Oracle Financial Services Enterprise Case Management

Administration and Configuration Guide

Release 8.1.2.6.0

October 2023

E83847-07

ORACLE
Financial Services

OFS ECM Administration and Configuration Guide

Copyright © 2025 Oracle and/or its affiliates. All rights reserved.

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are “commercial computer software” pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

For information on third party licenses, click here.

Document Control

Table 1 lists the document revision history.

Table 1: Document Control

Version Number	Revision Date	Change Log
8.1.2.8.1	December 2024	The following sections are added: • Conductor-related Data Movement for CA-STR • Displaying CA-STR Fields in ECM UI
8.1.2.8.0	August 2024	The following sections are updated/added: • Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload • Excel Upload • PMF Configuration • Displaying Case Statuses Based on Case Type & User Role • Case Allocation Assignment • Exporting Cases • Changing Order of Set Event Decision Dropdown • Auditing Search/View Details for Account and Customer in Research UI
8.1.2.7.0	February 2024	The following sections are updated/added: • System For Cross-Domain Identity Management (SCIM) • Configuring Issuing State & Country
8.1.2.6.0	October 2023	The following sections are updated/added: • ECM Business Table Data Synchronization with Source Business Data • Archiving/Unarchiving Events • Configuring Standard Comment Data • Continuing Activity Review & Continuing Activity Report • Configuring Case Title for Case Creation (Create Event and Promote to Case) API • Hint Configuration in Event Purge (EventPurgeConfig.cfg) • Case Purge Utility

Table 1: Document Control

Version Number	Revision Date	Change Log
8.1.2.5.0	June 2023	The following sections are updated/added: • Mapping a User with a User Group • Starting a batch run • Configuring Action • Configuring Case Due Date • Setting Due Date of New Cases via Correlation Batch • Configuring Case List Records Per Page Limit • Exclude Case Type from Create Case • Archiving Cases • Configuring Standard Comment Data • CS and ECM Table Mapping for Alert Status Customization • Configuring CAR Rules • Continuing Activity Review & Continuing Activity Report • Configuring Case Allocation • Adding Standard Comments for Event Decision • Configuring Labels for Transactions • Configuring Different Due Dates for Case Types • Load Data from BD to ECM • Load Data from Third-party to ECM
8.1.2.4.0	March 2023	The following sections are updated/added: • Configuring Case Due Date • Configuring Case Near Due Date • Trusted Pairs • Event Suppression • Configuring Continuous Activity Review • Configuring Labels for Transactions • Configuring Different Due Dates for Case Types
8.1.2.3.0	December 2022	1. The following section was added to help improve batch performance: ▪ Batch Performance Recommendations 2. The following sections were updated to support Quantifind configuration: ▪ Configuring Quantifind Bulk Entity Process ▪ Configuring SMTP- Based Email/RFI 3. Data Redaction
8.1.2.2.0.0	September 2022	The following sections were added to support Quantifind Batch Processing: • Configuring Quantifind Bulk Entity Process • Configuring Quantifind Bulk Event Creation Process

Table 1: Document Control

Version Number	Revision Date	Change Log
8.1.2.1.0	July 2022	The following section was added to support integration with Oracle Financial Services Transaction Filtering: • Configuring Transaction Filtering Server Details
8.1.2.1.0	June 2022	The following sections are added for enhancements in this release: • Mapping Read-Only Case typeConfiguring Token/Non-Token Based RFI • Configuring Customer Account Role • Trusted Pairs • Event Suppression
8.1.2.0.0	March 2022	The following sections are updated: • Setting Preferences • Configuring Quantifind Batch Processing for Customer Score Card Processing • Managing Case Designer The following sections are added for the enhancement in this release (V8.1.2.0.0): • Transaction Chart Configuration • Configuring Labels for Transactions • Trusted Pairs • Multi-locale Architecture

Table of Contents

1 About This Guide 18

1.1 Who Should Use This Guide 18

1.2 How this Guide is Organized 18

1.3 Where to Find More Information 19

1.4 Conventions Used in This Guide 19

2 About Oracle Financial Services Enterprise Case Management 20

2.1 Introduction 20

2.2 Administration and Configuration Activities 20

2.2.1 Loading Data 21

2.2.2 Correlation 21

2.2.3 Scoring 21

2.2.4 Promoted to Case 21

2.2.5 Processing Modelling Framework 21

2.2.6 Case Designer 21

2.2.7 Case Action Settings 21

3 Getting Started 23

3.1 System Requirements 23

3.2 Accessing OFS ECM Application 25

3.2.1 Masthead 26

3.2.2 Change Password 27

3.2.3 Copyright Information 28

3.2.4 Selecting Applications 29

3.3 Managing OFSAA Administration Page 30

3.4 Troubleshooting Your Display 31

3.4.1 Enabling JavaScript 31

3.4.2 Enabling Cookies 31

3.4.3 Enabling Temporary Internet Files 31

3.4.4 Enabling File Downloads 32

3.4.5 Setting Printing Options 32

3.4.6 Enabling Pop-up Blocker 32

3.4.7 Time Zone Offset *33*
3.5 Setting Preferences 33
4 Managing User Administration and Security Configuration 35
4.1 About User Administration 35
4.2 Administrator User Privileges 35
4.3 User Provisioning Process Flow 36
4.3.1 Requirements to Access ECM Application *36*
4.4 Managing User Administration 37
4.4.1 Managing Identity and Authorization *37*
4.5 Adding Security Attributes 42
4.5.1 Prerequisites *42*
4.5.2 About Security Attributes *42*
4.5.3 Loading Security Attributes *44*
4.6 Mapping Security Attributes to Organizations and Users 48
4.6.1 Introduction *48*
4.6.2 Prerequisites for Mapper Maintenance *49*
4.6.3 Using Mapper Maintenance *51*
4.7 Configuring JIT 55
4.7.1 Configure JIT for Existing Users *56*
4.7.2 Disable LDAP Users *56*
5 Pre-batch Execution Configuration 58
5.1 Configuring Processing Group 58
5.2 Configuring Correlation 58
5.3 Configuring Ending Batch Process 61
5.4 ASC Batch Configuration 61
6 Performing Batch Run 63
6.1 About Batch Run 63
6.2 Starting a Batch Run 63
6.3 Ending a Batch Run 65
6.4 Executing a Batch Run 66
6.5 Batch Performance Recommendations 68

7 Loading Data 70
7.1 About Loading Data 70
7.1.1 Types of Connectors 70
7.2 Using Connectors 70
7.2.1 Accessing Connector Processes 71
7.2.2 Loading OBD Data 71
7.2.3 Loading OCS Data 71
7.2.4 Loading TBAML Data 72
7.2.5 Loading Studio Data 73
7.3 Data Movement (DM) Utility 73
7.3.1 DM Metadata Tables 74
7.3.2 DM Audit and Error Details Tables 77
7.4 Configuring Data Movement from LA to CA 77
7.4.1 About Data Movement 78
7.4.2 Sample Processes 78
7.4.3 ECM Business Table Data Synchronization with Source Business Table 80
7.4.4 Using Precedence 82
7.4.5 Designing Processes 83
7.4.6 Adding Transformation Rule 85
8 Configuring Correlation 87
8.1 About Correlation 87
8.2 Using Business Entity Paths 87
8.2.1 Correlation Business Path 87
8.2.2 Correlation Business Entity Configuration 88
8.3 Executing Correlation Rules 89
8.3.1 Performing Jobs 89
8.4 Sample Correlation Rules 89
9 Scoring 91
9.1 About Scoring 91
9.1.1 Initial Scoring 91
9.1.2 Adjustment Scoring 92

9.2 Types of Scoring 94
9.2.1 Event Scoring 94
9.2.2 Entity Scoring 94
9.2.3 Correlation Scoring 94
9.2.4 Pre case Scoring 94
9.3 Configuring Scoring Rules 94
9.3.1 Configuring AML Event Initial Scoring 95
9.4 Scoring Samples 99
9.4.1 Event 99
9.4.2 Entity 101
9.4.3 Correlation 102
10 Promoting to Case 104
10.1 About Promoting to Case (PTC) 104
10.2 Configuring PTC 104
11 Configuring Processing Modelling Framework (PMF) 106
11.1 About PMF 106
11.1.1 ECM Workflow Development Life Cycle 106
11.1.2 ECM Workflows 106
11.2 Pre-configuration Activities 107
11.2.1 Configuring Status 107
11.2.2 Configuring Action 107
11.2.3 Configuring Attributes 107
11.3 Accessing Process Modeller 109
11.4 Configuring an ECM Workflow 110
11.4.1 Creating Workflow 110
11.4.2 Defining Datafields 112
11.4.3 Defining Application Rules 112
11.4.4 Using Process Modeller Editor 114
11.4.5 Starting a Process 114
11.5 Editing of an ECM Workflow 119
11.6 Deleting an ECM Workflow 120

11.7 Implementing the ECM PMF Workflow 120
11.7.1 Defining Metadata 120
11.7.2 Creating the Workflow in PMF 125
11.7.3 Mapping of Workflow to a Case Type(s) in Case Designer 131
11.7.4 Steps to customize the "Checklist" functionality in ECM 131
11.7.5 Configuring CRR Workflows in PMF 131
11.7.6 Configuring Change Case Type Action in PMF 132
12 Managing Case Designer 134
12.1 About Case Designer 134
12.2 Accessing Case Designer 135
12.3 Case Designer Home page 135
12.4 Defining Case Class 137
12.4.1 About Case Class 137
12.4.2 Adding Case Class 137
12.4.3 Editing Case Class 138
12.5 Defining Case Type 138
12.5.1 About Case Type 138
12.5.2 Adding Case Type 138
12.5.3 Editing Case Type 146
13 Case Allocation Management 147
13.1 Accessing Case Allocation Assignment Page 147
13.2 Searching an Allocation Rule 147
13.3 Associating a Rule 148
13.4 Disassociating a Rule 149
13.5 Setting the Out Of Office 150
13.6 Clearing the Out Of Office 150
14 General Configuration 152
14.1 Configuring the Client Logo Image 153
14.1.1 Logo Specification 153
14.1.2 Placing a new Client Logo 153
14.1.3 Removing a Client Logo 153

14.1.4 Configuring Application Label Text 154
14.2 Accessing Manage Parameters 154
14.3 Configuring the Default Currency Code 154
14.4 Configuring the Base Time Zone 155
14.4.1 Modifying Time Zone 155
14.5 Configuring Case Own Flag Consideration 155
14.6 Configuring Case Prefix 156
14.7 Configuring the Display of Value in By Field Name/ID 156
14.8 Configuring Case Due Date 157
14.8.1 Setting Due Date of New Cases via Correlation Batch 158
14.9 Configuring Case Near Due Date 159
14.10 Configuring Organization Type 159
14.11 Configuring Application Server 160
14.12 Configuring Case Age Calculation 161
14.13 Configuring Case Assignment Inheritance 161
14.14 Configuring Case Correlation Owner 162
14.15 Configuring Case Inheritance 163
14.16 Configuring Case Risk Values 164
14.17 Configuring Default Case Owner 164
14.18 Configuring Case List Records Per Page Limit 164
14.19 Configuring Default Case Search Created Date Lookback 164
14.20 Configuring Default Event Search Created Date Lookback 165
14.21 Configuring Default Suppression Administration Created Date Lookback 165
14.22 Configuring Default Trusted Pairs Administration Created Date Lookback 165
14.23 Configuring Default Trusted Pairs Transaction Date Lookback 166
14.24 Configuring E-mail 166
14.24.1 Configuring Token/Non-Token Based RFI 169
14.24.2 Configuring SMTP- Based Email/RFI 169
14.25 Configuring Mode of Transferring Alert Information 170
14.26 Configuring Mode of Transferring Case Information 170
14.27 Configuring Lock Time Period for Case Actions 171

14.28 Configuring Include Historical Migrated Alerts 172
14.29 Configuring View All Organization 173
14.30 Exporting Cases 173
14.31 Configuring OBIEE 173
14.32 Configuring File Size 174
14.33 Configuring Views 174
14.33.1 Adding Views 174
14.33.2 Modifying Views 175
14.33.3 Removing Views 176
14.34 Configuring ECM Security Function 176
14.35 Configuring Customer Account Role 177
14.36 DB configuration 178
14.37 Configuring Required Action Comments 178
14.38 Managing Additional Configurations 179
14.38.1 Configuring File Type Extensions 179
14.39 Managing KYC Configurations 179
14.40 Account Restriction 180
14.41 Right to be Forgotten 180
14.41.1 Introduction to Right to be Forgotten 180
14.41.2 Implementation of Right to be Forgotten by OFSAA 180
14.42 Data Redaction 182
14.42.1 Configuring Redaction for FCC Grids 182
14.42.2 Redaction on Research UI Screen 183
14.43 Configuring Sanctions Server Details for L2 Feedback 183
14.44 Exclude Case Type from Create Case 184
14.45 Archiving/Unarchiving Cases 185
14.46 Archiving/Unarchiving Events 189
15 Configuring Administration Tools 191
15.1 Configuring Administration Tools 191
15.2 Configuring Application Server 191
16 Configuring Actions 193

16.1 Working with Case Action Settings 193
16.1.1 Understanding Case Workflows 193
16.1.2 Adding New Case Statuses 193
16.1.3 Configuring Case Action Data 196
16.1.4 Configuring Standard Comment Data 198
16.2 Action Validation Framework 201
16.2.1 KDD_ACTION_VLDTN Table 202
16.2.2 Adding Custom JS file in ECM 204
16.3 CS and ECM Table Mapping for Alert Status Customization 205
17 Configuring Web Application 206
17.1 Configuring the Session Timeout Setting 206
17.1.1 Configuring the Session Timeout Setting 206
17.1.2 Configuring the Session Timeout Setting for Admin Tools 206
18 Multi-locale Architecture 207
19 Additional Configuration 208
19.1 Correlation Case Type Mapping 209
19.1.1 Case Priority 209
19.1.2 Case Domain and Jurisdiction 209
19.2 Configuring CAR Rules 209
19.3 Continuing Activity Review & Continuing Activity Report 211
19.4 Populating Country ID 214
19.5 Adding Relationship Type values for Involved Parties 214
19.6 Configuring Case Allocation 214
19.6.1 Distribution of Cases to Users 218
19.7 Custom Rule Attributes 219
19.7.1 Configuring Case Age 220
19.7.2 Executing Case Age Calculation Batch 220
19.8 Configuring Tabs based on Role 221
19.9 Adding Standard Comments for Event Decision 222
19.10 Adding Event Decision for Customer Screening 222
19.11 Adding Search Results Fields based on Case Type 223

19.12 Adding and Configuring Case Type Attribute 227
19.12.1 Adding and Configuring Search Attributes 229
19.12.2 Adding and Configuring Derived Attribute 233
19.12.3 Configuring Hierarchy Options based on Another Hierarchy Attribute 235
19.12.4 Configuring the Case Title 235
19.12.5 Configuring Case Title for Case Creation (Create Event and Promote to Case) API 238
19.13 Configuring a Case as Read Only 238
19.14 Adding a New Scenario 238
19.15 Configuring Quality Control (QC) Sampling Rules 239
19.16 Event Purge 243
19.16.1 Event Purging Using Tables 244
19.16.2 Hint Configuration in Event Purge (EventPurgeConfig.cfg) 246
19.17 Case Purge Utility 247
19.18 Event Expiry 250
19.18.1 Identifying Events by Age 250
19.18.2 Identifying Events by Score 250
19.18.3 Examples 251
19.18.4 Configuring Event Expiry 252
19.19 CSS Color Coding for FCC Columns 255
19.20 Enabling Quantifind for Quantifind Customer Score Card 257
19.21 Configuring Quantifind Batch Processing for Customer Score Card Processing 258
19.22 Configuring Quantifind for Bulk Entity Process 263
19.23 Configuring Quantifind for Bulk Event Creation Process 267
19.24 Transaction Chart Configuration 268
19.25 Configuring Labels for Transactions 269
19.25.1 Adding Customized Transaction Labels 269
19.25.2 Updating Labels in UI 269
19.26 Entities Tab Configuration 270
19.27 Configuring Different Due Dates for Case Types 271
19.28 Trusted Pairs 272
19.28.1 Configuring Trusted Pair Actions 272

19.28.2 Configuring Duration *274*
19.29 Event Suppression 274
19.29.1 Configuring Suppression Actions *275*
19.29.2 Configuring Duration *277*
20 List of Processes and Tasks 278
20.1 OBD Application Process 278
20.1.1 Start Batch *278*
20.1.2 Load Data from BD to ECM *278*
20.1.3 Correlation *279*
20.1.4 Scoring *279*
20.1.5 Promote to Case *279*
20.1.6 Create Case *279*
20.1.7 End Batch *299*
20.2 OCS Application Process 299
20.2.1 Start Batch *299*
20.2.2 Load Data from CS to ECM *299*
20.2.3 Correlation *299*
20.2.4 Scoring *299*
20.2.5 Promote to Case *299*
20.2.6 Create Case *300*
20.2.7 End Batch *300*
20.3 OKYC Application Process 300
20.3.1 Start Batch *300*
20.3.2 Load Data from KYC to ECM *300*
20.3.3 Correlation *301*
20.3.4 Scoring *301*
20.3.5 Promote to Case *301*
20.3.6 Create Case *301*
20.3.7 Update Case ID *301*
20.3.8 End Batch *301*
20.4 OSTDO Application Process 302

20.4.1 Start Batch 302
20.4.2 Load Data from STDO to Consolidation Area 302
20.4.3 Correlation 308
20.4.4 Scoring 308
20.4.5 Promote to Case 308
20.4.6 Create Case 308
20.4.7 End Batch 311
20.5 Third-party Application Process 311
20.5.1 Start Batch 311
20.5.2 Load Data from Third-party to ECM 311
20.5.3 Correlation 317
20.5.4 Scoring 317
20.5.5 Promote to Case 317
20.5.6 Create Case 317
20.5.7 End Batch 317
21 Configuring Parallel Graph AnalytiX (PGX) Correlation 318
21.1 Overview 318
21.2 Pre-requisites 318
22 FAQs 319
22.1 What should be done if the batch fails during the initial task? 319
22.2 What should be done if the second/third task is struggling to start? 319
22.3 What should be done if any process inside the batch fails? 319
22.4 What should be done if the batch needs a rerun? 319
22.5 What should be done if Correlation fails in the first-time run? 319
22.6 Can I run the Batch again if data-loaded to CA went wrong? 319
22.7 How can I create new attributes? 320
22.8 How do I manage the parameters of attributes? 320
22.9 Can I set the order of the tabs to define how the as seen in a case? 320
22.10 How do I define the tab a user lands on when entering the case details? 320
22.11 What is the Event Details tab? 320
22.12 Can I deactivate a case type or case class? 320

22.13 Can I rename tabs? 321
22.14 Can the business entities that I see in a case be dependent on the types of events associated with the case and not explicitly defined in the Case Type? 321
22.15 What happens if I change the attribute and entity configuration of a case type for a case type which is currently active? 321
22.16 What happens if I change the underlying PMF workflow definition for a case type which is currently active? 321
23 OFSAA Support Contact Details 323
24 Send Us Your Comments 324

1 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:

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

1.1 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.

1.2 How this Guide is Organized

This Administration and Configuration Guide includes the following chapters:

- About Oracle Financial Services Enterprise Case Management, provides a brief overview of the Oracle Financial Services Enterprise Case Management application architecture, and its components.
- Getting Started, provides the required day-to-day operations and maintenance of Enterprise Case Management application users, groups, and organizational units.
- 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.
- Pre-batch Execution Configuration, provides the details of pre-batch configuration activities.
- Performing Batch Run, provides the process to start, execute, and end batch.
- Loading Data, provides the details to load the data from various sources to the ECM application.
- Configuring Correlation, provides the concept and configuration of correlation.
- Scoring, provides the concept behind scoring, methods, and types of scoring.
- Promoting to Case, provides the configuration of promote to case activity.
- Configuring Processing Modelling Framework (PMF), provides the concept of PMF, pre-configuration activities, and configuring workflows.
- Managing Case Designer, provides step-by-step instruction to configure case class, case type, case attributes, case workflow, and case entities.
- General Configuration, provides instructions to configure general parameters for case management.
- Configuring Administration Tools, provides instructions to configure parameters specific to administration tools.

- Configuring Actions, provides procedures to configure the list of available actions.
- Configuring Web Application, provides customization features available in the Web Application UI. This chapter contains information to configure session time out.
- List of Processes and Tasks provides the details of batch processes and tasks.

1.3 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

1.4 Conventions Used in This Guide

Table 2 lists the conventions used in this guide.

Table 2: Conventions Used in This Guide

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

2 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:

- Administration and Configuration Activities
- Administration and Configuration Activities

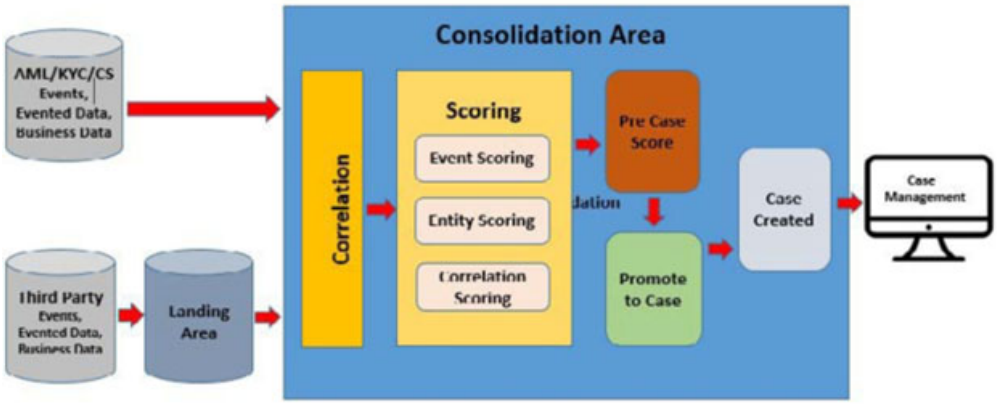
2.1 Introduction

Enterprise Case Management (ECM) supports the investigation and resolution of Anti-Money Laundering (AML), Know Your Customer (KYC), Customer Screening (CS), Studio (STDO), and third-party events. A newly created case passes through various statuses as part of the 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 are supported by various actions, which can be specific to the case type. Access to types of cases and actions are controlled based on the user role and access privileges. Cases are generated from various sources and cases are also manually created in the ECM.

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

Figure 1: ECM Work Flow



2.2 Administration and Configuration Activities

This section covers the following topics:

- Loading Data
- Correlation
- Scoring
- Promoted to Case
- Processing Modelling Framework

- Case Designer
- Case Action Settings

2.2.1 Loading Data

Data is loaded from the landing area to the 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.

2.2.2 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 is identified for correlation-based on business entities in an application (BD, KYC, CS, or third-party). For more information, see the Configuring Correlation section.

2.2.3 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.

2.2.4 Promoted to Case

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

2.2.5 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.

2.2.6 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.

2.2.7 Case Action Settings

Case Action configuration allows the Administrator to add new case statuses, configure case action data, configure standard comment data. The Administrator can configure whether or not the case

actions require a comment, a reassignment, or a due date. For more information, see the Configuring Actions section.

3 Getting Started

This chapter provides step-by-step instructions to log in to the OFS ECM application and manages the different features of the Oracle Financial Services Analytical Applications (OFSAA) application page.

The following sections are covered in this chapter:

- System Requirements
- Accessing OFS ECM Application
- Managing OFSAA Administration Page
- Troubleshooting Your Display
- Setting Preferences

3.1 System Requirements

The following applications are required to run the OFS ECM application:

Table 3 describes the versions of various operating systems.

Table 3: Configurations Supported for Java 8: Operating System

Operating System	Version
Oracle Linux / Red Hat Enterprise Linux (x86-64)	Oracle Linux Server release 7.5 and above - 64 bit Oracle Linux Server release 8 - 64 bit **NOTE:** Same version of RHEL is supported.
Oracle Solaris (SPARC)	11.3+- 64 bit
Shell	KORN Shell (KSH)
NOTE: If the operating system is RHEL, install the package lsb_release with one of the following commands by logging in as root user: ▪ yum install redhat-lsb-core ▪ yum install redhat-lsb	

Table 4 describes the Java Runtime Environment.

Table 4: Configurations Supported for Java 8: Java Runtime Environment

Operating System	Version
Oracle Linux / Red Hat Enterprise Linux	Oracle Java Runtime Environment (JRE) 1.8.x - 64 bit
Oracle Database Server and Client	Oracle Database Server Client 19.3+ Oracle Database Server Enterprise Edition 19.3+ - 64 bit RAC/ Non-RAC with/ without partitioning option

Table 5 describes the OLAP versions.

Table 5: Configurations Supported for Java 8: OLAP

Operating System/Version
V 11.1.2.1+ (Server and Client) with Oracle 11g Database V 11.1.2.3+ (Server and Client) with Oracle 12c Database V 11.2.0.3+ with Oracle 11g Database V 12.1.0.1+ with Oracle 12c Database

Table 6 describes the various operating systems with versions for Web Server/Web Application Server.

Table 6: Configurations Supported for Java 8: Web Server/Application Server

Operating System	Version
Oracle Linux / Red Hat Enterprise Linux/ IBM Solaris	Oracle HTTP Server 11.1.1.1/ Apache HTTP Server 2.2.x/ IBM HTTP Server. Oracle WebLogic Server 12.2.x and 14.1.x - 64 bit IBM WebSphere Application Server 9.0.0.x with bundled IBM Java Runtime - 64 bit Apache Tomcat v9.0.x - 64 bit
NOTE: OFSAA Infrastructure web component deployment on Oracle WebLogic Server with Oracle JRockit is not supported. For deployment on Oracle WebLogic Server (64 bit) with Java 8, download from My Oracle Support.	

Table 7 describes the desktop requirements.

Table 7: Desktop Requirements

Particulars	Version
Operating System	Windows 10
Browser	• Chrome Version 90.0.4430.212 • Firefox Version 78.10.1esr • Microsoft Edge Version 90.0.818.62 Turn off Pop-up blocker settings. For more information, see Configuring Internet Explorer Settings.
Office Tools	• MS Office 2010/2013 • Adobe Acrobat Reader 8 or above
Screen Resolution	Minimum screen resolution & Scaling must be 1366 * 768 with 100% scaling.

Table 8 describes the directory services.

Table 8: Other Software

Particular	Version
Directory Services	OFSAAI is qualified on both OPEN LDAP 2.2.29+ and Oracle Internet Directory v 11.1.1.3.0. However, it can be integrated with other directory services software such as MS Active Directory.
NOTE: • Configuration of Directory services software for OFSAAI installation is optional. For more information on configuration, see Setting Infrastructure LDAP Configuration. • Open LDAP must be installed on MS Windows Server machine.	

3.2 Accessing OFS ECM Application

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

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

Based on your firm's configuration, you can also log in with Single Sign-On (SSO). To access the OFS ECM Application, follow these steps:

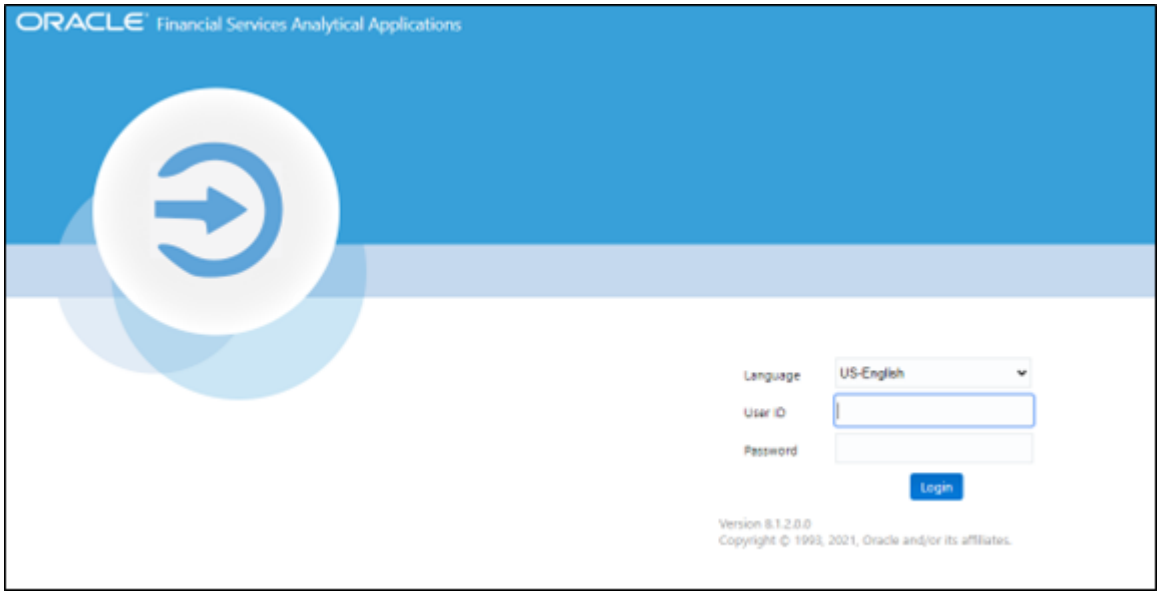
1. Enter the URL into your browser using the following format:

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

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

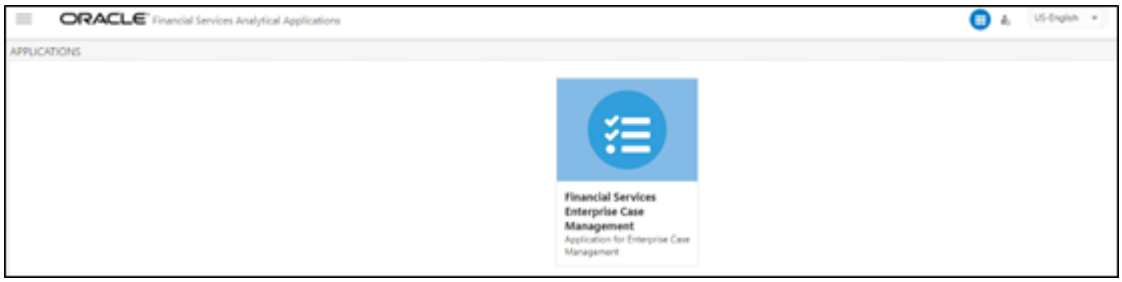
   The OFSAA login page displayed as shown in Figure 2 .

Figure 2: OFSAA Login page



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

Figure 3: Application Landing Page



3.2.1 Masthead

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

Figure 4 depicts the Masthead.

Figure 4: Masthead



The following are the components of Masthead:

- **Hamburger Icon**- This icon is used to trigger the Application Navigation Drawer.
- **Application Icon**- This icon is used to show the available Applications installed in your environment at any time.
- **Administration Icon**- This icon is used to go to the Administration module.

1. Click to view the last login details. It displays the last login date and time as well as the last failed login date and time.
2. Click to view the Information Domain to which you are connected. It also displays the setup details.
3. Click the logged-in user name and the sub-menu is displayed.
4. Click **Preferences** to set the Home Page.
5. Click **Change Password** to change your password. For more information, see the Click Log Out to exit Oracle Financial Services Analytical Applications Infrastructure. The built-in security system of Infrastructure ensures restricted access to the respective windows based on the user's role. This is based on the functions that you as a user are required to perform. section. This option is available only if SMS Authorization is configured.
6. Click **Log Out** to exit Oracle Financial Services Analytical Applications Infrastructure. The built-in security system of Infrastructure ensures restricted access to the respective windows based on the user's role. This is based on the functions that you as a user are required to perform.

3.2.2 Change Password

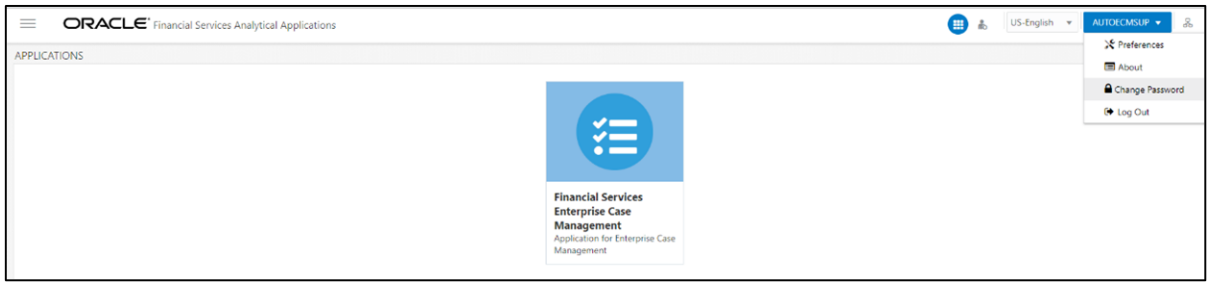
For security purposes, you can change the password. This section explains how to change the password.

To change the password, follow these steps:

1. Navigate to the OFSAA Applications page.

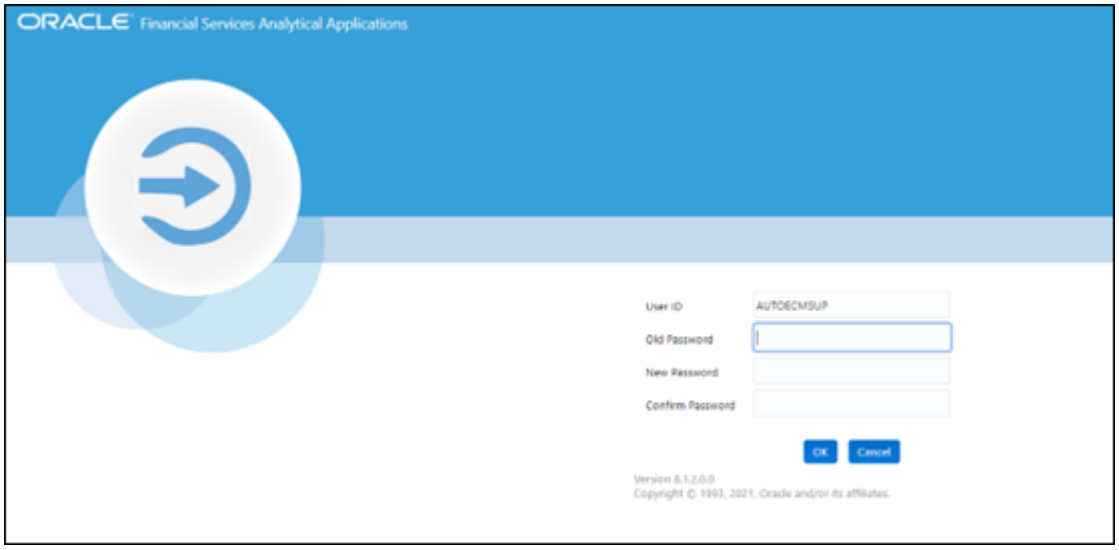
   Figure 5 depicts the applications page.

Figure 5: Applications page



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

Figure 6: Change Password page



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

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

3.2.3 Copyright Information

To access copyright information, click the User drop-down list and select about on the OFSAA login page.

The Copyright text displays in a new window as shown in Figure 7 .

Figure 7: Copyright Information



3.2.4 Selecting Applications

This section explains how to access the required applications.

The OFSAA Applications page has multiple tabs and each tab has specific links to OFSAA Infrastructure and Application modules. The modules which you can access depend on your user role and the OFSAA Application you select. The relevant tabs and links are displayed as shown in Figure 8 .

Figure 8: Selecting Application



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 the OFSAA Applications page.
2. Select **Financial Services Enterprise Case Management**. The Enterprise Case Management page is displayed as shown in Figure 9 .

Figure 9: Case Management page



3.Click **Case Management Configuration**. The Case Management Details are displayed as shown in Figure 10 .

Figure 10: Case Management Details page

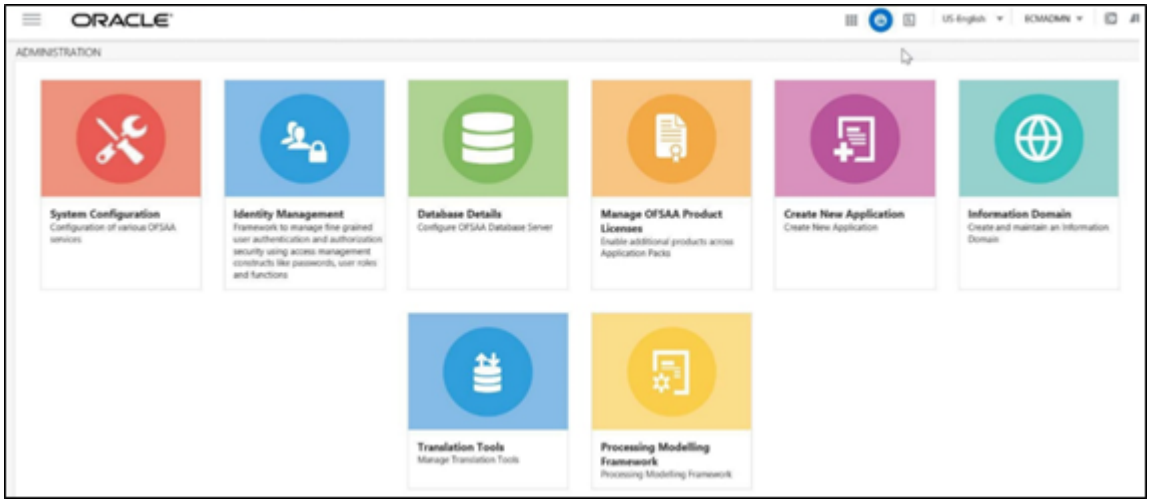


3.3 Managing OFSAA Administration Page

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

Figure 11 depicts the OFSAA administration page.

Figure 11: OFSAA Administration Page



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

3.4 Troubleshooting Your Display

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

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

This section covers the following topics:

- Enabling JavaScript
- Enabling Cookies
- Enabling Temporary Internet Files
- Enabling File Downloads
- Setting Printing Options
- Enabling Pop-up Blocker
- Time Zone Offset

3.4.1 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**.
5. The Security Setting - Local Intranet Zone dialog box displays.
6. In the Settings list and under the Scripting setting, ensure that Enable is selected for all options.
7. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

3.4.2 Enabling Cookies

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

3.4.3 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.

3.4.4 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**.
5. The Security Setting - Local Intranet Zone dialog box displays.
6. Under the Downloads section, ensure that **Enable** is selected for all options.
7. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

3.4.5 Setting Printing Options

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

1. From the Tools menu, click I**nternet Options**.
2. The Internet Options dialog box displays.
3. Click the **Advanced** tab.
4. In the Settings list, under the Printing setting, click **Print background colors and images**.
5. Click **OK** to exit the Internet Options dialog box.

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

3.4.6 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.

3.4.7 Time Zone Offset

The date and time displayed in the ECM application will be offset from the server time zone and correspond to the time zone the user has set on their personal computer.

The time zone offset does not impact:

- Date of Birth
- Date of Incorporation
- Summary grids
- Date/time an email/RFI is sent
- Date/time shown in Print PDF
- Derived Case Attributes which display date/time

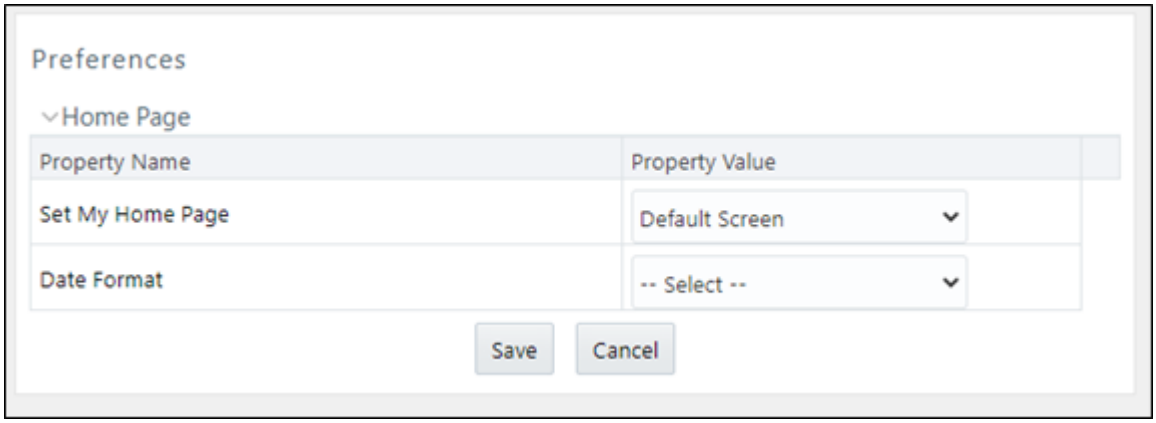
3.5 Setting Preferences

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 as shown in Figure 12 .

Figure 12: Preferences



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

> **NOTE** Whenever a new application is installed, the related value for that application is found in the drop-down list.

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

> **NOTE** In ECM Application, for DEFAULT_DATEFORMAT_REQ, PARAM-VALUE should be set to 'TRUE' in the CONFIGURATION table. Run the below update Query in CONFIG Schema and restart the servers, if the parameter is not set to TRUE.
>
> update CONFIGURATION t set t.PARAMVALUE = 'TRUE' where t.paramname = 'DEFAULT_DATEFORMAT_REQ';

4 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
- Configuring JIT

4.1 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

4.2 Administrator User Privileges

An ECM administrator has the following access permissions:

- User Security Administration
- Excel Upload
- Web Service Configuration
- Common Web Service
- Preferences
- User Administration
- Security Management System
- Security Attribute Administration
- Manage Common Parameters
- Case Management Configuration
- Unified Metadata Manager
- Processing Modelling Framework
- Case Designer

4.3 User Provisioning Process Flow

Figure 13 depicts the user provisioning process flow.

Figure 13: User Provisioning Process Flow

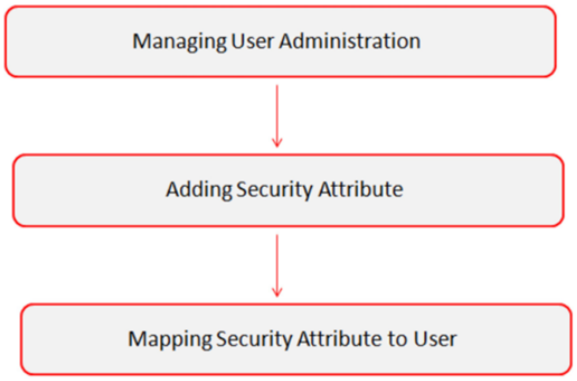


Table 9 lists the various actions and associated descriptions of the user administration process flow.

Table 9: 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.

4.3.1 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 as described in Table 10 :

Table 10: Requirements

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

4.4 Managing User Administration

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

4.4.1 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
- Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload
- Creating or Editing User
- Mapping a User with a User Group

4.4.1.1 Managing Identity and Authorization Process Flow

Figure 14 shows the process flow of identity management and authorization.

Figure 14: Managing Identity and Authorization Process Flow

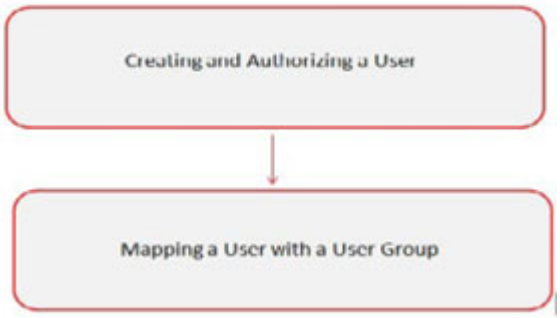


Table 11 describes the Administration Process Flow.

Table 11: 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.

4.4.1.2 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 the Security Management System (SMS) and are stored in the Config Schema. User security attribute associations are defined using Security Attribute Administration.

> **NOTE** Make sure the same User ID should not already exist as an organization in the KDD_ORG table.

For more information on creating and authorizing a user, see Chapter 9: Oracle Financial Services Analytical Applications Infrastructure User Guide.

4.4.1.3 Load User Configuration Data into CSSMS_ATTRIB_MAST table Using Excel Upload

To load user configuration data, follow these steps:

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

4.4.1.4 Creating or Editing User

To create or edit a user, follow these steps:

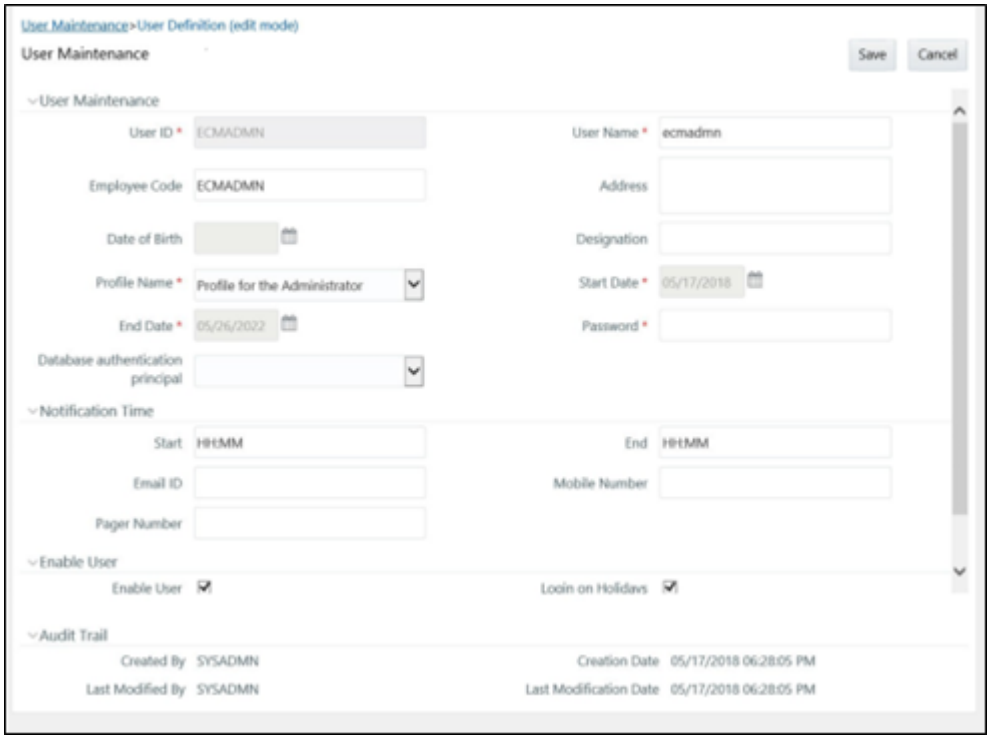
1. Create or Edit the user for which you must map the Security Attributes.

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

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

Table 15 depicts the user maintenace page.

Figure 15: User Maintenance



4.4.1.5 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 12 describes the Case Management User Roles and corresponding User Groups.

Table 12: Case Management Roles and User Groups

User Role	Group Name	User Group Code
Case Analyst2	Case Analyst2 User Group	CMANALYST2UG
Case Supervisor	Case Supervisor User Group	CMSUPERVISORUG
Case Viewer	Case Viewer User Group	CMVIEWERUG
Case Administrator	Case Administrator User Group	CMMANADMNUG
CM Level 1 Analyst*	CM Level 1 Analyst Group	CMANALYSTLVL1GRP
CM Level 1 Supervisor*	CM Level 1 Supervisor Group	CMSUPRVISRLVL1GRP
CM Front Office Analyst	CM Front Office Analyst Group	CMFRNTOFCANLYSTGRP
CMSECROLE	This role can be used for mapping to user groups, which are created only for security Attribute Mapping purposes. User groups mapped to this role will appear in the Mapper Maintenance screen, along with the OOB User Groups.	
ECM QC Analyst	This role is defined out of the box. Group must be created in the identity management and associate this role to the created group in User Group Role Map.	

Table 12: Case Management Roles and User Groups

User Role	Group Name	User Group Code
ECM QC Supervisor	This role is defined out of the box. Group must be created in the identity management and associate this role to the created group in User Group Role Map.	

* Applicable to Restricted Use License for AML Enterprise and Fraud Enterprise editions.

NOTE If a user logs in with multiple roles, then the system will display actions on the Case List and Case Details page based on the highest role. In the Take Action pop up window, if Supervisor and Analyst both roles are mapped to a user, then Analyst actions will be suppressed provided below notation is followed:

- If a user logs in with multiple roles, then the system will display actions on the Case List and Case Details page based on the highest role. In the Take Action pop up window, if Supervisor and Analyst both roles are mapped to a user, then Analyst actions will be suppressed provided below notation is followed:
  - **Supervisor Actions**: Action code should be suffixed with S.
  - **Analyst Actions**: Action code should be suffixed with A.
- Do not assign Admin roles and Investigation roles (Supervisor, Analyst, Viewer roles) together for a user.

Trusted Pair and Event Suppression:

- To get Trusted Pairs admin permission, user role must be mapped with the CMADMNTP (V_FUNCTION_CODE) function
- To get Designate Trusted Pairs in Case's Event Details page, user role must be mapped with the CMDSGTP (V_FUNCTION_CODE) function
- The Trusted Pairs administration menu will display for users having Trusted Pairs administration permission. To get the permission, user role to be mapped to CMADMNTP (V_FUNCTION_CODE) function. For more information on user role - function map see AAI Administration Guide.
- To get Designate Suppression permission, user role must be mapped with the CMDSGSUP (V_FUNCTION_CODE) function.
- To get Suppression view permission, user role must be mapped with the CMVIEWSUP (V_FUNCTION_CODE) function.
- To get Suppression edit permission, user role must be mapped with the CMEDITSUP (V_FUNCTION_CODE) function.
- The Suppression Administration menu will display for users having Suppression View permissions. For more information on user role - function map see AAI Administration Guide.

4.5 Adding Security Attributes

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

This section covers the following topics:

- Prerequisites
- About Security Attributes
- Loading Security Attributes

4.5.1 Prerequisites

Update the FCC_SECURITY_ATTRIBUTES table before triggering the batch.

Table 13 contains information about Jurisdiction, Business Domain, and their attribute priority.

Table 13: FCC_SECURITY_ATTRIBUTES

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

Here, the V_ATTRIBUTE_VALUE should be the same as mentioned in the V_JURISDICTION_CD and V_BUSINESS_DOMAIN_CD columns of the FCC_EVENTS table. For example, if we have events generated with V_JURISDICTION_CD as "AMEA" and V_BUSINESS_DOMAIN_CD as "a" then the same should be updated in the respective column of FCC_SECURITY_ATTRIBUTES table.

4.5.2 About Security Attributes

Security Attributes help an organization classify their users based on their geography, jurisdiction, and business domain, 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.

4.5.2.1 Types of Security Attributes

The following are the security attributes:

- Jurisdiction
- Business Domain
- Case Type
- Organization

4.5.2.1.1 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 jurisdiction and users of the system must be associated with one or more jurisdictions. In the Case Management system, users can view only data or cases associated with jurisdictions to which they have access. You can use jurisdiction to divide data into the database. For example:

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

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

4.5.2.1.2 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 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:

- Private Client
- Retail Banking

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

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

4.5.2.1.3 Case Type

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

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

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

4.5.2.1.4 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.

4.5.3 Loading Security Attributes

This section covers the following topics:

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

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

4.5.3.1 Loading Security Attributes through Excel

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

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

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

Security attributes are loaded through Excel using the following templates as shown in Table 14 :

Table 14: Security Attributes and Excel Templates

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

4.5.3.2 Uploading Excel

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

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

4.5.3.3 Loading Security Attributes through SQL Scripts

This section covers the following topics:

- `update KDD_CENTRICITY set bus_dmn_st = 'a' where KDD_CENTRICITY. CNTRY_TYPE_CD = 'SC'`
- `VALUES ('E', 'East', 'East', 'Eastern')`
- `update KDD_CENTRICITY set bus_dmn_st = 'a' where KDD_CENTRICITY. CNTRY_TYPE_CD = 'SC'`

4.5.3.3.1 Loading Jurisdictions

To load jurisdictions in the database, follow these steps:

Add the appropriate record to the KDD_JRSDCN and KDD_JRSDCN_TL database table as mentioned in Table 15 and Table 16 .

Table 15: 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_DSP- LY_NM	Display the name of the jurisdiction such as North or South.
JRSDCN_DESC_TX	Description of the jurisdiction such as Northern US or Southern US.

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

Table 16: KDD_JRSDCN_TL table details

Column Name	Description
V_LOCALE_CD	Locale code of the Data. Example: en_US
JRSDCN_CD	Code (one to four characters) that represents a jurisdiction such as N for North, or S for South.
JRSDCN_NM	Name of the jurisdiction such as North or South.
JRSDCN_DSPLY_NM	Display the name of the jurisdiction such as North or South.
JRSDCN_DESC_TX	Description of the jurisdiction such as Northern US or Southern US.
V_CREATED_BY	Not Applicable
D_CREATED_DT	Not Applicable
V_SOURCE_LOCALE	The data from the TL table will be auto replicated for all the support languages where there is no data.

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

2.
```
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.

4.5.3.3.2 Loading Business Domains

To load a business domain, follow these steps:

1. Add the appropriate user record to the KDD_BUS_DMN database table as mentioned in Table 17 .

Table 17: 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_DSP- LY_NM	Display the name of the business domain, such as INST or RET.

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

2. Add the appropriate user record to the KDD_BUS_DMN_TL database table as mentioned in Table 18 .

Table 18: KDD_BUS_DMN_TL Table Attributes

Column Name	Description
V_LOCALE_CD	Locale code of the Data. Example: en_US
BUS_DMN_CD	Single-character code that represents a business domain such as a, b, or c.
BUS_DMN_DESC_TX	Description of the business domain such as Institutional Broker-Dealer or Retail Banking.
BUS_DMN_DSPLY_NM	Display the name of the business domain, such as INST or RET.
V_CREATED_BY	NA
D_CREATED_DT	NA
V_SOURCE_LOCALE	The data from the TL table will be auto replicated for all the support languages where there is no data

3. Add more records to the table using a SQL script similar to the following sample script:
4. 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');

```
5. 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;
```

6. Update the `KDD_CENTRICITY` table to reflect access to all focuses within the business domain with the following command:
7. `update KDD_CENTRICITY set bus_dmn_st = 'a' where KDD_CENTRICITY. CNTRY_TYPE_CD = 'SC'`

4.5.3.3.3 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 19 .and Table 20

Table 19: 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	The parent organization of which this organization is considered to be a child. **NOTE**: This should reference an ORG_CD in the KDD_ORG table.

Table 19: KDD_ORG Table Attributes

Column Name	Description
MODFY_DT	Last modified date and time for this organization record.
MODFY_ID	User ID of the user who last modified this organization data. **NOTE**: This should reference a user in the Investigation Owner table (KDD_REVIEW_OWNER.OWNER_SEQ_ID). You can also set the value to `owner_seq_id` to 1, which is the SYSTEM value if another suitable ID is not available.
COMMENT_TX	Additional remarks are added by the user.

2. Add the appropriate user record to the `KDD_ORG_TL` database table as mentioned in Table 20 .

Table 20: KDD_ORG_TL Attributes

Column Name	Description
V_LOCALE_CD	Locale code of the Data. Example: en_US
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.
V_CREATED_BY	NA
D_CREATED_DT	NA
V_SOURCE_LOCALE	The data from the TL table will be auto replicated for all the support languages where there is no data.

3. Add more records to the table using a SQL script similar to the following sample script.
4.
```
INSERT INTO KDD_ORG (ORG_CD,ORG_NM,ORG_DESC_TX,PRNT_ORG_CD,MODFY_DT,MOD-
FY_ID,COMMENT_TX) VALUES ('ORG1','COMPLIANCE ORG','DEPARTMENT FOR INVES-
TIGATION','ORG1 PARENT ORG','01-JUN-2014',1234,'ADDING KDD_ORG ENTRIES')
```

4.6 Mapping Security Attributes to Organizations and Users

This section covers the following topics:

- Using Mapper MaintenanceIntroduction
- Prerequisites for Mapper Maintenance
- Using Mapper Maintenance

4.6.1 Introduction

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

The following are members of the Mapper:

- Usergroups

- Organization
- Jurisdiction
- Business Domain
- Case Type

4.6.2 Prerequisites for Mapper Maintenance

The following are the prerequisites for Mapper Maintenance:

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

4.6.2.1 Loading Security Attributes Data

To load security attribute data, follow these steps:

1. Load the security attribute data into the following tables as described in Table 21 :

Table 21: Security Attribute Table

Security Attribute	Table Name
Organization	KDD_ORG
Jurisdiction	KDD_JRSDCN
Business Domain	KDD_BUS_DMN
Organization Locale specification	KDD_JRSDCN_TL
Jurisdiction Locale specification	KDD_BUS_DMN_TL
Business Domain Locale specification	KDD_ORG_TL

For more information, see the Loading Data.

4.6.2.2 Configuring Function

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

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

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

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

4.6.2.3 Resaving Metadata

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

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

4.6.2.3.1 Hierarchy Re-save

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

4.6.2.3.2 Derived Entity Re-save

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

4.6.2.4 Loading User Configuration Data

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

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

4.6.3 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 user group) 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**.

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

   Figure 16 depicts the Map Maintenance page.

Figure 16: Map Maintenance



4. User Group Security mapper window is displayed. Click **Add**.

   Figure 17 depicts the User Group Security Mapper page.

Figure 17: User Group Security Mapper window



5. The Add Mapping Screen is displayed with all the Hierarchies.
   - User groups 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. For more information, see Configuring ECM Security Function.
   - Organization: A User or Organization's access to other Organizations depends on the selection(s) made for this organization parameter. For example, if a user is mapped to Org1 and Org2, then the user can access these two organizations, but other security attributes are also should match.

- Jurisdiction: Mapping of one or more jurisdictions to a usergroup, gives the privilege of accessing cases that belong to the mapped jurisdiction.
- Business Domain: Mapping of one or more business domains to a usergroup gives the privilege of accessing cases that belong to the mapped business domains.
- Case Type: Mapping of one or more Case Types to a usergroup gives them the privilege of accessing cases that belong to the mapped Case Type.

6. Select the required values from each hierarchy and click **Go**. Click **Save**.
7. Click **Save**. You are directed to the previous screen, where the Member combinations can be viewed. All the changes get saved in the ECM_SECURITY_ACCESS_MAPPER table and respective view ECM_SECURITY_ACCESS_MAPPER_VW.

> **NOTE** Member Combinations will show you the mappings you made in the Add Mapping Screen. Mapped Members section will show you all the actual members participating in the selection (same as the content stored in ecm_security_access_mapper/ ecm_security_access_mapper_vw).
>
> All the exploded mappings can be seen in this section. You can navigate to all the pages of the same section to see the mappings.
>
> If you want to remove the mapping from the mapper. Select a mapping from the first panel and click Remove. You should click Pushdown to effect these changes in the system.
>
> For more information on Mapper, see the Oracle Financial Services Analytical Applications Infrastructure User Guide.

4.6.3.1 Updating Control Access tables from Mapper

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

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

- Batch Maintenance
- Batch Execution
- Batch Monitor/Checking the Execution Status

4.6.3.2 Changing ICC Batch Ownership to ECM Admin from SYSADMN user

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

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

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

```
begin

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

OR
```

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

Here,

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

  For example:

```
begin
AAI_OBJECT_ADMIN.TRANSFER_BATCH_OWNERSHIP('SYS-
ADMN','ECMADMN','ECMINFO');
end;
```

4.6.3.2.1 Batch Maintenance

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

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

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

2. Select the `<Infodom>_ECM_SECURITY_BATCH` and select the Task1. Click Edit from the Task Details section.
3. Modify the Parameter List. Seeded values are p_create_id.
4. For the Parameter List-Syntax is `'p_create_id','p_user_id'`.
   - `op_create_id`: Current Admin User who is going to execute the Batch.
   - `op_user_id`: User(s) for which the Security Attribute Mapping changed through the Security Mapper.

   This can be changed in the following two ways:

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

4.6.3.2.2 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 as shown in Figure 18 .

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

   For more information, see the Oracle Financial Services Analytical Applications Infrastructure Guide.
3. The seeded batch (<Infodom>_ECM_SECURITY_BATCH) must be executed for the required MIS Date on this screen.
4. Select <Infodom>_ECM_SECURITY_BATCH and provide the Current Date in the Information Date section.
5. Click **Execute Batch**.

4.6.3.2.3 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.

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

   Following are the status messages in Batch Monitor:
   - N: Not Started
   - O: On Going
   - F: Failure
   - S: Success

2. 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.

4.6.3.3 Mapping Read-Only Case type

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

4.7 Configuring JIT

To configure Just in Time (JIT) security attributes, follow these steps:

1. Login as the SYSADMN and update the following in the System Configuration Details.
   a. Select the Authentication Type as LDAP Authentication and SMS Authorization and click **Add**. Provide your LDAP Server Details and click Save.
   b. Check the JIT Provisioning Enabled option.
2. Login to LDAP Server and create the Application UserGroups and users and map them.

In the Atomic Schema a new table FCC_GROUP_SEC_ATTR_MAP is introduced to configure the Security attributes mapping to the Application User Groups.

1. Login to Atomic Schema and configure security attributes to the User groups.
2. Populate the V_GROUP_CD column with the User groups mapped to User.

   For ECM, valid values are:

   - V_SEC_ATTR_CD column: JRSDCN, ORG, BUSDMN and CASETYPE.
   - V_SEC_ATTR_VAL column: Jurisdiction,Organization, Business Domain and Casetype
   - These values must be available in the KDD_JRSDCN and KDD_JRSDCN_TL,KDD_ORG and KDD_ORG_TL, KDD_BUS_DMN and KDD_BUS_DMN_TL,KDD_CASE_TYPE_SUBTYPE and KDD_CASE_TYPE_SUBTYPE_TL table respectively.
3. Configure the following additional User Attributes:
   - Case Own Flag: Create the CMCASEOWNFLUG group in the LDAP Server and map to the User in LDAP.

     If the Case Own Flag for a User should be Y, then map this group to the User.

     If the Case Own Flag for a User should be N , then make sure it is not mapped to the User.
   - Reporting/Line Organization : Create a User group with Prefix as ORG_CD (from KDD_ORG table) and suffix as LORG.

     For example: If TestOrgA is the Line organization then create a User group as TESTORGALORG.

> **NOTE** If the Usergroup is created and mapped to the Infodom/Segment and LINEORG Role in the OFSAA Application, then it should also be created in LDAP and mapped to the User. Verify that only one LORG group is mapped for a user. If the LORG Group is mapped as part of any other Application then there is no need to map again.

4. Configure the Security Mapping for the Pool Users in the FCC_GROUP_SEC_ATTR_MAP table in the Atomic Schema.
   - V_GROUP_CD column: Populated with the LORG group created above.
   - For ECM , Valid values for the V_SEC_ATTR_CD column are JRSDCN, BUSDMN and CASETYPE.
   - For ECM , Valid values for the V_SEC_ATTR_VAL column are Jurisdiction, Business domain and Casetype. These must be available in KDD_JRSDCN and KDD_JRSDCN_TL,KDD_ORG and KDD_ORG_TL, KDD_BUS_DMN and KDD_BUS_DMN_TL,KDD_CASE_TYPE_SUBTYPE and KDD_CASE_TYPE_SUBTYPE_TL table respectively.
5. Login with the New User in the Application and verify the completed security attributes mapping, and that the User is able to see pages based on their Roles and can see the Cases based on the security attribute mapping.

4.7.1 Configure JIT for Existing Users

Use this section to configure JIT for an existing user.

If extra User groups are mapped in the LDAP Server, then follow these steps:

Login with Admin user and verify the following:

- Security attributes mappings are complete.
- Users can view pages based on their Roles.
- Users can view Cases based on the security attribute mapping.

If any User groups are unmapped in the LDAP server then follow these steps:

1. Unmap the User groups from Application.
2. Login with Admin user and navigate to Batch Maintenance.
3. Create a Batch, and add the ECM task FCC_ECM_JIT_SYNCH.

If the User group mapping does not require any changes and only Security Attribute Mapping changes are required, follow these steps:

1. Login with Admin user and navigate to Batch Maintenance.
2. Create a Batch, and add the ECM task FCC_ECM_JIT_SYNCH.
3. In the Batch Execution screen, execute the Batch. You can monitor the batch progress in the Batch Monitor screen.

Running this batch will sync security attributes mapping for all users in the KDD_REVIEW_OWNER table.

4.7.2 Disable LDAP Users

To disable user who are disabled on LDAP, follow these steps:

1. Log in as the Admin user and Navigate to Batch Maintenance and create a Batch.

   For ECM ,add the ECM task FCC_ECM_JIT_DIS_USR to the newly created Batch.
2. Edit the Task by providing one or more User IDs, enclosed in Single Quotes (') in the Parameter Section. Multiple IDs must be comma (,) separated .

For example: 'CMSUP,CASEANA' where CMSUP,CASEANA are users to be disabled in the KDD_REVIEW_OWNER table.

5 Pre-batch Execution Configuration

This chapter provides the details of pre-batch configuration activities. Configure the following before executing a batch:

5.1 Configuring Processing Group

1. Add a new entry in the FCC_PROCESSING_GROUP table. For example, N_GROUP_ID can be 100 or 104 and V_GROUP_NAME can be E2E BATCH ALL SOURCE or MAN.

   For example, E2E BATCH ALL SOURCE and MAN are the group names provided in Table 22 FCC_PROCESSING_GROUP. N_GROUP_ID should be the next greater numeric value.

   Table 22: FCC_PROCESSING_GROUP (Metadata Table)

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

2. Configure the parameters in Process UI (under components) from the FCC_PROCESSING_GROUP table. For example:

   "MAN","","ALL","START","IND"

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

   For more information, see the Starting a Batch Run section.

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

5.2 Configuring Correlation

> **NOTE** From ECM 8.0.7.0.0 onwards, the default correlation is PGX.
>
> PGX correlation does the same job as JAVA/SQL correlation (BD_Correlation) do, but further drill down approach. It helps us to identify all the relationships between the entities and pres- ent it in a graph.
>
> If you want to use BD_Correlation process, then follow the below steps:
>
> 1. Remove the PGX Process.
> 2. Add the BD_Correlation process. Refer to below screenshot.
> 3. Trigger the batch.

3. Initiating Correlation

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

   To initiate the correlation, follow these steps:

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

4. Configuring Correlation Rules

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

   Table 23 shows an example of the rule logic defined in the FCC_CORRELATION_RULE table:

> **NOTE** In the `FCC_CORRELATION_RULE` table, the range of *N_CORRELATION_RULE_SKEY* must be *900-999* for customizations.

Table 23: Table 6: FCC_CORRELATION_RULE

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

- `N_CORRELATION_RULE_SKEY` (*required*): This is the correlation rule unique Identification number.
- `V_RULE_NAME` (*required*): Defines the name of the correlation rule.
- `N_PATH_PRECEDENCE` (*required*): Number indicating the maximum precedence value that a business entity shared between events must have to be considered a correlation by this rule. The lower the precedence number the stronger the relationship. Events are not considered for the correlation unless the precedence number associated with the business entity-to- event is less than or equal to (<=) the value defined.
- `V_EVENT_FILTER_OPERATIONS` and `V_EVENT_LINK_OPERATIONS` (*optional*): Defines operations used to further constrain the events to be used for correlation. An operation consists

of an event attribute compared to a numerical value, such as from event and to event which can be correlated if they both have `SCORE_CT >= 0`, represented by `CORR.SCORE_CT >= 0`, or a from event and to event which can be correlated if `CORR._CT > 2`. The set of supported comparison operators are: =, `!=`, <, >, <=, >=, `IN`, and `NOT IN`.

- Because the `SCNRO_ID` attribute of both events and correlations can potentially have multiple values, only the `IN` and `NOT IN` operators should be used in expressions involving `SCNRO_ID`. The rest of the operators can only support single value operands. Also, there should be no space in the scenario ID list specified. For example, `BOTH.SCNRO_ID IN (115600002,114690101)`.
- Multiple operations can be joined together by logical `AND` and `OR` operators and operation precedence can be defined with parentheses.
- `N_LOOKBACK_VALUE` (*optional*): The number attribute indicates the number of days to look back from the current date/time to create a time window to consider events for correlation. This is a created timestamp of the event.

  If the lookback value is defined, then the lookback unit is also required.
- `V_LOOKBACK_UNIT` (*required*): The unit attribute identifies the unit of the look back number. Possible values are D and CM for days and current month, respectively. All of these require a valid number value except for CM, which essentially makes the look back to 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 created timestamp of the event is used to determine whether or not an event falls within the lookback period.

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

  Changes made to the metadata are effective immediately and are utilized the next time correlation is run.
- `V_CASE_TITLE_RULE`: This is used for defining the title of the case.

5.3 Configuring Ending Batch Process

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.

5.4 ASC Batch Configuration

> **NOTE** You must apply Patch # 8.1.2.7.4 for the following configurations to work.

The following configurations must be completed before ASC batch run:

1. Add *AML_SURV_BTL* case type in Business Hierarchy. To add:
   a. Navigate to Common Tasks > Unified Metadata Manager > Business Metadata Management > Build Hierarchy.
   b. Select **PCASTYP** (Pre Case type) and click **Edit**.
   c. In the Business Hierarchy section, select the AML node and click **Edit**.
   d. Add *AML_SURV_BTL* case type in Node Identifier and click **Save**.

      For example: FCC_PRECASE.V_CASE_TYPE in ('AML_SURV','AML_SURV_BTL','AML_DD','AML_TER','AML_PAT')
2. Make sure the Auto Assignment rules are configured to pick and assign the cases with AML_SURV_BTL case type and also Security mapping and Security batch are executed so that Users can access cases with AML_SURV_BTL case type.

   For more information, see Configuring Case Allocation and Mapping Security Attributes to Organizations and Users.
3. If OFS BD and ECM are on the same schema, run the following query in the Config schema and commit the changes:

```
select * from PR2_PROCESS_TASK_PARAMETER where V_TASK_PARAMETER_VALUE
LIKE '%ASC%' ;

(Check the SOURCENAME and LOADTYPE  and replace it by empty string using
the below query  as reference)

update PR2_PROCESS_TASK_PARAMETER

set V_TASK_PARAMETER_VALUE = replace(replace(V_TASK_PARAMETER_VALUE,

'"SOURCENAME=##OFS_ECM_AML_SOURCE##"', '"SOURCENAME="'),
'"LOADTYPE=##OFS_ECM_AML_LOADTYPE##"', '"LOADTYPE="')

WHERE v_task_parameter_value LIKE '%ASC%';
```

   OR
4. If OFS BD and ECM are on different schemas:
   a. Create the Database Link in the ECM Schema to Connect to the ASC/BD Atomic Schema (Use the Database sys user to create the DB LINK)

```
CREATE PUBLIC DATABASE LINK <DB_LINK_NAME>

CONNECT TO <BD/ASC_ATOMIC_SCHEMA>

IDENTIFIED BY <password>

USING
'(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(PORT=<PORT_NO>)(H
OST=<hostname>)))(CONNECT_DATA=(SID=<SID_NAME>)))';
```

b. Run the following query after replacing ##OFS_ECM_AML_SOURCE## with DB_LINK_NAME and ##OFS_ECM_AML_LOADTYPE## as 'DBLINK' in the Config schema and commit the changes:

```
select * from PR2_PROCESS_TASK_PARAMETER where V_TASK_PARAMETER_VALUE
LIKE '%ASC%' ;
```

(Check the SOURCENAME and LOADTYPE and replace it by ##DB_LINK_NAME## and DBLINK using the below query as reference)

```
update PR2_PROCESS_TASK_PARAMETER

set V_TASK_PARAMETER_VALUE = replace(replace(V_TASK_PARAMETER_VALUE,

'"SOURCENAME=##OFS_ECM_AML_SOURCE##"',
'"SOURCENAME=##DB_LINK_NAME##"'),
'"LOADTYPE=##OFS_ECM_AML_LOADTYPE##"', '"LOADTYPE=DBLINK"')

WHERE v_task_parameter_value LIKE '%ASC%';
```

5. Run the following query in the ASC BD schema to find the MIS date for the batch:

```
SELECT V_RUN_ID, PRCSNG_DT

FROM fcc_am_events

WHERE V_RUN_ID IN (SELECT RUN_ID FROM asc_event_sample)

GROUP BY V_RUN_ID, PRCSNG_DT

ORDER BY V_RUN_ID, PRCSNG_DT ASC;
```

6. In the ECM UI, navigate to Common Tasks > Rule Run Framework > Run.
   a. Select the *Oracle_ASC_Event_Processing* batch, click **Fire Run**.
   b. Select Batch mode (Create and Execute), and provide the MIS Date from the query mentioned above.

6 Performing Batch Run

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

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

6.1 About Batch Run

The ECM application batch run comprises of the following processes:

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

> **NOTE** You must configure your own batches and default OOB must not be run as it is a sample run.

6.2 Starting a Batch Run

> **NOTE** For executing a batch, you cannot start two batches simultaneously for the same processing group.

This section explains how to start the batch run. To start the batch run, follow these steps:

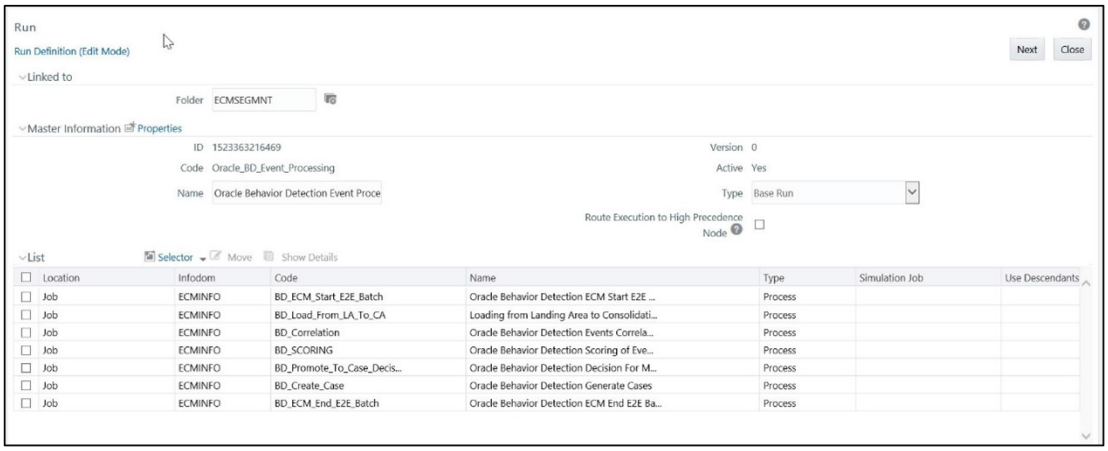
1. Navigate to Enterprise Case Management Application.
2. Go to the **Common Tasks** section. Select the `Rule Run Framework`.
3. Click **Run**. The Run window is displayed with the available Processes as shown in Figure 19 .

Figure 19: Application List



4. Go to the List section. Select an application for example (`Oracle_BD_Event_Processing`). The list of processes for the selected application is displayed as shown in Figure 20 .

Figure 20: List of Processes screen



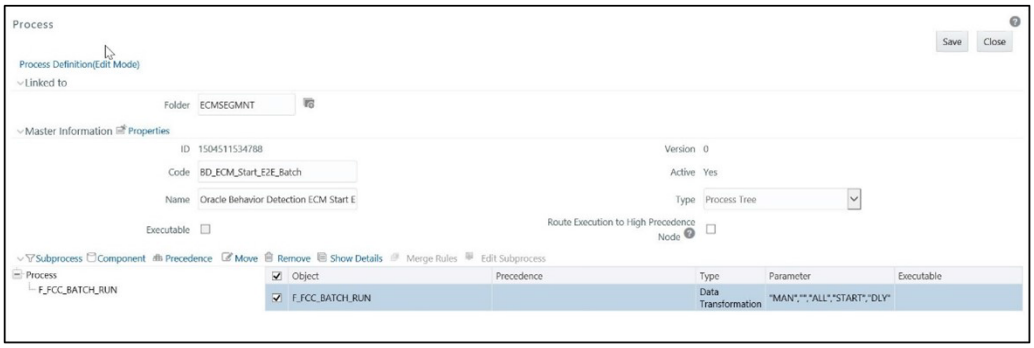
5. Navigate to Process Summary Page and search for **BD_ECM_Start_E2E_Batch**.
6. Select the batch **BD_ECM_Start_E2E_Batch** as shown in Figure 21 and click **Edit**.

Figure 21: Process screen



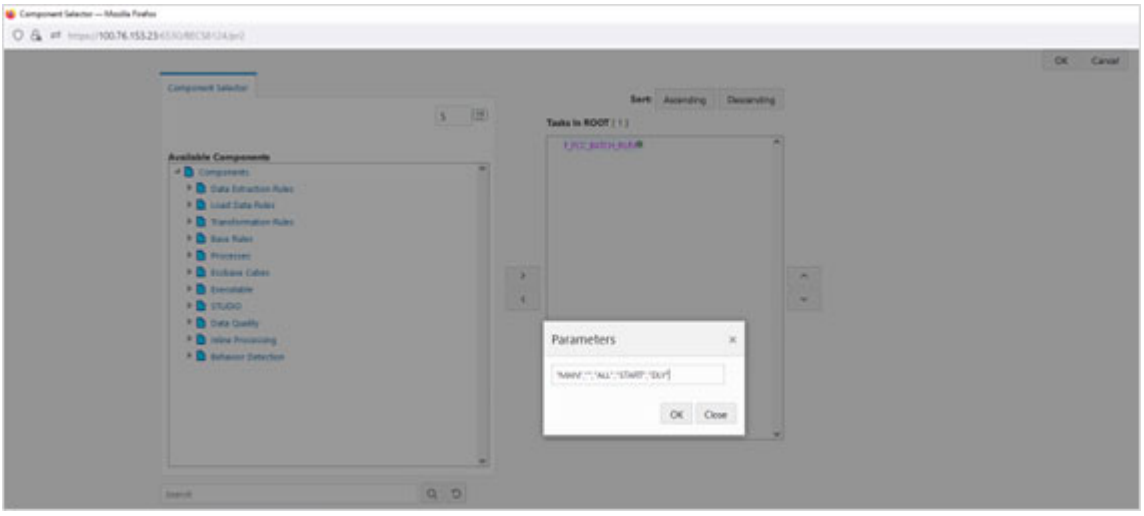
The Process Definition page is displayed as shown in Figure 22 .

Figure 22: Process screen



7. Click **Component**. The Component Selector window is displayed.
8. Under the **Tasks In ROOT** section, right-click on the required batch, and then click **Add Parameters**. The Parameters window is displayed as shown in Figure 23 .

Figure 23: Parameters



The following are default parameters: "MAN","","ALL","START","DLY"

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

The following is an example of a parameter

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

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

6.3 Ending a Batch Run

This section explains how to end the batch run.

To end the batch run, follow these steps:

1. Navigate to the Process Summary page and search for End Batch as shown in Figure 24 , for example, `BD_ECM_End_E2E`.

Figure 24: Process



2. Select the batch, and click **Edit**. The Process Definition page is displayed.

3. Click **Component**. The Component Selector window is displayed.
4. Under the **Tasks In ROOT** section, right-click on the required batch, and then click **Add Parameters**. The Parameters window is displayed.

   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**.

6.4 Executing a Batch Run

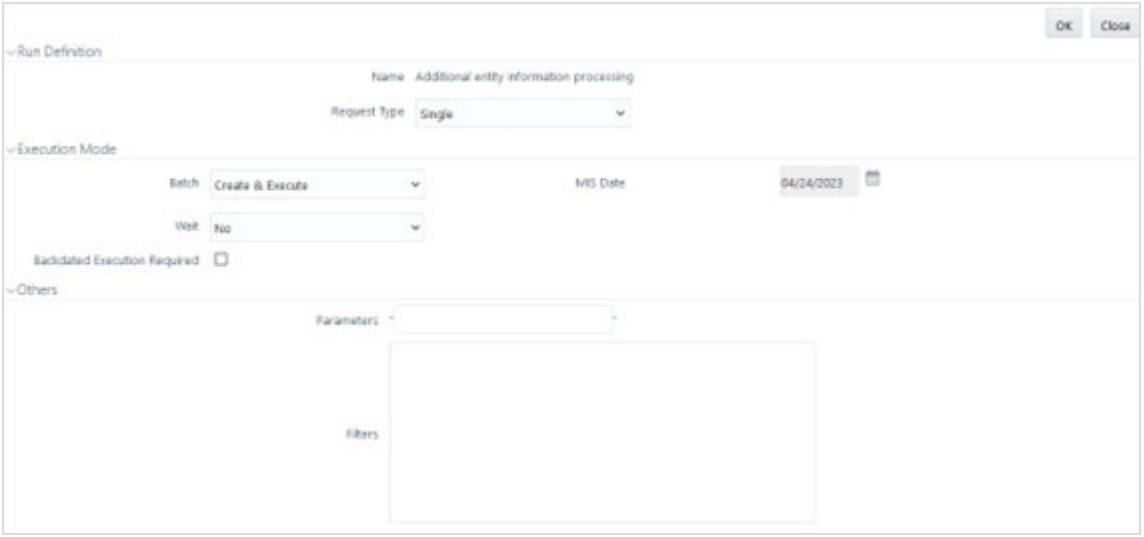
This section explains how to execute the batch run.

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

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

1. Navigate to Enterprise Case Management Application.
2. Go to the Common task section. Select the **Run Rule Framework**.
3. Click **Run**. The Run window is displayed with the available Processes.
4. Select the Application process from the Run definition page list that is to be executed and click **Fire Run**. The Fire Run window is displayed as shown in Figure 25 .

Figure 25: Fire Run



5. Enter the following details as shown in Table 24 :

Table 24: Adding Fire Run Details

Fields	Description
Request Type	Select Request Type based on the following options: • Single: If the batch must be executed once. • Multiple: If the batch must be executed multiple times at different intervals.
Batch	Select Batch. It has the following options: • Create • Create & Execute From these options, select Create & Execute.
Wait	Select Wait. It has the following options: • Yes: This executes the batch after a certain duration. Enter the duration as required. • No: This executes the batch immediately.
Filters	Enter the filter details. **NOTE**: $MISDATE option can be used to execute the run for that particular day. The format for it to enter the filter details is: `to_date(<ACTIVITY_TABLE_NAME>.<ACTIVITY_DT_COL>)=$MISDATE` **NOTE**: For $MISDATE option: • For either Date or Timestamp datatypes, to_date is mandatory for the filter. • Activity Table Name and Activity Column Name should be in the capital.

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

> **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.

8. Once the batch is triggered, the following processes get executed:
   a. Start ECM batch, select the required process code. For example, BD_ECM_Start_E2E_Batch. For more information on starting the batch, see Starting a Batch Run.
   b. Load events, evented, and business data to the Consolidation area, select the required process code. For example, BD_Load_From_LA_To_CA. For more information on using this connector, see Loading Data.
   c. Perform correlation on loaded events and select the required process code. For example, BD_Correlation. For more information on using correlation, see Configuring Correlation.
   d. Perform scoring on correlated events and select the required process code. For example, BD_SCORING. For more information on using scoring, see Scoring.

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

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

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

Table 25 provides you the details of Applications and related processes.

Table 25: Application Run processes

Process	Applications and Process Name					
	OBD	**OCS**	**OKYC**	**OTBAML**	**OSTDO**	**Third-party**
Start ECM batch	BD_EC-M_Start_E2E_Batc h	ECM_Start_E2E_Batch_- For_CS	ECM Start E2E Batch For KYC	TBAML_EC-M_Start_E2E_Batch	STDO_EC-M_Start_E2E_B atch	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_C A	TBAML_-Load_-From_LA_To_CA	STDO_Load_-From_LA_To_C A	Load_-From_LA_To_CA
Perform correlation on loaded events	BD_Correlation	Correlation	Correlation	TBAML_Correlation	STDO_Correlation	Correlation
Perform scoring on correlated events	BD_SCORING	Scoring_OCS	Scoring_OKYC	TBAML_SCORING	STDO_SCORING	Scoring
Decision to promote correlated events to a case	BD_Promote_To_Case_Decision	Promote_To_Case_Decision_OCS	Promote_To_Case_Decision_OKYC	TBAML_Promote_To_Case_Decision	STDO_Promote_To_Case_Decision	Promote_To_Case_Decision
Create a case	BD_Create_Case	Create_Case	Create_Case	TBAML_Create_Case	STDO_Create_Case	Create_Case
End ECM batch	BD_ECM_End_E 2E_Batch	ECM_End_E2E_Batch_For_CS	ECM_End_E2E_Batch_For_KYC	TBAML_ECM_End_E2E_Batch	STDO_ECM_End_E2E_Batch	ECM_End_E2E_Batch

6.5 Batch Performance Recommendations

This section provides some tips to improve batch performance.

- If any performance bottlenecks are coming up in the following tasks, try modifying to the data movement operation to Merge Insert (MI) instead of Delete Insert (DI).
  - Oracle Behavior Detection to CA Account Address - BD_ACCT_ADDR
  - Oracle Behavior Detection to CA Account - BD_ACCT
  - Oracle Behavior Detection to CA Customers - BD_CUST

- Oracle Behavior Detection to CA Customers Phone - BD_CUST_PHON

Sample Query: Process BD_ACCT_ADDR

```
UPDATE pr2_process_task_parameter
      SET V_TASK_PARAMETER_VALUE = replace(V_TASK_PARAMETER_VALUE,
                                    'DATAMOVEMENTOPERATION=DI',
                                    'DATAMOVEMENTOPERATION=MI')
    WHERE V_PROCESS_ID IN (SELECT V_PROCESS_ID
                     FROM pr2_process_b t
                    WHERE t.v_process_name = 'BD_ACCT_ADDR'
```

- The parallel hint degree can be modified as per system configuration. Oracle provides parallel (2) as part of the product. The degree can be modified using the following sample query.

Sample Query: Modify parallel (2) to parallel (8)

```
update fcc_dm_definition
set
       V_CREATE_SELECT_HINT = replace(V_CREATE_SELECT_HINT,'(2)','(8)'),
       V_INSERT_HINT = replace(V_INSERT_HINT,'(2)','(8)'),
       V_INSERT_SELECT_HINT = replace(V_INSERT_SELECT_HINT,'(2)','(8)'),
       V_MERGE_HINT = replace(V_MERGE_HINT,'(2)','(8)')
WHERE  dm_id in (SELECT dm_id FROM fcc_dm_definition where
```

- Increase the index cache to 100000, based on the task or table identified.

  For example:

```
"alter sequence CM_ACCT_ADDR_SEQ cache 100000;
"alter sequence cm_bd_party_party_rlshp_skey cache 100000;
"alter sequence CM_CUST_PHONS_SEQ cache 100000;
"alter sequence CM_CUST_ADDR_SEQ cache 100000;
"alter sequence CM_CUST_EMAIL_ADDR_SEQ cache 100000;
```

> **NOTE** In the case of a server restart, the sequence will be skipped based on the cache mentioned.

7 Loading Data

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

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

7.1 About Loading Data

Data is loaded from the landing area to the 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

- You must manage all FCC_* tables retention as per your business needs. For more details about the same, contact Oracle Support.
- ECM does not support Multi-Match alerts.

7.1.1 Types of Connectors

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

- OBD
- OKYC
- OCS
- OSTDO
- Third-party
- TBAML

7.2 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
- Loading OBD Data
- Loading OCS Data
- Loading TBAML Data
- Loading Studio Data

7.2.1 Accessing Connector Processes

This section explains how to access different application connectors list in the Run window. To access connectors, follow these steps:

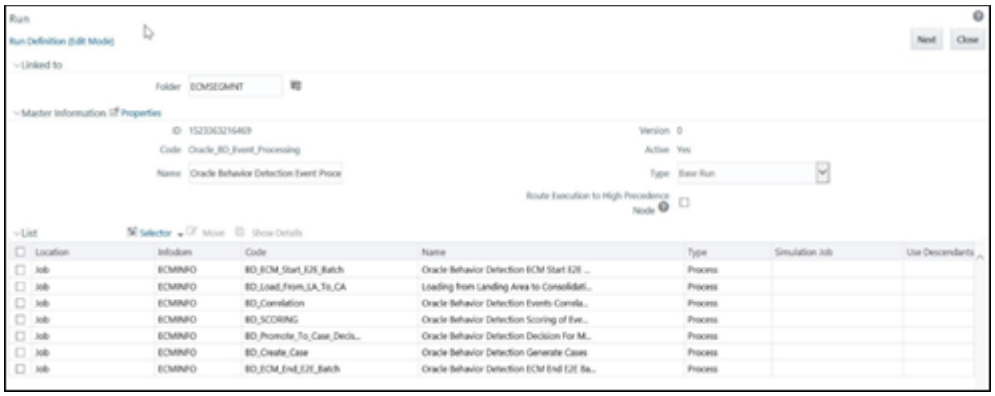
1. Navigate to Enterprise Case Management Application.
2. Go to the Common task section. Select the **Run Rule Framework**.
3. Click **Run**. The Run window is displayed.

7.2.2 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 as shown in Figure 26 .

Figure 26: 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 List of Processes and Tasks.

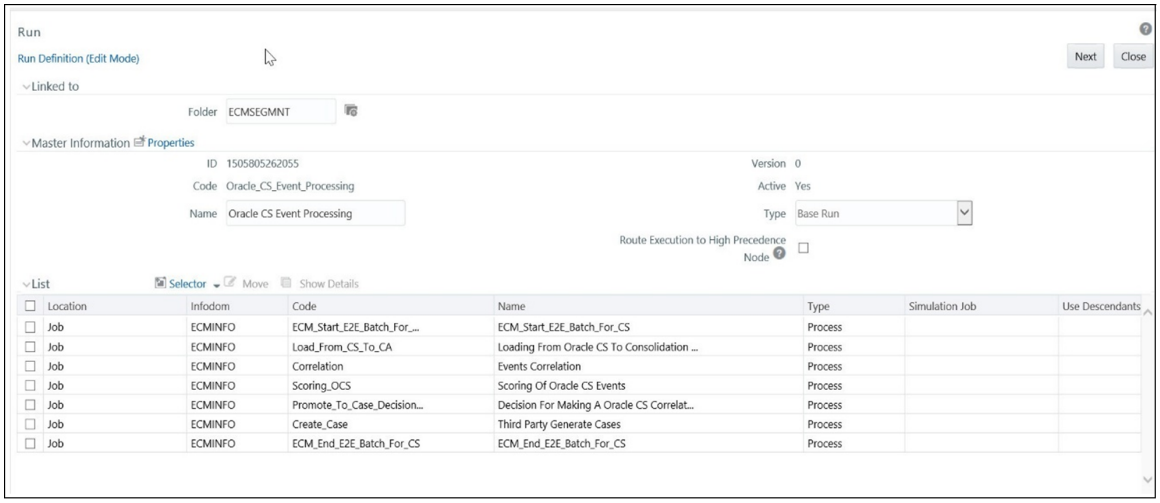
For more information on Configuring Data Movement from LA to CA, see the Configuring Data Movement from LA to CA .

7.2.3 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 as shown in Figure 27 .

Figure 27: 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 List of Processes and Tasks.

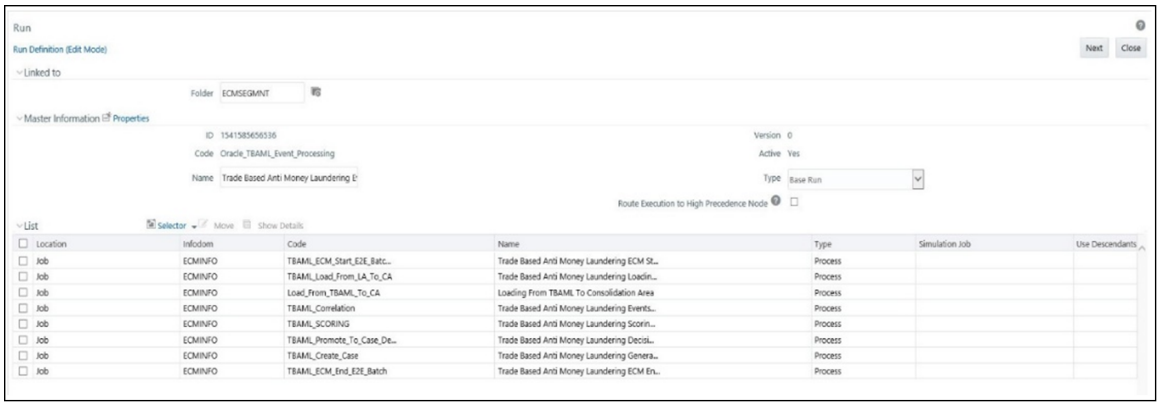
For more information on Configuring Data Movement from LA to CA, see the Configuring Data Movement from LA to CA .

7.2.4 Loading TBAML Data

The TBAML connectors are used to load data from the TBAML application to the ECM. To load data from the TBAML to the ECM, follow these steps:

1. Navigate to the Run window.
2. Go to the List section. Select **Oracle_TBAML_Event_Processing**. The list of processes for TBAML is displayed as shown in Figure 27 .

Figure 28: TBAML Connector



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

For more information on processes and tasks, see List of Processes and Tasks.

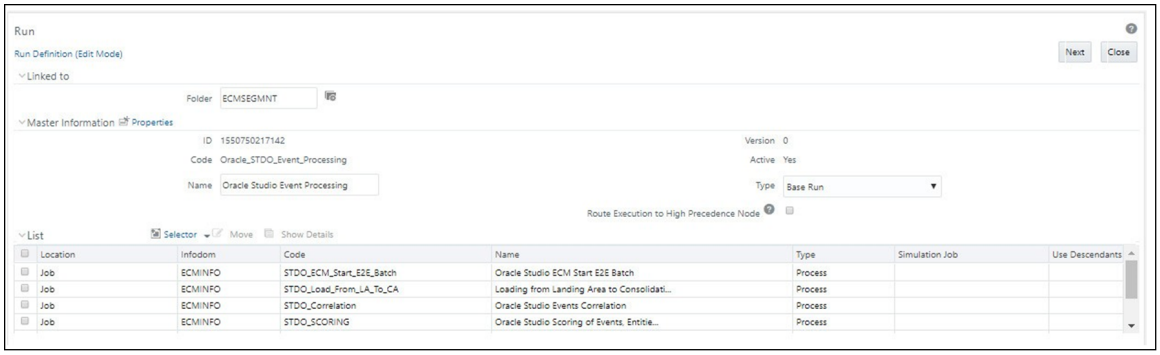
For more information on Configuring Data Movement from LA to CA, see the Configuring Data Movement from LA to CA.

7.2.5 Loading Studio Data

The STDO connectors are used to load data from the Studio application to the ECM. To load data from the Studio to the ECM, follow these steps:

1. Navigate to the Run window.
2. Go to the List section. Select **Oracle_STDO_Event_Processing**. The list of processes for Studio is displayed as shown in Figure 29 .

Figure 29: Studio Connector



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

7.3 Data Movement (DM) Utility

It is used to transfer data from one Oracle data source to another Oracle data source. This utility can be used for moving the data from the landing area to the consolidation area. And, then consolidation area to UI (KDD Case tables, example KDD_CASE_CUSTOMER, KDD_CASE_ACCOUNT, and so on.

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

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

The following data transfer modes are available:

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

7.3.1 DM Metadata Tables

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

  The structure of the DM definition table is described in Table 26 :

  Table 26: FCC_DM_DEFINITION (Metadata Table)

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

- DM_GROUP_ID: grouping code of DM definition. DM definitions can be grouped to pull the data together.
- DM_ID: unique identification ID of DM definition.
- DM_CODE: unique name of DM definition.
- DM_DESCRIPTION: description of DM definition.
- V_SOURCE_DATASET: name of the Source table. It can contain the join conditions with multiple source tables and conditions associated with it. All source tables must be put under the curly bracket '{'. For example: {EMP_PHON}

- V_TARGET: name of Target table.
- V_SRC_FILTER: source filter that contains the filter condition for the 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 the 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

  Table 27 describes the FCC_DM_DEFINITION (Metadata Table 1).

Table 27: FCC_DM_DEFINITION (Metadata Table 1)

DM_-GRO UP_ID	DM_ ID	DM_CODE	DM_ DESCRIP-TION	V_SOURC E_DATA-SET	V_TAR GET	V_SRC_FILTER	V_TA RG_-FILTER	V_TARGET_-DATASET
1	1	BD_EMP_P HON	T2T_FCCM _P ROD_E MP_PHON	{EMP_PH ON}		EMP_-PHON.DATA_DU MP_DT = $MISDATE AND EMP_-PHON.PRCSNG_ BATCH_ NM IN (SELECT FCC_BATCH_DAT AORI-GIN.V_DATA_ORI GIN FROM FCC_BATCH_-DATAORIGIN WHERE FCC_BATCH_DAT AORI-GIN.N_RUN_SKE Y = $RUNSKEY)		INNER JOIN FCC_EM-PLOYEE_-LOOKUP ON FCC_EM-PLOYEE_-LOOKUP.E MP_IN-TRL_ID = [EMP_-PHON].EMP _INTRL_ID

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

  The structure of the DM field mapping table is as shown in Table 28 :

Table 28: 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
V_TARG_DATA_TYPE		VARCHAR2(50)	Yes
V_EXECUTION_SPACE		VARCHAR2(5)	Yes

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

> **NOTE** It can contain expression and target table if source value is populating from any SQL expression or a particular column from target table.

Example: EXPRESSION, CM_EMP_SEQ.NEXTVAL

- V_FIELD_NAME: Name of Source field.

> **NOTE** It can contain target filed name if the value is coming from the target table.

- V_SRC_DATA_TYPE: Data type of Source field.
- V_FIELD_FORMAT: Data type format of the 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 the application interface, for example, $MISDATE (MIS date passed from the 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.

For example: Table 29 describes the Case statement & Sequences sample table.

Table 29: Case statement & Sequences sample table

DM_ID	V_ENTITY_NAME	V_FIELD_NAME	V_SRC_DATA_TYPE	V_FIELD_FORMAT	F_IS_NULL_ALLOWED	V_SQL_EXPRESSION	V_TARGET_ENTITY_NAME	V_TARGET_FIELD_NAME	V_SQL_FUNCTION	V_NULL_IF	V_DEFAULT_IF	V_TARG_DATA_TYPE	V_EXECUTION_SPACE
1	EXPRESSION	DATA_DUMP_DT	DATE		Y	$MIS-DATE	FCC_EMP_PHON	MIS_DATE				DATE	Trg
1	EMP_PHON	EMP_INTRL_ID	VARCHAR2(200)		Y		FCC_EMP_PHON	EMP_INTRL_ID				VARCHAR2(200)	Src
1	EXPRESSION	EMP_PHON_SEQ_ID	NUMBER(22,0)		Y	CM_EMP_PHON_SEQ.NEXTVAL	FCC_EMP_PHON	EMP_PHON_SEQ_ID				NUMBER(22,0)	Trg
1	EMP_PHON	PHON_EXT_NB	VARCHAR2(20)		Y		FCC_EMP_PHON	PHON_EXT_NB				VARCHAR2(20)	Src
1	EXPRESSION	PHONE_TYPE	VARCHAR2(20)		Y	'Business'	FCC_EMP_PHON	PHONE_TYPE				VARCHAR2(20)	Src

7.3.2 DM Audit and Error Details Tables

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

7.4 Configuring Data Movement from LA to CA

This section covers the following topics:

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

7.4.1 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, OTBAML, and Third-party. In the OOB process, you can run the processes in parallel as well as in sequence. However, you can configure these processes based on your requirements.

For example, you can configure processes based on entity and related data such as account, customer, employee, institution, and so on. The following are OOB processes as part of the Business data movement. These OOB sample processes can be used only for reference purposes.

7.4.2 Sample Processes

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

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

You can create processes based on your requirements. 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.

Table 30 lists of sample processes (Oracle Behavior Detection Business data from LA to CA) which has sub-processes attached to it.

Table 30: Sample Processes

Process Name	Description
Process1	This process is designed using the following sub-processes (OBD to CA Account): • Oracle Behavior Detection to CA Account, • Oracle Behavior Detection to CA Account Address, • Oracle Behavior Detection to CA Account Balance Position Summary, • Oracle Behavior Detection to CA Email Address, and so on
Process2	This process is designed using the following sub-processes (OBD to CA Customer): • Oracle Behavior Detection to CA Customers, • Oracle Behavior Detection to CA Customers Account, • Oracle Behavior Detection to CA Customers Address, • Oracle Behavior Detection to CA Customers Email Address, • Oracle Behavior Detection to CA Customers IMP License, and so on

Table 30: Sample Processes

Process Name	Description
Process3	This process is designed using the following sub-processes (OBD to CA Employee): • Oracle Behavior Detection to CA Employee, • Oracle Behavior Detection to CA Employee Address, • Oracle Behavior Detection to CA Employee Email Address, • Oracle Behavior Detection to CA Employee Phone, • Oracle Behavior Detection to CA Employee to Account, and so on
Process4	This process is designed using the following sub-processes: • Oracle Behavior Detection to CA Account, • Oracle Behavior Detection to CA Employee, • Oracle Behavior Detection to CA Customers, and so on
Process5	This process is designed using the following sub-processes: • Oracle Behavior Detection to CA Account Address • Oracle Behavior Detection to CA Account Balance Position Summary • Oracle Behavior Detection to CA Account Email Address, and so on
Process6	This process is designed using the following sub-processes: • Oracle Behavior Detection to CA Customers Account • Oracle Behavior Detection to CA Customers Address • Oracle Behavior Detection to CA Customers Email Address • Oracle Behavior Detection to CA Employee
Process7	This process is designed using the following sub-processes: • Oracle Behavior Detection to CA Employee Address, • Oracle Behavior Detection to CA Employee Email Address, • Oracle Behavior Detection to CA Employee Phone, • Oracle Behavior Detection to CA Employee to Account, and so on
Process8 & 9	These processes are designed using all sub-processes.

- The above process names are used for reference purposes.
- Process 1, 2, and 3 are designed based on a similar entity bucketed into one process.
- Process 4, 5, 6, and 7 are designed based on the distribution of the volume of data. For example, if Process4 has a huge volume of data compare to Process5, 6, and 7. You can design the process (business data movement) in such a way that the Process4 runs in parallel with Pro- cess5, internally, Process5, 6, and 7 can run in sequence.

Using the above sample processes, you can design entire Landing Area to Consolidation Area data movement based on your requirement.

NOTE If the Data Movement (DM) processes in different batch runs are same to fetch the data from a particular source, then additional configuration is required. This configuration avoids the duplicate data in the consolidation area of ECM and negative performance.

For example: If the DM processes in AML and KYC batches are the same, then exclude the DM tasks from the latter batch as it will run as part of AML Batch (considering AML batch is configured to run first).

Above step needs to be performed to avoid the following issues:

- If Batch is configured to run in DI (Delete Insert) or MI (Merge Insert) mode, then it will have performance impact due to duplicate task run.
- If Batch is configured to run in IS (Insert Select) mode, then unique constraints will be thrown by the latter batch due to duplicate data.

7.4.3 ECM Business Table Data Synchronization with Source Business Table

The ECM Business and Source Business tables must always be in sync. If the source table data is deleted, corresponding case table data must also be deleted. Any existing data modification will automatically be picked up by the existing ECM batch. But deletion in Source Business tables are not handled.

To avoid data de-synchronization between these tables, the Data Movement (DM) utility has been updated with the following parameters:

- **DDI**: Data origin DELETE insert - Data will be deleted with filter condition $DATAORIGIN
- **TI**: Truncate INSERT - Truncate data from the target table and perform insert without filter condition $MISDATE

You can modify the process parameter as DDI or TI to enable full load. Every time it deletes data from the target table and insert all data from the source table.

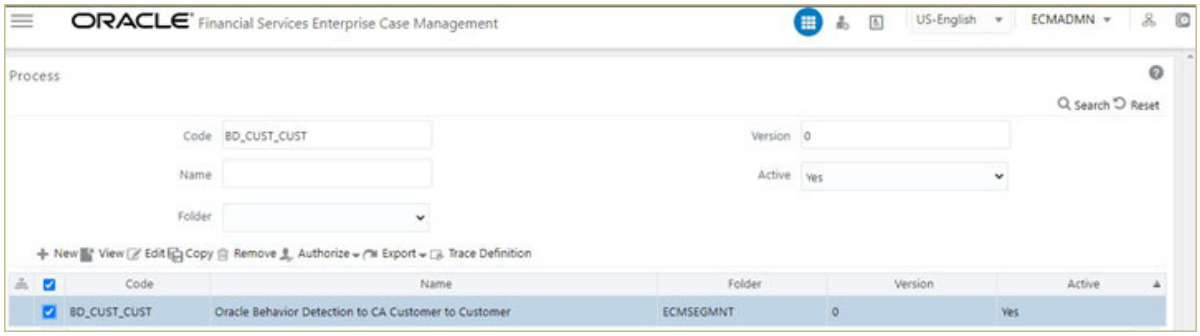
To configure DDI and TI, you must change the existing Process (e.g., BD_CUST_CUST) parameter to DDI or TI.

To modify the existing process for a full load, follow these steps:

1. Navigate to Enterprise Case Management Application.
2. Go to the Common Task section and select the **Run Rule Framework**.
3. Click **Process**. The Process Summary window is displayed with the available Processes.
4. Search for **BD_CUST_CUST** and click **Edit**.

   Figure 30 depcits the Searching a Process screen.

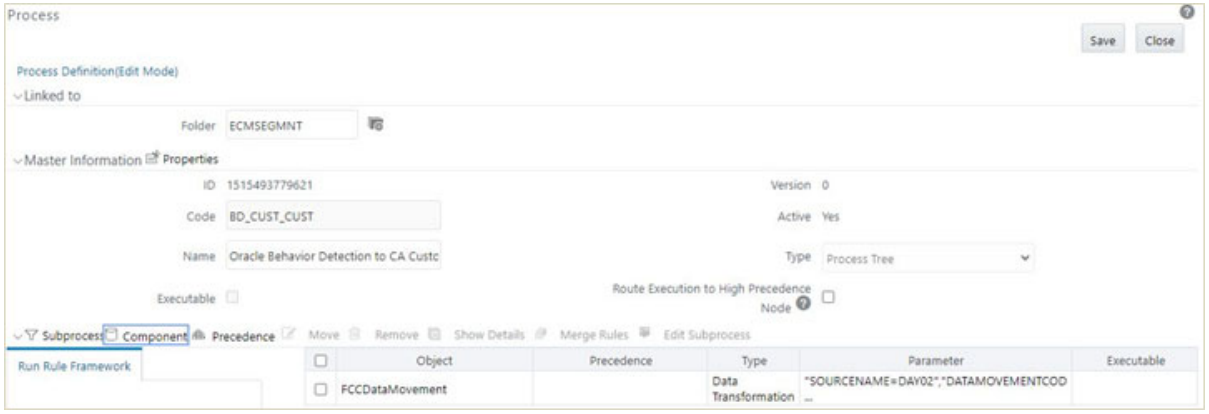
Figure 30: Searching a Process



5. Click **Component**.

   Figure 31 depcits the Process Component screen.

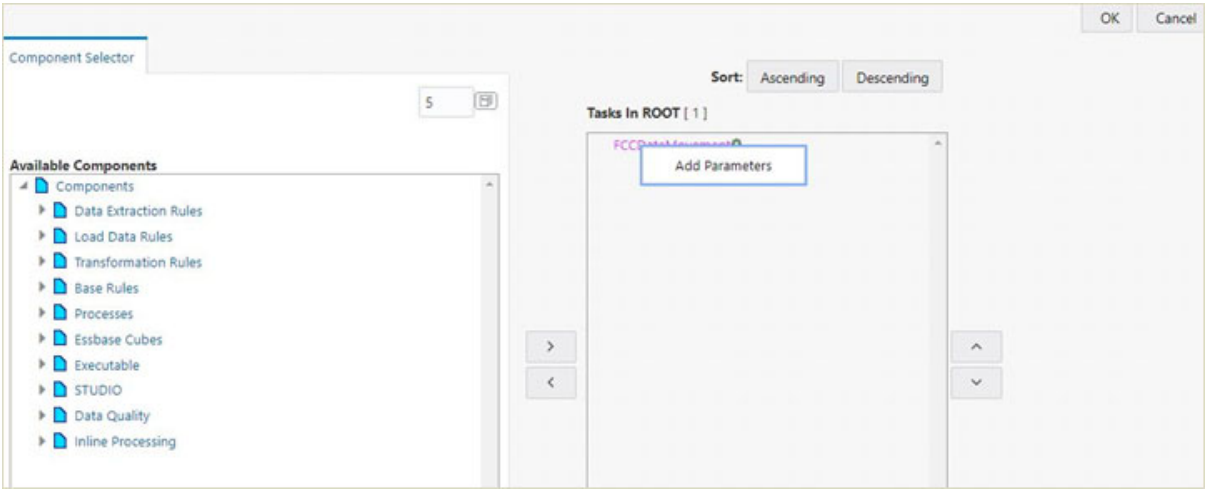
Figure 31: Process Component



6. Right-click on **FCCDataMovement** and then click **Add Parameters**.

   Figure 32 depcits the FCCDataMovement and Add Parameters screen.

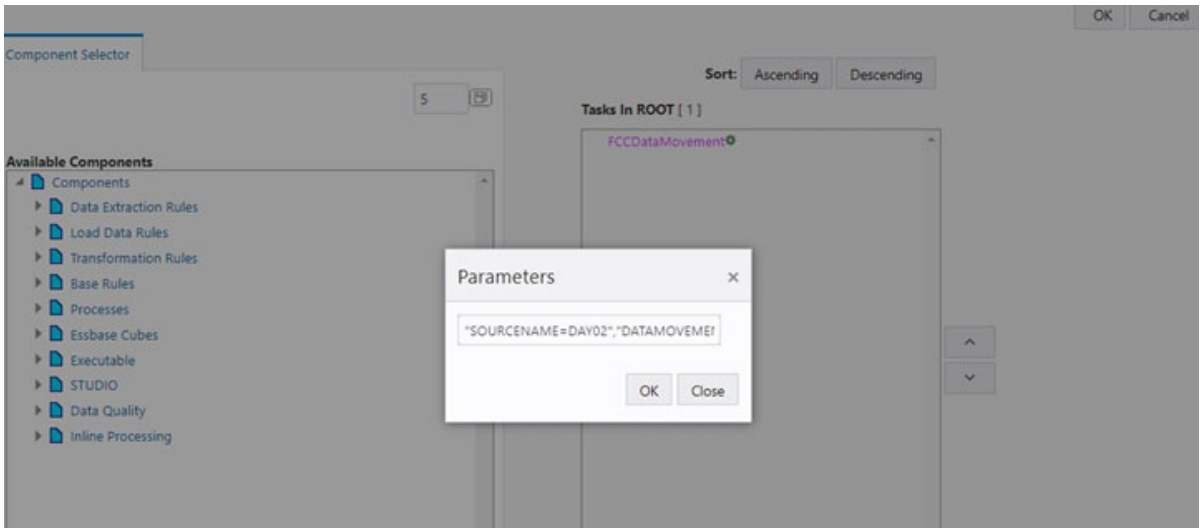
Figure 32: FCCDataMovement and Add Parameters



7. Replace the existing parameter value with: "SOURCENAME=DAY02","DATAMOVEMENTCODE=BD_CUST_CUST","LOADTYPE=DBLINK","DATAMOVEMENTOPERATION=DDI".
8. Click **OK**.

   Figure 33 depcits the Replace Existing Parameters screen.

Figure 33: Replace Existing Parameters



9. Click **Save** and then click **No** when prompted to save a new version.

NOTE

- The FCC_CUST_CUST table is fully refreshed from the CUST_CUST table during batch execution
- The DDI and TI parameters are applicable only for business data movement and lookup
- This data movement DDI and TI is done on the following scenarios:
  - Same Database Same Schema
  - Same Database Different Schema
  - Different Database Different Schema

7.4.4 Using Precedence

Follow the sequence of precedence while moving the data.

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

NOTE Make sure precedence is set for data movement.

7.4.5 Designing Processes

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

Figure 34 depicts sub-processes in Oracle Behavior Detection processes.

Figure 34: Oracle Behavior Detection processes

Oracle Behavior Detection Sub-Processes

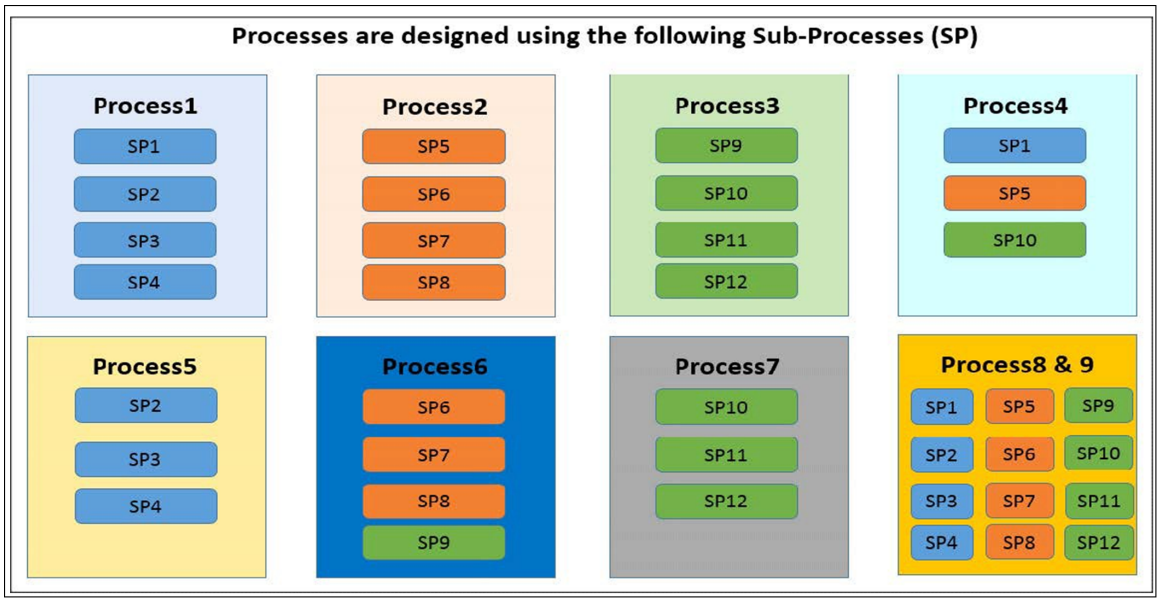
Sub Process (SP)	Description
SP1	Oracle Behavior Detection to CA Account
SP2	Oracle Behavior Detection to CA Account Address
SP3	Oracle Behavior Detection to CA Account Balance Position Summery
SP4	Oracle Behavior Detection to CA Account Email Address

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

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

Figure 35 illustrates the Processes (1 to 9) designed using sub-processes (SP).

Figure 35: Oracle Behavior Detection Subprocesses



You can run Processes using the list of options shown in Figure 36 .

Figure 36: Options- processes

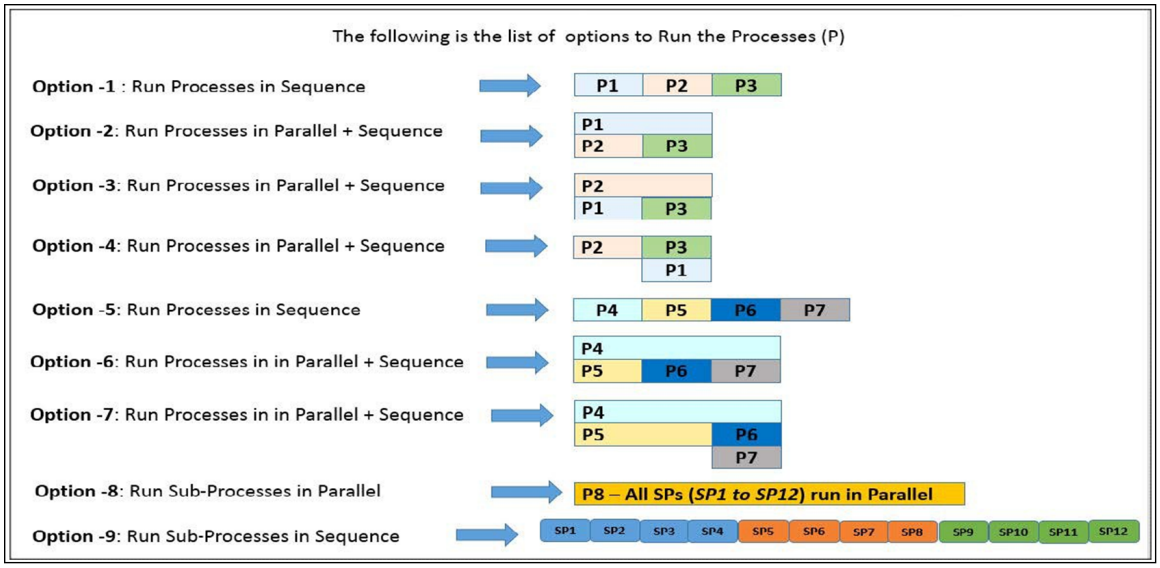


Table 31 provides a complete description of each option.

Table 31: Options

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

Table 31: Options

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

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

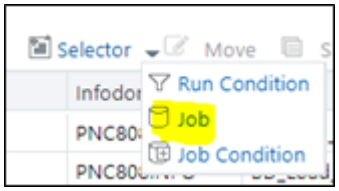
To design the above process, see the OFS AAI User Guide.

7.4.6 Adding Transformation Rule

To add a Transformation Rule, follow these steps:

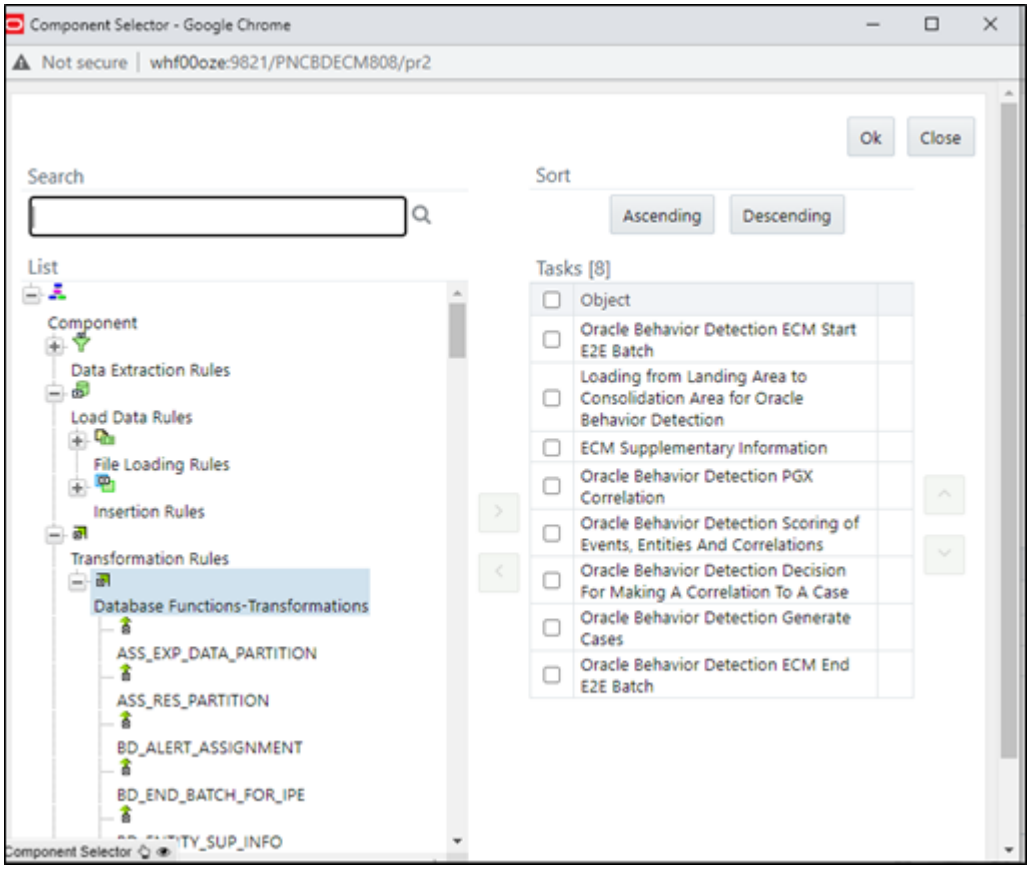
1. Navigate to Enterprise Case Management Application.
2. Go to the Common task section. Select the **Run Rule Framework**.
3. Click **Run**. The Run window is displayed.
4. Go to the List section. Select an application for example (Oracle_BD_Event_Processing) and click **Edit**. The list of processes for the selected application is displayed.
5. Select **Job** from **Selector** as shown in Figure 37 .

Figure 37: Job from Selector



6. Click **Components** and select required Transformation Rule, move to Tasks list using. Click **Ok**. Transformation Rule will be added to process as shown in Figure 38 .

Figure 38: Component Selector



8 Configuring Correlation

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

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

8.1 About Correlation

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

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

8.2 Using Business Entity Paths

Following two tables are used for configuring business entity paths:

- Correlation Business Path
- Correlation Business Entity Configuration

8.2.1 Correlation Business Path

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

Table 32 descibes the structure of the table:

Table 32: 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		VARCHAR2(50)	No
V_BUSINESS_ENTITY_PATH_NAME			
V_QUERY_DEFINITION_NAME		VARCHAR2(50)	Yes
N_BUSINESS_ENTITY_ID		NUMBER(10)	Yes
_FOCUS_ID		NUMBER(10)	Yes
V_ENTITY_TYPE		VARCHAR2(50)	Yes
V_QUERY_DEFINITION_NAME		VARCHAR2(50)	Yes

Table 32: FCC_CORR_BUS_ENTITY_PATH (Metadata Table)

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

To correlate events to business entities, follow these steps:

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

8.2.2 Correlation Business Entity Configuration

Table 33 depicts the structure of the Business Entity path configuration table:

Table 33: FCC_CORRELATION_BUS_ENTITY_CFG (Metadata Table)

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

To configure the Business Entity path, follow these steps:

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

   Populate the N_SCENARIO_MASTER_SKEY or the V_SCENARIO_CLASS_CD column to establish respectively.

> **NOTE** If neither of these columns is populated, this path configuration is considered for the case of any scenario or scenario group. The "importance" or "strength" of a correlation determined by this path can vary depending on the scenario or scenario group of the case.

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

   By default, For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY and V_SCENARI-

O_CLASS_CD is NULL and N_PATH_PRECEDENCE = 10 then the PATH_SKEY = 1004 will be considered for execution for all the scenario class except the below mentioned cases

2. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY is NULL and V_SCENARIO_CLASS_CD = 'FR' and N_PATH_PRECEDENCE = 15 then the PATH_SKEY = 1004 will be executed for 'FR' related scenarios
3. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD is NULL and N_PATH_PRECEDENCE is NULL then the PATH_SKEY = 1004 will not be considered for execution
4. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD = 'ML' and N_PATH_PRECEDENCE is NULL then the PATH_SKEY = 1004 will not be considered for execution.
5. For N_BUS_ENTITY_PATH_SKEY = 1004, if N_SCENARIO_MASTER_SKEY = '114697025' and V_SCENARIO_CLASS_CD = 'IML' and N_PATH_PRECEDENCE = 13 then the PATH_SKEY = 1004 will be considered for execution only for the above mentioned '114697025' and 'IML'

8.3 Executing Correlation Rules

You can execute the correlation using two methods:

Using the Run Rule Framework

Performing Jobs Using Run Rule Framework

You can run a correlation using the Run Rule Framework. For more information, refer to the Configuring Correlation section.

8.3.1 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 the date from FCC_BATCH_RUN

8.4 Sample Correlation Rules

OFS ECM delivers the following four sample correlation rules:

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

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

9 Scoring

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

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

9.1 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

9.1.1 Initial Scoring

The following figure depicts the initial scoring process.

Figure 39: Initial Scoring Process

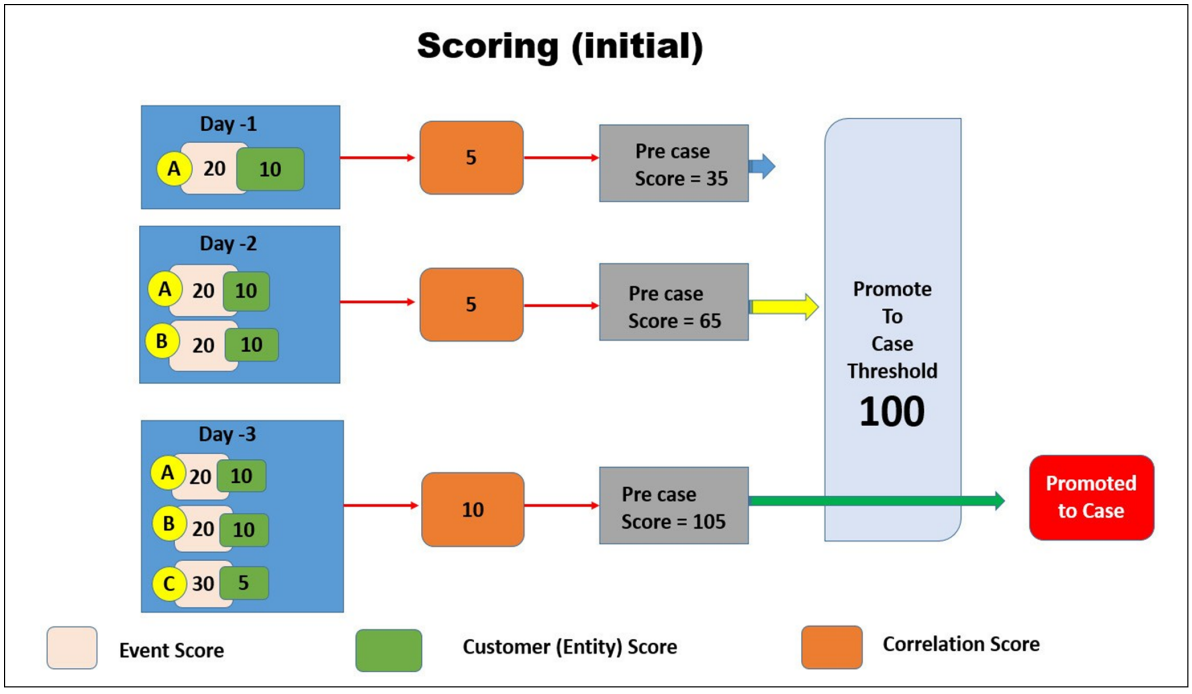


Table 34: Initial Scoring

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

9.1.1.1 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.

9.1.1.2 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.

9.1.1.3 Day - 3

- Another event (event C) is generated along with event (event B), event (A), associated entity (customer), and correlation is scored. A case to get promoted, the pre case should cross the threshold score (100).
- The pre case score is 65. It is the sum of event A + event B + event C + customer + correlation = pre case score. That is, 20 + 20 + 30 + 10 +10 = 105.
- A pre case is promoted to the case.

9.1.2 Adjustment Scoring

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

The following figure depicts the adjustment scoring process.

Figure 40: Adjustment Scoring

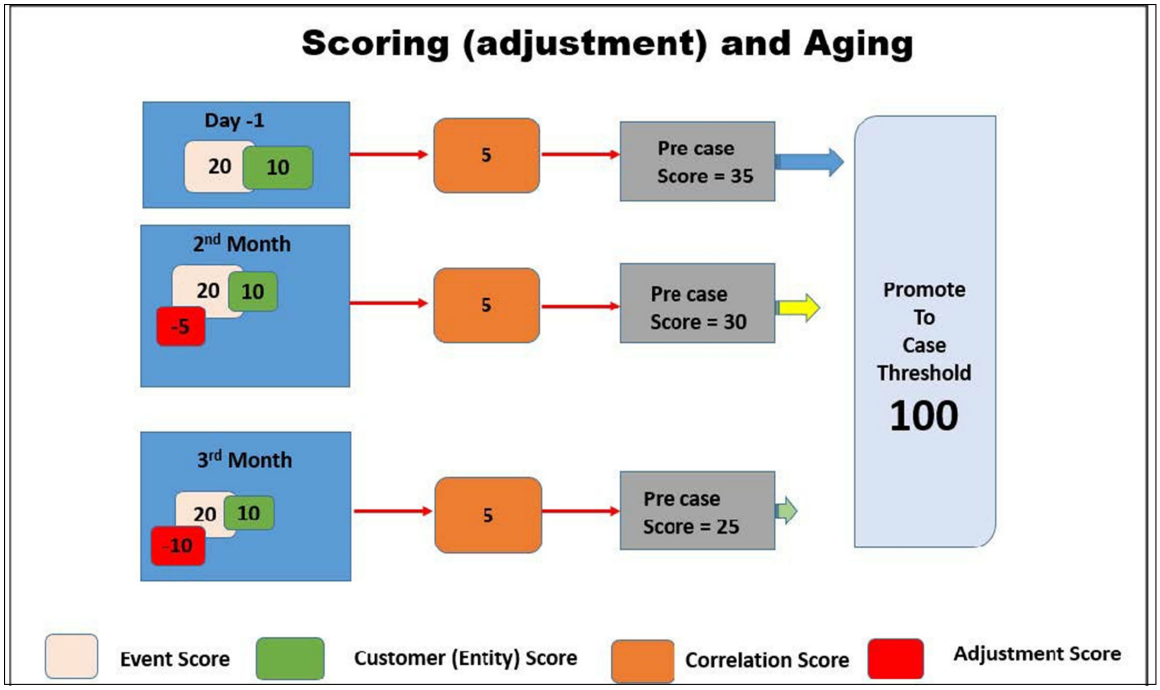


Table 35: Adjustment Scoring

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

9.1.2.1 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.

9.1.2.2 2nd Month

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

9.1.2.3 3rd Month

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

9.2 Types of Scoring

The following is the list scoring types:

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

9.2.1 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.

9.2.2 Entity Scoring

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

9.2.3 Correlation Scoring

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

9.2.4 Pre case Scoring

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

9.3 Configuring Scoring Rules

The following seeded scoring rules are used for scoring:

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

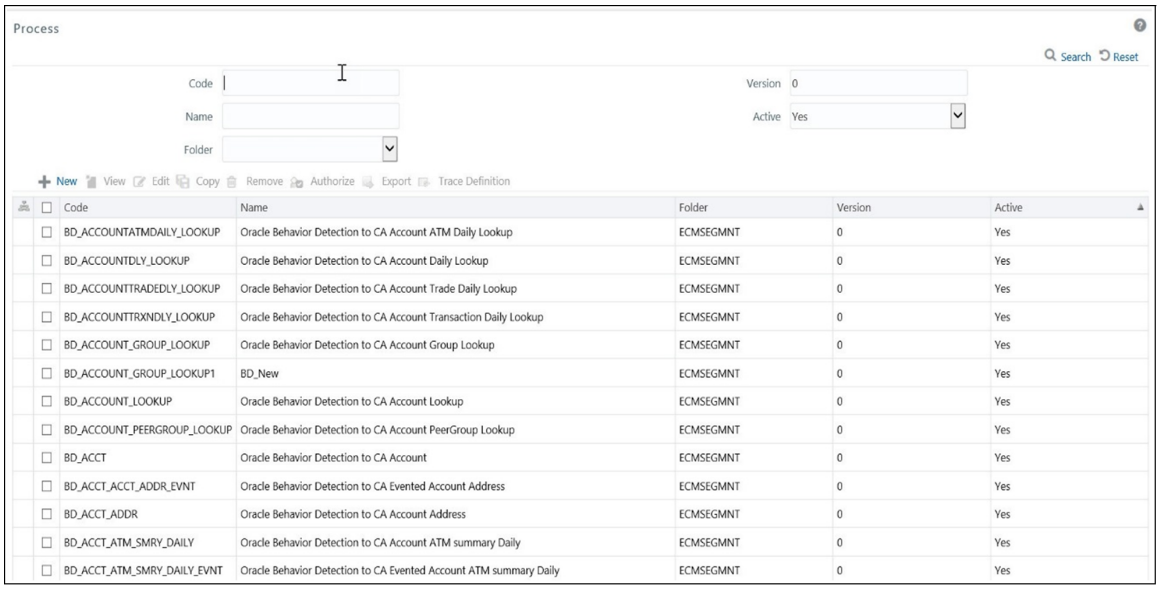
For more information configuring scores, see the Inline Processing Engine User Guide.

9.3.1 Configuring AML Event Initial Scoring

This section explains how to configure the initial scoring of the AML Event. To configure the AML Event initial scoring, follow these steps:

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

Figure 41: Process Summary Window



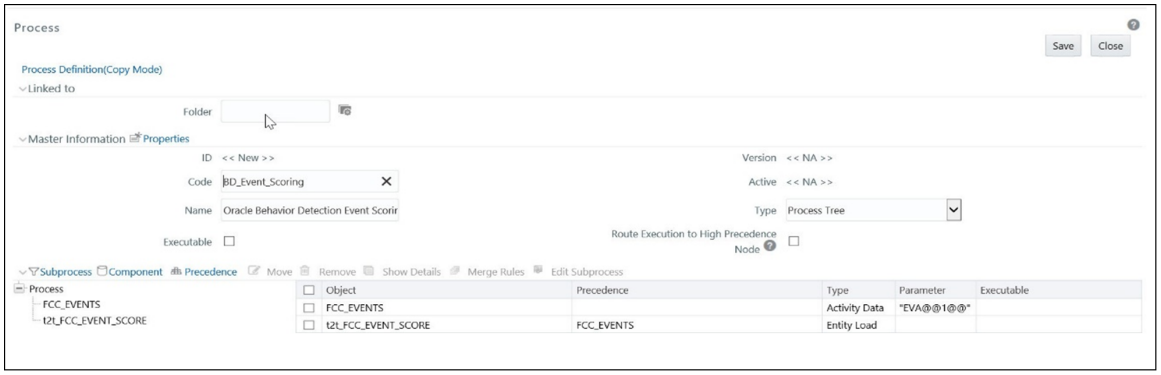
4. Search for BD Scoring code, for example, BD_Event_Scoring.

Figure 42: BD_Event_Scoring



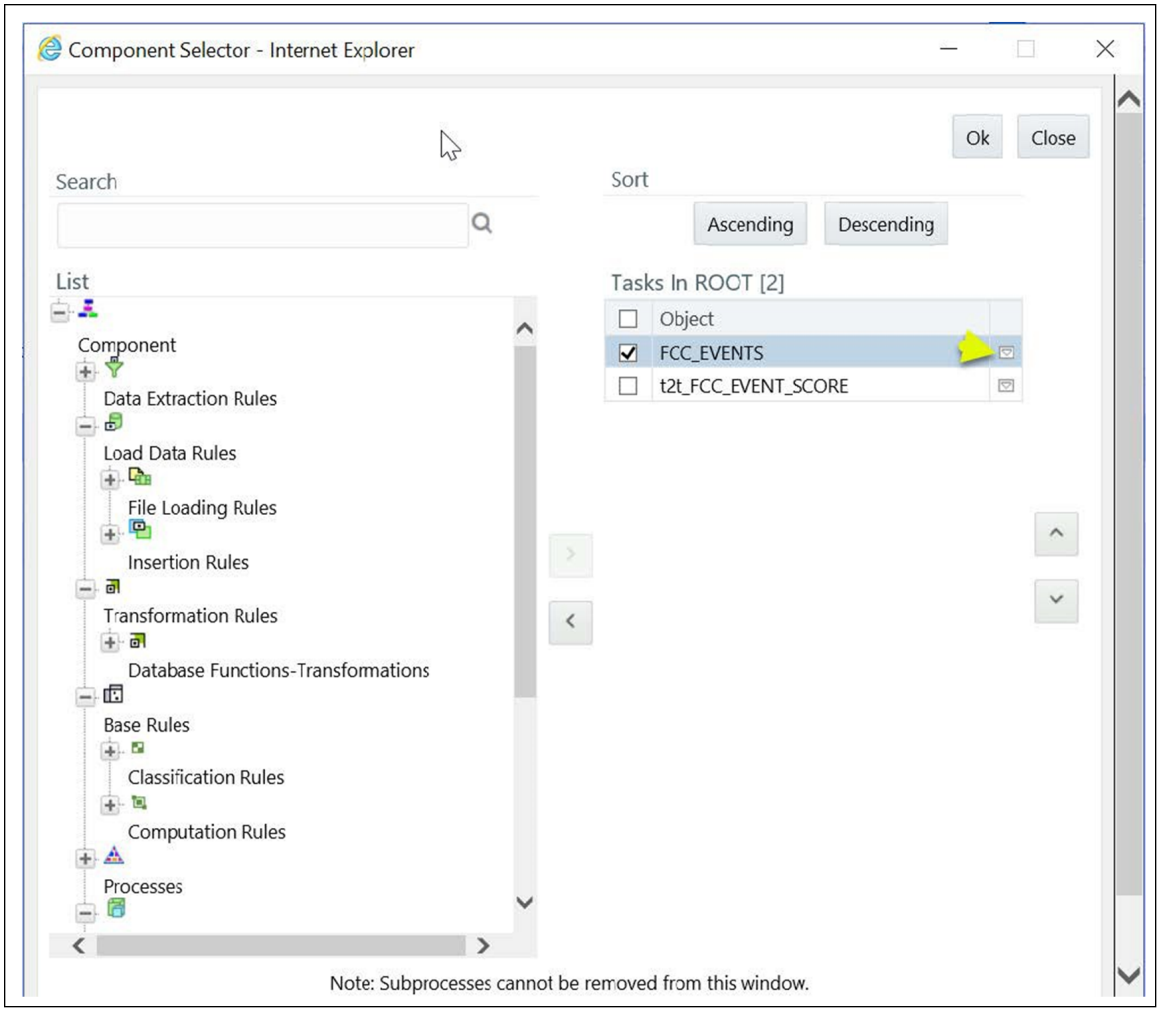
5. Click **Edit** after selecting the BD Event processing. The list of tasks is displayed.

Figure 43: List of Tasks



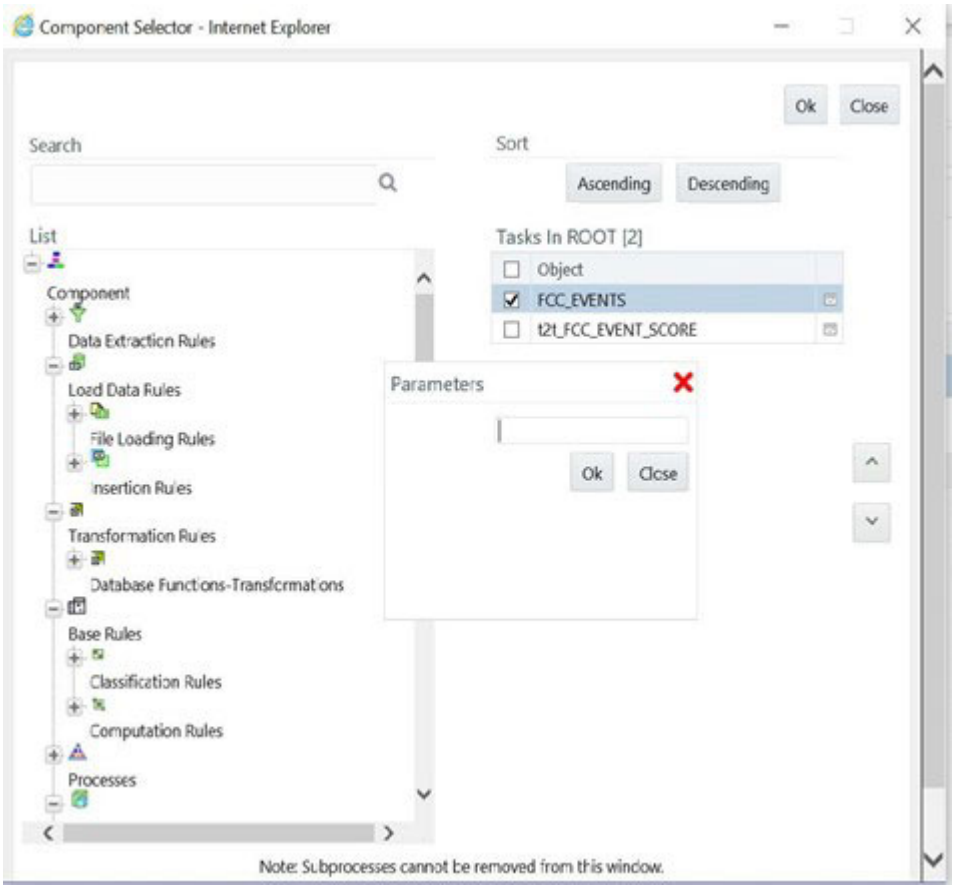
6. Click **Components**.

Figure 44: Components



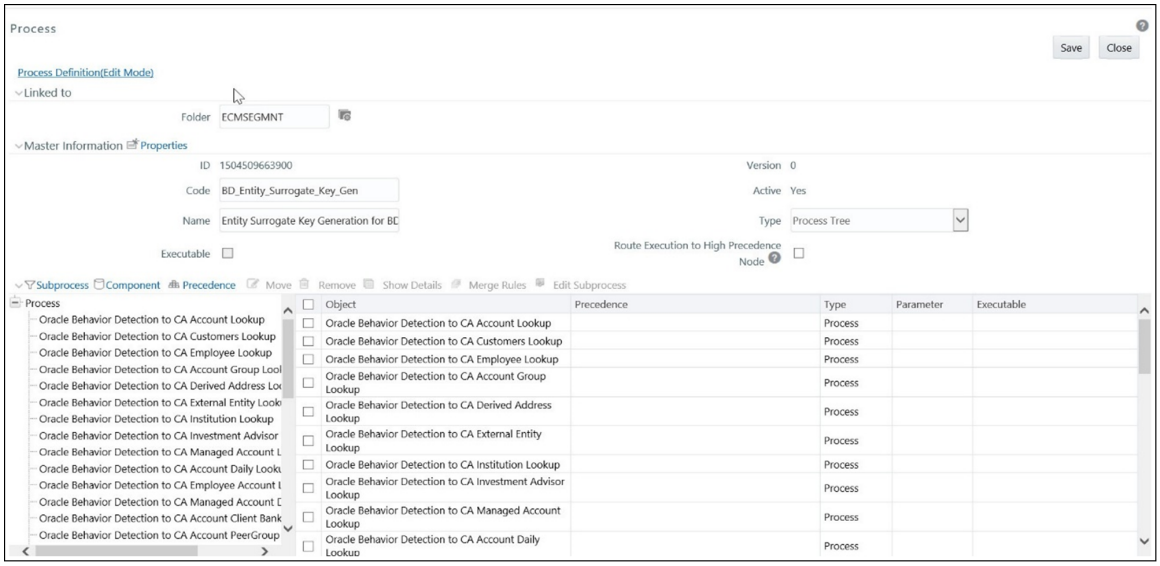
7. Delete all the parameters of the FCC_Events task and click **OK**.

Figure 45: Parameters



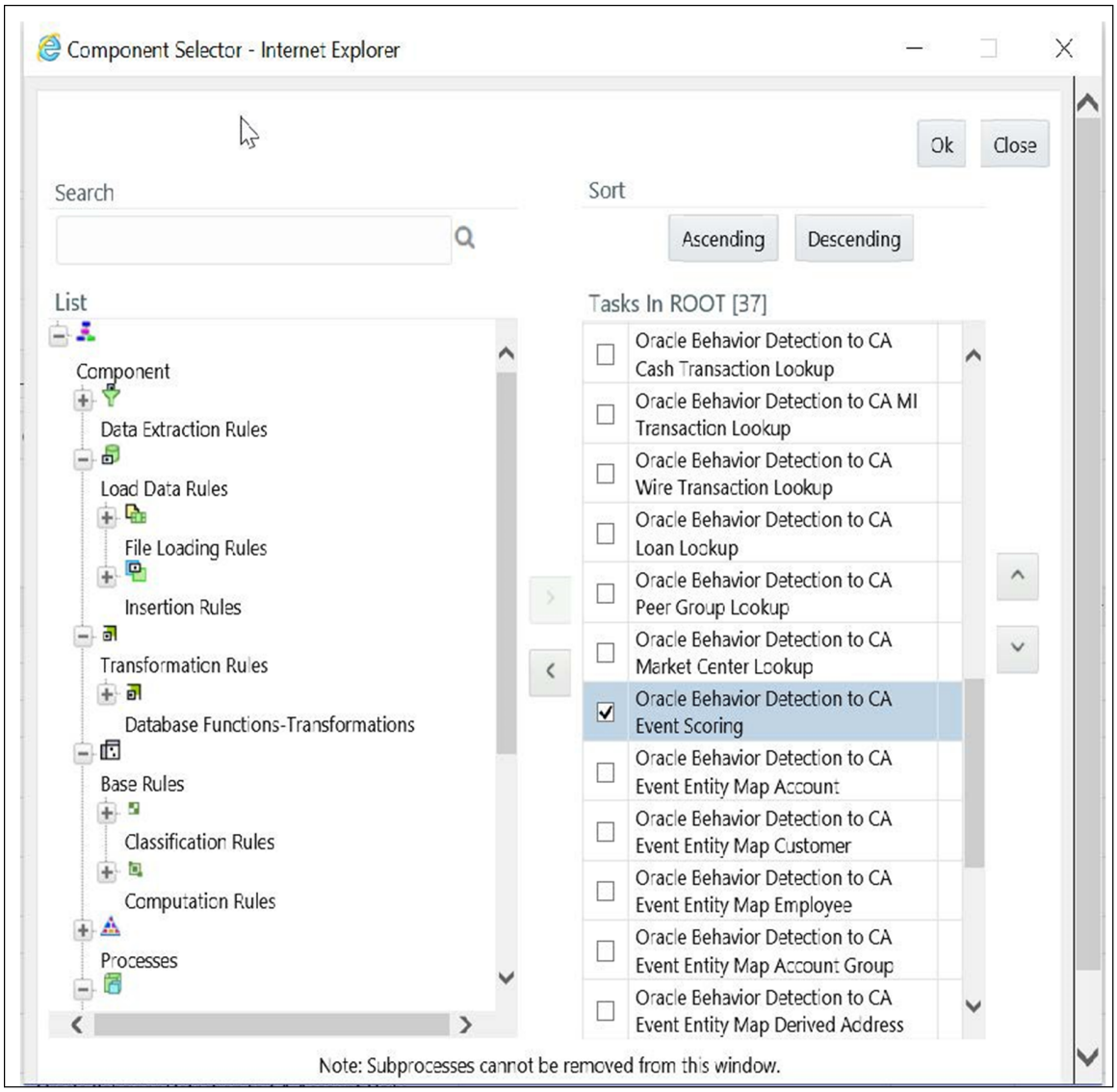
8. Navigate to the Process Summary window and search **BD_Entity_Surrogate_Key_Gen**.
9. The list of tasks is displayed. Click **Component**.

Figure 46: List of Tasks



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

Figure 47: Deselecting of Oracle Behavior Detection to CA Event Scoring Process



11. Save the Process.

9.4 Scoring Samples

This section covers the following scoring samples:

- Event
- Entity
- Correlation

9.4.1 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

9.4.1.1 Scenario

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

9.4.1.2 Total Transaction Amount and Risk Score

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

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

- Correlation is created for 2 events A and B by an ML and TF. Transaction amounts between 0 and 50000.99 get 10 points; Trxn amounts between 50001 and 100000 get 20 points; Trxn amounts

  > 100000 get 30 points. The Pre-case score should be calculated as below:

  - Event A - (Total amount of transactions - $ 80K) - 20
  - Event B - (Total transaction amount - $ 300K) - 30
  - Total pre-case score is 50 (A(20) + B(30) = 50)

9.4.1.3 Aging

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

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

The following is the scaling for aging events that are members of un-promoted correlations. Age scaling must be configurable and can be changed from the 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 for more than a year.

> **NOTE** You 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.

- The correlation creation date is 1st Jan 2016 and Event A with event creation date 1st Jan 2016 has an initial score of 10. So the pre-case score is 10.
- On 1st of February event B by (ML) Rapid Movement of Funds, All Activity CU with creation date 1st February 2016 is added to correlation. Event B score is 10 and the total pre-case score now is 20. A(10)+ B(10) = 20
- On 1st April, event A age is now 3 months. Event A score will be reduced by 3 points to 7 and the total pre-case score is now 17. A(7) + B(10) = 17
- On 1st May, event B age is now 3 months. Event B score will be reduced by 3 points to 7 and the total pre-case score is now 14. A(7) + B(7) = 14
- On 1st July, event A age is now 6 months. Event A score will be reduced by 3 points to 4 and now the total pre-case score will be 11. A(4) + B(7) = 11
- On 1st Aug, event B age is now 6 months. Event B score will be reduced by 3 points to 4 and now the 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 the 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 the total pre-case score will be 2. A(1) +B(1) = 2.
- On the 2nd Jan 2017 event, A age is now 12 months. The Score will be dropped to 0. And Event A will be closed and completely dropped from correlation. Event B is the only event in correlation and the total pre-case score will be now 1.
- On 2nd Feb 2017 event B age is now 12 months. The Score will be dropped to 0. And Event B will be closed and completely dropped from correlation.

9.4.2 Entity

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

- Watch List Screening
- Effective Risk

9.4.2.1 Watch List Screening

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

For example,

Entity A (10 for ML event) and B (10 for ML event) are part of the 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 the ML event. The correlation also now has an entity score of 60 for Entity C.

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

9.4.2.2 Effective Risk

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

The total customer score contributes to the pre-case. For example,

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

9.4.3 Correlation

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

- Number of events
- Combination of Scenarios
- Total Transaction Amount
- Repeated Scenario Events

9.4.3.1 Number of events

- If the number of events in the correlation is more than X, increase the correlation score.
- Scaling of correlation by the 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.
  - The number of events between 6 and less than or equal to 10 will be given 40.
  - Correlation with more than 10 events will be given 50.
- The additional score has to be added to the pre-case score.

  For example,

  A correlation has 4 events A, B, C, and D by ML. Event scores for 4 events are as follow.
  - A - 10
  - B - 20
  - C - 10
  - D - 30

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

9.4.3.2 Combination of Scenarios

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

  For example,

  Event A Rapid Movement of Funds All Activity CU focus and Event B Deposit Withdrawal Same or Similar Amount AC focus are correlated in the same correlation add 50 points
  - Event A - 10
  - Event B - 10
  - Correlation - 50
  - Pre-case score = 70

9.4.3.3 Total Transaction Amount

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

9.4.3.4 Repeated Scenario Events

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

For example,

- Assume customer CU1 had an event A on Rapid Movement of Funds (RMF) on 1st July 2016 and which had a score of 50 to start with.
- On 28th July 2016, the customer had another RMF event B with an Event score of 30. But since this a repeat event for the same scenario on the customer within a (Repeated scenario event lookback) 31 days, the correlation score could be increased by say 20 points. So overall the pre-case would tip over to 100 which is the score required to convert the pre-case to the case.
- The total correlation score contributes to the pre-case score.

10 Promoting to Case

The chapter focuses on the following topics:

- About Promoting to Case (PTC)
- Configuring PTC

10.1 About Promoting to Case (PTC)

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

The following event types are promoted to the case:

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

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

10.2 Configuring PTC

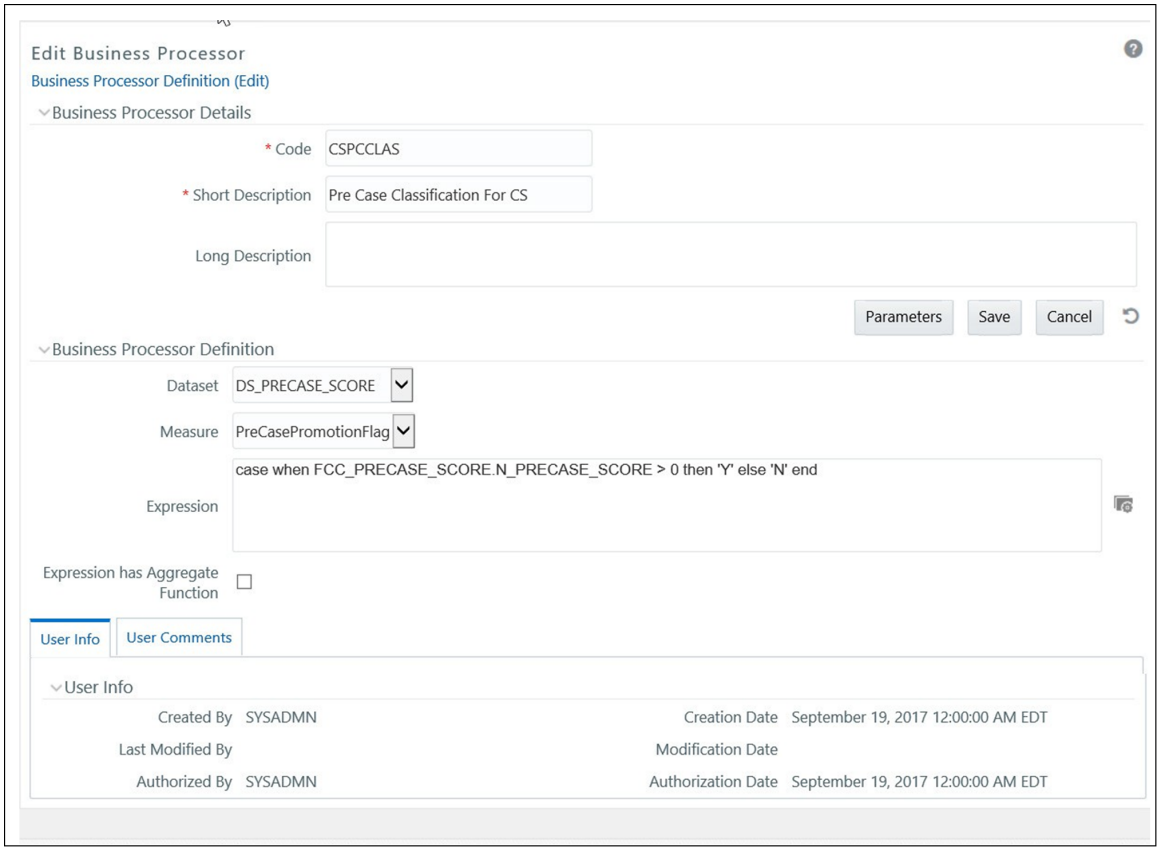
The scoring for PTC is performed in the Inline Processing Engine (IPE). For more information on scoring, see the Scoring section.

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

To configure PTC, follow these steps:

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

Figure 48: Adding Business Process



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

   The new threshold limit is defined.

11 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
- Implementing the ECM PMF Workflow

11.1 About PMF

The Enterprise Case Management Processing Modelling Framework (PMF) facilitates built-in tooling 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 that 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 Modeling Framework section of Oracle Financial Services Analytical Applications Infrastructure User Guide.

This section covers the following topics:

- ECM Workflow Development Life Cycle
- ECM Workflows

11.1.1 ECM Workflow Development Life Cycle

The ECM workflow follows various stages in the development lifecycle:

- **Modelling**: The CM Administrator models the workflow in line with the ECM requirement.
- **Implementing**: The CM Administrator implements the required service and 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.

11.1.2 ECM Workflows

The following are default workflows available in the ECM:

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

- TBAML
- KYCOB

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

11.2 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 the respective application tables.

11.2.1 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 the KDD_STATUS table of the Atomic Schema.

11.2.2 Configuring Action

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

> **NOTE** If you want to configure a new report type, you must add a new PMF action to the KDD_RRS_ACTN table. If the report type is based on the CRR framework, set the FRAMEWORK_ENABLE_FL parameter to Y. For example:
>
> insert into kdd_rrs_actn (ACTN_CD, ACTN_DESC_TX, ACTN_ERR_CD, SUPPL_RPT_FL, CRCTD_RPT_FL, ACTN_DT, RPT_TYPE_CD, FRAMEWORK_ENABLE_FL) values ('CA945S', null, 'CA264', 'N', 'N', null, 'SAR', null);

11.2.3 Configuring Attributes

You can define a new attribute that 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 the AAI_AOM_APP_COMP_ATTR_MAPPING table.

Table 36 is the format of this table:

Table 36: Configuring Attributes

Column Name	Description	Example
APP_COMP_ATTR_MAP_ID	App ID of the attribute	
N_ATTRIBUTE_ID	The ID of the attribute	

Table 36: Configuring Attributes

Column Name	Description	Example
V_ATTR_CODE	Name of the attribute	
N_ATTR_TYPE_ID	The ID of the attribute type. The values of the attributes are fetched based on the attribute type. 1001- Static 1002- Query 1003- JavaAPI For more information, see the Here, the V_ATTRIBUTE_VALUE should be the same as mentioned in the V_JURISDICTION_CD and V_BUSINESS_DOMAIN_CD columns of the FCC_EVENTS table. For example, if we have events generated with V_JURISDICTION_CD as "AMEA" and V_BUSINESS_DOMAIN_CD as "a" then the same should be updated in the respective column of FCC_SECURITY_ATTRIBUTES table..	
V_ATTRIBUTE_VALUE1 V_ATTRIBUTE_VALUE2	Values to be fetched for the attribute. Based on the attribute type, you need to pass the values.	t.action_cd,t.action_nm t.action_category_code t.action_category_code t.status_cd,t.status_nm s.v_role_code,s.v_role_code s.v_function_code = 'CMACCESS
N_APP_ID	Application code for which the current attribute is configured.	
N_COMP_ID	Component code for which the attribute is configured.	
V_UDP_CODE	Special property is 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.

Table 37 depicts the attribute types with their IDs:

Table 37: Attribute Types

Attribute Type ID	Attribute Type Name	Description
1001	Static	Store attribute values in the AAI_AO- M_STATIC table as V_STATIC_ID and V_STATIC_VAL.
1002	Query	Enter the SQL query in V_AT- TRIBUTE_VALUE1 in the AAI_AOM_APP_COMP_ATTR_MAPPING table, which has to be fired to fetch the attribute values.
1003	JavaAPI	Enter the method that is configured for V_ATTRIBUTE_VALUE1 for the required attribute. The configured method in the classpath is invoked to get the attribute values in this case.

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

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

11.3 Accessing Process Modeller

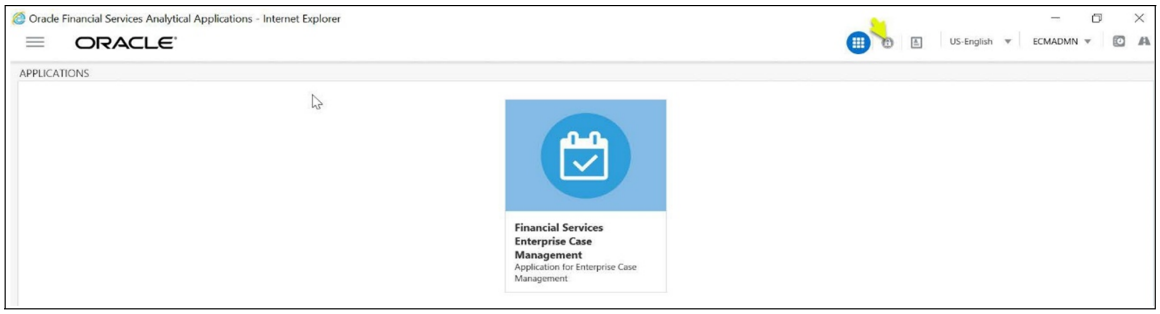
This section explains how to access the Process Modeller page.

To access the Process Modeller page, follow these steps:

1. Click the Administration icon.

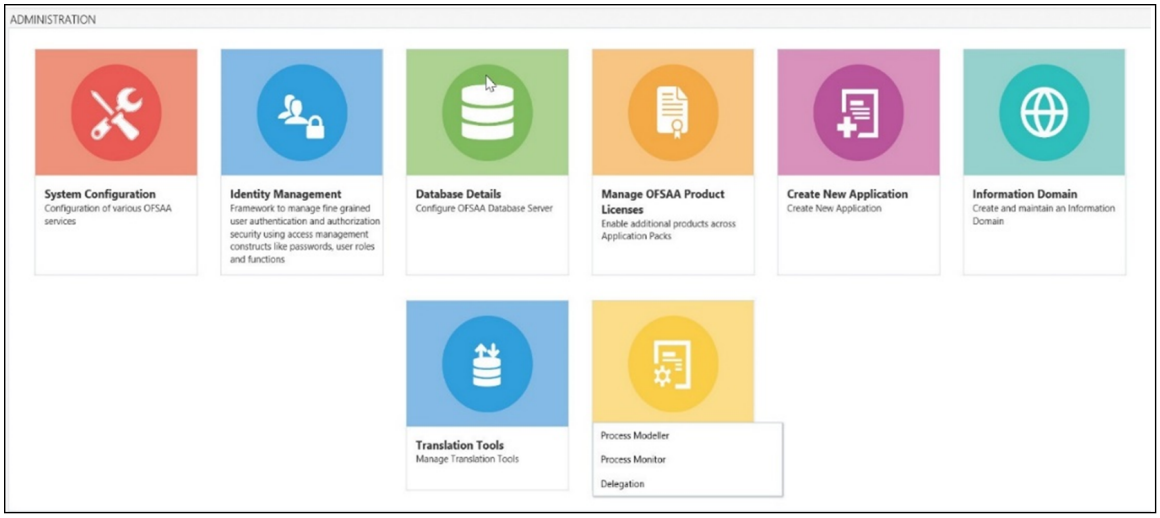
   Figure 49 depicts the Applications page.

Figure 49: Applications



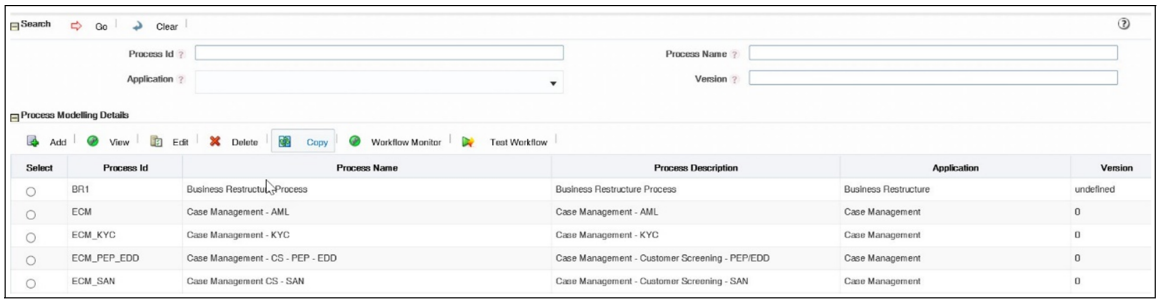
2. The Administration page is displayed as shown in Figure 50 . Click the Process Modeller option from the Process Modeling Framework.

Figure 50: Process Modeling Framework



The Process Modeller window is displayed as shown in Figure 51 .

Figure 51: 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.

11.4 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:

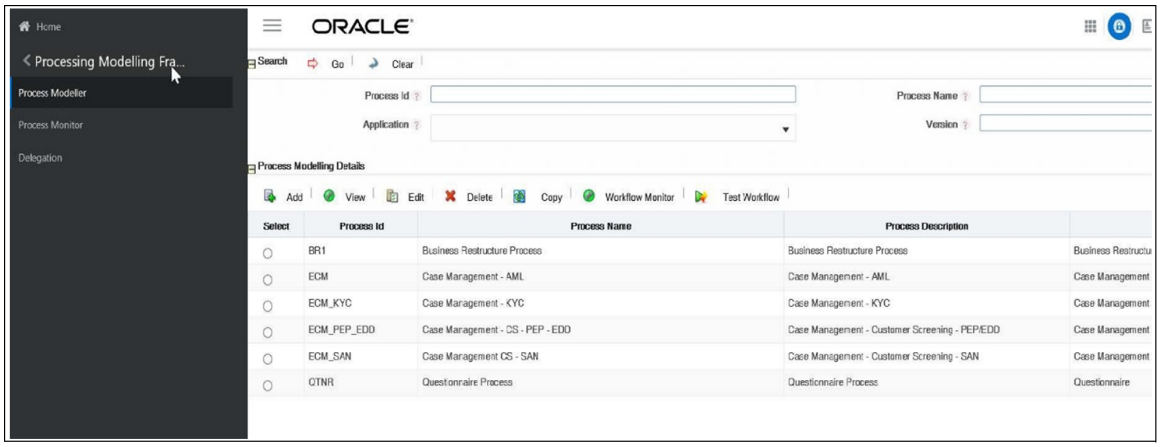
- Creating Workflow
- Defining Datafields
- Defining Application Rules
- Using Process Modeller Editor

11.4.1 Creating Workflow

This section explains how to create a new ECM workflow. To create a workflow, follow these steps:

1. Navigate to the Process Modeller window under Processing Modelling Framework as shown in Figure 52 .

Figure 52: Process Modeller Window



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

Figure 53: Process Details



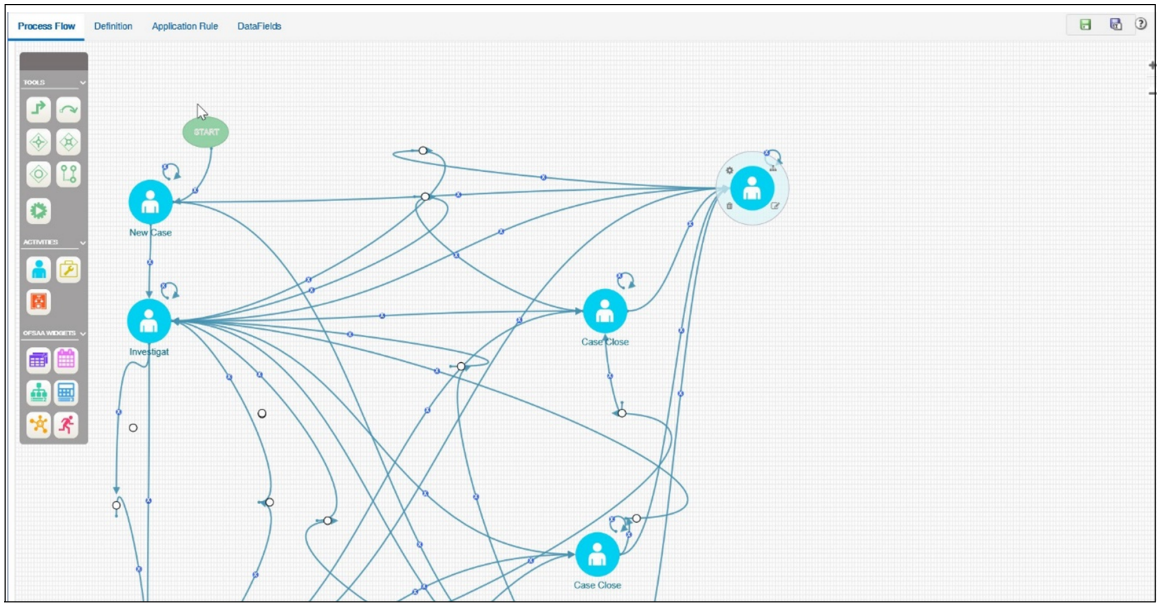
3. Enter the following details in the Process Details window as descibed in Table 38 :

Table 38: Process Details

Field Name	Description
Process ID	Enter the new ECM workflow Process ID.
Process Name	Enter the Process name for ECM workflow.
Process Description	Enter a brief description of the Process.
App Package ID	Select the Case Management from 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 the Process Modeller Summary window or **Save & Launch** to save the definition and open the Process Modeller Editor window as shown in Figure 54 .

Figure 54: Process Modeller Editor window



11.4.2 Defining Datafields

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

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

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

For more information, see the Defining Application Rules section.

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

11.4.3 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 the 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.

11.4.4 Using Process Modeller Editor

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

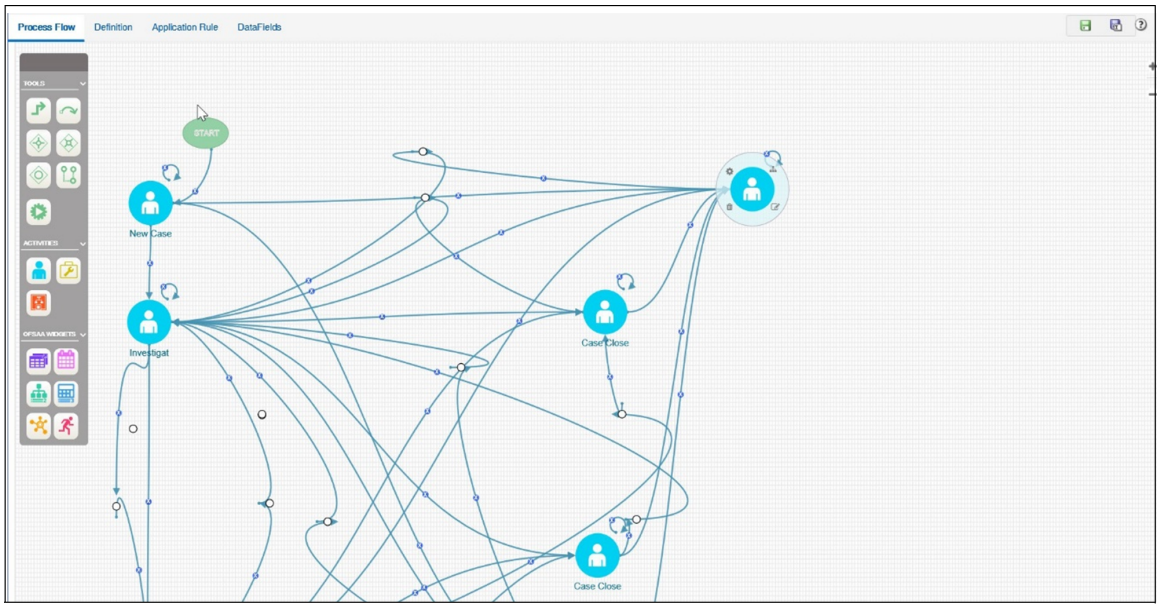
- Adding Transition
- Adding an Activity
- Adding Transition

11.4.5 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 as shown in Figure 55 . This Start activity indicates the first activity to be executed in the Process.
2. Double-click the **Start** icon.

Figure 55: Starting Process



3. Enter the following information in the respective fields as described in Table 39 :

Table 39: Process

Field Name	Description
Activity ID	Displays the automatically generated Activity ID.
Activity Name	The activity name is displayed automatically the same as the Activity ID. Modify the activity name if required.
Activity Desc	Enter the description of the Activity.
Activity Type	By default, the activity type of the selected activity is displayed. To change the activity type, select the required activity type from the drop-down list. The options are Manual, Automatic, Start, Parallel, Sequential, Connector, Run Task, Multi-choice, and sub-process.

Table 39: Process

Field Name	Description
Status	Select the status of the activity from the drop-down list. For example, Closed-SAR, New, Investigation. 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. This is not applicable if the Activity is a Service Task or Run Task.
File Upload	Click Attachment and browse to select the file you want to upload. The progress of file upload is shown. The following message is displayed: Your file has been uploaded after the 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 the Attachment icon adjacent to the file name to remove the file. If a file is attached, the Attachment icon is displayed. Click the Attachment icon to view or save the file.

11.4.5.1 Implementing a Process

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

11.4.5.2 Adding Transition

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

11.4.5.3 Adding an Activity

To add an activity, follow these steps:

1. Click an activity under the 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 as shown in Figure 56 .
3. Enter the following information in the respective fields as described in Table 40 :

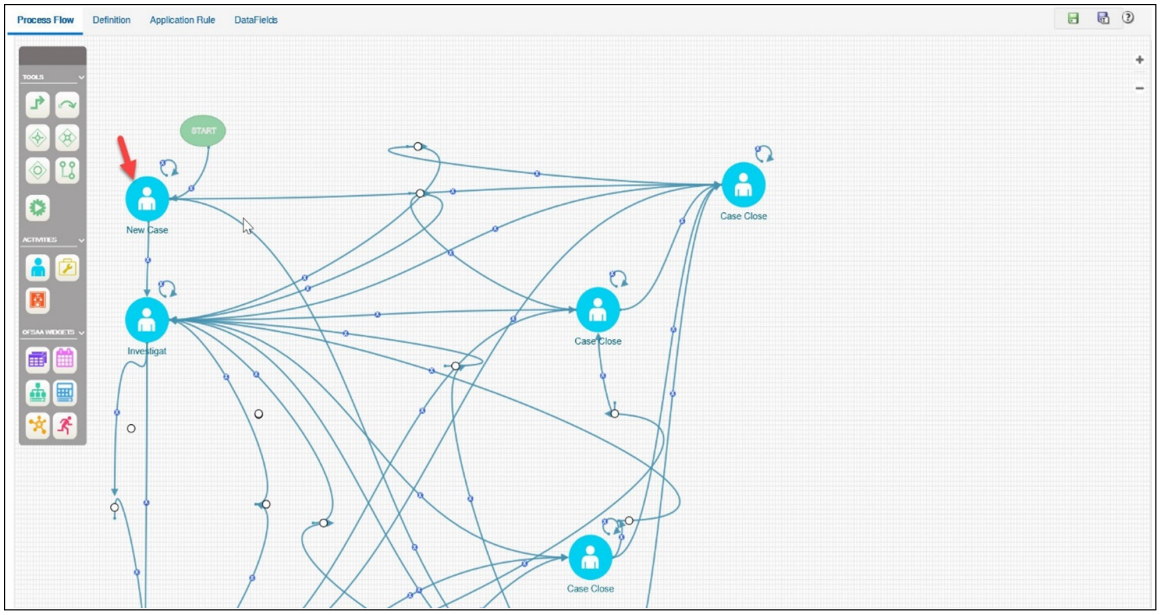
Table 40: Adding Activity

Field Name	Description
Activity ID	Displays the automatically generated Activity ID. For example, Job_1504159648899.
Activity Name	The activity name is displayed automatically the same as the Activity ID. Modify the activity name if required. For example, New Case.
Activity Desc	Enter the description of the Activity.

Table 40: Adding Activity

Field Name	Description
Activity Type	By default, the activity type of the selected activity is displayed. Select the activity type as Manual from the drop-down list. To change the activity type, you can select the required activity type from the drop-down list. The options are Manual, Automatic, Start, Parallel, Sequential, Connector, Run Task, MultiChoice, and sub-process.
Status	Select the status of the activity from the drop-down list as New. The list displays the seeded values in the AAI_WF_STATUS_B table.
Outcomes	Select the required Outcomes from the drop-down list. The list displays the seeded values in the AAI_WF_OUTCOMES_B table. This is not applicable if the Activity is a Service Task or Run Task

Figure 56: Adding Activity

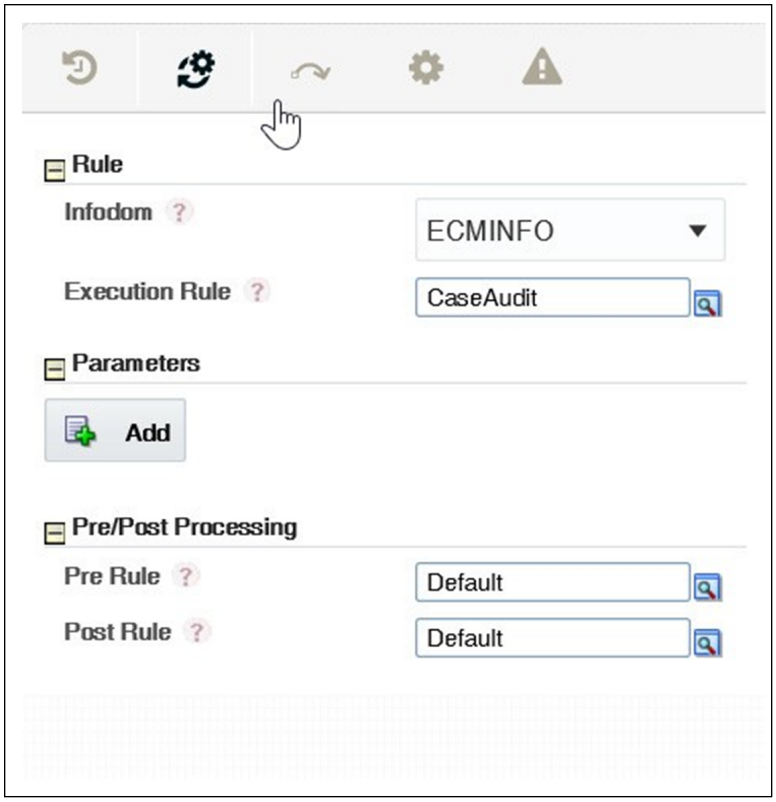


11.4.5.4 Implementing an Activity

This section explains how to implement the New Case as an activity. To implement the newly created activity, follow these steps:

1. Select the **Implementation** tab. The Implementation details are displayed as shown in Figure 57 .

Figure 57: Implementing Activity



2. Go to the 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**.

11.4.5.5 Adding Transition

Using this component you can add the transition to New Case. To add a transition, follow these steps:

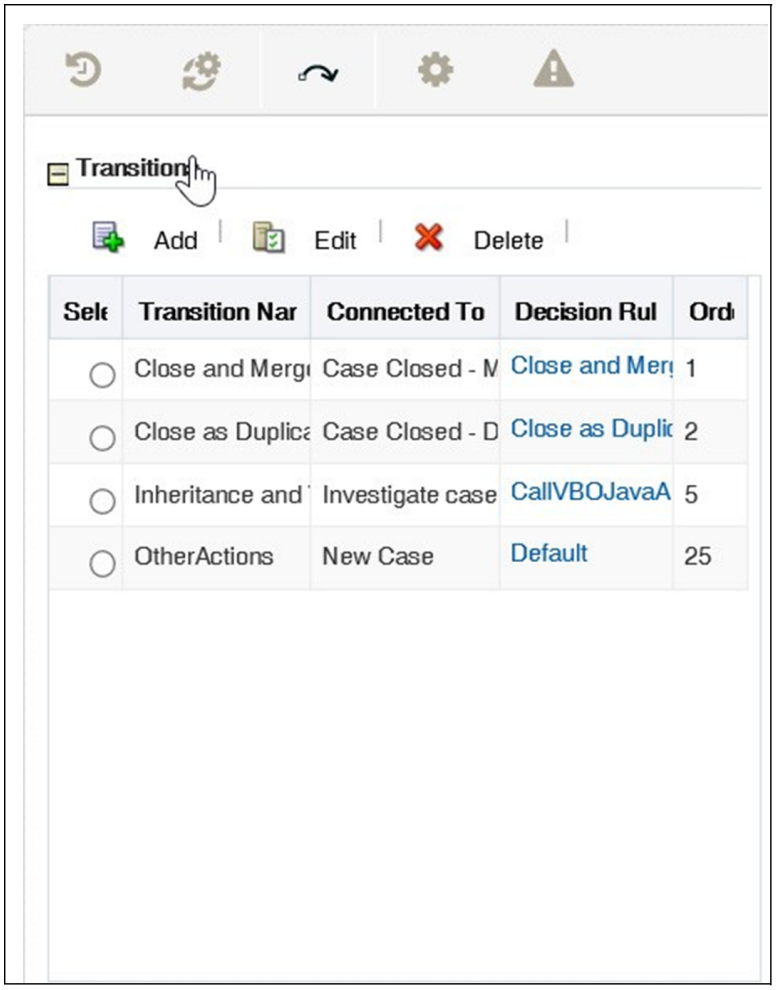
1. Go to the Process Flow tab, click **Transition** from Tools.
2. Click the activity from which you want to start the transition.

   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 the Transitions icon and click **Add**. The Add New Transition window is displayed as shown in Figure 58 .

Figure 58: Add Transition



3. Enter the following information in the respective fields as described in Table 41 :

Table 41: Transition

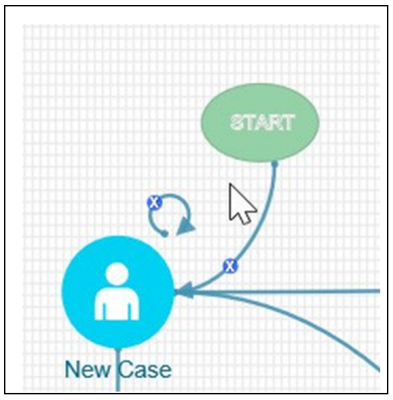
Field Name	Description
Transition Name	Enter the Transition Name. For example: 404688668_Job_1495627226471
Connected To	Select the activity (as New Case) to which you want to connect the current activity, from the Connected To drop-down list. All defined activities in the current Business Process are displayed.

Table 41: Transition

Field Name	Description
Decision Rule	Select the appropriate Decision Rule by clicking the 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 to the next activity. If the output value is FALSE which indicates Failure, the current transition is ignored and the next transition is taken for evaluation if available. If all the transition rules fail (that is evaluated to value FALSE), then the Process remains in the current State. For more information, see the Defining Application Rules section.
Order	Enter the Precedence value based on which the transition Decision rules must be executed for multiple transitions, in the Order field. This affects transitions from a Sequential gateway only.

4. Click **OK**. The transition has linked two activities - Start and New Case as shown in Figure 59 .

Figure 59: Adding Transition

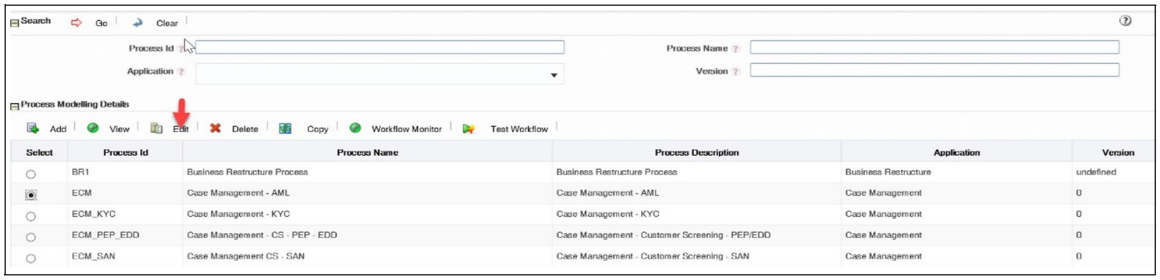


11.5 Editing of an ECM Workflow

To edit an ECM workflow, follow these steps:

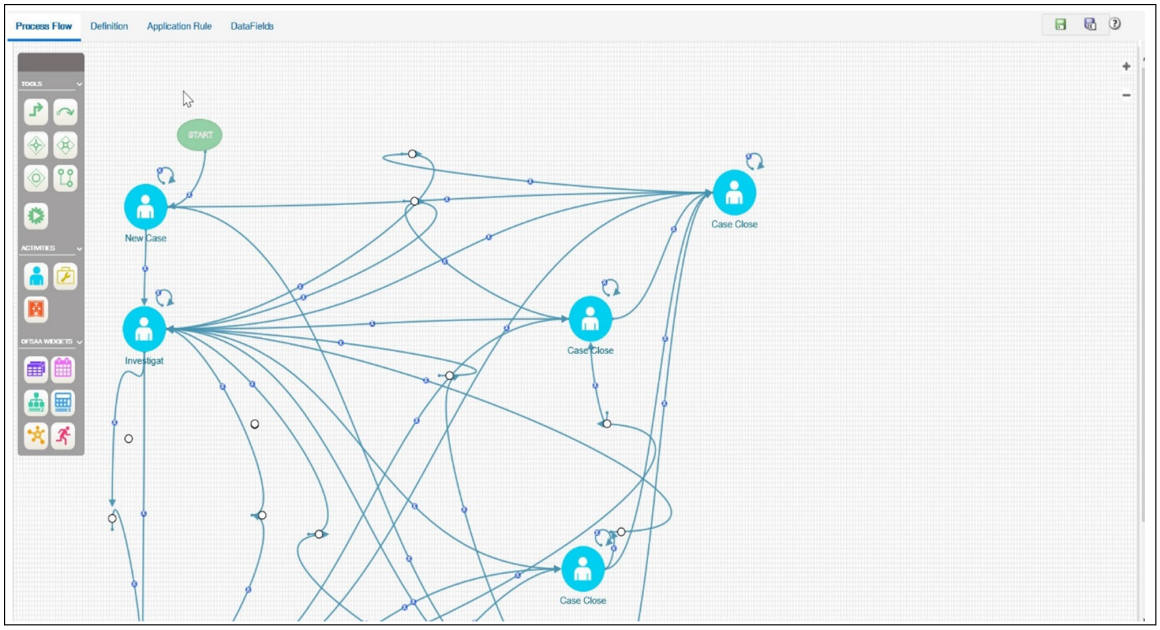
1. Navigate to the Process Modeller window as shown in Figure 60 .

Figure 60: Process Modeller window



2. Select the workflow using the corresponding radio button.
3. Click **Edit**. The Process Modeller window is displayed for editing as shown in Figure 61 .

Figure 61: Editing Workflow



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

11.6 Deleting an ECM Workflow

To delete a workflow, follow these steps:

1. Navigate to the 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**.

11.7 Implementing the ECM PMF Workflow

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

11.7.1 Defining Metadata

Define the following metadata before creating a workflow in PMF:

1. Define ALL actions (status changing and non-status changing) in the KDD_ACTION table as mentioned in Table 33.

> **NOTE** The status changing actions in this table which are left over from earlier versions are also displayed. These will be cleaned up over time. The status changing actions will have the OBS category, so these will not appear on the UI.

Table 42 describes the KDD_ACTION table.

Table 42: KDD_ACTION Table

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

Table 42: KDD_ACTION Table

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

2. Define all statuses in the KDD_STATUS table as as described in Table 43 :

Table 43: KDD_STATUS Table

Column Name	Description	Is column applicable to status-changing action?	Is column applicable to non-status-changing action?
STATUS_CD	Unique code for this status. This code is not displayed on the UI.	X	
STATUS_NM	Status name displayed on the UI.	X	
CLOSED_STATUS_FL	Indicator of whether this status is considered a "closed" status.	X	

Table 43: KDD_STATUS Table

Column Name	Description	Is column applicable to status-changing action?	Is column applicable to non-status-changing action?
CAN_NHRIT_FL	In previous releases, this column was used to indicate whether a case could be inherited when it is in this status. This is now handled by VBO in PMF. It is recommended that this value should be populated in sync with what's defined in PMF.	X	
VIEWD_BY_OWNER_ACTVY_TYPE_CD	In previous releases, this column was used to record the action code for the VBO action. This action would be recorded on a case with this status when the case was viewed by a user with privileges to own the case. This information is now defined in PMF. However, it is recommended that this value should be populated in sync with what's defined in PMF.	X	
VIEWD_RESULT_STATUS_CD	In previous releases, this column was used to record the resulting status of the VBO action. This information is now defined in PMF. How- ever, it is recommended that this value should be populated in sync with what's defined in PMF.	X	

3. Define which non-status changing action will be available for which user role in KDD_ROLE_ACTION_MAP table as described in Table 44 :

Table 44: KDD_ROLE_ACTION_MAP table

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

4. Define which non-status changing action will be available in which case status in KDD_STATUS_ACTION_MAP table as described in Table 45 :

Table 45: KDD_STATUS_ACTION_MAP Table

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

5. Define which non-status changing actions will be available for which case type in KDD_CASE-TYPE_ACTION_MAP table Table 46 :

Table 46: KDD_CASE_TYPE_ACTION_MAP Table

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

6. Add all statuses to AAI_WF_STATUS_B and AAI_WF_STATUS_TL tables in the Config schema
   - AAI_WF_STATUS_B table:
     i. Contains the status code and package map
     ii. In STATUS_ID enter the status code used in KDD_STATUS.STATUS_CD
     iii. The package ID should be OFS_NGECM if this workflow is for use with ECM
   - AAI_WF_STATUS_TL:
     i. Contains the status name and package map
     ii. Enter the Status ID, Status Name, and Status Description as you entered them in KDD_STATUS. (The Description should be the same as the Name)
7. The package ID should be OFS_NGECM if this workflow is for use with ECM.

11.7.2 Creating the Workflow in PMF

1. Add a new workflow from the Process Modeler landing page. This creates a blank workflow and the system will navigate the user to a Process Modeler page. This page contains several tabs (Process Flow, Definition, Application Rules, and so on.) that will be used to create the workflow. Below are some of the basic things you will need to define to create a workflow in PMF.
2. Define the "Application Rules"

- An "application rule" is a rule that is executed with an activity or a transition.
- Several rules can be created in PMF (Stored Procedure, Attribute Expression, Java API, and so on) - all these rules need to be categorized as one of the three main types of rules:
  - Execution Rule - this is the business logic executed by the activity. For example, the OOB AML workflow includes an execution rule called "Case Audit". This rule is used by all activities where the action leading to that activity is going to be recorded on the case audit history.
  - Decision Rule - This rule returns a "True/False" value that is used in decision making during a transition.
  - For actions that will be displayed on the Take Action window, an "Attribute Expression" decision rule should be created. This is how PMF will know which action should be displayed on the Take Action window for which user role and in which case status. To create an attribute expression on the Application Rule tab:

3. Click the **Add** button (on the top-left side of the tab) to open a menu. Select "Attribute Expression" from this list. "Rule Details" window is displayed.

   On the Rule Details window, enter the name of this attribute expression.

   Select "Action" in the Attribute drop-down and click Add. This will add a record in the Attributes Values section. In the Attributes Values section, the "Value" drop-down shows all the actions defined in KDD_ACTION. Select the action(s) you want to associate with this rule.

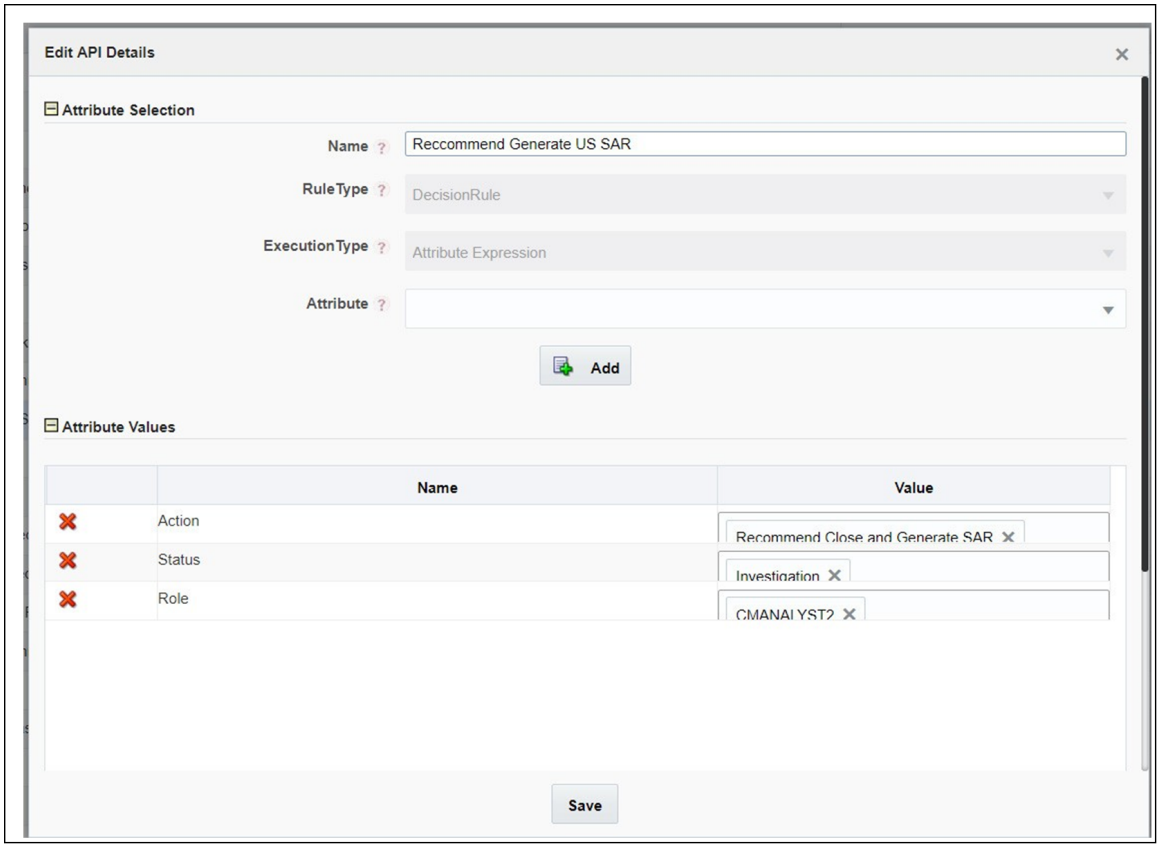
   Select "Status" in the Attribute drop-down and click Add. This will add another record in the Attributes Values section. The Value drop-down displays all the statuses defined in KDD_STATUS. Select the status(es) you want to associate with this rule.

   Now select "Role" in the Attribute drop-down and click Add. This will add another record in the Attributes Values section. The Value drop-down shows you all the roles defined for ECM. Select the role(s) you want to associate with this rule.

4. Click **Save**.

   Figure 62 depicts the Attribute Expression details window.

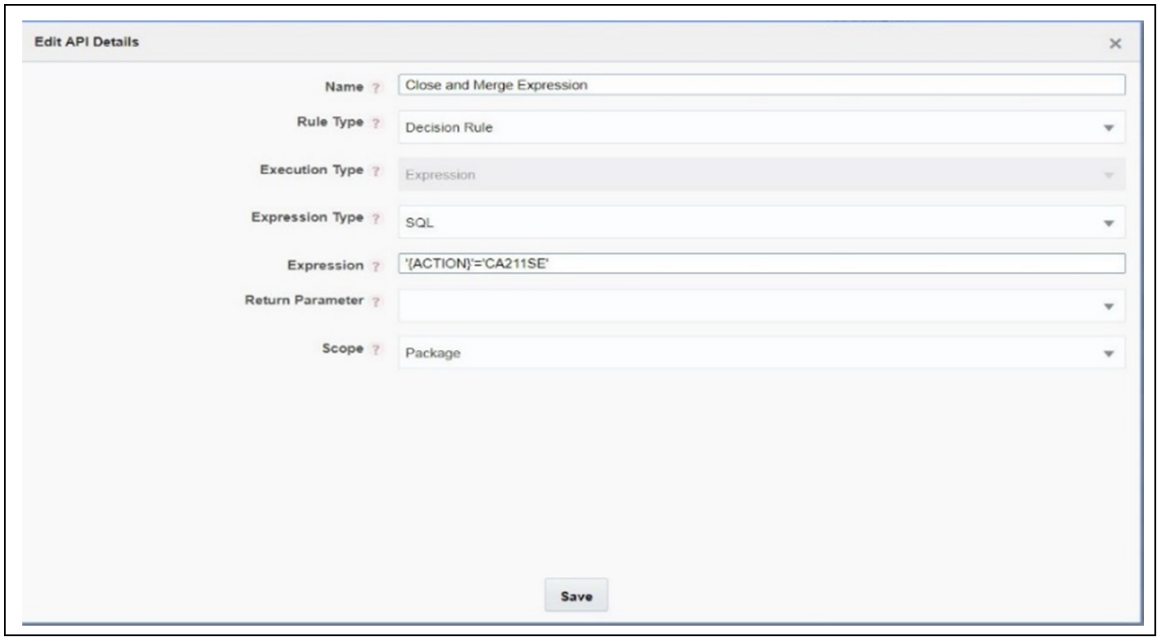
Figure 62: Attribute Expression details window



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

Figure 63 depicts the Expression Details.

Figure 63: Expression Details



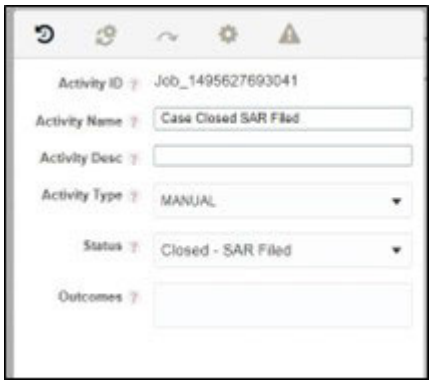
- **Selection Rule** - This rule fetches some value, useful to get value dynamically from a table or other source. OOB ECM does not use selection rules.
  - Define application rules on the "Application Rules" tab within Process Modeler before drawing activities and transitions on the Process Flow tab.
  - Workflow logic determines which types of rules need to be created. OOB ECM only uses execution and decision rules.
  - For more information about application rules refer to the AAI user guide.

5. Draw the "activities" (i.e. case statuses) on the "Process Flow" tab:
   - An "activity" means a case status. From the Left-Hand-Side menu, add the applicable type of "activity" to the canvas.
     - Select a "Human Task" if human action is required to move the case to the next status. This is what will be used most of the time as almost all case workflows require a user to take any action that moves the case to the next status.
     - Select a "Service Task" if an automatic activity is going to move the case to the next status.
     - Select a "Sub Process" if you want to call another Process/ Workflow from your current workflow.
   - After selecting an activity and adding it to the canvas, double click on the activity to open a window (that has many tabs) to enter details about this activity.
   - On the first tab of this window, enter "Activity Details" as follows:
     - **Activity Name** = name of status. This name is just for use in PMF - ECM UI displays the status name defined in KDD_STATUS.
     - **Activity Description** = description of this status for use in PMF.
     - **Activity Type** = pre-populated based on the type of activity selected from the LHS menu (human, service, and so on) but can be changed as needed.

- **Status** = associate this activity with a status defined in the database. This drop-down list displays the values in the AAI_WF_STATUS_B table.
- **Outcomes** = OOB workflows do not use this setting. For more details about this setting, refer to the AAI user guide.

Figure 64 depicts the Activity Details tab.

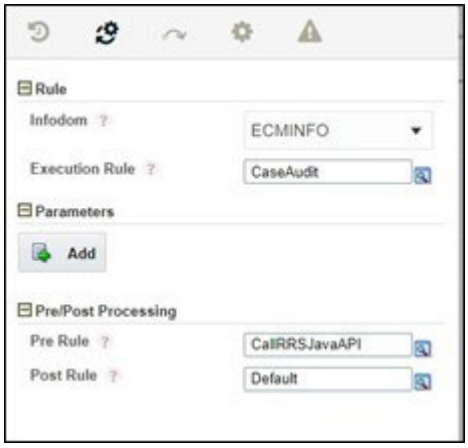
Figure 64: Activity Details tab



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

Figure 65 depicts the IMPL tab.

Figure 65: IMPL tab



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

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

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

   Figure 66 depicts the Workflow Diagram.

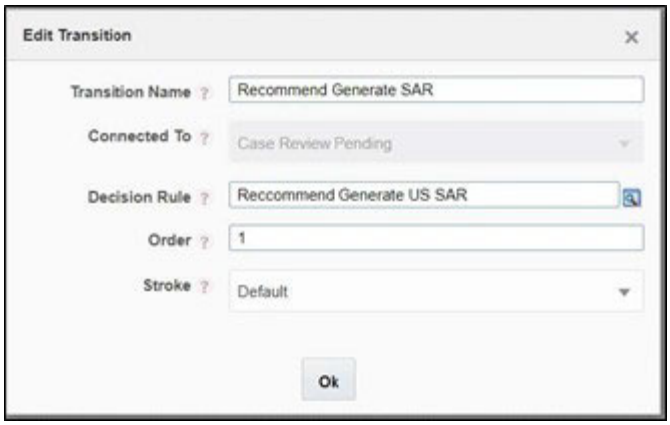
Figure 66: Workflow Diagram



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

Figure 67 depicts the Edit Transition window.

Figure 67: Edit Transition window



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

   Creating new data fields is possible in PMF but passing the value from ECM to PMF required a code change.
8. Save the workflow:
   - Following two buttons on the Process Flow tab to save the workflow:
     - **Save button** - use this form of saving if you are creating a brand new workflow OR editing an existing workflow and do not need to maintain the previous version of that workflow. This button overwrites the workflow being edited. As a result, all cases (in-flight and closed) using that workflow will follow the modified workflow as soon as the changes are saved in PMF. New cases (of the Case Type(s) using this workflow) will also use this modified workflow.

— **Save as New Version button** - use this form of saving if you are editing an existing workflow and do not want to change the version which you selected to edit. This button saves the modifications as a new version of the workflow and leaves the previous version unchanged. The version number assigned to this new version = parent workflow's version number + 1. For example: If the parent workflow had a version number 4, this new version will have a version number 5. But just saving a new version of a workflow does not have any impact on any case unless this new version is mapped to a Case Type in Case Designer. When the Case Type-Workflow mapping is updated in Case Designer, all cases of that Case Type created after the update will use the latest workflow mapped to the Case Type. All older cases of that Case Type continue on the version they were using previously. The moment a case type is mapped to a different workflow, new cases will start using the new workflow (but old cases will not be impacted).

NOTE In the Case of Designer you can associate any version of a workflow with a Case Type. Case Designer does not have any restrictions around which version of a workflow can be linked to a Case Type.

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

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

11.7.4 Steps to customize the "Checklist" functionality in ECM

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

11.7.5 Configuring CRR Workflows in PMF

You can configure CRR workflows for various STRs.

1. Navigate to the Process Modeller window.
2. Go to Case Management-AML. A new window with workflow will open.

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

11.7.6 Configuring Change Case Type Action in PMF

This section describes the overview and PMF configuration.

This section outlines how to configure PMF to allow for the Change Case Type action. This features allows a user to select a target case type and the resulting status the case should be in when the case type is changed. The action is only available to user roles and statuses as defined in the source workflow. In PMF the source workflow will display 'change case type' transitions from each status where the action can be taken pointing to 'dummy' task that acts as a portal to the target workflow. The target process flow will in turn have transitions coming in to each status in which the user can land once the case type is changed. If a user can come into and out of a single workflow you will see both in and out transitions in the workflow.

NOTE

- When the user selects from the list of case types they view all case types they have permission to see.
- When the user selects from the list of statuses available in the target case type the list displays all statuses in the target workflow. If the target workflow is not configured to allow the case to be landed in that status then it will default to the 'New' status once the case type is changed.

11.7.6.1 PMF Configuration

For PMF configuration, follow these steps:

1. Configuring the Source Workflow:
   a. Create a new Attribute Expression to define each change case type action, who can take that action and in which statuses it should be available. This will result in a new expression for each status where the user can change the case type.
   b. The Action attribute must have the value of 'Change Case Type' defined (code 1007)

c. For the NextStatus attribute if you want to have every status in the workflow allow the change case type action then do not define the NextStatus attribute. This expression can then be reused for all transitions.

2. In the Process Flow:
   a. Add a manual task and name it something like 'Change Case Type'. This is the dummy portal task and nothing else needs to be defined.
   b. Draw a transition from each status where the Change Case Type should be displayed pointing to portal status.
   c. In the properties of the transition, select the Attribute Expression created for that status (from #1 above).
   d. The portal status should also have a self-transition loop to ensure that the workflow doesn't end at that status.
3. Configure the Target Workflow. In all the workflows for the case types which the user can select, perform the following tasks:
   a. Create an attribute expression for each status where the user can land in the target workflow.
      i. The attribute expression only needs to have the NextStatus attribute added and the value should be the status where it can land.
      ii. It is best to name the expression as one that is related to changing the case type.
   b. In the Process Flow add a Service Task.
   c. From Start draw an arrow so it only goes to the Service Task. WHAT DO I NEED TO DEFINE HERE?
   d. From the Service Task draw a transition to all the statuses in which the user can land.
   e. In the properties of those transition select the NextStatus attribute expression for that status (as created in #3a).
   f. Draw a transition from the Service Task to the New status (or whatever status indicates it is a new case)
   g. This transition will not have any rule defined but the order should be a large number. This is because, if the workflow cannot find a route to the status the user selected it will default to land it in New.
4. If the users can change back to the source workflow from the target:
   a. In the Target workflow, create and draw the transitions and portal status as defined above.
   b. In the Source workflow, from the portal status draw transition to each of the statuses the case can land back in. These transitions should only have the NextStatus attribute.

12 Managing Case Designer

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

The following topics are covered in this chapter:

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

12.1 About Case Designer

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

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

List of features:

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

- Changes to Case Class and Case Type definitions are automatically reflected in the Case Management UI.

12.2 Accessing Case Designer

This section explains how to access the Case Designer page. To access the Case Designer page, follow these steps:

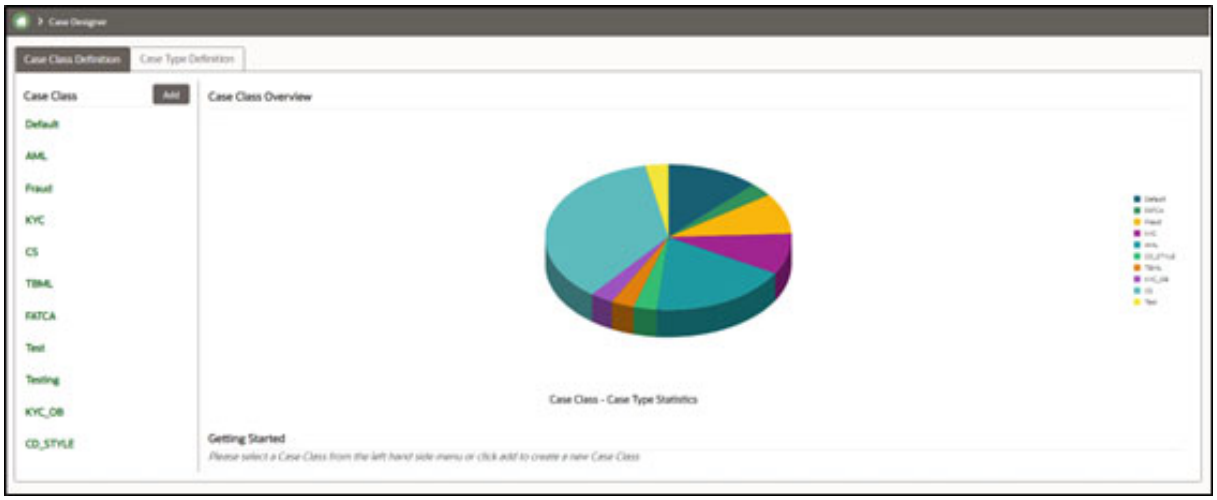
1. 1.Navigate to the Case Management Configuration page. For more information on how to navigate to the Case Management Configuration page, see Getting Started.
2. 2.Click **Case Designer**. The Case Designer page is displayed.

12.3 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 68 depicts the Case Designer Home Page - Case Class Definition.

Figure 68: Case Designer Home Page - Case Class Definition



To view the Case Designer Home page, follow these steps:

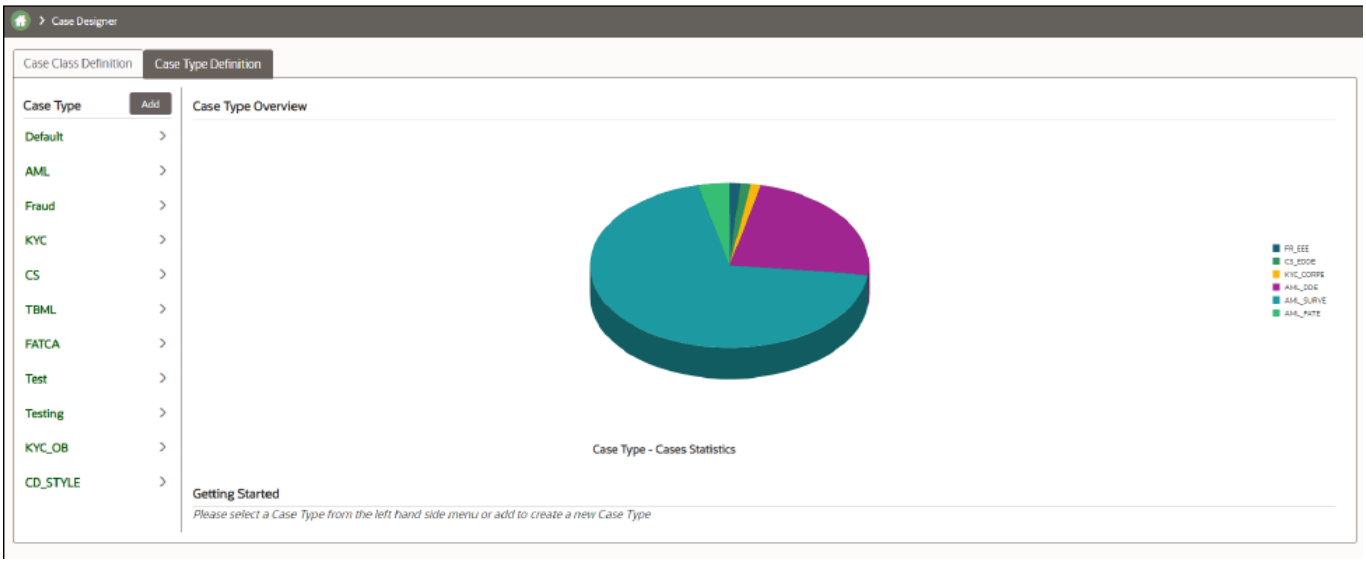
1. Navigate to the Case Designer page.
2. Click the **Case Class Definition** or **Case Type Definition** tab. The previously added Case Class or Case Type list is displayed in the Left Hand Side (LHS) menu.
3. Select the **Case Class Definition** tab and go to the **Case Class Overview** section. Hover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

   OR

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

   Figure 68 depicts the Case Designer Home Page - Case Type Definition.

Figure 69: Case Designer Home Page - Case Type Definition



4. 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.

12.4 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

12.4.1 About Case Class

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

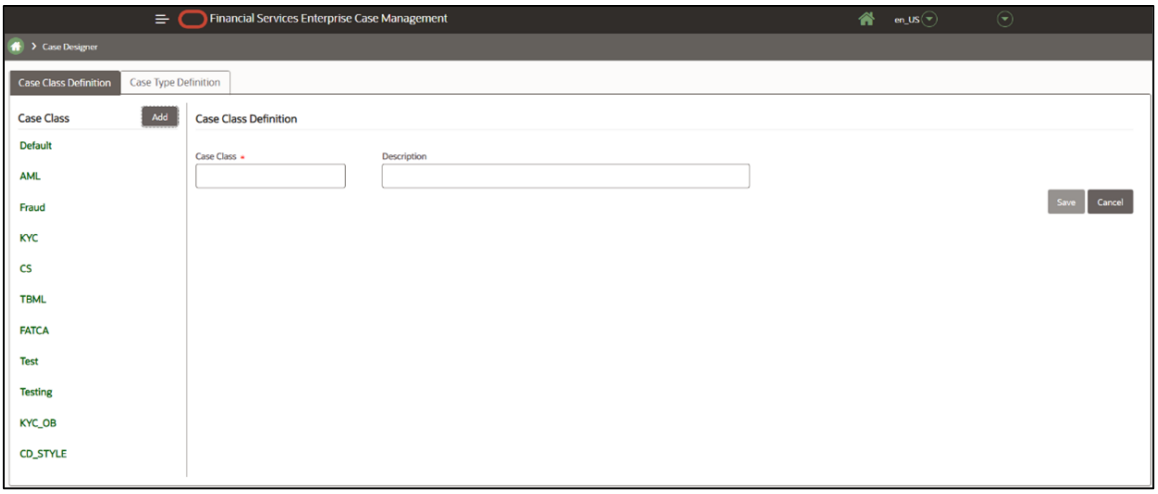
12.4.2 Adding Case Class

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

To add a new case class, follow these steps:

1. Navigate to the Case Designer page.
2. Click the **Case Class Definition** tab.
3. Click **Add**. The Case Class Definition page is displayed as shown in Figure 70 .

Figure 70: Case Class Definition



4. Enter the required information in the respective fields.
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.

12.4.3 Editing Case Class

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

> **NOTE** A Case Class is updated even if cases are linked to the case type.

To modify a case class, follow these steps:

1. Navigate to the Case Designer page.
2. Click the **Case Class Definition** tab.
3. Select the existing case class in the LHS menu. The case class details are displayed in the RHS panel.
4. Modify the necessary information in the required fields.
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.

12.5 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

12.5.1 About Case Type

- A Case Type is the second level definition after Case Class through which cases are created.
- Provides a more detailed classification of a case. For example, If the Class is *AML*, the 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.

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

12.5.2 Adding Case Type

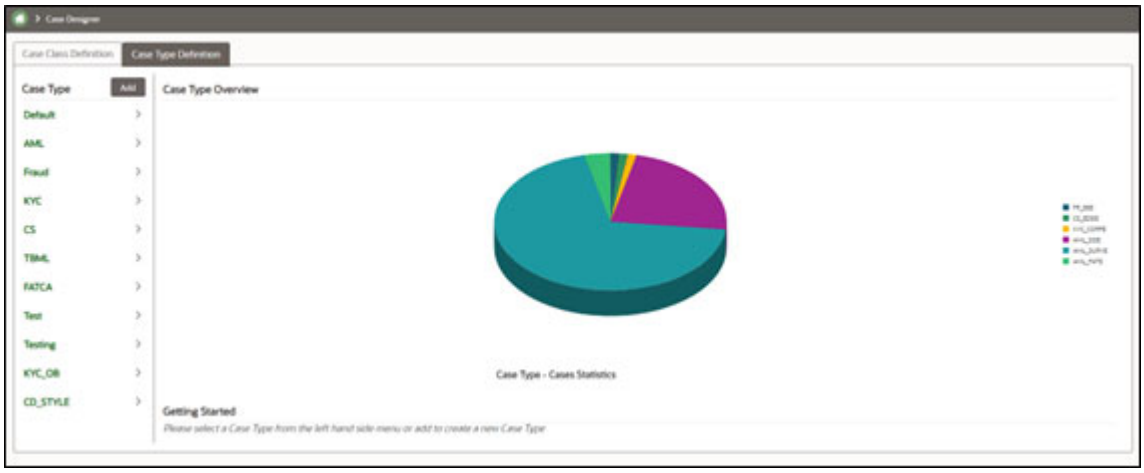
This section describes how to add a new case type to the existing case class along with related attributes, entities, and workflow.

To add a new case type, follow these steps:

1. Navigate to the Case Designer page.
2. Click the **Case Type Definition** tab.

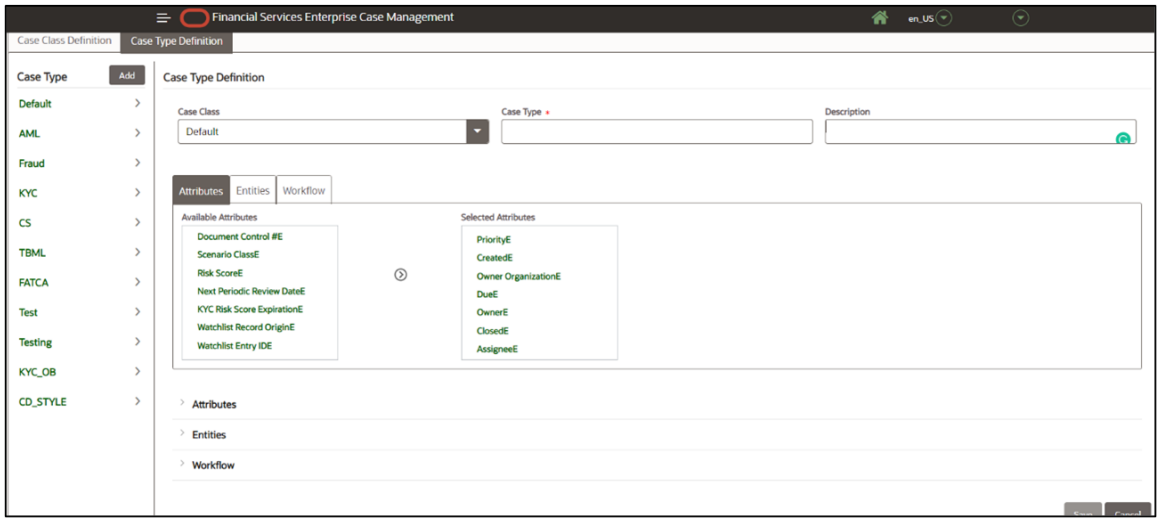
Figure 71 depicts the Case Type Definition page.

Figure 71: Case Type Definition



3. Click **Add**. The Case Type Definition page is displayed as shown in Figure 72 .

Figure 72: Case Type Definition



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.

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*.
6. When you modify case type definitions, you cannot edit the Case Type name.
7. 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.

8. 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.

12.5.2.1 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:

12.5.2.1.1 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.

12.5.2.1.2 Defining Attributes

This section describes additional attributes definitions and how to configure them in the Case Type. The following sections are covered in this topic:

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

12.5.2.1.3 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 their behavior across the different case pages. For example, the Case ID attribute is hidden on the Create Case page but it is disabled on the Case Context page.
- Whenever changes happen to attributes those changes are reflected on all case-related pages based on its behavior in the Enterprise Case Management UI.
- Due to performance concerns, we restrict the loading of Case Type Attributes' drop-down values in the Attributes section of Case designer screen. However, the Case Designer displays all types of fields.

12.5.2.1.4 Adding Optional Attributes to the Case Type

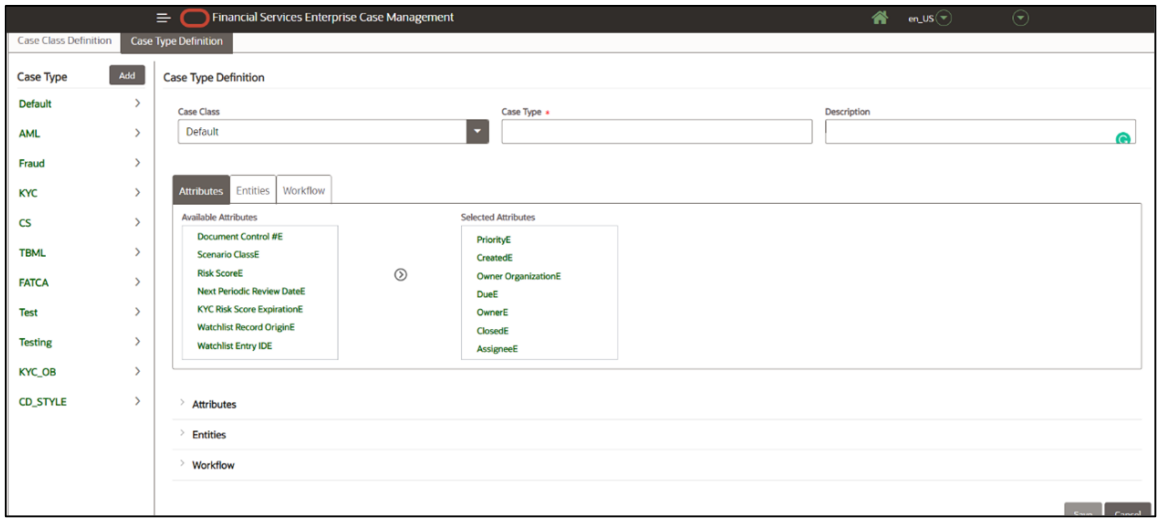
This section explains how to add optional attributes to a case type. By default, optional attributes are displayed in the Available Attributes box. The mandatory attributes are displayed in the Selected Attributes box. You can select optional attributes and move them to the Selected Attributes box. All

attributes that are in the Selected Attributes box appear as fields in the case related pages of ECM UI based on its behavior.

To add optional attributes, follow these steps:

1. Navigate to the Case Type Definition page.
2. Click the **Attributes** tab. The optional attributes are displayed in the Available Attributes menu as shown in Figure 73 .

Figure 73: Attributes Page



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

> **NOTE** CS Case Type Specific Attributes must not be mapped to other case types.

12.5.2.1.5 Deleting Attributes

This section explains how to remove optional attributes from the Case Type. To remove optional attributes, follow these steps:

1. Navigate to the Case Type Definition tab.
2. Select the required Case Type. Go to the Attribute section.
3. Click the **cross** icon against the required attributes to remove from the 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.

12.5.2.1.6 Defining Entities

This section describes an Entity and how to configure it in the Case Type. The following sections are covered in this topic:

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

12.5.2.1.6.1 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 the following:
  - Mandatory Entities - These entities are by default associated to the case type at the time of creation. These entities cannot be disassociated from the case type.
  - Optional-Default Entities - These entities are by default associated to the case type at the time of creation. These entities can be associated/disassociated to/from the case type using Case Designer. Evidence, Relationship, Audit History are the Optional-Default entities provided out of the box.
  - Optional Entities - These entities are not by default associated with the case type at the time of creation. These entities can be associated/disassociated to/from the case type using Case Designer. Event Details, Narrative, Correlation, Account, Customer, Employee, Household, Investment Advisor, External Entity, Correspondent Bank, Transactions, Financials, Involved Party, Network Analysis, Customer Screening, KYC Risk Score, External Entity Screening, Trade, Trade Finance, Real-Time Screening are the Optional entities provided out of the box.
- Case Summary section of ECM UI display entities (tabs) even there is no data is associated with the entity.
- Add or remove only optional and optional-default entities.
- Ordering of entities can be configured.
- Whenever changes happen to entities those changes are reflected in the Case Summary section for that Case Type in Enterprise Case Management UI.

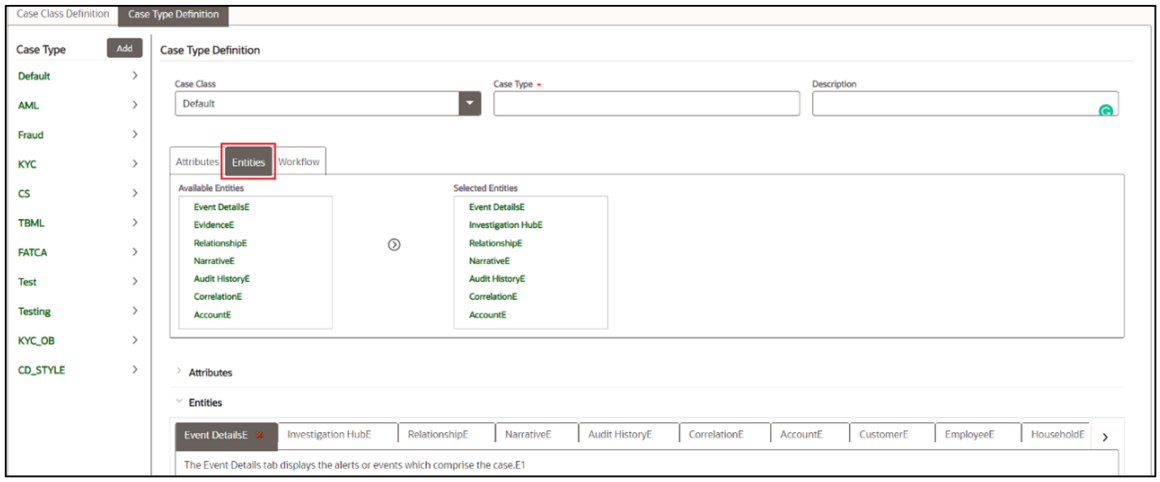
12.5.2.1.6.2 Adding Optional Entities to the Case Type

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

To add optional entities, follow these steps:

1. Navigate to the Case Type Definition page.
2. Click the Entities tab. The optional entities are displayed in the Available Entities menu as shown in Figure 74 .

Figure 74: 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 the Entities sections as tabs.

> **NOTE** The newly added entities are marked with **cross** icon.

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

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

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

12.5.2.1.6.3 Deleting Entities

This section explains how to remove optional entities from the case type. To remove optional entities, follow these steps:

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

> **NOTE** The deleted entities (tabs) do not display on the Case Summary section in the Enterprise Case Management UI.

12.5.2.1.7 Defining Workflow

This section describes the workflow and its usage in case type. The following sections are covered in this topic:

- About Workflows

- Adding Workflow
- Deleting Workflow

12.5.2.1.7.1 About Workflows

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

12.5.2.1.7.2 Adding Workflow

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

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

To add a workflow, follow these steps:

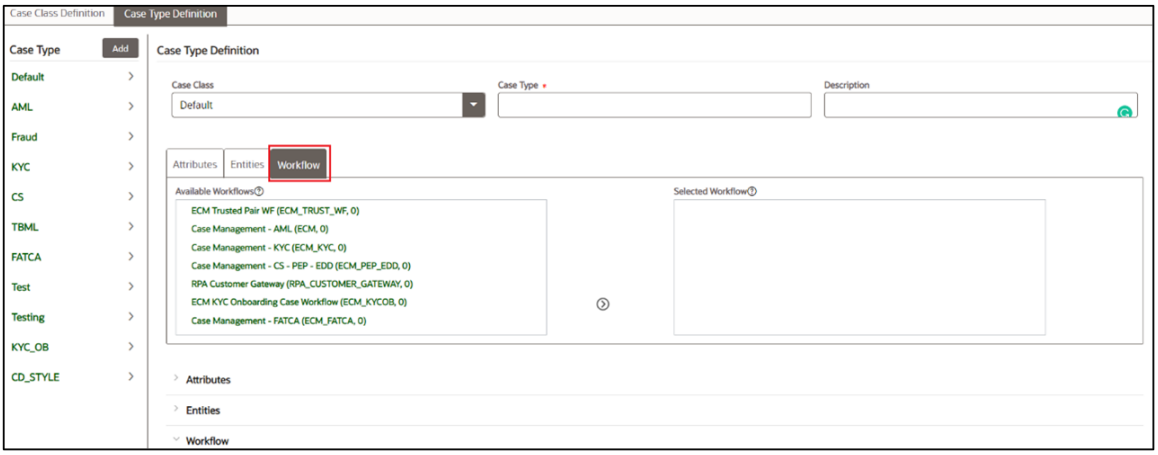
1. Navigate to the Case Type Definition page.
2. Click the **Workflow** tab. The defined workflows are displayed in the Available Workflows menu with the following format as shown in Figure 75 :

   Process Name (ProcessID) - v#

   Here:

   - Process Name is the name of the workflow.
   - ProcessID is the unique identifier assigned to this workflow.
   - v indicates that a version number is going to follow.
   - # is the actual version number assigned to this workflow.

Figure 75: Workflow Page



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

> **NOTE** The newly added attributes are marked with **cross** 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*.

12.5.2.1.7.3 Deleting Workflow

This section explains how to remove the workflow from the Case Type. To remove the workflow, follow these steps:

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

12.5.3 Editing Case Type

This section describes how to modify existing Case Type definitions.

To modify a case type, follow these steps:

1. Navigate to the Case Designer page.
2. Click the **Case Type Definition** tab.
3. Select an existing case type in the LHS menu. The Case Type Definition page is displayed.
4. Modify the necessary details in the Case Class and Description fields. Case Type is not editable.
5. Click **Save**. The Case Type Definition section is updated.

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

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

13 Case Allocation Management

The Automated Case Allocation feature assigns cases to individuals or pools at any point during the case investigation process based on the defined allocation rule. This feature saves managers/ administrators from having to go through each case and manually assign the case to team members based on the selected criteria.

This chapter covers the following topics:

- Accessing Case Allocation Assignment Page
- Searching an Allocation Rule
- Associating a Rule
- Disassociating a Rule
- Setting the Out Of Office
- Clearing the Out Of Office

13.1 Accessing Case Allocation Assignment Page

To access the Case Allocation Assignment tool, follow these steps:

1. Navigate to Enterprise Case Investigation: see the Getting Started section for more information.
2. From the Enterprise Case Investigation menu, select **Case Allocation Assignment**.

   Figure 76 depicts the Case Allocation Assignment page.

Figure 76: Case Allocation Assignment



13.2 Searching an Allocation Rule

The Allocation Search enables users to return all users and pools, based on select search criteria, who can then have a rule(s) assigned to them.

To search the allocation rule, follow these steps:

1. The following criteria are available in the Allocation Search pane as described in Table 47 .

Table 47: Search Fields

Field	Description
Name	This type-ahead box displays all users and pools. Note: This supports the wild-card search using the percent sign (%).
ID	This type-ahead box displays the user IDs of all users and pools

Table 47: Search Fields

Field	Description
Jurisdiction	Displays the list of all Jurisdictions and filters the results by the business jurisdictions associated with the user/pool. Note: The drop-down list contains only jurisdictions you are authorized to view.
Business Domain	Displays as all Domains and filters the results by the business domain associated with a user. Note: The drop-down list contains only business domains you are authorized to view.
Rule	Displays all rules defined in the FCC_ASSGN_RULE_DEFN table.
Active/Inactive	This filters the results by the status of the user or pool.

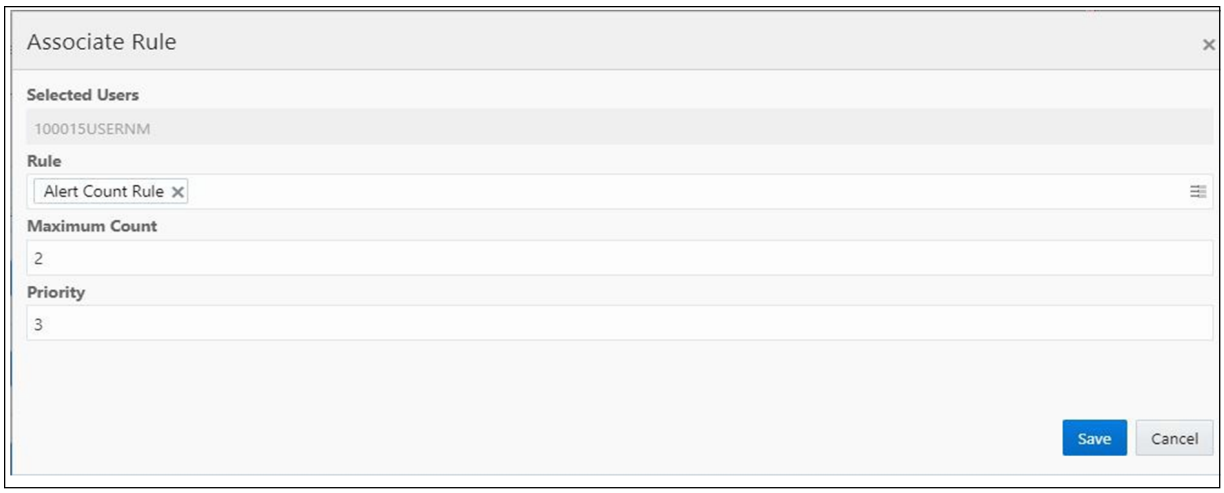
2. Select Search to return the list of users that match the criteria.
3. Select Save to save that search criteria. It will run automatically the next time the tool is accessed.

13.3 Associating a Rule

Individual users/pools are mapped to a rule using the Associate Rule option. A single user/pool can be mapped to multiple rules if necessary and a single rule can be mapped to multiple individuals/pools.

Figure 77 depicts the Associate a Rule page.

Figure 77: Associate a Rule



To associate a rule, follow these steps:

1. Select the user from the Assigned Allocation list.
2. Select the Associate Rule link to open the Associate Rule window.

3. The following information is available as described in Table 48 :

Table 48: Associating a Rule

Field	Description
Rule	This list contains all rules defined in the FCC_ASSGN_RULE_DEFN table. One or more rules can be selected.
Maximum Count	This value defines the maximum number of cases that can be assigned to that user at any given time for that rule(s).
Priority	Set the priority of the user. This value defines the priority in which the rules assigned to this individual will be run. This is done to assist with load balancing. The priority numbers must be defined in sequential order (1, 2, 3...). No two associations can have the same priority for a user.

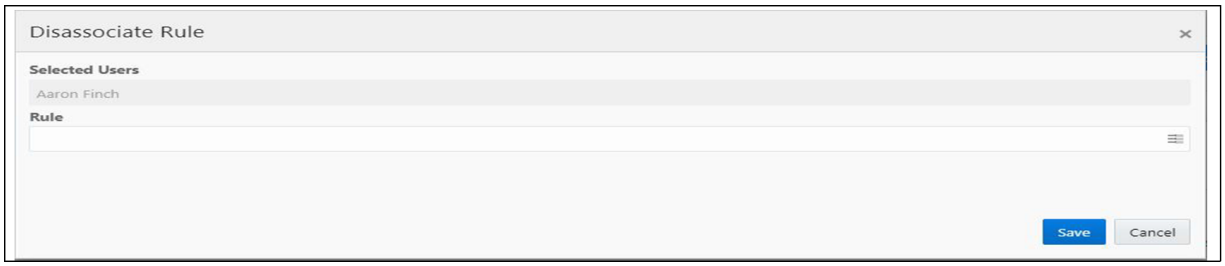
4. Select **Save**.

Example of Allocation Association: Let's assume the client has senior investigators who are to focus primarily on difficult cases but also help on easier cases when they are able. These investigators should never have more than 100 cases assigned to them at any given time. Two allocation rules would be created; one for easy cases and one for hard. A senior investigator would then have the hard allocation rule associated with them with a Maximum Amount of, for example, 75 and a Priority of 1. The easy rule would be associated with a Maximum Amount of 25 and a Priority of 2. This would ensure the investigator has mainly difficult cases but always has some easy ones.

13.4 Disassociating a Rule

You can remove a rule from an individual user/pool using the Disassociate Rule option as shown in Figure 78 .

Figure 78: Disassociate a Rule



To disassociate a rule, follow these steps:

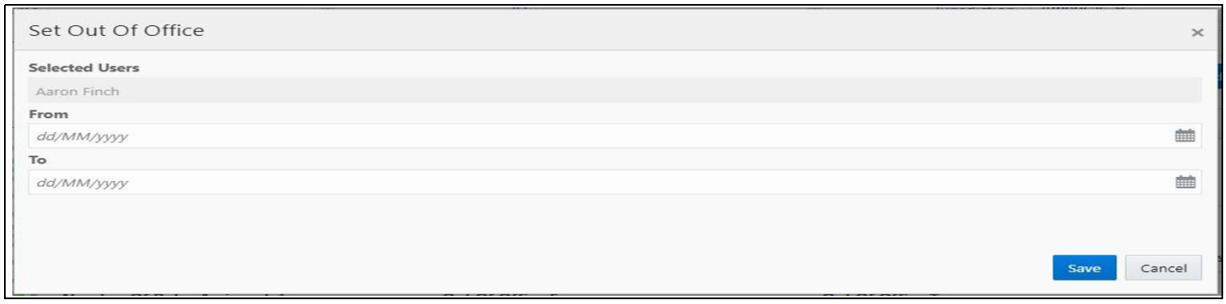
1. Select the user from the Assigned Allocation list.
2. Click **Disassociate Rule** to open the Disassociate window.
3. Select the Rule from the list of all the associated rules mapped to that user.
4. Select **Save**.

13.5 Setting the Out Of Office

You can set the Out Of Office option for the selected user. The allocation jobs will not assign any new cases between the selected dates when an individual is out of office. After the To date is reached, the user will start to receive cases again.

Figure 79 depicts the Set Out Of Office page.

Figure 79: Set Out Of Office



To set the Out Of Office, follow these steps:

1. Select the user from the Assigned Allocation list.
2. Click **Set Out of Office**.
3. Enter the From and To dates in dd/MM/yyyy format.
4. Select **Save**.

13.6 Clearing the Out Of Office

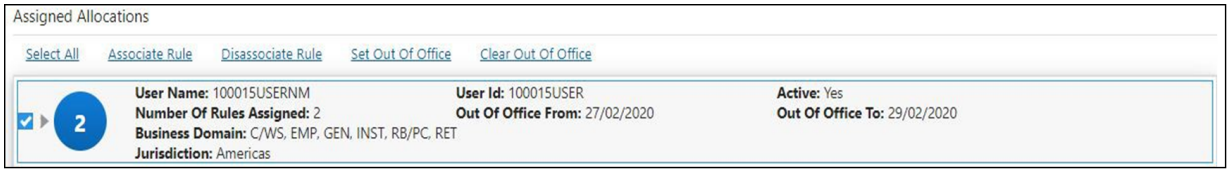
An Administrator can clear the out of office for the selected user.

To clear the Out Of Office, follow these steps:

1. Select the user from the Assigned Allocation list.

   Figure 80 depicts the Assigned Allocations page.

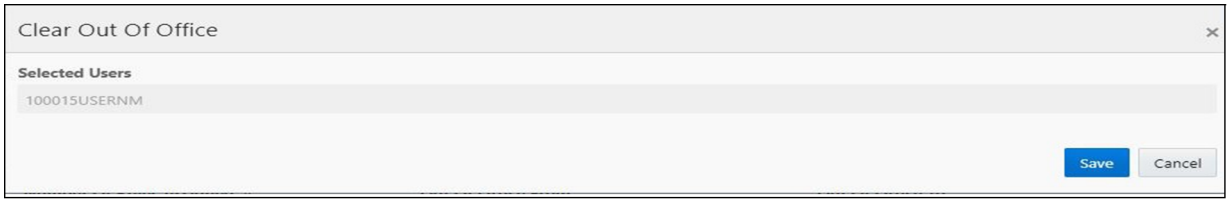
Figure 80: Assigned Allocations



2. Click **Clear Out of Office**.

   Figure 81 depicts the Clear Out Of Office page.

Figure 81: Clear Out Of Office



3. Select **Save**.

   Figure 82 depicts the Assigned Allocations page.

Figure 82: Assigned Allocations



14 General Configuration

This chapter provides instructions to configure the parameters for case management and includes the following topics:

- Configuring the Client Logo Image
- Accessing Manage Parameters
- Configuring the Default Currency Code
- Configuring the Base Time Zone
- Configuring Case Own Flag Consideration
- Configuring Case Prefix
- Configuring the Display of Value in By Field Name/ID
- Configuring Case Due Date
- Configuring Case Near Due Date
- Configuring Organization Type
- Configuring Application Server
- Configuring Case Age Calculation
- Configuring Case Assignment Inheritance
- Configuring Case Correlation Owner
- Configuring Case Inheritance
- Configuring Case Risk Values
- Configuring Default Case Owner
- Configuring Case List Records Per Page Limit
- Configuring Default Case Search Created Date Lookback
- Configuring Default Event Search Created Date Lookback
- Configuring Default Suppression Administration Created Date Lookback
- Configuring Default Trusted Pairs Administration Created Date Lookback
- Configuring Default Trusted Pairs Transaction Date Lookback
- Configuring E-mail
- Configuring Mode of Transferring Alert Information
- Configuring Mode of Transferring Case Information
- Configuring Lock Time Period for Case Actions
- Configuring Include Historical Migrated Alerts
- Configuring View All Organization
- Exporting Cases
- Configuring OBIEE
- Configuring File Size
- Configuring Views

- Configuring ECM Security Function
- Configuring Customer Account Role
- DB configuration
- Configuring Required Action Comments
- Managing Additional Configurations
- Managing KYC Configurations
- Account Restriction
- Right to be Forgotten
- Data Redaction
- Exclude Case Type from Create Case
- Archiving/Unarchiving Cases
- Archiving/Unarchiving Events

14.1 Configuring the Client Logo Image

The client logo has a default blank image included in all Oracle Financial Services .jsp files. You must replace the blank image for both the Oracle Financial Services product and the Administration Tools with a .svg file that contains your firm's name or logo.

14.1.1 Logo Specification

The following lists the client logo specification:

- The logo name must be client_logo.svg
- Dimensions must be width: 137px and height: 18px
- File format must be Scalar Vector Graphic (SVG)

14.1.2 Placing a new Client Logo

To place a new client logo, follow these steps:

1. Take a backup of the existing client_logo.svg file from the <deployed area>/ojff/css/ images/ client_logo.svg directory.
2. Copy the customer logo to the <deployed area>/ojff/css/images directory (for example, <deployed area>/ojff/css/images/client_logo.svg).
3. Refresh the web browser after copying the image file in the web server.
4. Refresh the application server's work folder.

14.1.3 Removing a Client Logo

To remove a custom client logo, follow these steps:

1. Replace the client_logo.svg file from the backup location.
2. Refresh the web browser after copying the image file in the web server.
3. Refresh the application server's work folder.

14.1.4 Configuring Application Label Text

To modify the Application Label text along with Logo change, update the following entries in the Configuration table:

```
select * from aai_app_tl where v_app_id='OFS_NGECM' v_app_id='OFS_NGECM'
v_app_name='app name'
```

Here, the app_name is the customized Application Label. For example, Enterprise Case Management.

14.2 Accessing Manage Parameters

To access the Manage Parameters, follow these steps:

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

14.3 Configuring the Default Currency Code

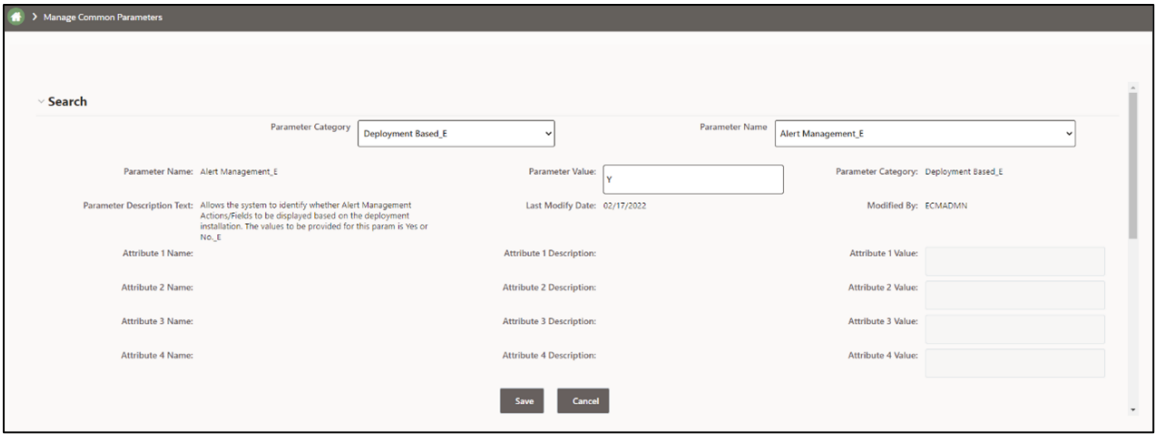
You can modify the default currency settings that display throughout the UI. The following section provides detailed instructions to modify the currency code.

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 83 illustrates the modified currency code as EUR.

Figure 83: Financials Tab-with Modified Currency Format



Perform the following steps from the back end:

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

   ```
   UPDATE AAI_FF_CONTROL_PROPERTIES SET V_CONTROL_SPECIFIC_11 = 'MMK' WHERE
   V_CONTROL_SPECIFIC_12 ='code' and V_CONTROL_SPECIFIC_11='USD';
   ```

3. Restart the servers and test the UI.

14.4 Configuring the Base Time Zone

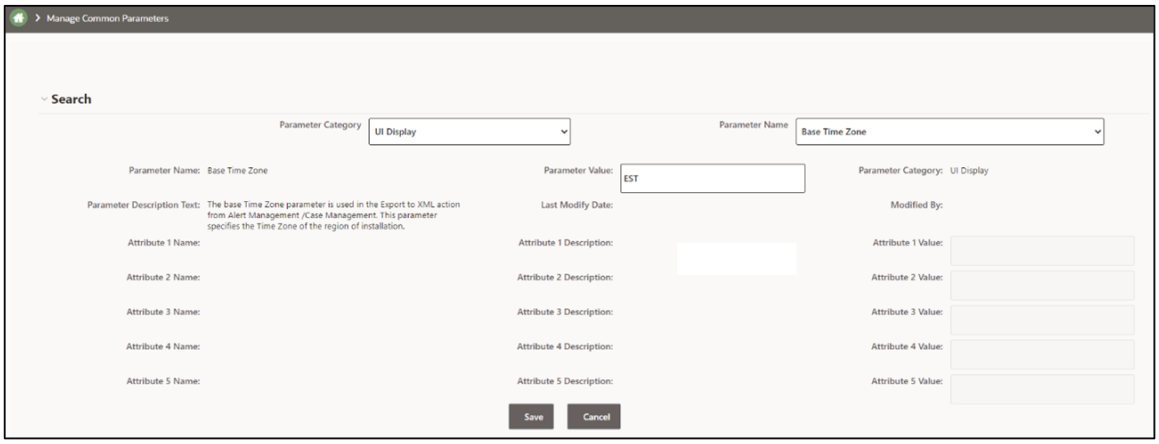
The Base Time Zone parameter is used in the Export to XML action from Case Management. You can modify the default Base Time Zone through the Manage Common Parameters screen as shown in Figure 84 .

14.4.1 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 84: 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.

14.5 Configuring Case Own Flag Consideration

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

The default value is Y.

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

1. Open the Manage Common Parameters screen.
2. Select **UI Display** from the Parameter Category drop-down list.

3. Select **Case Own Flag Consideration** from the Parameter Name drop-down list.
4. Edit the required parameter details and click Save. A confirmation dialog box appears with the message: *Would you like to Save these actions?*
5. Click **OK**. A dialog box appears with the message: *Update Operation Successful*.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.6 Configuring Case Prefix

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

To modify the Case Prefix parameter, follow these steps:

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

14.7 Configuring the Display of Value in By Field Name/ID

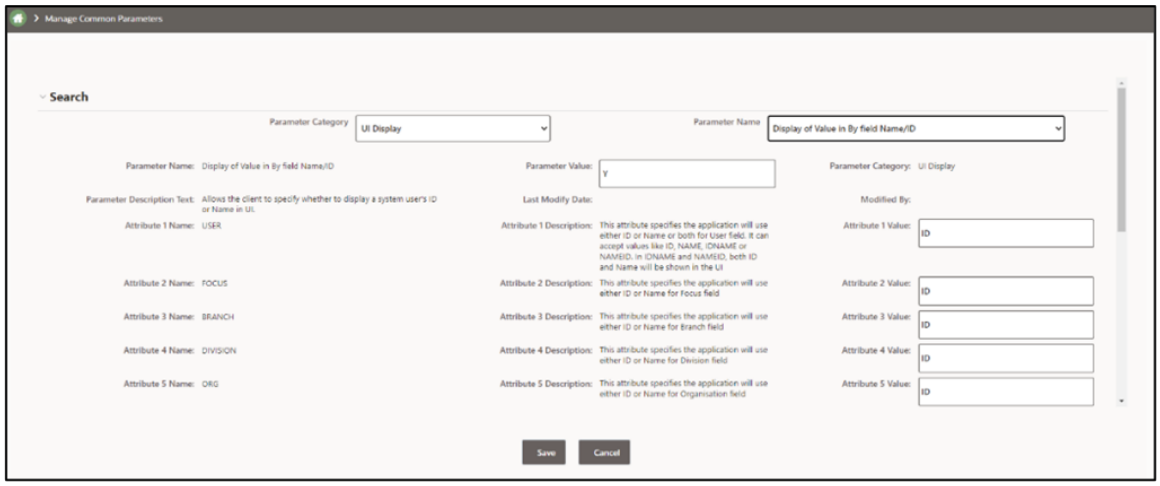
This configuration allows you to see either the ID or Name field for the User, Focus, Branch, Division, and Organization in the UI. This parameter specifies the client to specify the Name or ID value in the By field.

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.

   Figure 85 depicts the Display of Value in the By Field Name/ID page.

Figure 85: Display of Value in the By Field Name/ID



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

Table 49: Configuring Display of Value in By Field Name/ID Attributes

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

14.8 Configuring Case Due Date

Case Due Date is determined based on the configured data on the following three tables:

1. KDD_ACTION
2. KDD_CASE_TYPE_PARAM_CONFIG
3. KDD_INSTALL_PARAM

Scenario 1: Using KDD_ACTION

If the DFLT_DUE_DT_LM column value for the particular action in question (e.g., CREATE_CASE) is defined, the case due date is created based on it. And the process ignores the remaining two tables.

For example:

```
SELECT DFLT_DUE_DT_LM FROM KDD_ACTION ka;
```

The due date for the newly created case will be selected from the KDD_ACTION table's DFLT_DUE_DT_LM column.

Scenario 2: Using KDD_CASE_TYPE_PARAM_CONFIG

If the KDD_ACTION table does not have a preconfigured value for case due date, then it is determined based on the configurations done in the KDD_CASETYPE_PARAM_CONFIG for the specific Case Type and V_PARAM_CD - DUE_DT_LMT.

In the KDD_CASETYPE_PARAM_CONFIG table, define the Case Type and Due Date.

For example:

```
SELECT * FROM KDD_CASETYPE_PARAM_CONFIG kcpc;

V_PARAM_CD-DUE_DT_LMT

V_CASE_TYPE-AML_SURV

V_PARAM_VALUE-10
```

The AML_SURV Case Type has a due date of 10 days in the KDD_CASETYPE_PARAM_CONFIG table. You can change the case due date. In the KDD_ACTION table, clear the default due date, and configure the AML_SURV case type in the KDD_CASETYPE_PARAM_CONFIG table.

You can also configure different due dates for Case Types. For more information, see Configuring Different Due Dates for Case Types.

```
Scenario 3: Using KDD_INSTALL_PARAM
```

If both the KDD_ACTION and KDD_CASE_TYPE_PARAM_CONFIG tables do not contain any preconfigured value for case due date; Case due date is determined based on the KDD_INSTALL_PARAM table.

You can also configure the case due date via the UI.

To configure case due date via the UI, 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 (specify if calendar or business days will be used for due date calculation. Allowed values are C for Calendar days and B for Business days.):
   - Parameter Value = B
   - Attribute 1 Value = 30
5. Scroll down 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.

14.8.1 Setting Due Date of New Cases via Correlation Batch

You can set due dates of new cases via correlation batch.

To set due date via batch, follow these steps:

1. In the BD_Create_Case process of the Oracle_BD_EVENT_PROCESSING batch, add the BD_BATCH_CASE_DUEDATE_UPDATE Data Transformation (DT) task
2. Set the precedence of the task after `f_generatecaseid` and `f_insertcases`.

For more information, see Configuring Different Due Dates for Case Types.

14.9 Configuring Case Near Due Date

This section describes how to configure case near due date.

To configure case near due date, follow these steps:

1. Open the **Manage Common Parameters** screen.
2. Select **UI Display** from the Parameter Category drop-down list.
3. Select **Near Due Date** from the Parameter Name drop-down list.
4. Edit the required parameter details (specifies the Near Due days set for Alerts, Cases, Suppression Rules and Trusted Pairs. This parameter controls at which point the UI will provide a visual indicator that the due date is getting closer .The parameter value must be set to Y.):
   - Parameter Value = Y
   - Attribute 1 Value = 4
5. 5.Scroll down and click **Save**. A confirmation dialog box appears asking:

   Would you like to Save these actions?
6. 6.Click **OK**. A Confirmation dialog box appears with the message: Update Operation Successful.
7. 7.Click **OK**. The Manage Common Parameters page is displayed.

14.10 Configuring Organization Type

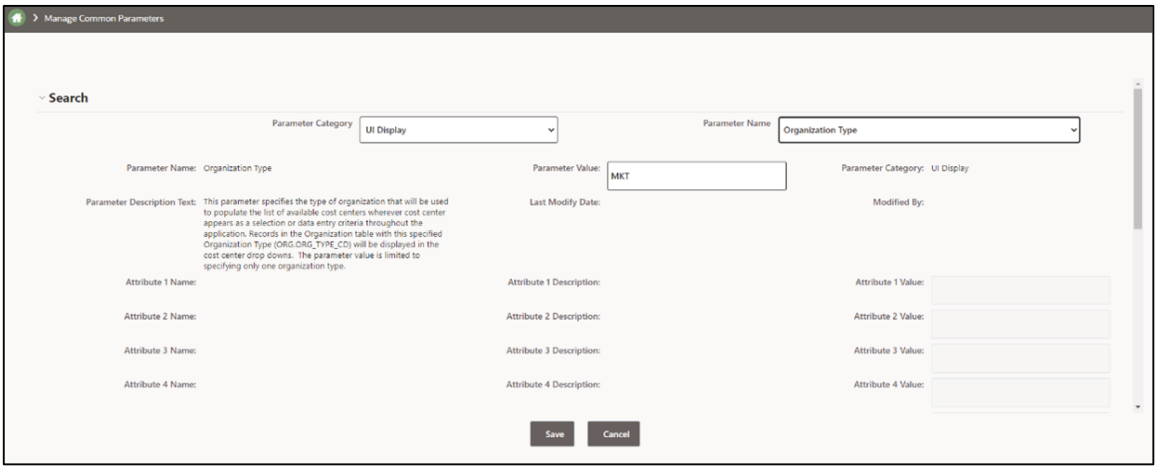
This parameter specifies the type of organization that is used to populate the list of available cost centers wherever the cost center appears as a selection or data entry criteria throughout the application.

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 as shown in Table 86 .

Figure 86: Organization Type



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.

14.11 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 50 describes the attributes to be configured for setting the application server.

Table 50: 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.

14.12 Configuring Case Age Calculation

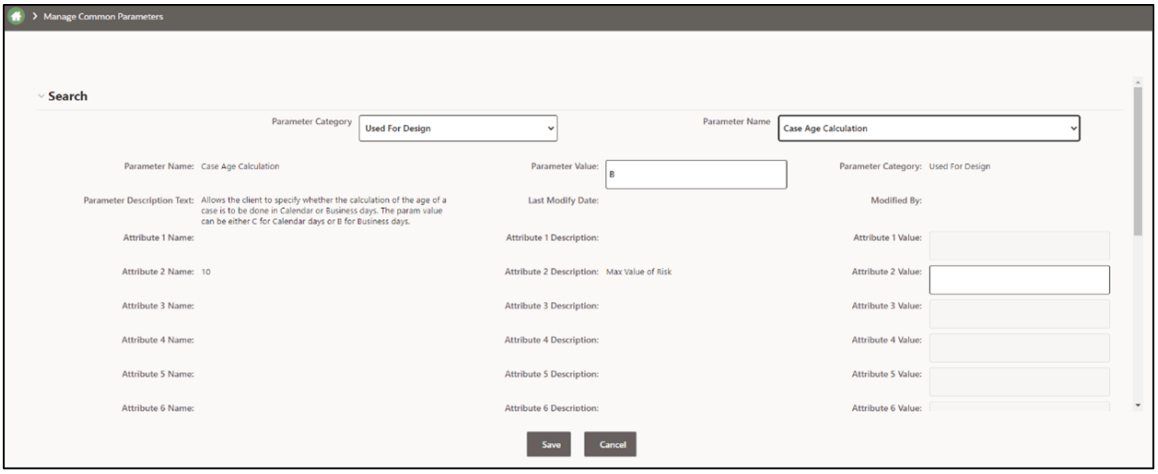
This parameter allows the client to specify whether the calculation of the age of a case is to be done in Calendar or Business days. The param value can be either C or B.

The default value is Business (B).

To modify the Case Age Calculation parameter, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Age Calculation** from the Parameter Name drop-down list as shown in Table 87 .

Figure 87: Case Age Calculation



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

14.13 Configuring Case Assignment Inheritance

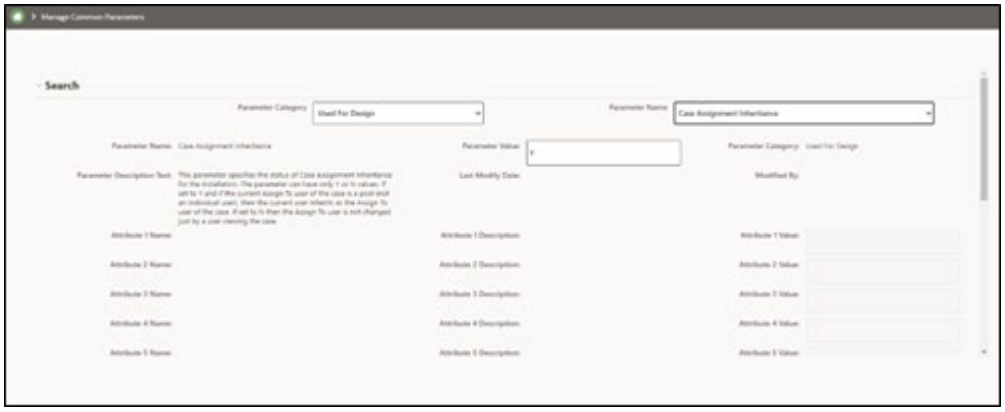
This parameter specifies the status of Case Assignment Inheritance for the installation. The parameter can have only Y or N values. If set to Y and if the current Assign To user of the case is a pool (not an individual user), then the current user inherits as the Assign To user of the case. If set to N, then the Assign To user is not changed just by a user viewing the case.

The default value is Y.

To modify the Case Assignment Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Assignment Inheritance** from the Parameter Name drop-down list as shown in Table 88 .

Figure 88: Case Assignment Inheritance



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

14.14 Configuring Case Correlation Owner

This parameter specifies the users or user pools who should be assigned as the Owner and Assign To users for cases created through correlation promotion. The users or user pools that need to be assigned as the Owner and Assign To users are identified from other attributes of this parameter based on the case type. Here every attribute specifies an owner for a Case Type Sub Type. Some of the Case Type Sub Type will be prepackaged.

Client can specify new case type sub type and default owner for the case type subtype. To add a new case type sub type, follow these steps:

1. If the Case Correlation Owner parameter has used up to attribute 4, then use the following query:

   ```
   update kdd_install_param set kdd_install_param.attr_5_cd='<Case Type Sub Type>' ,kdd_in- stall_param.attr_5_value_tx='<Owner>'
   ```

   where kdd_install_param.param_id=30 and kdd_install_param.param_nm='Case Correlation Owner 1'
2. If all the attributes have been filled then add one more case correlation owner Parameter. To add another Correlation parameter, follow these steps:
   a. Get maximum param ID of the kdd_install_param table by running the following query.

      ```
      select max (param_id) from kdd_install_param.

      Insert into kdd_install_param (param_id, param_nm, param_value_tx, param_cat_cd,param_desc_tx) values

      (< Max Param id > +1,'Case Correlation Owner 2','Y','Used for Design',
      ```

   b. This parameter specifies the users or user pools who should be assigned as the Owner and Assign To users for cases created through correlation promotion. The parameter value by default is kept as Y but can also be changed and the same is not validated. The users or user pools who need to be assigned as the Owner and Assign To users are identified from other attributes of this parameter based on the case type.

c. To add a new case type sub type and owner use the query mentioned in step 1 after replacing the filter clause with the new param ID and name.

To modify the Case Correlation Owner for an existing Case Type Sub Type, follow these steps:

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

Table 51 describes the DEF_OWNER attribute.

Table 51: Configuring Case Correlation Owner

Attribute	Description
DEF_OWNER	This attribute specifies the default Case owner. The attribute value can have only one user ID • Should be the same as of KDD_RE-VIEW_OWNER.OWNER_ID • Should have Case role and • Have access to all the security attributes defined in the Security Attribute Administration User Interface, if not the s would not be assigned to any user.

14.15 Configuring Case Inheritance

This parameter specifies the status of Case Inheritance for the installation. The parameter can have only Y or N values.

If set to Y, the case ownership changes for cases when in New or Reopened statuses based on the rules defined for case inheritance. If set to N, then ownership does not change when a user accesses the case.

If set to Y the system automatically assigns ownership of a case owned by pools (as long as not in a closed status) to the user who has selected to view the case. If set to N, case ownership is not inherited by a user just by viewing the case.

To modify the Case Inheritance parameter, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Case Inheritance** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message:

   Would you like to Save these actions?
5. Click **OK**. A dialog box appears with the message: Update Operation Successful.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.16 Configuring Case Risk Values

This parameter allows deployment level configuration of the minimum and maximum range of risk values during add and edit feature in Case related business tabs.

To modify the case risk value, follow these steps:

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

   Table 52 describes the Configuring Case Risk Values.

Table 52: Configuring Case Risk Values

Attribute	Description
Min Risk Value	Will define the minimum value of all the types of risks; will have a default value of -2.
Max Risk Value	Will define the maximum value of all the types of risks; will have a default value of 10.

14.17 Configuring Default Case Owner

Cases are assigned to users based on the case allocation rules set. For more information on configuring the Case Allocation rule, see the Configuring Case Allocation.

14.18 Configuring Case List Records Per Page Limit

In the case search list, the default Search page records per page count is 300. This can be customized based on your needs. To increase the limit to 500 or any other number, change the *maxPageSize* value in the `FCC_UI_MODULE_CONF` column to 500 or any other desired number.

14.19 Configuring Default Case Search Created Date Lookback

The Default Case Search Created Date Lookback parameter specifies the number of days (Date Range) between the Created From and Created To date fields in the Search Cases Screen. This parameter accepts only natural numbers.

To modify this parameter, 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 Case Search Created Date Lookback** from the Parameter Name drop-down list.
4. Edit the required parameter value 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.

14.20 Configuring Default Event Search Created Date Lookback

The Default Event Search Created Date Lookback parameter specifies the number of days (Date Range) between the Created From and Created To date fields in the Search Events Screen. This parameter accepts only natural numbers.

To modify this parameter, 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 Event Search Created Date Lookback from the Parameter Name drop-down list.
4. Edit the required parameter value 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.

14.21 Configuring Default Suppression Administration Created Date Lookback

The Default Suppression Administration Created Date Lookback parameter specifies the number of days (Date Range) between the Created From and Created To date fields in the Suppression Administration Screen. This parameter accepts only natural numbers.

To modify this parameter, 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 Suppression Administration Created Date Lookback** from the Parameter Name drop-down list.
4. Edit the required parameter value 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.

14.22 Configuring Default Trusted Pairs Administration Created Date Lookback

The Default Trusted Pairs Administration Created Date Lookback parameter specifies the number of days (Date Range) between the Created From and Created To date fields in the Trusted Pairs Administration Screen. This parameter accepts only natural numbers.

To modify this parameter, 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 Trusted Pairs Administration Created Date Lookback from the Parameter Name drop-down list.
4. Edit the required parameter value 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.

14.23 Configuring Default Trusted Pairs Transaction Date Lookback

The Default Trusted Pairs Transaction Date Lookback parameter specifies the number of days (Date Range) between the Created From and Created To date fields in the Trusted Pairs Administration Details Screen. This parameter accepts only natural numbers.

To modify this parameter, 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 Trusted Pairs Transaction Date Lookback** from the Parameter Name drop-down list.
4. Edit the required parameter value 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.

14.24 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 as shown in Figure 89 .

Figure 89: E-mail Parameter



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

Table 53: 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 the 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 the `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_RE- VIEW_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 for the Send Email action for the Cases selected. Text can be edited before sending an email and is what will appear in the email received by the respondent.
MAIL_FOOTER	This attribute specifies optional footer details which can be appended to the E-mail.
MAIL_ATTACH_LIMIT	This attribute specifies the attachment size limit. The value is given in MB.
DISPLAY_ACTIONS_TAKEN	This attribute specifies whether to display the 'Actions Taken' in the attached HTML or not.
HTML_REPORT_IN_BODY	This attribute specifies for a single case, whether the HTML report has to appear in the mail body or as an attachment.
DEF_ACTION_TAKER	This attribute specifies the default action taker for the received response if the system cannot identify the Response Sender as a valid User.
DEF_RFI_SUBJECT	This attribute specifies the default subject for the Send RFI action for the Cases selected. Text can be edited before sending an email and is what will appear in the email received by the respondent.

14.24.1 Configuring Token/Non-Token Based RFI

RFI access token validation allows RFI respondents to access the questionnaire without requiring administrators to create a user ID. When an RFI is sent to an individual, the user will receive a token-based link to access the RFI Questionnaire. On clicking this token-based Questionnaire link, an email will be sent to the user. This email will contain a unique captcha that the user will provide when logging in. This allows the ECM application to know specifically who the respondent is without requiring user log in.

To configure token based RFI, follow these steps:

1. Navigate to the CONFIGURATION table in the Config schema.
2. Update the RFI_TOKEN_VALIDITY parameter to provide the amount of time the RFI Token should remain valid. The value for this parameter must be provided in minutes. The default value is 60.
3. Configure the Captcha Email which respondents will receive by updating the following parameters:
   - QTNR_CAPTCHA_SENDER_MAIL_ID: Configure the RFI Captcha Sender Mail ID. For example: rfi@oracle.com
   - QTNR_CAPTCHA_MAIL_SUBJECT: Configure the RFI Captcha Mail Subject line. For example, RFI Unique Code.
   - QTNR_CAPTCHA_MAIL_BODY_TXT: Configure the RFI Captcha Mail Body text. For example: Please Enter this code to view the RFI page.
   - QTNR_CAPTCHA_MAIL_BODY_SENDER_NAME: Configure the RFI Captcha Sender Name, such as Administrator.
4. Service Authentication is done through the service account in the Token Enabled RFI screen. Configure the service account by updating the OFSAA_SRVC_ACC parameter. The default value is SYSADMN.

NOTE	Oracle recommends creating a "SMS Auth Only" user from the User Maintenance window for the service account rather than using SYSADMN.

ATTENTION	For Weblogic and Websphere environments, the configurations found in the OFSAAI Administration Guide must be completed for REST Services Authorization for the respective server. Refer to Section: 12.10.1 Configuring WebLogic for REST Services Authorization and Section: 12.11.1 Configuring WebSphere for REST Services Authorization.

To configure non-token based RFI, apply the Patch - 35667722 and then follow the configuration steps.

14.24.2 Configuring SMTP- Based Email/RFI

SMTP Configuration allows emails and RFIs to be sent using a Public Domain Facing SMTP server which has been configured with a user name and password.

To configure SMTP-based RFI, follow these steps:

1. Navigate to the KDD_INSTALL_PARAM table.

2. Update the PARAM_ID 3021 to store the SMTP host, username, password, port and sender mail ID.
   - If the PARAM_VALUE_TX flag is set to Y, provide correct values for the following attributes:
     - SMTP host
     - SMTP Username
     - SMTP password
     - SMTP port
   - SMTP_SENDR_ENABLED - This attribute specifies whether the system should use a pre-defined email address or the email address of the current logged in user as the default sender address (KDD_REVIEW_OWNER) for email action. Y sets the email of the sender as specified in SMTP_SENDR_EMAIL attribute as the default. If set to N, it will follow the existing configurations and set the Sender Mail ID as per param_id 8 configurations.
   - SMTP_PASSWD (ATTR_3_VALUE_TX) attribute can be encrypted from the Configuration of Web Service screen and automatically populated in the KDD_INSTALL_PARAM table.

14.25 Configuring Mode of Transferring Alert Information

This parameter specifies the mode in which business data from an alert to a case is transferred during Promote to Case or Link actions. The parameter value can have only S or A value. Synchronous (S) restricts the user from working on the alert or case until the data transfer action is complete. Asynchronous (A) allows the user to continue to work on the alert or case, while the data transfer is being carried out in the background.

The default value is synchronous (S).

To modify the Mode of Transferring Alert Information, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for design** from the Parameter Category drop-down list.
3. Select **Mode of Transferring Alert Information** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message:

   Would you like to Save these actions?
5. Click **OK**. A dialog box appears with the message: Update Operation Successful.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.26 Configuring Mode of Transferring Case Information

This parameter specifies the mode in which case information is transferred during Merge Action and is applicable for implementations that have installed Oracle Financial Services Enterprise Case Management. The parameter value can have only S or A value. S (Synchronous) restricts the user from working on the case until the data transfer action is complete. An Asynchronous allows the user to continue to work on the case, while the data transfer is being carried out in the background.

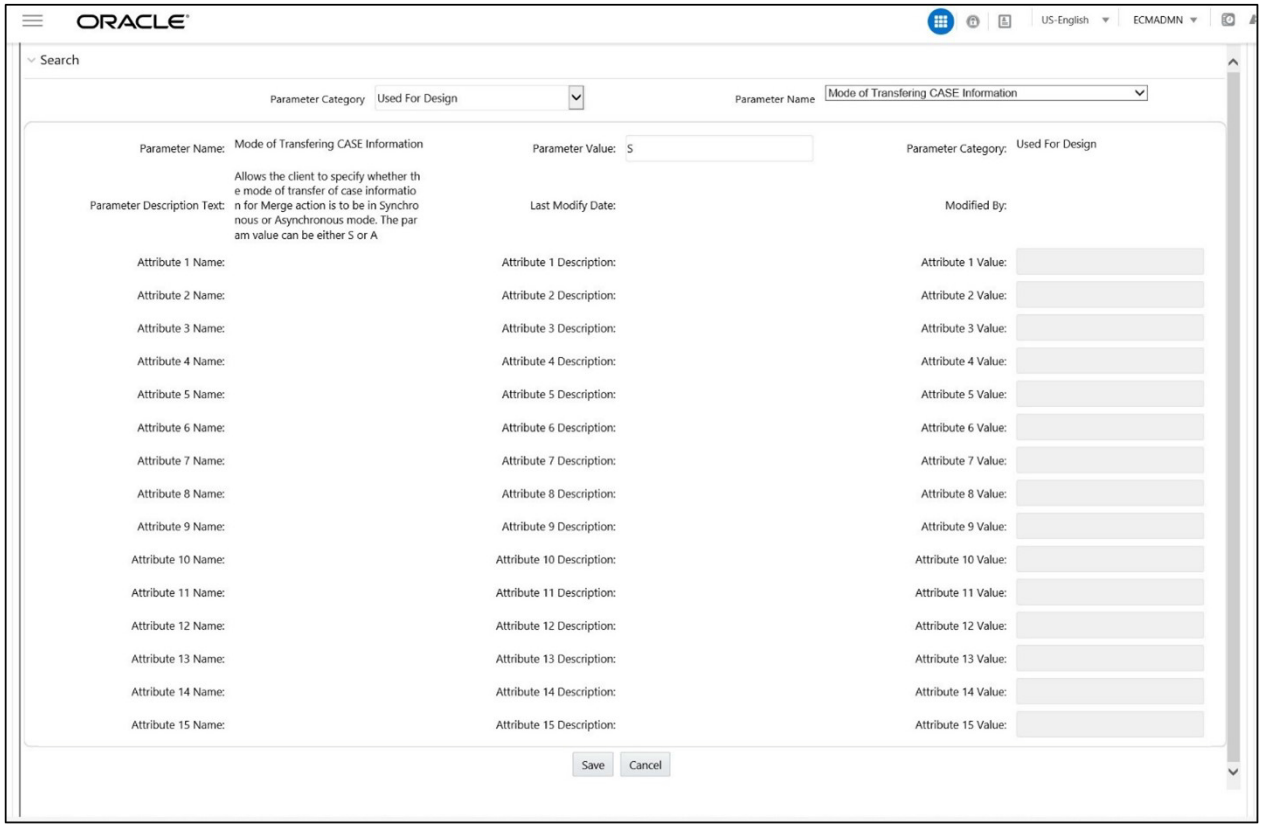
The default value is synchronous (S).

To modify the Mode of Transferring Case Information, follow these steps:

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

2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Mode of Transferring Case Information** from the Parameter Name drop-down list as shown in Figure 90 .

Figure 90: Mode of Transferring Case Information



4. Edit the required parameter details and click Save. A confirmation dialog box appears with the message:

   Would you like to Save these actions?

5. Click **OK**. A dialog box appears with the message: Update Operation Successful.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.27 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 to 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.

14.28 Configuring Include Historical Migrated Alerts

This parameter specifies whether the Include Historical Migrated Alerts check box should be displayed in the UIs (all **Relationship tabs**, **Research**, and **Search Events**). The parameter can have only Y or N values. Select **Include Historical Migrated Alerts** if you want to view migrated events. If Include Historical Migrated Alerts set to Y, then the Include Historical Migrated Alerts check box is displayed on the **Search Event** window.

The Attribute 1 (Is Checked) parameter should have only Y or N values. If the value is Y, then the checkbox is checked by default on UIs.

To modify the Include Historical Migrated Alerts parameter, follow these steps:

1. Open the Manage Common Parameters window.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **Include Historical Migrated Alerts** from the Parameter Name drop-down list as shown in Figure 91 .

Figure 91: Include Historical Migrated Alerts



4. Edit the required parameter details and click **Save**. A confirmation dialog box appears with the message:

   Would you like to Save these actions?

5. Click **OK**. A dialog box appears with the message: Update Operation Successful.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.29 Configuring View All Organization

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

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

To disable View All Organization, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **View All Organization** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking:

   Would you like to Save these actions?
5. Click **OK**. A Confirmation dialog box appears with the message: Update Operation Successful.
6. Click **OK**. The Manage Common Parameters page is displayed.

14.30 Exporting Cases

For all roles, ECM enables you to export data in Excel and CSV formats where you can then review and edit the data as necessary. The Excel function exports all records available on the list.

1. Execute the following query in Atomic Schema- select t.*,t.rowid from fcc_ui_module_conf t where t.v_ui_module_id = 'CM_CS_CASELIST_GRID'
2. In the column V_MODULE_PROP, find the following configuration - "noOfRowsToExport":100,
3. Modify the number 100 to the number required and commit.

14.31 Configuring OBIEE

This parameter specifies the OBIEE Server Application context and URL parameters. To configure OBIEE, follow these steps:

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select **OBIEE** from the Parameter Name drop-down list.
4. Edit the required parameter details and click **Save**. A confirmation dialog box appears asking:

   Would you like to Save these actions?
5. Click **OK**. A Confirmation dialog box appears with the message: Update Operation Successful.

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

14.32 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

   Update from:

   <PROPERTY NAME="MAXFILESIZE" VALUE="1024000"/>

   to:

   <PROPERTY NAME="MAXFILESIZE" VALUE="<desired value in bytes up to 10MB>"/>
2. 2.Recreate the ExeWebservices ear file and redeploy it.
3. 3.Restart the web application server.

The size that is allowed to be attached while performing document attachment action should be configured in the Configuration table of OFSSAAI configuration schema in its PARAMVALUE column where PARAMNAME is DOCUMENT_MAX_SIZE. It is the Maximum document file size (in bytes).

14.33 Configuring Views

Views help you to quickly view search results based on pre-defined search queries.

14.33.1 Adding Views

To add views, follow these steps:

1. Make an entry in the `KDD_QUEUE_MASTER` table.

   Table 54 describes the `KDD_QUEUE_MASTER` table.

   Table 54: KDD_QUEUE_MASTER table

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

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

Table 55 describes the KDD_QUEUE_FILTER table.

Table 55: KDD_QUEUE_FILTER table

QUEUE_SEQ_ID	ATTRBT_ID	ATTRBT_VAL_TX
Unique sequence ID	Unique Attribute ID. ATTRBT_ID will be referred from KDD_CASEATTRBT_MASTER	This Attribute value is the actual value used for the attribute of filter. In this, you can give hardcoded values (for example, put a filter condition on the status attribute for the cases which are in New status). The possible value for this is, NW. You can also specify session attributes for your filter. The session attributes are enclosed in curly brackets {}. For example: {userSeqId}, {userPool} You can define the SYSDATE value for the filter. Date filter requires the following two inputs: • From Date • To Date For example: #NS#, #SYSDATE# You should specify the date values in enclosed # Use #NS# to mention the date filter as blank.

3. Map Queue in the KDD_QUEUE_ROLE_MAP table.

   Table 56 describes the KDD_QUEUE_ROLE_MAP table.

Table 56: KDD_QUEUE_ROLE_MAP table

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

14.33.2 Modifying Views

Following are the various modifications for views:

- Modify An Existing View Query

  To modify the underlying filters for a view, changes are to be done in the `KDD_QUEUE_ FILTER` table column.

- Modifying View-Role Mapping

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

- Modifying the Display Name of the View

  To change the display name for a particular view, changes have to be done in the `KDD_QUEUE_MASTER.QUEUE_DISPLAY_NM` column.

14.33.3 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_MAPwhere QUEUE_SEQ_ID = <View Sequence Id>; COMMIT;

Delete KDD_QUEUE_FILTER where QUEUE_SEQ_ID = <View Sequence Id>; Delete
KDD_- QUEUE_ROLE_MAPwhere QUEUE_SEQ_ID = <View Sequence Id>; COMMIT;
```

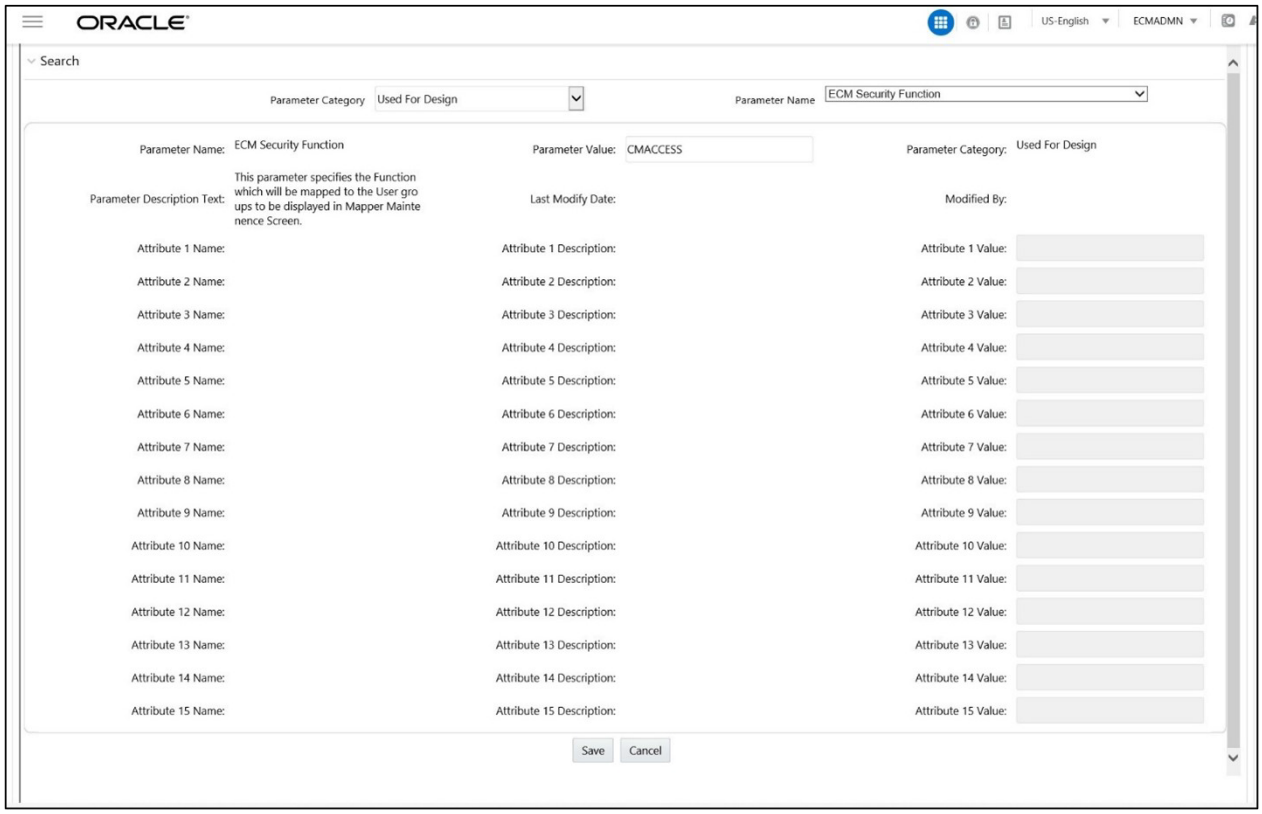
14.34 Configuring ECM Security Function

The user groups listed in the Mapper Maintenance screen can be configured/controlled by the associated function. By default, CMACCESS function code is currently configured out of the box.

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 the **ECM Security Function** from the Parameter Name drop-down list as shown in Figure 92 .

Figure 92: 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.

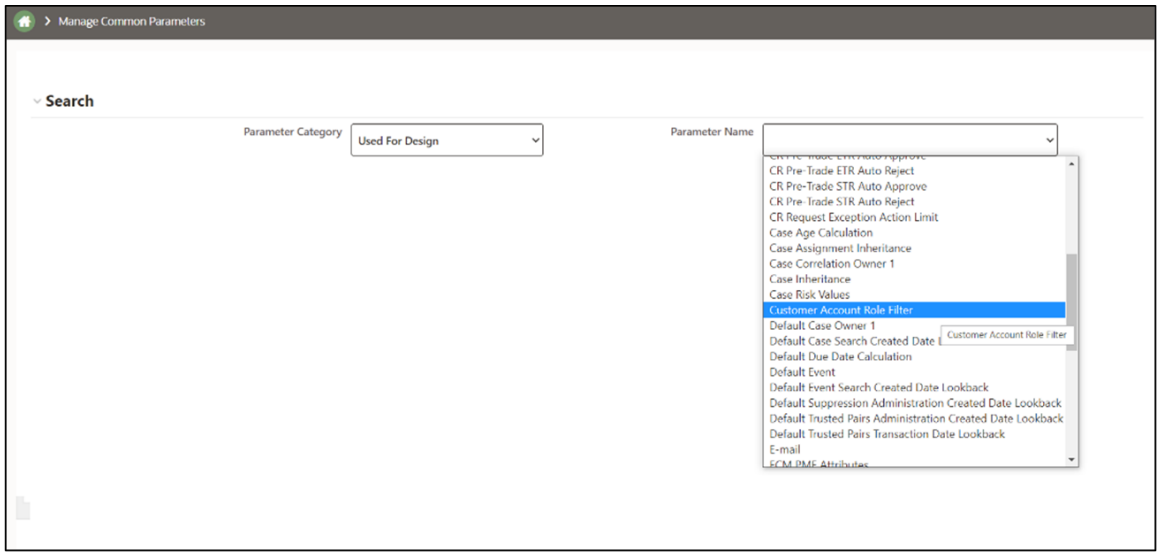
14.35 Configuring Customer Account Role

The Customer Account Role filter provides the option to reduce the number of individuals to be investigated when a case is created on a customer. This is achieved by introducing a parameter that allows clients to define which roles they want used to decide which accounts to be included in the case. Customer account will be filtered while adding customer based on the account role filter defined in the Manage Common parameter screen. Then, when a customer is added to a case (either through PTC or search/add) only the accounts with those roles are added to the account table. This parameter can accept multiple roles.

To configure the Customer Account Roles Filter, follow these steps:

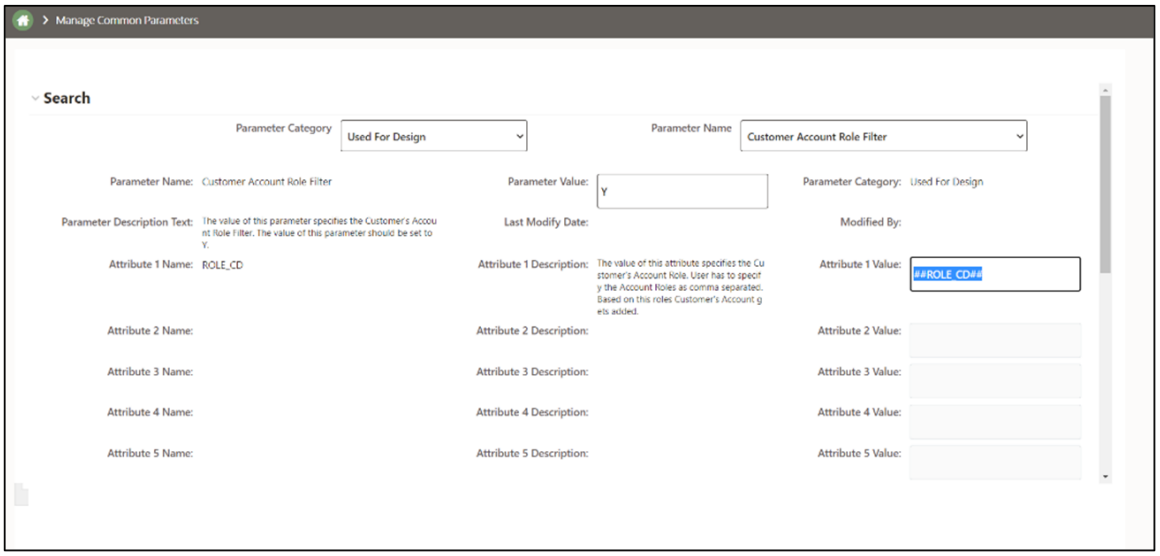
1. Navigate to **Case Management Configuration** and select the **Manage Common Parameters** option.
2. Open the **Manage Common Parameters** screen.
3. Select **Used For Design** from the Parameter Category drop-down list.
4. Select **Customer Account Role Filter** from the Parameter Name drop-down list as shown in Figure 97 .

Figure 93: Manage Common Parameters Screen



5. On the **Manage Common Parameters** page, enter roles in the **Attribute 1 Value** field, and click **Save**. The Roles entered in the Attribute 1 Value field specify the Customer's Account Role. The Account Roles must be specified as comma separated. The Customer's Account is added based on these roles as shown in Figure 94 .

Figure 94: Set Customer Account Role Filter



6. Scroll down and click **Save**.
7. A pop-up *Would you like to Save these actions* appears, click **Save**.
8. A pop-up *Update Operation Successful* appears, click **Save**.

The accounts associated with the Customer are added to the account table based on the roles defined.

14.36 DB configuration

To configure the Customer Account Roles Filter, follow these steps:

The `KDD_INSTALL_PARAM` table must be configured in the database using Parameter Name and Parameter ID with the following attributes in the table.

- Enter the Parameter Name as: Customer-Account Role Filter
- Enter the Parameter ID as: 3015

14.37 Configuring Required Action Comments

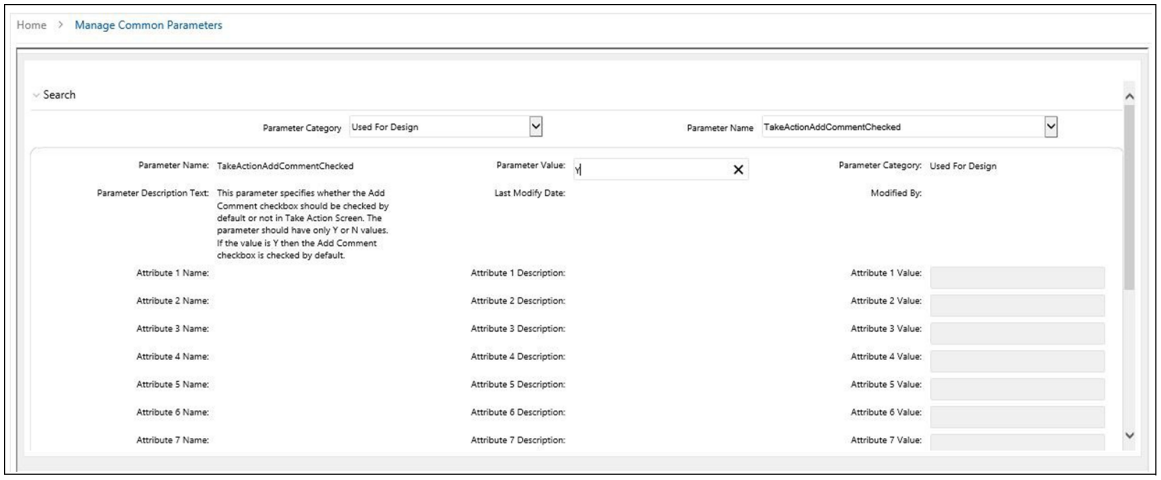
The application can be configured to specify whether the Add Comment checkbox is selected by default on the Take Action window in Enterprise Case Management. The parameter values can be Y or N. If the value is Y, then the Add Comment checkbox is checked by default.

The default value of this parameter is Y.

To configure the Add Comments check-box, follow these steps:

1. Open the Manage Common Parameters window.
2. Select **Used For Design** from the Parameter Category drop-down list.
3. Select **TakeActionAddCommentChecked** from the **Parameter Name** drop-down list as shown in Figure 95 .

Figure 95: Configuring Required Action Comments



4. Edit the Parameter Value and click **Save**. A confirmation dialog box is displayed with a message:

   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.

14.38 Managing Additional Configurations

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

14.38.1 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.

> **NOTE** Extension types are case sensitive. For example, files saved with a .png and a .PNG extension, the .PNG file fails when attaching to the case if it is configured for "png" only.

14.39 Managing KYC Configurations

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

- **Configuring KYC Close Service Parameters (KYC Batch case)**: Refer section Updating the URL for the KYC Close Service under Configurations in the ECM UI in the KYC Admin guide.
- **Configuring KYC Customer Dashboard Parameters (KYC Batch Case)**: Refer section Updating the BD Application URL for the KYC Customer Dashboard under Configurations in the ECM UI in the KYC Admin guide.
- **Configuring CommonGatewayService Parameters**: Refer section Updating the User Name and Password for the Common Gateway Service under Configurations in the ECM UI in the KYC Admin guide.

- **Configuring createJSONService Parameters**: Refer section Updating the User Name and Password for the Create JSON Service under Configurations in the ECM UI in the KYC Admin guide.
- **Configuring KYC Risk Score UI Service Parameters (Onboarding KYC Case)**: Refer section Updating the User Name and Password for the KYC Risk Score UI Service under Configurations in the ECM UI in the KYC Admin guide.
- **Configuring KYC Close Service Parameters (Onboarding KYC Case)**: Refer section Updating the User Name and Password for the JSON To Table Service under Configurations in the ECM UI in the KYC Admin guide.

14.40 Account Restriction

The account restrictions are added in the KDD_CODE_SET_TRNLN table for the

code_set='CMAccountRestriction'.

Also add the appropriate record to the KDD_CODE_SET_TRNLN_TL table as well for all the locale to be supported.

14.41 Right to be Forgotten

This section provides information about the Right to be Forgotten feature used in the OFSAA Data Foundation applications.

Topics:

- Introduction to Right to be Forgotten
- Implementation of Right to be Forgotten by OFSAA

14.41.1 Introduction to Right to be Forgotten

Right to be Forgotten is the task of dropping PII (Personally Identifiable Information) of a Data Subject for the given Party. The financial institution can drop PII for those Data Subjects who have exercised the Right to be Forgotten functionality.

The Data Subjects may have made significant financial transactions, and (or) financial information may be required for regulatory or compliance reporting. Deleting the complete record that consists of PII may lead to issues in data reconciliation. In OFSAA, the PII data is replaced with randomized values, and therefore, the complete Data Subject record is retained. As a result, financial information is retained; however, the associated Party PII is removed permanently.

14.41.2 Implementation of Right to be Forgotten by OFSAA

To implement Right to be Forgotten, follow these steps:

1. Use the FSI_PARTY_RIGHT_TO_FORGET table to collect the input list of Party IDs for which PII must be removed from the system. The financial institution must source this Party ID list into the

FSI_PARTY_RIGHT_TO_FORGET table, and then call the batch (<<INFODOM>>_RightToForget) or schedule it.

NOTE

- For the sample query, see the Sample Query for the FSI_PARTY_RIGHT_TO_FORGET Table section.
- If Redaction is already performed and if you want to implement Right to Forget, you must revert the redaction policy. For more information, see the *Disabling Data Redaction* section in Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.

2. Use the AAI table AAI_DRF_FUNCTION_COLUMN_MAP to store the PII attribute list. During the Right to Forget batch execution, the AAI_DRF_FUNCTION_COLUMN_MAP table is referred to as randomize the PII values. See the *Data Redaction* section in Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.
   a. Use the AAI table AAI_DRF_QUERY_METADATA to store the query metadata, which is used during the <<INFODOM>>_RightToForget batch execution. This is the query metadata table that can lead to the following two types of queries:
      i. When the table consists of Party Identifier as an attribute, a simple record is required in the metadata query table.

         For example:

         ```
         Select v_party_id from Dim_Party where v_party_id='10'
         ```

      ii. When the table does not consist of Party Identifier as an attribute, an interrelated set of records is required in the metadata query table AAI_DRF_QUERY_METADATA. Compose these set of records in a systematic way such that, for the selected Party Identifier, the table join procedure can be performed and traversed to reach the required PII attribute.

      iii. To see more information about the table in the above image, see the Table Definition for AAI_DRF_QUERY_METADATA section.

         For example:

         DIM_CLAIM table does not consist of N_CLAIM_SKEY (N_CLAIM_SKEY is the required Primary Key for the PII Attribute N_DRIVER_SKEY). Therefore, perform the table join procedure similar to the following query:

         ```
         Dim_driver.n_driver_skey from dim_driver dim_driver,
         fct_driver_details fct_driver_details,
         Fct_Claim_Driver_Vehicle_Map Fct_Claim_Driver_Vehicle_Map,
         Dim_Claim Dim_Claim where
         dim_driver.n_driver_skey=fct_driver_details.n_driver_skey and
         fct_driver_details.n_driver_skey=Fct_Claim_Driver_Vehicle_Map.n_dr
         iver_skey and
         Fct_Claim_Driver_Vehicle_Map.n_claim_skey=Dim_Claim.n_claim_skey
         and v_claim_id='GDPR'
         ```

In the preceding scenario, DIM_CLAIM.N_CLAIM_SKEY is a Number Datatype.

NOTE

- To arrive at the above-mentioned query, see the Steps to Perform the Table Join Procedure section.
- For a pictorial representation of the above query, see the Pictorial Representation of Query Formed from the AAI_DRF_QUERY_METADATA Table section.
- For more sample queries generated using the query metadata table, see Sample Queries Using the AAI_DRF_QUERY_METADATA Table section.

iv. You must arrive at the SKey or equivalent column in the table, which consists of the required PII attributes. Then the <<INFODOM>>_RightToForget batch uses this key to filter records (For example DIM_DRIVER) and randomize all the PIIs listed in the AAI_DRF_FUNCTION_COLUMN_MAP for that table.

3. Now, PII attributes can be queried and the values are randomized.

14.42 Data Redaction

Oracle Financial Services Analytical Application Infrastructure (OFSAAI) is enhanced to enable masking of sensitive data and Personal Identification Information (PII) to adhere to Regulations and Privacy Policies. Oracle Data Redaction provides selective, on-the-fly redaction of sensitive data in database query results prior to display by applications so that unauthorized users cannot view the sensitive data. The stored data remains unaltered, while displayed data is transformed to a pattern that does not contain any identifiable information.

For more information, see Oracle Financial Services Advanced Analytical Applications Infrastructure Administration and Configuration Guide Release 8.1.x.

NOTE

- The Redacted user must not have the Edit option in the UI
- To display the default value in the UI, configure the AAI_FF_FORM_CONTROLS_B table
- If you do not have data redact function rights and try to update any value in PII data, the application updates all redacted column values to null which leads to data loss.

Topics:

- Configuring Redaction for FCC Grids
- Redaction on Research UI Screen

14.42.1 Configuring Redaction for FCC Grids

Redaction can be configured for FCC grids that are configured using the FCC UI MODULE CONF table. The V MODULE PROP column must be configured under the columnProperties section.

The following is an example for Related Party grid in Customer tab (see the highlighted attributes):

```
"key": "customer_name",
"locale_code":"RENDERER.CM_RP_CUST_NAME",
"align": "left",
```

```
"headerAlign": "left",
"width": "0.13",
"dataType": "string",
"draggable":true,
"resizable":true,
"sortable":true,
"readOnly":true,
"visible": true,
"addToColMenu": true,
"isRedactedColumn": true,
"redactedValueToDisplay": "********"
```

For Date, Integer, and Float fields, regardless of the value provided for the redactedValueToDisplay attribute, the field will appear as blank.

14.42.2 Redaction on Research UI Screen

A new table FCC_NATIVE_REDACTION_CONFIG has been introduced in Atomic schema. Based on your requirement you can set the value of redaction under the V_REDACTED_VALUE_TO_DISPLAY column.

For the date fields irrespective of whatever value configured in the V_REDACTED_VALUE_TO_DISPLAY column it will be displayed as blank if redacted.

Redaction for Research Customer Overview is provided for now. You can also configure redaction for Account and External Entity. Refer to the FCC_NATIVE_REDACTION_CONFIG table for more information. Additionally you can also see the *Redaction_Account_External Entity_Info* spreadsheet in MOS.

14.43 Configuring Sanctions Server Details for L2 Feedback

If your environment is integrated with either Oracle Financial Services Transaction Filtering or Customer Screening application, you can configure the Sanctions Server information as shown in Figure 96 .

Figure 96: Sanctions Server Details page



To configure Transaction Filtering server details, follow these steps:

1. Enter the Sanctions URL for Attribute 1 Value.
2. Enter the Sanctions User ID for Attribute 2 Value.
3. For Attribute 3 Values, navigate to Configuration of Web Service, then enter the password for 'Enter password for TF SANC application URL' and click **Encrypt** as shown in Figure 97 .

Figure 97: Configuration of Web Service page



14.44 Exclude Case Type from Create Case

To exclude any Case Type from the Create Case drop-down add those Case Types Code (CASE_TYPE_CD) entries in the ATTR_11_VALUE_TX column of the KDD_INSTALL_PARAM table with param_id=3023.

You can also exclude the unwanted case types from the Create Case drop-down through the UI.

To exclude Case Type from the Create Case screen, follow these steps:

1. Open the **Manage Common Parameters** screen.
2. Select **Used for Design** from the **Parameter Category** drop-down list.
3. Select **Case Type Exclusion in the Create Case dropdown** from the **Parameter Name** drop-down list.
4. Edit the required parameter details as:

   Parameter Value = Y

   Attribute 11 Value = Add the case types which needs to be excluded from the Create Case drop-down list. For example: AML_CA, AML_DD.
5. 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.

14.45 Archiving/Unarchiving Cases

You can archive old-closed cases in order to improve performance. This Archived Cases page displays only the closed cases. It helps you in loading the search result quicker. However, you cannot archive old business data. You can also bring back the archived cases into production whenever required. All relationship tabs will display archived, and non-archived data.

Status and Non-Status changing actions can be performed in Archived Cases. However, it is not advised to do so.

ATTENTION

- Archived Cases are available under the Archived Case menu. To view the Archived Cases menu, the user must be mapped with the CMARCSRCH function. For more information, see Managing User Administration and Security Configuration.
- The Archival utility must only be used for archiving the old-closed cases.

There are three main archival tables:

- FCC_ARC_METADATA (Table 57)
- FCC_ARC_RESULTS (Table 58)
- FCC_ARCHIVE_AUDIT_LOG (Table 59)

Table 57: FCC_ARC_METADATA

Column Name	Description	Sample
V_APP_ID*	Is used to describe the application name.	OFS_NGECM

Table 57: FCC_ARC_METADATA

Column Name	Description	Sample
V_TABLE_NAME*	Refers the object, which need to be archived and compressed.	KDD_CASES
V_SCHEMA_NAME	Describes the schema name.	BECS_ATOMIC8124
V_COL_COND	Condition on which data needs to be filtered to be Archived. Multiple "OR" conditions can be defined on the same table.	STATUS_CD = 'CCNSAR' and created_tS<= TO_DATE('03/06/2023','DD/MM/YYYY')
N_PARALLEL_DEGREE	Database parallel degree applied in run time for better performance.	16
V_CHILD_TABLE_FLAG	Defaulted to N, When set to N - only FK's are considered else FK's+ User defined child metadata will also be picked.	N
V_ROLL_BACK	Defaulted to N, when set to 'Y', Archival will be disabled and table and all dependents will get to normal state.	Y
N_RETENTION_PERIOD	This value indicates the data that needs to be compressed automatically if not accessed/ modified for "defined" number of days.	

* denotes mandatory columns which must be filled in.

Table 58: FCC_ARC_RESULTS

Column Name	Description	Sample
N_SEQ_ID	Generates unique sequence for the insertion.	1000
V_APP_ID*	Is used to describe the application name.	OFS_NGECM
V_TABLE_NAME*	Refers the object, which need to be archived and compressed.	KDD_CASES
V_SCHEMA_NAME	Describes the schema name.	BECS_ATOMIC8124
V_COL_COND	Condition on which data has been be filtered to be Archived. This value is inherited from the Metadata table - FCC_ARC_METADATA.	STATUS_CD = 'CCNSAR' and created_tS<= TO_DATE('03/06/2023','DD/MM/YYYY')

Table 58: FCC_ARC_RESULTS

Column Name	Description	Sample
V_AFTER_ARC_CNT	Indicates the total record count after defined table is 'Archived'.	76
V_BEFORE_ARC_CNT	Indicates the total record count before defined table is 'Archived'.	95
T_TIMESTAMP	Used to capture the run time record insert into the table.	22-MAY-23 12.00.00.000000 AM
V_COMMENTS	Displays information about the performed action.	KDD_CASES- IS PARENT TABLE
V_CHILD_TABLE_NAME	Displays the child table name (both from DB derived FK's or metadata defined in FCC_ARC_CHILD_METADATA).	
V_ARCH_STATUS	Displays whether archival state is ENABALED OR DISABLEDCOMPLETED.	
N_RETENTION_PERIOD	This value is inherited from FCC_ARC_METADATA - N_RETENTION_PERIOD column.	

* denotes mandatory columns which must be filled in.

Table 59: FCC_ARCHIVE_AUDIT_LOG

Column Name	Description	Sample
N_RUN_ID	A unique run ID for the run.	
V_ACTIVITY	"Exception Encountered"	
V_ACTIVITY_TIME	Holds action performed time stamp.	
V_ACTIVITY_STATUS	Defines status of the current activity.	
V_ERROR_MSG	Holds ORA errors.	
V_OBJECT	Provides information on which process (Chunk process or Chunk re-process)	

Sample Statement for Archival:

```
select * from kdd_cases where STATUS_CD = 'CCNSAR'  and created_tS<=
TO_DATE('03/06/2023','DD/MM/YYYY')
```

Configure the FCC_ARC_METADATA table in Atomic Schema and run the below utility with arguments given in the FCC_ARC_METADATA table to archive cases in KDD_CASES table:

All the child table entries that are having FOREIGN_KEY reference to this table will also get archived.

```
set serveroutput on;

begin

PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.p_fcc_archival_proc('#APP_ID#','#SCHEM
A_NAME#','#TABLE_NAME#');

end;

/
```

For example:

```
set serveroutput on;

begin

PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.p_fcc_archival_proc('OFS_NGECM','UT_81
24ATOM','KDD_CASES');

end;

/
```

Here:

- V_APP_ID = OFS_NGECM
- V_TABLE_NAME = KDD_CASES
- V_SCHEMA_NAME = UT_8124ATOM

To view the archival data in database, execute the below command:

- ALTER SESSION SET ROW ARCHIVAL VISIBILITY = ALL;
- Select * from KDD_CASES where ORA_ARCHIVE_STATE ='1';

14.46 Archiving/Unarchiving Events

You can archive events based on your requirement. Archiving of events older than a defined period to be segmented into a separate storage area to improve performance. This is beneficial for customers who have large amounts of historical data which is still within the retention period. You can still query the data and retrieve it as needed.

There are three main archival tables:

- FCC_ARC_METADATA
- FCC_ARC_RESULTS
- FCC_ARC_AUDIT

For more information on the columns of these tables, see Archiving/Unarchiving Cases.

In the FCC_ARC_METADATA table events can be archived based on one or more column conditions (say event code (V_EVENT_CD) or event skey (N_EVENT_SKEY).

FCC_EVENTS is parent and FCC_EVENT_DETAILS is child table which are not having any foreign key. To archive event from both of these tables, V_CHILD_FLAG must be set to Y.

To unarchive, V_ROLL_BACK must be set to Y and run the Roll Back procedure.

After archival/unarchival, successful log msg is displayed.

Sample Statement for Archival:

Configure the FCC_ARC_METADATA table in Atomic Schema and run the below utility with arguments given in the FCC_ARC_METADATA table to archive events in the FCC_EVENTS table:

All the child table entries that are having FOREIGN_KEY reference to this table will also get archived.

```
set serveroutput on;

begin

PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.p_fcc_archival_proc('#APP_ID#','#SCHEM
A_NAME#','#TABLE_NAME#');

end;

/
```

For example:

```
set serveroutput on;

begin

PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.p_fcc_archival_proc('OFS_NGECM','UT_81
24ATOM','FCC_EVENTS');

end;

/
```

Here:

- V_APP_ID = OFS_NGECM
- V_TABLE_NAME = FCC_EVENTS
- V_SCHEMA_NAME = UT_8124ATOM

To view the archival data in database, execute the below command:

```
"ALTER SESSION SET ROW ARCHIVAL VISIBILITY = ALL;
"Select * from FCC_EVENTS where ORA_ARCHIVE_STATE ='1';
```

15 Configuring Administration Tools

This chapter provides instructions for configuring parameters specific to administration tools. This chapter covers the following topics:

- Configuring Administration Tools
- Configuring Application Server

15.1 Configuring Administration Tools

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

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

1. Open the Manage Common Parameters screen.
2. Select **Used for Design** from the Parameter Category drop-down list.
3. Select the **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 60 describes the attributes which should be configured for enabling and using the administration tools.

Table 60: Configuring Administration Tools

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

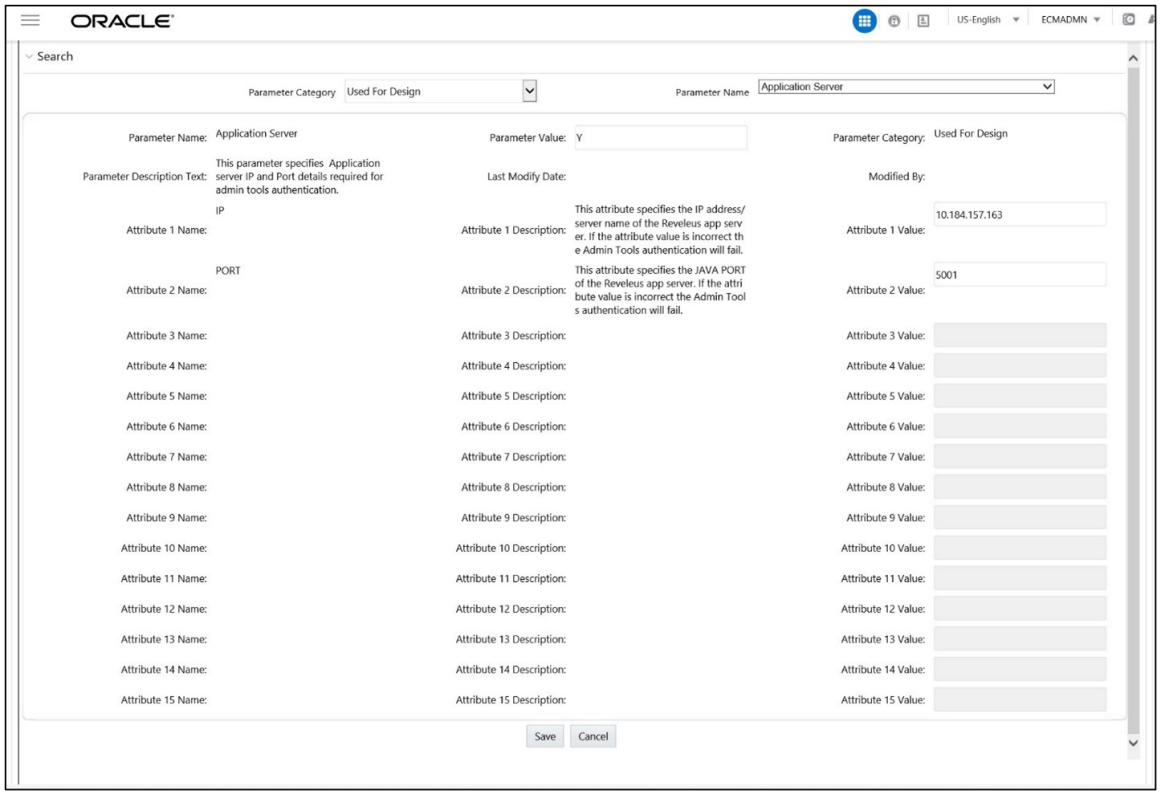
15.2 Configuring Application Server

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 as shown in Figure 98 .

Figure 98: Select Application Server page



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

Table 61: 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.

16 Configuring Actions

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

- Working with Case Action Settings
- Action Validation Framework
- CS and ECM Table Mapping for Alert Status Customization

16.1 Working with Case Action Settings

The following sections define how to configure case workflows:

- Understanding Case Workflows
- Adding New Case Statuses
- Configuring Case Action Data
- Configuring Standard Comment Data

16.1.1 Understanding Case Workflows

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

Defining a Case workflow consists primarily of the following tasks:

1. Create case types, see the Managing Case Designer, for more information.
2. Define case statuses that represent steps in the workflow. For more information, see Adding New Case Statuses.
3. Define actions to be used in the workflow. For more information, see Configuring Case Action Data.

> **NOTE** Define standard comments that is available in the workflow. For more information, see Configuring Standard Comment Data. When defining workflows, you specify individual actions or comments available at each step.

16.1.2 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 the appropriate record to the KDD_STATUS_TL database table as well for all the locale to be supported:

```
insert into KDD_STATUS_TL (V_LOCALE_CD, STATUS_CD, STATUS_NM,
V_CREATED_BY, D_CREATED_DT, V_SOURCE_LOCALE)

values ('en_US', 'CZZZ', 'Closed - Loss Recovered', null, null,
'en_US');
```

3. 3.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 Recov-
ered')
```

4. 4.Add the appropriate record to the KDD_CODE_SET_TRNLN_TL database table as well for all the locale to be supported

```
insert into KDD_CODE_SET_TRNLN_TL (CODE_SET, CODE_VAL, V_LOCALE_CD,
V_CREATED_BY, CODE_DISP_TX, D_CREATED_DT, V_SOURCE_LOCALE)

values ('CaseStatus', 'CZZZ', 'en_US', null, 'Closed - Loss Recovered',
null, 'en_US');
```

> **NOTE** Status is one of the masking parameter. Populate 'Open' status value as a parameter in AAI_MENU_B and cssms_start_page_-master. Here, we are passing parameter value as INV (code for the Investigation Status). If INV is a valid status code in the application, then do not change anything. In AAI_MENU_B, menu ID is 'OFS_NGECM_SRCH', and in cssms_start_page_master, start_page_id is 'ECM'. The parameter will look like '&mStatus=INV'.

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

16.1.2.1 Configuring Case Status in CRR

To configure the case status in CRR, follow the below steps:

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

```
insert into KDD_STATUS (STATUS_CD,CAN_NHRIT_FL,VIEWD_BY_OWNER_ACTVY_-
TYPE_CD,

VIEWD_RESULT_STATUS_CD,CLOSED_STATUS_FL,STATUS_NM) values

('CCASTR','N',null,null,'Y''Closed - CA STR Filed')
```

2. Add the appropriate record to the KDD_STATUS_TL database table as well for all the locale to be supported

```
insert into KDD_STATUS_TL (V_LOCALE_CD, STATUS_CD, STATUS_NM,
V_CREATED_BY, D_CREATED_DT, V_SOURCE_LOCALE)

values ('en_US', 'CCASTR', 'Closed - CA STR Filed', null, null, 'en_US');
```

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

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

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

   Here,

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

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

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

Here,

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

16.1.2.2 Restricting Case Status

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

16.1.2.3 Masking for New Statuses

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

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

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

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

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

> **NOTE** You cannot include closed status everywhere. Investigator and Admin roles should not be mapped to the same users.

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

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

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

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

5. Restart the servers to verify the updates.

16.1.3 Configuring Case Action Data

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

- Adding a New Action Category
- Adding a New Action
- Mapping New Action to User Role
- Mapping the New Action to Status
- Map the New Action to the Case Type

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

16.1.3.1 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')
```

2. Add the appropriate record to the KDD_ACTION_CAT_CD_TL database table as well for all the locale to be supported.

```
insert into KDD_ACTION_CAT_CD_TL (V_LOCALE_CD, ACTION_CAT_CD, DISPL_NM,
V_CREATED_BY, D_CREATED_DT, V_SOURCE_LOCALE)
values ('en_US', 'REV', 'Research & Review', null, null, 'en_US');
```

16.1.3.2 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)
```

2. Add the appropriate record to the KDD_ACTION_TL database table as well for all the locale to be supported

```
insert into KDD_ACTION_TL (V_LOCALE_CD, ACTION_ID, ACTION_NM,
ACTION_DESC, V_CREATED_BY, D_CREATED_DT, V_SOURCE_LOCALE)
values ('en_US', 73, 'Reviewed with Account Manager', 'Reviewed with
Account Manager', null, null, 'en_US');
```

3. While adding a new action, the set of supplemental values to be associated with the action should be decided based on the following criteria:
   - ACTION_CATEGORY_CODE - Category code that identifies the classification of an action. If you want to change the category of action, you need to change this column accordingly.
   - 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 the 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.

     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).
   - NEXT_REVIEW_STATUS_CD - Resulting status code to be set when this action type is performed on an investigation record.
   - REQ_REASN_FL - Indicator of whether this action type requires reassignment of an investigation record.
   - 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.

   - REQ_CMMNT_FL - Indicator of whether a comment, either the standard or free-text comment, is required for this action type.
   - REQ_REASN_OWNER_FL Indicator of whether this action type requires reassignment of ownership of a case investigation record.
   - LAST_ASSIGN_REQ - Used by the system to determine the last user who performed this action in the situation where this recommendation or escalation action is rejected and the case would need to be reassigned back to the last user who took the action. "Y" means that when this action appears on a case previous to a rejection action by another user the user who took this action would become the owner. "N" means this is not a recommendation for approval or escalation type action or is not an action that would be used by the system to determine reassignment.
   - RESOLUTION_ACTION_FL - Indicator of whether this action is a resolution action.

   NOTE If you are adding new actions, then start the action sequence number with a higher number like 30000. If any of the OOB actions not required, then change the category of that action to OBS. This is prevented that action to appear in the Search screens.

16.1.3.3 Mapping New Action to User Role

1. 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')
   ```

2. Each record in the Case Role to Action Map table represents the mapping between user roles and the actions that a particular user role is allowed to perform. Each Action can be mapped to multiple roles.

> **NOTE** If you are adding new records, then start the CASE_ROLE_ACTION_MAP_SEQ with a higher number like 30000.

16.1.3.4 Mapping the New Action to Status

1. 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')
   ```

2. Each record in the Case Status to Action table captures the actions that will be available for a case based on the case's current status.

> **NOTE** If you are adding new records, then start the CASE_STATUS_ACTION_MAP_SEQ with a higher number like 30000.

16.1.3.5 Map the New Action to the Case Type

1. Create a new Case Type Action mapping by adding a new record in the KDD_CASETYPE_ACTION_- MAP table as follows, where the CASE_CASETYPE_ACTION_MAP_SEQ represents the next sequential number for a record in this table:

   ```
   insert into KDD_CASETYPE_ACTION_MAP (CASE_CASETYPE_ACTION_MAP_SEQ,
   ACTION_CD, CASE_TYPE_SUBTYPE_CD) values (80, 'CA73S', 'AML_SURV')
   ```

> **NOTE** If you are adding new records, then start the CASE_CASETYPE_ACTION_MAP_SEQ with a higher number like 30000.

2. 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.

16.1.4 Configuring Standard Comment Data

When taking action on a case, you can configure the various types of Standard Comments based on Case Status and User Group. As a result, different Standard Comments can be displayed to different individuals at various stages of case ingestion. Action-related Standard Comments are based on Case

Type, Status and Role. Evidence and Assignee-related Standard Comments are based on Case Type. Other language characters and special characters can also be added in the Standard Comments.

NOTE

- When taking an action, adding evidence, assigning a case or adding a comment, the standard comments displayed will be specific to that action. When taking a combination of any of those actions, a super set of the standard comments are displayed.
- If you select to take a non-status changing action (e.g., Set Due Date and Add Comment), Evidence-related comments are displayed.

16.1.4.1 Standard Comments on Take Action Page

Configuring Standard Comments and standard comment categories are similar to configuring them for the Case Actions pop-up. The comments are created in the KDD_CMMNT and KDD_CMMNT_TL tables, and the categories (SDCT) 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);

NOTE In the KDD_CMMNT and KDD_CMMNT_TL tables, the range of cmmnt_id can be 200-1000 for customizations.

For filtering Standard Comments in Take Action dialog, a new table FCC_ENTITY_CMMNT_MAP has been created where you can configure and map Standard Comments based on Actions, Roles, and Status (V_ENTITY_TYPE). If the FCC_ENTITY_CMMNT_MAP table is empty, then Standard Comments will be filtered based on Case Type as before.

Sample Statement:

```
Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ACTION','CA945S',9205)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ACTION','CA307S',9204)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',9999)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',9205)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',9204)

/
```

```
Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',8105)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',8107)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMSUPRVISR',8102)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('ROLE','CMANALYST2',8105)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('STATUS','INV',9205)

/

Insert into FCC_ENTITY_CMMNT_MAP (V_ENTITY_TYPE,V_ENTITY_ID,V_CMMNT_ID)
values ('STATUS','INV',9204)

/
```

If any of the V_ENTITY_TYPE is not having any entry in the FCC_ENTITY_CMMNT_MAP table, then only the remaining V_ENTITY_TYPE is used for filtering. For example: If there's no configuration for ACTION, then comments is filtered based on Role, Status, and Case Type.

16.1.4.2 Standard Comments on Assignee Page

Add the entries in the KDD_CMMNT and KDD_CMMNT_TL tables in order to see the comments in the Assign section. The records must be inserted in these tables in order to see the entered comment in the UI.

In the KDD_CASE_TYPE_CMMNT table, map the entries for Assignee for AML_SURV Case Type. Since the Standard Comments of Assignee are based on Case Type, the mapping must be done in the table.

Sample Statement:

```
INSERT INTO KDD_CASE_TYPE_CMMNT

(CASE_TYPE_CD, CMMNT_ID)

VALUES('AML_SURV', 53);


INSERT INTO KDD_CMMNT

(CMMNT_ID, EDIT_FL, CMMNT_TX, DISPL_ORDER_NB, CMMNT_CAT_CD)

VALUES(53, 'N', 'Assign Standard cmnt1', 40, 'ASCT');


INSERT INTO KDD_CMMNT_TL

(CMMNT_ID, V_LOCALE_CD, CMMNT_TX, V_CREATED_BY, D_CREATED_DT,
V_SOURCE_LOCALE)

VALUES(53, 'en_US', 'Assign Standard cmnt1', NULL, NULL, 'en_US');
```

16.1.4.3 Standard Comments on Add Evidence Page

For the given comment category code (EVCT), comment ID ,name of the comment must be configured in the KDD_CMMNT_CAT_CD table.

Add the entries in the KDD_CMMNT and KDD_CMMNT_TL tables in order to see the comments in the Add Evidence section. The records must be inserted in these tables in order to see the entered comment in the UI.

Sample Statement:

```
INSERT INTO KDD_CASE_TYPE_CMMNT
(CASE_TYPE_CD, CMMNT_ID)
VALUES('AML_SURV', 52);


INSERT INTO KDD_CMMNT
(CMMNT_ID, EDIT_FL, CMMNT_TX, DISPL_ORDER_NB, CMMNT_CAT_CD)
VALUES(52, 'N', 'Evidence Std cmnt', 40, 'EVCT');


INSERT INTO KDD_CMMNT_TL
(CMMNT_ID, V_LOCALE_CD, CMMNT_TX, V_CREATED_BY, D_CREATED_DT,
V_SOURCE_LOCALE)
VALUES(52, 'en_US', 'Evidence Standard cmnt1', NULL, NULL, 'en_US');
```

In the KDD_CASE_TYPE_CMMNT table, map the entries for Add Evidence for AML_SURV Case Type. Since the Standard Comments of Add Evidence are based on Case Type, the mapping must be done in the table.

16.2 Action Validation Framework

The action validator framework allows you to perform the validation based on the configuration made in the KDD_ACTION_VLDTN table.

Examples:

1. If you want to set a validation rule where you want to exclude the comments action (CA8) when Send Email Action is taken , then for "Send Email Action"(CA921), set the below configuration entries in the KDD_ACTION_VLDTN table as described in Table 62 :

   Table 62: KDD_ACTION_VLDTN table

ACTION_CD	VLDTN_TYPE	VLDTN_CON-FIG_DATA	VLDTN_-FLD_MSG	VLDT-N_ORDER	ACTV_FL
CA921	EXCLUDE	CA8	(null)	(null)	Y

   When this validation rule is executed, an error message will display.

2. If you want to a set a validation rule where Case Owner and Case Assignee values should not be the same, then for "Set Case Owner" (CA938) and "Set Case Assignee" (CA939), set below JAVAS- CRIPT validator in KDD_ACTION_VLDTN table as described in Table 63 :

Table 63: KDD_ACTION_VLDTN table

ACTION_CD	VLDTN_TYPE	VLDTN_CONFIG_DATA	VLDTN_FLD_MSG	VLDTN_ORDER	ACTV_FL
CA938	JAVASCRIPT	validateOwnerAssignee	RENDERE.CM_TA_OWNRASSGN_NTSM	1	(null)
CA939	JAVASCRIPT	validateOwerAssignee	RENDERE.CM_TA_OWNRASSGN_NTSM	1	(null)

When this validation rule is executed, an error message will display.

16.2.1 KDD_ACTION_VLDTN Table

Table 64 describes the KDD_ACTION_VLDTN table.

Table 64: KDD_ACTION_VLDTN table

Column Name	Primary Key	Column Type	Nullable
ACTION_CD	Y	VARCHAR2 (20 CHAR)	No
VLDTN_TYPE	Y	VARCHAR2 (50 CHAR)	No
VLDTN_CONFIG_DATA	Y	VARCHAR2 (4000 CHAR)	No
VLDTN_FLD_MSG		VARCHAR2 (1000 CHAR)	Yes
VLDTN_ORDER		NUMBER(10)	Yes
ACTV_FL		VARCHAR2 (1 CHAR)	Yes

- **ACTION_CD**: This is the Action code for which validation will be performed.
- **VLDTN_TYPE**: Indicates the Validation Type. Below are the possible values
  - EXCLUDE: Exclude Action validator
  - INCLUDE: Include Mandatory Action validator
  - QUERY: Query-based validator
  - JAVASCRIPT: JavaScript-based client-side validator
- **VLDTN_CONFIG_DATA**: Indicates the configuration for the validator.

  For Exclude Type:

  Action codes which are mutually exclusive for this action must be provided. Multiple action codes need to be provided in separate rows with type as EXCLUDE.

  For Include Type:

Action codes which are mandatorily inclusive for this action must be provided. Multiple action codes need to be provided in separate rows with type as INCLUDE.

For Query Type:

Query needs to be provided in the VLDTN_CONFIG_DATA column. The query should be such that in case of failure should return false and in case of success should return true. Both request and session attributes are supported. You can specify them using the below notation:

Request Attributes: @@AttributeName@@ Session Attributes: ##AttributeName##

The following is list of seeded parameters to Query Validator:

- oactionCode (Action Code for which the validation is been performed)
- oReviewId (Case ID on which the action is performed)
- osetDDActnVal (Set Due Date Value)
- oclearDDActnVal (Clear Due Date Value)
- osetCAActnVal (Case Assignee Value)
- osetCOActnVal (Case Owner Value)
- oautoAssgnActnVal (Auto Assignment value)
- oemailFromIdActnVal (Email From Value)
- oemailSubjTextActnVal (Email Subject Value)
- oemailToIdActnVal (Email To Value)
- oemailBodyTextActnVal (Email Body Value)
- ocommentsStdActnVal (Standard Comments value under Comments Action)
- oaddInCommentsActnVal (Textual Comments value under Comments Action)
- oattachCommentsStdActnVal (Standard Comments value under Attachment Action)
- oattachAddInCommentsActnVal (Textual Comments value under Attachment Action)
- oattachFileNameActnVal (File Name under Attachment Action)
- oclosedCasesAvail (Indicates if any of the selected cases are in a closed status)
- opmfActionsAvail (Indicates if any PMF action is selected or not)

- For JAVASCRIPT Type:

  JavaScript method name should be provided in VLDTN_CONFIG_DATA column. The method can be defined in any custom JS file. Follow the steps mentioned in Adding a custom JS file in ECM.

  This method should have two inputs one is the actionCode for which this validator is defined and another input is the userEnteredValueMap which contains below attributes that holds user entered values on the Take Action page:

  - osetDDActnVal (Set Due Date Value)
  - oclearDDActnVal (Clear Due Date)
  - osetCAActnVal (Case Assignee Value)
  - osetCOActnVal (Case Owner Value)
  - oautoAssgnActnVal (Auto Assignment Value)

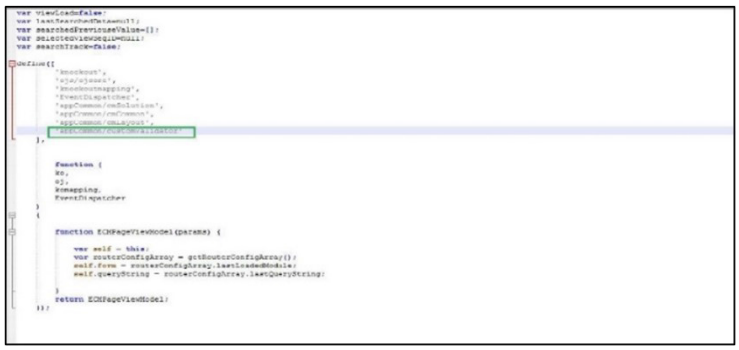
- oemailFromIdActnVal (Email From Value)
- oemailSubjTextActnVal (Email Subject Value)
- oemailToIdActnVal (Email To Value)
- oemailBodyTextActnVal (Email Body Value)
- ocommentsStdActnVal (Standard Comments value under Comments Action)
- oaddlnCommentsActnVal (Textual Comments value under Comments Action)
- oattachCommentsStdActnVal (Standard Comments value under Attachment Action)
- oattachAddlnCommentsActnVal (Textual Comments value under Attachment Action)
- oattachFileNameActnVal (File Name under Attachment Action)

The method should return true if the validation is successful or false if the validation fails.

16.2.2 Adding Custom JS file in ECM

1. Copy the custom JS file to <<deployedarea>>/ojff/js/appCommon
2. Go to <<deployedarea>>/ojff/js/appCommon/viewModels/aai-ecm.js. In aai-ecm.js add entry for your js file in the define block. For example, if your custom JS file name is customValidator.js, then add as shown in Figure 99 .

Figure 99: customValidator.js file



- **VLDTN_FLD_MSG**: This is used to specify a particular message constant to be shown in case of validation failure. If no message is configured default message will be shown. Default Messages are as below:

  Exclude Validator:

  ```
  <ACTION NAME1> is not permitted along with <ACTION_NAME2>
  ```

  Include Validator:

  ```
  <ACTION NAME1> must be mandatorily taken along with <ACTION_NAME2> Query Validator:
  ```

  ```
  Query validation failed for <ACTION NAME1> JavaScript Validator:
  ```

  Validation failed for <METHOD_NAME>

- **VLDTN_ORDER**: Numeric Sequence indicating the order of the validator within a particular action code.

- **ACTV_FL**: Flag to identify whether the mentioned action validator is active or not.

> **NOTE** After making the changes in the table, restart the server.

16.3 CS and ECM Table Mapping for Alert Status Customization

When L2 Investigation is enabled and if there is any customization of the alert workflow (status, action, or standard comments) done to the Customer Screening (CS) dimension tables listed in the following table, then update the same data in the corresponding ECM dimension table. As a result Alert summary for the escalated case will be visible in Enterprise Case Management (ECM) application.

Table 65 provides the list CS dimensions tables and corresponding ECM dimension table.

Table 65: CS and ECM Dimension Table

CS Dimension Tables	ECM Dimension Tables
FCC_ZCS_STATUS_DIM	FCC_CS_CM_STATUS_DIM
FCC_ZCS_STATUS_TL	FCC_CS_CM_STATUS_TL
FCC_ZCS_ALERT_PRIORITY_DIM	FCC_CS_CM_ALERT_PRIORITY_DIM
FCC_ZCS_ALERT_PRIORITY_TL	FCC_CS_CM_ALERT_PRIORITY_TL
FCC_ZCS_SCREENING_MODE_DIM	FCC_CS_CM_SCREENING_MODE_DIM
FCC_ZCS_SCREENING_MODE_TL	FCC_CS_CM_SCREENING_MODE_TL
FCC_ZCS_ALERT_TYPE_DIM	FCC_CS_CM_ALERT_TYPE_DIM
FCC_ZCS_ALERT_TYPE_TL	FCC_CS_CM_ALERT_TYPE_TL
FCC_SAN_ALERT_STD_CMNTS_MAP	FCC_CS_ESC_AL_STDCMNTS
FCC_SAN_STD_CMNTS_DIM	FCC_CS_CM_SAN_STD_CMNTS_DIM
FCC_SAN_STD_CMNTS_TL	FCC_CS_CM_SAN_STD_CMNTS_TL
FCC_ZCS_ALERT_ACTIONS_DIM	FCC_CS_CM_ALERT_ACTIONS_DIM
FCC_ZCS_ALERT_ACTIONS_TL	FCC_CS_CM_ALERT_ACTIONS_TL
FCC_ZCS_EVENT_STATUS_DIM	FCC_CS_CM_EVENT_STATUS_DIM
FCC_ZCS_EVENT_STATUS_TL	FCC_CS_CM_EVENT_STATUS_TL
FCC_SAN_EVENTS_STD_CMNTS_MAP	FCC_CS_ESC_EVNT_STDCMNTS
FCC_ZCS_MATCH_RULE_DIM	FCC_CS_CM_MATCH_RULE_DIM
FCC_ZCS_MTCH_RULE_ENT_ATTR_MAP	FCC_CS_CM_MTCH_RULE_ENT_ATRMAP
FCC_ZCS_ENTITY_ATTR_DIM	FCC_CS_CM_ENTITY_ATTR_DIM
FCC_ZCS_MTCH_RULE_WLS_ATTR_MAP	FCC_CS_CM_MTCH_RULE_WLS_ATRMAP
FCC_SAN_SCMNTS_ENTITY_ACTN_MAP	FCC_CSCM_SCMNTS_ENT_ACTN_MAP
FCC_SAN_STD_CMNTS_ENTITY_MAP	FCC_CSCM_STD_CMNTS_ENT_MAP

17 Configuring Web Application

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

17.1 Configuring the Session Timeout Setting

This section describes the following topics:

- Configuring the Session Timeout Setting
- Configuring the Session Timeout Setting for Admin Tools

17.1.1 Configuring the Session Timeout Setting

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

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

17.1.2 Configuring the Session Timeout Setting for Admin Tools

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

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

1. Open the web.xml file associated with the WebLogic or WebSphere application.
2. You can find this file in the WEB-INF directory under each Web application in the Oracle Financial Services installation.
3. Modify the XML code within the file that contains <session-config> in its `<session-descriptor>` entry.
4. 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.
5. Save the changes.
6. 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>
```

18 Multi-locale Architecture

Introducing following tables for supporting Multi-locale architecture.

- KDD_CASE_TYPE_SUBTYPE_TL
- KDD_ACTION_TL
- KDD_ACTION_CAT_CD_TL
- KDD_CMMNT _TL
- KDD_STATUS_TL
- KDD_CODE_SET_TRNLN_TL
- KDD_LINK_ANLYS_DISPLALY_INFO_TL
- KDD_QUEUE_MASTER _TL
- KDD_REG_REPORT_STATUS_TL
- FCC_EVENT_TYPE_TL
- KDD_INSTALL_PARAM_TL
- KDD_CASEATTRBT_MASTER_TL
- KDD_CASEENTITY_MASTER_TL
- KDD_JRSDCN_TL
- KDD_BUS_DMN_TL
- KDD_ORG_TL
- KDD_COUNTRY_TL
- FCC_SCENARIO_MASTER_TL
- FCC_TPG_SETUP_PARAMS_SRVCS_TL

There may be 2 scenarios:-OPTIONAL STEP ONLY IF below scenario is satisfied:

If any client has applied LP in earlier versions then the base tables will be holding translated strings.

OR

If client has customized few OOB Strings or added new entries to Base tables.

NOTE Client can make use of the attached MergeScript_TL_LP_Customizations.sql. Client need to replace the placeholder ##LOCALE_CD## with their respective locale and execute in Atomic Schema and commit.

19 Additional Configuration

This chapter provides the details on additional configuration activities.

- Correlation Case Type Mapping
- Configuring CAR Rules
- Continuing Activity Review & Continuing Activity Report
- Populating Country ID
- Adding Relationship Type values for Involved Parties
- Adding Relationship Type values for Involved Parties
- Configuring Case Allocation
- Custom Rule Attributes
- Configuring Tabs based on Role
- Adding Standard Comments for Event Decision
- Adding Event Decision for Customer Screening
- Adding Search Results Fields based on Case Type
- Adding and Configuring Case Type Attribute
- Configuring a Case as Read Only
- Adding a New Scenario
- Configuring Quality Control (QC) Sampling Rules
- Event Purge
- Case Purge Utility
- Event Expiry
- CSS Color Coding for FCC Columns
- Enabling Quantifind for Quantifind Customer Score Card
- Configuring Quantifind Batch Processing for Customer Score Card Processing
- Configuring Quantifind for Bulk Entity Process
- Configuring Quantifind for Bulk Event Creation Process
- Transaction Chart Configuration
- Configuring Labels for Transactions
- Entities Tab Configuration
- Configuring Different Due Dates for Case Types
- Trusted Pairs
- Event Suppression

19.1 Correlation Case Type Mapping

Define the Case Type mapping before executing the batch. This configuration activity allows you to define the mapping between correlation rule and case type. This is performed using the FCC_CORRELATION_CASE_TYPE_MAP table as described in Table 66 .

Table 66: Correlation Case Type Mapping

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 the case. This entry should be the same as mentioned in
- KDD_CASE_TYPE_SUBTYPE table. For more information, see the About Case Type section.

To perform this activity, follow these steps:

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

> **NOTE** The value of the N_CORRELATION_RULE_SKEY column (rule number) should be the same as defined in the FCC_CORRELATION_RULE table.

19.1.1 Case Priority

You can define the priority of the case using the FCC_CASE_PRIORITY table.

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

> **NOTE** If the entry is not present for a case type in table FCC_CASE_PRIORITY, then the Case Priority will be set as 'High'.

19.1.2 Case Domain and Jurisdiction

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

19.2 Configuring CAR Rules

You can configure which Case Types will generate a Continuous Activity Report (CAR) case when the File SAR Action is selected.

The CAR rule tables - FCC_CAR_CASE_RULES and FCC_CAR_CASE_RULE_ATTR_VAL_MAP define which Case Type must result in a CAR case with the specific actions.

You must add entries in FCC_CAR_CASE_RULES and FCC_CAR_CASE_RULE_ATTR_VAL_MAP tables to create a CAR case. If there are no CAR rules defined in these tables for the specific Case Type and Action, no CAR case will be created.

Table 67 describes the FCC_CAR_CASE_RULES table.

Table 67: FCC_CAR_CASE_RULES

N_RULE_ID	V_RULE_NAME	V_RULE_OUTCOME_CASE-TYPE
101	Continuous Activity Rule1	AML_CA
102	Continuous Activity Rule2	AML_CA

Table 68 describes the FCC_CAR_CASE_RULE_ATTR_VAL_MAP table.

Table 68: FCC_CAR_CASE_RULE_ATTR_VAL_MAP

N_RULE_ID	N_ATTRIBUTE_ID	V_ATTRIBUTE_VALUE	V_ATTRIBUTE_CD
101	1	AML_SURV	casetypecode
101	2	CA945	Sactioncd
102	1	AML_CA	casetypecode
102	2	CA1014	Sactioncd

For example:

```
Insert into FCC_CAR_CASE_RULES
(N_RULE_ID,V_RULE_NAME,V_RULE_OUTCOME_CASETYPE) values
(101,'Continuous Activity Rule1','AML_CA');

Insert into FCC_CAR_CASE_RULE_ATTR_VAL_MAP
(N_RULE_ID,N_ATTRIBUTE_ID,V_ATTRIBUTE_VAL,V_ATTRIBUTE_CD) values
(101,1,'AML_SURV','casetypecode');

Insert into FCC_CAR_CASE_RULE_ATTR_VAL_MAP
(N_RULE_ID,N_ATTRIBUTE_ID,V_ATTRIBUTE_VAL,V_ATTRIBUTE_CD) values
(101,2,'CA945S','actioncd');
```

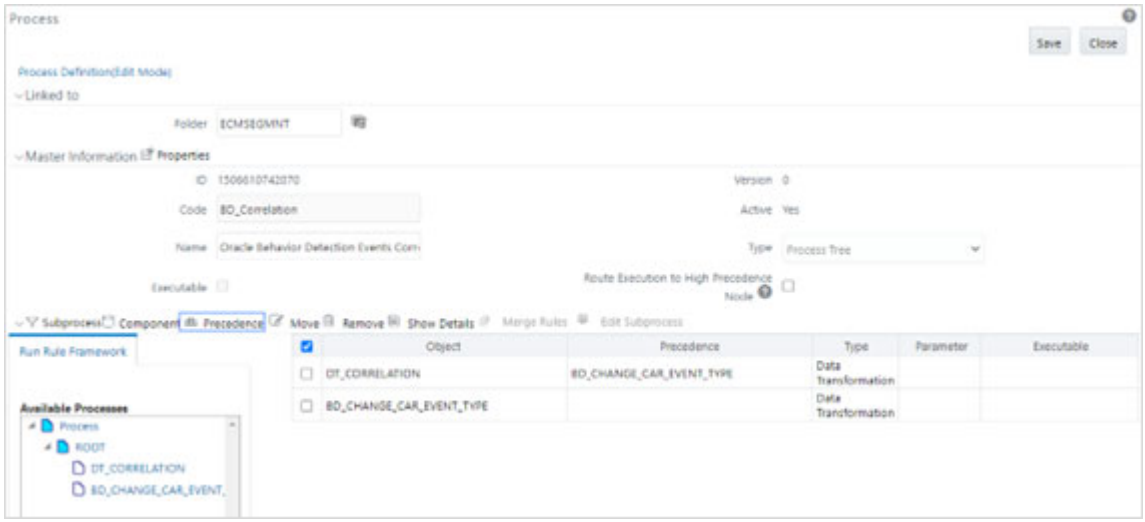
When an action with action code CA945S (ensure that this action code is configured in the workflow of the AML_SURV Case Type) has been taken on a case with Case Type AML_SURV, the resultant CAR Case Type will be AML_CA.

If the batch is run and there is an open CAR Case with the same focal entity, the event type of the upcoming events is changed to AML_CA and is correlated/extended to the CAR case. If the correlation/extension is not occurred,

- you must add the BD_CHANGE_CAR_EVENT_TYPE Data Transformation (DT) to Oracle Behavior Detection Events Correlation - BD_Correlation process
- the DT must be in precedence of DT_Correlation. hence the sequence must be:
  - DT_Correlation
  - BD_CHANGE_CAR_EVENT_TYPE

Figure 100 shows the BD_CHANGE_CAR_EVENT_TYPE precedence.

Figure 100: CAR Case Correlation



19.3 Continuing Activity Review & Continuing Activity Report

The Continuing Activity case allows investigators to review activities that occurred after filing the SAR on the previous case. This case must be investigated and concluded within your firm's review period, typically between 90-120 days. After this period, a continuing SAR must be filed, if necessary.

To fully implement the Continuing Activity Review process, your firm must implement Oracle FCCM Compliance Regulatory Reporting for US-SAR. This allows investigators to view select information from the parent SAR when reviewing the CAR case.

The Secure Direct Transfer Mode (SDTM) must be configured while setting up CAR Case Due Date. For more information, see Configuring Secure Direct Transfer Mode (SDTM) in the Oracle Financial Services Compliance Regulatory Reporting Admin Guide.

The setting of the CAR due date is based on receipt of a successful msg xml from the FINCEN after the CRR first sends the e-file. The information from CRR is sent to ECM via an API.

To enable this Continuing Activity Report (CAR) functionality, there are certain configurations to be set up both on the CRR and ECM sides.

CRR Side:

NOTE

- Ensure that individual users are available with `RRUSSUPER`, `RRUSSUPERVISOR` and `RRADMINISTRATOR` group mapped and having the required security mapping. For more information, see the *Configuring Security Attributes* section in CRR Administration Guide.
- Ensure that `DIM_DOMAIN1`, `DIM_DOMAIN2`, DIM_DOMAIN3, `DIM_DOMAIN4`, and `DIM_DOMAIN5` as well as associated _TL tables, contain the corresponding data with ECM security mapping tables.

For CRR side of configuration, follow these steps:

1. Log into the CRR UI with a user having mapped with the RRADMINISTRATOR group.

   This step allows the privileged user to access CRR for further configurations.

2. Go to **Webservice Configuration** and set the user as `rruser` and password as `password`.

   This step allows *handshake* between CRR and ECM using the credentials mentioned.

3. Update `V_ATTRIBUTE_VALUE4` in the `APPLN_PARAMETERS` table for `N_PARAM_IDENTIFIER=2` with `http://<Application URL>/ecmcrr-rest-api`

   This API URL update is required to send the Basic Details (Previous Case, Total Suspicious Amount, Date Range of Suspicious Activity, Prior BSA Identification Number, Cumulative Violation Amount, SAR Filed Date), Subject of Previous SAR (Customer, External Entity, and

Account), Typologies from the SAR (Cyber Events, Fraud Type, Gaming Activities, etc.), Narrative of the filed SAR, and CAR due date from CRR to ECM.

4. Update `PARAMNAME ='V_ABS_CONTEXT_PATH'` in the `CONFIGURATION` table with the deployed .war path. For example:

   ```
   /scratch/ofsaebas/WL14_j11/user_projects/domains/BECS8124/applications/BECS8124.ear/BECS8124.war
   ```

   This step is necessary to validate the XSD Parameters, which is required for report approval.

   For more information, see the *Configuring XSD Parameters* section in CRR Administration Guide.

5. Update the `UCM_GROUP_NAME` parameter value to `PRADMINISTRATOR` in the `CONFIGUARTION` table.
6. Update the `CRR_CONFIGURATION` table with `CRR_SERVICE_URL` (http://<Application URL>).

ECM Side:

For ECM side of configuration, follow these steps:

1. Log in as ECM Administrator.
2. Select **Case Management Configuration** and then select **Manage Common Parameters**.
3. Under the **Parameter** category, select `Deployment Based` and under **Parameter** name, select `Regulatory Report Solution Web Service`.
4. Update the following fields with required parameters to connect with CRR.
   - Parameter Value = Y
   - Attribute 1 Value = rruser
   - Attribute 3 Value = http:// <Application URL>/RRSService/InitiateRequest
   - Attribute 4 Value = http:// <Application URL>/CRRframeworkDataingestion
   - Attribute 5 Value = Y
5. Navigate to **Configuration of Web Service**.
6. For **Enter Password for Regulatory Reporting Web Service**, enter password as password and then click **Encrypt**.

   This step allows *handshake* between ECM and CRR using the credentials mentioned. This will encrypt the password for the `rruser` and the encrypted password will get saved in the Attribute 2 Value column of the kdd_install_param table.

7. Assign 775 permissions to the *MiscellaneousCRR* folder available in the deployed `.war` path.

   MiscellaneousCRR is used for XSD validation at the CRR side.

8. Restart APP and Web Servers.

Following the filing of the US-SAR, a report is generated at CRR, and once the filing in CRR is complete, the relevant information is sent to ECM UI under the Previous Summary Report tab. The relevant tables are:

- KDD_CASE_RR_MAP
- KDD_CASE_RR_TYPOLOGY
- KDD_CASE_RR_ENTITY_MAP
- KDD_CASE_RR_DETAILS.

19.4 Populating Country ID

To populate the country ID, follow these steps:

Populate the KDD_COUNTRY table using the below query. This query will select the data from STG_COUNTRY_MASTER and insert into KDD_COUNTRY table:

```
INSERT INTO kdd_country

(country_id, country_cd, country_nm, country_desc)

WITH country_data AS

(SELECT DISTINCT v_iso_country_cd, v_country_name, v_country_desc FROM
stg_country_master

WHERE TO_DATE(fic_mis_date, 'DD-Mon-YY') = TO_DATE(?, 'DD-Mon-YY'))

SELECT cm_geography_seq.nextval, v_iso_country_cd, v_country_name,
v_country_desc

FROM country_data WHERE NOT EXISTS (SELECT 1

FROM kdd_country kc

WHERE kc.country_cd = country_data.v_iso_country_cd);
```

19.5 Adding Relationship Type values for Involved Parties

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

if you have two relationship types as Primary Suspect and Secondary Suspect, then add the following entries for InvolvedPrtyRelType and RelationshipType-InvParty in the KDD_CODE_SET_TRNLN table (Atomic Schema) as described in Table 69 :

Table 69: KDD_CODE_SET_TRNLIN Table

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

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

19.6 Configuring Case Allocation

The Case Allocation feature automatically assigns the new and existing cases to individuals or pools at any point during the case investigation process based on a defined allocation rule. This feature saves

the time of managers/administrators who manually go through each case and assign them to team members based on the selected criteria.

Following tables are used for configuring this feature:

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

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

Administrators or Allocation Team Lead can create the Allocation Rules.

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

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

To configure this, follow these steps:

1. To define the rule, add entries in the `FCC_ASSGN_RULE_DEFN` table. Case allocation rules are defined in table `FCC_ASSGN_RULE_DEFN` as described in Table 70 .

   Table 70: FCC_ASSGN_RULE_DEFN Table

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

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

   NOTE The N_PRIORITY and V_ALGORITHM columns are not being used.

2. An individual user/pool is mapped to a rule in table FCC_ASSGN_RULE_USER_MAP. When these rules are run, then the administrator/manager can make the individual/pool the assignee and the owner of the case. A single user/pool can be mapped to multiple rules if necessary and a

single rule can be mapped to multiple individuals/pools. In the below example, a user is mapped to three different rules, so the user will get three different flavors of cases. User capacity is calculated by the cases assigned by each rule but not by the aggregated capacity of all the rules

mapped to him. Add the following entries in the FCC_ASSGN_RULE_USER_MAP table as described in Table 71 :

Table 71: FCC_ASSGN_RULE_USER_MAP Table

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

- V_RULE_NAME: The Rule Name to be mapped for the user/group as defined in table FCC_ASSGN_RULE_DEFN.
- "N_RULE_ID: The Rule ID of the rule is defined in table FCC_ASSGN_RULE_DEFN.
- "V_USER_NAME: The name of the user/pool.
- "N_USER_ID: The exact User/Pool ID as defined in the KDD_REVIEW_OWNER table.
- "V_ACTIVE: The status of the rule. Value 'Y' denotes to active the rule. For any value other than 'Y', the system considers the rule inactive and does not allocate the cases as per the rule to a user.
- "N_USER_CAP: The maximum number of cases that can be allocated to this user for that rule. The system will not allocate cases beyond that number.
- "N_PRIORITY: The priority of that assignment rule is based on which rule gets assigned. Here, N_USER_ID should be the same as given in the KDD_REVIEW_OWNER table.
- "D_FROM_OO: Stands for Date From Out of Office. Date from when a user is absent from the office.
- "D_TO_OO: Stands for Date To Out of Office. Date until a user is out of the office.

  The D_FROM_OO and D_TO_OO columns in the FCC_ASSGN_RULE_USER_MAP table can be set up to assign cases to users based on their availability.

  You can allocate cases to the users based on the D_FROM_OO and D_TO_OO columns in the FCC_ASSGN_RULE_USER_MAP table.

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

```
(Select t.case_intrl_id from kdd_cases t
inner join fcc_precase_case_map pcm on pcm.v_case_id = t.case_in-
trl_id
inner join fcc_correlation_event_map cor on cor.n_event_correla-
tion_skey = pcm.n_event_correlation_skey
inner join fcc_event_details s on s.n_event_skey
```

```
= cor.n_event_skey

where s.N_SCENARIO_SKEY in (279,403));
```

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

19.6.1 Distribution of Cases to Users

When a case comes in the system and it satisfies all conditions of rule definition, then it will be allocated to user who has Priority as '1.' For example, there are 2 users with priority '1'. When 10 new cases come in the system and they all satisfy the rule definition condition, then 5 cases will be allocated to the user1 (who has priority '1') and 5 cases will be allocated to the user2 (who has priority '1'). That is, the system equally distributes the cases among the users having the same priority. If the capacity of user1 and user2 is full, then cases will be allocated to users who has priority '2'. The cases would not be allocated to other users until the capacity of users with priority '1' is not full.

For example, the same rule is mapped to two different users as described in Table 72 . Let's assume, the rule has filtered 125 available cases for assignment, and Bob and Sue's buckets are empty. Here, the

priority of Bob is '1' and Sue's priority is '2'. The system will allocate 100 cases to Bob and then 25 cases to Sue.

Table 72: Load Balancing

V_USER_NAME	V_RULE_NAME	V_ACTIVE	N_USER_ID	N_USER_CAP	N_RULE_ID	N_CURR_CAP	N_PRIORITY
Bob Smith	TF Cases Older than 30 Days	Y	1234	100	1		1
Sue Green	TF Cases Older than 30 Days	Y	1234	100	1		2

Cases get assigned to the user only if the case security mapping is satisfied with that user. The assignment will happen based on the security mapping constraints (Jurisdiction, Business Domain, and Case Type).

The following seeded attributes are available for rule creation as described in Table 73 . All of these columns are defined in the KDD_CASES table.

Table 73: KDD_CASES Table

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

19.7 Custom Rule Attributes

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

Below is an example to define and insert the Event Scenario as a rule attribute.

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

```
insert into FCC_ASSGN_RULE_DEFN (V_RULE_NAME, N_RULE_ID, V_FILTER_NM, V_FILTER_OPERATOR, V_FILTER_VAL)

values ('rule1', 1, 'case_intrl_id', 'in ',('(Select t.case_intrl_id from kdd_cases t

inner join fcc_precase_case_map pcm on pcm.v_case_id = t.case_intrl_id

inner join fcc_correlation_event_map cor on cor.n_event_correlation_skey = pcm.n_event_correlation_skey
```

```
inner join fcc_event_details s on s.n_event_skey = cor.n_event_skey where
s.N_SCENARIO_SKEY in (XXX,XXX))'));
```

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

19.7.1 Configuring Case Age

Case age can be calculated based on Business Days or Calendar Days by updating the configurable parameter set in the Installation Parameter table, from the Manage Parameters screen.

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

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

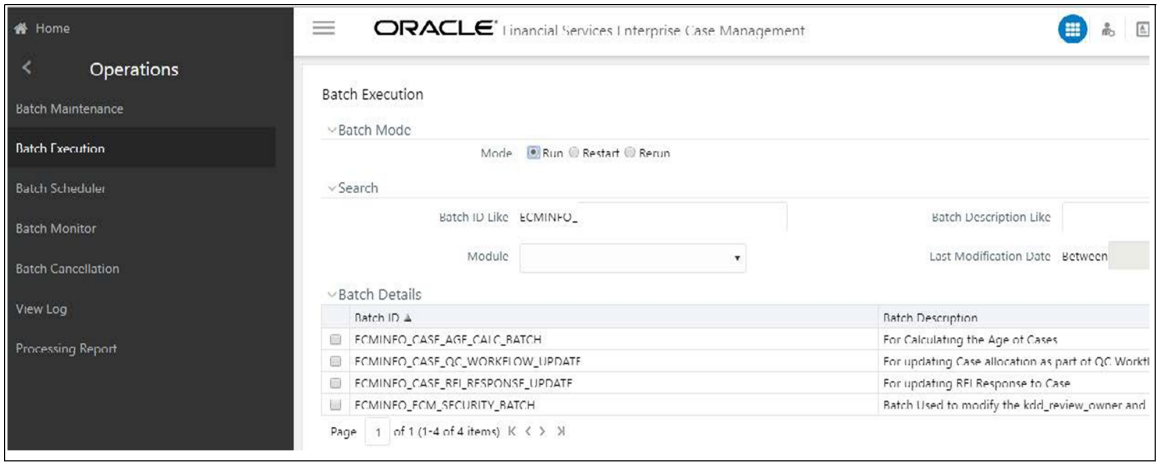
19.7.2 Executing Case Age Calculation Batch

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

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

   Figure 101 shows the Batch Execution page.

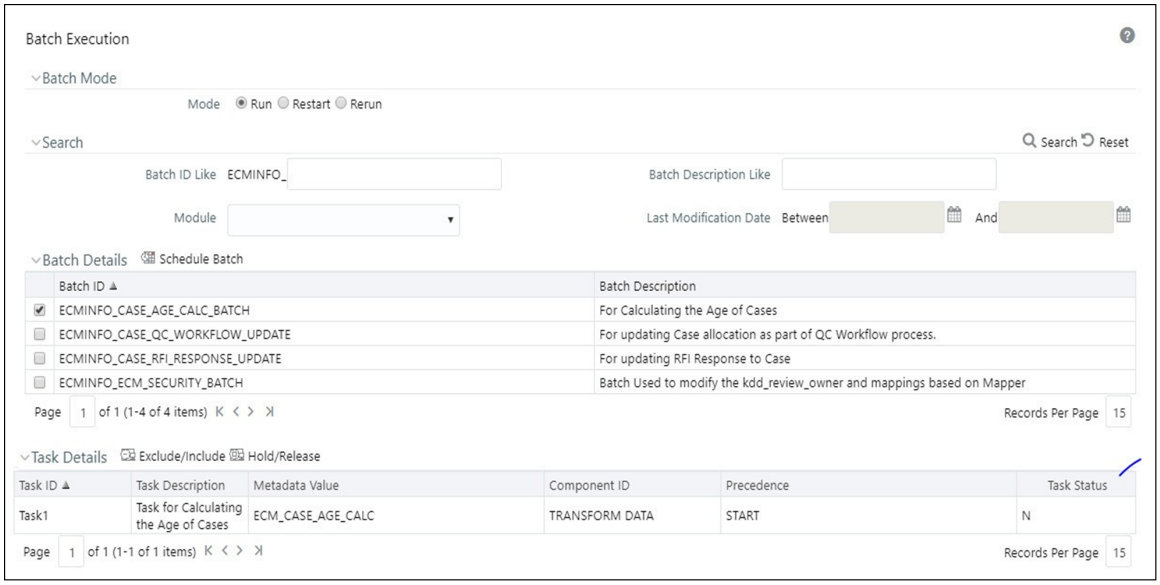
Figure 101: Batch Execution



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

   Figure 102 shows the Execute Batch page.

Figure 102: Execute Batch



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

19.8 Configuring Tabs based on Role

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

1. Identify the tab on which you want to provide the control access to the user (based on Role). Here, ##TAB_NAME## is the placeholder for tab Name.
2. Create an SMS function and map it to the User Role. Or
3. Select the unique Function Code. ##FUNCTION_CODE## is the placeholder for Function Code.
4. Take a backup of following query results from Config schema:

   ```
   select * from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_-
   CONTEXTN' and v_container_name='##TAB_NAME##';
   ```

   ```
   select * from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in
   (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where
   t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='##TAB_NAME##')
   ```

5. Execute following queries in Config schema before replacing the ##placeholder## with correct values:

   ```
   update AAI_FF_FORMS_CONTAINERS_B t set t.v_view_mode=1, t.v_func-
   tion_codes='##FUNCTION_CODE##' where t.v_form_code='CM_CASE_CONTEXTN'
   and v_container_name='##TAB_NAME##'
   ```

   ```
   delete from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in
   (select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where
   t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='##TAB_NAME##')
   ```

6. Restart Application and Web servers.

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

1. Create a function called "TEST".

2. Take a backup of following query from Config schema:

```
select * from AAI_FF_FORMS_CONTAINERS_B t where t.v_form_code='CM_CASE_-
CONTEXTN' and v_container_name='Account';

select * from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in
(select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where
t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='Account')
```

3. Execute following queries in Config schema before replacing the placeholders with correct values. That is, function code as TEST and tab name as Account.

```
update AAI_FF_FORMS_CONTAINERS_B t set t.v_view_mode=1, t.v_func-
tion_codes='TEST' where t.v_form_code='CM_CASE_CONTEXTN' and v_contain-
er_name='Account'

delete from AAI_FF_TAB_DISPLAY_FILTERS tt where tt.n_container_id in
(select t.v_container_id from AAI_FF_FORMS_CONTAINERS_B t where
t.v_form_code='CM_CASE_CONTEXTN' and t.v_container_name='Account')
```

4. Restart Application and Web servers.

19.9 Adding Standard Comments for Event Decision

If you want to add a new standard comment for event decisions in the Set Event Decision window, then update the KDD_CMMNT and KDD_CASE_TYPE_CMMNT tables. The standard comments can be seeded in the KDD_CMMNT table against CMMNT_CAT_CD=EVNT. These comments can be mapped against case type in the KDD_CASE_TYPE_CMMNT table. This is applicable for both Relevant and Non-Relevant decision.

The newly added standard comments will display in the Standard Comments drop-down list of the Set Event Decision window. These changes will be recorded in the Audit History tab.

19.10 Adding Event Decision for Customer Screening

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

To add a new status value, add the entries into FCC_EVENT_STATUS_B, FCC_EVENT_STATUS_TL, FCC_CASETYPE_EVENT_STATUS_MAP tables and make a corresponding entry into the KDD_ACTION

table describing the new status added. Mapping of that status has to be provided in the KDD_INSTALL_PARAMS table as described in Table 74 :

Table 74: KDD_INSTALL_PARAMS table

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

Status ID populates from FCC_EVENT_STATUS_B and Action ID comes from KDD_ACTION. These changes will be recorded in the Audit History tab.

19.11 Adding Search Results Fields based on Case Type

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

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

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

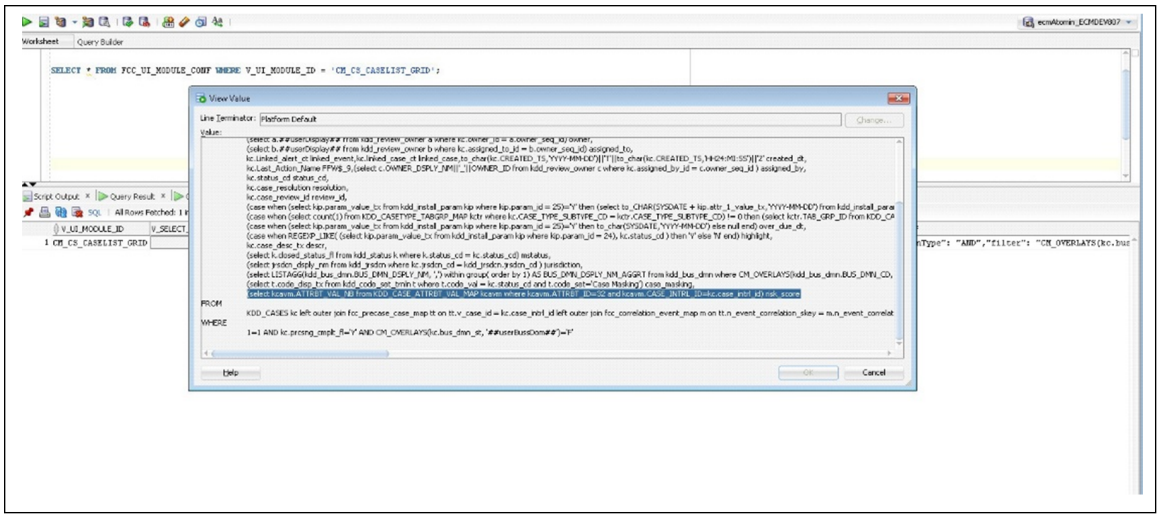
Below example shows adding a new column 'Risk Score' to the existing case type:

1. Update the select query that defines all fields that are returned in the search results to include the new field.

   In table FCC_UI_MODULE_CONF where V_UI_MODULE_ID equals to CM_CS_CASELIST_GRID, update the V_SELECT_QUERY field to include the new column in the select part of the query. In this example, we are adding 'risk_score'.

   Figure 103 shows the Adding Risk Score screen.

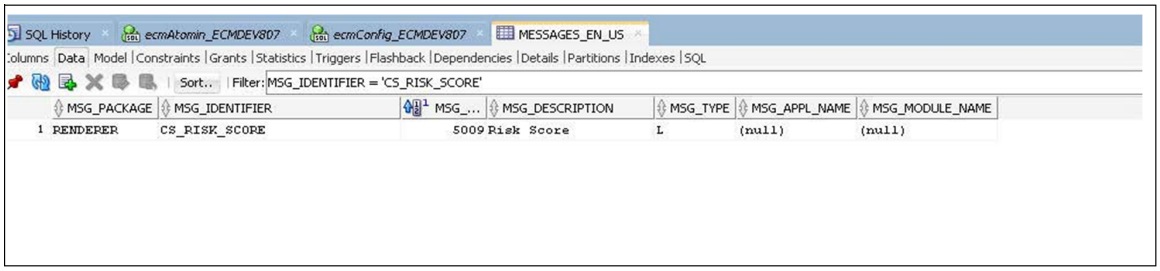
Figure 103: Adding Risk Score



2. The header label for the above column (that is, 'risk_score') needs to be rendered from the MESSAGES_EN_US table. If it is not already listed, then make an entry in the MESSAGES_EN_US

table (with config schema) with the MSG_IDENTIFIER as 'CS_RISK_SCORE' and MSG_PACKAGE as 'RENDERER' as shown in Figure 104 .

Figure 104: MESSAGES_EN_US table



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

   ```
   "key": "risk_score", "locale_code":"RENDERER.CS_RISK_SCORE", "align": "right",
   ```

   ```
   "headerAlign": "left", "width": "0.08",
   ```

   ```
   "dataType": "float", "displayType": "number", "draggable":true, "resizable":true,
   ```

   NOTE

   - 'key' property should match with the 'alias' name given in the query defined in Step 1.
   - The 'locale_code' is the label for the column header and it is rendered from the MESSAGES_EN_US table as explained in Step 2. It follows the convention [MSG_PACK- AGE].[MSG_IDENTIFIER] from the MESSAGES_EN_US table.

     For the new column, 'visible' property should be set to False.

     For the new column, 'addToColMenu' property should be set to False.

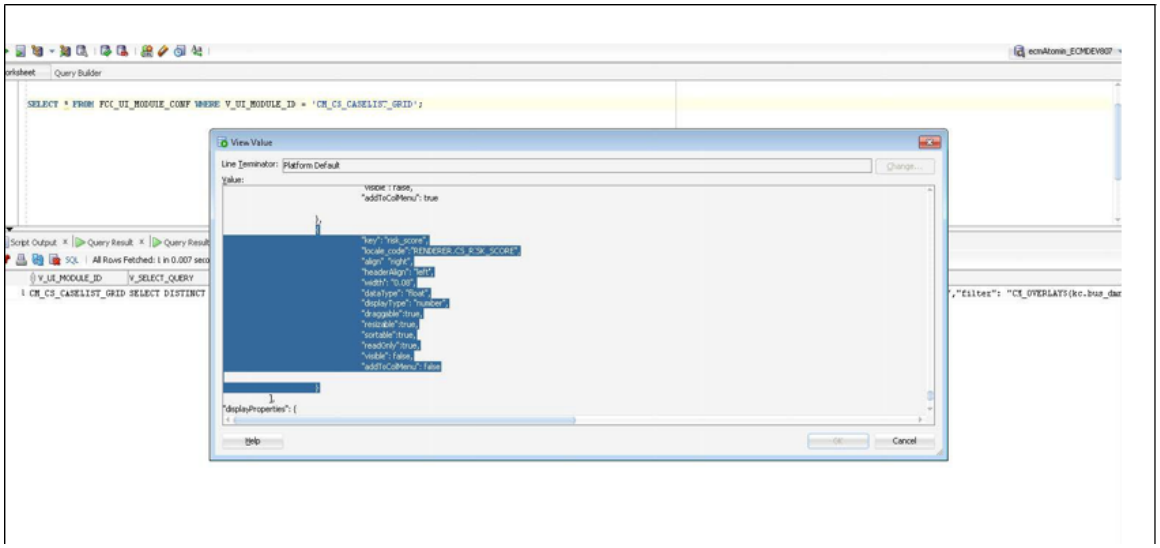
     The other variables define the column's functionality.

     If multiple case types are selected to be searched on that have conflicting search results a default set of fields are displayed, then set the "visible" and "addToColMenu" to True to show this field in that default setting.

   ```
   "sortable":true, "readOnly":true, "visible": false, "addToColMenu": false
   ```

4. Define the new field in table KDD_CASEATTRBT_MASTER and then enter it in table KDD_CASE-ATTRBT_COLMNID_MAP as shoen in Figure 105 .

Figure 105: Defining the KDD_CASEATTRBT_MASTER table



5. Assign the new column ID to the applicable case types and define the order. Define the visible as default, if required. Map all the required column IDs to the selected case type in the KDD_CASE-TYPE_COLMNID_MAP table as shown in Figure 106 .

Figure 106: KDD_CASE- TYPE_COLMNID_MAP table

KDD_CASEATTRBT_COLMNID_MAP

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

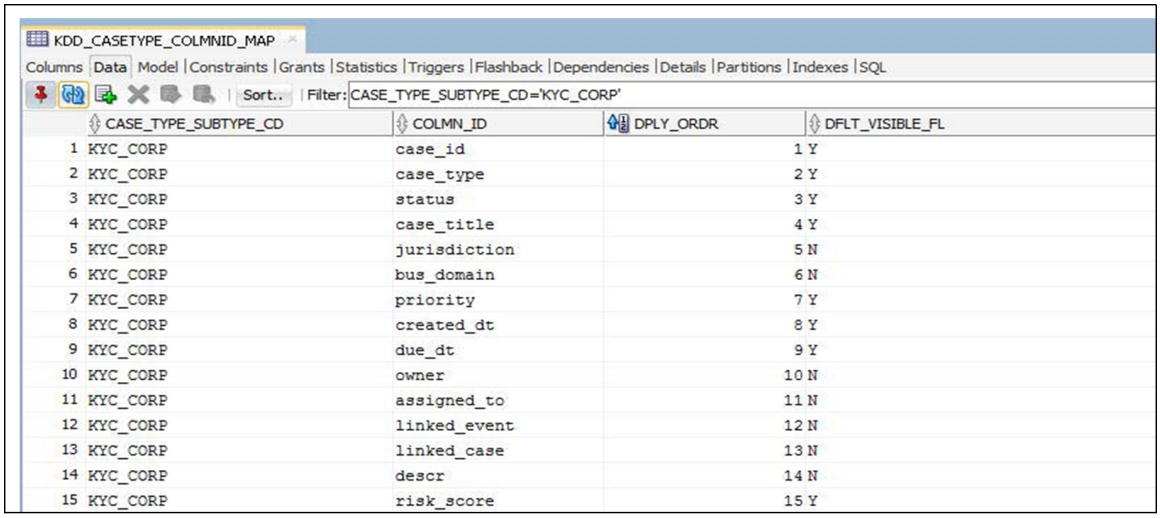
Sort.. | Filter:

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

6. After adding these columns for a new Case Type, create the new Case Type. If the new Case Type is created already or adding columns for an existing Case Type, then re-load the Case Designer screen and edit. Again save the Case Type as shown in Figure 107 .

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

Figure 107: KDD_CASE- TYPE_COLMNID_MAP table



KDD_CASETYPE_COLMNID_MAP

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

Sort.. | Filter: CASE_TYPE_SUBTYPE_CD='KYC_CORP'

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

7. Verify the configuration on the Search Case page.

19.12 Adding and Configuring Case Type Attribute

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

1. Define the type of attribute in the ATTRBT_TYPE_CD column.

   The following types are available:

   - Text box: Allows for string values
   - Hierarchy: The field brings the data from another table. The table it pulls from is defined in Case Attribute Value (KDD_CASEATTRBT_VAL). In this table, the following should be defined

for each hierarchy attribute. It is not possible at this time to have nested hierarchy drop-downs.

- The first row defines the table where the values should be retrieved.
- The second row is the ID attribute
- The third row defines which column to show in the drop-down list
- The fourth row is a Yes/No values to define if the multiple select options should be shown for the drop-down.
- The fifth row is used to specify the filter ('Where' clause) for the table if any is needed.
- The sixth row is used to specify the order by attribute. If not specified, it orders the values based on the description or shown column (third-row value).

- Drop-down: This is used for defining a finite set of values that do not come from a table. The Case Attribute Value table is also used to define the list. For each attribute, there should be one row for each value in the drop-down. The Drop-down will always be single select.
- Date: The format of the date field is defined in the ATTRBT_DT_FRMT column of the table.
- Textarea: Allows for text areas
- Checkbox: Allows for any number of values to be check-box options. The Case Attribute Value table is also used to define the list. For each attribute, there should be one row for each value that needs a checkbox. Checkbox attributes are multi-select
- Number: The number field automatically comes with the up/down arrows when displayed.
- Derived: This type allows you to derive the attribute from information related to the case in the case. Derived Attributes are only visible in the Case Context Area of the case. They are not shown on the Manual Case Creation page or the search page (even if configured as

such). They are also read-only in format. Any value can be derived as long as it can be obtained from the Case ID.

> **NOTE** If the attribute is mandatory for all case types, then the ATTRBT_MNDTRY_FL column is set to Y for that attribute.

2. For Derived type attributes code, define the query that retrieves the value. Enter the query into the ATTRBT_VAL column of the **KDD_CASEATTRBT_VAL** table. Both request and session parameters are supported. You can specify them using the below notation:
   - Request Parameter: @@ ParameterName@@
   - Session Parameter: ## ParameterName##
3. Define the behavior of each attribute that is how it behaves in the UI need to be defined. Define this in Case Attribute Behavior table **KDD_CASEATTRBT_BHVR**. Define the following page codes in the **PAGE_CD** column for every attribute:
   - Case Designer: Controls the attribute's behavior in Case Type Designer
   - Create: Controls the attribute's behavior in Manual Case Creation
   - Modify: Controls the attribute's behavior in the Case Context
   - Operator: If the attribute is a number field this controls if there is an operator in the search field for this attribute. Currently available operators are Greater than Equal to, Less than Equal to, and Equal To.
   - Search: Controls the attributes behavior in Case Search
4. Define the behavior of each page code in the ATTRBT_MODE_NB column:
   a. 1: Editable
   b. 2: Disabled
   c. 3: Hidden
5. For derived type attributes, a record for each page code needs to be added to the KDD_CASEAT-TRBT_BHVR table. You can define the following modes:
   - CaseDesigner: 1
   - Create: 3
   - Modify: 2
   - Operator: 3
   - Search: 3

19.12.1 Adding and Configuring Search Attributes

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

There are the following two types of Search attributes:

- Generic Search Attribute
- Case Type Specific Search Attributes

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

1. KDD_CASE_ATTRBT_VAL_MAP table (Pure Optional Attribute):
   - This type of search attribute performs the search only on the optional attributes present in KDD_CASE_ATTRBT_VAL_MAP. Example: Risk Score.
2. Searching on a field stored in any other table:
   - This type of search attribute performs the search on any table like KDD_CASES, KDD_-CASE_ACTIONS, or any other table which can be filtered based on join with KDD_CASES's CASE_INTRL_ID column.

19.12.1.1 Generic Search Attribute

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

Perform below additional changes in <<deployedir>>/ ojff/js/viewModels/searchCase.js

to customize the generic search attributes:

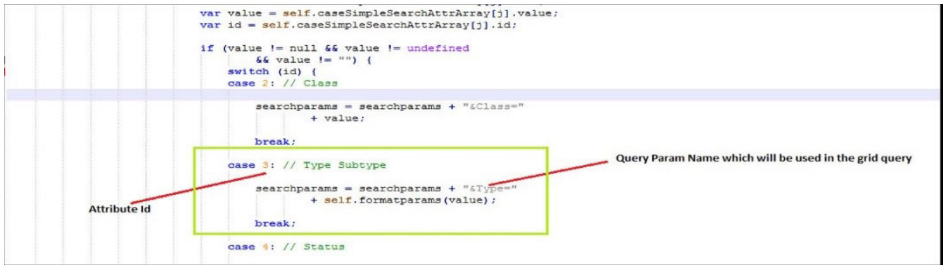
1. Add the Search Attribute in the **simpleSearchAtrArray** for the respective Attribute ID. Enter the attribute ID in this array in the order you want it to appear as shown in Figure 108 .

Figure 108: simpleSearchAtrArray



2. Add the search parameter passing code for respective Attribute ID under **self.buttonClickSimpleSearch** function as shown in Figure 109 .

Figure 109: self.buttonClickSimpleSearch



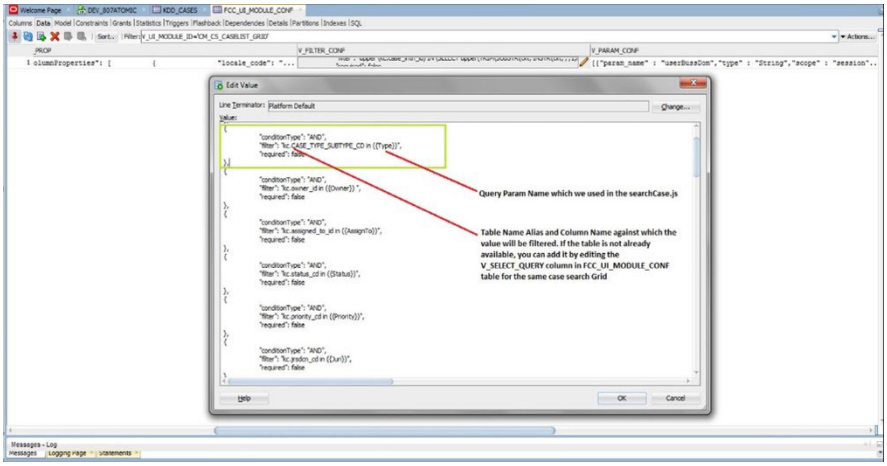
3. Add the search parameter passing code for respective Attribute ID under **self.buttonClickSearch** function as shown in Figure 110 .

Figure 110: self.buttonClickSearch



4. Configure the search parameter in the FCC_UI_MODULE_CONF table for V_UI_MODULE_ID='CM_CS_CASELIST_GRID'. To configure, the V_FILTER_CONF entry should be updated with the JSON object for the new search parameter as shown in Figure 111 .

Figure 111: Parameters



19.12.1.2 Case Type Specific Search Attributes

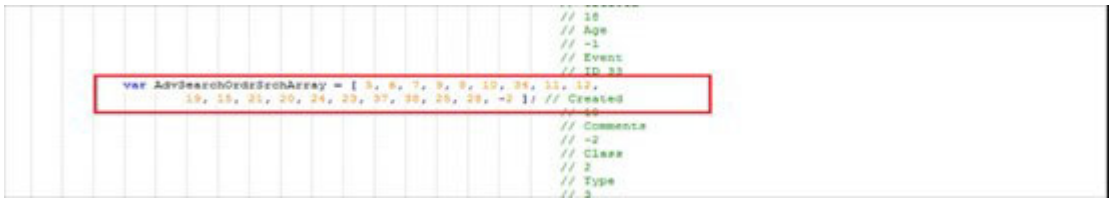
This type of search attribute applies only to the Case Type to which it is associated. It will be shown only in the Optional Attribute Area in More Criteria Section and only when the user selects a Case Type. An example is Risk Score which is displayed when the KYC Case Type is selected.

Perform below additional changes in <<deployedir>>/ ojff/js/viewModels/searchCase.js

To customize the search attributes:

1. Add the Search Attribute in **AdvSearchOrdrSrchArray** for the respective Attribute ID. Enter the attribute ID in this array in the order you want it to appear as shown in Figure 112 .

Figure 112: AdvSearchOrdrSrchArray



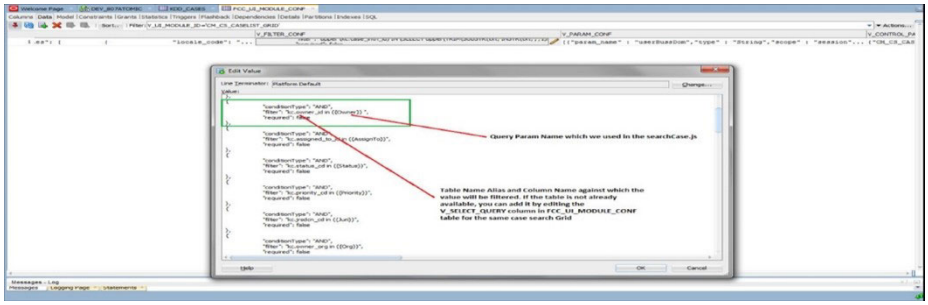
2. Add the search parameter passing code for respective **AttributeId** under **self.buttonClick-Search** function as shown in Figure 113 .

Figure 113: AttributeId



3. Configure the search param in the FCC_UI_MODULE_CONF table for V_UI_MODULE_ID='CM_CS_CASELIST_GRID. To configure, the V_FILTER_CONF entry should be updated with the JSON object for the new search parameter as shown in Figure 114 .

Figure 114: Search Parameter



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

Perform the following additional changes in <<deployedir>>/ ojff/js/viewModels/searchCase.js

to customize the Case Type Specific Search Attribute whose search is based on any other table:

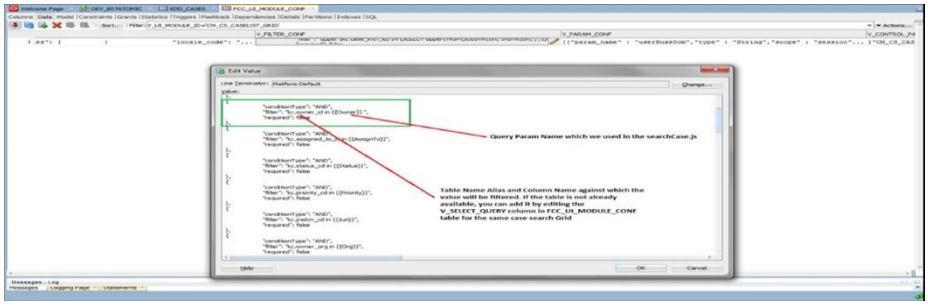
1. Add the search param passing code for respective Attribute ID under **self.buttonClickSearch** function as shown in Figure 115 .

Figure 115: self.buttonClickSearch



2. Configure the search param in the FCC_UI_MODULE_CONF table for V_UI_MODULE_ID='CM_CS_CASELIST_GRID. To configure, the V_FILTER_CONF entry should be updated with the JSON object for the new search param as shown in Figure 116 .

Figure 116: Search Parameter



19.12.2 Adding and Configuring Derived Attribute

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

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

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

1. Define the basic attribute details in KDD_CASEATTRBT_MASTER with type as "Derived" as shown in Figure 117 .

Figure 117: KDD_CASEATTRBT_MASTER table

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

2. Below is the request attribute passed as part of OOB to the getCaseDetails Service: caseId (CaseId of the case whose details page is currently accessed) as shown in Figure 113 .

Figure 118: Passed Request Attribute

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

3. Define the behavior of the attribute in the KDD_CASEATTRBT_BHVR table as shown in Figure 118 :

Figure 119: KDD_CASEATTRBT_BHVR table

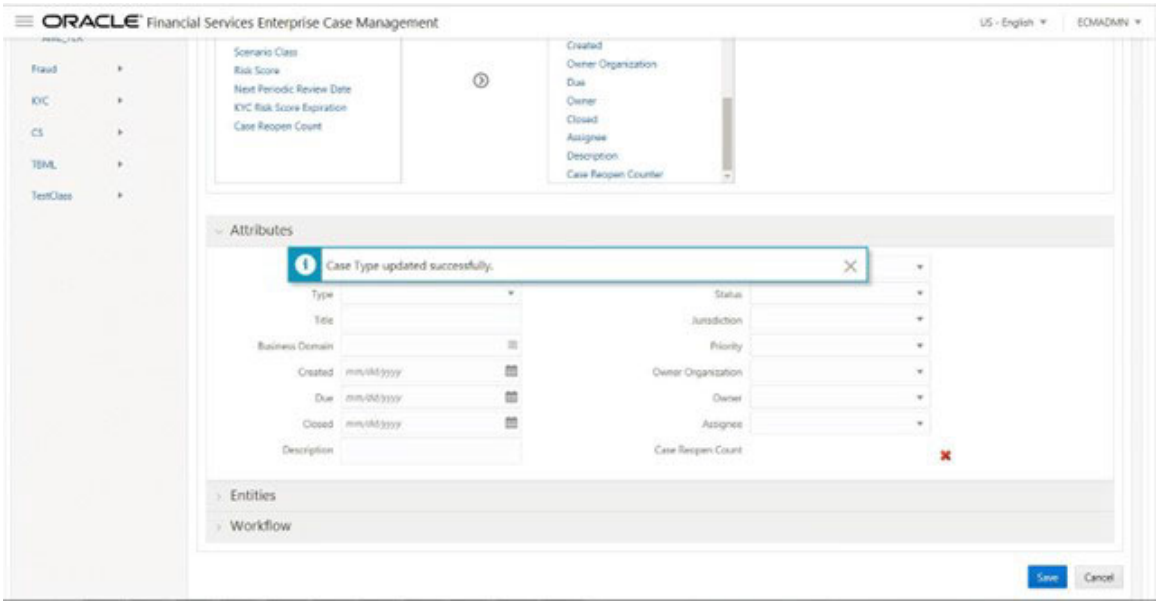
ATTRBT_ID	PAGE_CD	ATTRBT_MODE_NB
39	CaseDesigner	1
39	Create	3
39	Modify	2
39	Operator	3
39	Search	3

The derived attribute is supported only in Case Designer (for associating/Disassociating) the derived attributes to case types and in Case Details Page (Modify Page) for showing the derived attribute value.

Derived Attributes are not displayed on the Create/Search page even if configured as visible in the KDD_CASEATTRBT_BHVR table. Also, Derived attributes will be displayed in a read-only format.

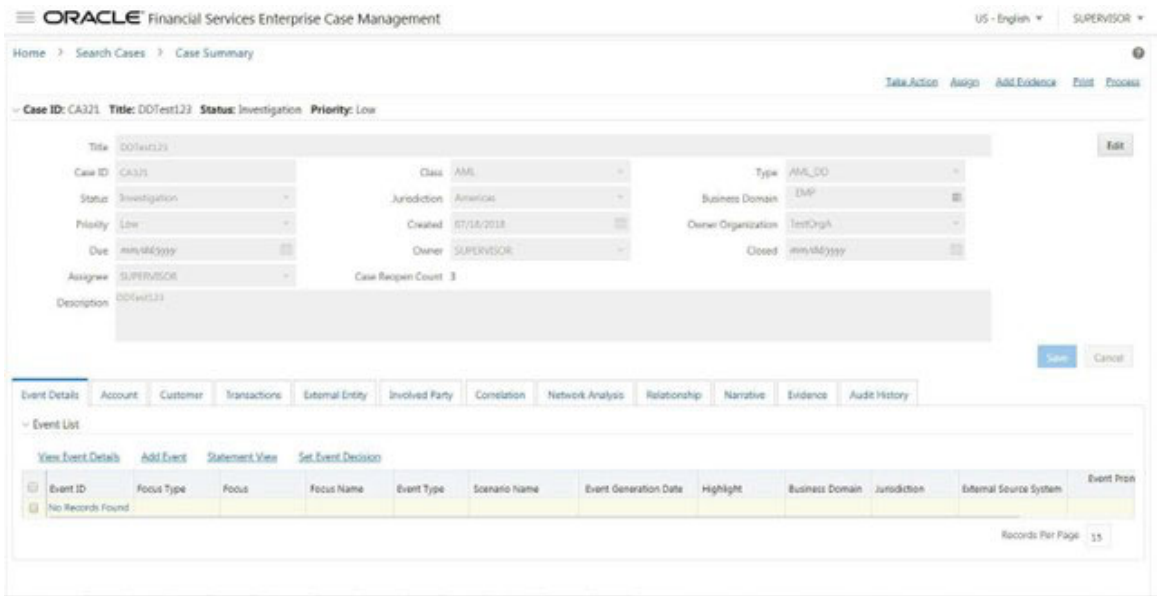
4. Associate the newly created attribute to the required case type using Case Designer UI as shown in Figure 119 .

Figure 120: Case Designer UI



5. Log in as a supervisor and check the Case details of the respective case type for which you have added the derived attribute as shown in Figure 121 .

Figure 121: Added Derived Attribute



19.12.3 Configuring Hierarchy Options based on Another Hierarchy Attribute

If a user selects a value in one case attribute then a second attribute filters its display values based on that selection.

For example: Case Type can filter a Standard Comments drop-down.

Table 75 shows the hierarchy dependency mapping.

Table 75: KDD_CASEATTRBT_HIERARCHY_DEP

Column Name	Column Type	Usage
N_PARENT_ATTRBT_ID	NUMBER(22,0)	This column is used to capture the parent hierarchy attribute ID.
N_CHILD_ATTRBT_ID	NUMBER(22,0)	This column is used to capture the child hierarchy attribute ID.

`N_PARENT_ATTRBT_ID` and `N_CHILD_ATTRBT_ID` are the primary keys.

Now to further define the relationship via query we can define in the `KDD_CASEATTRBT_VAL` table wherein we will have one more row (that is `ATTRBT_SEQ_NB = 7)` . This will capture the additional where clause for the dependent field value from the Parent.

For example: If the Parent Attribute ID is 3 (Case Type) and Child Attribute ID 4 then we mention it as `KDD_CASEATTRBT_VAL. ATTRBT_SEQ_NB =7`

`KDD_CASE_TYPE_SUBTYPE.CASE_TYPE_SUBTYPE_CD in (@@3@@)`

Once we have dependency captured, this information is made available to our Create Case, Search Case, and Case Context screens.

This mapping implies that when user selects the value in the Parent Attribute then the options in the Child Attribute will be filtered based on the values selected in the Parent.

19.12.4 Configuring the Case Title

During the Batch execution, all the cases will be updated with a common Case title (correlation rule name) thereby making it difficult to identify a case. To resolve this, you can update the values in the

V_CASE_TITLE_RULE field of FCC_CORRELATION_RULE, and add a task manually before batch execution.

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

To configure the case title, follow these steps:

1. Update the values in the V_CASE_TITLE_RULE field of FCC_CORRELATION_RULE. For example, customerName, eventType.

   For more information on the FCC_CORRELATION_RULE table, see Configuring Correlation section.

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

   AML: focusType, focusEntityName

   For example, ACCOUNT-YUV: CUSTOMER-CUSTOMER_NAME: ACCOUNT-SAPNA GOBA: ACCOUNT-SMITH

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

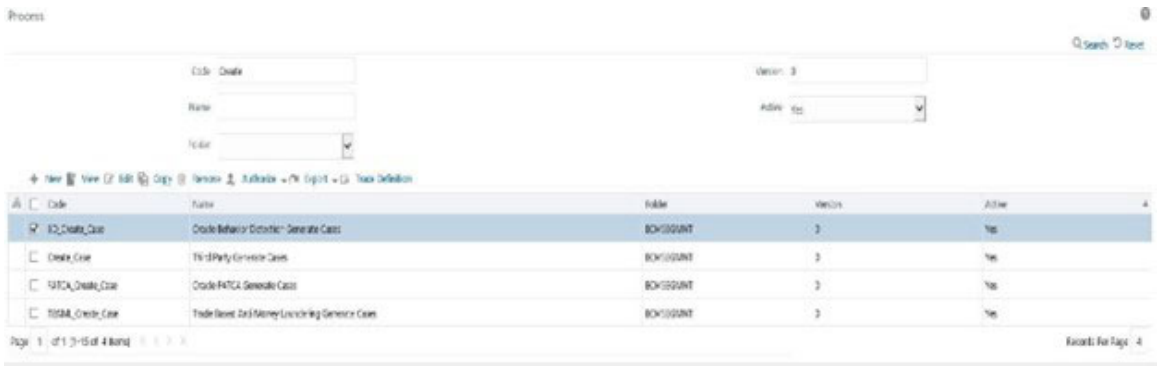
   CS: customerName, eventType

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

   KYC: customerName, kycRiskScore, jurisdiction, businessDomain

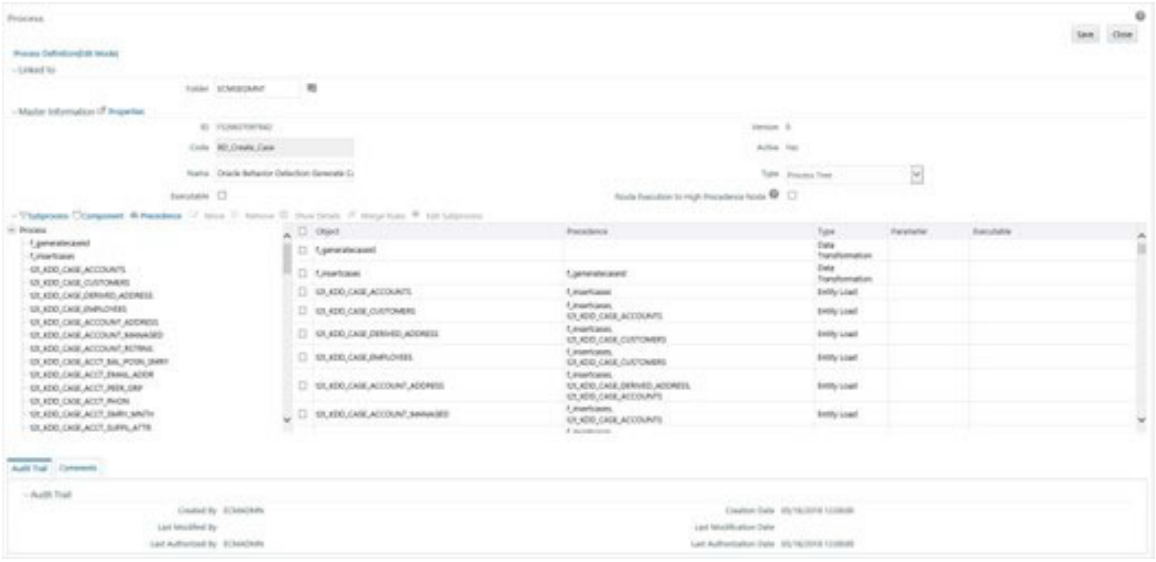
2. Create a task case title manually under BD_Create_Case/Create_Case process before batch execution.
3. Navigate to Enterprise Case Management Application.
4. Go to the Common task section. Select the **Run Rule Framework**.
5. Click **Process**. The Process window is displayed with the available Processes. Search for 'Create process'. The list of processes will be displayed as shown in Figure 122 .

Figure 122: List of Processes



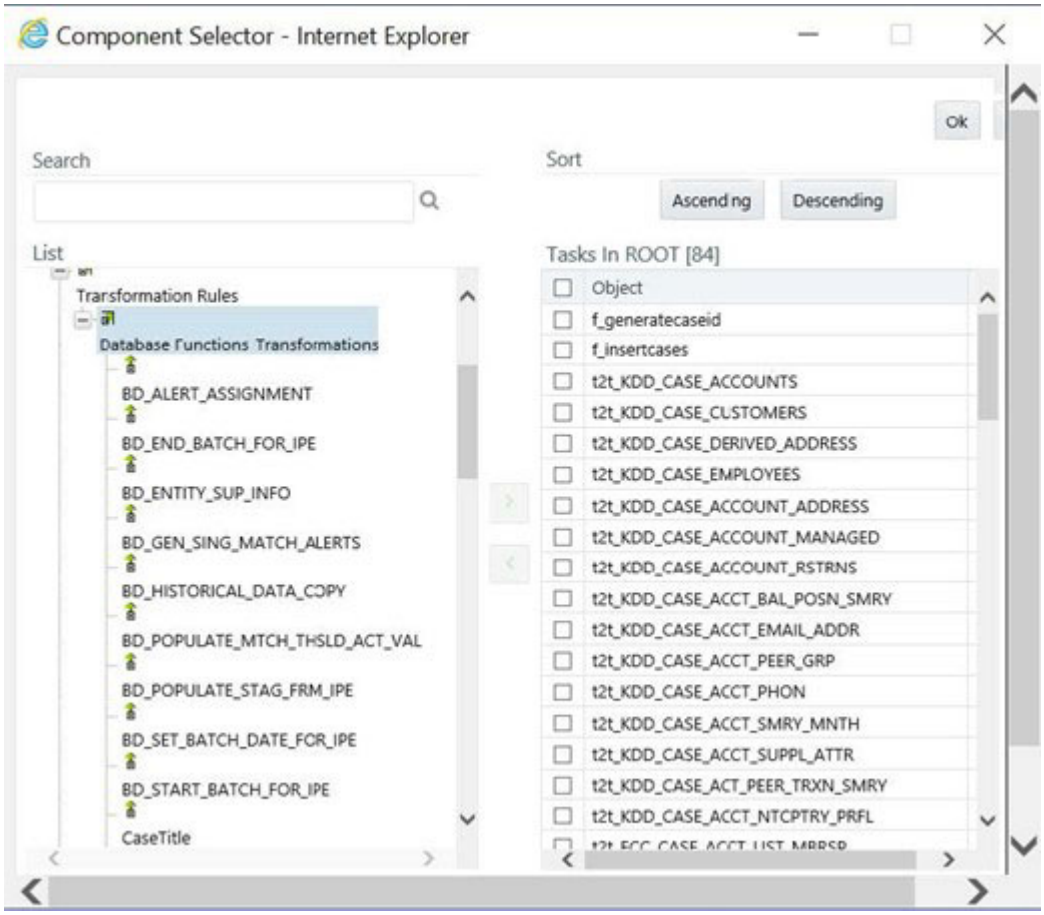
6. Select the BD_Create_Case and click **Edit** as shown in Figure 123 .

Figure 123: Edit Process



7. Click **Component**. The Component Selector window is displayed. Under **Transformation Rules**, select CaseTitle and move it to the task list as shown in Figure 124 .

Figure 124: Component Selector



8. Set the precedence of the task after f_insertcases.

19.12.5 Configuring Case Title for Case Creation (Create Event and Promote to Case) API

This feature is available only for AML, CS, and KYC_OB case types.

Case title can be configured for the API-created cases by configuring the required parameters available in the FCC_CORRELATION_RULE table before Case Creation API execution.

The value defined in this field will be populated on the UI after Case Creation API execution.

To configure the case title, in the FCC_CORRELATION_RULE table, go to the required N_CORRELATION_RULE_SKEY, and update the values under the V_CASE_TITLE_RULE field.

For example:

N_CORRELATION_RULE_SKEY = 21

V_RULE_NAME = AML_Events_Processing_Rule

V_CASE_TITLE_RULE = AML:focusType,focusEntityName

For more information, see Configuring the Case Title.

For KYC OB cases, the values are as follows:

N_CORRELATION_RULE_SKEY = 18 (KYC_OB case type)

V_RULE_NAME = Events_Assessment_Rule

V_CASE_TITLE_RULE = KYC:customerName,kycRiskScore,jurisdiction,businessDomain

For CS cases, the values are as follows:

N_CORRELATION_RULE_SKEY = 12 (CS_RT_SAN case type)

V_RULE_NAME = RT Screening rule - SAN

V_CASE_TITLE_RULE =

For more information on API services, see the Create Event and Promote to Case section in OFS ECM API and Services 8.1.2.6.0.

19.13 Configuring a Case as Read Only

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

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

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

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

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

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

19.14 Adding a New Scenario

Users can define their own scenarios in the FCC_SCENARIO_MASTER table as described in Table 76

Table 76: FCC_SCENARIO_MASTER Table

Column Name	Description	Primary Key	Column Type
N_SCENARIO_SKEY	Unique Sequence ID	Y	NUMBER(22)
V_SCENARIO_NAME	Name of the Scenario		VARCHAR2(250 CHAR)
V_SCENARIO_DESCRIPTION	Description of the Scenario		VARCHAR2(4000 CHAR)
V_SCENARIO_CLASS_CD	Class of scenario		VARCHAR2(250 CHAR)
V_SCENARIO_DISPLAY_NAME	Display name of the scenario		VARCHAR2(250 CHAR)
V_SCENARIO_CATALOG_ID	Catalog ID of scenario		VARCHAR2(250 CHAR)
V_SCENARIO_FOCUS_ENTITY_CD	Focus entity code of the scenario		VARCHAR2(250 CHAR)
N_SCENARIO_SCORE	Scenario score. This column can be Null.		NUMBER(22)
ORIG_SCENARIO_SKEY	Scenario ID from the Source system		NUMBER(22)

19.15 Configuring Quality Control (QC) Sampling Rules

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

To add a QC sampling rule:

1. Add the entries in the KDD_QC_RULE_MASTER table as shown in Table 77 . This table is used to define the overall structure of the sampling rules.

Table 77: KDD_QA_RULE_MASTER Table

Column Name	Primary Key	Column Type	Nullable
RULE_ID	Y	NUMBER(10)	
RULE_NM		VARCHAR2(1000 CHAR)	Y
RULE_DESC		VARCHAR2(4000 CHAR)	Y
SAMPLE_QNTITY_TYPE		VARCHAR2(300 CHAR)	Y
SAMPLE_QNTITY		NUMBER(10)	Y
DS_ID		NUMBER(10)	Y
ACTIVE_FL		VARCHAR2(1 CHAR)	Y
LAST_UPDATED_DT		DATE	Y
LAST_UPDATED_BY		VARCHAR2(20 CHAR)	Y
COMMENTS		VARCHAR2(4000 CHAR)	Y
PRIORITY_CD		NUMBER(10)	Y
ACTION_CD		VARCHAR2(20 CHAR)	Y

- **RULE_ID**: Unique identifier of the rule.
- **RULE_NM**: Name of the rule. This should be a unique name.
- **RULE_DESC**: Description of the rule.
- **SAMPLE_QNTITY_TYPE**: Define the quality type as PERCENTAGE or COUNT.
  - Enter PERCENTAGE if the system has to select a percentage of cases for QC from the candidate superset.
- Enter COUNT if the system has to select a specific count of cases for QC from the candidate superset.

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

2. Add the dataset entries in the KDD_QC_DATASET_MASTER table as described in Table 78 . This table is used to define the dataset associated with each rule.

Table 78: KDD_QC_DATASET_MASTER Table

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

- **DS_ID**: Unique identifier of the dataset that is associated with the rule. The dataset contains the sampling logic (SQL query) for the rule. This field references the DS_ID column in

KDD_QC_RULE_MASTER and KDD_QC_DATASET_VALUES tables.

- **DS_NM**: Name of the dataset. This should be a unique name.
- **DS_DESC**: Description of dataset
- **ACTIVE_FL**: This flag indicates whether or not this dataset can be used during the QC batch. If set to "Y", the system will run this rule during the QC batch. If set to "N", the system will ignore this rule when the QC batch is executed. Ideally, you should make sure that if the

ACTIVE_FL on a rule is set to Yes, the ACTIVE_FL on the dataset associated with that rule should also be set to Yes.

- **LAST_UPDATED_DT**: Date when this record was last updated.
- **LAST_UPDATED_BY**: User name who last updated this record.
- **COMMENTS**: Enter the comments

3. Define the dataset values in the KDD_QC_DATASET_VALUES table as described in Table 79 . This table is used to define the actual SQL logic for each dataset.

Table 79: KDD_QC_DATASET_VALUES table

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

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

4. The entries will be updated in the KDD_QC_RULE_XCUTN_AUDIT table as described in Table 80 .

Table 80: KDD_QC_RULE_XCUTN_AUDIT table

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

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

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

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

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

Here, the system also uses the action code defined on the sampling rule to call PMF and assign a resulting (QC) status to the case. These workflows need to be defined in PMF. For more information on PMF, see the Configuring Processing Modelling Framework (PMF) chapter. In out of the box workflows, the QC process is not configured.

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

19.16 Event Purge

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

There are two types of the purge:

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

Below is the list of features:

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

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

remain in the business tab. By default, only events that are part of the case in Extendible status can be purged. The events which are purged will not take part in the future correlation process.

19.16.1 Event Purging Using Tables

Perform the following steps to purge events using table updates:

1. Configure the parameters in table FCC_PURGE_INPUT. In this table, data with the event skey column can be added. For this, follow the below steps:
2. Locate EventPurge.cfg(path: <installed area>/ficdb/conf). Modify the following details:
   - Status: Status of case
   - Batchsize: Defines the maximum size of events in a batch
   - TestMode: If the testmode is True, then data will not be purged but purging is done for testing purpose.
3. Look at the existing table FCC_EVENTS as shown in Table 81 . In table FCC_PURGE_INPUT, the event skey should be the same as mentioned in table FCC_EVENTS.

Table 81: FCC_EVENTS Table

Column Name	Primary Key	Column Type	Nullable
n_err_seq_id		NUMBER	No
n_event_skey		NUMBER(22)	
n_run_skey		NUMBER(22)	
v_user_comments		VARCHAR2(4000 CHAR)	
f_purge_success_flag		CHAR(1 CHAR)	
d_requested_date		DATE	
d_fic_mis_date		DATE	
v_user_id		VARCHAR2(50 CHAR)	
v_data_origin		VARCHAR2(30 CHAR)	
d_prcsng_batch_date		DATE	
v_purge_type		VARCHAR2(20 CHAR)	

- `n_err_seq_id`: Enter the sequence ID. This field accepts only numeric values. This is a mandatory field.
- `n_event_skey`: Enter the skey of the event which you want to purge. This is a mandatory field if it is an individual event purge.
- `n_run_skey`: Enter the run skey of the batch you want to purge. This is a mandatory field if it is a complete batch event purge.
- `v_user_comments`: User comments if required
- `f_purge_success_flag`: Defines the purge success flag. If the purge is failed, then this flag will be displayed as E. By default, it has to be set to Null or N. This flag turns to Y if the

purge is successful. If purge fails (flag = E), then check and correct it, and update this entry as Null or N and again execute the purge.

- `d_requested_date`: Date of individual event purge request
- `d_fic_mis_date`: Date of BATCH. This is applicable only if n_run_skey is defined.
- `v_user_id`: User ID who is performing the purge.
- `v_data_origin`: Define the data region, like US, IND, and so on. This is applicable only for the batch purge. For example, a batch can have data for multiple data origins and if you want to delete data only for the India region, then define the region in this field.
- `d_prcsng_batch_date`: Date on which the purge process request is completed.
- `v_purge_type`: Define the type of purge. It can be a BATCH or EVENT.

4. Execute the following script:

   ```
   EventPurge.sh
   ```

19.16.2 Hint Configuration in Event Purge (EventPurgeConfig.cfg)

The *EventPurgeConfig.cfg* file is available in the #FIC_HOME#/ficdb/conf folder. This contains the list of tables that has to be purged in the following format:

`ActualTableName:PurgeTableName:deleteType:deleteKey`

Eg: `KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id`

The Table-Wise Hint and Global Hint Configurations are introduced to improve Insert/Delete Queries. If Table-wise configuration is available, it will be used; else, Global Hint configuration will be used.

- Table wise Hint Configuration
  - oTo optimize the Insert and Delete queries, the above format will additionally support the optimizer hint for insert and delete operations separated by semicolon (:).You can configure the required hint as per your optimizer:

    `ActualTableName:PurgeTableName`:deleteType:deleteKey:optimizerHintInsert:optimizer HintDelete

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id:/*+ parallel(8) */:/*+ parallel(8) */*
  - To optimize only for insert scripts, use the below format:

    `ActualTableName:PurgeTableName:deleteType:deleteKey:optimizerHintInsert`

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id:/*+ parallel(8) */*
  - To optimize only for delete scripts, use the below format:

    `ActualTableName:PurgeTableName:deleteType:deleteKey::optimizerHintDelete`

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id::/*+ parallel(8) */*
- Global Hint Configuration

  The following configurations must be used to apply any global optimizer hint. You can set up the required hint as per your optimizer.
  - For Delete operation

    `OptimizerHintDelGlobal`: - To apply the optimizer hint to all the tables provided in cfg files for delete scripts.

    E.g. *OptimizerHintDelGlobal:/*+ parallel(4) */*
  - For Insert operation

    `OptimizerHintInsGlobal`:- To apply the optimizer hint to all the table's information provided in cfg files for insert scripts

    E.g. *OptimizerHintInsGlobal:/*+ parallel(4) */*

19.17 Case Purge Utility

Case Purge utility is meant for purging of cases, case-related entity tables, events inside the case and evented table data for those events. The input criteria for purging is Case IDs, Case Created Date Range, Case Last Updated Date Range, and Case Status.

To use case purge utility, perform the following steps:

1. Defining Input Criteria

   The input criteria is defined in FCC_PURGE_CASE_INPUT in Atomic Schema. The criteria can be given in the following manner:

   - Particular Case IDs: If multiple, then give multiple rows
   - Created Date From and To
   - Last Updated Date From and To
   - Created Date From and To and Last Updated From and To

   Table 82 lists the columns in FCC_PURGE_CASE_INPUT where the criteria can be defined:

   Table 82: FCC_PURGE_CASE_INPUT

Criteria	Column Name
Particular Case ID	V_CASE_INTRL_ID
Created Date From and To	D_CREATED_DT_FRM, D_CREATED_DT_TO
Last Updated Date From and To	D_LAST_UPDATED_DT_FRM, D_LAST_UPDATED_DT_TO

   There are some columns in FCC_PURGE_CASE_INPUT which are only informational:

   - N_CASE_PUREG_SEQ_ID: Normal Numeric sequence for the filter/Criteria. Example:1 or 2
   - F_PURGE_SUCCESS_FLAG: This indicates the status of the Purge. It should be null or N for the filter or criteria to be picked up. After the purge is successfully completed it will automatically be updated to Y. If any error occurs during the purge it will be updated to E.
   - D_REQUESTED_DATE: This can be filled as the date when the filter criteria was inserted. It just kept for future use for informational purpose
   - V_USER_ID: This can be filled as the userid running the purge. It is just kept for future use for informational purposes.
   - D_PRCSNG_BATCH_DATE: This is updated by the case purge utility. It will be updated with the date the purge was run.

   The STATUS filter for the purge is captured in the CasePurgeConfig.cfg. The details are mentioned under the Configuration File section below.

2. Configuration File (CasePurgeConfig.cfg)

   This file is available in the #FIC_HOME#/ficdb/conf folder. This contains the list of tables that has to be purged in the following format:

   ```
   ActualTableName:PurgeTableName:deleteType:deleteKey
   ```

   Eg: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id*

   The Table-Wise Hint and Global Hint Configurations are introduced to improve Insert/Delete Queries. If Table-wise configuration is available, it will be used; else, Global Hint configuration

will be used.

- Table wise Hint Configuration
  - To optimize the Insert and Delete queries, the above format will additionally support the optimizer hint for insert and delete operations separated by semicolon (:).You can configure the required hint as per your optimizer:

    `ActualTableName:PurgeTableName:deleteType:deleteKey:optimizerHintInsert:optimizerHintDelete`

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id:/*+ parallel(8) */:/*+ parallel(8) */*
  - To optimize only for insert scripts, use the below format:

    `ActualTableName:PurgeTableName:deleteType:deleteKey:optimizerHintInsert`

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id:/*+ parallel(8) */*
  - To optimize only for delete scripts, use the below format:

    `ActualTableName:PurgeTableName:deleteType:deleteKey::optimizerHintDelete`

    E.g.: *KDD_CASES:KDD_CASES_PE:directDelete:case_intrl_id::/*+ parallel(8) */*
- Global Hint Configuration

  The following configurations must be used to apply any global optimizer hint. You can set up the required hint as per your optimizer.
  - For Delete operation

    `OptimizerHintDelGlobal`: - To apply the optimizer hint to all the tables provided in cfg files for delete scripts.

    E.g. *OptimizerHintDelGlobal:/*+ parallel(4) */*
  - For Insert operation

    `OptimizerHintInsGlobal`:- To apply the optimizer hint to all the table's information provided in cfg files for insert scripts

    E.g. *OptimizerHintInsGlobal:/*+ parallel(4) */*

    `OptimizerHintUpdtCaseTemp`:-To optimize insertion in the temp table FCC_PURGE_CASE_UPDTCNTINP_TEMP which is not in the cfg file but handled internally as part of the temp table population.

    E.g. *OptimizerHintUpdtCaseTemp:/*+ parallel(4) */*

  Following delete types are supported:
  - directDelete: Any table where data can be deleted directly (basically which has either case_intrl_id or n_event_correlation_skey or n_event_skey). For case_intrl_id since it appears with different names in different tables we have handled column names like case_intrl_id, v_case_id, parent_case_id . You can directly configure Direct Delete if on any of these columns mentioned for any new tables provided the new table and its purge table exists in the schema.
  - logicalDelete: Any table which requires join to find the case_intrl_id. For example: KDD_CASE_ACTION_NOTE. As of now we support logical deletion based on action_seq_id or note_id. In logical Delete, clients can configure delete for any new

tables which is based on action_seq_id or note_id provided the new table and its purge table exists in the schema.

- eventedEntityDelete: Any evented table which requires join on basis of mis_date,data_origin,entityskey,entitytype. The config should be given in following format

  ActualTableName:PurgeTableName:eventedEntityDelete:misdatecolumnname,dataorigincolumnname,skeycolumnname,entitytype.

  Example:FCC_ACCT_EVNT:FCC_ACCT_EVNT_PE:eventedEntityDelete:mis_date,data_origin,account_skey,ACCOUNT .

  oEvented Entity Delete can be configured directly by the customer for any new tables provided the new table and its purge table exists in the schema.

The configuration file also captures the STATUS filter to decide which case statuses should be picked. Statuses should be given in single quotes and multiple statuses should be comma-separated. For example: STATUS:'NW','INV'.

The configuration file has the following additional configurations:

- TESTMODE: If false, the temp tables created during purge will be dropped and the purge action will be committed. If true, the temp tables won't be dropped and the purge won't be committed. OOB value will be false. This flag is useful when analysis or debugging needs to be done by QA on which cases and events got picked for purge.
- CheckPurgeTablesDM: To check the Data Model of CM and CM_PE tables to bring it in sync, we call "compare_tables" proc for this. The list of tables compared is picked from the TEMP_COMPARE_TABLES table in the atomic schema. This supports only alter that is creation of the column if it's not present in the PE(Purge) table. It doesn't support modification to existing columns or drop of columns. Also, it doesn't support the creation of purge tables. OOB value will be true. If true it checks the data models. If false it doesn't check.
- BatchSize: This is used to do periodic batch executions based on the size. OOB value is 200.

3. Important Temp tables created during Purge

   Below temp tables are created during purge. These tables won't be dropped when testmode is true and helps in analyzing which cases and events got picked up during purge

   a. FCC_PURGE_CASE_INPUT_TEMP

      This table contains the eligible caseids for purge. The eligibility for delete is denoted by the f_delete_case column as Y. It also shows the number of events inside the case and also the event correlation skey.

   b. FCC_PURGE_CASE_EVNT_INPUT_TEMP

      This table contains the eligible eventids for purge. The eligibility for delete is denoted by f_delete_event column as Y.

   c. FCC_PURGE_CASE_EVNT_ENT_TEMP

      This table contains the eligible evented entities for purge.

4. Execution

   After doing the configuration as mentioned above, trigger the <<ficdb>>/bin/CasePurge.sh.

   Logs are generated in <<ficdb>>/log/CasePurge/CasePurge.log. Insert and Delete Scripts for reference and informational purpose is generated with timestamp at <<ficdb>>/CasePurge.

19.18 Event Expiry

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

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

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

19.18.1 Identifying Events by Age

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

- Age
- Event Type
- Jurisdiction
- Domain

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

19.18.2 Identifying Events by Score

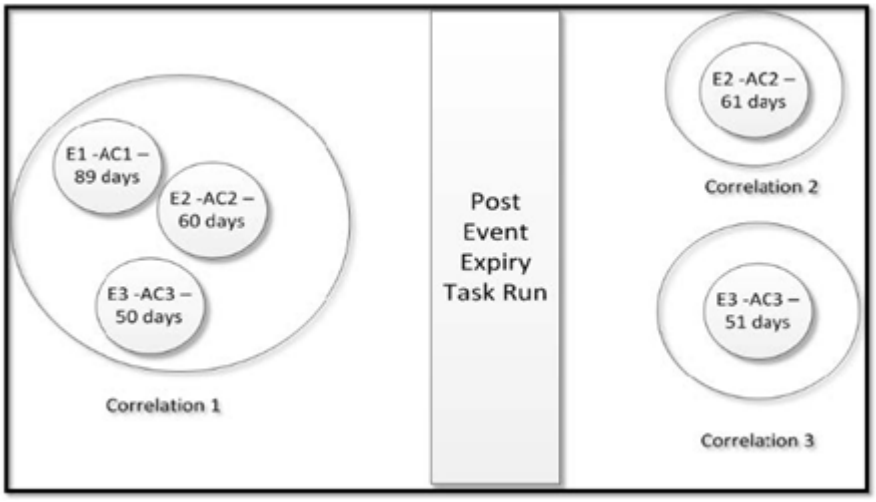
Events that need to be expired can be identified through event score.

19.18.3 Examples

Following is the list of examples:

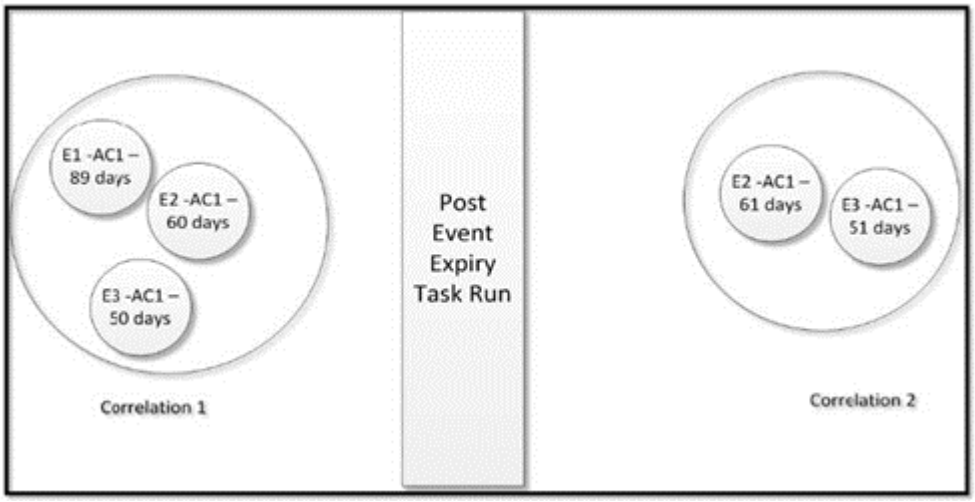
1. In the below example, Event E1, E2, and E3 are correlated in Correlation 1. When the task for Event expiry is executed, Event E1 will be out of the case correlation based on the defined IPE rule. Event E2 and Event E3 will be correlated to Correlation 2 and Correlation 3 respectively as shown in Figure 125 .

Figure 125: Example 1



2. In the below example, Event E1, E2, and E3 are correlated in Correlation 1. When the task for Event expiry is executed, Event E2 will not be promoted to the case based on the defined IPE rule. Event E1 and Event E3 will be correlated together in Correlation 2 as shown in Figure 126 .

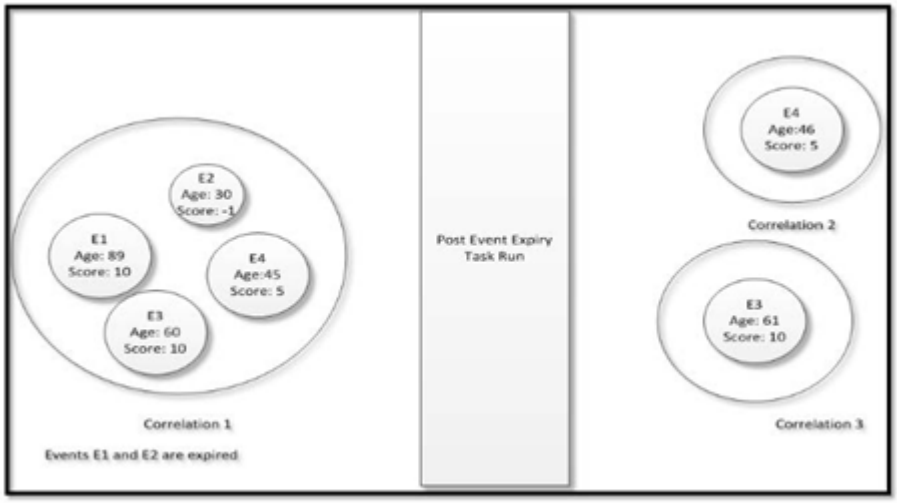
Figure 126: Example 2



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

scoring. Event E3 and Event E4 will be correlated to Correlation 2 and Correlation 3 respectively as shown in Figure 127 .

Figure 127: Example 3



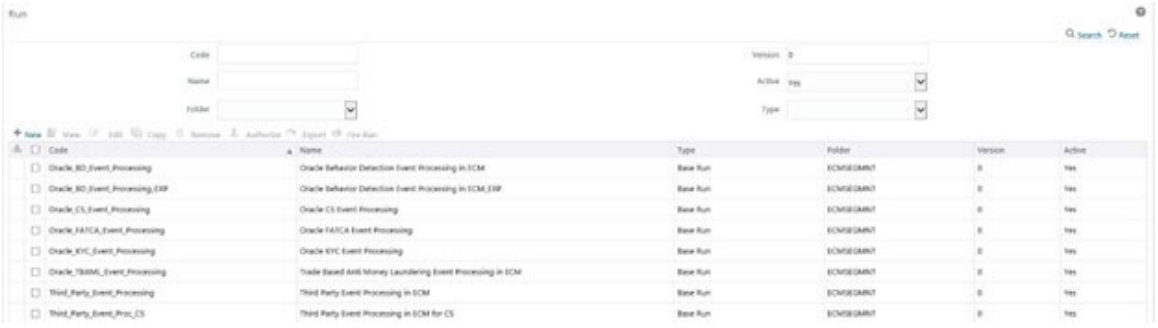
19.18.4 Configuring Event Expiry

This section explains how to configure the event expiry.

To configure the event expiry, follow these steps:

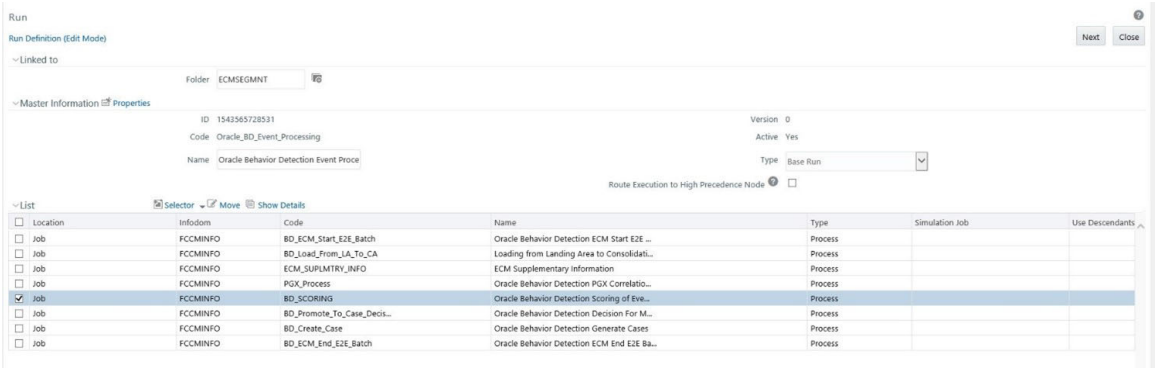
1. Create an IPE rule for event expiry. For more information, see the IPE User Guide on OHC.
2. Navigate to Enterprise Case Management Application.
3. Go to the Common task section. Select the **Run Rule Framework**.
4. Click **Run**. The Run Summary window is displayed with the available Processes as shown in Figure 128 .

Figure 128: Run Summary window



5. Go to the List section. Select **Oracle_BD_Event_Processing**. The list of processes for OBD is displayed. Select the **BD_Scoring** code and **Job** option from **Selector** as shown in Figure 129 .

Figure 129: Run Summary window

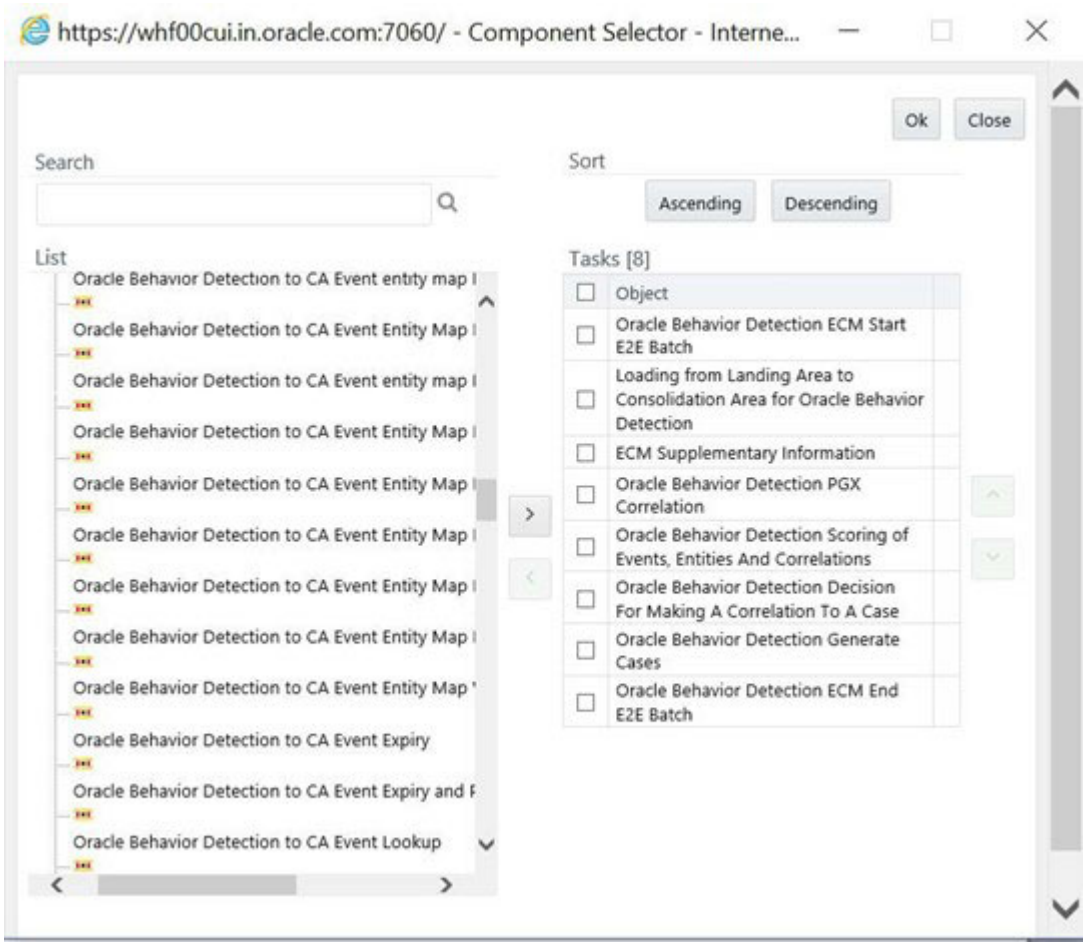


6. The **Component Selector** window is displayed. Select **Oracle Behavior Detection to CA Event Expiry and Purge** process from the list and move it to **Task** list as shown in Figure 130 .

   This process has the following two sub-processes:

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

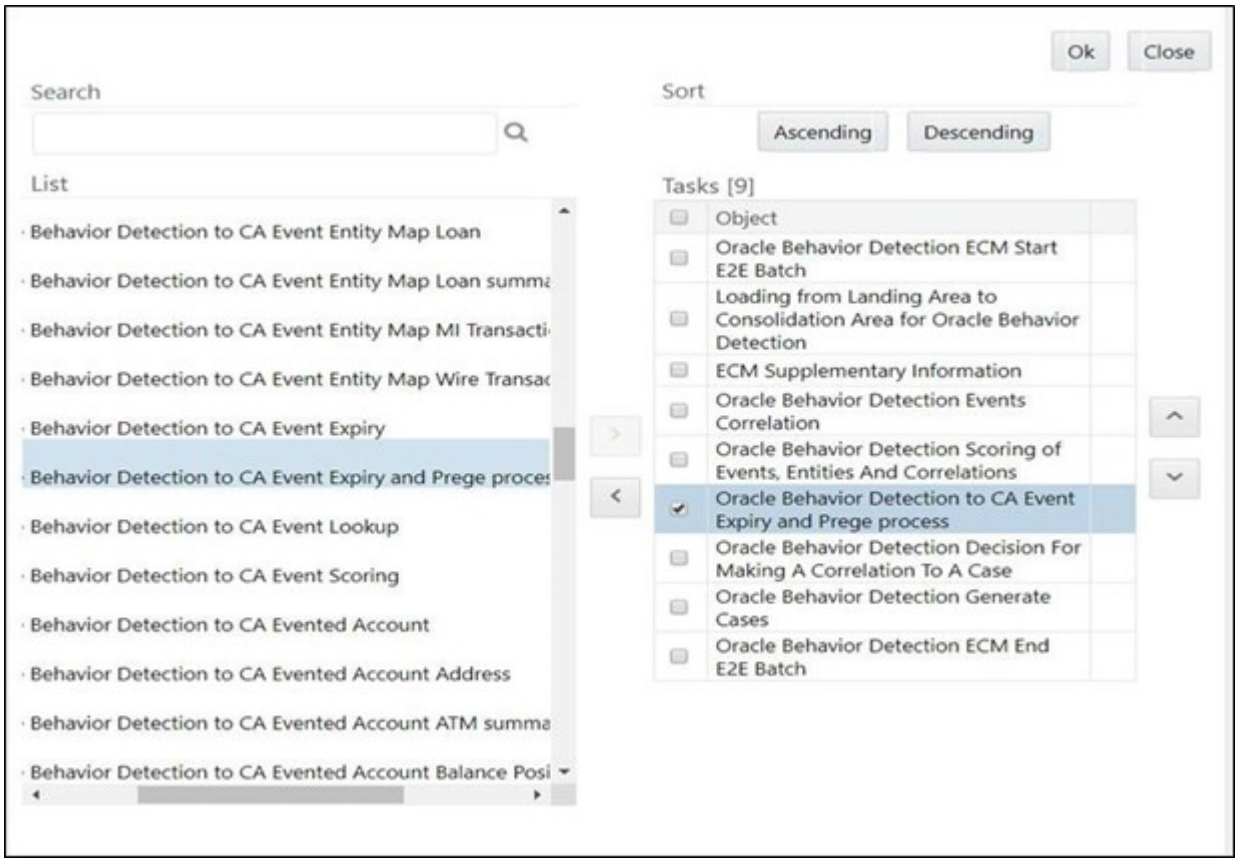
Figure 130: Component Selector



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

shown in Figure 131 .

Figure 131: Components



8. Modify the configuration table FCC_EVENT_EXPIRY_CONF as described in Table 83 .

Table 83: FCC_EVENT_EXPIRY_CONF Table

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

- **N_CONF_ID**: This is the sequence ID of the event. This should be a numeric value. For example, 1 and so on.
- N_GROUP_ID: Provide the ECM Processing Group ID
- F_IS_ASSMNT_ENABLED: Set this flag to Y if you want to enable the event assessment. If this value is set to Y, then provide the assessment ID in the **N_ASSESSMENT_ID** field.
- **N_ASSESSMENT_ID**: Provide the assessment ID if the **F_IS_ASSMNT_ENABLED** field is set to Y.

This assessment ID should be a valid IPE rule number.

- **F_IS_EVENT_SCORE_ENABLED**: Set this flag to Y if you want to enable the event score. Enable this flag before defining the threshold score in the **N_SCORE_THRESHOLD** field.
- **N_SCORE_THRESHOLD**: Define the threshold score value.

19.19 CSS Color Coding for FCC Columns

This section explains how to configure color coding in FCC ECM columns as follows:

1. Navigate to the `FCC_UI_MODULE_CONF` table in the atomic schema.
2. Search for the grid where the desired CSS must be implemented.

   For example,

   ```
   select * from fcc_ui_module_conf where
   v_ui_module_id='CM_CS_CASELIST_GRID'
   ```

3. In the V_MODULE_PROP column, add the following configuration under the column properties of the desired column where CSS must be implemented:
   - Type is externalStyle
   - Level is cell
   - externalCssFunction specifies the JavaScript function name where the externalCSS class will be decided based on user-defined validation.

     ```
     "formats": [{"type": "externalStyle", "level": "cell",
     "externalCssFunction": "<<javascriptfunctionname>>"}]
     ```

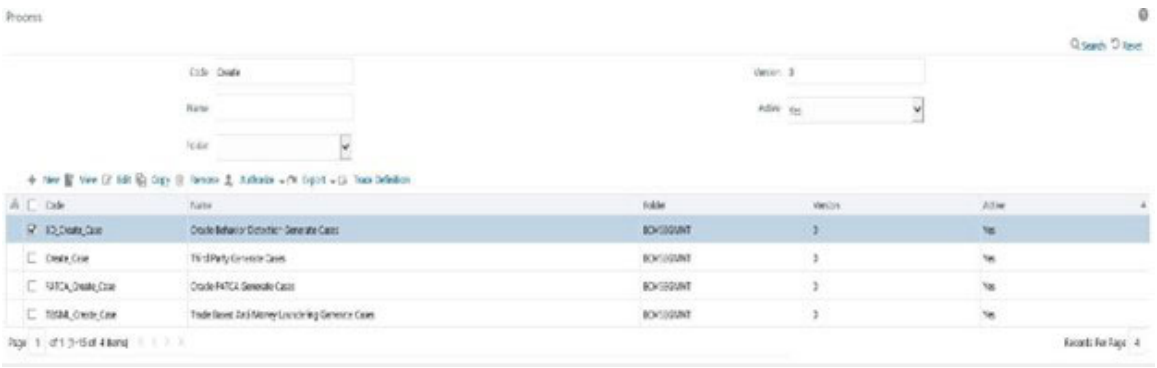
     For example,

     ```
     {
        "locale_code": "RENDERER.CS_PRIORITY",
        "headerAlign": "left",
        "visible": true,
        "draggable": true,
        "resizable": true,
        "dataType": "string",
        "width": "0.07",
        "readOnly": true,
        "sortable": true,
        "align": "left",
        "addToColMenu": true,
        "key": "priority",
        "formats": [{"type": "externalStyle", "level": "cell",
        "externalCssFunction": "colorCodeHandlerForSearchCase"}]
       }
     ```

4. The next step is to define the JavaScript function which will return the CSS class based on a

user-defined validation. For example, the sample JavaScript function is displayed following that allows for color coding of Priority and Due Date column in Case List as shown in Figure 132 .

Figure 132: Process - Define JavaScript



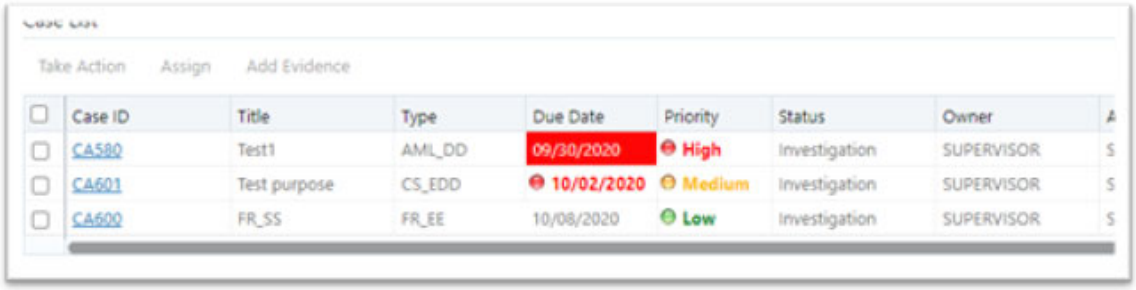
5. The JavaScript function mentioned in Step 4 can be defined in a custom JS file and that custom JavaScript file can be added in ECM as follows:
   - Copy the custom JavaScript file to the `<<deployedarea>>/ojff/js/appCommon` directory.
   - Go to the `<<deployedarea>>/ojff/js/viewModels/aai-ecm.js`. In aai-ecm.js directory, add entry for the JavaScript file in the defined block. For example, if your custom JavaScript file name is customValidator.js, then add as shown in Figure 133 :

Figure 133: Adding entry for the JavaScript file in the defined block



   - The external css classname mentioned in Step 4 should be defined in the `<<deployed_path>>/ ojff/css/appCss/OFS_NGECM.css` file.
   - Clear browser cache and access the grid. The custom CSS will come into effect as shown in Figure 134 .

Figure 134: Sample Screenshot



NOTE You can switch off the configuration if not required. To switch off the color-coding feature, remove the formats attribute from the column level configuration done in FCC_UI_MODULE_CONF.

19.20 Enabling Quantifind for Quantifind Customer Score Card

Quantifind is a third party company which provides risk information about entities. A contract with Quantifind is required to use this feature. Their product is integrated within FCCM Enterprise Case Management to allow the users to retrieve and view risk scores of a Customer. If clients are interested in implementing this feature, they have to work with Quantifind to enable this service. Once enabled, users with permission will be able to request and view Quantifind information by viewing a customer within a case. This process is enabled via PMF process (called from the ECM UI). The process sends relevant customer information to Quantifind's service, retrieves Customer's risk card and displays the risk card in ECM user interface. The following process outlines on how to configure the process and functions for a client's specific Quantifind implementation.

To enable Quantifind, follow these steps:

1. Deploy the **createJSONService.war** in the environment.
2. Execute the following script in the "**Config Schema**". Ensure that the URL and Header values are updated correctly as per the deployment. These values will be provided by Quantifind and are specific to each client's implementation. In the following sample script V_METHODNAME holds the Quantifind URL and V_HEADER_PARAMS holds the Quantifind headers.

   ```
   UPDATE AAI_WF_APPLICATION_API_B SET V_METHODNAME='https://api-
   test.quantifind.com/api/entity/summary', V_HEADER_PARAMS='{"Content-
   Type":"application/json","x-qf-app-name":"OracleIntegrationTest","x-qf-
   app-token":"nie9gieb9eSh8ohThe0luhahC7see0Queey5ienoiNa7Ie3ia1","User-
   ```

```
Agent":"PostmanRuntime/7.26.8"}' WHERE
V_PROCESS_ID='RPA_CUSTOMER_GATEWAY' AND V_APP_API_ID='1609860191729'
```

> **NOTE** By executing the above script, these values will be updated for CUSTOMER_QUANTIFIND_API application rule in the RPA Customer Gateway Process Modeling Framework workflow.
>
> To verify this in Process Modeling Framework, edit the CUSTOMER_QUANTIFIND_API application rule in the workflow found in the RPA Customer Gateway workflow. The values will be displayed in the 'Url' and 'Headers' parameters of the application rule.

3. To ensure the correct proxy is used when the Quantifind API is called, update the PMF proxy settings in the AAI_WF_GLOBAL_SETTINGS table in the config schema. The following values should be updated.
   - PROXY_SERVER_IP: <<PROXY_SERVER_IP>>
   - PROXY_SERVER_PORT: <<PROXY_SERVER_PORT>>

```
Insert into AAI_WF_GLOBAL_SETTINGS (V_PARAM_NAME,V_PARAM_VALUE) values
('PROXY_SERVER_IP',<<PROXY_SERVER_IP>>)

/

Insert into AAI_WF_GLOBAL_SETTINGS (V_PARAM_NAME,V_PARAM_VALUE) values
('PROXY_SERVER_PORT',<<PROXY_SERVER_PORT>>

/
```

> **NOTE** The above script is executed in config schema to configure the proxy and allow the application to access the Quantifind URL.

4. To enable the Quantifind icon on the Customer tab (ECM UI), run the QUANTIFIND_FORM_ENTRIES_OPT.sql in the Config Schema.
5. To allow the users to view and/or request Quantifind risk cards, following functions have to be assigned. These functions must be associated with the corresponding user roles as necessary.
   - **View Quantifind Information**

     This allows the users to view Quantifind risk cards received from Quantifind. If you want a user to view and not request for Quantifind information, assign this function to the user group only.
   - **Get Latest Quantifind Information**

     This allows user to request Quantifind risk cards.
6. Restart the servers and clear the browser Cache.

19.21 Configuring Quantifind Batch Processing for Customer Score Card Processing

The Quantifind batch process submits customer entities to an ECM processing layer where they are then submitted in batch to Quantifind. ECM users do have the ability to request Quantifind risk cards in an ad-hoc manner through the ECM UI but the Quantifind batch process allows for bulk processing of

customers which are extracted from the events created by the Behavior Detection Framework. This can provide great efficiency as cards are automatically available to the ECM users.

To configure the Quantifind batch process, follow these steps:

1. Configure the KDD_INSTALL_PARAM table in the database using Parameter Name and Parameter ID with the attributes as described in Table 84 .
   - Enter the Parameter Name as: ECMQuantifindService
   - Enter the Parameter ID as: 3010

> **NOTE** START_DATE and END_DATE attributes are not yet implemented. They are intended for the future use.

Table 84: KDD_INSTALL_PARAM table

Column Name	Attribute Code	Attribute Description	OOB Value
ATTR_1_CD	PROXY_REQUIRED	This attribute specifies whether a proxy is required to call the Quantifind batch API.	Y
ATTR_2_CD	QUANTIFIND_URL	This attribute specifies the Quantifind URL	##QUANTIFIND_API_URL##
ATTR_3_CD	QUANTIFIND_API_HEADER_PARAMS	This attribute specifies the header params required by the Quantifind Batch API. It should be provided in format For Example: {"Content-Type":"text/plain","x-qf-app-name":"sandbox","x-qf-app-token":"ceidaelah0Ahdeiteeyio6sooph0Eighuhuemie8faiZ6zah2d","User-Agent":"PostmanRuntime/7.26.10"}	##QUANTIFIND_API_HEADER_PARAMS##
ATTR_4_CD	STATUS_CHECK_INTERVAL	This attribute specifies the interval at which Quantifind status check API should be called. The value mentioned is in seconds.	60
ATTR_5_CD	SUBMIT_BATCH_SIZE	This attribute specifies the maximum number of requests which will be sent to Quantifind Submit API in one batch.	5000
ATTR_6_CD	RESULT_FETCH_SIZE	This attribute specifies maximum number of results received in one batch.	1000
ATTR_7_CD	START_DATE	This attribute is not yet supported.	NULL
ATTR_8_CD	END_DATE	This attribute is not yet supported.	NULL
ATTR_9_CD	AGING_PERIOD	This attribute specifies the total number of days, Quantifind card is valid. Till it is valid, New request for the same customer will not be sent to Quantifind	30
ATTR_10_CD	ALLOWED_ENTITY_TYPES	This attribute specifies the allowed entity types for obtaining Quantifind information. Only customer is supported.	CUSTOMER

2. Configure the business domain and jurisdiction in the FCC_EXTRNL_RQST_EVNT_FLTR table. Customer entities will be picked up by Quantifind batch for processing based on this

configuration. Currently the entity type can only be CUSTOMER. A sample entry for the filter table is shown below in Table 85 .

Table 85: FCC_EXTRNL_RQST_EVNT_FLTR table

V_FILTER	V_COLUMN_NAME	V_FILTER_VALUE
JURISDICTION	FCC_EVENTS.V_JURISDICTION_CD	'AMEA', 'EMEA'
BUSINESS_DOMAIN	FCC_EVENTS.V_BUSINESS_DOMAIN_CD	'a','b','c','d','ab','ac','ad','bc','bd','abc','bcd','abcd'
ENTITY_TYPE	FCC_EVENT_ENTITY_MAP.V_ENTITY_TYPE	'CUSTOMER'

3. To ensure the correct proxy is used when the Quantifind API is called, update the PMF proxy settings in the AAI_WF_GLOBAL_SETTINGS table in the Config Schema. The following values should be updated.
   - PROXY_SERVER_IP: <<PROXY_SERVER_IP>>
   - PROXY_SERVER_PORT: <<PROXY_SERVER_PORT>>

   ```
   Insert into AAI_WF_GLOBAL_SETTINGS (V_PARAM_NAME,V_PARAM_VALUE)
   values ('PROXY_SERVER_IP',<<PROXY_SERVER_IP>>)

   /

   Insert into AAI_WF_GLOBAL_SETTINGS (V_PARAM_NAME,V_PARAM_VALUE)
   values ('PROXY_SERVER_PORT',<<PROXY_SERVER_PORT>>)
   ```

4. Run QUANTIFIND_FORM_ENTRIES_OPT.sql in the Config Schema.
5. To allow ECM users to view and/or request Quantifind risk cards from the Customer tab within the ECM application, the following functions must be assigned. These functions must be associated with the corresponding user roles as necessary.
   - View Quantifind Information

     This allows the users to view Quantifind risk cards received from Quantifind.
   - Get Latest Quantifind Information

     This allows user to request a Quantifind risk card for the selected customer by automatically calling the Quantifind API.
6. Restart the servers and clear the browser cache.

Once the configuration is complete, follow these steps to run the Quantifind batch.

1. Login to the application with **Administrator** credentials.
2. Add the connector (**Oracle Behavior Detection to CA External Request HS**) before Entity Surrogate Key Generation for BD in ECM batch.
3. Execute the ECM batch. The **fcc_extrnl_request_hs** table will be populated with **BATCH_RUN_ID** and **N_RUN_SKEY**.
4. Navigate to Run screen in the **Rule Run Framework**.
5. Select the **Additional_Entity_Information** and click **Fire Run**.
6. In the pop-up window, enter the MIS Date and click OK to start the Quantifind batch.

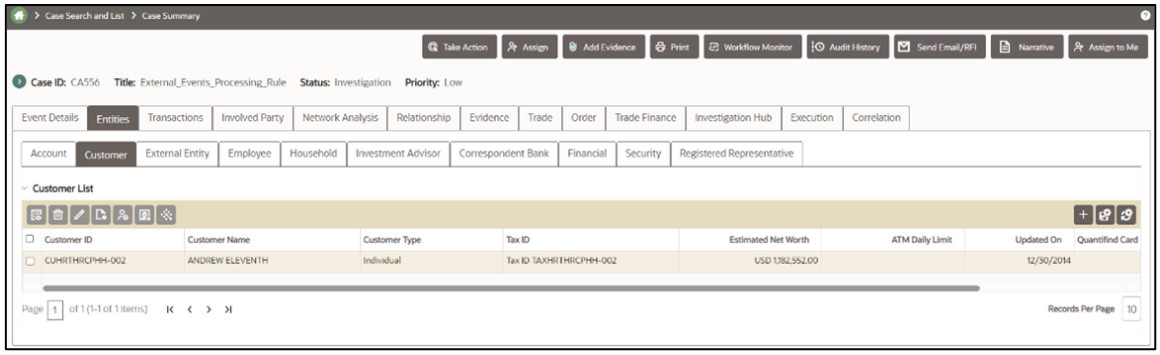
> **NOTE** The ECM batch must be completed before running the Quantifind batch.

7. The running batch can be monitored via Batch Monitor from the Admin UI. Once the batch is completed, the details are stored in the following tables.
   - FCC_EXTERNAL_REQUEST_AUDIT
   - FCC_EXTERNAL_RESULT

> **NOTE** Error with data during the batch process are only found in the error logs and will not be reprocessed by the batch (unless that customer shows up again the next day with the data corrected). The user can use the ad-hoc process if the risk card is missing.

8. Login to the application with **Supervisor** credentials.
9. Search the **Case**.
10. Click the **Customer Tab** to view the list of customer details as shown in Figure 135 .

Figure 135: Customer Tab



11. Click the required Quantifind Card **Details** to view the **Quantifind Details** with the current score and the request time as shown in Figure 136 .

Figure 136: Quantifind Details



19.22 Configuring Quantifind for Bulk Entity Process

Quantifind is a third-party company which provides risk information about entities. Their product is integrated within FCCM Enterprise Case Management to allow batch processing of entities, like customers, in order to produce events for investigation in ECM. If Oracle clients are interested in implementing this feature, they must work with Quantifind to enable this service.

Once enabled, a batch process gathers all applicable entities and produces a file in the Quantifind-defined format. After the Oracle client transmits this file to Quantifind, if Quantifind has a positive hit on that entity, an event is produced. All events are retrieved by the client and ECM processes the events via API into the event landing area. Case correlation will then produce cases based on the

client's configuration. The following process outlines how to configure the process and functions for an Oracle client's specific Quantifind implementation.

The Quantifind bulk entity process generates entities in the Quantifind-specified request format in a jsonl file and then zips the file and ensures that the zip file is SFTPed to the configured path in FTP share.

To configure the Quantifind Bulk Entity process, follow these steps:

1. Update the ECMQuantifindBulkService.properties in <<FIC_DB>>/conf folder as described in Table 86 .

Table 86: ECMQuantifindBulkService.properties

Property Name	Property Description	Example Value
ECM_CUSTOMER	This property specifies the query to get customer main details. Same aliases should be used when defining the query. For example: custId for Customer ID value and so on.	elect fcc_cust.CUST_INTRL_ID custId, case when fcc_cust.CUST_TYPE_CD='IND' then 'person' else 'organization' end entityType,nvl(fcc_cust.FIRST_NM,' ') firstName , nvl(fcc_cust.MIDL_NM,' ') middleName , nvl(fcc_cust.LAST_NM,' ') lastName , nvl(fcc_cust.MPLYR_NM,' ') employer,case when fcc_cust.BIRTH_DT is not null then to_char(fcc_cust.BIRTH_DT,'YYYY-MM-DD') else ' ' end birthDate, nvl(fcc_cust.ORG_NM,' ') orgName , case when fcc_cust.CUST_TYPE_CD='IND' then nvl(fcc_cust.FULL_NM,' ') else nvl(fcc_cust.ORG_NM,' ') end fullName , fcc_cust.DATA_ORIGIN dataOrigin, fcc_cust.JRSDCN_CD jrsdcnCode, fcc_cust.BUS_DMN_LIST_TX busDomain from fcc_cust where 1=1
INP_FILE_SFTP_FOLDER_PATH	This property specifies the relative ftpshare folder path where generated request files will be kept. The absolute path where the files will be placed will be the actual ftpshare path appended with the value mentioned under this property.	DEV/ECMQUANTIFINDBULKBATCH

2. Configure the filter conditions in the **FCC_EXT_BATCH_ENT_SCRN_FLTR** table based on any column available in the select query specified under the ECM_CUSTOMER property in

ECMQuantifindBulkService.properties. Customer entities will be picked up by the Quantifind bulk entity process based on this configuration.

Currently, only the CUSTOMER entity type is supported. A sample entry for the filter table as shown in Figure 137 .

Figure 137: Sample Customer Entity Entry

V_FILTER	V_COLUMN_NAME	V_FILTER_VALUE	N_SET_NUMBER
JURISDICTION	FCC_CUST.JRSDCN_CD	'AMEA','EMEA'	1
BUSINESS_DOMAIN	FCC_CUST.BUS_DMN_LIST_TX	'a','b','c','d','ab','ac','ad','bc','bd','abc','bcd','abcd'	1
JURISDICTION	FCC_CUST.JRSDCN_CD	'AUS'	2
BUSINESS_DOMAIN	FCC_CUST.BUS_DMN_LIST_TX	'a','b'	2

NOTE

To apply default MIS_DATE and DATA_ORIGIN filters with your custom filter conditions, modify the following filter conditions:

- MIS_DATE: filter_value as $FICMISDATE (the date given in the batch run UI)
- DATA_ORIGIN: filter_value as $BATCHDATAORIGIN

The system will automatically take values based on the batchrun id ** from the fcc_batch_run table.

Different filter sets can be configured based on the N_SET_NUMBER. The filterSetNumber which will be applied must be given in the <<FIC_DB>>/bin/ ECMQuantifindBulkService.sh file (filterSetNumber parameter).

NOTE

Currently, only the IN condition is applicable for the filters specified in the FCC_EXT_BATCH_ENT_SCRN_FLTR table. If there is no filterSetNumber configured, then the filter condition of mis_date and data_origin will be appended to the configured ECM_CUSTOMER query.

For example:

```
select fcc_cust.CUST_INTRL_ID custId, case when
fcc_cust.CUST_TYPE_CD='IND' then 'person' else 'organization' end
entityType,nvl(fcc_cust.FIRST_NM,' ') firstName , nvl(fcc_cust.MIDL_NM,'
') middleName , nvl(fcc_cust.LAST_NM,' ') lastName ,
nvl(fcc_cust.MPLYR_NM,' ') employer,case when fcc_cust.BIRTH_DT is not
null then to_char(fcc_cust.BIRTH_DT,'YYYY-MM-DD') else ' ' end
birthDate, nvl(fcc_cust.ORG_NM,' ') orgName from fcc_cust where 1=1

AND mis_date IN (SELECT  d_mis_date  FROM fcc_batch_run  WHERE
v_batch_run_id in ('"+batchRunId+"')) AND data_origin IN (SELECT
v_data_origin FROM fcc_batch_run INNER JOIN fcc_batch_dataorigin ON
```

```
fcc_batch_run.n_run_skey = fcc_batch_dataorigin.n_run_skey WHERE
v_batch_run_id in ('"+batchRunId+"'))
```

3. Once the configuration is complete, follow these steps to run the ECMQuantifindBulkService batch.
   a. Log in to the application with Administrator credentials.
   b. Navigate to the Run screen in the Rule Run Framework.
   c. Select the ECMQuantifindBulkService and click Fire Run.
   d. In the pop-up window, enter the MIS Date and click OK to start the ECMQuantifindBulkService batch.
   e. Monitor the running batch via Batch Monitor. Once the batch is completed, the details are stored in the following tables:
      — "FCC_EXT_BATCH_ENT_SCRN_RQST
      — "FCC_EXT_BATCH_ENT_SCRN_AUDIT

      The generated zip file is provided in the configured ftpshare location. The filename will be in the following format:

      ECMEntityInputJSON_<<BatchRunId>>.zip

      For example: ECMEntityInputJSON_ECMINFO_1663684879891_20141231_1.zip

19.23 Configuring Quantifind for Bulk Event Creation Process

The Quantifind bulk event creation process creates events based on the responses received from Quantifind. The responses are read from the results zip file placed in the configured path in FTPShare.

To configure the Quantifind Bulk Event Creation process, follow these steps:

1. Updated the ECMQuantifindBulkService.properties in the <<FIC_DB>>/conf folder as described in Table 87 .

Table 87: ECMQuantifindBulkService.properties

Property Name	Property Description	Example Value
OUT_FILE_SFTP_FOLDER_PATH	This property specifies the relative ftpshare folder path to accept response files from Quantifind. The absolute path where the response files should be placed will be the actual ftpshare path appended with the value mentioned under this property.	DEV/ ECMQUANTIFINDBULKBATCH_ OUTPUT
RESULTS_FILENAME	This property specifies quantifind results filename which will be available inside the quantifind response zip file. Multiple results filenames can be specified comma separated.	results-cs-batch.json,results-kyc-batch.json
ECM_SERVICE_URL	This property specifies the ECM event creation service URL.	http://<Application URL>/rest-api/CMRestService/ RealTimeCaseCreationService/ saveEvents

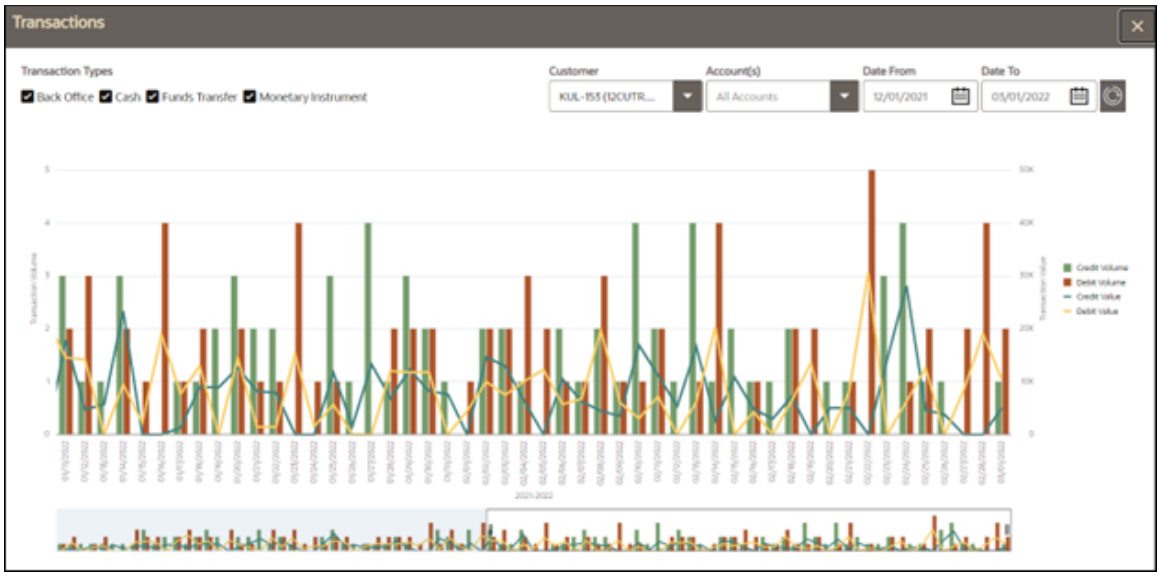
2. Once the configuration is complete and response files are available from Quantifind in the configured FTPShare path, follow these steps to run the ECMQuantifindBulkEventCreation batch.
   a. Log in to the application with Administrator credentials.
   b. Navigate to the Run screen in the Rule Run Framework.
   c. Select the ECMQuantifindBulkEventCreation and click Fire Run.
   d. In the pop-up window, enter the MIS Date and click OK to start the ECMQuantifindBulkEventCreation batch.
   e. Monitor the running batch via Batch Monitor. Once the batch is completed, the details are stored in the following tables:

- FCC_EXT_BATCH_ENT_SCRN_RQST
- FCC_EXT_BATCH_ENT_SCRN_AUDIT?

19.24 Transaction Chart Configuration

The Transaction Chart displays a graphical representation of all the transactions for all the customers involved in the selected case within the defined time period. This helps investigators identify patterns of expected customer activity as shown in Figure 138 .

Figure 138: Transaction Chart



This chart can be configured in the KDD_INSTALL_PARAM table of the Atomic schema using Param ID 3014 as described in Table 88 .

Table 88: Configuring Transaction Chart

Parameter Name	Default Value	Description
ECM Transaction Chart	Y	The value of this parameter specifies whether Transactions chart should be displayed or not in Transactions tab. The parameter value can have only Y or N value. If set to Y, Transactions chart will be displayed in Transactions tab. If set to N, Transactions chart will not be displayed in Transactions tab.
ATTR_1_CD: TRANS_SRCH_DFLT_DT_RANGE	3	The value of this attribute specifies the number of months (Date Range) allowed between Date From and Date To date fields for default search in Transactions Chart on the Transactions tab. This attribute accepts only natural numbers.
ATTR_2_CD: TRANS_SRCH_DT_RANGE	12	The value of this attribute specifies the number of months (Date Range) allowed between Date From and Date To date fields for manual search in Transactions Chart on the Transactions tab. This attribute accepts only natural numbers.

19.25 Configuring Labels for Transactions

Labels are used to easily segregate and filter transactions.

19.25.1 Adding Customized Transaction Labels

To add customized transaction labels in the KDD_CODE_SET_TRNLN and KDD_CODE_SET_TRNLN_TL tables, refer to the following scripts:

```
insert into KDD_CODE_SET_TRNLN (CODE_SET, CODE_VAL,
SRC_SYS_CD,CODE_DISP_TX) values ('TrxnLabels', '<Sample Tag value>',
null, '<Sample Tag>');

insert into KDD_CODE_SET_TRNLN_TL
(CODE_SET,CODE_VAL,CODE_DISP_TX,V_LOCALE_CD) values ('TrxnLabels',
'<Sample Tag Value>', '<Sample Tag>', 'en_US');
```

(here <Sample Tag> and <Sample Tag value> need to be replaced by the required Tag/Label and its value respectively).

> **NOTE** If a language pack is installed, you must configure the entries in the KDD_CODE_SET_TRNLN_TL table for all locale codes for which the language pack was installed.

19.25.2 Updating Labels in UI

Refer to the following scripts to update the Label display in UI:

```
update kdd_code_set_trnln t set t.code_disp_tx='<New Label Display>'
where t.code_set='TrxnLabels' and t.code_val='<Label Value>';

update kdd_code_set_trnln_tl t set t.code_disp_tx='<New Label Display>'
where t.code_set='TrxnLabels' and t.code_val='<Label Value>' and
t.v_locale_cd='<Required Locale>';

For example:

update kdd_code_set_trnln t set t.code_disp_tx='Evented New' where
t.code_set='TrxnLabels' and t.code_val='EVENTED';

update kdd_code_set_trnln_tl t set t.code_disp_tx='Evented New' where
t.code_set='TrxnLabels' and t.code_val='EVENTED' and
t.v_locale_cd='en_US';
```

> **NOTE** The code_val EVENTED and SAMPLED (label value) must not be modified as they are referred in the code. However, the display label or the code_disp_tx can be modified.

19.26 Entities Tab Configuration

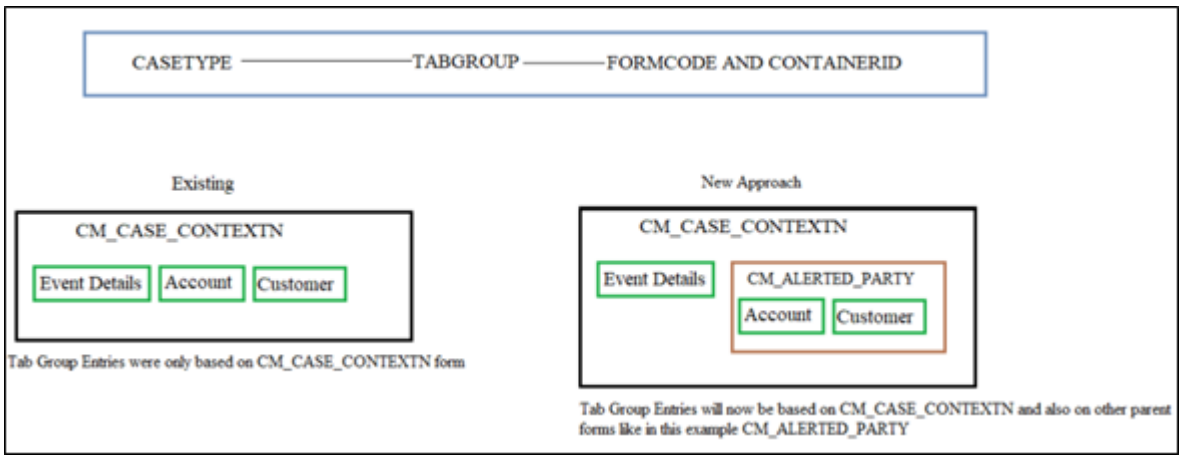
The Entities tabs provide Account, Customer, External Entity, Employee, Household, Investment Advisor, Correspondent Bank, Financial and Trade business information pertaining to the case.

The Entities tab is a parent tab and can be configured in the **KDD_CASEENTITY_MASTER** table. Parent Tab entries will be made in **KDD_CASEENTITY_MASTER**, **KDD_CASEENTITY_MASTER_TL**, **KDD_CASEENTITY_TAB_MAP**. There will be no entries of parent tab in **KDD_CASETYPE_ENTITY_MAP** table.

- The KDD_CASEENTITY_PARENT_MAP tab captures the entities which display in the parent tab. This table will hold the Entity ID, Parent Entity ID and Parent Form Code.
- During Save of Entity Association, an additional check will be done to verify if the respective entity has a parent ID provided. If yes, then the parents tabid will be populated to CM_CASE_CONTEXTN tab group entries in the AAI tables. Furthermore, the respective entity tab

IDs will be populated with respective parent form code in the AAI tables. The same tab group ID will be used for CM_CASE_CONTEXTN and the parent form codes as shown in Figure 139 .

Figure 139: Workflow



19.27 Configuring Different Due Dates for Case Types

You can set different due dates and near due dates for different case types by defining the case type and number of days for due date in KDD_CASETYPE_PARAM_CONFIG table as described in Table 89 .

To configure due date and near due dates, follow these steps:

1. Enter the `V_PARAM_CD` as `DUE_DT_LMT`.
2. Enter the different case types to which the due date is to be set under `V_CASE_TYPE`.
3. Enter the no. of days under `V_PARAM_VALUE`.

> **NOTE** START_DATE and END_DATE attributes are not yet implemented. They are intended for future use.

Table 89: Configuring Different Due Date and Near Due Dates

Column Name	Attribute Description	OBB Value
V_PARAM_CD	Due_dt_lmt and near_due_dt_lmt are the two param codes that can be defined in this column.	DUE_DT_LMT and NEAR_DUE_DT_LMT
V_CASETYPE	The case types for which different due dates must be set can be defined in this column.	All case types.
V_PARAM_VALUE	No. of days for due date and near due dates for the required case type are defined in this column.	NA.

You can also set due date for the cases which are created via the correlation batch. To configure due date, refer to the above table.

19.28 Trusted Pairs

This section explains the concept behind trusted pairs. Trusted Pair is the concept of reducing the number of false positive events by identifying transactions between parties viewed as having a trusted relationship. After analyzing events, you can determine two parties are trusted when the activity between the two parties is an acceptable business practice and poses little risk to the institution.

Topics:

- Configuring Trusted Pair Actions
- Configuring Duration

19.28.1 Configuring Trusted Pair Actions

You can configure the options which display in the Take Action window in the Trusted Administration screen for each status by updating the fields V_ACTION_CD and V_FIELD_CD in the FCC_TP_ACTION_FIELD_MAP table.

Table 90 describes how to configure the trusted pair status to action mappings.

Table 90: Trusted Pair Status/Actions

Table Name	Column Name	Description
FCC_TP_STATUS	V_STATUS_CD	Status Code of the Trusted Pair.
	V_STATUS_NM	Status Name of the Trusted Pair.
	F_ACTIVE_FL	Flag indicating whether or not the status is active. A value of "Y" indicates that the current status is active. A value of "N" indicates the current status is inactive. Only one status can have 'Y' for this column.
	F_SHARED_FL	A Trusted Pair status with value 'Y for this column will be part of the Trusted Pair. API response.
FCC_TP_STATUS_TL	V_STATUS_CD	Status Code of the Trusted Pair.
	V_STATUS_NM	Status Name of the Trusted Pair.
	V_SOURCE_LOCALE	Source Locale in which the record was initially added.
	V_LOCALE_CD	Locale Code of the Trusted Pair.
	V_CREATED_BY	Not in Use
	D_CREATED_DT	Not in Use

Table 90: Trusted Pair Status/Actions

Table Name	Column Name	Description
FCC_TP_ACTION	N_ACTION_ID	Action ID of the Trusted Pair.
	V_ACTION_CD	Action Code of the Trusted Pair.
	V_ACTION_NM	Action Name of the Trusted Pair.
	V_ACTION_DESC	Action Description of the Trusted Pair.
	F_START_ACTION	Action which is used to start the Trusted Pair.. A value of "Y" indicates this action is the starting action. Only one action can have 'Y' for this column.
	F_APPROVE_ACTION	Action which is used to approve the Trusted Pair. A value of "Y" indicates this action is the approving action. Only one action can have 'Y' for this column.
	F_EXPIRE_ACTION	Action which is used to expire the Trusted Pair. A value of "Y" indicates this action is the expiration action. Only one action can have 'Y' for this column.
FCC_TP_ACTION_TL	N_ACTION_ID	Action ID of the Trusted Pair.
	V_ACTION_CD	Action Code of the Trusted Pair.
	V_ACTION_NM	Action Name of the Trusted Pair.
	V_ACTION_DESC	Action Description of the Trusted Pair.
	V_LOCALE_CD	Locale Code of the Trusted Pair.
	V_CREATED_BY	Not in Use
	V_SOURCE_LOCALE	Source Locale in which the record was initially added.
	D_CREATED_DT	Not in Use

19.28.2 Configuring Duration

> **NOTE** Once expiration date is reached, you must set the Trusted Pair records to expiry. Use the batch infodom_ECM_TP_EXPIRY_BATCH for expiring Trusted Pair records.

The Duration drop-down list displays 3, 6, 9, and 12 month options by default. Configurable values will be done via a system parameter.

To configure additional options to display in the drop-down list, run the following script:

```
select * from KDD_CODE_SET_TRNLN where  code_set='CMTPDuration';

select * from KDD_CODE_SET_TRNLN_TL where  code_set='CMTPDuration';
```

> **NOTE** The CODE_VAL must be two digits. If the value is a single digit, prefix the month with 0. For example 03m,06m,09m. This will display the value in CODE_DISP_TX as 3 months, 6 months, and 9 months, respectively.

19.29 Event Suppression

Event Suppression enables the system to automatically suppress a particular entity's newly generated alerts based on criteria such as scenario, suppression begin and end dates. The rule captures information such as the creation date, the status, the generating scenario, the focal entity (focus type and focal entity ID) and the links to the comments by the user associated with the suppression.

Once a suppression rule is approved, the Behavior Detection (BD) engine will pull the rule into their tables via an API. The newly created alerts in BD that match the rule will be closed automatically based on the predefined BD algorithm. The ECM batch will move these alerts as events to ECM and then these events will be closed in batch.

The Suppression Administration page allows you to search for existing suppressions based on a set of user-specified parameters. The Manage Suppression Rules also enables you to modify certain

components of rules, in particular, to update or to end an existing suppression rule as well as to track all actions performed on that rule.

Topics:

- Configuring Suppression Actions
- Configuring Duration

19.29.1 Configuring Suppression Actions

You can configure the options which display in the Take Action window in the Suppression Administration screen for each status by updating the fields V_ACTION_CD and V_FIELD_CD in the FCC_SUP_ACTION_FIELD_MAP table.

Table 91 describes how to configure the suppression rule status to action mappings.

Table 91: Suppression Rule Status/Actions

Table Name	Column Name	Description
FCC_SUP_STATUS	V_STATUS_CD	Status Code of Suppression rule.
	V_STATUS_NM	Status Name of Suppression rule.
	F_ACTIVE_FL	Flag indicating whether or not the status is active. A value of "Y" indicates that the current status is active. A value of "N" indicates the current status is inactive. Only one status can have 'Y' for this column.
	F_SHARED_FL	A suppression rule status with value 'Y for this column will be part of the Suppression rule API response.
FCC_SUP_STATUS_TL	V_STATUS_CD	Status Code of Suppression rule.
	V_STATUS_NM	Status Name of Suppression rule.
	V_SOURCE_LOCALE	Source Locale in which the record was initially added.
	V_LOCALE_CD	Locale Code of the Suppression rule.
	V_CREATED_BY	Not in Use
	D_CREATED_DT	Not in Use
FCC_SUP_ACTION	N_ACTION_ID	Action ID of Suppression rule.
	V_ACTION_CD	Action Code of Suppression rule.
	V_ACTION_NM	Action Name of Suppression rule.
	V_ACTION_DESC	Action Description of Suppression rule.
	F_START_ACTION	Action which is used to start the Suppression rule. A value of "Y" indicates this action is the starting action. Only one action can have 'Y' for this column.
	F_APPROVE_ACTION	Action which is used to approve the Suppression rule. A value of "Y" indicates this action is the approving action. Only one action can have 'Y' for this column.
	F_EXPIRE_ACTION	Action which is used to expire the Suppression rule. A value of "Y" indicates this action is the expiration action. Only one action can have 'Y' for this column.

Table 91: Suppression Rule Status/Actions

Table Name	Column Name	Description
FCC_SUP_ACTION_TL	N_ACTION_ID	Action ID of Suppression rule.
	V_ACTION_CD	Action Code of Suppression rule.
	V_ACTION_NM	Action Name of Suppression rule.
	V_ACTION_DESC	Action Description of Suppression rule.
	V_LOCALE_CD	Locale Code of the Suppression rule.
	V_CREATED_BY	Not in Use
	D_CREATED_DT	Not in Use

NOTE Once expiration date is reached, you must set the Suppression records to expiry. Use the batch infodom_ECM_SUP_EXPIRY_BATCH for expiring Suppression records.

19.29.2 Configuring Duration

The Duration drop-down list displays 3, 6, 9, and 12 month options by default. Configurable values will be done via a system parameter.

To configure additional options to display in the drop-down list, run the following script:

```
select * from KDD_CODE_SET_TRNLN where  code_set='CMSUPDuration';

select * from KDD_CODE_SET_TRNLN_TL where  code_set='CMSUPDuration';
```

NOTE The CODE_VAL must be two digits. If the value is a single digit, prefix the month with 0. For example 03m,06m,09m. This will display the value in CODE_DISP_TX as 3 months, 6 months, and 9 months, respectively.

20 List of Processes and Tasks

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

- OBD Application Process
- OCS Application Process
- OKYC Application Process
- OSTDO Application Process
- Third-party Application Process

20.1 OBD Application Process

- Start Batch
- Load Data from BD to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

20.1.1 Start Batch

To start a batch, follow these steps:

1. Log in as ECM **ADMIN** and navigate to **Enterprise Case Management** Application.
2. Go to the **Common Tasks** section and select the **Rule Run Framework**.
3. Click **Run**. The **Run** window is displayed with the available Processes.
4. Go to the **List** section, select **Oracle_BD_Event_Processing**, and click **Edit**.
5. Add the **BD_POPULATE_ENTITY_RELATION** Data Transformation task after the **BD_Create_Task** Data Transformation task and click **Save**. This task populates data in the KDD_CASE_NTITY_REL_EVNT and KDD_CASE_NTITY_REL_CASE tables.

   NOTE Refer to the Adding Transformation Rule section.

6. Run the **Oracle_BD_Event_Processing** batch.

20.1.2 Load Data from BD to ECM

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

- Loading BD Events
  - If you use Event Suppression, the following process must be added to the batch Oracle Behavior Detection to CA Event Suppression - BD_EVENT_SUPPRESSION.

If the ECM Batch Run has selected the alerts that are closed automatically by Suppression in the BDF, it will close the Events and update the decision of the corresponding Events as Closed per Suppression Rule. The decision Closed per Suppression Rule is currently obtained from the FCC_EVENT_INVESTIGATION_STATUS table, n_status_id = 998. You can modify the decision name in the FCC_EVENT_INVESTIGATION_STATUS table for n_status_id = 998.

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

Below is the list of BD sub-process codes. These sub-processes can be used by OCS and OKYC applications along with their application-specific processes.

Here, Level 1 subprocess code execution is a prerequisite for Level 2 subprocess execution. Similarly, Level 2 sub-process code execution is a prerequisite for Level 3 sub-process execution and so on. Subprocess within a level can be executed in any order or it can be executed in parallel.

BD_ENTITY_SUP_INFO sub-process code has to be executed after the business data population (see the Business Metadata Movement).

20.1.3 Correlation

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

- PGX_CORRELATION
- BD_CORRELATION

20.1.4 Scoring

BD_SCORING is used to perform the scoring of OBD events. This has the 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

20.1.5 Promote to Case

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

- Pre Case Promotion Rule

20.1.6 Create Case

BD_Create_Case process is used for case creation if an OBD event is promoted to case. Below is the list of T2T tasks for BD application:

- f_generatecaseid
- f_insertcases
- t2t_KDD_CASE_ACCOUNTS

- t2t_KDD_CASE_CUSTOMERS
- t2t_KDD_CASE_DERIVED_ADDRESS
- t2t_KDD_CASE_EMPLOYEES
- t2t_KDD_CASE_ACCOUNT_ADDRESS
- t2t_KDD_CASE_ACCOUNT_MANAGED
- t2t_KDD_CASE_ACCOUNT_RSTRNS
- t2t_KDD_CASE_ACCT_BAL_POSN_SMRY
- t2t_KDD_CASE_ACCT_EMAIL_ADDR
- t2t_KDD_CASE_ACCT_PEER_GRP
- t2t_KDD_CASE_ACCT_PHON
- t2t_KDD_CASE_ACCT_SMRY_MNTH
- t2t_KDD_CASE_ACCT_SUPPL_ATTR
- t2t_KDD_CASE_ACT_PEER_TRXN_SMRY
- t2t_KDD_CASE_ACCT_NTCPTRY_PRFL
- t2t_FCC_CASE_ACCT_LIST_MBRSP
- t2t_KDD_CASE_CLIENT_BANK
- t2t_KDD_CASE_CLIENT_BANK_SMRY_MNTH
- t2t_KDD_CASE_CUST_ADDR
- t2t_KDD_CASE_CUST_EMAIL_ADDRS
- t2t_KDD_CASE_CUST_LIST_MEMBERSHIP
- t2t_KDD_CASE_CUST_PHONE
- t2t_KDD_CASE_CUST_SUPPL_ATTR
- t2t_KDD_CASE_CUST_SMRY_MNTH
- t2t_KDD_CASE_CUST_CUST
- t2t_KDD_CASE_EMP_ACCT
- t2t_KDD_CASE_EMP_ADDR
- t2t_KDD_CASE_EMP_EMAIL_ADDR
- t2t_KDD_CASE_EMP_PHONE
- t2t_KDD_CASE_INSTL_ACCT_SMRY_MNTH
- t2t_KDD_CASE_INSTN_MASTER
- t2t_KDD_CASE_INSURANCE_POLICY
- t2t_KDD_CASE_INSURANCE_PRODUCT
- t2t_KDD_CASE_NTWK_USER_ACCT_MAP
- t2t_KDD_CASE_ONLINE_ACCT
- t2t_KDD_CASE_ONLINE_ACCT_ACCT
- t2t_KDD_CASE_PEER_GRP

- t2t_KDD_CASE_CB_LIST_MEMBERSHIP
- t2t_KDD_CASE_CB_PEER_TXN_SMRY_MNTH
- t2t_KDD_CASE_CLIENT_BANK_PEER_GRP
- t2t_KDD_CASE_EXTERNAL_ENTITY
- t2t_KDD_CASE_EXTERNAL_ENTITY_MEMBERSHIP
- t2t_KDD_CASE_HH_ACCT_BAL_SMRY
- t2t_KDD_CASE_HH_SMRY_MNTH
- t2t_KDD_CASE_INSURANCE_PLCY_CUST
- t2t_KDD_CASE_NVSMT_MGR_SMRY_MNTH
- t2t_KDD_CASE_NVSMT_MGR
- t2t_KDD_CASE_ACCT_ID_INSTN_ID_MAP
- t2t_KDD_CASE_ACCT_GRP
- t2t_KDD_CASE_WIRE_TRXN
- t2t_KDD_CASE_CASH_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_CASH_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_MI_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_WIRE_TRXN
- t2t_KDD_CASE_BACK_OFFICE_TRXN
- t2t_KDD_CASE_CUST_IMP_LICENSE_GOODS
- t2t_KDD_CASE_CUST_IMP_LICENSE
- t2t_KDD_CASE_DOC_COLL_CNTRCT
- t2t_KDD_CASE_DOC_COLL_CNTRCT_EVENT
- t2t_KDD_CASE_DOC_COLL_DISCRP_DTL
- t2t_KDD_CASE_DOC_COLL_INVOICE
- t2t_KDD_CASE_DOC_COLL_MULTNR_DTL
- t2t_KDD_CASE_DOC_COLL_SHPMT_DTL
- t2t_KDD_CASE_EXTERNAL_INSURANCE_PLCY
- t2t_KDD_CASE_EXTERNAL_ORG
- t2t_KDD_CASE_TRADE_FIN_SWIFT_MSG
- t2t_KDD_CASE_TRADE_FIN_PARTY
- t2t_KDD_CASE_TRADE_FIN_GOOD_SRVC
- t2t_KDD_CASE_TRADE_FIN_DRAFT
- t2t_KDD_CASE_TRADE_FIN_DOC
- t2t_KDD_CASE_TRADE_FIN_CNTRCT
- t2t_KDD_CASE_TRADE_FIN_BRKRGE_DIST
- t2t_KDD_CASE_TRADE_FIN_BRKRGE

- t2t_KDD_CASE_TRADE_FIN_ACCT
- t2t_KDD_CASE_TRADE
- t2t_KDD_CASE_ORDER
- t2t_KDD_CASE_TRADE
- t2t_KDD_CASE_MI_TRXN
- t2t_KDD_CASE_LOAN_ACCOUNT
- t2t_KDD_CASE_LOAN
- t2t_KDD_CASE_LOAN_SMRY_MONTH
- t2t_KDD_CASE_INSTRUCTION
- t2t_KDD_CASE_ORDR_EVENT
- t2t_KDD_CASE_SCRTY_FIRM_DAILY
- t2t_KDD_CASE_SCRTY_MKT_DAILY
- t2t_KDD_CASE_TRADE_EXECUTION_EVENT
- t2t_KDD_CASE_SCRTY
- t2t_KDD_CASE_EXECUTION
- CASE_COMPLETION_FLAG

CASE_ASSIGNMENT

Here, Level 1, Level 2, Level 2, Level 2, Level 3, Level 4, Level 5, Level 6, and Level 7 should run in sequence as described in Table 92 . Sub-processes within any level (for example, level3) can be executed in any order in parallel (depending upon the hardware specification) or sequentially. as described in Table 94 .

Table 92: Level Details

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

Table 93: Process Details

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
BD_EVENT_LOOKUP	BD_EVENT	BD_ACCOUNT_GROUP_LOOKUP	BD_EVENT_ENTITY_MAP_AC	Business Metadata Movement	Evented Data Movement
	BD_EVENT_BINDING	BD_ACCOUNT_LOOKUP	BD_EVENT_ENTITY_MAP_AG	BD_ACCT	BD_ACCT_EVENT
	BD_EVENT_DETAILS	BD_CUSTOMER_LOOKUP	BD_EVENT_ENTITY_MAP_BOT	BD_ACCT_ADDR	BD_ACCT_ACCT_ADDR_EVNT
		BD_DERIVED_ADDRESS_LOOKUP	BD_EVENT_ENTITY_MAP_CT	BD_ACCT_BAL_POS N_SMRY	BD_ACCT_BAL_POSN_SMRY_EVNT
		BD_EMPLOYEE_LOOKUP	BD_EVENT_ENTITY_MAP_CUST	BD_ACCT_EMAIL_ADDR	BD_ACCT_GRP_EVNT
		BD_EVENT_LOOKUP	BD_EVENT_ENTITY_MAP_DA	BD_ACCT_GRP	BD_ACCT_PEER_GRP_EVNT
		BD_EXTERNAL_ENTITY_LOOKUP	BD_EVENT_ENTITY_MAP_EE	BD_ACCT_ID_INSTN_ID_MAP	BD_ACCT_PR_TXN_SMRY_MN_EVNT
		BD_INSTITUTION_LOOKUP	BD_EVENT_ENTITY_MAP_EMPL	BD_ACCT_LIST_MEMBERSHIP	BD_ACCT_RSTRN_EVNT
		BD_INVESTMENT_ADVISOR_LOOKUP	BD_EVENT_ENTITY_MAP_IA	BD_ACCT_PEER_GRP	BD_ACCT_SMRY_MNTH_EVNT
		BD_LOAN_LOOKUP	BD_EVENT_ENTITY_MAP_IM	BD_ACCT_PEER_TRXN_SMRY_MNTH	BD_BACK_OFFICE_TRXN_EVNT
		BD_MARKET_CENTER_LOOKUP	BD_EVENT_ENTITY_MAP_MIT	BD_ACCT_PHON	BD_CASH_TRXN_EVNT
		BD_PEER_GROUP_LOOKUP	BD_EVENT_ENTITY_MAP_WT	BD_ACCT_RSTRN	BD_CB_PR_TXN_SM_MNT_EVNT
				BD_ACCT_SMRY_MNTH	BD_CLIENT_BANK_EVNT
				BD_BACK_OFFICE_TRXN	BD_CLINT_BNK_PR_GRP_EVNT
				BD_CASH_TRXN	BD_CLNT_BNK_SM_MNT_ EVNT
				BD_CB_LIST_MEMBERSHIP	BD_CUST_EVNT

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				BD_CB_PR_TRXN_SMRY_MNTH	BD_CUST_IMP_LICENSE_EVNT
				BD_CLIENT_BANK	BD_CUST_IMP_LIC_GOD_EVNT
				BD_CLIENT_BANK_PEER_GRP	BD_CUST_SMRY_MNTH_EVNT
				BD_CLIENT_BANK_SMRY_MNTH	BD_CUST_SUPPL_ATR_EVNT
				BD_CUST	BD_DERIVED_ADDRESS_EVNT
				BD_CUST_ACCT	BD_EMP_ACCT_EVNT
				BD_CUST_ADDR	BD_EMP_ADDR_EVNT
				BD_CUST_E-MAIL_ADDR	BD_EMP_E-MAIL_ADDR_EVNT
				BD_CUST_IMP_LICENSE	BD_EMP_EVNT
				BD_CUST_IMP_LICENSE_GOOD	
				BD_CUST_LIST_MEMBERSHIP	
				BD_CUST_PHON	
				BD_CUST_SMRY_MNTH	
				BD_CUST_SUPPLEMENTAL_ATR	BD_EMP_PHON_EVNT
				BD_DERIVED_ADDRESS	BD_HH_BAL_POSN_SMRY_EVNT
				BD_EMP	BD_INSTL_ACCT_SMRY_MNTH_EVNT
				BD_EMP_ACCT	BD_INSTN_MASTER_EVNT
				BD_EMP_ADDR	BD_INSURANCE_POLICY_EVNT

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				BD_EMP_E-MAIL_ADDR	BD_INSURANCE_PRODUCT_EVNT
				BD_EMP_PHON	BD_INS_PLCY_CUST_EVNT
				BD_EVENT_SCORE	BD_LOAN_EVNT
				BD_EXTERNAL_ENTITY	BD_LOAN_SMRY_MNTH_EVNT
				BD_EXTERNAL_ENTITY_ADDR	BD_MANGD_ACCT_EVNT
				BD_EXTRNAL_ENTTY_MMBRSHP	BD_MI_TRXN_EVNT
				BD_FCC_EXTERNAL_ENTITY_LINK	BD_NTCPTRY_PRFL_EVNT
				BD_HH_BAL_POSN_SMRY	BD_NVSMT_MGR_EVNT
				BD_INSTN_MASTER	BD_NVSMT_MGR_SMRY_MNTH_EVNT
				BD_INSURANCE_POLICY	BD_PEER_GRP_EVNT
				BD_INSURANCE_POLICY_CUST	BD_WIRE_TRXN_EVNT
				BD_INSURANCE_PRODUCT	BD_XTRNL_ENTY_ADR_EVNT
				BD_LOAN	
				BD_LOAN_SMRY_MNTH	
				BD_MANGD_ACCT BD_MI_TRXN	
				BD_NTCPTRY_PRFL	
				BD_NVSMT_MGR	
				BD_NVSMT_MGR_SMRY_MNTH	

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				BD_PEER_GRP	
				BD_WIRE_TRXN	
				BD_ENTITY_SUP_INFO This sub-process code must be executed after the business data population (see the Business Metadata Movement).	

Table 94 describes the variuos sub-processes.

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Event	Oracle Behavior Detection to CA Event	BD_EVENT
CA Event	Oracle Behavior Detection to CA Event Binding	BD_EVENT_BINDING
CA Event	Oracle Behavior Detection to CA Event Details	BD_EVENT_DETAILS
CA Event	Oracle Behavior Detection to CA Trade Lookup	BD_TRADE_LOOKUP
CA Event	Oracle Behavior Detection to CA Order Lookup	BD_ORDER_LOOKUP
CA Event	Oracle Behavior Detection to CA Security Lookup	BD_SECURITY_LOOKUP
CA Event	Oracle Behavior Detection to CA Event Entity Map Trade	BD_EVENT_ENTITY_MAP_TRADE
CA Event	Oracle Behavior Detection to CA Event Entity Map Order	BD_EVENT_ENTITY_MAP_ORDER
CA Event	Oracle Behavior Detection to CA Event Entity Map Security	BD_EVENT_ENTITY_MAP_SCRTY
CA Event	Oracle Behavior Detection to CA Event Entity Map Customer Account Position	BD_EVENT_ENTITY_MAP_ACCT_POSN
CA Event	Oracle Behavior Detection to CA Trade	BD_TRADE
CA Event	Oracle Behavior Detection to CA Evented Trade	BD_TRADE_EVNT
CA Event	Oracle Behavior Detection to CA Order	BD_ORDR
CA Event	Oracle Behavior Detection to CA Evented Order	BD_ORDR_EVNT
CA Event	Oracle Behavior Detection to CA Order Event	BD_ORDR_EVENT
CA Event	Oracle Behavior Detection to CA Security	BD_SCRTY

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Event	Oracle Behavior Detection to CA Evented Security	BD_SCRTY_EVNT
CA Event	Oracle Behavior Detection to CA Security Market Daily Profile	BD_SCRTY_MKT_DAILY
CA Event	Oracle Behavior Detection to CA Evented Security Market Daily Profile	BD_SCRTY_MKT_DAILY_EVNT
CA Event	Oracle Behavior Detection to CA Security Firm Daily Profiles	BD_SCRTY_FIRM_DAILY
CA Event	Oracle Behavior Detection to CA Evented Security Firm Daily Profiles	BD_SCRTY_FIRM_DAILY_EVNT
CA Event	Oracle Behavior Detection to CA Event Entity Map Execution	BD_EVENT_ENTITY_MAP_EXCTN
CA Event	Oracle Behavior Detection to CA Evented Execution	BD_EXECUTION_EVNT
CA Event	Oracle Behavior Detection to CA Trade Execution	BD_TRADE_EXECUTION_EVENT 4. BD_Create_Case
CA Lookup	Oracle Behavior Detection to CA Account ATM Daily Lookup	BD_ACCOUNTATMDAILY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account ATM Daily Lookup	BD_CustomerBalance_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Balance Summary Lookup	BD_ACCT_SMRY_MNTH_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Client Bank Lookup	BD_ACCT_CLIENTBANK_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Daily Lookup	BD_ACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Group Lookup	BD_ACCOUNT_GROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Lookup	BD_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account PeerGroup Lookup	BD_ACCOUNT_PEERGROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Trade Daily Lookup	BD_ACCOUNTTRADEDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Account Transaction Daily Lookup	BD_ACCOUNTTRXNDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Anticipatory Profile Lookup	BD_ANTICIPATORYPRFL_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Back Office Transaction Lookup	BD_BACK_OFFICE_TRXN_LOOKUP

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Lookup	Oracle Behavior Detection to CA Cash Transaction Lookup	BD_CASH_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank Peer Transaction Summary Lookup	BD_CBPEERTRXNSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank PeerGroup Lookup	BD_CLIENTBANK_PEERGRP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Client Bank Summary Lookup	BD_CLINETBANKBSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA ClientBank Transaction Summary Lookup	BD_ACCT_PR_TRXN_SMR_MN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Account Lookup	BD_CUSTOMER_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Customer Lookup	BD_CUSTOMER_CUSTOMER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Daily Lookup	BD_CUSTOMERDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer MarketServed Lookup	BD_CUSTOMER_MRKTSRV_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Product Lookup	BD_CUSTOMER_PRODUCT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Summary Lookup	BD_CUSTOMERSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customers Lookup	BD_CUSTOMER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Customer Account Position	BD_ACCT_POSN
CA Lookup	Oracle Behavior Detection to CA Derived Address Lookup	BD_DERIVED_ADDRESS_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Employee Account Lookup	BD_EMPLOYEE_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Employee Lookup	BD_EMPLOYEE_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Event Lookup	BD_EVENT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA External Entity Daily Lookup	BD_EXTERNALENTITYDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA External Entity Lookup	BD_EXTERNAL_ENTITY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA House Hold Summary Lookup	BD_HOUSEHOLDSMRY_LOOKUP

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Lookup	Oracle Behavior Detection to CA Household Balance Lookup	BD_HOUSEHOLDBALDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Account Daily Lookup	BD_INSTLACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Account Summary Lookup	BD_INSTACCOUNTSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Institution Lookup	BD_INSTITUTION_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Insurance Policy Balance Lookup	BD_INSURANCEPOLICYBAL_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Insurance Policy Daily Lookup	BD_INSURANCEPOLICYDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA InsurancePolicy Customer Lookup	BD_INSURPOLICY_CUST_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Lookup	BD_INVESTMENT_ADVISOR_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Lookup	BD_INVESTMENTADVISORLOOKUP
CA Lookup	Oracle Behavior Detection to CA Investment Advisor Summary Lookup	BD_INVESTMENTSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA LinkAnalysis Lookup	BD_LINKANALYSIS_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Loan Lookup	BD_LOAN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Loan Summary Lookup	BD_LOANSMRY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA MI Transaction Lookup	BD_MI_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Managed Account Daily Lookup	BD_MANAGEDACCOUNTDLY_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Managed Account Lookup	BD_MANAGEDACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Market Center Lookup	BD_MARKET_CENTER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA NetworkLogon Lookup	BD_NETWORKLOGON_LOOKUP
CA Lookup	Oracle Behavior Detection to CA NetworkUser Account Lookup	BD_NTWKUSER_ACCOUNT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Online Account Lookup	BD_ONLINEACCOUNT_LOOKUP

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Lookup	Oracle Behavior Detection to CA OnlineAccount Account Lookup	BD_ONLINEACCT_ACCT_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Peer Group Lookup	BD_PEER_GROUP_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Trade Lookup	BD_TRADE_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Wire Transaction Lookup	BD_WIRE_TRXN_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Execution Lookup	BD_EXECUTION_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Issuer Lookup	BD_ISSUER_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Issuer	BD_ISSUER
CA Lookup	Oracle Behavior Detection to CA Organization Lookup	BD_ORG_LOOKUP
CA Lookup	Oracle Behavior Detection to CA Organization	BD_ORG**
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account	BD_EVENT_ENTITY_MAP_AC
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Balance Position Summary	BD_EVENT_ENTITY_MAP_ABPS
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Group	BD_EVENT_ENTITY_MAP_AG
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Account Summary Month	BD_EVENT_ENTITY_MAP_ASM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Back Office Transaction	BD_EVENT_ENTITY_MAP_BOT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Cash Transaction	BD_EVENT_ENTITY_MAP_CT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Client Bank Summary Month	BD_EVENT_ENTITY_MAP_CBSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Customer	BD_EVENT_ENTITY_MAP_CUST
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Customer Summary Month	BD_EVENT_ENTITY_MAP_CSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Derived Address	BD_EVENT_ENTITY_MAP_DA
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Employee	BD_EVENT_ENTITY_MAP_EMPL
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map External Entity	BD_EVENT_ENTITY_MAP_EE
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Institution Master	BD_EVENT_ENTITY_MAP_IM

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Investment Advisor	BD_EVENT_ENTITY_MAP_IA
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Loan	BD_EVENT_ENTITY_MAP_LOAN
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Loan summary month	BD_EVENT_ENTITY_MAP_LSM
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map MI Transaction	BD_EVENT_ENTITY_MAP_MIT
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Trade	BD_EVENT_ENTITY_MAP_TRADE
CA Event Entity Map	Oracle Behavior Detection to CA Event Entity Map Wire Transaction	BD_EVENT_ENTITY_MAP_WT
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Account ATM summary daily	BD_EVENT_ENTITY_MAP_AASD
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Anticipatory Profile	BD_EVENT_ENTITY_MAP_NP
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Employee Account	BD_EVENT_ENTITY_MAP_EA
CA Event Entity Map	Oracle Behavior Detection to CA Event entity map Household Balance position summary	BD_EVENT_ENTITY_MAP_HBPS
CA Event Entity Map	Oracle Behavior Detection to CA Event Scoring	BD_EVENT_SCORE
CA Business	Oracle Behavior Detection to CA Account	BD_ACCT
CA Business	Oracle Behavior Detection to CA Account ATM summary Daily	BD_ACCT_ATM_SMRY_DAILY
CA Business	Oracle Behavior Detection to CA Account Address	BD_ACCT_ADDR
CA Business	Oracle Behavior Detection to CA Account Balance Position Summary	BD_ACCT_BAL_POSN_SMRY
CA Business	Oracle Behavior Detection to CA Account Email Address	BD_ACCT_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Account Group	BD_ACCT_GRP
CA Business	Oracle Behavior Detection to CA Account Institution mapping	BD_ACCT_ID_INSTN_ID_MAP
CA Business	Oracle Behavior Detection to CA Account List Membership	BD_ACCT_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Account Peer Group	BD_ACCT_PEER_GRP
CA Business	Oracle Behavior Detection to CA Account Peer Transaction Summary Month	BD_ACCT_PEER_TRXN_SMRY_MNTH

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Business	Oracle Behavior Detection to CA Account Phone	BD_ACCT_PHON
CA Business	Oracle Behavior Detection to CA Account Restriction	BD_ACCT_RSTRN
CA Business	Oracle Behavior Detection to CA Account Summary Month	BD_ACCT_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Account Supplemental Attribute	BD_ACCT_SUPPLEMENTAL_ATR
CA Business	Oracle Behavior Detection to CA Anticipatory Profile	BD_NTCPTRY_PRFL
CA Business	Oracle Behavior Detection to CA Back Office Transaction	BD_BACK_OFFICE_TRXN
CA Business	Oracle Behavior Detection to CA Cash Transaction	BD_CASH_TRXN
CA Business	Oracle Behavior Detection to CA Client Bank	BD_CLIENT_BANK
CA Business	Oracle Behavior Detection to CA Client Bank List Membership	BD_CB_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Client Bank Peer Group	BD_CLIENT_BANK_PEER_GRP
CA Business	Oracle Behavior Detection to CA Client Bank Peer Transaction Summary Month	BD_CB_PR_TRXN_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Client Bank Summary Month	BD_CLIENT_BANK_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Customer Account Role	BD_CUST_ACCT_ROLE
CA Business	Oracle Behavior Detection to CA Customer to Customer	BD_CUST_CUST
CA Business	Oracle Behavior Detection to CA Customers	BD_CUST
CA Business	Oracle Behavior Detection to CA Customers Account	BD_CUST_ACCT
CA Business	Oracle Behavior Detection to CA Customers Address	BD_CUST_ADDR
CA Business	Oracle Behavior Detection to CA Customers Email Address	BD_CUST_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Customers IMP License	BD_CUST_IMP_LICENSE
CA Business	Oracle Behavior Detection to CA Customers IMP License Good	BD_CUST_IMP_LICENSE_GOOD
CA Business	Oracle Behavior Detection to CA Customers List Membership	BD_CUST_LIST_MEMBERSHIP
CA Business	Oracle Behavior Detection to CA Customers Phone	BD_CUST_PHON
CA Business	Oracle Behavior Detection to CA Customers Summary Months	BD_CUST_SMRY_MNTH

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Business	Oracle Behavior Detection to CA Customers Supplemental Attribute	BD_CUST_SUPPLEMENTAL_ATR
CA Business	Oracle Behavior Detection to CA Derived Address	BD_DERIVED_ADDRESS
CA Business	Oracle Behavior Detection to CA Employee	BD_EMP
CA Business	Oracle Behavior Detection to CA Employee List	BD_EMPLOYEE
CA Business	Oracle Behavior Detection to CA Employee Address	BD_EMP_ADDR
CA Business	Oracle Behavior Detection to CA Employee Email Address	BD_EMP_EMAIL_ADDR
CA Business	Oracle Behavior Detection to CA Employee Phone	BD_EMP_PHON
CA Business	Oracle Behavior Detection to CA Employee to Account	BD_EMP_ACCT
CA Business	Oracle Behavior Detection to CA External Entity	BD_EXTERNAL_ENTITY
CA Business	Oracle Behavior Detection to CA External Entity Address	BD_EXTERNAL_ENTITY_ADDR
CA Business	Oracle Behavior Detection to CA External Entity Link	BD_FCC_EXTERNAL_ENTITY_LINK
CA Business	Oracle Behavior Detection to CA External Entity Membership	BD_EXTRNAL_NTTY_MMBRSHP
CA Business	Oracle Behavior Detection to CA House Hold Summary Month	BD_EVENT_ENTITY_MAP_HSM
CA Business	Oracle Behavior Detection to CA HouseHold Balance Position Summary	BD_HH_BAL_POSN_SMRY
CA Business	Oracle Behavior Detection to CA Household summary Month	BD_HH_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Institution Master	BD_INSTN_MASTER
CA Business	Oracle Behavior Detection to CA Institutional Account Summary Month	BD_INSTL_ACCT_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA Insurance Policy	BD_INSURANCE_POLICY
CA Business	Oracle Behavior Detection to CA Insurance Policy Customer	BD_INSURANCE_POLICY_CUST
CA Business	Oracle Behavior Detection to CA Insurance Product	BD_INSURANCE_PRODUCT
CA Business	Oracle Behavior Detection to CA Investment Manager	BD_NVSMT_MGR
CA Business	Oracle Behavior Detection to CA Investment Manager Summary Month	BD_NVSMT_MGR_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA LinkAnalysis Link	BD_LINKANALYSIS_LINK
CA Business	Oracle Behavior Detection to CA LinkAnalysis LinkSummary	BD_LINKANALYSIS_LINKSUMMARY

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Business	Oracle Behavior Detection to CA LinkAnalysis Network	BD_LINKANALYSIS_NETWORK
CA Business	Oracle Behavior Detection to CA LinkAnalysis Node	BD_LINKANALYSIS_NODE
CA Business	Oracle Behavior Detection to CA LinkAnalysis TypeSummary	BD_LINKANALYSIS_TYPESUMMARY
CA Business	Oracle Behavior Detection to CA Loan	BD_LOAN
CA Business	Oracle Behavior Detection to CA Loan Summary Month	BD_LOAN_SMRY_MNTH
CA Business	Oracle Behavior Detection to CA MI Transaction	BD_MI_TRXN
CA Business	Oracle Behavior Detection to CA Managed Account	BD_MANGD_ACCT
CA Business	Oracle Behavior Detection to CA Online Account	BD_ONLINE_ACCT
CA Business	Oracle Behavior Detection to CA Online Account	BD_ONLINE_ACCT_ACCT
CA Business	Oracle Behavior Detection to CA Peer Group	BD_PEER_GRP
CA Business	Oracle Behavior Detection to CA Trade	BD_TRADE
CA Business	Oracle Behavior Detection to CA TransactionPartyCrossReference BOT	BD_TRXN_PARTY_XREF_BOT
CA Business	Oracle Behavior Detection to CA TransactionPartyCrossReference FOT	BD_TRXN_PARTY_XREF_FOT
CA Business	Oracle Behavior Detection to CA Wire Transaction	BD_WIRE_TRXN
Additional Information	BD_ENTITY_SUP_INFO This sub-process code has to be executed after the business data population (see the Business Metadata Movement)	BD_ENTITY_SUP_INFO
CA Evented	Oracle Behavior Detection to CA Evented Account	BD_ACCT_EVENT
CA Evented	Oracle Behavior Detection to CA Evented Account ATM summary Daily	BD_ACCT_ATM_SMRY_DAILY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Address	BD_ACCT_ACCT_ADDR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Balance Position Summary	BD_ACCT_BAL_POSN_SMRY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Group	BD_ACCT_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Peer Group	BD_ACCT_PEER_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Peer Transaction Summary Month	BD_ACCT_PR_TXN_SMRY_MN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Restriction	BD_ACCT_RSTRN_EVNT

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Evented	Oracle Behavior Detection to CA Evented Account Summary Month	BD_ACCT_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Account Supplemental Attribute	BD_ACCT_SUPPLEMENTAL_ATR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Anticipatory Profile	BD_NTCPTRY_PRFL_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Back Office Transaction	BD_BACK_OFFICE_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Cash Transaction	BD_CASH_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank	BD_CLIENT_BANK_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Peer Group	BD_CLINT_BNK_PR_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Peer Transaction Summary Month	BD_CB_PR_TXN_SM_MNT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Client Bank Summary Month	BD_CLNT_BNK_SM_MNT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customer Balance Position Summary	BD_CUST_BAL_POSN_SMRY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers	BD_CUST_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers IMP License	BD_CUST_IMP_LICENSE_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers IMP License Good	BD_CUST_IMP_LIC_GOD_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers Summary Months	BD_CUST_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customers Supsupplemental Attribute	BD_CUST_SUPPL_ATR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Customer Account Position	BD_ACCT_POSN_ARC
CA Evented	Oracle Behavior Detection to CA Evented Derived Address	BD_DERIVED_ADDRESS_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee	BD_EMP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee Address	BD_EMP_ADDR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee Email Address	BD_EMP_EMAIL_ADDR_EVNT

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Evented	Oracle Behavior Detection to CA Evented Employee Phone	BD_EMP_PHON_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Employee to Account	BD_EMP_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Entity	BD_EXTERNAL_ENTITY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Entity Address	BD_XTRNL_ENTY_ADR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented External Org	BD_EXTRL_ORG_EVNT
CA Evented	Oracle Behavior Detection to CA Evented HouseHold Balance Position Summary	BD_HH_BAL_POSN_SMRY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Household summary Month	BD_HH_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Institution Master	BD_INSTN_MASTER_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Policy	BD_INSURANCE_POLICY_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Policy Customer	BD_INS_PLCY_CUST_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Insurance Product	BD_INSURANCE_PRODUCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Investment Manager	BD_NVSMT_MGR_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Investment Manager Summary Month	BD_NVSMT_MGR_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Loan	BD_LOAN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Loan Summary Month	BD_LOAN_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented MI Transaction	BD_MI_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Managed Account	BD_MANGD_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Online Account	BD_ONLINE_ACCT_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Peer Group	BD_PEER_GRP_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Trade	BD_TRADE_EVNT

Table 94: Sub-processes

CA Area	Process Name	Process Parameter
CA Evented	Oracle Behavior Detection to CA Evented Wire Transaction	BD_WIRE_TRXN_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Institutional Account Summary Month	BD_INSTL_ACCT_SMRY_MNTH_EVNT
CA Evented	Oracle Behavior Detection to CA Evented Execution	BD_EXECUTION_EVNT

The following processes are related to network building block:

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

Table 95 describes the Promote to Case T2Ts.

Table 95: Promote_To_Case T2Ts

LEVEL 0	LEVEL 1	LEVEL2	LEVEL 3
KDD_CASES	KDD_CASE_ACCOUNTS	KDD_CASE_ACCT_ADDRS	
	KDD_CASE_ACCT_ATM_SMRY_DAILY	KDD_CASE_ACCT_BAL_POSN_SMRY	
	KDD_CASE_ACCT_GRP	KDD_CASE_ACCT_LIST_MEMBERSHIPS	
	KDD_CASE_ACCT_ID_INSTN_ID_MAP	KDD_CASE_ACCT_RSTRNS	
	KDD_CASE_ACCT_PEER_GRP	KDD_CASE_ACCT_SMRY_MNTH	
	KDD_CASE_ACT_PEER_TXN_SMR_MNTH	KDD_CASE_ACCT_SUPPL_ATTR	
	KDD_CASE_ATTRBT_VAL_MAP	KDD_CASE_INSTL_ACCT_SMRY_MNTH	
	KDD_CASE_BACK_OFFICE_TRXN	KDD_CASE_MANGD_ACCT	
	KDD_CASE_CASH_TRXN	KDD_CASE_ACCT_EMAIL_ADDR	
	KDD_CASE_CB_PEER_TXN_SMRY_MNTH	KDD_CASE_ACCT_PHON	
	KDD_CASE_CUSTOMERS	KDD_CASE_HH_BAL_POSN_SMRY	
	KDD_CASE_CUST_ACCT	KDD_CASE_HH_SMRY_MNTH	
	KDD_CASE_CUST_CREDIT_RTNG	KDD_CASE_CUST_ADDRS	
	KDD_CASE_DERIVED_ADDRESS	KDD_CASE_CUST_EMAILS	
	KDD_CASE_EMP	KDD_CASE_CUST_LIST_MEMBERSHIPS	
	KDD_CASE_EMP_ACCT	KDD_CASE_CUST_PHONS	

Table 95: Promote_To_Case T2Ts

LEVEL 0	LEVEL 1	LEVEL2	LEVEL 3
	KDD_CASE_INSTN_MASTER	KDD_CASE_CUST_SMRY_MNTH	
	KDD_CASE_INSTRUCTION	KDD_CASE_CUST_SUPPL_ATTR	
	KDD_CASE_INVOLVED_PARTY_LINK	KDD_CASE_EMP_ADDR	
	KDD_CASE_LINKS	KDD_CASE_EMP_EMAIL_ADDR	
	KDD_CASE_LOAN	KDD_CASE_EMP_PHONE	
		KDD_CASE_CUST_CUST	
	KDD_CASE_LOSS_RECOVERY	KDD_CASE_CB_LIST_MEMBERSHIP	KDD_CASE_EXTRNL_NTITY_ADDR KDD_CASE_EXTRNL_NTITY_MBRSHP KDD_CASE_EXTRL_NTITY_SMRY_MNTH
	KDD_CASE_LOSS_RECVRY_COST_CR	KDD_CASE_CLIENT_BANK	
	KDD_CASE_MI_TRXN	KDD_CASE_CLIENT_BANK_PEER_GRP	
	KDD_CASE_NARRATIVE	KDD_CASE_CLIENT_BANK_SMRY_MNTH	

- KDD_CASE_ACCOUNTS (Level 1) process has to be executed before the execution of KDD_CASE_ACCT_ADDRS, KDD_CASE_ACCT_BAL_POSN_SMRY, KDD_CASE_ACCT_LIST_MEMBERSHIPS, KDD_CASE_ACCT_RSTRNS, KDD_CASE_ACCT_SMRY_MNTH, KDD_CASE_ACCT_SUPPL_ATTR, KDD_CASE_INSTL_ACCT_SMRY_MNTH, KDD_CASE_MANGD_ACCT, KDD_CASE_ACCT_EMAIL_ADDR, and KDD_CASE_ACCT_PHON.
- KDD_CASE_ACCT_GRP (Level 1) process has to be executed before the execution of KDD_CASE_HH_BAL_POSN_SMRY, and KDD_CASE_HH_SMRY_MNTH.
- KDD_CASE_CUSTOMERS (Level 1) process has to be executed before the execution of KDD_CASE_CUST_ADDRS, KDD_CASE_CUST_EMAILS, KDD_CASE_CUST_LIST_MEMBERSHIPS, KDD_CASE_CUST_PHONS, KDD_CASE_CUST_SMRY_MNTH, and KDD_CASE_CUST_SUPPL_ATTR.
- KDD_CASE_EMP (Level 1) process has to be executed before the execution of KDD_CASE_EMP_ADDR, KDD_CASE_EMP_EMAIL_ADDR, and KDD_CASE_EMP_PHON.
- KDD_CASE_INSTN_MASTER (Level 1) process has to be executed before execution of KDD_CASE_CB_LIST_MEMBERSHIP, KDD_CASE_CLIENT_BANK, KDD_CASE_CLIENT_BANK_PEER_GRP, KDD_CASE_CLIENT_BANK_SMRY_MNTH, and KDD_CASE_EXTERNAL_ENTITY.
- KDD_CASE_LOAN (Level 1) process has to be executed before the execution of KDD_CASE_LOAN_SMRY_MNTH.
- KDD_CASE_NVSMT_MGR (Level 1) process has to be executed before the execution of KDD_CASE_NVSMT_MGR_SMRY_MNTH.
- KDD_CASE_EXTERNAL_ENTITY (Level 2) process has to be executed before execution of KDD_CASE_EXTRNL_NTITY_ADDR, KDD_CASE_EXTRNL_NTITY_MBRSHP, and KDD_CASE_EXTRL_NTITY_SMRY_MNTH.

20.1.7 End Batch

BD_ECM_End_E2E_Batch is used for ending the batch execution for BD.

20.2 OCS Application Process

The following processes are used for this:

- Start Batch
- Load Data from CS to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

20.2.1 Start Batch

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

20.2.2 Load Data from CS to ECM

Load_From_CS_To_CA is used for loading the CS data from the Landing area to the Consolidation area. This has the 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

20.2.3 Correlation

This is used to perform correlation on loaded CS events.

- DT_CORRELATION

20.2.4 Scoring

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

- Pre-Case-Scoring For Oracle CS

20.2.5 Promote to Case

Promote_To_Case_Decision_OCS is used to decide if an OCS correlation can be promoted to a case. This is based on the defined threshold limit.

This has the following sub-process:

- Pre Case Promotion Rule

20.2.6 Create Case

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

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts
- CASE_COMPLETION_FLAG

20.2.7 End Batch

ECM_End_E2E_Batch_For_CS is used for ending the batch execution for CS.

20.3 OKYC Application Process

The following processes are used for this:

- Start Batch
- Load Data from KYC to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- Update Case ID
- End Batch

Perform these steps:

1. Login as ECM ADMIN.
2. Before executing the "Oracle KYC Event Processing" batch, add the Data Transformation task "BD_POPULATE_ENTITY_RELATION" in the "Oracle KYC Event Processing" batch after the "Third Party Generate Cases" task and save.

> **NOTE** Refer to the Adding Transformation Rule section.

20.3.1 Start Batch

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

20.3.2 Load Data from KYC to ECM

Load_From_OKYC_To_CA process loads OKYC data from the Landing area to the Consolidation area. This has the 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

20.3.3 Correlation

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

- DT_CORRELATION

20.3.4 Scoring

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

- Pre-Case Scoring For Oracle KYC

20.3.5 Promote to Case

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

- POPULATE_P2C_FL_OKYC

20.3.6 Create Case

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

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts
- CASE_COMPLETION_FLAG

20.3.7 Update Case ID

UPD_CaseId_To_OKYC is used for updating the Case IDs to OKYC.

20.3.8 End Batch

ECM_End_E2E_Batch_For_KYC is used for ending the batch execution for KYC.

20.4 OSTDO Application Process

The following processes are used for this:

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

20.4.1 Start Batch

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

20.4.2 Load Data from STDO to Consolidation Area

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

- STDO_Event_Load
- STDO_Entity_Surrogate_Key_Gen
- STDO_Business_Data_Load
- STDO_SUPLMTRY_INFO
- STDO_Evented_Data_Load

Here, Level 0 sub-process code execution is a prerequisite for Level 1 subprocess execution. Similarly, Level 1 sub-process code execution is a prerequisite for Level 2 sub-process execution and so on. Subprocess within a level can be executed in any order or it can be executed in parallel as shown in Table 96

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
STDO_Event_Load	STDO_EVENT_LOOKUP	
	STDO_EVENT	
	STDO_EVENT_BINDING	
	STDO_EVENT_DETAILS	
STDO_Entity_Surrogate_Key_Gen	BD_ACCOUNTATMDAILY_LOOKUP	STDO_EVENT_ENTITY_MAP
	BD_ACCOUNTDLY_LOOKUP	STDO_EVENT_ENTITY_MAPII
	BD_ACCOUNTTRADEDLY_LOOKUP	STDO_EVENT_ENTITY_MAPIII

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
	BD_ACCOUNTTRXNDLY_LOOKUP	STDO_EVENT_ENTITY_MAPIV
	BD_ACCOUNT_GROUP_LOOKUP	
	BD_ACCOUNT_PEERGROUP_LOOKUP	
	BD_ACCT_CLIENTBANK_LOOKUP	
	BD_ACCT_PR_TRXN_SMR_MN_LOOKUP	
	BD_ACCT_SMRY_MNTH_LOOKUP	
	BD_CBPEERTRXNSMRY_LOOKUP	
	BD_CLIENTBANK_PEERGRP_LOOKUP	
	BD_CLINETBANKBSMRY_LOOKUP	
	BD_CUSTOMERBALANCE_LOOKUP	
	BD_CUSTOMERDLY_LOOKUP	
	BD_CUSTOMERSMRY_LOOKUP	
	BD_CUSTOMER_ACCOUNT_LOOKUP	
	STDO_ACCOUNT_LOOKUP	
	STDO_CUSTOMER_LOOKUP	
	STDO_BACK_OFFICE_TRXN_LOOKUP	
	STDO_CASH_TRXN_LOOKUP	
	STDO_MI_TRXN_LOOKUP	
	STDO_WIRE_TRXN_LOOKUP	
	BD_CUSTOMER_PRODUCT_LOOKUP	
	BD_DERIVED_ADDRESS_LOOKUP	
	BD_EMPLOYEE_ACCOUNT_LOOKUP	

Table 96: Load Data from STDO to Consolidation Area

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

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
	BD_ACCT_ID_INSTN_ID_MAP	
	BD_ACCT_LIST_MEMBERSHIP	
	BD_ACCT_PEER_GRP	
	BD_ACCT_PEER_TRXN_SMRY_MNTH	
	BD_ACCT_SMRY_MNTH	
	BD_ACCT_SUPPLEMENTAL_ATR	
	BD_BACK_OFFICE_TRXN	
	BD_CASH_TRXN	
	BD_CB_LIST_MEMBERSHIP	
	BD_CB_PR_TRXN_SMRY_MNTH	
	BD_CLIENT_BANK	
	BD_CLIENT_BANK_PEER_GRP	
	BD_CLIENT_BANK_SMRY_MNTH	
	BD_CUST	
	BD_ONLINE_ACCT_ACCT	
	STDO_ACCT	
	STDO_ACCT_ADDR	
	STDO_ACCT_EMAIL_ADDR	
	STDO_ACCT_PHON	
	STDO_ACCT_RSTRN	
	STDO_ACCT_LIST_MEMBERSHIP	
	BD_CUST_ACCT	
	BD_CUST_ACCT_ROLE	
	BD_CUST_ADDR	
	BD_CUST_CUST	
	BD_CUST_EMAIL_ADDR	
	BD_CUST_LIST_MEMBERSHIP	
	BD_CUST_PHON	
	BD_CUST_SMRY_MNTH	

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
	BD_CUST_SUPPLEMENTAL_ATR	
	BD_DERIVED_ADDRESS	
	BD_EMP	
	BD_EMP_ACCT	
	BD_EMP_ADDR	
	BD_EMP_EMAIL_ADDR	
	BD_EMP_PHON	
	BD_EXTERNAL_ENTITY	
	BD_EXTERNAL_ENTITY_ADDR	
	BD_EXTRNAL_NTTY_MMBRSHP	
	BD_HH_BAL_POSN_SMRY	
	BD_HH_SMRY_MNTH	
	BD_HOUSE_HOLD	
	BD_INSTL_ACCT_SMRY_MNTH	
	BD_INSTN_MASTER	
	BD_INSURANCE_POLICY	
	BD_INSURANCE_POLICY_CUST	
	BD_INSURANCE_PRODUCT	
	BD_LOAN	
	BD_LOAN_SMRY_MNTH	
	BD_MANGD_ACCT	
	BD_MI_TRXN	
	BD_NTCPTRY_PRFL	
	BD_NVSMT_MGR	
	BD_NVSMT_MGR_SMRY_MNTH	
	BD_ONLINE_ACCT	
	BD_WIRE_TRXN	
STDO_SUPLMTRY_INFO	Studio Supplementary Information	
STDO_Evented_Data_Load	STDO_ACCT_EVENT	
	STDO_CUST_EVENT	

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
	STDO_EMP_EMAIL_ADDR_EVNT	
	STDO_ACCT_PR_TXN_SMRY_MN_EVNT	
	STDO_ACCT_SMRY_MNTH_EVNT	
	STDO_MI_TRXN_EVNT	
	STDO_ACCT_BAL_POSN_SMRY_EVNT	
	STDO_HH_BAL_POSN_SMRY_EVNT	
	STDO_INSTN_MASTER	
	STDO_BOT_EVNT	
	STDO_CASH_TRXN_EVNT	
	STDO_EMP_ACCT_EVNT	
	STDO_ACCT_PEER_GRP_EVNT	
	STDO_NTCPTRY_PRFL_EVNT	
	STDO_ACCT_SUPPLEMENTAL_ATR_EVN	
	STDO_WIRE_TRXN_EVNT	
	STDO_EMP_PHON_EVNT	
	STDO_ONLINE_ACCT_ACCT_EVNT	
	STDO_EMP_ADDR_EVNT	
	STDO_ACCT_ADDR_EVNT	
	STDO_CUST_SMRY_MNTH_EVNT	
	STDO_ONLINE_ACCT_EVNT	
	STDO_EMP_EVNT	
	STDO_ACCT_RSTRN_EVNT	
	STDO_CUST_SUPPL_ATR_EVNT	
	STDO_ACCT_GRP_EVNT	
	STDO_MANGD_ACCT_EVNT	
	STDO_HH_SMRY_MNTH_EVNT	
	STDO_CLIENT_BANK_EVNT	

Table 96: Load Data from STDO to Consolidation Area

Level 0	Level 1	Level 2
	STDO_ACCT_ATM_SMRY_DAILY_EVNT	
	STDO_DERIVED_ADDRESS_EVNT	

20.4.3 Correlation

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

- DT_CORRELATION

20.4.4 Scoring

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

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

20.4.5 Promote to Case

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

- Pre Case Promotion Rule

20.4.6 Create Case

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

The following is the list of Promote_To_Case T2Ts:

- Oracle Behavior Detection Generate Cases Below is the list of T2T tasks for STDO application:
- f_generatecaseid
- f_insertcases
- t2t_KDD_CASE_ACCOUNTS
- t2t_KDD_CASE_CUSTOMERS
- t2t_KDD_CASE_DERIVED_ADDRESS
- t2t_KDD_CASE_EMPLOYEES
- t2t_KDD_CASE_ACCOUNT_ADDRESS
- t2t_KDD_CASE_ACCOUNT_MANAGED
- t2t_KDD_CASE_ACCOUNT_RSTRNS
- t2t_KDD_CASE_ACCT_BAL_POSN_SMRY

- t2t_KDD_CASE_ACCT_EMAIL_ADDR
- t2t_KDD_CASE_ACCT_PEER_GRP
- t2t_KDD_CASE_ACCT_PHON
- t2t_KDD_CASE_ACCT_SMRY_MNTH
- t2t_KDD_CASE_ACCT_SUPPL_ATTR
- t2t_KDD_CASE_ACT_PEER_TRXN_SMRY
- t2t_KDD_CASE_ACCT_NTCPTRY_PRFL
- t2t_FCC_CASE_ACCT_LIST_MBRSP
- t2t_KDD_CASE_CLIENT_BANK
- t2t_KDD_CASE_CLIENT_BANK_SMRY_MNTH
- t2t_KDD_CASE_CUST_ADDR
- t2t_KDD_CASE_CUST_EMAIL_ADDRS
- t2t_KDD_CASE_CUST_LIST_MEMBERSHIP
- t2t_KDD_CASE_CUST_PHONE
- t2t_KDD_CASE_CUST_SUPPL_ATTR
- t2t_KDD_CASE_CUST_SMRY_MNTH
- t2t_KDD_CASE_EMP_ACCT
- t2t_KDD_CASE_EMP_ADDR
- t2t_KDD_CASE_EMP_EMAIL_ADDR
- t2t_KDD_CASE_EMP_PHONE
- t2t_KDD_CASE_INSTL_ACCT_SMRY_MNTH
- t2t_KDD_CASE_INSTN_MASTER
- t2t_KDD_CASE_INSURANCE_POLICY
- t2t_KDD_CASE_INSURANCE_PRODUCT
- t2t_KDD_CASE_NTWK_USER_ACCT_MAP
- t2t_KDD_CASE_ONLINE_ACCT
- t2t_KDD_CASE_ONLINE_ACCT_ACCT
- t2t_KDD_CASE_PEER_GRP
- t2t_KDD_CASE_CB_LIST_MEMBERSHIP
- t2t_KDD_CASE_CB_PEER_TXN_SMRY_MNTH
- t2t_KDD_CASE_CLIENT_BANK_PEER_GRP
- t2t_KDD_CASE_EXTERNAL_ENTITY
- t2t_KDD_CASE_EXTERNAL_ENTITY_MEMBERSHIP
- t2t_KDD_CASE_HH_ACCT_BAL_SMRY
- t2t_KDD_CASE_HH_SMRY_MNTH
- t2t_KDD_CASE_INSURANCE_PLCY_CUST

- t2t_KDD_CASE_NVSMT_MGR_SMRY_MNTH
- t2t_KDD_CASE_NVSMT_MGR
- t2t_KDD_CASE_ACCT_ID_INSTN_ID_MAP
- t2t_KDD_CASE_ACCT_GRP
- t2t_KDD_CASE_WIRE_TRXN
- t2t_KDD_CASE_CASH_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_CASH_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_MI_TRXN
- t2t_KDD_CASE_DERIVED_ADDRESS_WIRE_TRXN
- t2t_KDD_CASE_BACK_OFFICE_TRXN
- t2t_KDD_CASE_CUST_IMP_LICENSE_GOODS
- t2t_KDD_CASE_CUST_IMP_LICENSE
- t2t_KDD_CASE_DOC_COLL_CNTRCT
- t2t_KDD_CASE_DOC_COLL_CNTRCT_EVENT
- t2t_KDD_CASE_DOC_COLL_DISCRP_DTL
- t2t_KDD_CASE_DOC_COLL_INVOICE
- t2t_KDD_CASE_DOC_COLL_MULTNR_DTL
- t2t_KDD_CASE_DOC_COLL_SHPMT_DTL
- t2t_KDD_CASE_EXTERNAL_INSURANCE_PLCY
- t2t_KDD_CASE_EXTERNAL_ORG
- t2t_KDD_CASE_TRADE_FIN_SWIFT_MSG
- t2t_KDD_CASE_TRADE_FIN_PARTY
- t2t_KDD_CASE_TRADE_FIN_GOOD_SRVC
- t2t_KDD_CASE_TRADE_FIN_DRAFT
- t2t_KDD_CASE_TRADE_FIN_DOC
- t2t_KDD_CASE_TRADE_FIN_CNTRCT
- t2t_KDD_CASE_TRADE_FIN_BRKRGE_DIST
- t2t_KDD_CASE_TRADE_FIN_BRKRGE
- t2t_KDD_CASE_TRADE_FIN_ACCT
- t2t_KDD_CASE_TRADE
- t2t_KDD_CASE_ORDER
- t2t_KDD_CASE_MI_TRXN
- t2t_KDD_CASE_LOAN_ACCOUNT
- t2t_KDD_CASE_LOAN
- t2t_KDD_CASE_LOAN_SMRY_MONTH
- t2t_KDD_CASE_INSTRUCTION

- CASE_COMPLETION_FLAG
- CASE_ASSIGNMENT

20.4.7 End Batch

STDO_ECM_End_E2E_Batch is used for ending the batch execution for Studio.

20.5 Third-party Application Process

The following processes are used for this:

- Start Batch
- Load Data from Third-party to ECM
- Correlation
- Scoring
- Promote to Case
- Create Case
- End Batch

20.5.1 Start Batch

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

20.5.2 Load Data from Third-party to ECM

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

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

Table 97 contains the list of Third-party sub-process codes.

Here, Level 1 sub-process code execution is a prerequisite for Level 2 subprocess execution. Similarly, Level 2 sub-process code execution is a prerequisite for Level 3 sub-process execution and so on. Subprocess within a level can be executed in any order or it can be executed in parallel. **BD_ENTITY_SUP_INFO** sub-process code has to be executed after the business data population (see the **Business Metadata Movement**).

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
t2t_LOOKUP_EVENT	t2t_EVENTS	t2t_LOOKUP_ACCOUNT	t2t_FCC_EVENT_ENTITY_MAP_ACCOUNT	t2t_EVENTED_ACCT	t2t_FCC_TRXN_PIVOT_TRANSFORM_DS

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
	t2t_FC-C_EVENT_BINDING	t2t_LOOKUP_CUSTOMER	t2t_FCC_EVENT_ENTITY_MAP_CUSTOME R	t2t_EVENTED_ACCT_ADDR	t2t_FCC_TRXN_BNK2BNK_FL_DS
	t2t_FCC_EVENT_DETAILS	t2t_LOOKUP_EMPLOYEE	t2t_FCC_EVENT_ENTITY_MAP_EMPLOYE E	t2t_EVENTED_ACCT_RSTRN	t2t_FCC_TRXN_PARTY_XREF_BOT
		t2t_LOOKUP_EXTERNAL_ENTITY	t2t_FCC_EVENT_ENTITY_MAP_EXTERNAL_ENTITY	t2t_EVENTED_CUST	t2t_FCC_TRXN_PARTY_XREF_BOT_OFFSET
		t2t_LOOKUP_INSTITUTION_CB		t2t_EVENTED_CUST_CREDIT_RTNG	t2t_FCC_TRXN_PARTY_XREF_FOT
		t2t_LOOKUP_ACCOUNT_GROUP		t2t_EVENTED_EMP	
		t2t_LOOKUP_BOT t2t_LOOKUP_FOT		t2t_EVENTED_EMP_ACCT	
				t2t_EVENTED_EMP_ADDR	
			t2t_FCC_EVENT_ENTITY_MAP_CLIENT_B ANK	t2t_EVENTED_EMP_EMAIL_ADDR	
			t2t_FCC_EVENT_ENTITY_MAP_ACCOUNT	t2t_EVENTED_NTCPTRY_PRFL_ACCT	
			_GROUP	t2t_EVENTED_NTCPTRY_PRFL_CUST	
			t2t_FCC_EVENT_ENTITY_MAP_FOTWIRE	t2t_EVENTED_ACCT_BAL_POSN_SMRY	
			t2t_FCC_EVENT_ENTITY_MAP_FOTCASH	t2t_EVENTED_ACCT_GRP	
			t2t_FCC_EVENT_ENTITY_MAP_FOTMI	t2t_EVENTED_AUTO_QUOTE	

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				t2t_EVENTED_BACK_OFFICE_TRXN	
				t2t_EVENTED_CLIENT_BANK	
				t2t_EVENTED_CORP_ACTN	
				t2t_EVENTED_CUST_ADDR	
				t2t_EVENTED_CUST_SUPPLEMENTAL_ATTR	
				t2t_EVENTED_DERIVED_ADDRESS	
				t2t_EVENTED_EMP_PHON	
				t2t_EVENTED_EXTERNAL_ENTITY	
				t2t_EVENTED_INSTN_MASTER	
				t2t_EVENTED_MANGD_ACCT	
				t2t_EVENTED_ONLINE_ACCT	
				t2t_EVENTED_ONLINE_ACCT_ACCT	
				t2t_EVENTED_PEER_GRP	
		Stage to CA Customer Account Lookup		Stage to CA Account	
		Stage to CA Customer Customer Lookup		Stage to CA Account Address Email Address	

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
		Stage to CA Employee Account Lookup		Stage to CA Account Address Email Phone	
				Stage to CA Account Addrss	
		Stage to CA Account Daily Lookup		Stage to CA Customer	
				Stage to CA Customer Account	
				Stage to CA Customer Address	
				Stage to CA Customer Country	
				Stage to CA Customer Email Address	
				Stage to CA Customer Phone	
				Stage to CA Customer Supplemental Attribute	
				Stage to CA Customer to Customer Relation	
				Stage to CA Correspondent Bank	
				Stage to CA Back Office Transaction	
				Stage to CA Derived Address	
				Stage to CA Derived Entity	

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				Stage to CA Derived Entity Link	
				Stage to CA Derived Entity to Derived Address	
				Stage to CA Front Office Transaction Party	
				Stage to CA Financial Institution	
				Stage to CA Employee	
				Stage to CA Employee Address	
				Stage to CA Employee Email Address	
				Stage to CA Employee Phone	
				Stage to CA Front Office Transaction	
				Stage to CA Employee Account	
				Stage to CA Account Leases	

Table 97: Third-party sub-process codes

Level 1	Level 2	Level 3	Level 4	Level 5	Level 6
				BD_ENTITY_SUP_INFO This sub-process code has to be executed after the business data population (see the Business Metadata Movement). This sub-process code has to be executed after the business data population.	

The following tables are used for ECM third-party landing areas:

- STG_FCC_EVENT_CNTRCT_MSG
- STG_FCC_EVENT_CUST_IMP_LICENSE
- STG_FCC_EVENT_DOC_COLL_CNTR
- STG_FCC_EVENT_DOC_COLL_CNTR_EV
- STG_FCC_EVENT_DOC_COLL_DIS_DTL
- STG_FCC_EVENT_DOC_COLL_INVOICE
- STG_FCC_EVENT_DOC_COLL_MUL_DTL
- STG_FCC_EVENT_DOC_COLL_SHP_DTL
- STG_FCC_EVENT_TRADE_FIN_ACCT
- STG_FCC_EVENT_TRADE_FIN_BRKRGE
- STG_FCC_EVENT_TRADE_FIN_CNTRCT
- STG_FCC_EVENT_TRADE_FIN_DOC
- STG_FCC_EVENT_TRADE_FIN_DRAFT
- STG_FCC_EVENT_TRADE_FIN_PARTY
- STG_FCC_EVENT_TRD_FIN_BRK_DSTR
- STG_FCC_EVENT_TRD_FIN_CNTRCT
- STG_FCC_EVENT_TRD_FIN_CNTRCTET
- STG_FCC_EVENT_TRD_FIN_GD_SRVC
- STG_FCC_EVNT_CUST_IMP_LIC_GOOD

- STG_FCC_GOOD_SRVC

20.5.3 Correlation

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

- PGX_CORRELATION
- BD_CORRELATION

20.5.4 Scoring

This is used to perform the scoring of third-party events, entities, and correlation. This has the following sub-process:

- Entity_Scoring
- Event_Scoring
- Correlation_Scoring
- Pre_Case_Scoring

20.5.5 Promote to Case

Promote_To_Case_Decision is used to decide if a Third-party correlation can be promoted to a case. This is based on the defined threshold limit.

20.5.6 Create Case

Create_Case is used to create a case if a third-party event is promoted to the case. Following is the list of Promote_To_Case T2Ts:

- f_generatecaseid
- f_insertcases
- Promote_To_Case T2Ts
- CASE_COMPLETION_FLAG

20.5.7 End Batch

ECM_End_E2E_Batch is used for ending the batch execution.

21 Configuring Parallel Graph AnalytiX (PGX) Correlation

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

- Overview
- Pre-requisites

21.1 Overview

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

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

21.2 Pre-requisites

The following are the list of pre-requisites:

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

22 FAQs

This section of the document consists of resolution to the frequently asked questions during the configuration.

22.1 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).

22.2 What should be done if the second/third task is struggling to start?

Login to Config Schema and execute the following query:

Select * from PR2_PROCESS_TASK_PARAMETER

Make sure that the V_TASK_PARAMETER_VALUE column has the correct SOURCENAME, and also LOAD- TYPE is correct.

22.3 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.

22.4 What should be done if the batch needs a rerun?

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

There can be cases where the source schema is different but data resides in the same instance. In this case, Grant select to all user tables that need to be provided to the ECM Atomic schema from the source schema.

22.5 What should be done if Correlation fails in the first-time run?

Make sure to run the correlation.sh file. For more information, see the Pre-batch Execution Configuration.

22.6 Can I run the Batch again if data-loaded to CA went wrong?

- Yes, you can trigger a new batch. Before running the batch, you must clear all the data from all business, evented, and event tables for that MIS Date and Data Origin.
- Yes, you can trigger a new batch. Before that, you must remove the data from the Event tables. This will take more time than the above option.

What should I do, if I have loaded a few wrong records into a few business tables?

- You can trigger a new batch. Before running the batch, you must clear all the data from all business, evented and event tables for that MIS Date and Data Origin
- You can remove the data from the business tables for MIS Date and Data Origin, then run the batch only including the process for which you need to correct the data, and then end this batch. This will take more time than the above option.

22.7 How can I create new attributes?

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

22.8 How do I manage the parameters of attributes?

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

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

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

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

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

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

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

22.11 What is the Event Details tab?

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

22.12 Can I deactivate a case type or case class?

Unavailable in the current version.

22.13 Can I rename tabs?

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

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

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

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

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

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

For more information, see the Configuring Processing Modelling Framework (PMF) section.

Table 98 describes the ECM Licencing Information.

Table 98: ECM Licencing Information

Products	Licensing Description

Each Oracle Financial Services Enterprise Case Management application pack includes the following product:
• Oracle Financial Services Enterprise Case Management (ECM)
• Oracle Financial Services Enterprise Case Management Front Office User
	Prerequisites
	• Operating System
	  ▪ Oracle Linux / Red Hat Enterprise Linux (x86-64)
	  ▪ Oracle Solaris(SPARC)
	  ▪ IBM AIX (PowerPC)
	  ▪ Shell
	• Java Runtime Environment
	  ▪ Oracle Linux / Red Hat Enterprise Linux
	  ▪ Oracle Solaris
	  ▪ IBM AIX
	• Oracle Database Server and Client
	• Web Server/ Web Application Server
	  ▪ WebLogic
	  ▪ WebSphere
	  ▪ Apache Tomcat
	• Third party software tools used in the application pack
	  ▪ Fontbox 2.0.11
	  ▪ Pdfbox 2.0.11
	Important Notes:
	• "Application Users can only be assigned the Front Office Analyst role. The permissions associated to this role cannot be modified.
	• "The Front Office Analyst role can only be implemented to allow for the initial disposition of a case. Users can only have access to a case in a New status and then only take one of two types of actions: Close or Move to Investigation.
	• "Front Office Analyst users cannot create manual events or manual cases.

OFSAA Support Contact Details

Raise a Service Request (SR) in My Oracle Support (MOS) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.