Class is created successfully*.
6. Click **OK**. The Case Class is added to the Left Hand Side (LHS) menu.

Editing Case Class

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

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

To modify a case class, follow these steps:

1. Navigate to the Case Designer page.
2. Click **Case Class Definition** tab.
3. Select the existing case class in LHS menu. The case class details are displayed in Right Hand Side (RHS) pane.
4. Modify the necessary information in the required fields. For more information on the fields, see [Table 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](#)
- [Adding Case Type](#)
- [Editing Case Type](#)

About Case Type

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

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

Adding Case Type

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

To add a new case type, follow these steps:

1. Navigate to the Case Designer page.

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

Figure 54. 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 Case Type name.

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

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

Configuring Optional Definitions in CaseType

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

This section covers the following topics:

About Optional Definitions

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

Defining Attributes

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

The following sections are covered in this topic:

- [About Attributes](#)
- [Adding Optional Attributes to the Case Type](#)
- [Deleting Attributes](#)

About Attributes

- Attributes are fields that display on the Case Search, Case Context, and Create Case page of ECM UI.
- Classified into mandatory and optional definitions.
- Mandatory Attributes - Case ID, Class, Type, Status, Title, Jurisdiction, Business Domain, Priority, Created, Owner Organization, Due, Owner, Closed, Assignee, Description.
- Optional Attributes - Document Control, Scenario Class, and Risk Score.
- Configure Attributes definitions to show or hide them on ECM UI.
- By default, all mandatory attributes are shown in the Attributes section.
- Can add or remove only optional attributes using Case Designer.
- Dynamic rendering of the attributes based on its behavior across the different case pages. For example, Case ID attribute is hidden on the Create Case page but it is disabled on the Case Context page.
- Whenever changes happen to attributes those changes are reflected on all case related pages based on its behavior in the Enterprise Case Management UI.

Adding Optional Attributes to the Case Type

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

To add optional attributes, follow these steps:

1. Navigate to the Case Type Definition page.
2. Click **Attributes** tab. The optional attributes are displayed in the *Available Attributes* menu.

Figure 55. 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 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 about an Entity and how to configure in the Case Type.

The following sections are covered in this topic:

- [About Entities](#)
- [Adding Optional Entities to the Case Type](#)
- [Deleting Entities](#)

About Entities

- Entities are tabs that display on the Case Summary section of ECM UI after you define them in Case Designer.
- Defines entities to show or hide them on the Case Summary.
- Entities are classified into mandatory and optional.
- Mandatory Entities – Event Details, Evidence, Relationship, Narrative, Audit History.
- Optional Entities - Correlation, Account, Customer, Employee, Household, Investment Advisor, External Entity, Correspondent Bank, Transactions, FATCA Assessment, Financials, Involved Party, Network Analysis, Enhanced Due Diligence, and Risk Assessment.
- Case Summary section of ECM UI display entities (tabs) even there is no data is associated with the entity.
- Add or remove only optional entities.
- Ordering of entities can be configured.
- Whenever changes happen to entities those changes are reflected on Case Summary section for that Case Type in Enterprise Case Management UI.

Adding Optional Entities to the Case Type

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

To add optional entities, follow these steps:

1. Navigate to the Case Type Definition page.
2. Click **Entities** tab. The optional entities are displayed in the *Available Entities* menu.

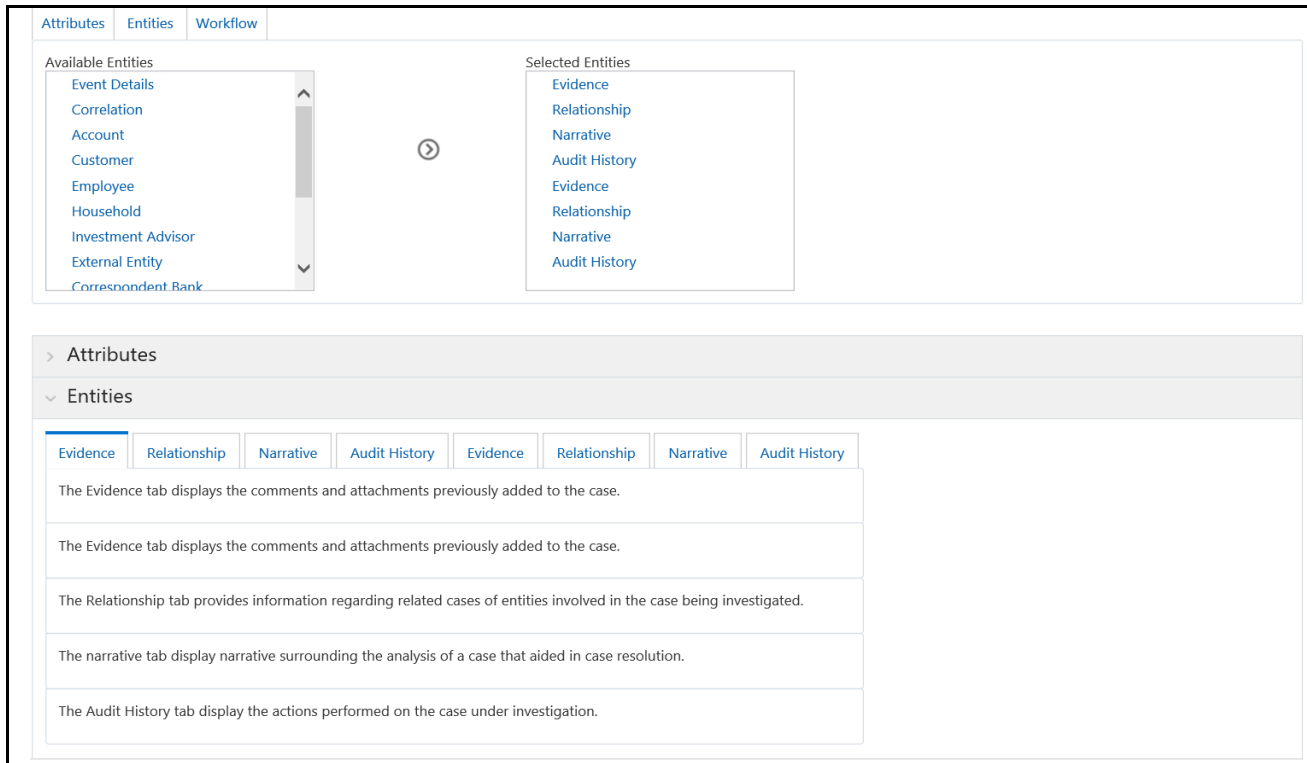




Figure 56. Entities Page

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

Note: The newly added entities are marked with  icon.

4. Select the required tab. Hold it and move to position it according to your requirement.
5. Click **Save**. The following message is displayed: *Case Type is created successfully.*


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

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

Deleting Entities

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

To remove optional entities, follow these steps:

1. Navigate to the Case Type Definition tab.
2. Select required Case Type. Go to the Entities section.
3. Click  against required entities to remove from Entities section. The deleted entities are moved back to the Available Entities menu.

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

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

Defining Workflow

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

The following sections are covered in this topic:

- [About Workflows](#)
- [Adding Workflow](#)
- [Deleting Workflow](#)

About Workflows

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

Adding Workflow

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

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

To add a workflow, follow these steps:

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

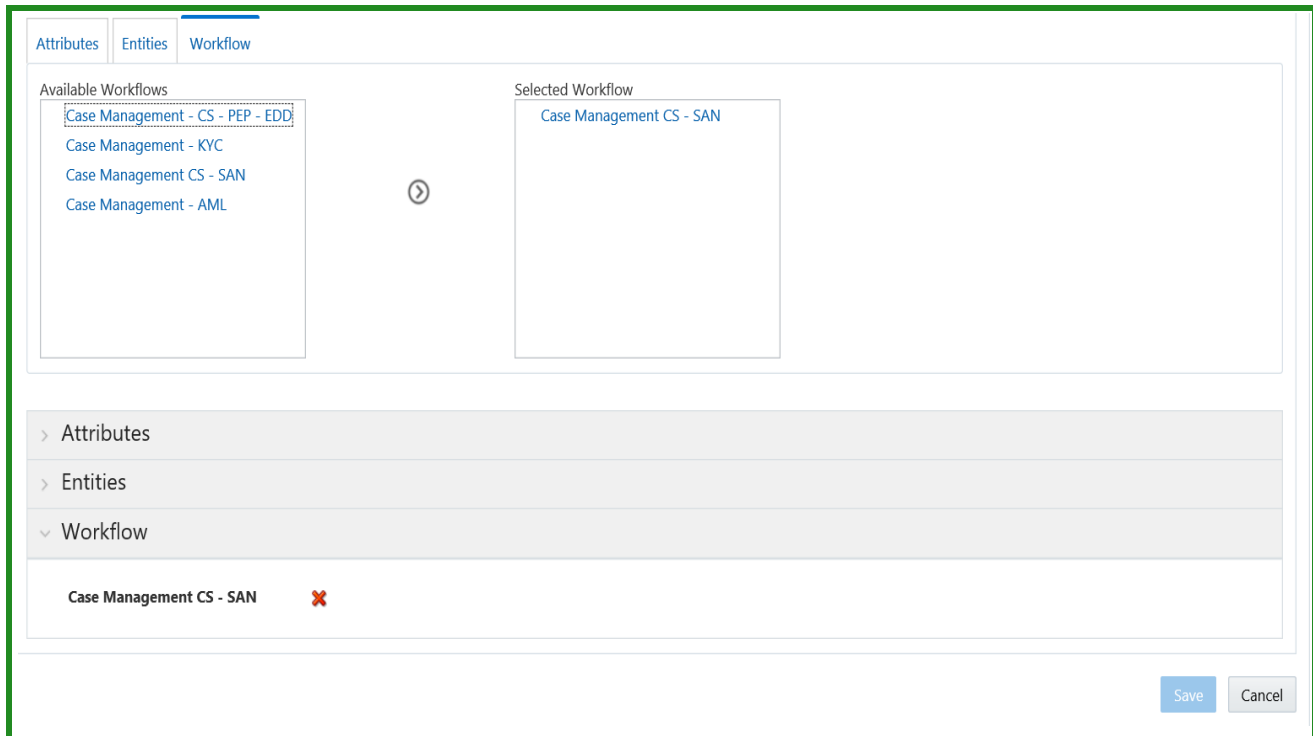


Figure 57. Workflow Page

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

Note: The newly added workflow is marked with icon.

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

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

Deleting Workflow

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

To remove the workflow, follow these steps:

1. Navigate to the Case Type Definition tab.
2. Select required Case Type. Go to the Workflow section.
3. Click against the required workflow to remove from Workflow section. The deleted workflow is moved back to the **Available Workflows** box.
4. Click **Save**. The Workflow section is updated.

Editing Case Type

This section describes how to modify existing Case Type definitions.

To modify a case type, follow these steps:

1. Navigate to the Case Designer page.
2. Click **Case Type Definition** tab.
3. Select an existing case type in LHS menu. The Case Type Definition page is displayed.
4. Modify the necessary details in the Case Class and Description fields. For more information on the fields, see [Table 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 Attributes or Entities definitions, see [Defining Attributes](#) and [Defining Entities](#) respectively.

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

- [Configuring the Client Logo Image](#)
- [Configuring the Base Time Zone](#)
- [Configuring the Default Currency Code](#)
- [Configuring Lock Time Period for Case Actions](#)
- [Configuring E-mail](#)
- [Configuring Organization Type](#)
- [Configuring View All Organization](#)
- [Configuring the Display of Value in By Field Name/ID](#)
- [Configuring the Default Due Date Calculation](#)
- [Configuring File Size](#)
- [Configuring Views](#)
- [Configuring ECM Security Function](#)

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:

6. Make a backup of existing `client_logo.gif` from the location: <AAI deployed area>/images (for example, /OFSAAI/images/).
7. Place the customer logo from location: <AAI deployed area>/images (for example, /OFSAAI/images/).
8. After placing the image in the web server, refresh the IE browser.
9. Refresh the Appserver's work folder.

Removing a Client Logo

To remove a custom client logo, follow these steps:

1. Replace `client_logo.gif` from the backup location.
2. After placing the image in the web server, refresh the IE browser.
3. Refresh the Appserver's work folder.

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).

Accessing Manage Parameters

To access the Manage Parameters, follow these steps:

1. Navigate to Administration tab and select Manage Parameters option.
2. Select Manage Common Parameters to access the Manage Common Parameters window.

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 58. 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 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 Figure 59.

Figure 59. Financials Tab—Default Currency Format

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 60 illustrates the modified currency code as EUR.

Details

Account

HouseHold

Customer

Investment Advisor

Employee

External Entity

Involved Party

Transactions

Financials

Current Loss and Recovery Summary

Edit

Remove

History

Total Potential Loss Amount:

EUR 6,546,546.00

Primary GL Account:

456789

Charge Off Date:

09/30/2013

Total Averted Loss Amount:

EUR 6,565.00

Primary Cost Center:

FI006A

Last Updated Date:

09/26/2013

Total Loss Recovery Amount:

EUR 456,748.00

Offset Account:

23879

Last Updated By:

SUPERVISOR

TotalNet Loss Amount:

EUR 6,083,233.00

Offset Cost Center:

FI006A

Potential Loss

Expand All

Add

Edit

Remove

Excel

History

AV

AV

AV

Date

Amount

GL Account

Cost Center

Loss Payee

Entered By

Entered Date

Description

09/24/2013

EUR 6,546,546.00

156789

FI006A

--

SUPERVISOR

09/26/2013

--

Figure 60. Financials Tab—with Modified Currency Format

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

1. Locate the `CFG_Env.xml` file in the following directory:
`<MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config`
2. Save a copy of the original `CFG_Env.xml` file in the custom directory that contains backup files:
`<MANTAS_HOME>/alert_management/alert_mgmt/WEB-INF/classes/conf/ui_config/custom/backup`
3. Open the original `CFG_Env.xml` in an editor.
4. Locate the default currency code that you want to modify, that is similar to the following:
`<I18N lang="en" country="US" dateFormat="MM/dd/yyyy" baseTimeZone="EST" defaultCurrency="USD" pdfFont="ArialUnicodeMS"/>`
5. Modify the currency code.

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

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

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

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

Configuring 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 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 31 describes the attributes which need to be configured for E-mail parameters.

Table 31. 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.

Table 31. Configuring E-mail Attributes

Attribute	Description
HTML_REPORT_IN_BODY	This attribute specifies for a single case, whether the HTML report should come in mail body or as attachment.
DEF_ACTION_TAKER	This attribute specifies the default action taker for the received response if the system cannot identify the Response Sender as a valid User.

Configuring 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 View All Organization

This parameter, along with other access permissions defined for the user, determines the cases that can be viewed by a user in the Related Cases matrices of the Relationship tab for Case Management implementations. The parameter value can have only Y or N value. Y enables the current user to view cases as related events and- related cases respectively, even if the user does not have viewing rights for the case's primary organization, which is defined based on the organization associated with the owning user. N restricts the user from viewing, as related, events or cases whose primary organizations the user does not have access to view.

For example, User Joe Smith may be not be allowed to see the details of cases owned by users (or a pool) who have Employee Compliance as their primary organization. However, if this parameter is set to Y, Joe Smith would be able to see cases associated with the organization of Employee Compliance in a list of related cases, as long as they have a relationship to the current case being viewed. If this parameter is set to N, Joe Smith would have no ability to see the above mentioned cases, even as related.

To disable View All Organization, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **View All Organization** from the Parameter Name drop-down list.

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring 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 32 describes the attributes which should be configured for Display of Value in By Field Name/ID.

Table 32. Configuring Display of Value in By Field Name/ID Attributes

Attribute	Description
User	ID or Name for User field.

Configuring the Default Due Date Calculation

This parameter allows the client to specify the use of Business days versus Calendar days. Here you can specify **C** for Calendar days and **B** for Business days.

Note: The default value is Calendar days (C).

To modify the Default Due Date Calculation, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Default Due Date Calculation** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

Configuring 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 33. KDD_QUEUE_MASTER table

QUEUE_SEQ_ID	QUEUE_CD	QUEUE_DISPLAY_NM	QUEUE_TYPE
Unique sequence ID	Unique Queue Code	The name of the view that will be displayed in the UI	ECM : If the view is related to Cases

2. Make the entries in the KDD_QUEUE_FILTER table for each filter for respective view.

QUEUE_SEQ_ID	ATTRBT_ID	ATTRBT_VAL_TX
Unique sequence ID	Unique Attribute ID. ATTRBT_ID will be referered from KDD_CASEATTRBT_MASTER	<p>This Attribute value is the actual value used for the attribute of filter. In this, you can give hardcoded values (for example, put a filter condition on status attribute for the cases which are in New status). The possible value for this is NW.</p> <p>You can also specify session attributes for your filter. The session attributes are enclosed in curly brackets {}.</p> <p>For example: {userSeqId}, {userPool}</p> <p>You can define SYSDATE value for filter. Date filter requires following two inputs:</p> <ul style="list-style-type: none">● From Date● To Date <p>For example: #NS#, #SYSDATE#</p> <p>You should specify the date values in enclosed #</p> <p>Use #NS# to mention the date filter as blank.</p>

3. Map Queue in the KDD_QUEUE_ROLE_MAP table.

Table 34. KDD_QUEUE_ROLE_MAP table

QUEUE_SEQ_ID	ROLE_CD
Queue sequence id as given in the above table	Role code

Modifying Views

Following are the various modifications for views:

1. **Modify An Existing View Query**

In order to modify the underlying filters for a view, changes are to be done in the KDD_QUEUE_FILTER table column.

2. Modifying View-Role Mapping

In order to make a view available for an existing role, the mapping has to be done in KDD_QUEUE_ROLE_MAP table.

3. Modifying the Display Name of the View

In order to change the display name for a particular view, changes have to be done in KDD_QUEUE_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.

The screenshot shows the 'Manage Common Parameters' interface. At the top, there is a breadcrumb 'Home > Manage Common Parameters'. Below it is a search bar. The main area has two dropdown menus: 'Parameter Category' set to 'Used For Design' and 'Parameter Name' set to 'ECM Security Function'. The parameter details are as follows:

Parameter Name: ECM Security Function	Parameter Value: CMACCESS	Parameter Category: Used For Design
Parameter Description Text: This parameter specifies the Function which will be mapped to the User groups to be displayed in Mapper Maintenance Screen.	Last Modify Date: 11/17/2017	Modified By: ECMADMN

Below the details, there are 15 attribute rows, each with a description and a value field:

Attribute Name	Attribute Description	Attribute Value
Attribute 1 Name:	Attribute 1 Description:	Attribute 1 Value:
Attribute 2 Name:	Attribute 2 Description:	Attribute 2 Value:
Attribute 3 Name:	Attribute 3 Description:	Attribute 3 Value:
Attribute 4 Name:	Attribute 4 Description:	Attribute 4 Value:
Attribute 5 Name:	Attribute 5 Description:	Attribute 5 Value:
Attribute 6 Name:	Attribute 6 Description:	Attribute 6 Value:
Attribute 7 Name:	Attribute 7 Description:	Attribute 7 Value:
Attribute 8 Name:	Attribute 8 Description:	Attribute 8 Value:
Attribute 9 Name:	Attribute 9 Description:	Attribute 9 Value:
Attribute 10 Name:	Attribute 10 Description:	Attribute 10 Value:
Attribute 11 Name:	Attribute 11 Description:	Attribute 11 Value:
Attribute 12 Name:	Attribute 12 Description:	Attribute 12 Value:
Attribute 13 Name:	Attribute 13 Description:	Attribute 13 Value:
Attribute 14 Name:	Attribute 14 Description:	Attribute 14 Value:
Attribute 15 Name:	Attribute 15 Description:	Attribute 15 Value:

At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 61. Configuring ECM Security Function

4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

Managing Additional Configurations

The section describes the additional configurations that need to be carried out by the system administrator.

This section covers the following topics:

- Configuring File Type ExtensionsConfiguring ECM Security Function

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.

This chapter provides instructions for configuring parameters specific to administration tools.

This chapter covers the following topics:

- [Configuring Administration Tools](#)
- [Configuring Application Server](#)

Configuring Administration Tools

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

Follow these steps incase admin tools deployed web application context and URL were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Admin Tool** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 35 describes the attributes which should be configured for enabling and using the administration tools.

Table 35. Configuring Administration Tools

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

Configuring Application Server

This parameter specifies the OFSAAI Application Server IP Address and Java Port.

Follow these steps if in case the values were different from the default values populated by the Installer.

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Application Server** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking: *Would you like to Save these actions?*
5. Click **OK**. A Confirmation dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

Table 36 describes the attributes to be configured for setting the application server.

Table 36. 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.

This chapter describes how you can assign ownership of cases, and covers the following topics:

- [About Case Assigner Editor](#)
- [Case Assigner Screen Elements](#)
- [Using Case Assigner Editor](#)

About Case Assigner Editor

The Case Assigner Editor allows the application Administrator to view and modify the rules used to assign ownership of cases. The Case Assigner Editor allows you to perform the following tasks:

- Create, modify, or delete a rule
- Define Role-Based Assignment Limits

Each case generated within the application is assigned an initial owner before it is available for analysis. The application automatically determines an appropriate owner (a user or group of users) for each case based on the initial assignment logic you configured or configured for your firm. Initial assignment logic is composed in a set of operations that evaluate various attributes of the case. For example, scenario, score, or related entities. Case assignment rules apply only to those cases created automatically as a result of promotion of a event Correlation to a case. They do not impact cases created directly by a user.

You can add, modify, or delete assignment rules. The following elements are combined to form a set of logic against which the cases are evaluated:

- Each assignment rule is defined as an attribute of a case, an operator, and a value.

[Table 37](#) shows a sample of a case assignment rule.

Table 37. Sample of a Case Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
1	Case Type	<ul style="list-style-type: none">● Cases with case type AML Surveillance are assigned to the AML Compliance Pool.● Cases with case type Fraud - Online Fraud are assigned to the FR Risk Pool.

Table 37. Sample of a Case Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
2	Case Type and Jurisdiction	<ul style="list-style-type: none">● Cases with case type AML Surveillance AND with a Jurisdiction of High Wealth Customer are assigned to the AML Compliance - Wealth Management Pool.● Cases with case type AML Surveillance AND with Jurisdiction of Eastern Region Retail are assigned to the AML Compliance - Eastern Region Pool.
3	Default	<ul style="list-style-type: none">● All cases that do not meet other rules are assigned to the AML & Fraud Risk Management pool.

- Each assignment rule consists of an operation set that identifies a grouping of rules of which it is a member.
- Operations are logical expressions that can be used to evaluate cases (for example, score > 50). A set of operations based on the same attribute (for example, score) are grouped into an operation set.
- All operations within an operation set must be mutually exclusive and should collectively cover the entire spectrum of values for a given attribute.
- Each operation specifies the next step that is applied to cases that satisfy the operation. This next step is either an owner for the case, or the next operation set, or branch, to further evaluate the cases.
- Each case is evaluated against the operations within operation set one (1). Each case then branches out based upon the next operation set specified for the operation within Operation Set one (1) that they satisfy. Each case continues through a chain of operation sets until it satisfies an operation for which an owner has been specified. Cases that do not reach an operation that they satisfy and for which an owner has been specified, are assigned to the Default Owner that has been specified through initial configuration using installation parameters.

Note: Manually posted cases, generated by the event correlation process, are not assigned to the default owner that is specified through the assignment editor.

Accessing Case Assigner Editor

To access Case Assigner Editor, follow these steps:

1. Navigate to the Administration menu and select **Case Management Configuration**.
2. Select the **Case Assigner Editor** option. The Case Assigner Editor page is displayed.

Case Assigner Screen Elements

The following pages are associated with the Case Assigner Editor:

- **Case Assigner Editor:** This is the first page displayed when accessing the Case Assigner Editor. You can delete a rule from this page or navigate to the Assignment Rule Editor to add a new rule or modify an existing rule. See the *Case Assigner Editor* for more information.
- **Assignment Rule List for Cases:** This page enables you to create a new rule or modify an existing rule. See the *Assignment Rule List for Cases* for more information.

- **Role Based Assignment Rule Editor:** This page allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. See the *Assignment Rule Editor* for more information.

Case Assigner Editor

The Case Assigner Editor displays the assignment rules associated to cases.

The screenshot shows the Case Assigner Editor interface. At the top, there is a section titled "Assignment Rule List for Cases" with a blue header. Below the header, there is a message: "Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule." Below this message, there is a text area that says "There are no rules currently exists." Below this, there is a section titled "Role Based Assignment Limits Editor" with a blue header. Below the header, there is a button labeled "Add Exception". Below the button, there is a table with the following columns: "Role" and "Maximum Limits". The table has the following rows:

Role	Maximum Limits
<input type="checkbox"/> Case Analyst1	
<input type="checkbox"/> Case Analyst2	
<input type="checkbox"/> Case External Auditor	
<input type="checkbox"/> Case Executive	
<input type="checkbox"/> Case Internal Auditor	
<input type="checkbox"/> Case Initiator	
<input type="checkbox"/> Case Administrator	
<input type="checkbox"/> Case Supervisor	
<input type="checkbox"/> Case Viewer	

Below the table, there are two buttons: "Save" and "Cancel".

Figure 62. Case Assigner Editor

The components of the Case Assigner Editor include the following:

- [Assignment Rule List for Cases](#)
- [Role Based Assignment Limits Editor](#)

Assignment Rule List for Cases

The assignment rule list displays in the Case Assigner Editor. The rules in the list are sorted in ascending order by operation set number ([Figure 63](#)).

The screenshot shows the Assignment Rule List for Cases table. The table has the following columns: "Operation Set", "Attribute", "Operator", "Value", "Next Operation Set", "Owner", and "Strategy". The table contains the following data:

Operation Set	Attribute	Operator	Value	Next Operation Set	Owner	Strategy
1	INVESTIGATION Case Type	=	FR		TestOrgC	
1	INVESTIGATION Case Type	=	AML		Analyst3(ANALYST3)	
1	INVESTIGATION Case Type	=	KYC		KYCINV(KYCINV)	
2	INVESTIGATION Case SubType	=	FIRM		KYCINV1(KYCINV1)	

Figure 63. Assignment Rule List for Cases

The Assignment Rule List for Cases includes the following components:

- **Add button:** Navigates you to the Assignment Rule Editor.
- **Update button:** Navigates you to the Assignment Rule Editor.
- **Delete button:** Deletes the assignment rule.
- **Assignment Rule List for Cases** page displays the column headings: Operation Set, Attribute, Operator, Value, Next Operation Set, and Owner. See *Assignment Rule Editor* for more information.

Role Based Assignment Limits Editor

The Role Based Assignment Limits Editor allows you to limit the number of cases that can be assigned to members of a pool based on user role. For example, if a member pool contains 25 investigators, you can limit junior investigators to have a maximum of 10 cases assigned to them, and assign a senior investigator no cap.

Cases are assigned based on the available assignment rules until members reach their caps, then cases are assigned only to members who have not reached their caps. If all members have reached their limit, cases are assigned to the pool, and can be accessed by using the Auto-Assignment option.

	Role	Maximum Limits
<input type="checkbox"/>	Case Analyst1	
<input type="checkbox"/>	Case Analyst2	
<input type="checkbox"/>	Case External Auditor	
<input type="checkbox"/>	Case Executive	
<input type="checkbox"/>	Case Internal Auditor	
<input type="checkbox"/>	Case Initiator	
<input type="checkbox"/>	Case Administrator	
<input type="checkbox"/>	Case Supervisor	
<input type="checkbox"/>	Case Viewer	

Save Cancel

Figure 64. Role Based Assignment Limits Editor

The Role Based Assignment Limits Editor includes the following components:

- **User Role grid:** When a user role is selected, you can edit the maximum limit. A *Null* value indicates there is no limit for the assignment of cases.
- **Add Exception button:** Allows you to enter exceptions to the limit assigned to the user role. See *Adding an Exception to a Role Based Assignment Limit* for more information.
- **Save button:** Saves all modifications to the database.
- **Cancel button:** Redispays the Assignment Editor. The New Maximum Limits value is not saved.

Assignment Rule Editor

The Assignment Rule Editor displays after you click **Add** or **Update** (Figure 65). This editor allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. The decision trees are used to determine the owner (an individual or group of users) of each case generated by the system.

Figure 65. Assignment Rule Editor

The components of the Assignment Rule Editor include the following:

- **Operation Set:** Specifies a grouping of mutually exclusive rules based on an attribute.
 - If you select **Add**, the **Operation Set** text box displays as blank.
 - If you select **Update**, the **Operation Set** text box field is populated with the current data for the selected rule.
 - You must create rules within Operation Set 1 before creating any additional rules. Any condition not covered by Operation Set 1 is assigned to the default assignment owner, as are all other operation sets when cases are added to them.
- **Investigation Attribute:** Populates alphabetically with values for each attribute of the case. For example, Jurisdiction, Business Domain, Case Type, Linked Events, Linked Cases, and Priority, off which to base the rule.
 - If you select **Add**, the **Investigation Attribute** drop-down list displays a blank value (“ ”) (the default).
 - If you select **Update**, the **Investigation Attribute** drop-down list displays the current value of the selected rule.
- **Operator** drop-down list: Contains the following values =, !=, >, <, <=, >=, in, contains, blanks (“ ”), and else.
 - If you select **Add**, the **Operator** drop-down list displays a blank value (“ ”) (the default).
 - If you select **Update**, the **Operator** drop-down list displays the current value of the selected rule.
 - If you base your rule on an investigation attribute for which an enumerated list of values has been defined, only the values = and != are available in the **Operator** drop-down list.
 - If you have a list of values and you want to check if the database field is one of the values in the list, select the *in* operator in the **Operator** drop-down list.
 - If you want to check a database field that contains a comma-delimited list of values for a specific value, select the **contains** operator in the **Operator** drop-down list.

Note: The selection between the *in* and *contains* operators depends on the type of search you want to perform. Using the *contains* operator allows you to check if a database field containing a comma-delimited list of values contains a specific value. For example, checking if the Business Domain contains a particular business domain. The *contains* operator is similar to the *in* operator, but it reverses the comparison. With the *in* operator, the single value is in the field in the database, and a list of values is provided as the argument. With the *contains* operator, the list is in the database, and the single value is provided as an argument.

- If you select the *else* operator, the *value* must be NULL; followed by a subsequent operation or case owner recipient specification. The system evaluates the *else* operation after evaluating all other operations.
- **Value** text box or drop-down: Within the rule, the value of the investigation is compared to the **Value** field. If you have selected an attribute in the **Investigation Attribute** drop-down list with defined values (Jurisdiction, Business Domain, Case Type, Linked Events, Linked Cases, and Priority), the **Value** drop-down list will contain those values. The **Value** field displays as a text box for all other attributes (for example, score or account balance).
 - If you select **Add**, the **Value** text box displays a blank value (“”).
 - If you select **Update**, the **Value** text box displays the current value of the selected rule.
 - If you enter multiple values in the **Value** text box after having selected *IN* as the operator, separate the values with pipe (|).
 - If you select the *else* operator, the **Value** must be NULL therefore, the system disables the Value text box or drop-down list.
- **Next Operation Set** text box: The number of the next operation set, or branch, to further evaluate the case or assign to an owner.
 - If you select **Add**, the **Next Operation Set** text box displays a blank value (“”) (the default).
 - If you select **Update**, the **Next Operation Set** text box displays the current value of the selected rule.
 - If the result of your rule is to continue to the next operation set, you must not select an owner to assign the or case.
- **Owner** drop-down list: Displays available owners for both cases.
 - If you select **Add**, the **Owner** drop-down list displays a blank value (“”) (the default).
 - If you select **Update**, the **Owner** drop-down list displays the current value of the selected rule.
 - If the result of your rule is to assign case, you must not select to continue to the next operation set.
- **Strategy** drop-down list (*Optional*): Displays available strategies for the assignment rule. This drop-down list is disabled unless an owner is selected and that owner is a pool and not an individual user.
 - If you select **Round Robin**, cases are assigned to the members of a pool in a circular order until all the cases have been assigned.
 - If you select **Load Leveling**, the pool member's current load is taken into consideration when assigning cases.
 - If a strategy is selected and then an individual user is selected in the **Owner** drop-down list, then the value in the Strategy drop-down list is made blank.

Using Case Assigner Editor

This section explains the following functions of the Assignment Editor:

- [Adding a New Rule](#)
- [Modifying a Rule](#)
- [Deleting a Rule](#)
- [Adding a Role Based Assignment Limit](#)
- [Adding an Exception to a Role Based Assignment Limit](#)

Adding a New Rule

To add a new rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Click **Add**. The Assignment Rule Editor displays.
2. Type an operation set number in the **Operation Set** text box.
You can add to an existing operation set based on the same attribute by entering the same number as the other rules in that set or you can start a new set by entering the next sequential number.
3. Select either an investigation attribute on which to base the rule in the **Investigation Attribute** drop-down list.
This attribute must be the same for any other rules within the same operation set.
4. Select an operator in the **Operator** drop-down list. If you select the *else* operation, skip to Step #6 since no value is required for this operand.
5. Type a value in the **Value** text box.
Depending on the attribute, this value can be a numeric or a text string.
6. Select either the next operation set to attach additional rules to this rule in the **Next Operation Set** text box, or select an owner to assign cases to in the **Owner** drop-down list.
Note: Ensure that the new owner has permission to view cases with the attributes specified in the rule.
7. If you selected a pool in the **Owner** drop-down list, select a strategy for case assignment from the **Strategy** drop-down list.
8. Click **Save**.

The system creates the new rule and redisplay the Case Assigner Editor with the new rule.

Modifying a Rule

To modify the rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Click **Update** for the desired rule.
The Assignment Rule Editor displays.

2. Do one or more of the following:

- Modify the operation set number in the **Operation Set** text box.
- Modify the investigation attribute on which to base the rule from the **Investigation Attribute** drop-down list.

This attribute must be the same for any other rules within the same operation set.

- Modify the operator in the **Operator** drop-down list.
- Modify the value in the **Value** text box.

Depending on the attribute, this value can be a numeric or a text string.

- Modify the next operation set to attach additional rules to this rule in the **Next Operation Set** text box, or select an owner to assign cases to in the **Owner** drop-down list.
- Modify the strategy selected to assign cases to the pool in the **Strategy** drop-down list.

3. Click **Save**.

The system updates the rule and redisplay the Case Assigner Editor with the rule's updates.

Deleting a Rule

To delete an existing Assignment Rule for a case from the Assignment Rule Editor, follow these steps:

1. Click **Delete** for the associated rule.

The Confirmation dialog box displays the message: *Are you sure you want to delete the selected Assignment Rule?*

2. Click **OK** to delete the rule.

The system removes the rule and redisplay the Case Assigner Editor.

Adding a Role Based Assignment Limit

To add an assignment limit for a user role, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Enter the Maximum Limit for this user role.

3. Click **Save**.

The Confirmation dialog box displays the message: *Are you sure you want to modify the limits of this user role?*

4. Click **OK** to set the assignment limit.

The system sets the limit and redisplay the Case Assigner Editor.

Adding an Exception to a Role Based Assignment Limit

To add an exception for a use role based assignment limit, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.

2. Click **Add Exception**.

3. Select the user you want to add the exception for from the dropdown list.
4. Enter the Maximum Limit.
5. Click **Save**.

The Confirmation dialog box displays the message: *Are you sure you want to add the user with the mentioned limits?*

6. Click **OK** to set the assignment limit.

The system sets the limit and redisplay the Case Assigner Editor.

Modifying an Exception

To modify the rule that establishes the conditions of the assignment from the Assignment Rule Editor, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.
2. Click **Add Exception**.
3. Select the user you want to modify the exception for from the drop-down list.
4. Click **Edit**.
5. Modify the limits.
6. Click **Save**.

The system updates the rule and redisplay the Case Assigner Editor with the rule's updates.

Deleting an Exception

To delete an existing exception for a case from the Assignment Rule Editor, follow these steps:

1. Select the user role in the Role Based Assignment Limits Editor.
2. Click **Add Exception**.
3. Select the user you want to modify the exception for from the drop-down list.
4. Click **Delete**.

The Confirmation dialog box displays the message: *Are you sure you want to delete the selected exception?*

5. Click **OK** to delete the rule.

The system removes the exception and redisplay the Case Assigner Editor.

This chapter provides procedures for configuring the list of available actions. Configuration of actions requires database privileges. Using actions pop-ups, you can document your analysis and close cases. You can take action on a selected case, such as, closing it, taking a follow-up action on it, or assigning it to other users. The following sections are detailed in this chapter:

- [Working with Case Action Settings](#)
- [Configuring Mandatory Action Attributes](#)

Working with Case Action Settings

The following sections defines how to configure case workflows:

- [Understanding Case Workflows](#)
- [Adding New Case Statuses](#)
- [Configuring Case Action Data](#)
- [Configuring Standard Comment Data](#)

Understanding Case Workflows

In general, Case workflows consist of a series of steps and actions. The actions that are available at each step of the workflow determine the next step (or status) in the workflow. With each action, the case can change its status to advance through the workflow.

Defining a Case workflow consists primarily of the following tasks:

1. Create case types, see the [Managing Case Designer](#), for more information.
2. Define case statuses that represent steps in the workflow. For more information, see [Adding New Case Statuses](#).
3. Define actions to be used in the workflow. For more information, see [Configuring Case Action Data](#).
4. Define standard comments that is available in the workflow. For more information, see [Configuring Standard Comment Data](#).

Note: When defining workflows, you specify individual actions or comments available at each step.

Adding New Case Statuses

You can add a new case status by following these steps:

1. Add an entry to the KDD_STATUS table, as follows:

```
insert into KDD_STATUS (STATUS_CD,CAN_NHRIT_FL,VIEWD_BY_OWNER_ACTVY_TYPE_CD,
VIEWD_RESULT_STATUS_CD,CLOSED_STATUS_FL,STATUS_NM) values
('CZZZ','N',null,null,'Y','Closed - Loss Recovered')
```

2. Add an entry to the KDD_CODE_SET_TRNLN table, as follows:

```
insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL, SRC_SYS_CD, CODE_DISP_TX) values
('CaseStatus', 'CZZZ',null, 'Closed - Loss Recovered')
```

Configuring Case Action Data

This section defines how to configure case action. The configured actions will display in UI. You can configure case actions as described in the following subsections:

- [Adding a New Action Category](#)
- [Adding a New Action](#)
- [Mapping New Action to User Role](#)
- [Mapping the New Action to Status](#)
- [Map the New Action to the Case Type](#)

Note: Sections [Mapping New Action to User Role](#), [Mapping the New Action to Status](#), [Map the New Action to the Case Type](#) applicable only for Non-status changing actions. Use PMF for Status changing actions. You can configure these Status changing actions using **Attribute Builder** in PMF. For more information, see the [Configuring Processing Modelling Framework \(PMF\)](#).

Adding a New Action Category

To add a new case action item, follow these steps:

1. Create a new action category by adding a new record in the KDD_ACTION_CAT_CD as follows:

```
insert into KDD_ACTION_CAT_CD (ACTION_CAT_CD,DISPL_NM,DISPL_ORDER_NB,
MANTAS_ACTVY_CAT_FL) values ('REV','Research & Review',40, 'Y')
```

Adding a New Action

To add a new record code, follow these steps:

1. Create a new action code by adding a new record in the KDD_ACTION table as follows:

```
insert into KDD_ACTION (ACTION_ID, ACTION_CATEGORY_CODE, ACTION_NM, ACTION_CD,
ACTION_DESC, LAST_UPDATED_DT, LAST_UPDATED_BY, COMMENTS, ACTION_ORDER, REQ_CMMNT_FL,
DFLT_DUE_DT_LM, REQ_REASN_FL, REQ_DUE_DATE_FL, NEXT_REVIEW_STATUS_CD, REG_TYPE_CD,
REQ_REASN_OWNER_FL, LAST_ASSIGN_REQ, RESOLUTION_ACTION_FL, EXPORT_DIR_REF) values (73,
'REV', 'Reviewed with Account Manager', 'CA73A', 'Reviewed with Account Manager', null,
null, null, 90, 'Y', null, 'N', 'N', 'INV', null, 'N', 'N', null, , null)
```

While adding a new action, the set of supplemental values to be associated with the action should be decided based on the following criteria:

- a. ACTION_CATEGORY_CODE - Category code that identifies the classification of an action. If you want to change the category of an action, you need to change this column accordingly.

b.ACTION_ORDER - Integer that represents the order in which action is performed by the system in the scenario of multiple actions take together. The larger the number the higher the precedence. This allows for multiple actions with differing resulting statuses to be taken at the same time and enforcing that the action with the highest action order will be the one to affect the resulting status. For example, action with resulting status *Followup* has action order 10. It is taken at the same time as action with resulting status Closed that has action order 20. Both actions will be applied and visible in the Audit. But the resulting status will be Closed.

Note: The action order of client-created actions should be less than the action order of system-initiated actions for Re-assignment (CA202A) and Ownership Change (CA103S).

c.NEXT_REVIEW_STATUS_CD - Resulting status code to be set when this action type is performed on an investigation record.

d.REQ_REASN_FL - Indicator of whether this action type requires reassignment of an investigation record.

e.REQ_DUE_DATE_FL - Indicator of whether this action type requires the user to enter a due date on a case.

Note: Unless superseded by another action being taken on the investigation record that has a Closed status as the resulting status based on the lowest order precedence established in the Investigation Status table the provided due date will be applied on the investigation record.

f.REQ_CMMNT_FL - Indicator of whether a comment, either the standard or free-text comment, is required for this action type.

g.REQ_REASN_OWNER_FL Indicator of whether this action type requires reassignment of ownership of a case investigation record.

h. LAST_ASSIGN_REQ - Used by the system to determine the last user who performed this action in the situation where the this recommendation or escalation action is rejected and the case would need to be reassigned back to the last user who took the action. “Y” means that when this action appears on a case previous to a rejection action by another user the user who took this action would become the owner. “N” means this is not a recommend for approval or escalation type action or is not an action that would be used by the system to determine reassignment.

i.RESOLUTION_ACTION_FL - Indicator of whether this action is a resolution action.

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: You can find the highest CASE_ROLE_ACTION_MAP_SEQ used in the table and add 1 to that number while inserting a new record to this table. You can find highest CASE_ROLE_ACTION_MAP_SEQ by running the following query:

```
select max(t. CASE_ROLE_ACTION_MAP_SEQ) from KDD_ROLE_ACTION_MAP t
```

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: You can find the highest CASE_STATUS_ACTION_MAP_SEQ used in the table and add 1 to that number while inserting a new record to this table. We can find highest CASE_STATUS_ACTION_MAP_SEQ by running the below mentioned Query.

```
select max(t. CASE_STATUS_ACTION_MAP_SEQ) from KDD_STATUS_ACTION_MAP t
```

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: You can find the highest CASE_CASETYPE_ACTION_MAP_SEQ used in the table and add (1) to that number while inserting a new record to this table. We can find highest CASE_CASETYPE_ACTION_MAP_SEQ by running the query:

```
select max(t. CASE_CASETYPE_ACTION_MAP_SEQ) from KDD_CASETYPE_ACTION_MAP t
```

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)
```

Configuring Mandatory Action Attributes

You can configure whether or not case actions require a comment, a reassignment, or a due-date. These requirements are configured by setting column values in the KDD_ACTIVITY_TYPE_CD or KDD_ACTION table in the Case Management schema.

Making Comments Mandatory

To specify comments that are mandatory for a case action type, follow these steps:

1. Set the REQ_CMMNT_FL to Y (Yes) in the KDD_ACTION table for a case action type.

For example, if you want to make comments mandatory for a particular case action type, the SQL code should be similar to the following:

```
update KDD_ACTION set REQ_CMMNT_FL = 'Y' where ACTION_ID= 72
```

2. Save your changes to the KDD_ACTION table.

Making Reassignment Mandatory

To specify that a reassignment is mandatory for a case action type, follow these steps:

1. Set the REQ_REASN_FL to Y (Yes) in the KDD_ACTION table case action type.

For example, if you want to make reassignment mandatory for a particular case action type, the SQL code should be similar to the following:

```
update KDD_ACTION set REQ_REASN_FL = 'Y' where ACTION_ID= 72
```

2. Save your changes to the KDD_ACTION table.

Making a Due-Date for an Action Mandatory

To specify that a due-date is mandatory for a case action type, follow these steps:

1. Set the REQ_DUE_DATE_FL to Y (Yes) in the KDD_ACTION table for a case action type.

For example, if you want to make a due date mandatory for a particular case action type the SQL code should be similar to the following:

```
update KDD_ACTION set REQ_DUE_DATE_FL = 'Y' where ACTION_ID = 72
```

2. Save your changes to the KDD_ACTION table.

For Case Action:

```
update KDD_ACTION set DFLT_DUE_DT_LM = 7 where ACTION_ID = 72
```

Note: For specifying a default due date for any action, the DFLT_DUE_DT_LM column of KDD_ACTIVITY_TYPE_CD and KDD_ACTION can be updated with corresponding values respectively for case actions. The value defined represents the number of days which will get added to the current date and set as the due date when the corresponding action is taken.

As an Oracle Financial Services Administrator you can customize features in the Web Application UI. This chapter contains information about configuring session time out.

Configuring the Session Timeout Setting

This section describes the following topics:

- [Configuring the Session Timeout Setting](#)
- [Configuring the Session Timeout Setting for Admin Tools](#)

Configuring the Session Timeout Setting

As an Oracle Financial Services Administrator, you can set the inactive web application users to automatically log off by setting the number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

For more information on how to set the duration before logout for inactive sessions, see the [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

Configuring the Session Timeout Setting for Admin Tools

As Oracle Financial Services Administrator, you can optionally log off inactive Web Application users by establishing a set number of minutes that a user can remain inactive. This results in automatic user log-off that terminates the user's session.

To modify the idle session timeout for idle or inactive users, follow these steps:

1. Open the web.xml file associated with the WebLogic or WebSphere application.

You can find this file in the WEB-INF directory under each Web application in the Oracle Financial Services installation.

2. Modify the XML code within the file that contains `<session-config>` in its `<session-descriptor>` entry.

Do this by setting the `<session-timeout>` part of the entry so that the number of minutes equals the current quantity of minutes of inactivity that result in a logoff.

3. Save the changes.

After setting the parameter to 30 minutes, the edited XML code should look similar to the following:

```
<session-config>
<session-timeout>30</session-timeout>
</session-config>
```


This appendix describes the list of Processes and Tasks used in various application batches.

OBD Application Process

- [Start Batch](#)
- [Load Data from BD to ECM](#)
- [Correlation](#)
- [Scoring](#)
- [Promote to Case](#)
- [Create Case](#)
- [End Batch](#)

Start Batch

To start batch, use BD_ECM_Start_E2E_Batch.

Load Data from BD to ECM

BD_Load_From_LA_To_CA process is used for load data from Landing area to Consolidation area for OBD. This has following four sub processes:

- Loading BD Events
- Entity Surrogate Key Generation for BD
- Oracle Behavior Detection Evented Data Load
- Oracle Behavior Detection Business Data Load

Correlation

BD_Correlation is used to perform correlation on loaded BDevents. This has following two tasks:

- DT_Correlation
- BD_Entity_Sup_Info

Scoring

BD_SCORING is used to perform scoring of OBD events. This has following four sub processes:

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

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

Promote to Case

BD_Promote_To_Case_Decision is used to make the decision if a OBD correlation can be promoted to a case. This is based on defined threshold limit. This has following task. The task type of this is Computation Rule.

- Pre Case Promotion Rule

Create Case

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

- f_generatecaseid
- f_insertcases
- 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_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_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_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_SMRY_MONTH
- t2t_KDD_CASE_LOAN_ACCOUNT
- t2t_KDD_CASE_LOAN
- t2t_KDD_CASE_INSTRUCTION
- CASE_COMPLETION_FLAG

End Batch

BD_ECM_End_E2E_Batch is used for ending the batch execution for BD.

OCS Application Process

Following process are used for this:

- [Start Batch](#)
- [Load Data from CS to ECM](#)
- [Correlation](#)
- [Scoring](#)
- [Promote to Case](#)

- [Create Case](#)
- [End Batch](#)

Start Batch

ECM_Start_E2E_Batch_For_CS process is used to start the batch to move the data from OCS to ECM.

Load Data from CS to ECM

Load_From_CS_To_CA is used for loading the CS data from Landing area to Consolidation area. This has following four sub processes:

- Loading Oracle CS Events: loads the CS events to Consolidation area
- Entity Surrogate Key Generation For Oracle CS
- Evented Data Load for CS
- Business Data Load for CS

Correlation

This is used to perform correlation on loaded CS events.

- DT_CORRELATION

Scoring

Scoring_OCS is used to perform scoring of OCS events. This has following sub process:

- Pre-Case-Scoring For Oracle CS

Promote to Case

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

- Pre Case Promotion Rule

Create Case

Create_Case is used to create a case if a OCS event is promote to case.

End Batch

ECM_End_E2E_Batch_For_CS is used for ending the batch execution for CS.

OKYC Application Process

Following process are used for this:

- [Start Batch](#)
- [Load Data from KYC to ECM](#)
- [Correlation](#)
- [Scoring](#)
- [Promote to Case](#)
- [Create Case](#)
- [Update Case ID](#)
- [End Batch](#)

Start Batch

ECM Start E2E Batch For KYC process is used to start the batch execution to move the data from OKYC to ECM.

Load Data from KYC to ECM

Load_From_OKYC_To_CA process loads OKYC data from Landing area to Consolidation area. This has following four sub processes:

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

Correlation

This is used to perform correlation on loaded KYC events.

- DT_CORRELATION

Scoring

Scoring_OKYC is used to perform scoring of OKYC events. This has following sub process:

- Pre-Case Scoring For Oracle KYC

Promote to Case

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

- POPULATE_P2C_FL_OKYC

Create Case

Create_Case is used to create a case if a OKYC event is promote to case.

Update Case ID

UPD_CaseId_To_OKYC is used for updating the Case IDs to OKYC.

End Batch

ECM_End_E2E_Batch_For_KYC is used for ending the batch execution for KYC.

Third party Application Process

Following process are used for this:

- [Start Batch](#)
- [Load Data from Third Party to ECM](#)
- [Correlation](#)
- [Scoring](#)
- [Promote to Case](#)
- [Create Case](#)
- [End Batch](#)

Start Batch

ECM Start E2E Batch process is used to start the batch execution to move the data from Third party application to ECM.

Load Data from Third Party to ECM

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

- Loading Events: This has following tasks
- Entity Surrogate Key Generation: This has following tasks:

- Evented Data Load
- Derive Wire, Cash and MI Transaction

Correlation

This is used to perform correlation on loaded events.

- DT_CORRELATION

Scoring

This is used to perform scoring of Third Party events, entities and correlation. This has following sub process:

- Entity_Scoring
- Event_Scoring
- Correlation_Scoring
- Pre_Case_Scoring

Promote to Case

Promote_To_Case_Decision is used to make the decision if a Third Party correlation can be promoted to a case. This is based on defined threshold limit.

Create Case

Create_Case is used to create a case if a Third Party event is promote to case.

End Batch

ECM_End_E2E_Batch is used for ending the batch execution.

Configuring Parallel Graph AnalytiX (PGX) Correlation

This appendix describes the configuration activities for Parallel Graph AnalytiX (PGX) Correlation. This appendix covers following sections:

- [Overview](#)
- [Configuring Parallel Graph AnalytiX \(PGX\) Correlation](#)

Overview

PGX is a toolkit for graph analysis - both running algorithms such as PageRank against graphs, and performing SQL-like pattern-matching against graphs, using the results of algorithmic analysis. Algorithms are parallelized for extreme performance. The PGX toolkit includes both a single-node in-memory engine, and a distributed engine for extremely large graphs. Graphs can be loaded from a variety of sources including flat files, SQL and NoSQL databases and Apache Spark and Hadoop; incremental updates are supported.

Configuring Parallel Graph AnalytiX (PGX) Correlation

Perform the following steps to test the PGX configuration:

Note: Ensure that Java_HOME is pointing to Java 8.

1. Login as ECMADMN.
2. Navigate to Common Task. Select Unified Metadata Manager and click Data Integrator Framework.
3. Select Post Load Changes. A new screen is displayed.
4. Click DT_CORRELATION under transformation in the LHS.
5. Click Input Parameters in the RHS.

In External Library Detail section, select External Library, update the value `./correlation.sh` to `./pgxCorrelation.sh`

OFSECM provides utilities that enable you to set up and modify a selection of batch-related database processes. The chapter focuses on the following topics:

- [About Batch Processing Utilities](#)
- [Managing Annual Activities](#)
- [Managing Alert and Case Purge Utility](#)
- [Managing Batch Control Utility](#)
- [The utility returns the batch name to standard output.](#)
- [Managing Data Retention Manager](#)
- [Database Statistics Management](#)
- [Managing Flag Duplicate Alerts Utility](#)
- [Managing Notification](#)
- [Managing Push E-mail Notifications](#)
- [Refreshing Temporary Tables](#)
- [Managing Truncate Manager](#)
- [Managing ETL Process for Threshold Analyzer Utility](#)
- [Managing Deactivate Expired Alert Suppression Rules](#)

About Batch Processing Utilities

Behavior Detection database utilities enable you to configure and perform batch-related system pre-processing and post-processing activities.

- **Managing Alert and Case Purge Utility:** Provides the capability to remove alerts and cases (along with their matches and activities) generated erroneously or which have exceeded the retention policies of the organization.
- **Managing Batch Control Utility:** Manages the start and termination of a batch process (from data management to alert post-processing) and enables access to the currently running batch.
- **The utility returns the batch name to standard output.:** Updates calendars in the OFSBD system based on predefined business days, holidays, and days off or non-business days.
- **Managing Data Retention Manager:** Provides the capability to manage the processing of partitioned tables in Behavior Detection. This utility purges data from the system based on configurable retention period defined in database.
- **Database Statistics Management:** The system uses a script to manage Oracle database statistics. These statistics determine the appropriate execution path for each database query.

- **Managing Flag Duplicate Alerts Utility:** Enables you to run a script daily after the generation of alerts to identify pairs of alerts that are possible duplicates and adds a system comment to each alert.
- **Push E-mail Notification:** Enables you to configure users of the Alert Management subsystem to receive e-mail when alerts are assigned to them.
- **Managing Notification:** Enables you to configure users of Alert Management and Case Management to receive UI notifications based upon actions taken on alerts or cases, to which, they are associated or when the alert or case is nearing a due date.
- **Refreshing Temporary Tables:** Refreshes temporary tables that the behavior detection process uses and estimates statistics for the newly populated tables.
- **Managing Truncate Manager:** Truncates tables that require complete replacement of their data.

Figure 66 illustrates the frequency with which you use these batch-related database utilities when managing activities: daily, weekly, monthly, annually, or as needed.

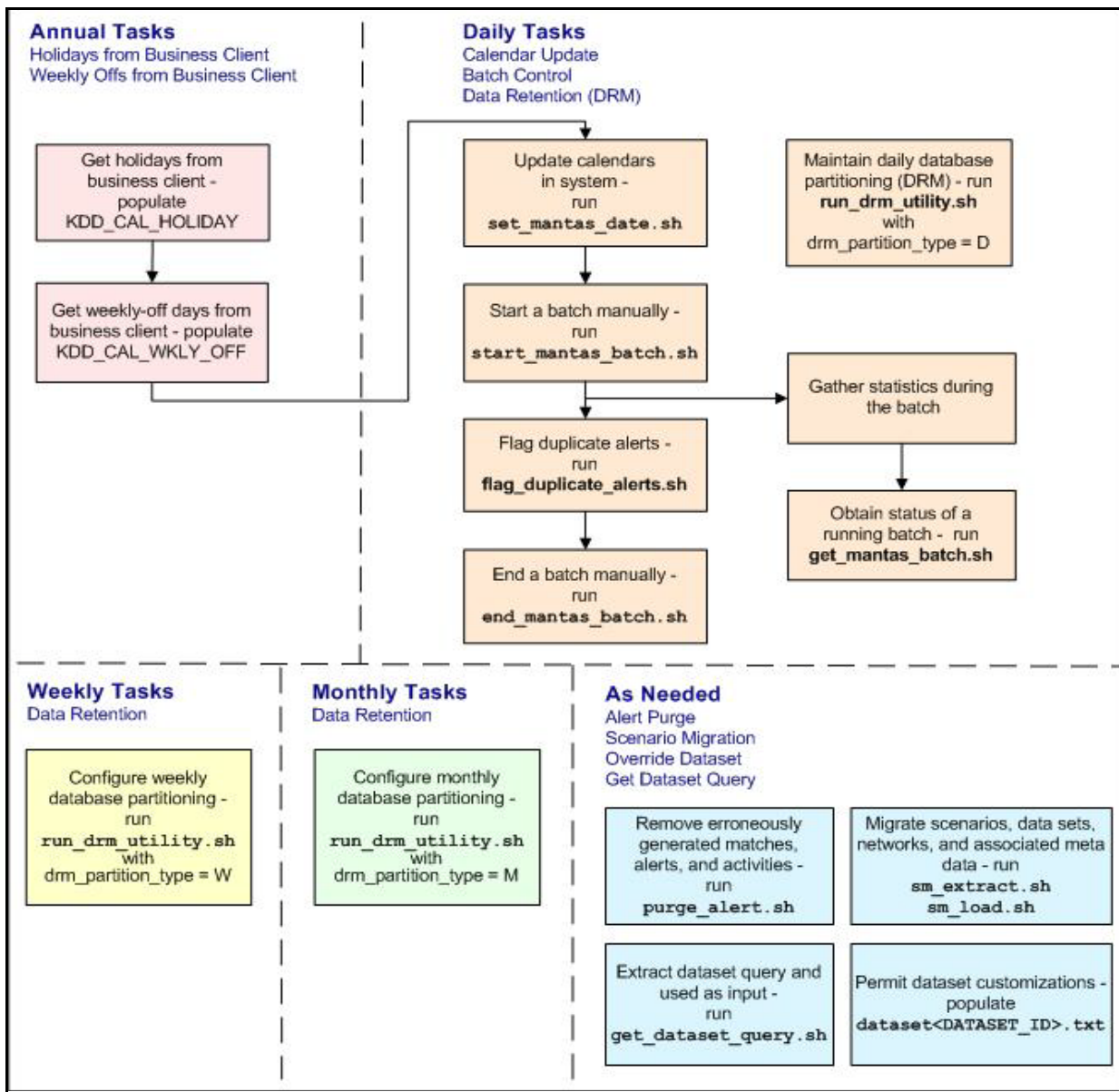


Figure 66. Managing Database Activities with Utilities

Figure 66 illustrates the following:

- Daily tasks are initially dependent on the annual tasks that you perform, such as obtaining holiday and weekly off-days from an Oracle client.
- Daily tasks can include updating Behavior Detection calendars and managing batch processes. You may must configure data partitioning on a daily, weekly, or monthly basis.

Tasks that you perform when needed can include deleting extraneous or invalid matches and alerts, or migrating scenarios and other information from one environment to another , such as from test to production.

Prerequisites for an Administrator User

User must have knowledge of UNIX and LINUX.

Managing Common Resources for Batch Processing Utilities

Configuration files enable the utilities to share common resources such as database configuration, directing output files, and setting up logging activities. Common resources include the following:

- [Install.cfg File](#)
- [Categories.cfg File](#)

Install.cfg File

Configuration information resides in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg configuration file. The configuration file contains modifiable instructions for Oracle database drivers and provides information that each utility requires. It also provides the user name and password that you must connect to the database. In this file, you can modify values of specific utility parameters, change the locations of output files, and specify database details for extraction and data loading.

The install.cfg file contains information unique to each utility and common configuration parameters; headings in the file clearly identify a utility's parameters. You can also modify the current logging configuration, such as activate or deactivate particular logging levels and specify locations for logging entries.

Figure 67 (which appears on the next several pages) provides a sample install.cfg file with common and utility-specific information. Logging information appears at the end of the file. You should ensure that the ATOMIC schema name is in uppercase.

```
# @(#)Copyright (c) 2016 Oracle Financial Services Software Inc. All Rights Reserved.
# @(#) $Id: install.cfg $
#
# This configuration file supports the following database utilities:
#   Calendar Manager
#   Batch Control
#   Truncate Manager
#   Scenario Migration
#   Alert Purge
#   Data Retention Manager
#   Email Notification
#   Data Analysis Tool
(Continued on next page)
```


(Continued from previous page)

```
# The file contains some properties that are common and specific properties for
each
# of the tools.

##### COMMON CONFIGURATION ENTRIES #####

NLS_LENGTH_SEMANTICS=CHAR
database.driverName=oracle.jdbc.driver.OracleDriver
utils.database.urlName=jdbc:oracle:thin:@ofss2221324.in.oracle.com:1521:Ti5012L64
utils.database.username=f802_fccm
utils.database.password=NzBXdzslR43hh0nWkaqYvA==
schema.algorithms.owner=f802_fccm
schema.algorithms.password=NzBXdzslR43hh0nWkaqYvA==
schema.web.owner=f802_fccm
schema.web.password=NzBXdzslR43hh0nWkaqYvA==
schema.report.owner=f802_fccm
schema.report.password=NzBXdzslR43hh0nWkaqYvA==

schema.mantas.owner=f802_fccm
schema.mantas.password=NzBXdzslR43hh0nWkaqYvA==
utils.miner.user=f802_fccm
utils.miner.password=NzBXdzslR43hh0nWkaqYvA==
schema.business.owner=f802_fccm
schema.business.password=NzBXdzslR43hh0nWkaqYvA==
schema.market.owner=f802_fccm
schema.market.password=NzBXdzslR43hh0nWkaqYvA==
utils.data.directory=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data
ingest.user=f802_fccm
ingest.password=NzBXdzslR43hh0nWkaqYvA==

schema.kdd.owner=f802_fccm
schema.kdd.password=NzBXdzslR43hh0nWkaqYvA==
casemng.schema.owner=f802_fccm
casemng.schema.password=NzBXdzslR43hh0nWkaqYvA==
(Continued on next page)
```

(Continued from previous page)

```
##### CALENDAR MANAGER CONFIGURATION #####

# The look back and look forward days of the provided date.
# These values are required to update the KDD_CAL table. The maximum look back or
# forward
# is 999 days.
calendar.lookBack=400
calendar.lookForward=14

##### BATCH CONTROL CONFIGURATION #####

# When ending the batch, age alerts in calendar or business days
age.alerts.useBusinessDays=Y

##### TRUNCATE MANAGER #####

# Specify the database username and password for truncation manager
truncate.database.username=${ingest.user}
truncate.database.password=${ingest.password}

##### SCENARIO MIGRATION CONFIGURATION #####

#### GENERAL SCENARIO MIGRATION SETTINGS

#Specify the flags for whether scoring rules and wrapper datasets need to be
#extracted or loaded
score.include=N
wrapper.include=N

#Specify the Use Code for the scenario. Possible values are 'BRK' or 'EXP'
load.scnro.use=BRK

#If custom patterns exist for a product scenario, set to 'Y' when loading a
#scenario hotfix.
#This should normally be set to 'N'.
load.ignore.custom.patterns=N
```

(Continued on next page)

(Continued from previous page)

```
#Specify the full path of depfile and name of fixfile used for extraction and
loading

#Note : fixfile need not be specified in case of loading
sm.depfile=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/mantas_cfg/dep.
cfg

sm.release=5.7.1

#### EXTRACT

# Specify the database details for extraction
extract.database.username=${utils.database.username}
extract.database.password=${utils.database.password}

# Specify the case schema name for both extraction and load .
caseschema.schema.owner=f802_fccm

# Specify the jdbc driver details for connecting to the source database
extract.conn.driver=${database.driverName}
extract.conn.url=jdbc:oracle:thin:@ofss2221324.in.oracle.com:1521/Ti5012L64

#Source System Id
extract.system.id=

# Specify the schema names for Extract
extract.schema.mantas=${schema.mantas.owner}
extract.schema.case=f802_fccm
extract.schema.business=${schema.business.owner}
extract.schema.market=${schema.market.owner}
extract.user.miner=${load.user.miner}
extract.miner.password=${utils.miner.password}

# File Paths for Extract
```

(Continued on next page)

(Continued from previous page)

```
#Specify the full path in which to place extracted scenarios
extract.dirname=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data

#Specify the full path of the directory where the backups for the extracted
scripts would be maintained
extract.backup.dir=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data/te
mp

#Controls whether jobs and thresholds are constrained to IDs in the product range
(product.id.range.min
# through product.id.range.max). Values are Y and N. If the range is not
restriced, you can use range.check
# to fail the extract if there are values outside the product range.
extract.product.range.only=N
extract.product.range.check=N

#### LOAD

# Specify the jdbc driver details for connecting to the target database
load.conn.driver=${database.driverName}
load.conn.url=${utils.database.urlName}

#Target System ID
load.system.id=Ti5012L64
# Specify the schema names for Load
load.schema.mantas=${schema.mantas.owner}
load.schema.case=f802_fccm
load.schema.business=${schema.business.owner}
load.schema.market=${schema.market.owner}
load.user.miner=${utils.miner.user}
load.miner.password=${utils.miner.password}.
#Directory where scenario migration files reside for loading
load.dirname=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data
# Specify whether threshold can be updated
load.threshold.update=Y
# Specify whether score can be updated
load.score.update=Y
```

(Continued on next page)

(Continued from previous page)

```
# Specify whether or not to verify the target environment on load
verify.target.system=N

##### ALERT PURGE CONFIGURATION #####
# Set the Alert Purge input variables here.
# (use the word "null" as the value of any parameters that are not
#  to be used)
#

# Specify whether or not to consider Matches
limit_matches=N

# Specify whether or not to purge the data
purge=Y

# Specify batch size for which commit should perform
batch_size=5000
job=null
scenario=null
# enter dates, with quotes in the following format:
#   'DD-MON-YYYY HH24:MI:SS'
start_date=null
end_date=null
alert_status=NW

# Specify purge db user
purge.database.user=f802_fccm

# Specify purge db user password.
purge.database.password=

# Specify whether alerts has to be purged or not.
purge_alert_flag=Y
```

(Continued on next page)

(Continued from previous page)

```
# Specify whether fatca cases/assessments has to be purged or not.
purge_fatca_flag=Y

# Specify whether case has to be purged or not.
purge_case_flag=Y

# Specify default rule set.
purge_default_rule_set=

# Specify total number of threads should be used for the process.
purge_threads_no=10

# Specify report directory for report on process performed.
purge_report_directory=

# Specify product version
purge_product_version=
#Base Working Directory required to put the temporary log from Database Server
ap.storedproc.logdir=/tmp

#The common Path required to put the SQL files to execute
commonSQLFilePath=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data
##### DATA RETENTION MANAGER CONFIGURATION #####
#
# Set the Data Retention Manager input variables here.
##
drm_operation=P
drm_partition_type=D
drm_owner=${schema.business.owner}
drm_object_name=A
drm_weekly_proc_fl=N
##### Email Notification #####
#
# The following sections contain information on configuring email
# notification information. If you wish to use Exchange, you must purchase
# Java Exchange Connector, obtain a license and the jec.jar file. The license
```

(Continued on next page)

(Continued from previous page)

```
# file must be placed in the mantas_cfg file, and the jec.jar file must be
# copied to the db_tools/lib directory. Then, edit the file
# db_tools/bin/run_push_email.ksh, uncomment the JEC_JARS= line.
#
#####
# Currently only smtp, smtps, or exchange
email.type=smtp

# Number of notifications that can run in parallel
notification.threads=4

# Max number of active db connections
utils.database.max_connections=4

# From address for sent mails. This is ignored in Exchange mode. If omitted in SMTP
mode, the mail account associated
# with the Unix/Linux account is used.
email.from=

# SMTP settings
email.smtp.host=mailhost.us.oracle.com
# smtp port is usually 25 for smtp, 465 for smtps
email.smtp.port=25
email.smtp.auth=false
email.smtp.user=
email.smtp.password=
email.smtp.useHTML=true
# Exchange settings *** See above for instructions to enable this ***
# Your Exchange administrator should help identify these settings
#
email.exchange.server=
email.exchange.domain=
email.exchange.user=
email.exchange.password=
email.exchange.prefix=Exchange
email.exchange.mailbox=
email.exchange.useSSL=true
email.exchange.useFBA=true
```

(Continued on next page)

(Continued from previous page)

```
email.exchange.useNTLM=false
email.exchange.draftsfoldername=drafts
email.exchange.useHTML=true

#HTML email styles
email.style.header=font-family:Arial, Helvetica, sans-serif;font-size:10pt;
color:black;
email.style.hr=color: #555; background-color: #f00; height: 1px;
email.style.title=font-family:Arial, Helvetica, sans-serif;font-style:
bold;font-size:12pt;
email.style.message=font-family:Arial, Helvetica, sans-serif;font-size:11pt;
email.style.table=font-family:Arial, Helvetica, sans-serif;border:1px solid #000;
border-collapse:collapse;
email.style.th=font-style: bold;border:1px solid #000; border-collapse:collapse;
padding: 4px; background:#C7DAED
email.style.tr=font-size:10pt
email.style.td=border:1px solid #000; border-collapse:collapse; padding: 4px
email.style.footer=font-family:Arial, Helvetica, sans-serif;font-size:10pt;
color:black;
email.style.disclaimer=font-style: italic;

##### PDF ARCHIVE CONFIGURATION #####
# Set the maximum number of pdf export threads.
pdf.archival.maxthreads=3
# Number of alerts/cases per export web service call.
pdf.archival.service.batchsize=5
# URL of the Alert Management service
alertmanagement.service.url=@ALERT_MANAGEMENT_SERVICE_URL@
##### HIGHLIGHTS GENERATION CONFIGURATION #####
#
# Set the default currency code.
#
# See /mantas_cfg/etc/xml/CUR_Currencies.xml for supported currency
# codes.
#
currency.default=USD

##### HDC CONFIGURATION #####
```

(Continued on next page)

(Continued from previous page)

```
#
# Set the maximum number of hdc threads.
#
hdc.maxthreads=1
hdc.batchsize=10000

##### Data Analysis Tool CONFIGURATION #####
#
# Username and password for connecting to the database

dat.database.username=${ingest.user}
dat.database.password=${ingest.password}

# Input file for analysis
dat.analysis.input=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/mantas_
cfg/analysis_aml.xml

# Output file and file format control
dat.analysis.output=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/data/a
nalysis.html

# Valid values for dat.output.format are HTML and TEXT
dat.output.format=HTML
# Delimiter only applies to TEXT output format
dat.output.delimiter=,
##### Execute Query Tool CONFIGURATION #####
#
# Username and password for connecting to the database

eqt.database.username=${ingest.user}
eqt.database.password=${ingest.password}
##### Database Builder Utility Configuration #####
#
# File containing tokens and their value
db_tools.tokenfile=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/mantas_
cfg/db_variables.cfg
```

(Continued on next page)

(Continued from previous page)

```
Oracle.DuplicateRow=1
Oracle.ObjectExists=955,2260,2275,1430,1442,1451,957,1408,2261,1543
Oracle.ObjectDoesNotExist=942,1418,1434,2441,904,4043,1927,2443

dbscript.execution.users=(system|business|mantas|market|miner|ingest|report|kdd|algorithms|case|config|fatca|ctr|kyc|fsdf|dbutil|web)

##### Correlation Migration Utility Configuration #####
#
corrRuleMig.CorrRuleFileNm=
corrRuleMig.loadHistory=Y
aps.service.url=http://:8070/mantas/services/AlertProcessingService
aps.service.user=test
aps.service.user.password=

##### Config Migration Utility Configuration #####
config.filenm.prefix=Config

##### LOG CONFIGURATION #####
#
# Trace SQL exception. Set to "true" for SQL tracing,
# "verbose" to trace low-level JDBC calls
#
com.sra.kdd.tools.database.debug=true
# Specify which priorities are enabled in a hierarchical fashion, i.e., if
# DIAGNOSTIC priority is enabled, NOTICE, WARN, and FATAL are also enabled,
# but TRACE is not.
# Uncomment the desired log level to turn on appropriate level(s).
# Note, DIAGNOSTIC logging is used to log database statements and will slow
# down performance. Only turn on if you need to see the SQL statements being
# executed.
# TRACE logging is used for debugging during development. Also only turn on
# TRACE if needed.
log.fatal=true
log.warning=true
log.notice=true
log.diagnostic=true
```

(Continued on next page)

(Continued from previous page)

```
log.trace=true
log.time.zone=US/Eastern

# Specify whether logging for a particular level should be performed
# synchronously or asynchronously.
log.fatal.synchronous=true
log.warning.synchronous=true
log.notice.synchronous=true
log.diagnostic.synchronous=true
log.trace.synchronous=true

# Specify the format of the log output. Can be modified according to the format
# specifications at:
# http://logging.apache.org/log4j/docs/api/org/apache/log4j/PatternLayout.html
# NOTE: Because of the nature of asynchronous logging, detailed information
# (class name, line number, etc.) cannot be obtained when logging
# asynchronously. Therefore, if this information is desired (i.e. specified
# below), the above synchronous properties must be set accordingly (for the
# levels for which this detailed information is desired). Also note that this
# type of detailed information can only be obtained for Java code.
log.format=%d [%t] %p %m%n

# Specify the full path and filename of the message library.
log.message.library=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/mantas_
_cfg/etc/mantas_database_message_lib_en.dat

# Specify the full path to the categories.cfg file
log.categories.file.path=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/m
antas_cfg/

# Specify where a message should get logged for a category for which there is
# no location property listed above.
# This is also the logging location of the default MANTAS category unless
# otherwise specified above.
# Note that if this property is not specified, logging will go to the console.
log.default.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/
Utilities.log

# Specify the location (directory path) of the mantaslog, if the mantaslog
# was chosen as the log output location anywhere above.
```

(Continued on next page)

(Continued from previous page)

```
# Logging will go to the console if mantaslog was selected and this property is
# not given a value.
log.mantaslog.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/log
s/mantaslog.log

# Specify the hostname of syslog if syslog was chosen as the log output location
# anywhere above.
# Logging will go to the console if syslog was selected and this property is
# not given a value.
log.syslog.hostname=

# Specify the hostname of the SMTP server if an e-mail address was chosen as
# the log output location anywhere above.
# Logging will go to the console if an e-mail address was selected and this
# property is not given a value.
log.smtp.hostname=

# Specify the maxfile size of a logfile before the log messages get rolled to
# a new file (measured in MBs).
# If this property is not specified, the default of 10 MB will be used.
log.max.size=

#NOTE: The values for the following variables need not be changed
# Specify the ID range for wrapper datasets
dataset.wrapper.range.min=113000001
dataset.wrapper.range.max=114000000
```

Figure 67. Sample install.cfg File

Categories.cfg File

In the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg file, you can modify the default location to where you want to direct logging output for each utility. The entries that you make require a specific format; the file contains instructions and examples of correct formatting. Figure 68 provides a sample categories.cfg file.

```
# @(#)Copyright (c) 2016 Oracle Financial Services Software Inc. All Rights Reserved
# @(#) $Id: categories.cfg $
# Common Logging categories configuration for Mantas Database
#
# Specify the log location for messages of a specific category.
# The property name should be of the form: log.category.{CATEGORY_NAME}.location
# If logging to a category that is not specified below, the messages are
# logged to a configurable default location.
# Valid values are console, syslog, eventviewer, mantaslog, an e-mail
# address, or the full path to a file.
# If specifying mantaslog, also specify the property log.mantaslog.location
# with the desired path to the logfile in install.cfg. If running the algorithms,
# use the format job<job #>-datetimestamp for the mantaslog filename.
# For other subsystems, the format is mantaslog-datetimestamp.
#
# NOTE: Category names cannot contain the following reserved words: fatal,
# warning, notice, diagnostic, trace, category, or location.
# List multiple locations for each property by using a comma delimiter.
#
# NOTE: These are commented out because Mantas does not currently route by
# category. Entries are placed in the configured default location in install.cfg.
# These can be uncommented and modified if routing by category is necessary.
#
log.category.PURGE_UTIL.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_
/logs/purge.log
log.category.BATCH_CONTROL.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/
ols/logs/batch_control.log
log.category.CALENDAR_MANAGER.location=/scratch/ofsaadb/BD802_Final/BD802FL/databa
_tools/logs/calendar_manager.log
log.category.DATA_RETENTION_MANAGER.location=/scratch/ofsaadb/BD802_Final/BD802FL/
ase/db_tools/logs/DRM_Utility.log
log.category.TRUNCATE_MANAGER.location=/scratch/ofsaadb/BD802_Final/BD802FL/databa
_tools/logs/truncate_manager.log
log.category.COMMON_UTILITIES.location=/scratch/ofsaadb/BD802_Final/BD802FL/databa
db_tools/logs/common_utilities.log
```

(Continued on next page)

(Continued from previous page)

```
log.category.EXTRACT.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.LOAD.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.REFRESH_TEMP_TABLE.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/refresh_temp_table.log
log.category.RUN_STORED_PROCEDURE.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/run_stored_procedure.log
log.category.GET_DATASET_QUERY.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/get_dataset_query.log
log.category.HDC.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/hdc.log
log.category.PUSH_EMAIL.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/push_email.log
log.category.HIGHLIGHT_GENERATOR.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/highlight_generator.log
log.category.REPORT.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/report.log
log.category.DATA_ANALYSIS_TOOL.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/data_analysis_tool.log

log.category.DB_BUILDER.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/db_builder.log
log.category.DB_BUILDER_SQL.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/db_builder.log,/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/db_builder_sql.log

log.category.CORRRULEMIGRATIONUTIL_EXTRACT.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.CORRRULEMIGRATIONUTIL_LOAD.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.CONFIGURATIONMIGRATIONUTIL_EXTRACT.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.CONFIGURATIONMIGRATIONUTIL_LOAD.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.ARCHIVE_PDF.location=/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/pdf_archive.log
# Specify the location of messages of a specific severity and category.
# The valid values are the same as for category.
# List multiple locations for each property by using a comma delimiter.
```

(Continued on next page)

(Continued from previous page)

```
# If an entry for a severity does not appear here, the message is logged to
# the location specified for the category by the above property. If that
# does not exist, it is logged to the configured default location in install.cfg.
#
# NOTE: The entry below is just an example. It is commented out because Mantas
# does not route by category/severity. These can be uncommented and modified if
# routing by category/severity is necessary.
#
#log.EXAMPLE_CATEGORY.warning.location=syslog

log.category.DB_BUILDER.notice.location=console
log.category.ARCHIVE_PDF.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/pdf_archive.log

log.category.CORRRULEMIGRATIONUTIL_LOAD.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log

log.category.CORRRULEMIGRATIONUTIL_LOAD.fatal.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.CORRRULEMIGRATIONUTIL_EXTRACT.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.CORRRULEMIGRATIONUTIL_EXTRACT.fatal.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.CONFIGURATIONMIGRATIONUTIL_LOAD.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.CONFIGURATIONMIGRATIONUTIL_LOAD.fatal.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/load.log
log.category.CONFIGURATIONMIGRATIONUTIL_EXTRACT.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log
log.category.CONFIGURATIONMIGRATIONUTIL_EXTRACT.fatal.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/extract.log

log.category.PURGE_UTIL.notice.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/purge.log
log.category.PURGE_UTIL.warning.location=console,
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/purge.log
log.category.PURGE_UTIL.fatal.location=/scratch/ofsaadb/BD802_Final/BD802FL/datab
ase/db_tools/logs/purge.log
log.category.PURGE_UTIL.trace.location=/scratch/ofsaadb/BD802_Final/BD802FL/datab
ase/db_tools/logs/purge.log
```

Figure 68. Sample Logging Information in the categories.cfg File

Configuring Console Output

Figure 69 displays a section of the sample `categories.cfg` file from Figure 68.

Note: The log routing information is in bold text.

```
log.category.PURGE_UTIL.notice.location=console,  
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/purge.log  
log.category.PURGE_UTIL.warning.location=console,  
/scratch/ofsaadb/BD802_Final/BD802FL/database/db_tools/logs/purge.log  
log.category.PURGE_UTIL.fatal.location=/scratch/ofsaadb/BD802_Final/BD802FL/databa  
b_tools/logs/purge.log  
log.category.PURGE_UTIL.trace.location=/scratch/ofsaadb/BD802_Final/BD802FL/databa  
b_tools/logs/purge.log
```

Figure 69. Sample Log Routing Information

The bolded text in the above example (**console**) implies that a specific utility displays logging information at the console in addition to recording the information in the appropriate log file. In Figure 69, Alert and Case Purge and Calendar Manager display relevant utility information in addition to logging it.

Note: If an entry in the `categories.cfg` file does not already include this information, you must add it manually, including the comma.

Managing Annual Activities

OFSBD requires that you perform certain calendar management tasks at least annually: loading holidays and weekly off-days from an Oracle client. This ensures that OFSBD has the necessary information for populating its own business calendars.

This section covers the following topics:

- [Loading Holidays](#)
- [Loading Non-business Days](#)

Loading Holidays

On an annual basis, you must populate holidays for the upcoming calendar year into the Behavior Detection KDD_CAL_HOLIDAY database table. This ensures that the table contains holidays for at least the next year. Figure 70 provides an example of a SQL script for loading the table.


```

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '01/01/2017',
'MM/DD/YYYY'), 'New Year's Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '01/16/2017',
'MM/DD/YYYY'), 'Martin Luther King Jr.'s Birthday - 2017',
'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '02/20/2017',
'MM/DD/YYYY'), 'President's Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '04/14/2017',
'MM/DD/YYYY'), 'Good Friday - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '05/29/2017',
'MM/DD/YYYY'), 'Memorial Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '07/04/2017',
'MM/DD/YYYY'), 'Independence Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '09/04/2017',
'MM/DD/YYYY'), 'Labor Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '11/22/2017',
'MM/DD/YYYY'), 'Thanksgiving Day - 2017', 'C');

INSERT INTO KDD_CAL_HOLIDAY ( CLNDR_NM, CLNDR_DT, HLDY_NM,
HLDY_TYPE_CD ) VALUES ( 'SYSCAL', TO_DATE( '12/25/2017',
'MM/DD/YYYY'), 'Christmas Day - 2017', 'C');

```

Figure 70. Sample KDD_CAL_HOLIDAY Table Loading Script

The following table describes the contents of the KDD_CAL_HOLIDAY table.

Table 38. KDD_CAL_HOLIDAY

Column Name	Description
CLNDR_NM	Specific calendar name.
CLNDR_DT	Date that is a holiday.
HLDY_NM	Holiday name , such as Thanksgiving or Christmas.
HLDY_TYPE_CD	Indicates whether the business is Closed (C) or Shortened (S).
SESSN_OPN_TM	Indicates the opening time of the trading session for a shortened day. The format is HHMM.
SESSN_CLS_TM	Indicates the closing time of the trading session for a shortened day. The format is HHMM.
SESSN_TM_OFFSE T_TX	Indicates the timezone offset for SESSN_OPN_TM and SESSN_CLS_TM.

When the system runs the `set_mantas_date.sh` script, it queries the KDD_CAL_HOLIDAY table for the maximum date for each calendar in the table.

Note: If the maximum date is less than 90 days ahead of the provided date, the process logs a warning message that the specific calendar's future holidays need updating. If any calendars have no holiday records, the system logs a Warning message that the specific calendar has no recorded holidays for the appropriate date range.

Loading Non-business Days

After obtaining non-business days (or weekly off-days; typically Saturday and Sunday) from an Oracle client, load this information for the upcoming calendar year into the KDD_CAL_WKLY_OFF table.

The following text provides an example of an SQL script for loading the table.:

```
INSERT INTO KDD_CAL_WKLY_OFF (CLNDR_NM, DAY_OF_WK) VALUES (
  'SYSCAL', 1);

INSERT INTO KDD_CAL_WKLY_OFF (CLNDR_NM, DAY_OF_WK) VALUES (
  'SYSCAL', 7);

COMMIT;
```

Figure 71. Sample KDD_CAL_WKLY_OFF Table Loading Script

Note: By default, the system identifies Saturdays and Sundays as non-business days in the system calendar (SYSCAL).

The following table describes the contents of the KDD_CAL_WKLY_OFF table.

Table 39. KDD_CAL_WKLY_OFF

Column Name	Description
CLNDR_NM	Specific calendar name.
DAY_OF_WK	Value that represents the day of the week: Sunday=1, Monday=2, Tuesday=3, Wednesday=4, Thursday=5, Friday=6, Saturday=7.

Note: If the table does not contain records for any calendar in the list, the system logs a Warning message that the specific calendar contains no weekly off-days.

Managing Alert and Case Purge Utility

The ingestion of certain data can result in the creation of false matches, alerts, and activities. While correction and data re-ingestion is possible, the system does not remove these erroneously generated matches, alerts, and activities automatically.

There may also be cases when the alerts or cases have been residing in the database due to the retention policies imposed by the regulatory bodies, or the internal policies of the respective organization.

The Alert and Case Purge Utility enables you to identify and remove such matches, alerts and cases, and activities selectively, based on a number of parameters (like the Behavior Detection Job ID, Behavior Detection Scenario ID, Behavior Detection Scenario Class, or a date range with optional alert status codes). Additional parameters enable you to simulate a purge run to determine all found matches, alerts, and activities using the input parameters. You can also limit the alerts in the purge process only to those that contain false matches.

The utility consists of a UNIX shell script, Java executables, a XML File and a configuration file in which you define the process parameters to use in the purge processing. The system directs output to a configurable log file; processing appends this log with information about subsequent executions of the scripts.

This section covers the following topics:

- [Directory Structure](#)
- [Logs](#)
- [Precautions](#)
- [Using the Alert and Case Purge Utility](#)
- [Sample Alert And Case Purge Processes](#)

Directory Structure

The following table describes the directory structure for the Alert and Case Purge Utility.

Table 40. Alert and Case Purge Utility Directory Structure

Directory	Description
bin/	Contains executable files, including the <code>run_alert_purge.sh</code> shell script.
lib/	Contains required class files in <code>.jar</code> format.
mantas_cfg/	Contains configuration files, such as <code>install.cfg</code> and <code>categories.cfg</code> , in which you can configure properties and logging attributes.
logs/	Keeps the <code><OFSAAI Installed Directory>/database/db_tools/logs/purge.log</code> file that the utility generates during execution.
data/	Keeps <code>.sql</code> files for execution.
.xml	Contains the Purge Rules Configuration File (<code>PurgeRules.xml</code>), which is used for configuring the Alert and Case purge rules.

Logs

As the Alert and Case Purge Utility performs alert detection activities, it generates a log that it enters in the <OFSAAI Installed Directory>/database/db_tools/logs/purge.log file (the logging process time-stamps all entries). The log file contains relevant information such as status of the purge processing, log-relevant information, and error records.

You can modify the current logging configuration for the Alert and Case Purge Utility in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg and categories.cfg files. For more information about logging in these configuration files, Refer to *Managing Common Resources for Batch Processing Utilities* on page 158 and Appendix A, *Logging*, on page 235 for more information.

Precautions

You use the utility to rid the system of falsely-generated matches and alerts or cases. Other than recorded information in the <OFSAAI Installed Directory>/database/db_tools/logs/purge.log file, the system does not capture audit information for this process. The utility does not update other alerts' prior counts as a result of purging alerts.

Note: The utility also purges any alert or case which is used to trigger Auto Suppression or establish Trusted Parties. However, this would not affect the Suppression Rule or the Trusted Pair except that the kdd_auto_suppr_alert.trgr_alert_id, kdd_trusted_pair.trgr_alert_id, or kdd_trusted_pair.trgr_case_id columns are set to a null value

Note: Run the Alert and Case Purge Utility one process at a time. Multiple, simultaneous executions of the utility may lead to unexpected results and compromise the relational integrity of match, alert, and action data. When no users are editing or viewing any of the alerts, actions, or associated information (including matches derived from the alerts and actions specified, alerts derived from the specified actions, and actions derived from the specified alerts). However, you can run the utility during editing or viewing of other alerts and related information. You can also run the utility during alert post-processing, subject to time constraints.

Using the Alert and Case Purge Utility

The Alert and Case Purge Utility is not part of an automated batch process. You run this manual process only when necessary (Refer to Figure 66). The following sections describe configuring and executing the utility, as well as the utility's process flow:

- [Configuring the Alert and Case Purge Utility](#)
- [Executing the Alert and Case Purge Utility](#)
- [Processing for Purging](#)

Configuring the Alert and Case Purge Utility

To configure the Alert and Case Purge Utility, follow these steps:

1. Navigate to the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file contains common configuration information that the Alert and Case Purge Utility and other utilities require for processing (Refer to Figure 67).
2. Refer the following sample section from the install.cfg file for configuration information specific to this utility:

```
##### ALERT PURGE CONFIGURATION #####
# Set the Alert Purge input variables here.
# (use the word "null" as the value of any parameters that are not
#  to be used)
#
# Specify whether or not to consider Matches
limit_matches=N
# Specify whether or not to purge the data
purge=Y
# Specify batch size for which commit should perform
batch_size=5000
job=null
scenario=null
# enter dates, with quotes in the following format:
#  'DD-MON-YYYY HH24:MI:SS'
start_date=null
end_date=null
alert_status=NW
# Specify purge db user
purge.database.user=f802_fccm
```

(Continued on next page)

(Continued from previous page)

```
# Specify purge db user password.
purge.database.password=

# Specify whether alerts has to be purged or not.
purge_alert_flag=Y

# Specify whether fatca cases/assessments has to be purged or not.
purge_fatca_flag=Y

# Specify whether case has to be purged or not.
purge_case_flag=Y

# Specify default rule set.
purge_default_rule_set=

# Specify total number of threads should be used for the process.
purge_threads_no=10

# Specify report directory for report on process performed.
purge_report_directory=

# Specify product version
purge_product_version=

#Base Working Directory required to put the temporary log from Database Server
ap.storedproc.logdir=/tmp
```

Figure 72. Configuration Information

Note: Not specifying a value of *null*, such as leaving a value blank, in this section of the `install.cfg` file causes undesirable results.

The following table describes required and optional parameters for this utility.

Table 41. Alert and Case Purge Utility Parameters

Parameter	Description
purge	Determines how the utility performs processing, depending on the specified value: <ul style="list-style-type: none"> ● N (default): Performs all processing up to the point of the purge. The utility identifies resulting matches, alerts, and actions, but performs no purging. ● Y: Performs the above in addition to purging matches, alerts, and actions.
limit_matches	Identifies restrictions on the matches to delete: <ul style="list-style-type: none"> ● Y (default): If a match that you want to delete is part of an alert that contains matches that you do not want to delete, do not delete this match either (applies to multi-match alerts). ● N: Deletes all selected matches for purging based on the input criteria. The utility deletes only alerts and associated actions that exclusively contain matches to be purged. <p>Note: The system purges matches that do not relate to alerts, regardless of the value of <code>limit_matches</code>.</p>
batch_size	<i>Optional:</i> Sets the batch size of purge actions to minimize log space use. Specifying a non-positive value or specifying no value uses the default of 5,000 rows.
purge_alert_flag	Determines whether or not the utility would purge alerts, depending on the specified value: <ul style="list-style-type: none"> ● N: Does not purge the alerts irrespective of whether or not they identified according to the purge rule being used. This may be used when purging only the cases. ● Y (default): Purges the alerts as identified by the purge rule used to perform the purge operation.
purge_case_flag	Determines whether or not the utility would purge cases, depending on the specified value: <ul style="list-style-type: none"> ● N: Does not purge the cases irrespective of whether or not they identified according to the purge rule being used. This may be used when purging only the cases. ● Y (default): Purges the cases as identified by the purge rule used to perform the purge operation.
purge_default_rule_set	<i>(Optional)</i> Indicates the default set of rules to be used for purging alerts/cases. You may either specify the purge rules to be used against this parameter, or pass the name of the specific purge rules) as command line parameters You may specify a single purge rule, or a comma separated list of purge rules to be used as default when no other purge rule is provided from the command line.
purge_threads_no	<i>(Optional)</i> Identifies the number of concurrent threads to create for purging the alerts to optimize the performance. Specifying a non-positive value or specifying no value uses the default of 10 threads.
purge_report_directory	Identifies the absolute path to the directory where the purge activity report should be generated. The report file name has a name similar to <code>Purge_<YYYYMMDD.HH.MM.SS>.txt</code> . Here <code><YYYYMMDD.HH.MM.SS></code> represents current timestamp when the utility was executed.
purge_product_version	Identifies the OFSBD Product Version installed by the client.

The <OFSAAI Installed
Directory>/database/db_tools/mantas_cfg/etc/xml/PurgeRules.xml file contains purge rules

configuration information that the Alert and Case Purge Utility requires for processing. The following sample section from the `PurgeRules.xml` file provides configuration information for this utility.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:RuleSet xmlns:xs="http://namespaces.mantas.com/RuleSet">
  <Alert>
    <Rule id="1">
      <IdentifierList>286,4565,4537</IdentifierList>
      <ScenarioIdList>114697002</ScenarioIdList>
      <ScenarioClassList>CR</ScenarioClassList>
      <CreateDate>
        <StartDate>2011-05-25</StartDate>
        <EndDate>2011-05-25</EndDate>
      </CreateDate>
      <DomainCode>MTS</DomainCode>
      <BatchId>2</BatchId>
      <ThresholdSetIds>118745206,118710066</ThresholdSetIds>
      <LastActionDate>
        <StartDate>2016-05-25</StartDate>
        <EndDate>2016-05-25</EndDate>
      </LastActionDate>
      <Status>CL</Status>
      <JobIds>102202</JobIds>
    </Rule>
  </Alert>
  <Case>
    <Rule id="2">
      <IdentifierList>CA51300004,CA3773,CA3757,CA3766</IdentifierList>
      <CaseTypeList>FR_EE,FR_ON</CaseTypeList>
      <CreateDate>
        <Age>1Y</Age>
      </CreateDate>
      <LastActionDate>
        <StartDate>2016-06-22</StartDate>
        <EndDate>2016-06-22</EndDate>
      </LastActionDate>
    </Rule>
  </Case>
</RuleSet>
```

(Continued on next page)

Figure 73. Configuration Information

(Continued from previous page)

```
</LastActionDate>
  </Rule>
</Case>
</xs:RuleSet>
```

Figure 74. Configuration Information

The following table describes the Purge Rules Configuration Parameters.

Table 42. Alert and Case Purge Utility Parameters

Parameter	Description
Alert/Case	Identifies and encapsulates the purge rules for Alerts/Cases. You may define any number of purge rules for both alerts and cases.
Rule	Identifies a set of rules to be used for purging Alert/Case Information. All Alert and Case purge rules defined in this file must be provided a unique positive integer ID (as specified against the ID attribute). The value provided against the ID attribute is used by the utility to identify the rules to be used for carrying out the purge operations. Note: Not specifying a unique value for the ID attribute may lead to undesirable results.
IdentifierList	Identifies a list of Alert and Case IDs to be purged. You may specify more than one alert or case ID by separating them by comma.
ScenarioIdList	Identifies a list of Scenario IDs for which the alerts are to be purged. You may specify more than one Scenario ID by separating them by comma. Note: This property is specific to alerts only. This should not be specified for cases
ScenarioClassList	Identifies a list of Scenario Class for which the alerts are to be purged. You may specify more than one Scenario Class by separating them by comma. Note: This property is specific to alerts only. This should not be specified for cases

Table 42. Alert and Case Purge Utility Parameters (Continued)

Parameter	Description
CreateDate	<p>Identifies the dates to be considered for purging the alerts or cases by their creation date. The date range may be provided in terms of Start Date or End Date, or the Age of the Alert or Case calculated from the current day/month/year.</p> <ul style="list-style-type: none"> ● StartDate: Identifies the date from when the alerts/cases are to be considered for purging. The date should be provided in the format YYYY-MM-DD. ● EndDate: Identifies the date up to which the alerts are to be purged. The date should be provided in the format YYYY-MM-DD ● Age: Identifies the age of the Alert/Case to be purged relative to the current date/month/year. Acceptable values for this parameter constitutes a non-negative number followed by D (Days), M (Months) or Y (Years). If we specify age of a record is 1 Day means it should complete 1 day in the database. That is from current day to yesterday. <p>The example below gives more details: (Assume Current date: 21 NOV 2012)</p> <p>Case1:</p> <p>(i) if age = 1Y: Date range would be considered: 21 NOV 2012 to 21 NOV 2011 (includes both days)</p> <p>(ii) if age = 5Y: Date range would be considered: 21 NOV 2012 to 21 NOV 2007 (includes both days)</p> <p>Case2:</p> <p>(i) if age = 1M: Date range would be considered: 21 NOV 2012 to 21 OCT 2012 (includes both days)</p> <p>(ii) if age = 5M: Date range would be considered: 21 NOV 2012 to 21 JUN 2012 (includes both days)</p> <p>Case3:</p> <p>(i) if age = 1D: Date range would be considered: 21 NOV 2012 to 20 NOV 2012 (includes both days)</p> <p>(ii) if age = 5D: Date range would be considered: 21 NOV 2012 to 16 NOV 2012 (includes both days)</p> <p>(iii) if age = 0D: Date range would be considered: 21 NOV 2012 to 21 NOV 2012 (that is, current date only)</p> <p>Note: If only EndDate is specified, utility would consider it as on or before that date, in case of only StartDate being provided, utility would consider it as on or after that date. In-case both dates are specified utility would consider both the dates and the dates in between them.</p>
BatchId	<p>Identifies the list of Batch IDs for which the alerts should be purged.</p> <p>Note: This property is specific to alerts only. This should not be specified for cases.</p>
DomainCode	<p>Identifies the list of domains for which the alerts should be purged. Acceptable values include:</p> <ul style="list-style-type: none"> ● MTS ● TST ● PFM ● NVZ <p>Note: This property is specific to alerts only. This should not be specified for cases.</p>

Table 42. Alert and Case Purge Utility Parameters (Continued)

Parameter	Description
LastActionDate	<p>Identifies the dates to be considered for purging the alerts and cases by the date on which last action was taken on them. The date range may be provided in terms of Start Date or End Date, or the Age of the Alert or Case calculated from the current day/month/year.</p> <ul style="list-style-type: none"> ● StartDate: Identifies the date from when the alerts/cases are to be considered for purging. The date should be provided in the format YYYY-MM-DD ● EndDate: Identifies the date up to which the alerts are to be purged. The date should be provided in the format YYYY-MM-DD ● Age: Identifies the age of the Alert or Case to be purged relative to the current date/month/year. Acceptable values for this parameter constitute a non-negative number followed by D (Days), M (Months) or Y (Years). If we specify age of a record is 1 Day means it should complete 1 day in the database. That is from current day to yesterday. <p>The example below gives more details: (Assume Current date: 21 NOV 2012)</p> <p>Case1:</p> <p>(i) if age = 1Y: Date range would be considered: 21 NOV 2012 to 21 NOV 2011 (includes both days)</p> <p>(ii) if age = 5Y: Date range would be considered: 21 NOV 2012 to 21 NOV 2007 (includes both days)</p> <p>Case2:</p> <p>(i) if age = 1M: Date range would be considered: 21 NOV 2012 to 21 OCT 2012 (includes both days)</p> <p>(ii) if age = 5M: Date range would be considered: 21 NOV 2012 to 21 JUN 2012 (includes both days)</p> <p>Case3:</p> <p>(i) if age = 1D: Date range would be considered: 21 NOV 2012 to 20 NOV 2012 (includes both days)</p> <p>(ii) if age = 5D: Date range would be considered: 21 NOV 2012 to 16 NOV 2012 (includes both days)</p> <p>(iii) if age = 0D: Date range would be considered: 21 NOV 2012 to 21 NOV 2012 (that is, current date only)</p> <p>Note: If only EndDate is specified, utility would consider it as on or before that date, in case of only StartDate being provided, utility would consider it as on or after that date. If both dates are specified utility would consider both the dates and the dates in between them.</p>
Status	<p>Identifies a list of Status Codes against which the Alert or Case should be purged. You may specify more than one Status Code by separating them by comma.</p>
JobIds	<p>Identifies the list of Job IDs for which the alerts should be purged. You may specify more than one Job ID by separating them by comma.</p> <p>Note: This property is specific to alerts only. This should not be specified for cases.</p>
ThresholdSetIds	<p>Identifies the list of Threshold Set IDs for which the alerts should be purged. You may specify more than one Threshold Set ID by separating them by comma.</p> <p>Note: This property is specific to alerts only. This should not be specified for cases.</p>

Executing the Alert and Case Purge Utility

To execute the Alert and Case Purge Utility, follow these steps:

1. Verify that the Behavior Detection database is operational:

```
tnsping <database instance name>
```

2. Verify that the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg configuration file contains the correct source database connection and logging information.

3. Access the directory where the shell script resides:

```
cd <OFSAAI Installed Directory>/database/db_tools/bin
```

4. Start the alert and case purge shell script:

```
run_alert_purge.sh -purge
```

Executing this command sets the environment classpath and starts the utility. You may also pass command line arguments to the utility, and execute the utility in any of the following ways:

- You may pass a list of purge rules (as configured in PurgeRules.xml file) separated by a comma (,) following the convention of alert_rule_<i0> for alert-related rules and case_rule_<i0> for case-related rules; here i0 is an integer representing the corresponding rule number in the purgeRules.xml file.

```
./run_alert_purge.sh -purge alert_rule_<i0>,alert_rule_<i1>,case_rule_<i2>...
```

- You may instruct the utility not to purge any alerts, but only cases, and vice-versa. If the value passed is 'alert=N' the utility considers this as no to purge alerts

```
./run_alert_purge.sh -purge alert=N
```

If the value passed is 'case=N' the utility considers this as no to purge cases

```
./run_alert_purge.sh -purge case=N
```

You may instruct the utility only to simulate the purge process and not purge the alerts and cases by passing a command line parameter 'test=Y'. In this case, the utility considers this as running in test mode and generates the report of alerts and cases that would have purged.

```
./run_alert_purge.sh -purge test=Y
```

You can provide all these parameters or a combination of these parameters irrespective of order, once at a time, to the utility as shown in the example below:

```
./run_alert_purge.sh -purge case=N alert_rule_<i0>,alert_rule_<i1> test=Y
```

Note: If the utility is executed without any command line arguments, the utility considers purging the alerts and cases as configured in the install.cfg file.

Processing for Purging

The process for purging is as follows:

1. Once you execute the run_alert_purge.sh script, the Alert and Case Purge Utility generates a listing of actions, matches, and alerts or cases that it must purge according to the rules specified at the command line, or the default rule set configured in the install.cfg file.
2. After the script is executed, the actions, alerts, and cases are recorded in the <OFSAAI Installed Directory>/database/db_tools/logs/purge.log file.

Note: The utility presumes that you have determined the input parameters to specify what matches, alerts, and actions to purge. The utility does not check against the data to verify what it should purge.

Note: To capture the SQL statements naming, set `log.diagnostic=true` in the `install.cfg`.

3. The utility then purges actions, then matches, then alerts, according to the contents of the `KDD_AP_ACTION`, `KDD_AP_MATCH`, and `KDD_AP_ALERT` tables.
4. The utility captures purging results and any errors in the `purge.log` and a report (having the naming convention `Purge_<YYYYMMDD.HH.MM.SS>.txt`) files.

Note: The Alert and Case Purge Utility purges data from archive tables for erroneous alerts. Also, the system does not update score and previous match count values associated with generated matches and alerts since creation of the erroneous matches.

Automatic Restart Capability

The Alert and Case Purge Utility has an automatic restart capability in that any interruption in the purge processing resumes at that point, regardless of the input parameters. The system documents log information about the interruption in the `<OFSAAI Installed Directory>/database/db_tools/logs/purge.log` file. Otherwise, any restart that has not progressed to the purge component behaves as a new processing run.

The restart capability allows interrupted purges to resume at a convenient point, but is unable to execute all desired input parameters.

Sample Alert And Case Purge Processes

This section includes examples of the Purge Alerts process based on input parameters. These example patterns are also applicable for filtering cases.

Example 1

If user specifies only one rule 'xyz' for purging alerts and assume it as follows:

```
<Alert>
.....
    <Rule id="xyz">
        <IdentifierList>3775,3731,3669,3663</IdentifierList>
    <Status>CL</Status>
</Rule>
.....
</Alert>
```

The utility filters in the existing alerts for IDs 3775,3731,3669,3663 and* status having Closed (CL).

Here and* specifies the logical and operation specified by sql.

In this case, the alert has closed status among the existing alert IDs of (3775, 3731, 3669, and 3663).

```
<Alert>
.....
    <Rule id="xyz">
        <IdentifierList>3775,3731,3669,3663</IdentifierList>
```

```
<Status>CL</Status>
<ScenarioIdList>114697002, 114690106</ScenarioIdList>
<JobIds>456789</JobIds>
</Rule>
.....
</Alert>
```

The utility filters in the existing alerts for IDs 3775,3731,3669,3663 and* having status Closed (CL) and* having Scenario IDs 114697002,114690106 and having Job Id 456789.

Example 2

If user specifies multiple rules for purging:

```
<Alert>
.....
<Rule id="pqr">
<IdentifierList>3775, 3731,3669,3663</IdentifierList>
<Status>CL</Status>
<JobIds>456789</JobIds>
</Rule>
<Rule id="xyz">
<ScenarioIdList>114697002,114690106</ScenarioIdList>
<CreateDate>
<StartDate>2011-05-25</StartDate>
<EndDate>2011-05-29</EndDate>
</CreateDate>
</Rule>
.....
</Alert>
```

The utility prepares a query to filter alerts so that rule 'pqr' (fetches alerts as per the single rule de-scribed above) or* rule 'xyz' (fetches alerts as per the single rule described above) or*... That is, union of the alerts from all the rules would be filtered.

Here or* specifies the logical or operation specified by sql.

Managing Batch Control Utility

The Batch Control Utility enables you to manage and record the beginning and ending of a Behavior Detection batch process. It also enables you to access the currently running batch. You control the process through a job scheduling tool such as Maestro or Unicenter Autosys.

This utility consists of a Java file that resides in the directory <OFSAAI Installed Directory>/database/db_tools/lib and UNIX script files that reside in <OFSAAI Installed Directory>/database/db_tools/bin:

- `start_mantas_batch.sh` starts the batch process.
- `end_mantas_batch.sh` ends the batch process.
- `get_mantas_batch.sh` obtains the name of the currently running batch.

The utility also uses common parameters in the configuration file <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg (Refer to *Install.cfg File* on page 158 for more information).

This section covers the following topics:

- [Batches in Behavior Detection](#)
- [Directory Structure](#)
- [Logs](#)
- [Using the Batch Control Utility](#)

Note: To calculate the age in business days versus calendar days, verify that the `age.alerts.useBusinessDays` setting in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file has a value of Y (yes).

Batches in Behavior Detection

Except for the Alert Management subsystem, batches govern all other activity in the Behavior Detection system. A batch provides a method of identifying a set of processing. This includes all activities associated with data management and Behavior Detection.

Deployment of a system can be with a single batch or with multiple batches. You can use multiple batches to permit intra-day processing to generate results several times per day, or to separate processing based on servicing multiple time zones.

Behavior Detection provides two types of batches:

- **End-of-day:** Represent processing at the completion of a business day for a set of data. Some processes are only appropriate for end-of-day batches. For example, daily activity summary derivations and calculating alert ages are activities that occur only in end-of-day batches. Multiple end-of-day batches per day can run if the Behavior Detection installation supports multiple time zones, such as New York and Singapore.
- **Intra-day:** Used when loading data between end-of-day batches to obtain more frequent detection results. For example, running a batch of trading-compliance scenarios at 10:00 A.M. can identify behaviors relevant to the opening of the market without waiting for the end of the day to be able to act.

Directory Structure

Table 43 provides the directory structure for the Batch Control Utility, in <OFSAAI Installed Directory>/database/db_tools/:

Table 43. Batch Control Utility Directory Structure

Directory	Contents
bin/	Executable files, including the start_mantas_batch.sh, end_mantas_batch.sh, and get_mantas_batch.sh shell scripts.
lib/	Required class files in .jar format.
mantas_cfg/	Configuration files , such as install.cfg and categories.cfg, in which you can configure properties and logging attributes.
logs/	File batch_control.log that the utility generates during execution.

Logs

As the Batch Control Utility manages batch processing, it generates a date-stamped log in the <OFSAAI Installed Directory>/database/db_tools/logs/batch_control.log file. The log file contains relevant information such as status of various batch control processes, results, and error records.

You can modify the current logging configuration for this utility in the configuration files <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg and categories.cfg. For more information about logging in these configuration files, Refer to *Managing Common Resources for Batch Processing Utilities* on page 158, and Appendix A, *Logging*, on page 235, for more information.

Using the Batch Control Utility

The Batch Control Utility typically runs as part of automated processing that a job scheduling tool such as Maestro or Unicenter AutoSys controls. The utility starts and terminates through a shell script, using values in parameters that particular configuration files contain.

You can use the Batch Control Utility to run the following types of batches:

- **End-of-day:** Represent processing at the completion of a business day for a set of data. Some processes are only appropriate for end-of-day batches. For example, daily activity summary derivations and calculating alert ages are activities that occur only in end-of-day batches. Multiple end-of-day batches per day can run if the Behavior Detection installation supports multiple time zones , such as New York and Singapore.
- **Intra-day:** Used when loading data between end-of-day batches to obtain more frequent detection results. For example, running a batch of trading-compliance scenarios at 10:00 A.M. can identify behaviors relevant to the opening of the market without waiting for the end of the day to be able to act.

The following sections describe this process, including tasks that you can perform when configuring the utility or running it manually (that is, starting, stopping, or obtaining a batch name).

- [Configuring the Batch Control Utility](#)
- [Setting Up Batches](#)
- [Starting a Batch Process Manually](#)

- [Processing for Batch Start](#)
- [Ending a Batch Process](#)
- [Processing for End Batch](#)
- [Identifying a Running Batch Process](#)
- [Obtaining a Batch Name](#)

Configuring the Batch Control Utility

To configure the batch control utility, follow these steps:

1. Navigate to the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file. This file contains common configuration information that Batch Control and other utilities require for processing (see Figure 67).
2. Use the following sample section from the install.cfg file to input configuration information specific to this utility, including the single parameter that batch control requires.

```
##### BATCH CONTROL CONFIGURATION
#####

# When ending the batch, age alerts in calendar or business
days.
```

Figure 75. Configuring Batch Control Utility

The value of the `age.alerts.useBusinessDays` parameter indicates that at completion of an end-of-day batch process, the Behavior Detection application calculates the age of active alerts by number of calendar days (N) or business days (Y). The value of this parameter resides in the `KDD_CAL` table (Refer to Table 51, “KDD_CAL Table Contents,” on page 199, for more information).

The utility connects to the database employing the user that the `utils.database.username` property specifies in the `install.cfg` file.

Setting Up Batches

OFSBD delivers with a default batch called DLY. The `KDD_PRCSNG_BATCH` table includes this batch and must contain all batches in the system. When a batch starts as part of an automated process, it uses the batch names and other start-up information in this table.

The following table provides the contents of the `KDD_PRCSNG_BATCH` table.

Table 44. KDD_PRCSNG_BATCH Table Contents

Column Name	Description
PRCSNG_BATCH_NM	Name of the batch , such as DLY.
PRCSNG_BATCH_DSPLY_NM	Readable name for the batch , such as Daily.
PRCSNG_ORDER	Relative order of a batch run within processing.
EOD_BATCH_NM	Name of the batch that is this batch's end-of-day. This name is the same as the name for PRCSNG_BATCH_NM if the row represents an end-of-day batch.

Each row in the `KDD_PRCSNG_BATCH` table represents a batch. Each batch identifies the batch that is the corresponding end-of day batch. The following examples illustrate this concept:

- [Single Batch](#)
- [Single Site Intra-day Processing](#)
- [Multiple Countries](#)

Single Batch

In this example, the KDD_PRCNSG_BATCH table contains a single batch per day. This is typical of deployment of a single geography for which a solution set does not require detection more than once daily. The KDD_PRCNSG_BATCH table may look similar to the example in Table 45.

Table 45. Sample KDD_PRCNSG_BATCH Table with Single Batch

PRCSNG_BATCH_NM	PRCSNG_BATCH_DSPLY_NM	PRCSNG_ORDER	EOD_BATCH_NM
DLY	Daily Batch	1	DLY

Single Site Intra-day Processing

In this intra-day batch example, the system is servicing a single time zone but runs an additional batch during the day to identify behaviors related to overnight trading, as Table 46 describes.

Table 46. Sample KDD_PRCNSG_BATCH Table with Intra-day Processing

PRCSNG_BATCH_NM	PRCSNG_BATCH_DSPLY_NM	PRCSNG_ORDER	EOD_BATCH_NM
MAIN	Main Evening Batch	2	MAIN
MORN	Morning Batch	1	MAIN

In this configuration, run the Calendar Manager Utility only during the MORN batch. Refer to *The utility returns the batch name to standard output.* on page 197, for more information. You can run the Data Retention Manager either in the MORN or MAIN batch. If you run it in the MAIN batch, define at least one *buffer* partition so that the MORN batch does not fail due to inadequate partitions.

Refer to [Managing Data Retention Manager](#), for more information.

Multiple Countries

A single deployment supports detection against data from New York, London, and Hong Kong. In this case, three batches are all end-of-day batches, as Table 47 describes.

Table 47. Sample KDD_PRCNSG_BATCH Table with Multiple Country Processing

PRCSNG_BATCH_NM	PRCSNG_BATCH_DSPLY_NM	PRCSNG_ORDER	EOD_BATCH_NM
HK	Hong Kong	1	HK
LND	London	2	LND
NY	New York	3	NY

Since Hong Kong's markets open first, this is the first batch. You should run the Calendar Manager and Data Retention Manager at the start of the HK batch.

Upon setup of the batches, Behavior Detection processing begins with the `start_mantas_batch.sh` shell script. The final step in a batch is calling the `end_mantas_batch.sh` shell script.

Starting a Batch Process Manually

To start a batch manually, follow these steps:

1. Verify that the Behavior Detection database is operational:

```
tnsping <database instance name>
```

2. Verify that the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg configuration file contains the correct source database connection information.

3. Access the directory where the shell script resides:

```
cd <OFSAAI Installed Directory>/database/db_tools/bin
```

4. Run the batch control shell script:

```
start_mantas_batch.sh <batch name>
```

where <batch name> is the name of the batch. This parameter is case-sensitive.

Note: If you enter an invalid batch name, the utility terminates and logs a message that describes the error. The error message appears on the console only if you have output to the console enabled in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg file. Refer to “*Configuring Console Output*,” for more information.

Processing for Batch Start

After establishing the required Java environment and initiating various Java processing activities, the Batch Control Utility does the following:

1. The utility verifies that the provided batch name contains only the characters A-Z, a-z, and 0-9 by querying the KDD_PRCSNG_BATCH table (Table 47).
2. The utility determines whether a batch is running by querying the KDD_PRCSNG_BATCH_CONTROL table. The following table describes the KDD_PRCSNG_BATCH_CONTROL table.

Table 48. KDD_PRCSNG_BATCH_CONTROL Table Contents

Column Name	Description
PRCSNG_BATCH_ID	Current batch process ID.
PRCSNG_BATCH_NM	Name of the current batch process.
DATA_DUMP_DT	Current business day. The Calendar Manager Utility places this information in the table.
EOD_PRCSNG_BATCH_FL	Flag that indicates whether the batch is an end-of-day process (Y or N).

3. The utility records information about the batch in the KDD_PRCSNG_BATCH_HIST table. This table contains a history of all batches that appear by start date and end date.

The following table describes the KDD_PRCSNG_BATCH_HIST table.

Table 49. KDD_PRCSNG_BATCH_HIST Table Contents

Column Name	Description
PRCSNG_BATCH_ID	Current batch process ID.
PRCSNG_BATCH_NM	Name of the current batch process.
DATA_DUMP_DT	Business day on which the batch ran.

Table 49. KDD_PRCSNG_BATCH_HIST Table Contents

START_TS	Time that the batch started.
END_TS	Time that the batch ended (if applicable).
STATUS_CD	Status code that indicates whether the batch is currently running (<i>RUN</i>) or has finished (<i>FIN</i>).

4. The Batch Control Utility logs a message in the <OFSAAI Installed Directory>/database/db_tools/logs/batch_control.log file, stating that the batch process has begun. Querying the KDD_PRCSNG_BATCH_HIST table for confirmation that the batch has started displays information similar to that in Figure 76. In the last entry, note the appearance of RUN for STATUS_CD and lack of end time in END_TS.

PRCSNG_BATCH_ID	PRCSNG_BATCH_NM	DATA_DUMP_DT	START_TS	END_TS	STATUS_CD
1	DLY	10-Nov-06	11-Nov-06 6:45:32 AM	11-Nov-06 7:32:56 AM	FIN
2	DLY	11-Nov-06	12-Nov-06 7:54:45 AM	12-Nov-06 8:23:12 AM	FIN
3	DLY	12-Nov-06	13-Nov-06 6:12:32 AM	13-Nov-06 7:23:20 AM	FIN
4	DLY	13-Nov-06	14-Nov-06 6:23:49 AM	14-Nov-06 7:10:45 AM	FIN
5	DLY	14-Nov-06	15-Nov-06 6:25:32 AM	15-Nov-06 7:12:56 AM	FIN
6	DLY	15-Nov-06	16-Nov-06 6:34:37 AM	16-Nov-06 7:56:32 AM	FIN
7	DLY	16-Nov-06	17-Nov-06 6:21:34 AM	17-Nov-06 7:48:26 AM	FIN
8	DLY	17-Nov-06	18-Nov-06 6:11:23 AM	18-Nov-06 7:13:56 AM	FIN
9	DLY	18-Nov-06	19-Nov-06 6:34:36 AM	19-Nov-06 7:45:56 AM	FIN
10	DLY	19-Nov-06	20-Nov-06 6:39:35 AM	20-Nov-06 7:32:56 AM	FIN
11	DLY	20-Nov-06	21-Nov-06 6:35:32 AM		RUN

Figure 76. Sample KDD_PRCSNG_BATCH_HIST Table—Batch Start Status

Ending a Batch Process

When a batch ends as part of an automated process, the utility retrieves the batch name and other information from the KDD_PRCSNG_BATCH table (Refer to Table 44). To stop a batch process manually, follow these steps:

1. Verify that the Behavior Detection database is operational.
tnsping <database instance name>
2. Verify that the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg configuration file contains the correct source database connection information.
3. Access the directory where the shell script resides:
cd <OFSAAI Installed Directory>/database/db_tools/bin
4. Start the batch shell script:
end_mantas_batch.sh

If you enter an invalid batch name, the utility terminates and logs a message that describes the error. The error message appears on the console only if you have output to the console enabled in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg configuration file.

Processing for End Batch

After establishing the required Java environment and initiating various Java processing activities, the Batch Control Utility does the following:

1. Determines whether a batch is running by querying the KDD_PRCSNG_BATCH_CONTROL table (Refer to Table 48, “KDD_PRCSNG_BATCH_CONTROL Table Contents,” on page 194).

- Records information about the batch in the KDD_PRCNSNG_BATCH_HIST table (Refer to Table 49, “KDD_PRCNSNG_BATCH_HIST Table Contents,” on page 194). This table contains a history of all batches that appear by start date and end date. Figure 77 illustrates a sample table query; an end time-stamp in END_TS and status of FIN in STATUS_CD for the bolded entry indicates that the batch has ended.

PRCSNG_BATCH_ID	PRCSNG_BATCH_NM	DATA_DUMP_DT	START_TS	END_TS	STATUS_CD
1	DLY	10-Nov-06	11-Nov-06 6:45:32 AM	11-Nov-06 7:32:56 AM	FIN
2	DLY	11-Nov-06	12-Nov-06 7:54:45 AM	12-Nov-06 8:23:12 AM	FIN
3	DLY	12-Nov-06	13-Nov-06 6:12:32 AM	13-Nov-06 7:23:20 AM	FIN
4	DLY	13-Nov-06	14-Nov-06 6:23:49 AM	14-Nov-06 7:10:45 AM	FIN
5	DLY	14-Nov-06	15-Nov-06 6:25:32 AM	15-Nov-06 7:12:56 AM	FIN
6	DLY	15-Nov-06	16-Nov-06 6:34:37 AM	16-Nov-06 7:56:32 AM	FIN
7	DLY	16-Nov-06	17-Nov-06 6:21:34 AM	17-Nov-06 7:48:26 AM	FIN
8	DLY	17-Nov-06	18-Nov-06 6:11:23 AM	18-Nov-06 7:13:56 AM	FIN
9	DLY	18-Nov-06	19-Nov-06 6:34:36 AM	19-Nov-06 7:45:56 AM	FIN
10	DLY	19-Nov-06	20-Nov-06 6:39:35 AM	20-Nov-06 7:32:56 AM	FIN
11	DLY	20-Nov-06	21-Nov-06 6:35:32 AM	21-Nov-06 7:39:32 AM	FIN

Figure 77. Sample KDD_PRCNSNG_BATCH_HIST Table—Batch End Status

- Calculates the age of all open alerts and writes it to KDD_REVIEW.AGE if the EOD_BATCH_FL is Y in the KDD_PRCNSNG_BATCH_CONTROL table.
- Updates the KDD_REVIEW table for all alerts from the current batch to set the Processing Complete flag to Y. This makes the alerts available for alert management.
- Deletes any records in the KDD_DOC table that the system marks as temporary and are older than 24 hours.
- Logs a message in the <OFSAAI Installed Directory>/database/db_tools/logs/batch_control.log file, stating that the end batch process has begun.

Identifying a Running Batch Process

Caution: At times, you may must know the name of a currently running batch, or verify that a batch is active. For example, during intra-day detection processing, many batches may be running simultaneously and you must identify one or more by name. If you set the batch control logging to display at the console, be aware that log messages are mixed with the output of the shell script; the output can be difficult to read.

To Obtain a Batch Name

To identify a running batch process, follow these steps:

- Access the directory where the shell script resides:
`cd <OFSAAI Installed Directory>/database/db_tools/bin`
- Start the batch shell script:
`get_mantas_batch.sh`

The name of the currently running batch is written to standard output (Refer to *Configuring Console Output* on page 174, for more information).

Obtaining a Batch Name

After establishing the required Java environment and initiating various Java processing activities, the Batch Control Utility does the following:

1. The utility retrieves the name of the currently running batch from the KDD_PRCSNG_BATCH_CONTROL table (Refer to Table 48, “KDD_PRCSNG_BATCH_CONTROL Table Contents,” on page 194).

The utility returns the batch name to standard output.

Managing Calendar Manager Utility

After loading holidays into the KDD_CAL_HOLIDAY table and weekly off-days into the KDD_CAL_WKLY_OFF table, you can use the Calendar Manager Utility to update and manage OFSBD system calendars. The <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg configuration file contains modifiable inputs that you use to run the utility (Refer to *Install.cfg File* for more information).

This section contains the following topics:

- Directory Structure
- Logs
- Calendar Information
- Using the Calendar Manager Utility

Directory Structure

The following table provides the directory structure for the Calendar Manager Utility in <OFSAAI Installed Directory>/database/db_tools/.

Table 50. Calendar Manager Utility Directory Structure

Directory	Description
bin/	Contains executable files, including the shell script <code>set_mantas_date.sh</code> .
lib/	Includes required class files in .jar format.
mantas_cfg/	Contains configuration files , such as <code>install.cfg</code> and <code>categories.cfg</code> , in which you can configure properties and logging attributes.
logs/	Keeps the <code>calendar_manager.log</code> log file that the utility generates during execution.

Logs

As the utility updates the calendars in the OFSBD system, it generates a log that it enters in the <OFSAAI Installed Directory>/database/db_tools/logs/calendar_manager.log file (the logging process time-stamps all entries). The log file contains relevant information such as status of the various Calendar Manager processes, results, and error records.

You can modify the current logging configuration for this utility in the configuration files <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg and categories.cfg. For more information about logging in these configuration files, Refer to *Managing Common Resources for Batch Processing Utilities* on page 158, and Appendix A, *Logging*, on page 235, for more information.

Calendar Information

The Calendar Manager Utility obtains all holidays and weekly off-days for loading into the OFSBD calendars by retrieving information from the KDD_CAL_HOLIDAY and KDD_CAL_WKLY_OFF tables (Refer to Table 38 and Table 39). These tables contain calendar information that an Oracle client has provided regarding observed holidays and non-business days.

Using the Calendar Manager Utility

The Calendar Manager Utility runs as part of automated processing that a job scheduling tool such as Maestro or Unicenter AutoSys controls. The utility runs through a shell script, using values in parameters that the `install.cfg` file contains. The utility then populates the KDD_CAL database table with relevant OFSBD business calendar information.

The following sections describe this process, including tasks that you can perform when configuring the utility or running it manually.

- [Configuring the Calendar Manager Utility](#)
- [Executing the Calendar Manager Utility](#)
- [Updating the KDD_CAL Table](#)

Configuring the Calendar Manager Utility

The <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file contains common configuration information that Calendar Manager and other utilities require for processing (Refer to Figure 67). The following sample section from the `install.cfg` file provides configuration information specific to this utility, including default numerical values in the utility's two required parameters.

```
##### CALENDAR MANAGER CONFIGURATION
#####

# The look back and look forward days of the provided date.
# These values are required to update the KDD_CAL table. The
# maximum look back or forward is 999 days.
calendar.lookBack=365
calendar.lookForward=10
```

- `calendar.lookBack`: Determines how many days to iterate backward from the provided date during a calendar update.
- `calendar.lookForward`: Determines how many days to iterate forward from the provided date during a calendar update.

The maximum value that you can specify for either of these parameters is 999 days.

Note: The lookback period should be at least 90 days and as long as any alerts are likely to be open. The lookforward period does not must be more than 10 days. This is used when calculating projected settlement dates during data management.

Warning: When you have configured the system to calculate alert and case age in Business Days, the calendar date of the current system date and the calendar date of the alert or case creation must be included in the calendar. As such, if you are running with a business date that is substantially behind the current system date, you should set the `lookForward` parameter for the calendar manager sufficiently high to ensure that the system date is included on the calendar. Additionally, if you have alerts that are open for a very long period, you should set the `lookBack` parameter sufficiently high to include the dates of your oldest open alerts. If the business calendar does not cover either of these dates, the processing reverts to calculating age in Calendar days.

The utility connects to the database employing the user that the `utils.database.username` property specifies in the `install.cfg` file.

Executing the Calendar Manager Utility

You can manage the Calendar Manager Utility as part of automated processing. You can run the utility either inside a batch process (that is, after calling the `start_mantas_batch.sh` script) or outside a batch.

Starting the Utility Manually

To start the Calendar Manager Utility, follow these steps:

1. Verify that the Behavior Detection database is operational:
`tnsping <database instance name>`
2. Verify that the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg` configuration file contains the correct source database connection information.
3. Go to the directory where the shell script resides:
`cd <OFSAAI Installed Directory>/database/db_tools/bin`
4. Start the calendar manager shell script:
`set_mantas_date.sh YYYYMMDD`

where `YYYYMMDD` is the date on which you want to base the calendar, such as `20161130` for November 30, 2016. The utility then verifies that the entered date is valid and appears in the correct format.

If you do not enter a date or enter it incorrectly, the utility terminates and logs a message that describes the error. The error message displays on the console only if you have output to the console enabled in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg` configuration file. Refer to *Configuring Console Output*, on page 174, for more information.

Updating the KDD_CAL Table

The Calendar Manager Utility retrieves information that it needs for updating OFSBD business calendars from the `KDD_CAL_HOLIDAY` and `KDD_CAL_WKLY_OFF` database tables. It then populates the `KDD_CAL` table accordingly. That is, for each calendar name found in the `KDD_CAL_WKLY_OFF` and `KDD_CAL_HOLIDAY` tables, the utility creates entries in `KDD_CAL`.

The following table provides the contents of the `KDD_CAL` table.

Table 51. KDD_CAL Table Contents

Column Name	Description
<code>CLNDR_NM</code>	Specific calendar name.
<code>CLNDR_DT</code>	Date in the range between the lookback and lookforward periods.

Table 51. KDD_CAL Table Contents (Continued)

Column Name	Description
CLNDR_DAY_AGE	Number of calendar days ahead or behind the provided date. The provided date has age 0, the day before is 1, the day after is -1. For example, if a specified date is 20061129, the CLNDR_DAY_AGE of 20061128 = 1, and 20061130 = -1.
BUS_DAY_FL	Flag that indicates whether the specified date is a valid business day (set the flag to Y). Set this flag to N if the DAY_OF_WK column contains an entry that appears as a valid non-business day in the KDD_CAL_WKLY_OFF table, or a valid holiday in KDD_CAL_HOLIDAY.
BUS_DAY_AGE	Number of business days ahead or behind the provided date. If BUS_DAY_FL is N, BUS_DAY_AGE receives the value of the previous day's BUS_DAY_AGE.
DAY_OF_WK	Value that represents the day of the week: Sunday=1, Monday=2, Tuesday=3, ... Saturday=7.
WK_BNDRY_CD	Week's start day (SD) and end day (ED). <ul style="list-style-type: none"> • If this is the last business day for this calendar name for the week (that is, next business day has a lower DAY_OF_WK value), set to ED<x>, where <x> is a numeric counter with the start/end of the week that the provided date is in = 0. • If it is the first business day for this calendar name for this week (that is, previous business day has a higher DAY_OF_WK value), set to SD<x>. Weeks before the provided date increment the counter, and weeks after the provided date decrement the counter. Therefore, "ED0" is always on the provided date or in the future, and "SD0" is always on the provided date or in the past.
MNTH_BNDRY_CD	Month's start day (SD) and end day (ED). <ul style="list-style-type: none"> • If this is the last business day for this calendar name for the month (that is, next business day in a different month), set to ED<y>, where y is a numeric counter with the start/end of the month that the provided date is in = 0. • If it is the first business day for this calendar for this month (that is, previous business day in a different month), set to SD<y>. Months before the provided date increment the counter, and months after the provided date decrement the counter. Therefore, "ED0" is always on the provided date or in the future, and "SD0" is always on the provided date or in the past.
BUS_DAY_TYPE_CD	Indicates the type of business day: <ul style="list-style-type: none"> • N = Normal • C = Closed • S = Shortened
SESSN_OPN_TM	Indicates the opening time of the trading session for a shortened day. The format is HHMM.
SESSN_CLS_TM	Indicates the closing time of the trading session for a shortened day. The format is HHMM.

Table 51. KDD_CAL Table Contents (Continued)

Column Name	Description
SESSN_TM_OFFST_TX	Indicates the timezone offset for SESSN_OPN_TM and SESSN_CLS_TM. The format is HH:MM.
QTRT_BNDRY_CD	<p>Quarter's start day (SD) and end day (ED).</p> <ul style="list-style-type: none"> ● If this is the last business day for this calendar name for the quarter (that is, next business day in a different quarter), set ED to <y>, where y is a numeric counter with the start/end of the quarter that the provided date is in = 0. ● If it is the first business day for this calendar name for this quarter (that is, previous business day is in a different quarter), set SD to <y>. <p>Quarters before the provided date increment the counter, and quarters after the provided date decrement the counter. Therefore, "ED0" is always on the provided date or in the future, and "SD0" is always on the provided date or in the past.</p>

If a batch is running, the system uses the date provided in the call to start the `set_mantas_date.sh` script. This script updates the `KDD_PRCNG_BATCH_CONTROL.DATA_DUMP_DT` field.

Managing Data Retention Manager

Behavior Detection relies on Oracle partitioning for maintaining data for a desired retention period, providing performance benefits, and purging older data from the database. The data retention period for business and market data is configurable. Range partitioning of the tables is by date.

The Data Retention Manager enables you to manage Oracle database partitions and indexes on a daily, weekly, and/or monthly basis (Refer to Figure 66 on page 157). This utility allows special processing for trade-related database tables to maintain open order, execution, and trade data prior to dropping old partitions. As administrator, you can customize these tables.

The utility accommodates daily, weekly, and monthly partitioning schemes. It also processes specially configured Mixed Date partitioned tables. The Mixed Date tables include partitions for Current Day, Previous Day, Last Day of Week for weeks between Current Day and Last Day of Previous Month, and Last Business Day of Previous Two Months.

The Data Retention Manager can:

- Perform any necessary database maintenance activities, such as rebuilding global indexes.
- Add and drop partitions, or both, to or from the date-partitioned tables.

Data Retention Manager provides a set of SQL procedures and process tables in the Behavior Detection database. A shell script and a configuration file that contain the various inputs set the environment that the utility uses.

This section covers the following topics:

- [Directory Structure](#)
- [Logs](#)

- [Processing Flow](#)
- [Using the Data Retention Manager](#)
- [Utility Work Tables](#)

Directory Structure

The following table provides the directory structure for the Data Retention Manager.

Table 52. Data Retention Manager Directory Structure

Directory	Contents
bin/	Executable files, including the <code>run_drm_utility.sh</code> shell script.
lib/	Required class files in <code>.jar</code> format.
mantas_cfg/	Configuration files , such as <code>install.cfg</code> and <code>categories.cfg</code> , in which you can configure properties and logging attributes.
logs/	File <OFSAAI Installed Directory>/database/db_tools/logs/DRM_Utility.log that the utility generates during execution.

Logs

Oracle stored procedures implement Data Retention Manager and conducts some logging on the database server. A configuration parameter in the `install.cfg` file controls the path to which you store the logs on the database server.

As the Data Retention Manager performs partitioning and indexing activities, it generates a log that it enters in the <OFSAAI Installed Directory>/database/db_tools/logs/DRM_Utility.log file (the logging process time-stamps all entries). The log file contains relevant information such as status of the various processes, results, and error records.

You can modify the current logging configuration for Data Retention Manager in the configuration files <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg and categories.cfg. For more information about logging in these configuration files, Refer to *Managing Common Resources for Batch Processing Utilities*, on page 158, and Appendix A, *Logging*, on page 235, for more information.

Processing Flow

Figure 78 illustrates the Data Retention Manager’s process flow for daily, weekly, and monthly partitioning. Based on a table’s retention period, the utility drops the oldest partition and then adds a new partition.

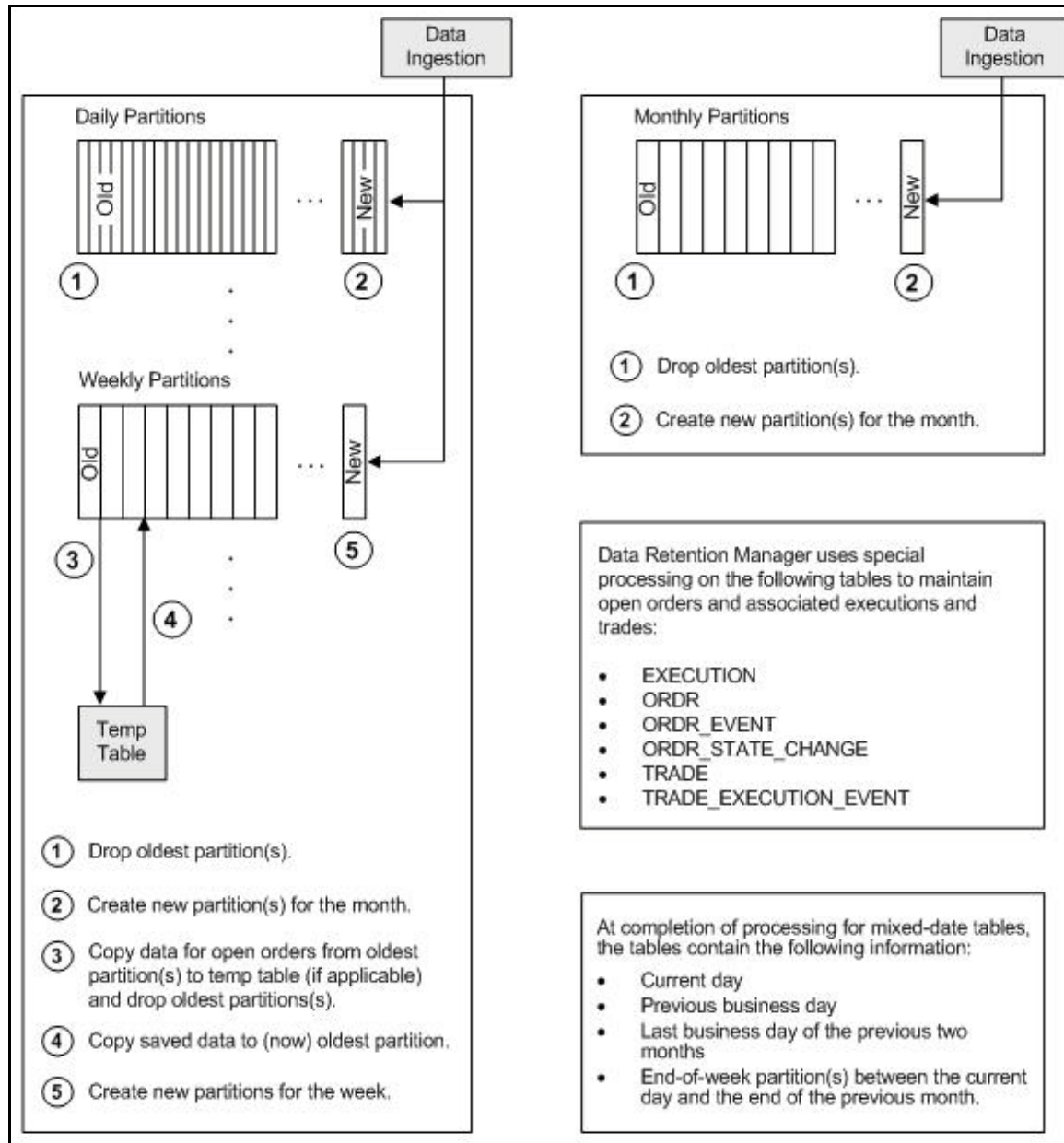


Figure 78. Database Partitioning Process

Using the Data Retention Manager

The Data Retention Manager typically runs as part of automated processing that a job scheduling tool such as Maestro or Unicenter AutoSys controls. However, you can run Data Retention Manager manually on a daily, weekly, or monthly basis to manage database tables.

The following sections describe how to configure and execute the utility and maintain database partitions and indexes.

- [Configuring the Data Retention Manager](#)
- [Executing the Data Retention Manager](#)
- [Creating Partitions](#)
- [Maintaining Partitions](#)
- [Maintaining Indexes](#)

Configuring the Data Retention Manager

To configure the Data Retention Manager, follow these steps:

1. Navigate to the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file. This file contains common configuration information that Data Retention Manager and other utilities require for processing
2. Use the sample install.cfg file in Figure 67 to do a configuration.

Note: The configuration parameters in the install.cfg are only used if command line parameters are not provided. It is strongly recommended that you provide command line parameters instead of using the install.cfg parameters.

The Data Retention Manager automatically performs system checks for any activity that may result in an error, such as insufficient space in the tablespace. If it discovers any such activity, it logs a Warning message that identifies the potential problem. If Data Retention Manager fails to run successfully, you can configure the utility so that the ingestion process for the following day still proceeds.

The following sample section from the install.cfg file provides other configuration information specific to this utility, including required and optional parameters.

```
##### DATA RETENTION MANAGER CONFIGURATION
#####
# Set the Data Retention Manager input variables here.
##
drm_operation=P
drm_partition_type=A
drm_owner=${schema.mantas.owner}
drm_object_name=A
drm_weekly_proc_fl=Y
```

Figure 79. install.cfg Data Retention Manager Configuration

This example shows default values that the system uses only when calling the utility with no command line parameters. The following table describes these parameters.

Table 53. Data Retention Manager Processing Parameters

Parameter	Description
drm_operation	Operation type: P-Partition AM-Add Monthly Partition DM -Drop Monthly Partition RI - Rebuild Indexes RV - Recompile Views T-Truncate Current Partition
drm_partition_type	Partition type: D-Daily W-Weekly M- Monthly X- Mixed-Date A- All Partitions (Daily, Weekly, Monthly)
drm_owner	Owner of the object (Atomic schema owner).
drm_object_name	Object name. If performing an operation on all objects, the object name is A.
drm_weekly_proc_fl	Flag that determines whether partitioning occurs weekly (Y and N).

Note: The system processes Daily partitioned tables (drm_partition_type=D) and Mixed-date partitioned tables (drm_partition_type=X) simultaneously. Therefore, you need only specify D or X to process these tables.

An example for the Mixed-date partition, for the present date 20050711, is:

```
P20050711 (Current Day)
P20050708 (Previous Day and End of week #1)
P20050701 (End of previous week #2)
P20050630 (End of previous Month #1)
P20050624 (End of previous week #3)
P20050617 (End of previous week #4)
P20050531 (End of previous Month #2)
```

Executing the Data Retention Manager

Before you execute the Data Retention Manager, ensure that users are not working on the system. To avoid conflicts, Oracle recommends that you use this utility as part of the end-of-day activities.

The Data Retention Manager should be executed nightly for Daily partitioned and Mixed-date partitioned tables, after the calendar has been set for the next business day. For weekly and monthly partitioned tables, the Data Retention Manager should be executed prior to the end of the current processing period.

Note: Oracle recommends running the Data Retention Manager on Thursday or Friday for weekly partitioned tables and on or about the 23rd of each month for monthly partitioned tables.

Note: Be sure to set the system date with the Calendar Manager Utility prior to running the Data Retention Manager (Refer to *The utility returns the batch name to standard output.*, for more information).

Running the Data Retention Manager

To run the Data Retention Manager manually, follow these steps:

1. Verify that the Behavior Detection database is operational:

```
tnsping <database instance name>
```

2. Verify that the <OFSAAI Installed

Directory>/database/db_tools/mantas_cfg/install.cfg configuration file contains the correct source database connection information.

3. Access the directory where the shell script resides:

```
cd <OFSAAI Installed Directory>/database/db_tools/bin
```

4. Start the batch shell script with the parameters in Table 53:

```
run_drm_utility.sh <drm_operation> <drm_partition_type> <drm_owner> <drm_object_name>  
<drm_weekly_proc_fl>
```

The following are examples of running the script:

- To run the utility for all daily tables in the ATOMIC schema, execute the script:

```
run_drm_utility.sh P D BUSINESS A N
```

- To run the utility to drop a monthly partition of the BUSINESS table ACCT_SMRY_MNTH, execute the script as follows (using the same parameters as in the previous example):

```
run_drm_utility.sh DM M BUSINESS ACCT_SMRY_MNTH N
```


Creating Partitions

To create partition names, use the formats in the following table.

Table 54. Partition Name Formats

Partition Type	Format and Description
Monthly	<p>PYYYYMM</p> <p>where YYYY is the four-digit year and MM is the two-digit month for the data in the partition.</p> <p>For example: Data for November 2006 resides in partition P200611.</p> <hr/> <p>Note: The Data Retention Manager uses information in the <code>KDD_CAL</code> table to determine end-of-week and end-of-month boundary dates.</p>
Weekly or Daily	<p>PYYYYMMDD</p> <p>where YYYY is the four-digit year, MM is the two-digit month, and DD is either the date of the data (daily) or the date of the following Friday (weekly) for the data in the partition.</p> <p>For example: Data for November 30, 2006 resides in partition P20061130. Data for the week of November 19 - November 23, 2006 resides in partition P20061123.</p> <hr/> <p>Note: The Data Retention Manager uses information in the <code>KDD_CAL</code> table to determine end-of-week and end-of-month boundary dates.</p>

Note: Data Retention Manager assesses the current status of partitions on the specified table to determine the requested partition. If the system previously fulfilled the request, it logs a warning message.

The Data Retention Manager does not support multiple partition types on a single table. If an Oracle client wants to alter the partitioning scheme on a table, that client must rebuild the table using the new partitioning scheme prior to utilizing the Data Retention Manager. Then you can update the values in the Data Retention Manager tables to reflect the new partitioning scheme.

Maintaining Partitions

Partition maintenance procedures remove old data from the database so that the database does not continue to grow until space is insufficient. Daily, weekly, or monthly maintenance is necessary for tables that have daily, weekly, and monthly partitions, respectively.

To maintain Partitions, follow these steps:

1. Copies information related to open orders from the oldest partitions to temp tables (`EXECUTION`, `ORDR`, `ORDR_EVENT`, `ORDR_STATE_CHANGE` `TRADE` and `TRADE_EXECUTION_EVENT`)
2. Drops the oldest partitions for all partition types.
3. Inserts the saved data into what is now the oldest partition (applicable to tables with open orders).
4. Creates new partitions.
5. Recompiles the views that scenarios use.

Managing Daily Partitioning Alternative

The Data Retention Manager also enables you to build five daily partitions on a weekly basis. To build partitions, follow these steps:

1. Execute the `run_drm_utility.sh` shell script
2. Set the `drm_weekly_proc_flg` parameter to Y. For more information, refer to Table 53.

This procedure eliminates the must perform frequent index maintenance; Oracle recommends doing this for large market tables.

This approach builds the daily partitions for the next week. When creating the five daily partitions on a weekly basis, the Data Retention Manager should be executed prior to the end of the current week, to create partitions for the next week.

Note: You must set the `WEEKLY_ADD_FL` parameter in the `KDD_DR_MAINT_OPRTN` table to Y so that the procedure works correctly. For more information about this parameter, Refer to Table 55, “`BUSINESS.KDD_DR_MAINT_OPRTN` Table Contents,” on page 209, for more information.

Partition Structures

The structures of business data partitions and market data partitions differ in the following ways:

- Business data partitions are pre-defined so that weekdays (Monday through Friday) are business days, and Saturday and Sunday are *weekly off-days*. Business data tables use all partitioning types.

You can use the Calendar Manager Utility to configure a business calendar as desired. For more information about this utility, Refer to *The utility returns the batch name to standard output.* on page 197, for more information.

- Market data partitions hold a single day of data. The partitions use the `PYYYYMMDD` convention, where `YYYYMMDD` is the date of the partition.

Recommended Partition Maintenance

You should run partition maintenance as appropriate for your solution set. Oracle recommends that you run partition maintenance for AML on a daily basis (after setting the business date through the Calendar Manager Utility, and prior to the daily execution of batch processing), and Trading Compliance at least once a week.

Oracle recommends that you use the P (Partition) option when running the Data Retention Manager, as it drops older partitions and adds appropriate partitions in a single run of the utility.

When performing monthly maintenance, you can add or drop a partition independently, as the following procedures describe.

Note: If you ingest data belonging to a date less than the current date, you should run the DRM utility till current date. This avoids the error *Partition Not Found* while accessing trade records in Trade Blotter UI.

Managing Alternative Monthly Partition

As part of an alternative method of monthly partition maintenance, you can either add or drop a monthly database partition. as described in the following section:

Adding a Monthly Database Partition

To add a monthly partition, run the utility's shell script as follows (Refer to Table 53 for parameters):

```
run_drm_utility.sh AM M BUSINESS <object> N
```

where AM is the `drm_operation` parameter that implies adding a monthly partition.

Dropping a Monthly Database Partition

To drop a monthly partition, run the utility's shell script as follows (Refer to Table 53 for parameters):

```
run_drm_utility.sh DM M BUSINESS <object> N
```

where, DM is the `drm_operation` parameter that implies dropping a partition.

Maintaining Indexes

As part of processing, the Data Retention Manager automatically rebuilds the database index and index partitions that become unusable. You do not need to maintain the indexes separately.

The utility enables you to rebuild global indexes by executing the following command:

```
run_drm_utility.sh RI M BUSINESS <object> N
```

where RI is the `drm_operation` parameter that implies rebuilding indexes.

Utility Work Tables

The Data Retention Manager uses the following work tables during database partitioning:

- KDD_DR_MAINT_OPRTN Table
- KDD_DR_JOB Table
- KDD_DR_RUN Table

KDD_DR_MAINT_OPRTN Table

The KDD_DR_MAINT_OPRTN table contains the processing information that manages Data Retention Manager activities. The following table provides these details.

Table 55. BUSINESS.KDD_DR_MAINT_OPRTN Table Contents

Column Name	Description
PROC_ID	Identifies the sequence ID for the operation to perform.
ACTN_TYPE_CD	Indicates the activity that the utility is to perform on the table: <ul style="list-style-type: none"> ● A: Analyze ● RI: Rebuild Indexes ● P: Partition ● RV: Recompile Views
OWNER	Identifies an owner or user of the utility.
TABLE_NM	Identifies a database table.

Table 55. BUSINESS.KDD_DR_MAINT_OPRTN Table Contents (Continued)

Column Name	Description
PARTN_TYPE_CD	Indicates the partition type: <ul style="list-style-type: none">● D: Daily● W: Weekly● M: Monthly● X: Mixed Date
TOTAL_PARTN_CT	Specifies the total number of partitions to be created, including the current partition. For example, for a daily partitioning scheme of four previous days and the current day, the value of this field is five (5).
BUFFER_PARTN_CT	Specifies the number of buffer partitions the utility is to maintain, excluding the current partition. For example, a two-day buffer has a value of two (2).
CNSTR_ACTN_FL	Determines whether to enable or disable constraints on the table during processing.
WEEKLY_ADD_FL	Indicates whether daily partitions are added for a week at a time. If set to Y, creates Daily Partitions for the next week. For example, if run on a Thursday, the DRM creates the five (5) partitions for the next week beginning with Monday.
NEXT_PARTN_DATE	Indicates starting date of the next partition that may get created, based on the current partitioned date.

Caution: For weekly partitioned tables, do not set the value to Y.

KDD_DR_JOB Table

The KDD_DR_JOB table stores the start and end date and time and the status of each process that the Data Retention Manager calls. The following table provides these details.

Table 56. BUSINESS.KDD_DR_JOB Table Contents

Column Name	Description
JOB_ID	Unique sequence ID.
START_DT	Start date of the process.
END_DT	End date of the process.
STATUS_CD	Status of the process: <ul style="list-style-type: none">● RUN: Running● FIN: Finished successfully● ERR: An error occurred● WRN: Finished with a warning

KDD_DR_RUN Table

The KDD_DR_RUN table stores the start and end date and time and status of individual process runs that are associated with a table. The following table provides these details.

Table 57. BUSINESS.KDD_DR_RUN Table Contents

Column Name	Description
JOB_ID	Unique sequence ID.
PROC_ID	Process ID.
START_DT	Start date of the process.
END_DT	End date of the process.
RESULT_CD	Result of the process: <ul style="list-style-type: none">● FIN: Finished successfully● ERR: An error occurred● WRN: Finished with a warning
ERROR_DESC_TX	Description of a resulting error or warning.

The system also uses the KDD_CAL table to obtain information such as the dates of the last-day-of-previous-month and end-of-weeks. Refer to Table 51 for contents of the KDD_CAL table.

Database Statistics Management

The system uses a script to manage Oracle database statistics. These statistics determine the appropriate execution path for each database query.

Logs

The `log.category.RUN_STORED_PROCEDURE` property controls logging for the `process.location` entry in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg` file.

Using Database Statistics Management

The system calls the script as part of nightly processing at the appropriate time and with the appropriate parameters:

- `analyze_mantas.sh <analysis_type> [TABLE_NAME]`

The `<analysis_type>` parameter can have one of the following values:

- `DLY_POST_LOAD`: Use this value to update statistics on tables that the system just loaded (for BUSINESS and MARKET related tables).
- `ALL`: Use this once per week on all schemas.
- `DLY_POST_HDC`: Use this value to update statistics of the alert-related archived data (in _ARC tables) that the Behavior Detection UI uses to display alerts. It is recommended that you do not modify this table. The Behavior Detection Historical Data Copy procedures uses this table to archive alert-related data.
- `DLY_PRE_HDC`: Use this value to update statistics of the Mantis related tables that contain the alert-related information. It is recommended that you do not modify this table. The Behavior Detection Historical Data Copy procedures uses this table to archive alert-related data.

- `DLY_POST_LINK`: Use this value to update statistics of the Mantas related tables that contain network analysis information. Run this option at the conclusion of the network analysis batch process.

The `[TABLE_NAME]` parameter optionally enables you to analyze one table at a time. This allows scheduling of the batch at a more granular level, analyzing each table as processing completes instead of waiting for all tables to complete before running the analysis process.

The metadata in the `KDD_ANALYZE_PARAM` table drive these processes. For each table this table provides information about the method of updating the statistics that you should use for each analysis type. Valid methods include:

- `EST_STATS`: Performs a standard statistics estimate on the table.
- `EST_PART_STATS`: Estimates statistics on only the newest partition in the table.

Note: For the `EST_STATS` and `EST_PART_STATS` parameters, the default sample size that the analyze procedure uses is now based on `DBMS_STATS.AUTO_SAMPLE_SIZE`.

- `IMP_STATS`: Imports statistics that were previously calculated. When running an ALL analysis, the system exports statistics for the tables for later use.

Failure to run the statistics estimates can result in significant database performance degradation.

These scripts connect to the database using the user that the `utils.database.username` property specifies, in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg` file. The `install.cfg` file also contains the following properties:

- `schema.mantas.owner`

The system derives schema name from this property.

For the ATOMIC Schema, there is no separate script for managing Oracle database statistics. But for improved query performance, we have to manage the Oracle database statistics periodically. Following are the sample commands.

To analyze table wise use, use the following commands:

```
ANALYZE table <Table name> compute statistics;
```

```
Example: ANALYZE table KDD_CASES compute statistics;
```

We can also perform whole schema analyze periodically.

Managing Flag Duplicate Alerts Utility

This section covers the following topics:

- Using Flag Duplicate Alerts Utility
- Executing Flag Duplicate Alerts Utility

The Flag Duplicate Alerts Utility enables you to run a script daily after the generation of alerts. This script identifies the pairs of alerts that are possible duplicates. It then adds a system comment to each alert and identifies the paired alert in the comment as a *Possible Duplicate*.

External Entity-focused scenarios in Behavior Detection can generate alerts either on external identifiers , such as external account ID, or on names of parties outside the bank. The logic of the scenarios only generates the name-focused alerts when the name has been found with multiple (or no) external identifiers. This check is made

across all transactions, not just the transactions involved in a particular alert. As a result, a single run of an External Entity-focused scenario can generate alerts involving the exact same transactions, one alert focused on the external Party ID, and one alert focused on the external Party Name.

Using Flag Duplicate Alerts Utility

The Flag Duplicate Alerts Utility looks at alerts that meet the following criteria:

- Entity focus (EN)
- Status of New (NW)
- Generated in the current running batch on the current date

The utility selects and compares alerts that meet the listed criteria above. It then determines whether generation of the alert is based on the same set of transactions for the same scenario and with different focuses, such as if one alert is an ID and the other is a Name. The utility flags these alerts as possible duplicates and adds a system comment which can be viewed on the Audit tab of the alert (each alert cross-references the other). For example:

Possible duplicate of alert **xxxxx**.

Executing Flag Duplicate Alerts Utility

To execute the Flag Duplicate Alerts Utility, run the following script after the Alert Creator, Assigner, and Auto-Close processes (jobs) have completed:

```
<OFSAAI Installed Directory>/database/db_tools/bin/flag_duplicate_alerts.sh
```

The system writes log information for this process to the following location:

```
<OFSAAI Installed Directory>/database/db_tools/logs/run_stored_procedure.log
```

Managing Notification

Notifications appear on the UI on the Home page and help alert users to items requiring their attention.

Notifications can be classified into two categories (depending on the method of generation):

- Event Based
- Batch Based

Event Based

These notifications are always associated with an event. Following are the event based notifications:

- **New Case Creation notification:** Whenever a user manually creates a new case, a notification is generated to the owner of the case and if owner is a pool then notification is generated to all the users who fall under that pool. If the user who created the case is also assigned as the owner, no notification is generated.
- **Re-assigned case notification:** Notification is generated to new owner of the case upon reassignment of the case. If the user who reassigned the case is also the new owner, no notification is generated. If the new owner is a pool then notification is generated to all users who are members of the organization represented by that pool.

- **Re-assigned alerts notification:** Notification is generated to the new owner of the Alert upon reassignment of the alert. If the user who reassigned the alert is also the new owner, no notification is generated. If the new owner is a pool then notification is generated to all users who are members of the organization represented by that pool.
- **Alert Data Transfer Unsuccessful:** In Asynchronous alert data transfer mode, if the data transfer during promotion of an alert to a case or linking of an alert to a case is Unsuccessful, then a notification is generated to the user who is taking the action, the owner of the alert, and the owner of the case, and then assigned to the user of the case.

Batch Based

These notifications are the result of processing of `end_mantas_batch.sh`. Following are the batch based notifications:

- **Cases Near Due Date notification:** Notification is generated to the owner of the cases if the due date of the case falls within the configurable parameter set in the Installation parameter table.
- **Alerts Near Due Date notifications:** Notification is generated to the owner of the alerts if the due date of the alert falls within the configurable parameter set in Installation parameter table.

These notifications are generated after the complete execution of Batch (provide the batch name) and can be seen in the Notification Grid in landing page. Each user sees the notifications which are relevant to them.

Note: You can set the near due date and display of notification parameters from the Manage Parameters screen. (Refer to the [Configuration Guide](#) for more information).

Managing Push E-mail Notifications

Alert Management provides the Push E-mail Notification utility to send e-mail to users about activity that is pending for them or about activity that has occurred on their alerts. The user sets a preference on the Preferences page to indicate whether they wish to receive notification messages or not. The system is delivered with two notification sets:

- **Activity:** This notification tells users of any actions that have occurred on alerts that they own since the last time this notification job was run. This notification also identifies any alerts that have been assigned to the user that the user has not yet opened.
- **OverDue:** This notification identifies alerts that are either past their due date or are nearing their due date (within 4 days).

Notifications can be run individually, in groups, or all at once. Notification jobs can be run at any time of the day as is appropriate for the information that is to be provided. For example, it is appropriate to run the OverDue notification at the beginning of each day, whereas it may be appropriate to run the Activity notification multiple times per day. If there is no information to provide to a user, no e-mail is sent. If sections of a notification contain no information, that section is suppressed, such as the Reassignment section may be populated, but there may not be a section for Actions taken on your alerts.

For a user to receive notification, the user must have an e-mail address identified through their user configuration.

Using Push E-mail Notification

To run this utility, follow these steps:

1. Navigate to <OFSAAI Installed Directory>/database/db_tools/bin/run_push_email.ksh [notification list].

Note: If you do not include any command-line parameter, the system runs all notifications. You can provide one or more notifications as command line arguments. The notification names are case-sensitive.

2. Run the run_push_email.ksh script. The script runs a java class that attaches to the database using the user that the `utils.database.username` property identifies in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg file. The java process then runs the queries associated with the desired notifications and sends e-mail to the users. By default, the system sends e-mails using unauthenticated SMTP, however it also supports authenticated SMTP, authenticated or unauthenticated SMTPS and Microsoft Exchange.

Note: When the notification runs, the date and timestamp for the notification is stored in the <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/notification.config file.

Warning: The notification.config file must not be edited.

To avoid corruption of this file, do not run two instances of the run_push_email.ksh script at once.

The script returns a status code to indicate whether it was successful. The following table lists the status codes returned.

Table 58. Return Codes for run_push_email.ksh script

Return Code	Meaning
0	Success
1	The process failed, check the log for reasons.
100-200	The process succeeded, but not all e-mails were delivered the percent not delivered is calculated using (return code – 100).

Configuring Push E-mail Notification

The following files are used to configure Push E-mail notification:

- Configuration for connectivity and mail format parameters are modified in:
<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg
- The definition of notification types and the sections of each notification (including headers, footers and disclaimers) is configured in:
<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/NotificationDetails.xml
- The queries that are run against the database for notification are configured in:
<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/etc/xml/QBD_Notification.xml

The following sections provide configuration guidance for each of these files.

Configuring General Notification Properties

Table 59 identifies the configurable parameters associated to Push E-mail Notification in the database tools `install.cfg` file.

Note: The Password Manager Utility should be used to set the `email.smtp.password` and `email.exchange.password` properties in the `install.cfg` file. These properties should never be modified directly in the file. Run the following commands and enter the appropriate passwords:

```
<OFSAAI Installed Directory>/changePasswords.sh email.smtp.password
```

```
<OFSAAI Installed Directory>/changePasswords.sh email.exchange.password
```

Table 59. Push E-mail Notification Configurable parameters

Property	Description	Sample Value
<code>email.type</code>	The type of e-mail connection to use. The valid values are <code>smtp</code> , <code>smtps</code> and <code>exchange</code> . This defaults to <code>smtp</code> .	<code>smtp</code>
<code>notification.threads</code>	The number of threads to use for sending out notification e-mails. Default value is 4.	2
<code>utils.database.max_connectios</code>	The maximum number of database connections to open to run notification queries in parallel. Default value is 4.	2
<code>email.from</code>	The e-mail address shows as the From address on the notification e-mail. This value is only used for SMTP and SMTPS mail. If it is omitted, then the e-mail address associated with the Unix or Linux user running the process will appear as the From address.	<code>ofsbd@yourdomain.com</code>
<code>email.smtp.host</code>	The host name for SMTP or SMTPS server.	<code>mailhost.yourdomain.com</code>
<code>email.smtp.port</code>	The port on which the SMTP or SMTPS server listens. For SMTP, this is 25, for SMTPS, this is typically 465.	25
<code>email.smtp.auth</code>	To connect to the SMTP or SMTPS server using a username/password, set this value to <code>true</code> . To connect unauthenticated, set to <code>false</code> .	<code>true</code>
<code>email.smtp.user</code>	The username for authenticated connections.	User
<code>email.smtp.password</code>	The password for authenticated connections. This is set by the Password Manager Utility.	
<code>email.smtp.useHTML</code>	If set to <code>true</code> , e-mail is sent with an HTML body. If set to <code>false</code> , e-mail is sent in plain text only. This defaults to <code>true</code> .	<code>true</code>
<code>email.exchange.server</code>	If using Exchange, this is your Exchange server.	<code>webmail.yourdomain.com</code>
<code>email.exchange.domain</code>	Domain for the user.	YourDomain
<code>email.exchange.user</code>	Username to connect to Exchange.	<code>ofsbd</code>
<code>email.exchange.password</code>	Password to connect to Exchange. This is set by the Password Manager Utility.	

Table 59. Push E-mail Notification Configurable parameters (Continued)

Property	Description	Sample Value
<code>email.exchange.prefix</code>	The prefix used for Exchange. Consult your Exchange administrator for this value. This defaults to <code>exchange</code> .	<code>exchange</code>
<code>email.exchange.mailbox</code>	The mailbox for the user. Consult your Exchange administrator for this value.	<code>ofsbd.System</code>
<code>email.exchange.useSSL</code>	To connect using SSL, set this value to <code>true</code> .	<code>true</code>
<code>email.exchange.useFBA</code>	To use Form Based Authentication, set this value to <code>true</code> . This value defaults to <code>true</code> .	<code>true</code>
<code>email.exchange.useNTLM</code>	To use NTLM authentication, set this value to <code>true</code> . This value defaults to <code>false</code> .	<code>false</code>
<code>email.exchange.draftsfolder</code>	The name of the Drafts folder within the mailbox. This defaults to <code>drafts</code> .	<code>drafts</code>
<code>email.exchange.useHTML</code>	If set to <code>true</code> , e-mail is sent with an HTML body. If set to <code>false</code> , e-mail is sent in plain text only. This defaults to <code>true</code> .	<code>true</code>

The connectivity to Microsoft Exchange is implemented using a third party product called Java Exchange Connector (JEC). Oracle does not provide a copy of this product, it must be purchased separately. After you have purchased JEC, place the `jec.jar` in the <OFSAAI Installed Directory>/database/db_tools/lib directory, and copy your `jeclicense` file into <OFSAAI Installed Directory>/database/db_tools/mantas_cfg.

In addition to the configuration parameters identified in Table 59 above, there are series of configuration parameters that are used to control the formatting of the HTML e-mail messages. These parameters use HTML style syntax to control styles for different sections of the generated e-mail message.

Configuring Notifications

To configure notifications, follow these steps:

1. Navigate to OFSAAI Installed Directory>/database/db_tools/mantas_cfg/NotificationDetails.xml. The list of notifications to be delivered are configured in the NotificationDetails.xml file.<
2. Use the following sample to configure notifications.

```
<NotificationDetails>

    <Disclaimer>This message is for the designated recipient only and may
    contain privileged or confidential information.</Disclaimer>
    <HTMLDisclaimer><![CDATA[This message is for the designated recipient only
    and may contain privileged or <B>confidential</B>
    information.]]></HTMLDisclaimer>

    <Notification name="Activity" userQueryDef="AllActiveUsers">
        <Subject>Mantas Activity Notification</Subject>
        <Header>*** This message was system-generated. Do not reply to this
    message. ***</Header>
        <HTMLHeader><![CDATA[*** This message was system-generated. Do not reply
    to this message. ***]]></HTMLHeader>
        <Footer>*** This message was system-generated. Do not reply to this
    message. ***</Footer>
        <HTMLFooter><![CDATA[*** This message was system-generated. Do not reply
    to this message. ***]]></HTMLFooter>

        <Section queryDef="ReassignedAlerts">
            <Title>Reassigned Alerts:</Title>
            <HTMLTitle><![CDATA[Reassigned Alerts:<BR>]]></HTMLTitle>
            <Message>The following alerts have been recently assigned to
    you:</Message>
            <HTMLMessage><![CDATA[<BR>The following alerts have been recently
    assigned to you:]]></HTMLMessage>
            <Column text="Alert ID" key="REVIEW_ID"/>
            <Column text="Assigned By" key="ASSIGNED_BY"/>
            <Column text="Assigned On" key="ASSIGNED_DATE" format="datetime"/>
        </Section>
    </Notification>
</NotificationDetails>
```

Figure 80. Sample NotificationDetails.xml file

The file starts with disclaimer configuration. The disclaimer is included in all e-mail sent by the system. The `<DisclaimerHTML>` tag permits use of HTML within the disclaimer section for emphasis, embedded links, etc. In general, where there is a tag and a tag with the same name but HTML added, the message will include the appropriate element based on whether the message is being sent in Text or HTML mode. If a message is sent in HTML mode, and there is no HTML tag, the basic element is used for that element.

Each Notification begins with a name and identifies the queryDef used to select the candidate users. A queryDef is a configurable query, and will be discussed in detail the next section. The queryDef `AllActiveUsers` selects all active users who have an e-mail address configured and have not specified in their user preferences that they do not want notifications. A notification has a Subject, which is the subject of the delivered e-mail and a header and footer. These are used for introductory text of the e-mail message.

After the header and footer, a number of sections are defined. Each section specifies a queryDef to run to find the records that are reflected in the section. The following table contains the additional elements.

Table 60. Additional Elements of NotificationDetails.xml file

Element	Description
Title HTMLTitle	The title is a title for the section.
Message HTMLMessage	The Message appears between the title and the table of results.
Column	There is a Column element for each column that your query displays. The column element has a text attribute, which is the column header in the rendered table, and a key, which refers to a column in the query results that is displayed in this section.

The queries that are run for identifying users and for populating each section of the notification are configured in queryDefs. The queryDefs for the default notifications are configured in <OFSAAI Installed Directory>/database/db_tools/mantas_cfg/etc/xml/QBD_Notification.xml.

Configuring Notification Queries

To configure notification queries, follow these steps:

1. Navigate to OFSAAI Installed Directory>/database/db_tools/mantas_cfg/etc/xml/QBD_Notification.xml. The queryDefs for the default notifications are configured in <. the QBD Notification.xml file.
2. Use the following sample to configure notification queries:

Note: The Notification process reads all QBD files in this directory, so custom notifications can be placed in the existing file or in a new file , such as QBD_CustomNotification.xml.

Figure 81 shows the sample structure of the QBD_CustomNotification.xml file.

```
<queries>
  <ReassignedAlerts>
    <baseQuery>
      select
        kdd_activity.new_review_owner_id owner_seq_id,
        kdd_activity.review_id,
        old_owner.owner_id assigned_by,
        kdd_activity.start_dt assigned_date
      from
        mantas.kdd_review inner join mantas.kdd_activity
          on kdd_review.review_id = kdd_activity.review_id
          and kdd_activity.new_review_status_cd = 'RA'
        inner join mantas.kdd_review_owner old_owner
          on kdd_activity.creat_id = old_owner.owner_seq_id
    <usingColumns/>
    <groupingColumns/>
  </baseQuery>
  <filterProperties>
    <property name="_filter_MIN_DATE" operator=">="
table="kdd_activity" columnName="start_dt" type="Timestamp"/>
    <property name="_filter_MAX_DATE" operator="<="
table="kdd_activity" columnName="start_dt" type="Timestamp"/>
  </filterProperties>
  <sortProperties>
    <sort name="default">
      <property table="kdd_activity" columnName="start_dt"
direction="ASC" order="1"/>
    </sort>
  </sortProperties>
</ReassignedAlerts>
</queries>
```

Figure 81. Sample Structure of QBD_CustomNotification.xml

Note: This is an example, and may not represent what is in the deployed product.

Each query is defined as an XML element (in this example, ReassignedAlerts is the element). The following table lists the other sub-elements of the QBD_CustomNotification.xml file.

Table 61. Sub-Elements of the Sample File

Element	Description
baseQuery	The base query is where the query is defined. The query can be any query, however it must return a column OWNER_SEQ_ID that identifies the owner to whom the notification should be sent. Other columns depend on what is appropriate for the query. The query may not contain a group by or order by clause, it must either end after the FROM clause or after the WHERE clause. If the query contains any XML-reserved characters, be sure to surround the query with <![CDATA[]>. The base query has two sub-elements defined below.
usingColumns	You can either include all of the join conditions in the FROM clause, or you can have a using clause appended to the FROM clause by identifying columns in this section. If you do use this element, then each column you will include in the USING clause is specified as follows: <column name="OWNER_SEQ_ID"/>

Table 61. Sub-Elements of the Sample File

Element	Description
groupingColumns	If you wish to have a query that performs a group by, then the GROUP BY clause is specified in this element. Each column that is part of the clause is specified using the same notation specified under <code>usingColumns</code> above.
filterProperties	The <code>filterProperties</code> element allows you to specify filters that are applied to the query. The filters are provided programmatically. The two filters provided in the sample above are the only filters that are accepted for Notification. The filter <code>_filter_MIN_DATE</code> is replaced by the date of the last execution of the notification. The filter <code>_filter_MAX_DATE</code> is replaced by the current system date. When specifying the filter properties, identify the table (or table alias) and column against which the filter is applied.
sortProperties	The <code>sortProperties</code> element allows you to define sorts for the query. Only the sort with the name <i>default</i> is used by Notifications. When specifying a sort, identify the table (or table alias) and column for the sort. You can specify more than one sort column (distinguishing them with the order attribute). You can specify either ASC for ascending sorts or DESC for descending sorts.

QueryDefs are used broadly in the Behavior Detection Framework user interface definition. Only the subset of queryDef capabilities that are used by Notification have been addressed in this section.

Logs

The `log.category.PUSH_EMAIL_NOTIFICATION.location` property in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg` file controls logging for this process. The system writes log information for this process to the following location:

`<OFSAAI Installed Directory>/database/db_tools/logs/push_email.log`

Refreshing Temporary Tables

Some behavior detection patterns use the temporary tables as part of the detection process.

Logs

The `log.category.REFRESH_TEMP_TABLE.location` property in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg` file controls logging for this process. The system writes log information for this process to the following location:

```
<OFSAAI Installed Directory>/database/db_tools/logs/refresh_temp_table.log
```

Using Refreshing Temporary Tables

The BD ATOMIC schema defines these tables; the tables have corresponding views that are used to populate them. Prior to running these patterns, run the `refresh_temp_table.sh` script. The script has the following calling signature:

```
refresh_temp_table.sh <table_name> <view_name>
```

where:

- `table_name` identifies the name of the table to populate.
- `view_name` identifies the name of the view to run to populate the table.

This procedure deletes all records in the target table prior to running the view to populate it. It then estimates statistics for the newly populated table. This procedure logs into the database with the user that the `utils.miner.user` property identifies in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg` file.

Populating Temporary Tables for Scenarios

Scenarios typically depend on data management to complete processing. However the following scenarios depend on population of Temp Tables to populate data.

1. (IML/CU) Hidden Relationships
2. (FR/AC) Networks of Accounts, Entities, and Customers
3. (ML/AC) Networks of Accounts, Entities, and Customers
4. (CST/AC) Customers Who Have Experienced a Large Loss Recently
5. (CST/HH) Customers Who Have Experienced a Large Loss Recently

The Link Analysis scenario also depends on the network job creation before the sequence matcher part of the scenario runs.

IML-HiddenRelationships-dINST

To populate the temporary tables for IML-HiddenRelationships-dINST scenario, follow these steps:

1. Execute these refresh temporary table processes (these commands can be run in parallel):

```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_HIDREL_NT_JRNL TMP_HIDREL_NT_JRNL_VW
```



```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_WIRE TMP_HIDREL_NT_WIRE_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_ACTAXID TMP_HIDREL_NT_ACTAXID_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_ACADDR TMP_HIDREL_NT_ACADDR_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_ACPHONE TMP_HIDREL_NT_ACPHONE_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_ACEMAIL TMP_HIDREL_NT_ACEMAIL_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_ACPSWRD TMP_HIDREL_NT_ACPSWRD_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_INST TMP_HIDREL_NT_INST_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_WIREACBENE TMP_HIDREL_NT_WIREACBENE_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_WIREACORIG TMP_HIDREL_NT_WIREACORIG_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_CUACTAXID TMP_HIDREL_NT_CUACTAXID_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_CUACADDR TMP_HIDREL_NT_CUACADDR_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_CUACPHONE TMP_HIDREL_NT_CUACPHONE_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_HIDREL_NT_CUACEMAIL TMP_HIDREL_NT_CUACEMAIL_VW
```

2. Execute the link analysis/network generation job. The product job template ID is 114698616.
3. Execute the scenario job. The product job template ID is 116200024.

ML-NetworkOfAcEn-fAC

To populate the temporary tables for ML-NetworkOfAcEn-fAC scenario, follow these steps:

1. Execute these refresh temporary table processes (these commands can be run in parallel):

```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_ACCTADDR TMP_NETACENCU_NT_ACCTADDR_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_ACCTEMAIL TMP_NETACENCU_NT_ACCTEMAIL_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_ACCTPHONE TMP_NETACENCU_NT_ACCTPHONE_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_ACCTPSWRD TMP_NETACENCU_NT_ACCTPSWRD_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_ACCTTAXID TMP_NETACENCU_NT_ACCTTAXID_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_CUACADDR TMP_NETACENCU_NT_CUACADDR_VW

<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh
TMP_NETACENCU_NT_CUACEMAIL TMP_NETACENCU_NT_CUACEMAIL_VW
```

```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_CUACPHONE TMP_NETACENCU_NT_CUACPHONE_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_CUACTAXID TMP_NETACENCU_NT_CUACTAXID_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_JRNL TMP_NETACENCU_NT_JRNL_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_WIREACBENE TMP_NETACENCU_NT_WIREACBENE_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_WIREACORIG TMP_NETACENCU_NT_WIREACORIG_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_NETACENCU_NT_WIRETRXN TMP_NETACENCU_NT_WIRETRXN_VW
```

2. Execute the link analysis/network generation job. The product job template ID is 114698120.
3. Execute the scenario job. The product job template ID is 114698631.

FR-NetworkOfAcEn-fAC

To populate the temporary tables for FR-NetworkOfAcEn-fAC scenario, follow these steps:

1. Execute these refresh temporary table processes (these commands can be run in parallel.):

```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_NT_ACCTADDR TMP_FRNTWRK_NT_ACCTADDR_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_ACCTEMAIL TMP_FRNTWRK_ACCTEMAIL_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_ACCTPHONE TMP_FRNTWRK_ACCTPHONE_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_ACCTPSWRD TMP_FRNTWRK_ACCTPSWRD_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_ACCTAXID TMP_FRNTWRK_ACCTAXID_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_CUACADDR TMP_FRNTWRK_CUACADDR_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_CUACEMAIL TMP_FRNTWRK_CUACEMAIL_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_CUACPHONE TMP_FRNTWRK_CUACPHONE_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_CUACTAXID TMP_FRNTWRK_CUACTAXID_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_JRNL TMP_FRNTWRK_JRNL_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_WIREACBENE TMP_FRNTWRK_WIREACBENE_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_WIREACORIG TMP_FRNTWRK_WIREACORIG_VW  
  
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
TMP_FRNTWRK_WIRETRXN TMP_FRNTWRK_WIRETRXN_VW
```

2. Execute the link analysis/network generation job. The product job template ID is 118745091.
3. Execute the scenario job. The product job template ID is 117350084.

CST-Losses

To populate the temporary tables for CST-LOSSES scenario, follow these steps:

1. Execute this refresh temporary table process:

```
<OFSAAI Installed Directory>/database/db_tools/bin/refresh_temp_table.sh  
VWCST_LOSSES_AC_ASM_TMP VWCST_LOSSES_AC_ASM
```

2. Execute the scenario job.

CST-UncvrdLongSales-dRBPC

To populate the temporary table UNCVRD_LONG_TRADE_TEMP for CST-UncvrdLongSales-dRBPC scenario, follow these steps:

Note: This should be run after the ingestion is completed, just before the scenario job runs.

1. Execute this to refresh temporary table process:

```
<OFSAAI Installed Directory>/database/db_tools/run_p_uncvrdlongsales_ew.sh
```

2. Execute the scenario job.

Managing Truncate Manager

The data management subsystem calls the `run_truncate_manager.sh` script to truncate tables that require complete replacement of their data.

Logs

The `log.category.TRUNCATE_MANAGER.location` property in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/categories.cfg` file controls logging for this utility. The system writes log information for this process to the following location:

```
<OFSAAI Installed Directory>/database/db_tools/logs/truncate_manager.log
```

Using the Truncate Manager

For the `run_truncate_manager.sh` script to take the table name as an argument, the table must exist in the BD ATOMIC schema. The script logs into the database using the user that the `truncate.database.username` property specifies in the `<OFSAAI Installed Directory>/database/db_tools/mantas_cfg/install.cfg` file.

The script has the following calling signature:

```
run_truncate_manager.sh <table_name>
```

Note: This process is not intended to be called independently; only the Ingestion Manager subsystem should use it.

Managing ETL Process for Threshold Analyzer Utility

For inserting and updating records into the `KDD_TA_ML_DATA`, `KDD_TA_BC_DATA`, and `KDD_TA_TC_DATA` tables, there are two shell scripts that are used to call the database procedures. These are:

- `run_insert_ta_utility.sh` – This script calls the `P_TA_ML_INSERT_BREAKS`, `P_TA_BC_INSERT_BREAKS`, and `P_TA_TC_INSERT_BREAKS` procedures, which insert data into the `KDD_TA_ML_DATA`, `KDD_TA_BC_DATA`, and `KDD_TA_TC_DATA` tables, respectively, based on the `CREAT_TS` of the alerts in relation to the `LAST_RUN_DT` from `KDD_TA_LAST_RUN` (values for `RUN_TYPE_CD` are `ML_I`, `BC_I`, and `TC_I`).
- `run_update_ta_utility.sh` – This script calls the `P_TA_ML_UPDATE`, `P_TA_BC_UPDATE`, and `P_TA_TC_UPDATE` procedures, which update `QLTY_RTNG_CD` in the `KDD_TA_ML_DATA`, `KDD_TA_BC_DATA`, and `KDD_TA_TC_DATA` tables, respectively, for any *Review* closed since the last run based on `LAST_RUN_DT` from `KDD_TA_LAST_RUN` (values for `RUN_TYPE_CD` are `ML_U`, `BC_U`, and `TC_U`). The `CLS_CLASS_CD` value from `KDD_REVIEW` is used as the new `QLTY_RTNG_CD`.

Note: The log for these scripts is written in the `run_stored_procedure.log` file under the `<OFSAAI Installed Directory>/database/db_tools/logs` directory.

Note: The `LAST_RUN_DT` column in the `KDD_TA_LAST_RUN` table is only updated for *inserts* and *updates* if at least one or more records were inserted or updated. The `LAST_RUN_DT` column is not updated for significant errors that resulted in no records being updated. These scripts are a part of the database tools and reside in the `<OFSAAI Installed Directory>/database/db_tools/bin` directory.

You can run this utility anytime, that is, it is not necessary to run this utility during specific processing activities.

Running Threshold Analyzer

To run the threshold analyzer, follow these steps:

1. Go to `ATOMIC` schema and execute below query:

```
select distinct (creat_ts)
  from kdd_review t
 where t.review_type_cd = 'AL'
       and SCNRO_DISPL_NM <> 'User Defined'
       and PRCSNG_BATCH_NM = 'DLY';
```

2. Set date as per dates returned from above SQL. Say `CREATE_TS` is 05/21/2013 in `kdd_review` table than we will set a date 05/17/2013 (Friday of last week) from the `$FICHOME/database/db_tools/bin` folder.

3. Execute the following command:

```
start_mantas_batch.sh DLY
set_mantas_date.sh 20130517 --(Friday of last week)
```

4. Execute `DRM` utility to create partitions:

```
run_drm_utility.sh P W ATOMIC KDD_TA_ML_DATA N
run_drm_utility.sh P W ATOMIC KDD_TA_BC_DATA N
run_drm_utility.sh P W ATOMIC KDD_TA_TC_DATA N
P Partition
W Weekly
ATOMIC Schema
KDD_TA_ML_DATA Table name
```

Extend N

5. Execute Insert and Update Threshold Analyzer scripts from \$FICHOME/database/db_tools/bin folder.
6. Execute the following command:

```
run_insert_ta_utility.sh  
run_update_ta_utility.sh
```
7. Repeat the above process if you have more than one date returned from query in point 1.

Managing Deactivate Expired Alert Suppression Rules

The following shell script should be executed in order to deactivate Alert Suppression Rules that have expired based on the current system date:

```
-- run_upd_suppression_recs.sh
```

This script should be run as the last step in batch processing just prior to ending the batch. It is important that this script is run after post-processing has been completed (that is, not before the Alert Suppression job is executed). Also, after the batch is executed, it makes an audit entry

This section of the document consists of resolution to the frequently asked questions during the configuration.

What should be done if the batch fails during the initial task?

Check if V_GROUP_NAME has been passed correctly in the START batch and Backend servers are UP (such as, ICC as well as agent servers)

What should be done if the second/third task is struggling to start?

Login to Config Schema and execute the following query:

```
Select * from PR2_PROCESS_TASK_PARAMETER
```

Make sure that V_TASK_PARAMETER_VALUE column has correct SOURCENAME, and also LOADTYPE is correct.

What should be done if any process inside the batch fails?

Follow these steps:

1. Navigate to \$FIC_HOME/ficdb/log and check the logs, and resolve the issues.
2. Once the issue is resolved, then navigate to Common Tasks UI and select Operations.
3. Select Batch execution and Restart the batch which is failed.

What should be done if batch needs a rerun?

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

There can be the cases where source schema is different but data resides in the same instance. In this case, Grant select to all user tables needs to be provided to the ECM Atomic schema from the source schema.

What should be done if Correlation fails in first time run?

Make sure to run the correlation.sh file. For more information, see the [Pre Batch Execution Configuration](#)

Can I run the Batch again if data-loaded to CA went wrong?

- Yes, you can trigger a new batch. Before running the batch, you must clear all the data from all business, evented and event tables for that MIS Date and Data Origin.
- Yes, you can trigger a new batch. Before that you must remove the data from the Event tables. This will take more time than the above option.

What should I do, if I have loaded few wrong records into few business tables?

- You can trigger a new batch. Before running the batch, you must clear all the data from all business, evented and event tables for that MIS Date and Data Origin
- You can remove the data from the business tables for MIS Date and Data Origin, then run the batch only including the process for which you need to correct the data and then end this batch. This will take more time than the above option.

