Administration Tools User Guide

Release 8.0.7.0.0
Dec 2018

ORACLE®
FINANCIAL SERVICES

ORACLE®

Administration Tools User Guide

Release 8.0.7.0.0
Dec 2018

Part Number: E90544-01

Revision History

The following table describes the revision history of the Administration Tools User Guide.

Date	Edition	Description
Oct 2017	First edition of 8.0.5	Removed all case-related information for 805.
Jan 2019	First edition of 8.0.7	Removed the IPE chapter.

Contents

List of Figures

List of Tables

List of Tables

About this Guide

This guide identifies the Administration Tools used with the Oracle Financial Services Behavior Detection Framework, and describes how to use them. This chapter details the following:

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

Who Should Use this Guide

The *Administration Tools User Guide* is designed for data miners and Oracle Administrators. Their roles and responsibilities include the following:

- **Data Miner:** Accesses the Administration Tools to modify the threshold values used by patterns to detect matches in Firm data.
- **Oracle Administrator:** Accesses the Administration Tools to modify the logic parameters used by the system to process matches into alerts, score the alerts, and distribute the alerts. In addition, Oracle Administrators can reload the cache. This user is usually an employee of a specific Oracle customer.

Scope of this Guide

This guide describes how to use the Administration Tools to customize the scenario threshold, alert creation, and alert scoring.

How this Guide is Organized

The *Administration Tools User Guide* includes the following chapters:

- Chapter 1, *Overview of FCCM,* provides an overview of Oracle Financial Services Financial Crimes and Compliance Management, how it works, and what it does.

- Chapter 2, *About the Administration Tools,* describes how to access the tools and identifies what elements are common to all tools.

- Chapter 3, *Scenario Threshold Editor,* describes how to use this tool to modify the threshold values

- Chapter 4, *Scenario Wizard,* describes how to use the Scenario Wizard tool to create scenarios.

- Chapter 5, *Alert Creator Editor,* describes how to use this tool to automatically group the matches that share similar information into a single alert. It also explains how to create new rules, modify the logic behind existing rules, and delete rules. The tool also displays the job ID and the job template ID for all the rules created.

- Chapter 6, *Alert Scoring Editor,* describes how to create new rules or modify the logic behind existing rules that prioritize alerts automatically.

- Chapter 7, *Alert Assigner Editor,* describes how to assign ownership of alerts.

- Chapter 8, *Threshold Analyzer,* introduces you the Threshold Analyzer utility and describes how to view and operate the source business and Threshold Analyzer data.

- Chapter 9, *Security Configuration,* covers the required day-to-day operations and maintenance of OFSBDF users, groups, and organizational units.

- The *Index* provides access to specific topics for this tool.

Where to Find More Information

For more information about Oracle Financial Services Behavior Detection Framework, refer to the following documents:

- *Installation Guide*

- *Oracle Financial Services Advanced Analytical Applications Infrastructure (OFS AAAI) Applications Pack Installation and Configuration Guide*

- *Scenario Manager User Guide*

- *Services Guide*

These documents can be found at the following link:

http://docs.oracle.com/cd/E60570_01/homepage.htm

To find more information about the Oracle Financial Services and complete product line, visit Web site at www.oracle.com/financialservices.

Conventions Used in this Guide

Table 1 lists the conventions used in this guide.

Table 1. Conventions Used in this Guide

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

CHAPTER 1 — *Overview of FCCM*

This chapter describes Oracle Financial Services Financial Crimes and Compliance Management (FCCM) applications, how they are used by financial institutions and what a typical workflow would be. It contains the following sections:

- About Financial Crimes and Compliance Management
- Functions
- Workflow

About Financial Crimes and Compliance Management

In today's complex banking environment, there are many different factors that financial institutions must address to deter crime, safeguard their reputation, increase efficiency, minimize risk, and comply with regulatory agencies. Oracle Financial Services Financial Crime and Compliance Management (FCCM) provides automated, comprehensive, and consistent surveillance of all accounts, customers, correspondents, and third parties in transactions, trades, orders across all business lines. The solution allows organizations such as banks, brokerage firms, and insurance companies to monitor customer transactions daily, using customer historical information and account profiles to provide a holistic view of all transactions, trades, orders and other activities. It also allows organizations to comply with national and international regulatory mandates using an enhanced level of internal controls and governance. FCCM is a common platform that supports the following OFSAA products:

- **Anti-Money Laundering Enterprise Edition (AML EE)** monitors transactions to identify possible money-laundering activities. These scenarios consider whether the geographical location or entities involved warrant enhanced scrutiny; monitor activity between accounts, customers, correspondents, and other entities to reveal relationships that could indicate efforts to launder funds; address sudden, significant changes in transaction activity that could indicate money laundering or fraud; and detect other types of activities that are considered potentially suspicious or indicative of money laundering.
  For example, the Journals Between Unrelated Accounts scenario detects accounts that conduct journal transactions, within a specified period, to one or more accounts that do not share tax identifiers, do not share a customer, are not in the same household, and are not known to have a formal relationship. This behavior might indicate that money launderers have established a number of accounts using aliases or slightly different identifying information, and then moving money between accounts as part of a layering strategy, often consolidating the funds in a single account before removing them from the institution.

- **Know Your Customer (KYC)** assesses the risk associated with a customer by considering different attributes of the customer and enables financial institutions to perform Due Diligence, Enhanced Due Diligence, and continuous monitoring of customers. Cases generated in Know Your Customer can be managed within Enterprise Case Management to track investigations until they have been resolved or reported to the appropriate regulatory authorities.

- **Enterprise Fraud Management (EFM)** detects behaviors and patterns that evolve over time and are indicative of sophisticated, complex fraud activity. These scenarios monitor check and deposit / withdrawal activity, electronic payments, such as funds transfer and payments completed through clearing house (ACH) mechanisms, and ATM and Bank Card to identify patterns of activities that could be indicate fraud, counterfeiting or kiting schemes, identity theft or account takeover schemes. Fraud scenarios also monitor

employee transactions to identify situations in which employees, acting as insiders, take advantage of access to proprietary customer and account information to defraud the financial institution's customers.

For example, the Excessive Withdrawals at Multiple Locations scenario monitors a sudden increase in a customer's withdrawals at ATMs that may indicate money laundering, terrorist financing, or an account takeover.

- **Oracle Financial Services Currency Transaction Reporting (CTR)** analyzes transaction data from the organization and identifies any suspicious activities within the institution that may lead to fraud or money laundering and must be reported to the regulatory authorities. Currency Transaction Reports (CTRs) are created either at the branches or through the end of day files, where the CTR application aggregates multiple transactions performed at the branch, ATMs and Vaults. Oracle Financial Services Currency Transaction Reporting then helps the organization file the CTR online with the U.S. Financial Crimes Enforcement Network (FinCEN) using a discreet form or uploaded in a batch form in a specific text file format.

  Unlike alerts for other Oracle Financial Services Behavior Detection products such as Anti-Money Laundering, Fraud, Trading Compliance, Broker Compliance, or Energy and Commodity Trading Compliance which appear in an Alert Management user interface, CTR alerts are automatically processed and converted into CTR reports or Monetary Instrument Log reports which can be worked through the CTR user interface.

  For example, the Bank Secrecy Act Currency Transaction Report scenario detects activity meeting the requirements for filing a Bank Secrecy Act Currency Transaction Report (CTR) and reconciles alerts generated by this scenario which are considered batch CTRs with Branch CTRs. The resulting CTRs are prepared for electronic filing in accordance with FinCEN's BSA Electronic Filing Requirements for Bank Secrecy Act Currency Transaction Report (BSA CTR).

- **Foreign Account Tax Compliance Act (FATCA) Management** allows financial institutions to comply with FATCA regulations from the Internal Revenue Service and the US Treasury Department which prevent US taxpayers who hold financial assets in non-US financial institutions and other offshore vehicles from avoiding their US tax obligations. The FATCA Management solution integrates with Enterprise Case Management to track investigations until they have been resolved or reported to the appropriate regulatory authorities.

- **Trading Compliance (TC)** examines prices and timing of orders and executions by comparing them to market conditions and detect behaviors or situations that violate exchange, market center, and individual broker or dealer policies and procedures, including behaviors that violate the Chinese Wall policies and procedures established by the Firm or those with confidential information held by the Firm about a security. For example, the Trading Ahead of Material Events scenario detects possible insider trading by analyzing trades which occur prior to "events", which can be defined by the Oracle client. The type and volume of trades which occur prior to an event may indicate that an employee, customer, trader, or trading desk was in possession of material non-public information. As there may also be non-fraudulent reasons for this trading activity, this scenario minimizes false alerts by excluding accepted hedging or trading strategies.

- **Oracle Financial Services Personal Trading Approval** monitors employee investment accounts and trades. Employees of the financial institution submit trade requests to be made from their approved investment accounts. Compliance officers can then review, approve, or reject the trade requests to ensure that their employees are acting in compliance with regulations. Financial institutions can also use this solution to maintain employee attestations.

- **Trade Blotter (TB)** allows trades to be viewed and reviewed, primarily for suitability issues within the wealth management sector, by compliance analysts an or business supervisors after a trade has been executed. The Trade Blotter is a list of trades returned after a search based on specified criteria. Users can view trade details,

view related trade documents, enter a comment on a specific trade, and then mark the trade as reviewed or requiring follow-up.

- **Broker Compliance (BC)** identifies activities or situations in customer accounts that involve either a significant amount of risk-and therefore may be unsuitable for the customer-or may violate trading rules set by the exchanges or regulators; trades in mutual fund securities that may violate regulatory trading guidelines, Commission policies, or are unsuitable for a particular customer; and activities performed by employees that may violate regulatory conduct rules or may be prohibited by firm policies. These scenarios also detect instances in which an investment advisor may be managing client accounts in a manner that is unsuitable for their customers, giving preferential treatment to particular customers, or manipulating transactions between accounts; and instances in which a portfolio manager may be placing orders on material, non-public information, misrepresenting portfolio performance, or unfairly allocating orders to accounts they manage. For example, the Reps Concentrating Solicitations in Too Few Securities scenario verifies that Registered Representatives are not exposing their clients to undue risk by recommending a significant percentage of buy solicitations in a single security, which can result in an unbalanced and volatile portfolio.

- **Energy and Commodity Trading Compliance (ECTC)** monitors trading activities that involve the financial institution as the buyer or seller on energy and commodity related trades, including commodities, options, futures, and swaps.
  For example, the Energy Trading Limits scenario monitors trading of energy instruments to detect excessive hourly amounts of energy traded, based on internal limits which consider physical and financial power as well as Financial Transmission Rights (FTR). The scenario generates alerts when the amount of energy approaches or exceeds these internal limits. This behavior may indicate an attempt to manipulate the market by knowingly creating congestion with the purpose of benefiting from the creation of that congestion.

- **Enterprise Case Management (ECM)** manages and tracks the investigation and resolution of cases related to one or more business entities involved in potentially suspicious behavior. Cases can be manually created within Enterprise Case Management or your firm may integrate other Oracle Financial Services solutions, such as Alert Management, Know Your Customer, and FATCA Management, which can be used to create cases.

- **Regulatory Reporting** supports the management, delivery, and resolution of required regulatory reports across multiple geographic regions and financial lines of business. Organizations are required to analyze and report any suspicious activities that may lead to fraud or money laundering within the institution to regulatory authorities.

Functions

The following figure depicts the functionality of Oracle Financial Services Financial Crimes and Compliance Management.
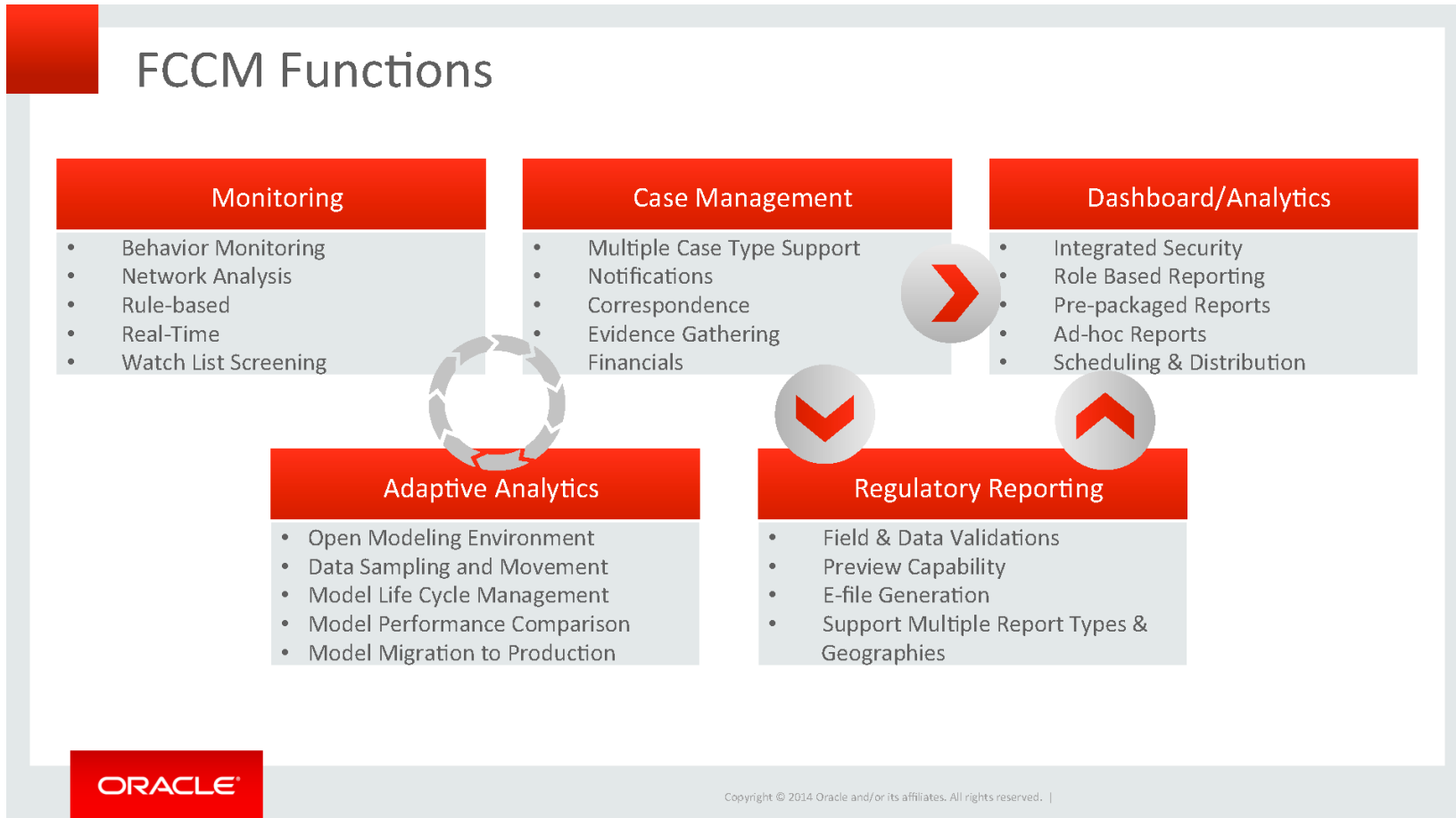
Workflow

Oracle Financial Services Financial Crimes and Compliance Management applications integrate fully - creating a complete workflow to address a financial institution's compliance needs. The following figure shows this process.

Business Analysts and IT staff identify the appropriate client data sources - drawn from the firm's transactions, developing processes to extract data in the form Oracle requires.

The Financial Services Data Model ingests the information and uses that data to popluate the user interface and scenarios.

Batch Scenarios are run at real time, near real time, and regular intervals (typically nightly, weekly, monthly, and quarterly) to extract transaction information.

Scenarios identify behaviors that may indicate illegal or risky behavior. When one or more data records meet a scenario's pattern of behavior, an Alert is created.

Alerts are assigned to an employee or group of employees who are tasked with assessing the Alert. During analysis, an Alert can be acted upon, resolved, or promoted to a case.

Cases manage and track the investigation and resolution related to business entities involved in suspicious behaviors. Cases are managed in Enterprise Case Management.

If it is determined that a case must be reported to authorities, Regulatory Reporting allows users to generate reports automatically populated with investigation information.

The financial institution files the report with regulatory agencies, such as FinCen, using a discreet form or batch uploaded in a specific file format, generated by Regulatory Reporting.

Detailed information about these processes is available in the user documentation.

CHAPTER 2 *About the Administration Tools*

This chapter describes how to access the Administration Tools in order to configure alert and case generation. The following sections are detailed in this chapter:

- About the Administration Tools

- Logging in to the Administration Tools

- Using Common Screen Elements

- Logging off of the Administration Tools

- Saving Changes to a Log File

About the Administration Tools

The application provides the following tools to configure the alert generation process:

- **Scenario Threshold Editor:** This tool is used for modifying the threshold values that patterns use to detect matches. Refer to Chapter 3, *Scenario Threshold Editor,* on page 11, for more information.

- **Scenario Wizard:** This tool is used to create or edit a scenario. Refer to **Chapter 4,** *Scenario Wizard,* **on page 23** for more information.

- **Alert Creator Editor:** Using this tool you can automatically group matches that share similar information into a single alert. You can create new rules, modify the logic behind existing rules, and delete rules. The tool also displays the job ID and job template ID for all rules created. Refer to Chapter 5, *Alert Creator Editor,* on page 57, for more information.

- **Alert Scoring Editor:** This tool is used for creating new rules or modify the logic behind existing rules that prioritize alerts automatically. Refer to Chapter 6, *Alert Scoring Editor,* on page 65, for more information.

- **Alert Assigner Editor:** This tool is used for assigning ownership of alerts. Refer to Chapter 7, *Alert Assigner Editor,* on page 99, for more information.

- **Case Assigner Editor:** This tool is used for assigning ownership of cases. Refer to Chapter 8, *Case Assigner Editor,* on page 113, for more information.

- **Threshold Analyzer:** This tool is used to reduce the number of false positive alerts by analyzing and categorizing past alerts to identify correlations between alert attributes and alert quality. Refer to Chapter 8, *Threshold Analyzer,* on page 113 for more information.

Logging in to the Administration Tools

Access to Administration Tools depends on the type of user role assigned by the application administrator. The following rules apply:

- Users assigned to the Data miner role can access the following:

    - Scenario Threshold Editor

    - Scenario Wizard

- Users assigned to the Administrator role can access the following:

    - User Administration

    - Security Attribute

    - Administration

    - Alert Creator Editor

    - Alert Scoring Editor

    - Alert Assigner Editor

    - Case Assigner Editor

Refer to the *Administration Guide,* for more information about how to install the tools. Refer to the *Scenario Wizard User Guide,* for more information about the Scenario Wizard. Contact your system administrator for the URL to access the Administrator Tools.

Accessing the Administration Tools

To access the Administration Tools, follow these steps:

1. Open the Login Page through your browser.

2. Type your user ID in the **User ID** text box.

3. Type your password in the **Password** text box.

4. Click **Login**. After verifying the user ID and password, the system displays the OFS AM page as defined by the system's defaults and as per your role.

Note: After typing your user ID and password, allow the system adequate time to process your login. If you click **Login** a second time, a *busy page* may display, designating that the Administration Tools are processing the access request. Wait for 10 seconds, then click **Go Back** to redisplay the Login page and log on again.

5. Click **FCCM**. The OFESCM Home page is displayed.

6. Hover over the Administration menu to choose the Tool which you want to access. Depending upon your role, possible actions include the following:

- **User Administration**

    - Security Management System

    - Security Attribute Administration

- **Alert Management Configuration**

  - Alert Assigner Editor

  - Alert Creator

  - Alert Scoring Editor

  - Threshold Editor

- **Case Management Configuration**

  - Case Assigner Creator

The Administration Tools Overview provides a brief description of each Administration Tool that you can access.

Using Common Screen Elements

The following screen elements display and function the same within each of the Administration Tools:

- Help Button

- Icons Button

Help Button

A Help button [icon] displays on the Administration Tools' Context Controls bar above the tab options. Click **Help** while working in a tool to get the following:

- More detailed information about the tool

- Explanations of the screen elements that comprise the tool

- Definitions of the fields that display on the screen

- *How to* instructions on the tasks that the tool enables you to perform

You can also click **Help** on the Overview tab for complete online information of Administration Tools in a HTML Help format.

Icons Button

The Administration Tools contain icons that enable you to perform actions within the tools. Table 2 describes the icons found within the Administration tools:

Table 2. Icons Used

Icon	Description
Add	Enables you to add rules.
Update	Enables you to modify existing rules.
Delete	Enables you to delete existing rules.

Table 2. Icons Used

Icon	Description
Expand	Enables you to view threshold history details (only in the Scenario Threshold Editor).
Contract	Enables you to hide threshold history details (only in the Scenario Threshold Editor).

Logging off of the Administration Tools

To log off of the Administration Tools, follow these steps:

1. Click **Logout** on the navigation bar.

   A dialog box displays the following message: *Are you sure you want to log out? If you log out and you have not saved all of your changes, the information will be lost*.

2. Click **OK** to log out.

   The Logout page displays.

3. Click **Close Browser** to close your browser.

Saving Changes to a Log File

Before the system accepts any values changed within an Administration Tool, a confirmation dialog box opens asking you to confirm the change by clicking either on **OK** or **Cancel**. When you click **OK**, the system records the changes in a log file with the following information:

- User
- Date and time
- Changed values
- Prechange values

Refer to the *Administration Guide* for more information about logging.

CHAPTER 3

Scenario Threshold Editor

This chapter describes how the Scenario Threshold Editor administration tool can be used to modify the threshold values that scenarios use to detect matches. This chapter provides information on the following topics:

- About the Scenario Threshold Editor
- About the Scenario Threshold Editor Screen Elements
- Using the Scenario Threshold Editor
- Review Test Scenario Results

About the Scenario Threshold Editor

When scenarios are created, thresholds are established that enable you to modify the values of these thresholds in a production environment. Once the application is in the production environment, any user assigned the Data miner role can use the Scenario Threshold Editor to modify threshold values of any installed scenario, and threshold sets to fine-tune how that scenario finds matches. Using this tool, you can enter a new value for a threshold (within a defined range) or reset the thresholds to their sample values.

Scenario Editor threshold page can be used for modifying the scenario thresholds and test run the scenario to know the number of matches that are generated through the test run. It can also be used to create a new threshold set based on the already available threshold set to modify the threshold and test the scenario.

A scenario is installed using the sample list of thresholds and values. This sample list of thresholds is referred to as the *base threshold set*. During deployment, you can create additional threshold sets to support specific business needs using the Oracle Financial Services Scenario Manager application.

Note: Changing scenario threshold values can generate significantly more or less alerts, depending upon the modifications made.

Note: If Anti-Money Laundering (AML) is not enabled, editing of thresholds can be done through scenario manager.

The following subsections discuss features you encounter while using the Scenario Threshold Editor:

- Threshold Sets
- Inactive Thresholds

For more information about scenarios, refer to the respective Technical Scenario Description document (for example, for trading compliance scenario information, refer to the *Trading Compliance Technical Scenario Descriptions).*

Threshold Sets

Threshold sets allow you to run the same scenario multiple times against a variety of sources (for example, exchanges, currencies, or jurisdictions) with separate threshold values for each source.

For example, you may have a scenario with the base threshold set and two additional threshold sets that were created during deployment. You decide that you need this scenario to detect matches in transactions with a minimum value in US currency, European currency, and Japanese currency. Rather than changing the base threshold set for each situation, you can set the value of the base threshold set to detect US currency (for example, USD 100,000), the second threshold set to detect European currency (for example, EUR 150,000), and the third threshold set to detect Japanese currency (for example, JPY 125,000).

Since threshold sets two and three have only a few fields that differ from the base threshold set, you can check the Inherit Base Value check box feature for those fields that are exactly the same as the base threshold set. This feature associates the threshold values in the threshold set you are modifying with the corresponding values in the base threshold set. This association copies the corresponding base threshold set values to the set you are modifying and automatically updates them if the base value changes (refer to *<Scenario–Threshold Set> Area,* on page 14 for more information).

You do not have to run all three jobs all the time. Each threshold set has a unique ID, so you can tell the system which set to run and how often to run it. Refer to your scheduling tool's (for example, Control-M) documentation to sequence these jobs.

Note: Use the Scenario Threshold Editor to modify the values of existing threshold sets. Threshold sets can be created either through the add new threshold set button or through the Scenario Manager.

Inactive Thresholds

For scenarios to work properly, thresholds that are not being used by a scenario must have their values set to Inactive. The following groups of thresholds can have values set to Inactive:

- Mutually Exclusive Thresholds
- Additional Scenario Thresholds

Mutually Exclusive Thresholds

In some situations, scenarios apply the value of one threshold only when the value of another threshold is set to *N* for no. These types of thresholds are referred to as a *mutually exclusive* thresholds.

For example, the use of the *Included Jurisdiction Codes* threshold is contingent upon the value of the *All Jurisdictions* threshold.

Table 3 shows how mutually exclusive thresholds work in two different situations.

Table 3. Mutually Exclusive Thresholds

Threshold	Situation 1	Situation 2
All Jurisdictions	Y	N
Included Jurisdiction Codes	Inactive	North, East

If the value of the *All Jurisdictions* threshold is set to Y for yes (Situation 1), then the *Included Jurisdiction Codes* threshold values are not used and have the value set to Inactive. Conversely, if the value of the *All Jurisdictions* threshold is set to *N* for no (Situation 2), then the scenario only uses the value specified by the *Included Jurisdiction Codes* threshold (that is, North, East).

Additional Scenario Thresholds

Your deployment may not need to utilize all the thresholds established within a particular scenario. The mutually exclusive thresholds not used by the scenario are set to Inactive.
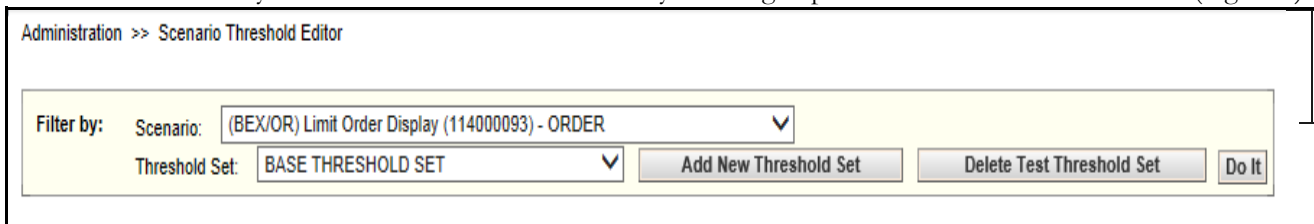
About the Scenario Threshold Editor Screen Elements

The following screen elements display in the Scenario Threshold Editor:

- Search Bar

- <Scenario–Threshold Set> Area

Search Bar

The search bar allows you to search for threshold values by selecting a specific scenario and threshold set (Figure 1).

Figure 1. Search Bar

The components of the search bar includes the following:

- **Filter by: Scenario** drop-down list: Provides a list of scenarios displayed by the scenario's short name, ID number, and focus type (for example, Avoid Report Thresh (106000129) – ACCOUNT).

- **Filter by: Threshold Set** drop-down list: Provides a list of Threshold Sets associated with the scenario displayed in the Scenario drop-down list. The base threshold set displays first, followed by additional threshold sets listed in ascending alphabetical order.

- **Add New Threshold Set**: When clicked, enables you to add new threshold sets.

- **Delete Test Threshold Set:** When clicked, enables you to delete test threshold sets.

- **Do It** button: When clicked, displays the threshold values for the scenario and threshold set selected in the search bar.

<Scenario–Threshold Set> Area

The <Scenario-Threshold Set> Area displays the list of threshold values for a selected scenario and threshold set (Figure 2). This list displays after you select a scenario and threshold set in the search bar and click **Do It**.

(BEX/OR) Limit Order Display - BASE THRESHOLD SET

Threshold Editor

Name	Description	Current Value	New Value	Min Value	Max Value	Sample Value	Data Type
All Currencies	This parameter allows coverage of all currency codes without enumerating them in the "Included Currency Codes" threshold. Y: cover all currency codes regardless of the "Included Currency Codes" threshold value. N: cover only those currency codes that are listed in the "Included Currency Codes" threshold	'N'	'N'	--	--	'N'	STRING
All Desk IDs	This parameter allows coverage of all desk IDs without enumerating them in the "Included Desk IDs" threshold. Y: cover all desk IDs regardless of the "Included Desk IDs" threshold value. N: cover only those desk IDs that are listed in the "Included Desk IDs" threshold.	'Y'	'Y'	--	--	'Y'	STRING
All Exchange Codes	This parameter allows coverage of the all exchange codes without enumerating them in the Included Exchange Codes parameter. " Y: Cover all exchange codes regardless of the Included Exchange Codes parameter value " N: Cover only those exchange codes that are listed in the Included Exchange Codes parameter.	'N'	'N'	--	--	'N'	STRING
All Jurisdictions	This parameter allows coverage of all jurisdictions without enumerating them in the "Included Jurisdiction Codes" threshold. Y: cover all jurisdiction codes regardless of the "Included Jurisdiction Codes" threshold value. N: cover only those jurisdictions that are listed in the "Included Jurisdiction Codes" threshold.	'Y'	'Y'	--	--	'Y'	STRING
All Product Subtypes	This parameter allows coverage of all product sub-types without enumerating them in the "Included Product Sub-types" threshold. Y: cover all product sub-types regardless of the "Included Product Sub-types" threshold value. N: cover only those product sub-types that are listed in the "Included Product Sub-types" threshold.	'Y'	'Y'	--	--	'Y'	STRING
All Product Types	This parameter allows coverage of all product types without enumerating them in the "Included Product Types" threshold. Y: cover all product types regardless of the "Included Product Types" value. N: cover only those product types that are listed in the "Included Product Types" threshold.	'Y'	'Y'	--	--	'Y'	STRING
Excluded Order Buyer/Seller Acct IDs	Buyer/seller account IDs of an order that this scenario excludes. The firm defines allowable values for the Buyer/Seller Account Identifier field in the Order table, as described in the DIS.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Excluded Order Buyer/Seller IDs	Buyer/seller IDs of an order that this scenario excludes. The firm defines allowable values for the Buyer/Seller Identifier field, as described in the DIS.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Included Currency Codes	The list of product issuing currency codes covered by the scenario. The value of this field must be a valid ISO Standard 4217 alpha currency code.	'USD'	'USD'	--	--	'USD'	LIST
Included Desk IDs	The list of trading desk IDs covered by the scenario. Allowable values are defined by the Firm.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Included Exchange Codes	This list of exchange codes covered by the scenario. The exchange codes indicate exchanges on which the security is listed. Allowable values are defined by the DIS for the Primary Exchange field.	'XNAS', 'XNMS'	'XNAS', 'XNMS'	--	--	'XNAS', 'XNMS'	LIST
Included Jurisdiction Codes	The list of jurisdiction codes covered by the scenario. Allowable values are defined by the Firm.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Included Order Buyer/Seller Types	Buyer/seller types of an order that the scenario covers. Allowable values are defined in the Order Buyer/Seller Type field in the Trade Code Values table, as described in the DIS	'CR', 'CI', 'EE', 'IA','EC'	'CR', 'CI', 'EE', 'IA','EC'	--	--	'CR', 'CI', 'EE', 'IA','EC'	LIST
Included Product Categories	The list of product category codes covered by the scenario. Allowable values are defined by DIS. Default values set in the product scenarios depend on the application domain of the scenario: EQT: For scenarios that cover Equity products OPT: For scenarios that cover Equity Options FI: For scenarios that cover Fixed Income products The value of this parameter depends on the scenario definition. The default value for each scenario is defined in the Scenario Configuration section, the Application Domain column.	'EQT'	'EQT'	--	--	'EQT'	LIST
Included Product Subtypes	The list of codes describing product sub-types within the selected product categories and types covered by the scenario. Allowable values are defined by the customer.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Included Product Types	The list of codes describing product types within the selected product categories covered by the scenario. Allowable values are defined by the customer.	'Inactive'	'Inactive'	--	--	'Inactive'	LIST
Min Batch Not Displayed Duration	A parameter for the acceptable number of consecutive seconds within the current processing batch an order can spend in a displayable but not displayed state before an LOD alert is warranted.	15	15	0	300	15	INTEGER
Min Batch Total Seconds Not Displayed	A parameter for the acceptable total amount of time within the current processing batch an order can spend in a displayable but not displayed state before an LOD alert is warranted.	20	20	0	300	20	INTEGER
Min Total Seconds Not Displayed	A parameter for the acceptable total amount of time an order can spend in a displayable but not displayed state before an LOD alert is warranted.	30	30	0	300	29	INTEGER

Add A Comment

Type between 3 and 4,000 characters in the Comment text area.

The text area contains 0 characters.

Save Test Update Product Threshold Set Cancel

Figure 2. <Scenario-Threshold Set> Area

The <Scenario-Threshold Set> Area includes the following components and contents:

- Long name of the scenario and the name of the threshold set in the title of the <Scenario-Threshold Set> bar.

- List of scenario thresholds by threshold name, sorted in ascending alphabetical order.

- Threshold information as follows:

  - **Threshold History Icon**: Expands or contracts the Threshold History inset that displays a history of all modifications to the selected threshold value in reverse chronological order by creation date. Information displayed includes the creation date, user name, threshold value, and any comment associated with the threshold value change.

    If comments are displayed and the comment text consists of more than 100 characters, the Scenario Threshold Editor displays the first 100 characters followed by an ellipsis (...) indicating that more text is available. When you click the ellipsis, the entire comment displays in the Expanded Comments dialog box for ease of viewing.

  - **Name**: Displays the name of the threshold.

  - **Description**: Displays the description of the threshold.

  - **Current Value**: Displays the current value of the threshold. If the data type of the threshold is *LIST*, multiple values are displayed in a comma-delimited list, with each value contained in single quotes (' '). Thresholds with an *Inactive* current value are not being used by the scenario (refer to *Inactive Thresholds,* on page 12 for more information).

  - **Inherit Base Value**: Enables you to select the check box to apply the corresponding threshold values from the base threshold set to the threshold set displayed. Selecting the check box disables the New Value text box. This option does not display for the base threshold set.

  - **New Value**: Displays the current value of the threshold in the editable New Value text box if the Inherit Base Value check box is not selected. If the data type for the threshold is *LIST*, multiple values are displayed in a comma-delimited list, with each value contained in single quotes (' ').

  - **Min Value**: The minimum value of the threshold.

  - **Max Value**: The maximum value of the threshold.

  - **Sample Value**: The sample value of the threshold.

  - **Data Type**: The type of data that is utilized by a threshold in a scenario. There are five data types: Integer, Boolean, Real, String, and List. Place your cursor over this value to display the threshold unit of measure (for example, days, percentage, or distance).

  - **Add A Comment**: Provides a place to type comments. When you type a comment and click **Save**, the same comment is applied to each modified threshold.

- **Restore Samples Values:** Restores all thresholds within the selected scenario threshold set to the sample values

- **Save**: Saves all modifications to the database.

- **Cancel**: Redisplays the Scenario Threshold Editor without the <Scenario-Threshold Set> Area and does not save your changes.

- **Test:** When the Test button is clicked**,** the *Scenario Test Execution* pop-up window is displayed.

Figure 3. Scenario Test Execution window

The Scenario Test Execution window displays the following fields:

Table 4. Scenario Test Execution components

Field	Description
Scenario Name	This field is non-editable and displays the scenario that has been selected in the drop-down list from the threshold editor page.
Threshold Set	This is a non-editable text box which displays the threshold set name that has been selected for test run.
Pattern	Select the pattern from the drop-down list that are part of the selected scenario. **Note:** Since the scenario job runs based on the pattern, you cannot run multiple patterns of the scenario at the same time.
Processing Batch Date	Select the date based on which the scenario patterns will run.
Processing Batch Name	Select the batch name from the drop-down list. **Note:** If a Batch with the selected Processing Batch Name and Date is already running, then the following error message is displayed: *A Batch with the selected Processing Batch Name and Date is already running. Please wait till the Batch completes*.

After selecting these values, click the **Run** button to run the scenario and the results can be viewed in the *Review Test Scenario Results* page.

- **Update Product Threshold Set**: Enables you to update the test threshold set to product threshold set. This button is enabled only when the threshold set selected is newly created threshold.

Using the Scenario Threshold Editor

The Scenario Threshold Editor configures scenario threshold values by:

- Providing threshold values for a specific scenario and threshold set

- Accepting and validating user-entered threshold values

- Saving the modified threshold values to the database

This section explains the following functions of the Scenario Threshold Editor:

- Adding a new Threshold Set

- Deleting the Test Threshold Set

- Changing a Scenario Threshold

- Resetting a Scenario Threshold to the Sample Values

- Viewing a Scenario Threshold's History

- Viewing Expanded Comments

Adding a new Threshold Set

To add a new Threshold Set, follow these steps:

1. Under the **Administration** menu, hover over **Alert Management Configuration**, click **Threshold Editor.**

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

3. Click **Add New Threshold Set**.

4. The *Add New Threshold Set* pop-up window is displayed.

Figure 4. Add new Threshold Set window

5. Enter the required details in the following fields:

Table 5. Add New Threshold Set Components

Field	Description
Scenario	This field is non editable and displays the scenario that has been selected in the drop-down list from the threshold editor page.
Available Threshold Sets	This dropdown box displays all the available threshold sets in the system for the selected scenario. Also, this is required to acquire the thresholds for the new threshold set that is being created. **Note :** - If the user do not select a value from the "Available Threshold sets" drop-down list, the following error message is displayed: *Please select a threshold set from the available threshold sets dropdown to create a new threshold set.* - If the user has selected a threshold set which doesn't have an associated job, then the following error message is message: *The selected threshold set doesn't have the required Job and Job Dataset for running the scenario test execution. Please select any other threshold set and take action.*

Table 5. Add New Threshold Set Components

Field	Description
Test Threshold Set	Select this checkbox if the threshold set created is a test threshold set or not. The threshold set name is available `threshold set name + _TST_datetimestamp.`
New Threshold Set Name	By default, this field is kept blank. You can enter the threshold set name only when the *Create Test Threshold Set* checkbox is not selected. When the user has selected the Test Threshold Set checkbox, then this textbox is pre populated with a value that has been selected from the available threshold sets along with a time stamp.

6. Click **Save**. The Threshold Set is added.

Deleting the Test Threshold Set

To delete a test Threshold Set, follow these steps:

1. Under the **Administration** menu, hover over **Alert Management Configuration**, click **Threshold Editor.**

2. Click **Delete Test Threshold Set**.

3. The Threshold Set is deleted.

Changing a Scenario Threshold

To change a scenario threshold value, follow these steps:

1. Select the desired scenario from the **Filter by: Scenario** drop-down list.

2. Select the desired threshold set from the **Filter by: Threshold Set** drop-down list.

3. Click **Do It**.

   The system displays the threshold values for the scenario and threshold set selected.

4. Type a new value in the **New Value** box for each threshold that you wish to update.

   If you are not updating a base threshold set, you can inherit corresponding values from the base threshold set by checking the **Inherit Base Value** check box.

   Optional: Enter any comments in the **Add A Comment** text box.

5. Click **Save**.

   The new threshold values display in the Threshold List for <Scenario-Threshold Set>.

Resetting a Scenario Threshold to the Sample Values

To reset a scenario's threshold sample values, follow these steps:

1. Select the desired scenario from the **Filter by: Scenario** drop-down list.

2. Select the desired threshold set from the **Filter by: Threshold** Set drop-down list.

3. Click **Do It**.

   The system displays the threshold values for the scenario and threshold set selected.

4. Click **Restore Sample Values** button.

The Confirmation dialog box displays the following message: *Are you sure you want to restore the threshold values of the displayed threshold set to their sample values?*

To restore thresholds that have the Inherit Base Value check box selected, you must clear the check box. Click **OK** to return to the Threshold Editor with the sample values displayed, then click **Save.** Click **Cancel** to retain the current values.

5. Click **OK**.

The dialog box closes and the sample values display in the [Scenario-Threshold Set] Area.

6. Click **Save**.

The database is updated to reflect the changes.

Viewing a Scenario Threshold's History

To view the modification history for a specific threshold, follow these steps:

1. Click **Expand** next to the desired threshold.

The Threshold History inset displays with the history for the threshold selected.

2. Click **Contract** next to the threshold to hide the Threshold History inset.

Viewing Expanded Comments

To view an expanded comment in the Scenario Threshold inset, follow these steps:

1. Click the **ellipsis (...)** at the end of the comment in the Scenario Threshold inset.

The entire comment, up to 4,000 characters, displays in the Expanded Comments dialog box (Figure 5).
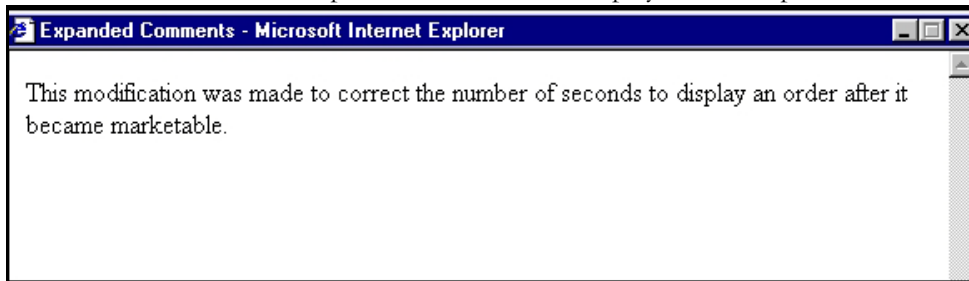
Figure 5. Example Expanded Comment Dialog Box

2. Click **X (Close button)** on the top right corner to close the dialog box.

Review Test Scenario Results

The Review Test Scenario Results page allows you to review the results of the test scenarios that are run from the threshold editor page.
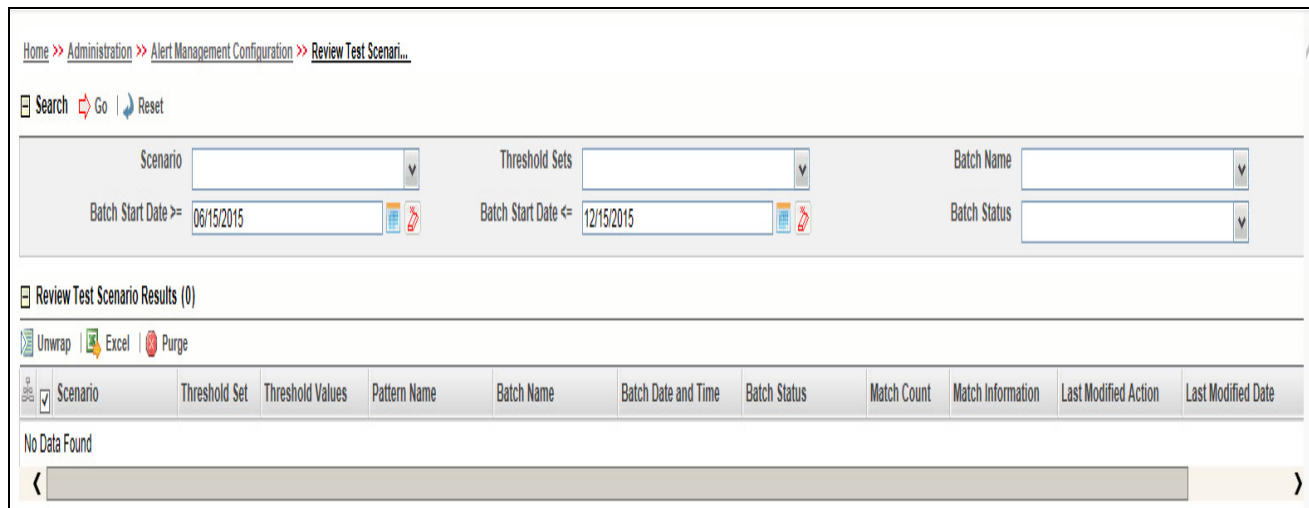
Figure 6. Review Test Scenario Details page

About the Review Test Scenario Details Screen Elements

The following screen elements display in the review scenario details:

- Search Bar

- Search and List Grid

Search Bar
The components of the search bar includes the following:

Table 6. Search Bar Components

Field	Description
Scenario Name	Select the scenario name from the drop-down list.
Threshold Sets	Select the threshold set from the drop-down list. **Note:** This field will display the value only when the scenario name is selected. When no scenario name is selected, then it is assumed that all the threshold sets are included for the search.
Batch Name	Select the Batch name on which the scenario is run. **Note:** By default, this field is kept as blank. This fetches value only when the scenario name is selected.
Batch Start Date >=	Select the current date from the calendar. By default, this column will display Current Date - 6months.
Batch Start Date <=	Select the current date from the calendar. By default, this column will display Current Date
Batch Status	Select the batch status from the drop-down list. Following are the options available: • Running • Finished • Error • Cancelled

Search and List Grid

The search results are displayed in the *Search and List* grid.

This grid displays the following columns:

Table 7. Search and List grid components

Field	Description
Scenario	This field displays the scenario name, as displayed in the Threshold Editor Page.
Threshold Set	This field displays the threshold set name, as displayed in the Threshold Editor Page.
Threshold Value	This field displays the threshold value, as displayed in the Alert Details Page.
Pattern Name	This field displays the pattern name for the selected pattern ID.
Batch Name	This field displays the batch name on which the scenario is run.
Batch Date and Time	This field displays the batch date and time.
Batch Status	This field displays the batch status. Following is the batch status: • Running • Finished • Error • Cancelled
Match Count	This field displays the number of match generated for the run.
Match Information	This field displays an excel icon. When clicked, an auto generated spreadsheet in the format "`<Scenario Name>_<BatchDate>_Matched Details.xlsx`" is displayed. The details are dynamic based on the scenario selection.
Last Modified Action	This field displays the action that was last modified.
Last Modified Date	This field displays the date on which the last action has been taken..
Last Modified User	This field displays the user who have taken the last action.

Action Buttons

The following action button is available on the *Search and List* grid:.

- **Purge:** When clicked**,** this button purges all the matches that are generated for the selected scenario and threshold set combination.

CHAPTER 4 — Scenario Wizard

This chapter describes how the Scenario Wizard tool can be used to create scenarios. This chapter provides information on the following topics:

- About the Scenario Wizard
- Scenario Wizard Navigation
- Creating a New Scenario
- Editing a Scenario

About the Scenario Wizard

The Scenario Wizard is a tool that allows business users to create scenarios that run within OFSBDF. Users create scenarios based on pre-defined templates. These templates contain scenario classes, focuses, and other data that can be combined to detect unique behaviors of interest. The wizard-like interface allows novice users to create fully functional scenarios.

Scenarios created with the Scenario Wizard can be further refined in the Scenario Manager. Refer to the *Scenario Manager User Guide* for more information.

Scenario Wizard Workflow

Figure 7 illustrates the Scenario Wizard workflow. The following buttons in the navigation bar provide access to the workflow pages, where you can perform tasks.

- Scenario Overview
- Focus Selection
- Associated Data
- Highlights
- Thresholds
- Threshold Sets
- Review & Save
- Test Scenario
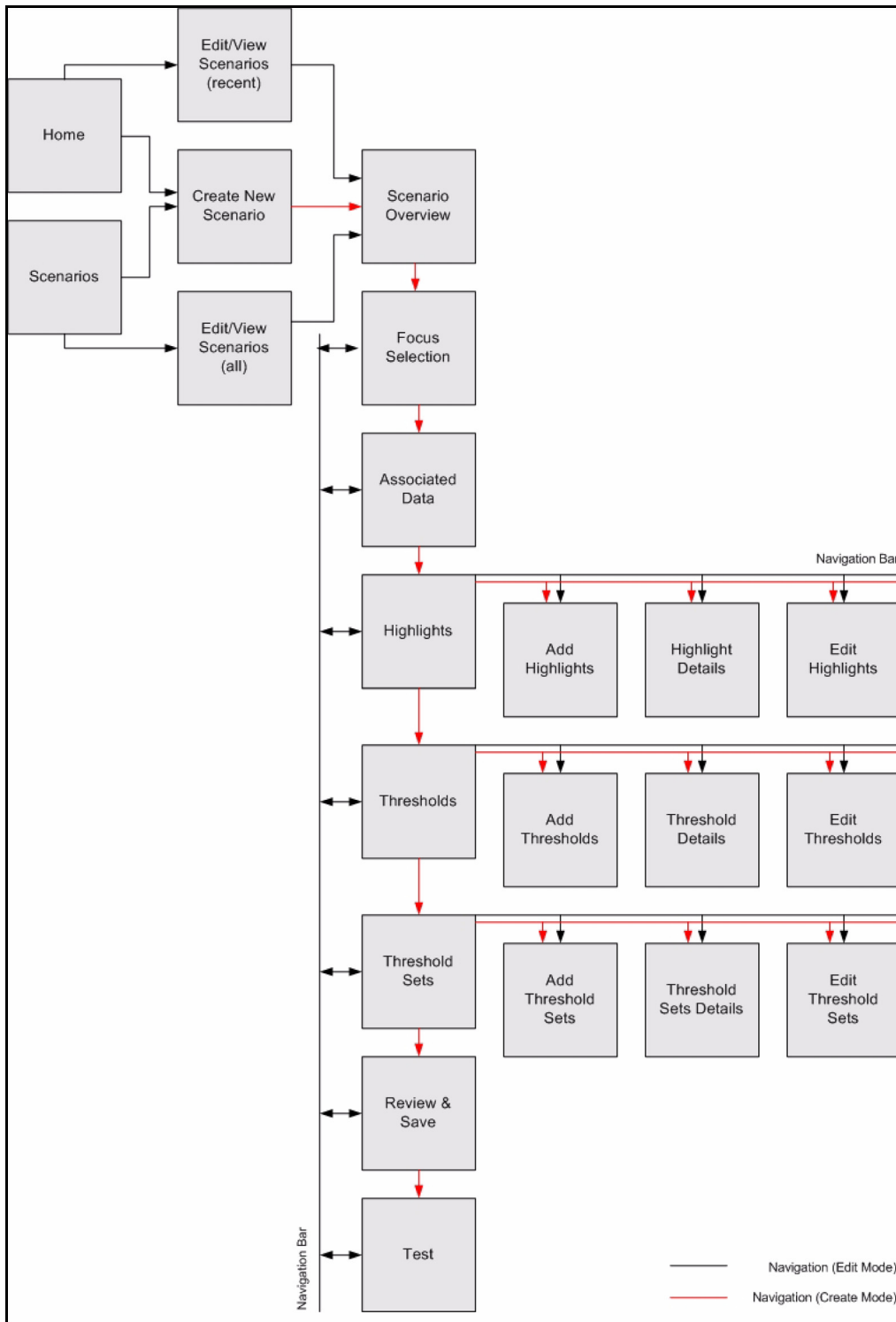
Figure 7. Scenario Wizard Workflow

Scenario Wizard Navigation

Navigation in the Scenario Wizard can be accomplished by using the **Previous** and **Next** buttons present on each page of the wizard to move sequentially through screens. It is also possible to navigate the Scenario Wizard by clicking page links located in the left hand side (LHS) menu frame. This menu tree is visible on each page of the wizard and your current page is highlighted in the tree.

When in the Create Scenario workflow, you can only navigate backwards using the LHS menu to select screens already completed. You cannot select future screens using the LHS menu. You must use the **Next** button on each page to move through the remaining pages in the correct order.

When in the Edit Scenario workflow for a completed scenario, you can navigate forwards and backwards to any page in the wizard using the LHS menu. If in the Edit Scenario workflow, you can choose to create a new scenario rather than edit the existing one. In this case, the LHS menu changes to reflect that you have entered the Create workflow and restricts forward movements using LHS menu accordingly.

About the Home Page

The Home page is the default display for the Scenario Wizard user interface (UI). This page contains a list of recently edited scenarios, as well as the Focus, Class, Last Edited Date/Time, and By (user who last edited the scenario).

From this page you can create a new scenario or modify an existing scenario. To create a new scenario, click the **Create New Scenario** button and follow the steps within the Scenario Wizard. To edit an existing scenario, click the **Edit** button (Figure 8).
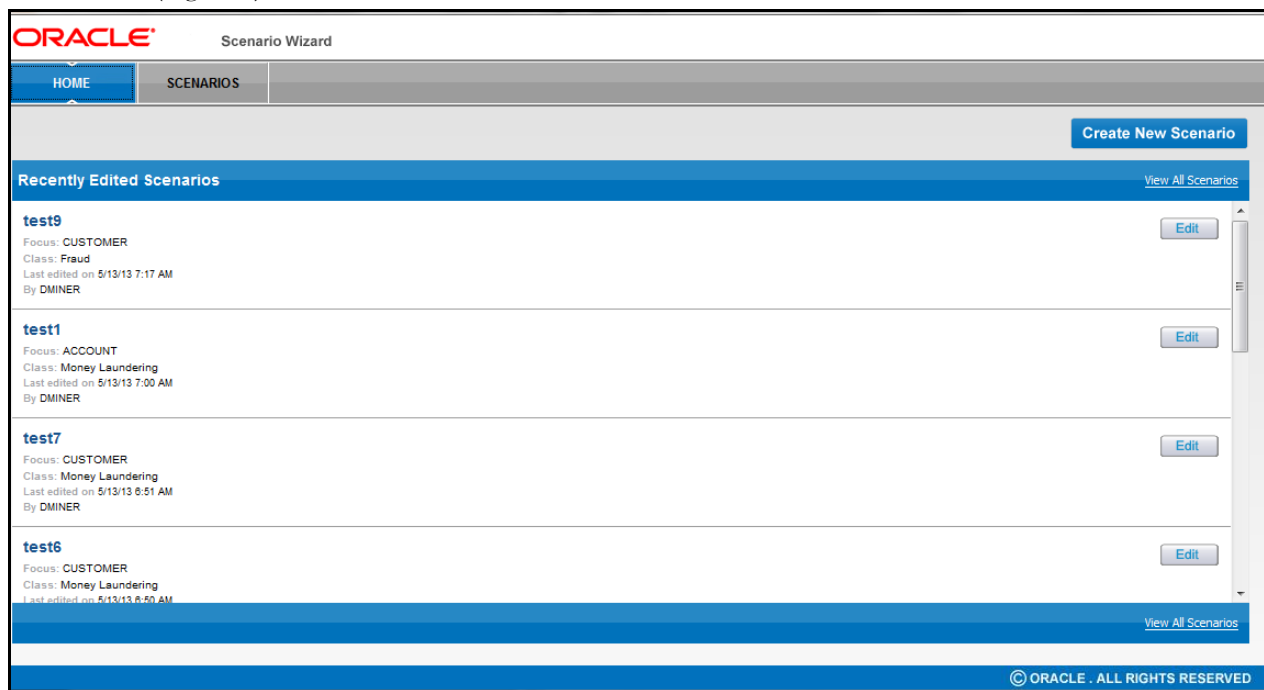
Figure 8. Home Page

The Home page displays the 10 most recently edited scenarios. This page does not display scenarios that meet the following criteria:

- Scenarios created in Scenario Manager

- Scenarios created in Scenario Wizard that have been edited using Scenario Manager

- Deactivated scenarios

About the Scenarios Page

The Scenarios page enables you to search for the scenarios that you create using the Scenario Wizard. You can navigate to this page by clicking the **View All Scenarios** link from the Home page (Figure 9).
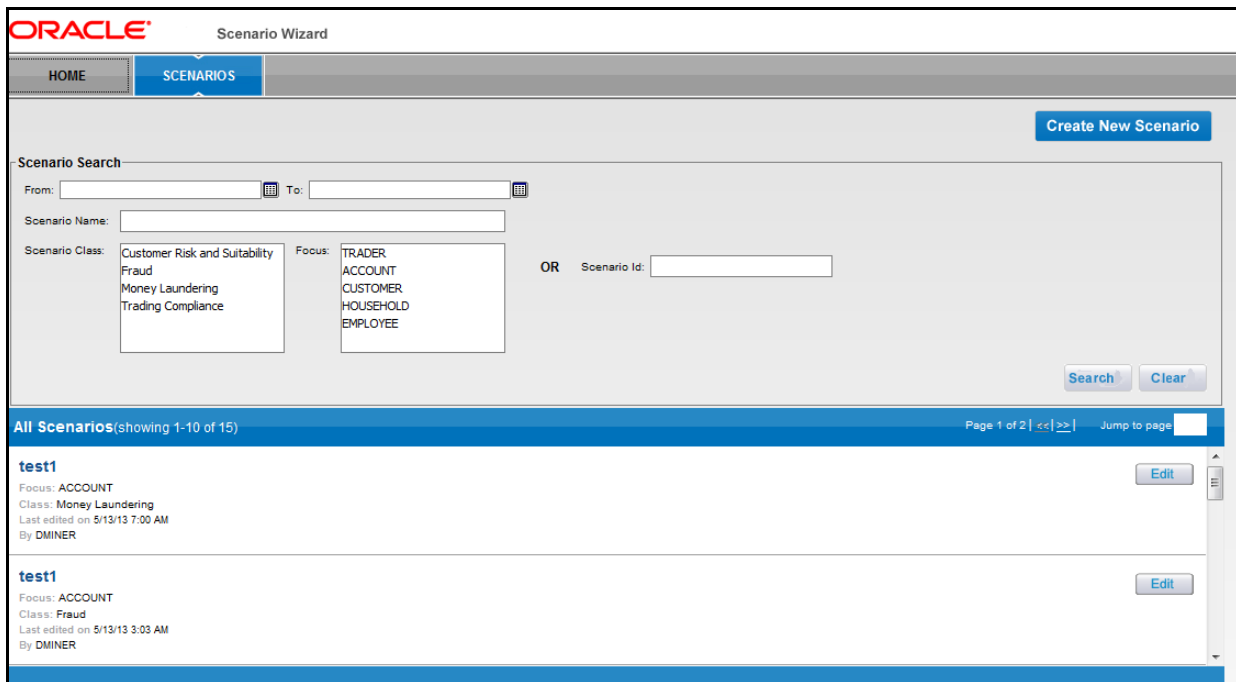
Figure 9. Scenario Page

Scenario Page Components

The Scenarios page consists of the **Scenario Search** bar and the **All Scenarios** list sections. The **Scenario Search** bar enables you to display and view data for scenarios based on criteria that you select within this search bar. Text boxes, multi-select list boxes, and calendar controls enable you to filter scenarios precisely for analysis.

The **All Scenarios** list displays the list of scenarios resulting from the search criteria. The title bar displays a count of scenarios (Showing X - Y of Z) and a page count (Page X of Y). You can traverse the list page forward or backward, or jump to a specific page.

Scenario Search Bar Components
The **Scenario Search** bar contains the following components:

- **From/To Date** calendar control: Allows you to specify the time frame in which you want search for scenarios. When you specify the From and To dates, the UI displays only those scenarios created in the Scenario Wizard within the time frame.

● **Scenario Name** text box: Allows you to specify the name of a scenario for which to search which has been created in Scenario Wizard. This text box enables you to enter text up to 80 characters in length. You can also search via Scenario Name using the wildcard character (%).

● **Scenario Class** multi-select list: Lists the available scenario class in alphabetical order (ascending). Select one or more classes to filter your search.

● **Focus** multi-select list: Lists the available focus types in alphabetical order (ascending). Select one or more focus types to filter your search.

● **Scenario ID** text box: Enables you to search using a unique scenario ID. If you want to perform a search using multiple values, you can enter a string of comma-separated values.

● **Search** button: Refreshes the page with new search results.

● **Clear** button: Resets the search fields.

All Scenarios List Components

The **All Scenarios** list contains the following components:

● **Scenario Name**: Displays the scenario name.

● **Focus**: Displays the focus type of the scenario.

● **Class**: Displays the class of the scenario.

● **Last Edited**: Displays the most recent date of the scenario.

● **By:** Displays the user who last edited the scenario.

● **Edit** button: Allows you to edit this scenario.

Creating a New Scenario

The Scenario Wizard application enables you to create custom scenarios using an eight-step wizard. The eight-steps are:

● Scenario Overview

● Selecting a Focus

● Associating the Data

● Adding Highlights

● Adding Thresholds

● Adding Threshold Sets

● Saving the Scenario

● Testing the Scenario

Scenario Overview

The Scenario Overview (Figure 10) is the first step in creating a new scenario. The page enables you to enter the basic information about the scenario. Click **Create Scenario** to open this page.
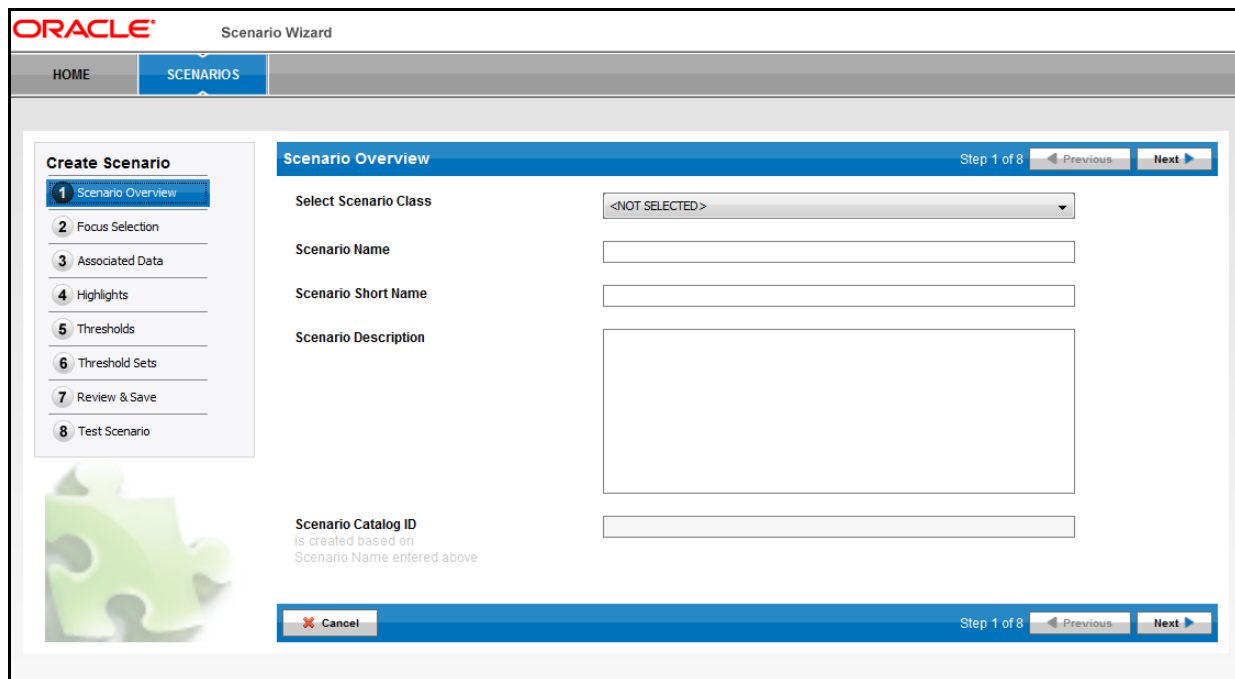
Figure 10. Scenario Overview Page

Components of the Scenario Overview Page

The Scenario Overview page contains the following components:

- **Select Scenario Class** drop-down list: Lists all available Scenario Classes (for example, Mutual Funds, Money Laundering). You can select a scenario class from the list, based on your requirements.

- **Scenario Name** text field: Enables you to specify a scenario name of up to 80 characters in length.

- **Scenario Short Name**: Enables you to specify a scenario short name of up to 40 characters in length. The scenario short name is the name that displays within the Alert Management UI.

- **Scenario Description** text field: Enables you to enter additional information for the scenario, if available. You can provide a description of up to 4000 characters in length. This is an optional field.

- **Scenario Catalog ID** text field: Auto-generates the scenario catalog ID on entering the Scenario Name. The catalog ID generates with the naming convention as `<Scenario Class>-<Scenario Name>`. You can change the catalog ID name, if required.

- **Next** button: Navigates you to the next page.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

Table 8 lists the available scenario classes on the Scenario Overview page. The list of scenario classes available in your installation depends on the scenario templates installed.

Table 8. Scenario Class

Abbreviation	Scenario Class
CST	Customer Risk and Suitability
FR	Fraud

Table 8. Scenario Class

Abbreviation	Scenario Class
ML	Money Laundering
TC	Trading Compliance

To provide information for the new scenario on the Scenario Overview page, follow these steps:

1. Select the scenario class from the **Select Scenario Class** drop-down list.

2. Type the name in the **Scenario Name** text box.

3. Type the short name in the **Scenario Short Name** text box.

   Optional: Type the additional information for the scenario in the **Scenario Description** text box.

4. Modify the catalog ID that is auto-generated by the application, if required.

Note: Spaces are not allowed for values in this field.

5. Click **Next**.

If you have missed entering data in any of the mandatory fields, an error message displays along with the missing fields highlighted in the color red.

Any attempt to modify the scenario class after you have completed this step and navigated to a subsequent page of the wizard results in a resetting of the scenario and the loss of any selections made in later steps of the wizard. The wizard warns you of the consequences of this change and allows you to decide whether to proceed with the change.

The combination of the selected Scenario Name, Scenario Class and Focus Type must be unique. If you have navigated back to the Scenarios Overview page after selecting a Focus Type, and attempted to change the Scenario Name, Scenario Class, or both, and the wizard determines the revised scenario definition is no longer unique, the utility warns you to modify the selection.

Selecting a Focus

The Focus Selection page enables you to select the focus of the scenario based on the scenario information provided on the Scenario Overview page. The Focus Selection page contains fields to select the focus type. The focus types available on this screen depend on the scenario class you selected on the prior screen (Figure 11).
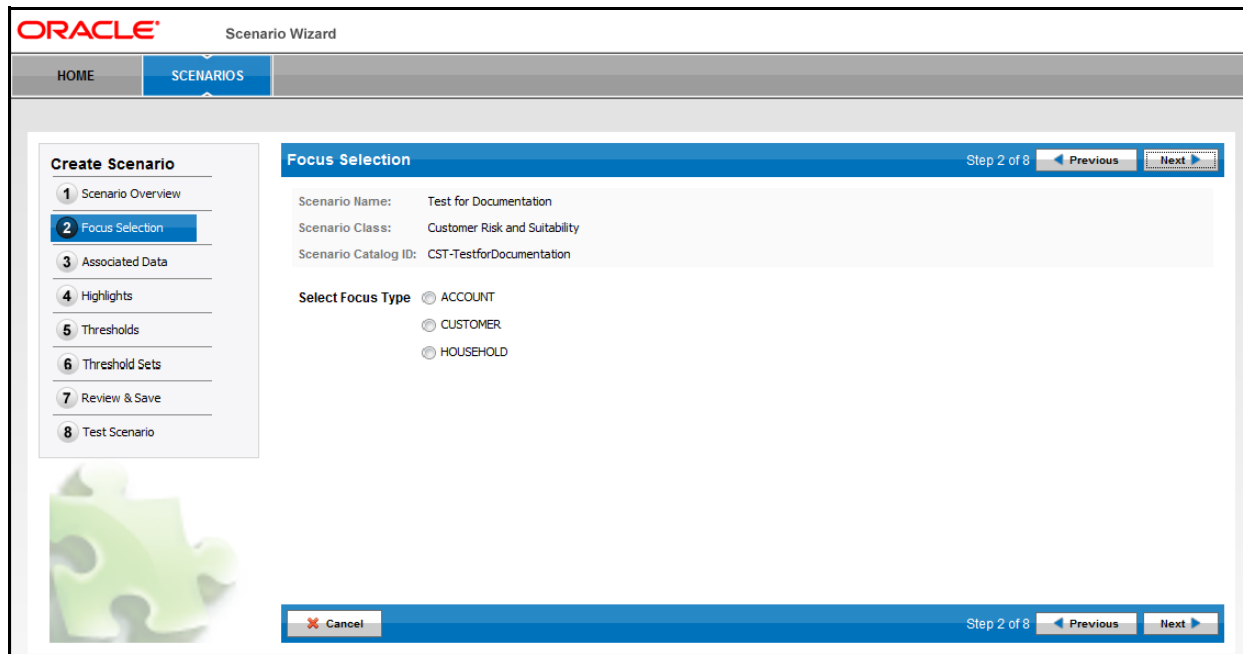
Figure 11. Focus Selection Page

Components of the Focus Selection Page

The Focus Selection page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario Class** label: Displays the selected scenario class.

- **Scenario Catalog ID** label: Displays the scenario catalog ID.

- **Select Focus Type** radio button: Displays the focus types available for this scenario.

- **Previous** button: Navigates you to the previous page.

- **Next** button: Navigates you to the next page.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

Table 9 lists the available scenario class and focus type combination available on the Focus Selection page. The list of focus types available in your installation depends on the scenario templates installed.

Table 9. Scenario Class and Focus Type Combination

Scenario Class	Focus Type
CST	Account
	Customer
	Household

Table 9. Scenario Class and Focus Type Combination (Continued)

Scenario Class	Focus Type
FR	Account
	Customer
	Employee
ML	Account
	Customer
TC	Account
	Trader

To select a focus for the scenario on the Focus Selection page, follow these steps:

1. Select the focus type from the **Select Focus Type** option.

Note: It is mandatory to select at least one focus type from the **Select Focus Type** option.

---

2. Click **Next**.

If you have missed entering data in any of the mandatory fields, an error message displays along with the missing fields highlighted in the color red.

The combination of the selected Scenario Name, Scenario Class, and Focus Type must be unique. If the wizard determines that the Focus Type you have selected is in combination with the previously defined Scenario Name, and the Scenario Class does not represent a unique scenario, the utility warns you to modify the selection.

Any attempt to modify the Focus Type after you have completed this step and navigated to a subsequent page of the wizard results in a resetting of the scenario and the loss of any selections made in the later steps of the wizard. The wizard warns you of the consequences of this change and allows you to decide whether to proceed with the change.

Associating the Data

The Associated Data page is the core of the Scenario Wizard application. This page enables you to select from a set of pre-defined source datasets. The available datasets are based on the selection made on the scenario class and focus type earlier. The associated dataset information that you provide decides the logic of the scenario being created. The associated data selection identifies the data that the scenario analyzes for behaviors of interest.

On selecting the Associated Data, the utility displays a Records to Match section. This section defines what record types are displayed in the Investigation Management interface when this scenario produces alerts. Selected Records to Match typically display as individual building blocks within the Matched Information section of the Alert Management UI Alert Details page.

By default, records used in identifying the behavior are matched; you can view additional record types that may help in the analysis of alerts (Figure 12).
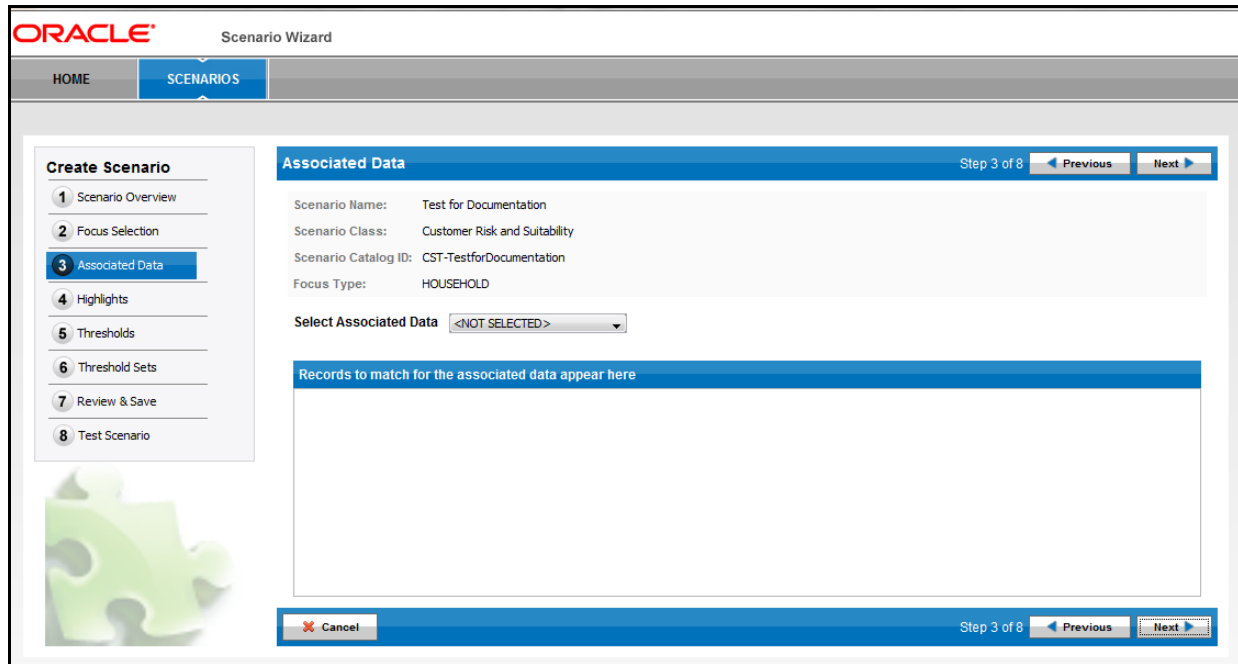
Figure 12. Associated Data Page

Components of the Associated Data Page

The Associated Data page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario Class** label: Displays the selected scenario class.

- **Scenario Catalog ID** label: Displays the scenario catalog ID.

- **Focus Type** label: Displays the focus of the scenario.

- **Select Associated Data** drop-down list: Enables you to select the associated dataset. Based on your selection, the Records to Match list section is populated.

- **Records to Match** list section: Records used in detecting the behavior are always matched. You can select additional records to match to support the investigation.

- **Previous** button: Navigates you to the previous page.

- **Next** button: Navigates you to the next page.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

To add the associated data for the scenario, follow these steps:

1. Select the dataset from the **Select Associated Data** drop-down list.

    The Records to Match list section displays with default dataset records.

    Optional: Select the additional dataset record that you want to include in the scenario.

2. Click **Next**.

Any attempt to modify the Associated Data selection after you have completed this step, and navigated to a subsequent page of the wizard results in a resetting of the scenario and the loss of any selections made in later steps of the wizard. The wizard warns you of the consequences of this change and allows you to decide whether to proceed with the change.

Adding Highlights

The Highlights page enables you to add, modify, and delete highlights to the scenario. In addition, it provides an option to choose the display name, format and related information of the highlight (Figure 13).
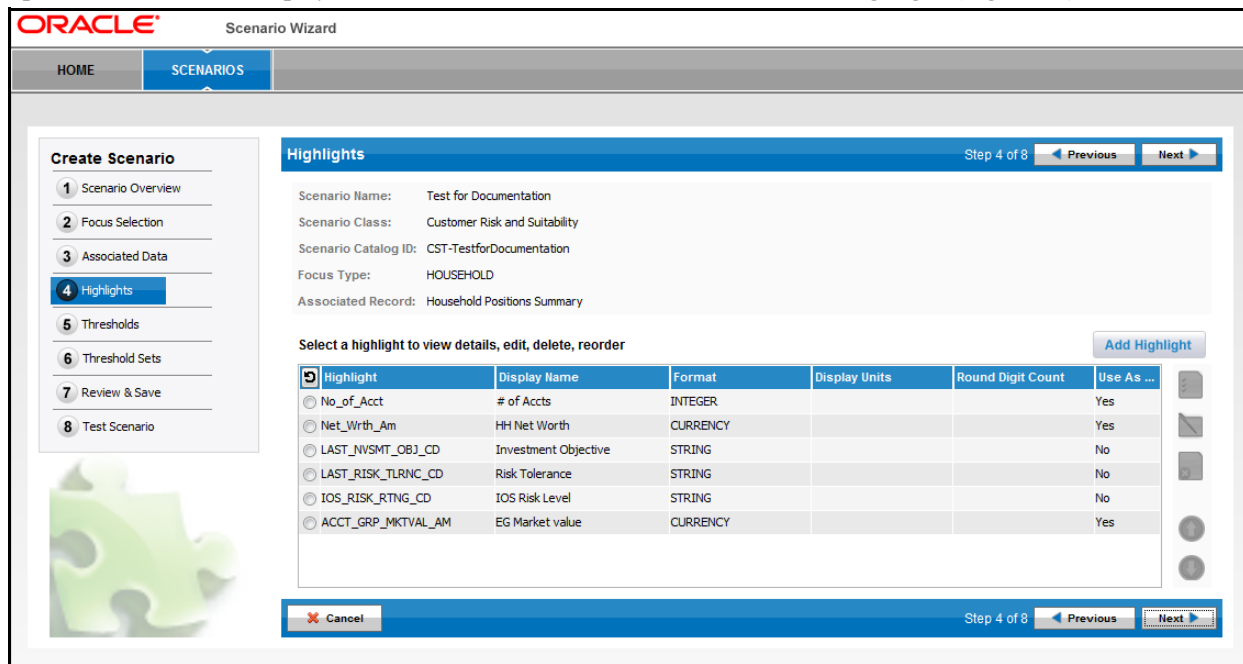
Figure 13. Highlights Page

Components of the Highlights Page

The Highlights page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario Class** label: Displays the selected scenario class.

- **Scenario Catalog ID** label: Displays the scenario catalog ID.

- **Focus Type** label: Displays the focus of the scenario.

- **Associated Record** label: Displays the associated data record of the scenario.

- **Highlights List** section: Displays the list of highlights defined for the scenario being created. By default, when creating a new scenario, the wizard displays the complete list of highlights pre-defined for the selected Associated Data datasets. A radio button precedes each highlight in the list. Selecting a radio button de-selects a previously selected highlight.

  The Highlight List section contains the following columns:

- ■ **Unselect Al**l icon: De-selects previously selected highlights from the list.

- ■ **Highlight:** Displays the system-defined highlight name.

- ■ **Display Name:** Displays the logical highlight name.

- ■ **Format:** Displays both numeric and non-numeric type formats of the highlight. For example, REAL2 and STRING.

- ■ **Display Units:** Displays the value (for example, Hundreds, Thousands, and so forth) based on the specified numeric type format. If the format is non-numeric, the column is empty.

- ■ **Round Digit Count:** Displays the round digit count (for example, 0, 1, 2, and so forth) based on the specified numeric type format.

- ■ **Use As Axis:** Displays a **Yes** or **No**, indicating whether or not this highlight can be used by the Threshold Analyzer utility as an axis on a graph.

- ● **Add Highlight** button: Create a new highlight on the Highlight section. This button is enabled only if there are no highlights selected on the list.

- ● **View Highlight** button: View full details of the selected highlight.

- ● **Edit Highlight** button: Modify details of a selected highlight.

- ● **Delete Highlight** button: Delete the selected highlight.

- ● **Move Up** button: Move the selected highlight up in the order. The order in which the highlights display on the list indicate the order in which they display for an alert in the Alert Management UI for an alert.

- ● **Move Down** button: Move the selected highlight down in the order.

- ● **Previous** button: Navigates you to the previous page.

- ● **Next** button: Navigates you to the next page.

- ● **Cancel** button: Cancels the current process and navigates you to the Home page.

Adding Highlights

The Add Highlight dialog box enables you to add **Pre-defined** or **User-defined** highlights to the scenario. By default, the **Pre-defined** option is disabled on initial display; however, if you remove one or more pre-defined highlights from the Highlight list section, the **Pre-defined** option is enabled (Figure 14).

Figure 14. Add Highlight Dialog Box

The Add Highlight dialog box contains the following fields:

- **Pre-defined/User-defined** radio buttons: Selecting Pre-defined allows you to select from a set of highlights that have all attributes already defined. As mentioned previously, this option is only available if one or more pre-defined highlights appropriate for the associated data have been deleted from the Highlight List. Selecting **User-defined** enables additional options within the Add Highlight dialog box, allowing you to define a completely new highlight for use by the scenario.

- **Highlight** drop-down list: Enabled upon selection of either the **Pre-defined** or **User-defined** highlight option. By default, the value selected is **<NOT SELECTED>**. The Highlight drop-down list populates values dynamically based upon the type of highlight being created.

- **Display Name** text box: Displays the highlight name. By default, it is populated dynamically based on your selection in the Highlight field. The field is editable with up to 40 characters in length.

- **Entity** drop-down list: Enabled upon selection of the **User-defined** highlight option. By default, the value selected is **<NOT SELECTED>**. The field contains table names, which are used in the inner query of the Primary rule. For the User-defined option, this is a mandatory field.

- **Attribute** drop-down list: Enabled upon selection of **User-defined** highlight option. By default, the value selected is **<NOT SELECTED>**. The field populates columns associated with the table that you select from the **Select Entity** drop-down list. For the User-defined option, this is a mandatory field.

- **Format** drop-down list: Enables you to select the format type of the highlight. By default, the value selected is **<NOT SELECTED>**. For the User-defined highlight option, the list populates the formats applicable to the selected attribute.

Table 10 describes the various format types that you can select from the **Format** drop-down list.

Table 10. Format Type Description

Format Type	Description
STRING	Does not apply formatting to the value returned from the database. This format is useful for numbers that should not have thousands separators. For example, numeric account numbers.
INTEGER	Applies thousands separators to whole numbers.
REAL2	Applies thousands separators to real numbers, truncating to two digits of fractional data.
REAL5	Applies thousands separators to real numbers, truncating to five digits of fractional data.
$.00	Applies thousands separators and a currency symbol, for example, $, to a number. Fractions are displayed as $1,234.56 and a negative number is displayed as ($1,234.56).
$	Applies thousands separators and a currency symbol, for example, $, to a number. Fractions are rounded to the nearest whole number. For example, positive numbers are displayed as $1,234 and negative numbers as ($1,234).
$K	Applies thousands separators and a currency symbol, for example, $, to a number. Fractions are rounded to the nearest whole number. If the number is 1,000,000 or greater, the utility rounds the number to the nearest thousand and replaces the final three digits with the letter K. For example, positive numbers display as $1,234 or $2,3456K for $2,345,678.90, while negative numbers display as ($1,234) or ($2,346K).
CURRENCY	Applies the appropriate currency format to a value.
MMDDYY	Displays the short form of the date, for example 02/28/01.
MMDDYYYY	Displays the long form of the date, for example 02/28/2001.
DATETIME	Displays the short date format and time format in the 24-hour clock, for example, 02/28/01 23:59:59.
HHMMSS	Displays the long time format in a 24-hour clock. The expected input is an integer that represents a number of seconds; for example, the display of 93599 seconds is 23:59:59.
%	Displays the data as a percentage.

- ■ If the attribute is of type numeric with a precision of > 0, the field populates the REAL2, REAL5, $, $.00, $K, %, and CURRENCY as options; REAL5 being a default value.

- ■ If the attribute is of type numeric with a precision of = 0, the field populates the INTEGER and % as options; INTEGER being a default value.

- ■ If the attribute is of type non-numeric, the field populates the STRING, MMDDYY, MMDDYYYY, DATETIME, and HHMMSS as options; STRING being the default value.

- ● **Function** drop-down list: Enabled upon selection of the **User-defined** highlight option. By default, the value selected is **<NOT SELECTED>**. The possible value includes MINIMUM, MAXIMUM, AVERAGE, SUM, COUNT, and COUNT DISTINCT. For the User-defined option, this is a mandatory field.

● **Round Digit Count** drop-down list: Enables you to select the round digit count of the selected format of type numeric. By default, the value selected is **<NOT SELECTED>**. For the User-defined highlight option, the list populates the 0, 1, 2, 3, 4, 5, and 6 values. For a numeric type format, this is a mandatory field. The field is disabled upon selection of a non-numeric type format.

● **Display Units** text box: Displays the unit value based upon the selection of the round digit count. This is a non-editable field.

Table 11 provides the relationship between the Round Digit Count and the Display Unit value.

Table 11. Relationship between Round Digit Count and Display Unit Value

Round Digit Counts selection	Display Unit Value
0	Units
1	Tens
2	Hundreds
3	Thousands
4	Ten Thousands
5	Hundred Thousands
6	Millions

● **Use as Axis** drop-down list: Displays the value based on the specified numeric type format. This component controls whether the Threshold Analyzer utility considers this value as an axis for threshold analysis. Only numeric type fields are suitable for use as an axis in Threshold Analyzer.

Adding Pre-defined Highlights

To add a pre-defined highlight to the scenario, follow these steps:

1. On the Highlights page, click the **Add Highlight** button.

   The Add Highlight dialog box displays (Figure 14).

2. In the Add Highlight dialog box, do the following:

   a. Select the **Pre-defined** option.

   b. Select the highlight from the **Highlight** drop-down list.

      The Display Name auto-populates based upon the highlight selected. This value is editable.

   c. Select the format type from the **Format** drop-down list.

   d. Select the round-off value from the **Round Digit Count** drop-down list.

      The unit of display in the Display Unit text box automatically refreshes based upon your Round Digit Count selection. This value is not editable.

Note: This only option impacts the granularity with which this highlight displays on a graph in the Threshold Analyzer utility. It is applicable only for numerical format highlights that are flagged for Use as Axis.

   e. Select a **Yes** or **No** value from the **Use As Axis** drop-down list to indicate use by Threshold Analyzer as an axis.

Note: This option determines whether or not the highlight binding can be used as an axis variable by the Threshold Analyzer utility. Only non-string highlights are considered for axis display.

---

    f. Click **Save**.

       If you miss filling in any of the mandatory fields, a warning displays along with the missing field in the color red.

       The Add Highlight dialog box closes and an entry displays on the Highlight List section of the Highlight page.

  3. Enter additional highlights as needed or click **Next** to move to the next step in creating a scenario.

Adding User-Defined Highlights

To add a user-defined highlight to the scenario, follow these steps:

  1. On the Highlights page, click the **Add Highlight** button.

    The Add Highlight dialog box displays (Figure 14).

  2. In the Add Highlight dialog box, do the following:

    a. Select the **User-defined** option.

       By default, the Highlight drop-down list displays **<NOT SELECTED>**. If there are highlight attributes that exist based on the scenario's class, but which have not been pre-defined as a highlight for this scenario, those attributes display in the drop-down list. Additionally, there is an option to **<Create New>**.

       Selecting an existing attribute auto-populates the remaining fields in the Add Highlight dialog box, based upon what has already been defined for that attribute.

       Selecting **<Create New>** enables a text box in which you can enter a new custom highlight name.

    b. If you have selected to use an existing attribute for your highlight, the Display Name auto-populates but can be edited. If you have selected to create a new custom highlight, this text box is blank and you must enter a Display Name.

    c. Select the table name from the **Entity** drop-down list. This is the table from which you select an attribute to be used in your highlight.

    d. Select the associated column from the **Attribute** drop-down list. This is the data field upon which the value for your highlight is calculated.

    e. Select the format type from the **Format** drop-down list. The **Format** drop-down pre-populates with formats that are applicable to the selected attribute.

    f. Select the function from the **Function** drop-down list. Function allows you to specify some calculation to be performed on the selected attribute. For example, you may wish to calculate and display the SUM of the transaction amounts across all of the wire transactions bound to an alert as a result of detection. On the other hand, you may wish to display a COUNT DISTINCT of the number of accounts involved in the alert activity.

    g. Select the round-off value from the **Round Digit Count** drop-down list.

The unit of display in the **Display Unit** text box automatically refreshes based upon your Round Digit Count selection. This value is not editable.

This option only impacts the granularity with which this highlight displays on a graph in the Threshold Analyzer utility. It is applicable only for numerical format highlights that are flagged for Use as Axis.

h. Select a **Yes** or **No** value from the **Use As Axis** drop-down list to indicate use by Threshold Analyzer as an axis.

This option determines whether or not the highlight binding can be used as an axis variable by the Threshold Analyzer utility. Only non-string highlights are considered for axis display.

i. Click **Save**.

If you miss filling in any of the mandatory fields, a warning displays along with the missing field in the color red.

The Add Highlight dialog box closes and an entry displays on the Highlight List section of the Highlight page.

3. Enter additional highlights as needed or click **Next** to move to the next step in creating a scenario.

Viewing Highlights

To view the details of a highlight for the scenario, follow these steps:

1. Select a highlight entry from the Highlight List section.

   The View Highlight Details button enables.

2. Click the **View Highlight Details** button.

   The Highlight Details window displays in read-only mode where you can view the highlight information.

3. Click **Cancel** to close the window.

Modifying Highlights

You can modify both pre-defined or user-defined highlights. To modify the highlight details, follow these steps:

1. Select a highlight entry from the Highlight List section.

   The Edit Highlight Details button enables.

2. Click the **Edit Highlight Details** button.

   The Edit Highlight dialog box displays where you can modify the highlight information. You cannot modify the designation of the highlight as user-defined or pre-defined nor you can change the Highlight selection.

3. In the Edit Highlight dialog box, perform one or more of the following edits:

   a. Modify the name in the **Display Name** text box.

   b. Modify the selected table from the **Entity** drop-down list. For a pre-defined highlight, the **Entity** field is disabled.

   c. Modify the associated column from the **Attribute** drop-down list. For a pre-defined highlight, the **Attribute** field is disabled.

   d. Modify the selected format type from the **Format** drop-down list.

e. Modify the selected function from the **Function** drop-down list.For a pre-defined highlight, the **Function** field is disabled.

f. Modify the selected round-off value from the **Round Digit Count** drop-down list.

The unit of display in the Display Unit text box automatically refreshes based upon your Round Digit Count selection. This value is not editable.

g. Modify the selection of the **Use As Axis** drop-down list to indicate use by Threshold Analyzer as an axis.

h. Click **Save**.

If you neglect to complete any of the mandatory fields, a warning displays along with the missing field in the color red.

The modifications made to the highlight displays in the refreshed Highlight List.

Deleting Highlights

To delete a highlight, follow these steps:

1. Select a highlight entry from the Highlight List section.

   The Delete Highlight button enables.

2. Click **Delete Highlight**.

   A message box displays: *Do you really want to delete highlight?*

3. Click **OK**.

   The existing highlight entry is removed from the Highlight List section of the Highlights page.

Re-ordering Highlights

To re-order the highlight details of the scenario, follow these steps:

1. Select a highlight entry from the Highlight List section.

   The **Move Up/Move Down** button enables.

2. Click **Move Up/Move Down** to re-order the highlight information.

Adding Thresholds

The Thresholds page enables you to create and modify the custom-defined thresholds in addition to viewing the default thresholds list. Based on your selection for Associated Data, the scenario is defined with default thresholds representative of typical thresholds used in scenarios. You can add thresholds to the scenario through this step of the wizard.

For the default thresholds, you can only modify the **Default Value**, **Min Value**, and **Max Value** fields. For the custom-defined thresholds, you can modify all the threshold fields value with the exception of the **Threshold Name** field. In addition, you can only delete the custom-defined thresholds from the threshold list (Figure 15).
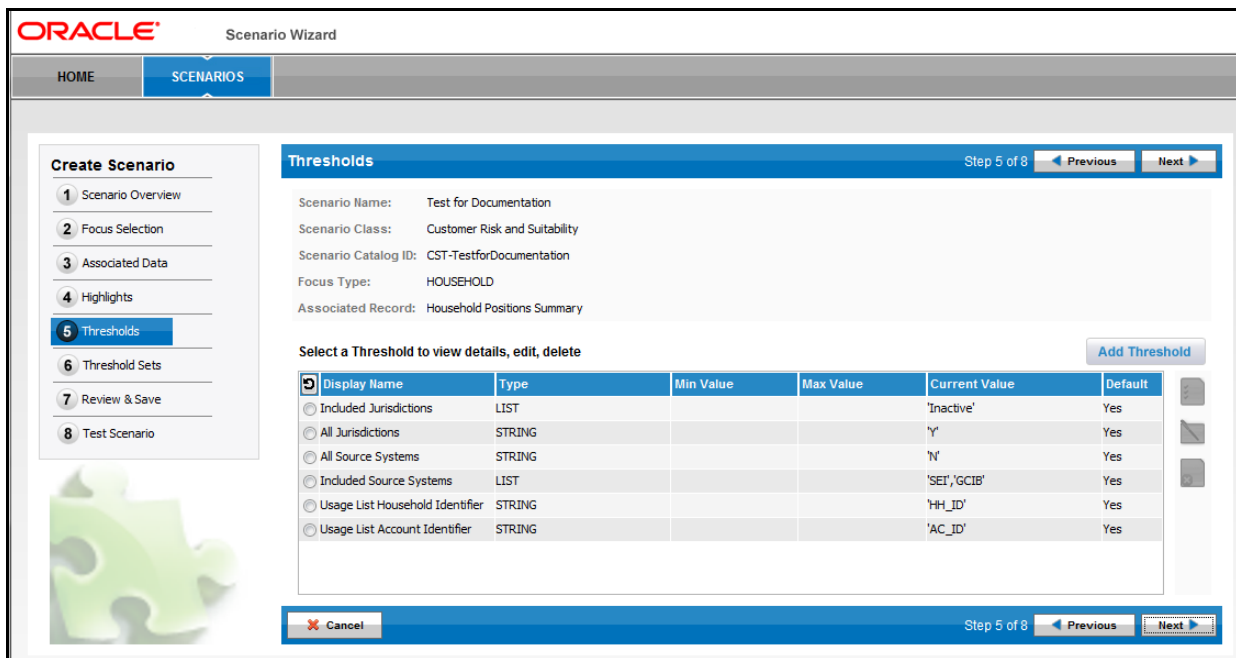
Figure 15. Thresholds Page

Components of the Thresholds Page

The Thresholds page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario Class** label: Displays the selected scenario class.

- **Scenario Catalog ID** label: Displays the scenario catalog ID.

- **Focus Type** label: Displays the focus of the scenario.

- **Associated Record** label: Displays the associated record of the scenario.

- **Threshold List** section: Displays the list of default and custom-defined thresholds for the scenario being created. A radio button precedes each threshold in the list. Selecting a radio button de-selects a previously selected threshold.
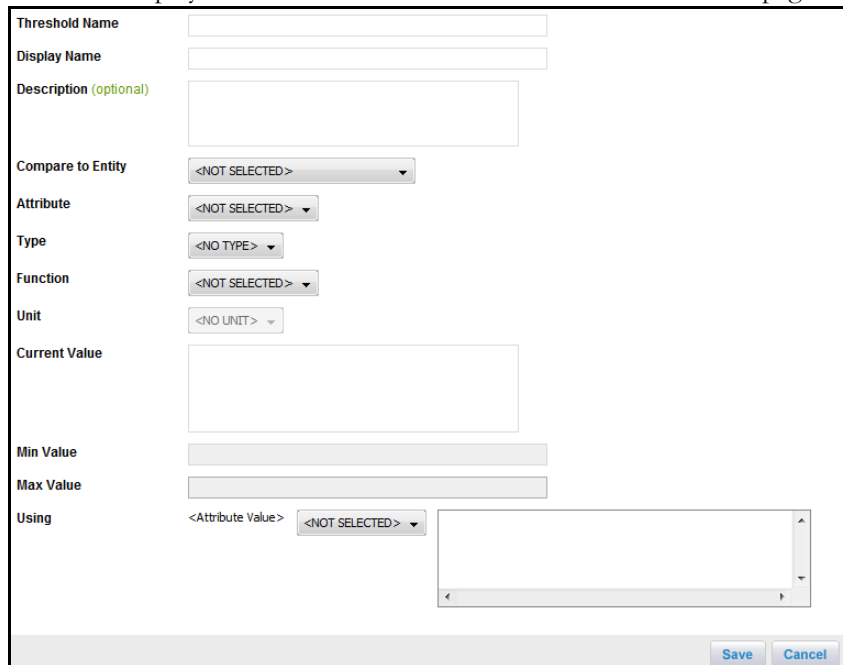
  The Threshold List section contains the following columns:

  - Unselect All icon: De-selects previously selected thresholds from the list.

  - **Display Name:** Displays the threshold name.

  - **Type:** Displays the threshold type, for example, STRING, INTEGER, REAL, LIST, and BOOLEAN.

  - **Min Value:** Displays the minimum possible value that can be defined for the threshold.

  - **Max Value:** Displays the maximum possible value that can be defined for the threshold.

  - **Current Value:** Displays the default/current value of the threshold. For the threshold type boolean, the value display is TRUE/FALSE.

  - **Default:** Displays a **Yes** or **No** value as an indicator of whether this is a default or custom-defined threshold. The default threshold displays as **Yes**.

- **Add Threshold** icon: Enables you to create a custom-defined threshold in the Threshold section.

- **View Threshold Details** button: Enables you to view the selected threshold details.

- **Edit Threshold** button: Enables you to modify the selected threshold details in a read-only mode.

- **Delete Threshold** button: Enables you to delete the selected custom-defined threshold.

- **Previous** button: Navigates you to the previous page.

- **Next** button: Navigates you to the next page of the wizard.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

Adding Thresholds

The Add Threshold dialog box enables you to add user-defined thresholds to the scenario (Figure 16). The added threshold displays in the Thresholds List section of the Threshold page.

Figure 16. Add Threshold Dialog Box

The Add Threshold dialog box contains the following fields:

- **Threshold Name** text box: Enables you to specify the threshold's logical name up to 40 characters in length. This is a mandatory field.

- **Display Name** text box: Enables you to specify the threshold's display name up to 40 characters in length. This is a mandatory field.

- **Description (optional)** text field: Enables you to enter the threshold's additional information up to 1000 characters in length.

- **Compare to Entity** drop-down list: Populates with the names of tables, which are used in the inner query of the Primary rule. By default, the value selected is **<NOT SELECTED>**. This is a mandatory field.

- **Attribute** drop-down list: Populates with the columns associated with the table selected in the Compare to Entity drop-down list. By default, the value selected is **<NOT SELECTED>**. This is a mandatory field

- **Type** drop-down list: Populates with the possible format types (for example, STRING, INTEGER, REAL, LIST, and BOOLEAN).

  - If the attribute is of type numeric with a precision of > 0, the field populates REAL as an option.

  - If the attribute is of type numeric with precision = 0, the field populates INTEGER as an option.

  - If an attribute is of type non-numeric, the field populates STRING as an option.

- **Function** drop-down list: Enables you to select the function for the attribute type. By default, the value selected is **<NOT SELECTED>**. For an attribute of type numeric (Boolean or Integer), COUNT and COUNT DISTINCT display. The possible values include:

  - **MINIMUM:** When selected, the threshold is applied in the HAVING clause of the primary dataset, returning where the minimum value for the attribute meets the threshold criteria.

  - **MAXIMUM:** When selected, the threshold is applied in the HAVING clause of the primary dataset, returning where the maximum value for the attribute meets the threshold criteria.

  - **AVERAGE:** When selected, the threshold is applied to the aggregate instead of individual rows in the HAVING clause of the primary dataset, returning where the average value for the attribute meets the threshold criteria.

  - **SUM:** When selected, the threshold is applied to the aggregate instead of individual rows in the HAVING clause of the primary dataset, returning where the aggregate value of the attribute meets the threshold criteria.

  - **COUNT:** When selected, the threshold would then be applied to the aggregate instead of individual rows in the HAVING clause of the primary dataset, returning where the number of records meets the threshold criteria.

  - **COUNT DISTINCT:** When selected, the threshold would then be applied to the aggregate instead of individual rows in the HAVING clause of the primary dataset, returning where the number of distinct records meets the threshold criteria.

- **Unit** drop-down list: Enables you to select the unit value based upon the selection of the threshold type from the **Type** drop-down list. This field is disabled for the **<No Unit>** value.

  Table 12. provides unit value for different threshold types.

Table 12. Unit Value for the Threshold Type

Threshold Type	Unit
Integer	Seconds
Integer	Minutes
Integer	Hours
Integer	Days
Integer	Money No Frac
Real	Money
Real	Percentage
Boolean	<No Unit>

Table 12. Unit Value for the Threshold Type (Continued)

Threshold Type	Unit
String	<No Unit>
List	<No Unit>

- **Current Value** text field: Enables you to enter the current value of the threshold. For the selected threshold type *Boolean*, the page refreshes to display a drop-down list with possible values as **<NOT SELECTED>**, **TRUE**, and **FALSE**.

- **Min Value** text box: Enables you to enter the minimum value that can be used as the Current Value for the threshold. The Min Value text box is disabled unless the selected threshold type is INTEGER or REAL.

- **Max Value** text box: Enables you to enter the maximum value that can be used as the Current Value for the threshold. The Max Value text box is disabled unless the selected threshold type is INTEGER or REAL.

- **Using (operator)** drop-down list: Precedes with the dynamic label, which reflects the selected attribute name. When a function is selected from the **Function** drop-down list, the label applies the function as a prefix to the attribute name, for example, SUM(TRXN_BASE_AM).

  The drop-down list contains the following operator options: >, < , >=, <=,=, !=, IN, and is followed by a dynamic display of the Current Value. If no Current Value is specified, the page displays the **<Threshold Value>**.

Adding Thresholds

To add a user-defined threshold to the scenario, follow these steps:

1. On the Threshold page, click the **Add Threshold** button.

   The Add Threshold dialog box displays (Figure 16).

2. In the Add Threshold dialog box, do the following:

   a. Type the threshold name in the **Threshold Name** text box.

Note: Do not provide spaces in the threshold name field.

   b. Type the display name of the threshold in the **Display Name** text box.

      Optional: Type the description in the **Description** text box.

   c. Select the table name from the **Compare to Entity** drop-down list. This is the table from which you select an attribute to be use in your threshold.

   d. Select an associated table column from the **Attribute** drop-down list. This is the data field upon which the value for your threshold is calculated and compared.

   e. Select the function for an attribute from the **Function** drop-down list. Function allows you to specify some calculation to be performed on the selected attribute.

   f. Select the threshold type from the **Type** drop-down list.

   g. Select the unit from the **Unit** drop-down list.

   h. Type the current threshold value in the **Current Value** text box.

   i. Type the minimum allowed threshold value in the **Min Value** text box.

j. Type the maximum allowed threshold value in the **Max Value** text box.

k. Select the operator (for example, !=, <=) from the drop-down list.

l. Click **Save**.

The Add Threshold dialog box closes and a custom-defined entry of threshold displays on the Threshold List section of the Threshold page.

3. Enter additional thresholds as needed or click **Next** to move to the next step in creating a scenario.

Viewing Thresholds

To view the details of a threshold for the scenario, follow these steps:

1. Select a threshold entry from the **Threshold List** section.

The View Threshold Details button enables.

2. Click the **View Threshold Details** button.

The Threshold Details window displays where you can view the threshold information.

3. Click **Cancel** to close the window.

Modifying Thresholds

To modify threshold details, follow these steps:

1. Select a threshold entry from the **Threshold List** section.

The Edit Threshold Details button enables.

2. Click the **Edit Threshold Details** button.

The Edit Threshold dialog box displays where you can modify the threshold information.

3. In the **Edit Threshold** dialog box of the default threshold, perform one or more of the following edits:

a. Modify the display name of the threshold in the **Display Name** text box.

b. Modify the description in the **Description** text box.

c. Modify the current threshold value in the **Current Value** text box.

d. Modify the minimum threshold value in the **Min Value** text box.

e. Modify the maximum threshold value in the **Max Value** text box.

f. Click **Save**.

The modifications made to the threshold displays in the refreshed Threshold List.

4. *Alternatively*: In the **Edit Threshold** dialog box of the custom-defined threshold, perform one or more of the following edits:

a. Modify the display name of the threshold in the **Display Name** text box.

b. Modify the description in the **Description** text box.

c. Modify the selected table name from the **Compare to Entity** drop-down list.

d. Modify the selected associated table column from the **Attribute** drop-down list.

e. Modify the selected function for an attribute from the **Function** drop-down list.

f. Modify the selected threshold type from the **Type** drop-down list.

g. Modify the selected unit from the **Unit** drop-down list.

h. Modify the current threshold value in the **Current Value** text box.

i. Modify the minimum threshold value in the **Min Value** text box.

j. Modify the maximum threshold value in the **Max Value** text box.

k. Modify the selected operator (for example, !=, <=) from the drop-down list.

l. Click **Save**.

The modifications made to the threshold display the refreshed Threshold List.

Deleting Thresholds

To delete a threshold, follow these steps:

1. Select a threshold entry from the **Threshold List** section.

   The Delete Threshold button enables.

2. Click **Delete Threshold**.

   A message displays: *Do you really want to delete threshold?*

3. Click **OK**.

   The existing threshold entry is removed from the Threshold List section of the Threshold page.

Note: You can only delete a custom-defined threshold from the Threshold page.

Adding Threshold Sets

The Threshold Sets page enables you to create different threshold sets from the base threshold set by changing the Initial or Current value of the available thresholds. You cannot add or remove any thresholds from the new threshold sets.

The page displays the list of available thresholds for the threshold set (both the base threshold set and the custom-defined threshold set) that you select. By default, when creating a new scenario, the page displays only the base threshold set. For the base threshold set, you can only view their threshold values. For the custom-defined threshold sets, you can view, modify, and delete the thresholds values (Figure 17).
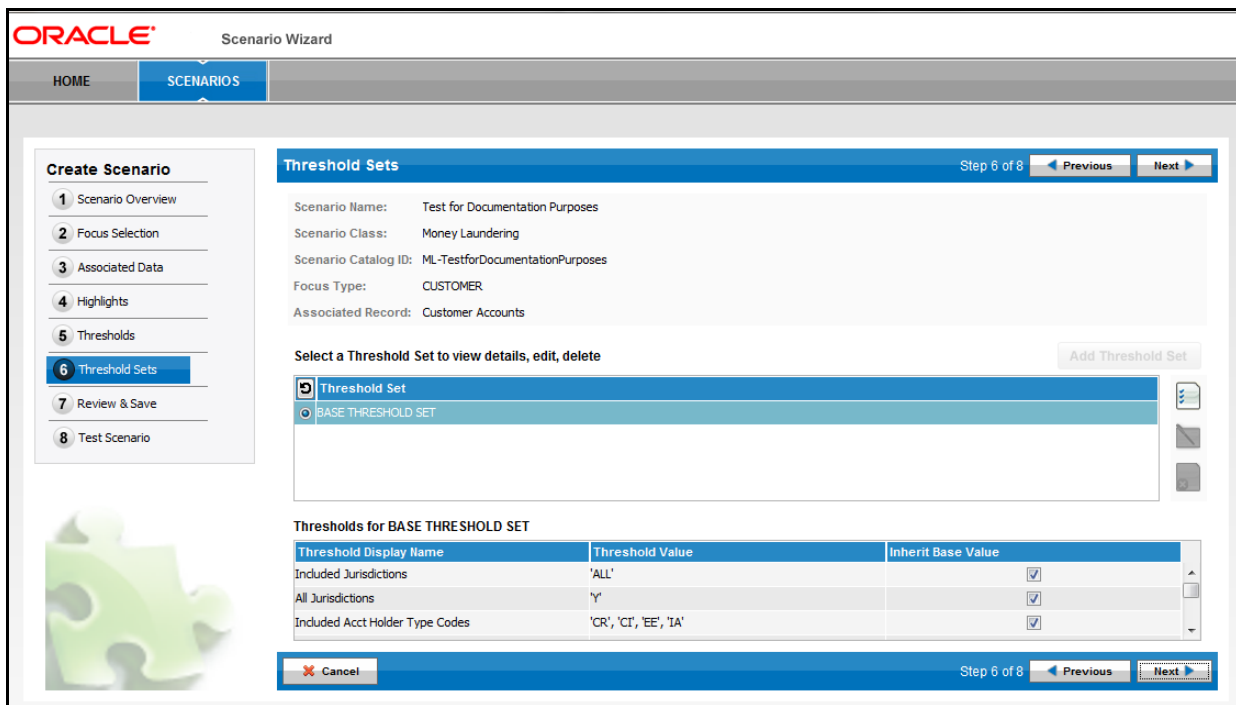
Figure 17. Threshold Sets Page

Components of the Threshold Sets Page

The Threshold Sets page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario Class** label: Displays the selected scenario class.

- **Scenario Catalog ID** label: Displays the scenario catalog ID.

- **Focus Type** label: Displays the focus of the scenario.

- **Associated Record** label: Displays the associated record of the scenario.

- **Threshold Set List** section: Displays the list of base and custom-defined threshold sets for the scenario being created. You can select the corresponding options to display their thresholds in the Thresholds List section.

- **Thresholds for BASE THRESHOLD SET** section: Displays the list of thresholds available for the threshold set that you select from the Threshold Set List section.

  This section contains the following columns:

  - **Threshold Display Name:** Displays the threshold name.

  - **Threshold Value:** Displays the current value of the threshold. For a threshold type of boolean, the value display is TRUE/FALSE.

  - **Inherit Base Value:** Displays an indicator of inherited base value. For the base threshold set, the **Inherit Base Value** check box is selected for each threshold. For thresholds belonging to a custom threshold set, the **Inherit Base Value** check box may not be checked if the custom threshold set is using a different current value for the threshold parameter than the base threshold set.

- **Add Threshold Set** button: Enables you to create a custom-defined threshold set on the Threshold Set List section.

- **View Threshold Set Details** button: Enables you to view the selected threshold set details.

- **Edit Threshold Set** button: Enables you to modify the selected custom-defined threshold set details.

- **Delete Threshold Set** button: Enables you to delete the selected custom-defined threshold set.

- **Previous** button: Navigates you to the previous page.

- **Next** button: Navigates you to the next page.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

Adding Threshold Sets

To add a custom-defined threshold set to the scenario, follow these steps:

1. On the Threshold Sets page, click the **Unselect All** icon to de-select the **BASE THRESHOLD SET** option.

   The Add Threshold Set button enables.

2. Click **Add Threshold Set**.

   The Add Threshold Set dialog box displays (Figure 18).

Threshold Dis...	Format	Min Value	Max Value	Current Value	Inherit Base V...
Included Jurisdic...	LIST			'ALL'	☑
All Jurisdictions	STRING			'Y'	☑
Included Acct H...	LIST			'CR', 'CI', 'EE', 'IA'	☑
Included Acct Bu...	LIST			'RBK', 'RBR'	☑
Min Open Acct Ct	INTEGER	1	100	2	☑
Min Close Acct Ct	INTEGER	1	100	2	☑
Lookback (Days)	INTEGER	1	120	30	☑

Figure 18. Add Threshold Set Dialog Box

3. In the Add Threshold Set dialog box, do the following:

   a. Type the threshold set name in the **Threshold Set Name** text box.

   b. In the **Inherit Base Value** column, click to de-select the check box for the threshold you want to modify. This enables the **Current Value** column for editing.

   c. Type the new value in the enabled **Current Value** column for the corresponding threshold. It is necessary to double-click in the field to fully enable the edit function.

d. Click **Save**.

The Add Threshold Set dialog box closes and a new custom-defined entry of threshold set displays in the Threshold Set List section of the Threshold Sets page.

4. Enter additional thresholds as needed or click **Next** to move to the next step in creating a scenario.

Viewing Threshold Sets

To view the details of a threshold set for the scenario, follow these steps:

1. Select a threshold set entry from the Threshold Set List section.

   The View Threshold Set Details button enables.

2. Click the **View Threshold Set Details** button.

   The Threshold Set Details window displays where you can view the threshold information.

3. Click **Cancel** to close the window.

Modifying Threshold Sets

To modify a custom-defined threshold set, you can perform one or more of the following modifications:

1. Select a threshold set entry from the Threshold Set List section.

   The **Edit Threshold Set Details** button enables.

2. Click the **Edit Threshold Set Details** button.

   The Edit Threshold Set dialog box displays where you can modify the threshold current value.

3. In the Edit Threshold Set dialog box, perform one or more of the following modifications:

   a. Modify the current value for a threshold which is not currently checked as inheriting the base threshold value by double-clicking within the **Current Value** field.

   b. To modify a threshold that is currently checked as inheriting the base threshold value, in the **Inherit Base Value** column, click to de-select the check box for the threshold you want to modify.

   c. Type the new value in a **Current Value** column for the corresponding threshold.

   d. Click **Save**.

   e. The Edit Threshold Set dialog box closes. The Threshold List is refreshed to show the changes for the thresholds used in the custom threshold set.

Deleting Threshold Sets

To delete a threshold set, follow these steps:

1. Select a custom-defined threshold set entry from the Threshold Set List section.

   The Delete Threshold Set button enables.

2. Click **Delete Threshold Set**.

   A message displays: *Do you really want to delete the Threshold Set?*

3. Click **OK**.

The existing threshold set entry removes from the Threshold Set List section of the Threshold Set page.

Note: User can create a scenario using the wizard and the threshold sets can be created and scenario execution can be done from the threshold editor page to run/view the scenario execution results. You can only delete the custom-defined threshold set from the Threshold Set page.

Saving the Scenario

The Scenario Wizard allows you to review the scenario information that has been entered. You can review and then save the scenario by clicking the **Save** button (Figure 19).
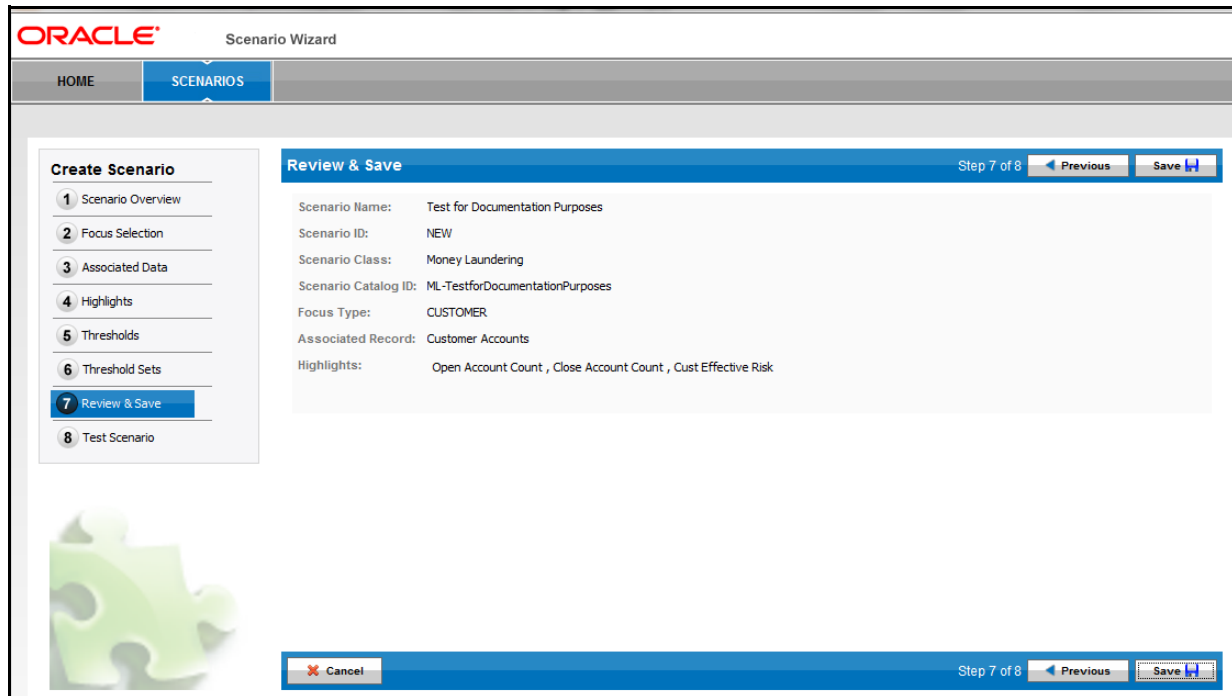
Figure 19. Review & Save page

Components of the Review & Save Page

The Review & Save page contains the following components:

- **Scenario Name** label: Displays the scenario name.
- **Scenario ID** label: Displays the scenario ID. On clicking the **Save** button, a unique ID is assigned to a newly created scenario.
- **Scenario Class** label: Displays the scenario class.
- **Scenario Catalog ID** label: Displays the scenario catalog ID.
- **Focus Type** label: Displays the focus type of the scenario.
- **Associated Record** label: Displays the associated record used for the scenario.
- **Highlights** label: Displays the highlights used for the scenario.
- **Previous** button: Navigates you to the previous page.

- **Cancel** button: Cancels the current process and navigates you to the Home page.

- **Save** button: Saves the scenario. The wizard verifies that there are no errors with the construction of the scenario that have not previously been identified and corrected. The warning messages display as appropriate to indicate where there may be errors.

Testing the Scenario

The Test Scenario page enables you to run the primary rule of the scenario with threshold values substituted from a selected threshold set. The results display the alerts you generate when running the scenario in a batch. The display includes the focus of the alert and the default highlights that are available if you selected all possible highlights during step four of the wizard.

To test the scenario, select a threshold set from the **Select a threshold set to test the scenario** drop-down list and click **Test Scenario**. The resultant output displays a paginated list, where you can navigate between pages (Figure 20).

Figure 20. Test Scenario page

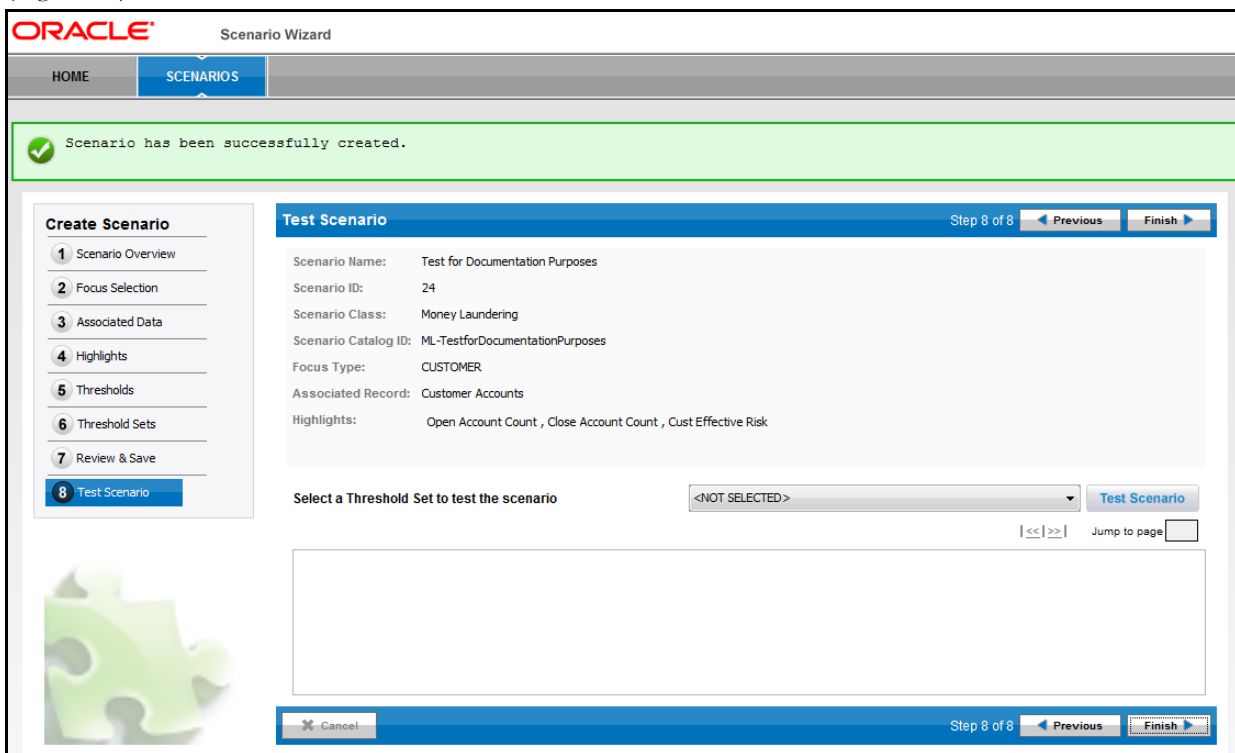### Components of the Test Scenario Page

The Test Scenario page contains the following components:

- **Scenario Name** label: Displays the scenario name.

- **Scenario ID** label: Displays the scenario ID

- **Scenario Class** label: Displays the scenario class.

- **Scenario Catalog** ID label: Displays the scenario catalog ID

- **Focus Type** label: Displays the focus type of the scenario.

- **Associated Record** label: Displays the associated record of the scenario.

- **Highlights** label: Displays the highlights used for the scenario.

- **Select a Threshold Set to test the scenario** drop-down list: Enables you to select the threshold set for test.

- **Test Scenario** button: Enables you to run the scenario with the selected threshold set.

Note: Threshold set can be created and tested using threshold editor where the scenario results are purged in the database until it is purged. You can change threshold sets and test again at any time on the Test page.

- **Finish** button: Enables you to close the scenario creation/editing wizard and redirect to the Home page.

- **Cancel** button: Enables you to cancel the current process and navigate to the Home page. When you click **Cancel**, a message displays: *Do you want to skip testing the scenario?*

  If you select **OK**, the wizard redirects to the Home page.

- **Previous** button: Enables you to navigate to the Review & Save page of the wizard.

To test a new scenario, follow these steps:

1. In the Test page, select the threshold sets from the **Select a Threshold Set to test the scenario** drop-down list.

2. Click **Test Scenario**.

   The Test page displays the scenario and focus data along with all the information that is pertinent for creating the match. The columns in the test results matrix corresponds to the highlights that you defined for the scenario.

Editing a Scenario

The Scenario Wizard enables you to modify existing scenarios. The editing process starts from the Home or Scenario page, where you select the scenario to modify. The Scenario Wizard navigates you to the Create Scenario wizard, where you can modify the scenario. Unlike creating the scenario, editing the scenario allows you to navigate directly to any page of the wizard.

When choosing to edit a scenario, depending on the extent of the changes required, you have three options:

- Modify and save basic edits to the current scenario.

- Deactivate the current scenario and create a new version of it with your changes.

- Leave the current scenario as active and create a new scenario using the Save As feature. This new scenario is basically a copy of the existing scenario.

Note: You cannot edit a scenario using the Scenario Wizard if you previously edited that scenario using the Scenario Manager.

Scenario Overview Page

In the Scenario Overview page, you can modify the values for existing scenario components. Refer to *Components of the Scenario Overview Page,* on page 28 for more information. If you modify the scenario class, the wizard warns you for resetting of the scenario. You have the option to deactivate the current scenario and proceed with your changes, creating a new scenario. Alternatively, you can select the **Save As** option, leaving the current scenario active, and proceed with creating a new scenario.

For both options, you are placed in the Create a Scenario workflow and must complete the subsequent pages in order.

If you elect to proceed with deactivating the current scenario, the utility refreshes the page with a newly selected Class and Scenario Catalog ID, deactivating the previous scenario/pattern. The navigation flow begins with a new scenario creation.

If you elect to create a new scenario by clicking the **Save As** button, the utility refreshes the page with a newly selected Class and Scenario Catalog ID, leaving the previous scenario/pattern still activated. The navigation flow begins with a new scenario creation.

On clicking the **Cancel** button, no change is applied. Changes to components other than Scenario Class do not result in a new scenario. Click the **Next** button to proceed to the next page or click any other page using the left hand side menu to make additional changes or proceed directly to Review and Save.

Selecting a Focus

In the Focus Selection page, you can modify the values for an existing scenario focus. Refer to *Components of the Focus Selection Page,* on page 30 for more information. If you modify the focus type, the wizard warns you for resetting of the scenario. You have the option to deactivate the current scenario and proceed with your changes, creating a new scenario. Alternatively, you can select the **Save As** option, leaving the current scenario active, and proceed with creating a new scenario.

For both options, you are placed in the Create a Scenario workflow and must complete the subsequent pages in order.

If you elect to proceed with deactivating the current scenario, the utility refreshes the page with a newly selected focus, deactivating previous scenario/pattern. The navigation flow begins with a new scenario creation.

If you elect to create a new scenario by clicking the **Save As** button, the utility refreshes the page with a newly selected Focus, leaving the previous scenario/pattern still activated. The navigation flow begins with a new scenario creation.

On clicking the **Cancel** button, no change is applied. Click the **Next** button to proceed to the next page or click any other page using the left hand side menu to make additional changes or proceed directly to Review and Save.

Associating the Data

In the Associated Data page, you can modify the value for data associated to the scenario. Refer to *Components of the Associated Data Page,* on page 32 for more information. If you modify the associated data, the wizard warns you for resetting of the scenario. You have the option to deactivate the current scenario and proceed with your changes, creating a new scenario. Alternatively, you can select the **Save As** option, leaving the current scenario active, and proceed with creating a new scenario.

For both options, you are placed in the Create a Scenario workflow and must complete the subsequent pages in order.

If you elect to proceed with deactivating the current scenario, the utility refreshes the page with a newly selected Associated Data, deactivating previous scenario/pattern. The navigation flow begins with a new scenario creation.

If you elect to create a new scenario by clicking the **Save As** button, the utility refreshes the page with a newly selected Associated Data, leaving the previous scenario/pattern still activated. The navigation flow begins with a new scenario creation.

On clicking the **Cancel** button, no change is applied. Click the **Next** button to proceed to the next page or click any other page using the left hand side menu to make additional changes or proceed directly to Review and Save.

Adding Highlights

On the Highlights page, you can add, modify, or delete the highlights for the scenario. Refer to *Components of the Highlights Page,* on page 33 for more information.

During the scenario editing process, you can perform the following tasks on the Highlights page:

- **Add Highlight:** Refer to section *Adding Pre-defined Highlights,* on page 37 and *Adding User-Defined Highlights,* on page 38 for more information.

- **View Highlight:** Refer to section *Viewing Highlights,* on page 39 for more information.

- **Modify Highlight:** Refer to section *Modifying Highlights,* on page 39 for more information.

- **Delete Highlight:** Refer to section *Deleting Highlights,* on page 40 for more information.

- **Re-order Highlight:** Refer to section *Re-ordering Highlights,* on page 40 for more information.

Adding Thresholds

On the Thresholds page, you can add, modify, or delete the thresholds for the scenario. Refer to *Components of the Thresholds Page,* on page 41 for more information.

During the scenario editing process, you can perform the following tasks on the Thresholds page:

- **Add Threshold:** Refer to section *Adding Thresholds,* on page 44 for more information.

- **View Threshold:** Refer to section *Viewing Thresholds,* on page 45 for more information.

- **Modify Threshold:** Refer to section *Modifying Thresholds,* on page 45 for more information.

- **Delete Threshold:** Refer to section *Deleting Thresholds,* on page 46 for more information.

Adding Threshold Sets

On the Threshold Sets page, you can add, modify, or delete the threshold sets for the scenario. Refer to *Components of the Threshold Sets Page,* on page 47 for more information.

During the scenario editing process, you can perform the following tasks on the Threshold Set page:

- **Add Threshold Set:** Refer to section *Adding Thresholds,* on page 42 for more information.

- **View Threshold Set:** Refer to section *Viewing Threshold Sets,* on page 49 for more information.

- **Modify Threshold Set:** Refer to section *Modifying Threshold Sets,* on page 49 for more information.

- **Delete Threshold Set:** Refer to section *Deleting Threshold Sets,* on page 49 for more information.

Saving the Scenario

On the Review & Save page, you can save the modification made on the preceding pages of the wizard. Refer to *Saving the Scenario,* on page 50 for more information.

CHAPTER 5 *Alert Creator Editor*

This chapter describes how to use the Alert Creator Editor administration tool to automatically group matches that share similar information into a single alert that is centered on the same focal entity. You can create new rules, modify the logic behind existing rules, and delete rules. The tool also displays the job ID and job template ID associated with each rule. This chapter focuses on the following topics:

- About the Alert Creator Editor
- About the Alert Creator Editor Screen Elements
- Using the Alert Creator Editor

About the Alert Creator Editor

By design, the application is configured to run a system job that generates an alert for every match detected. To increase work efficiency, you can use this tool to create custom jobs to run *before* the system job that group matches and share similar information into a single *multi-match* alert. The system job runs last to generate alerts for any matches that cannot be grouped.

The Alert Creator Editor enables you to view the logic used to group matches into alerts and allows you to add, delete, or update the logic. In addition, the Alert Creator Editor creates and updates the jobs that execute the rules and creates and updates job templates associated to the job for the particular rule.

Alert Creator Rule Guidelines

The following guidelines apply to the Alert Creator Editor:

- Each Alert Creation Rule is associated with a focus type. Matches grouped into an alert must share the same value for a given focus type. For example, account-focused matches that share the account identifier *12345* are grouped to create one alert, while account-focused matches with the account identifier *12346* are grouped into another alert.

- Each Alert Creation rule can also specify zero (0) or more additional bindings that must be shared by all matches.

  Bindings are variables captured in a scenario pattern.

● Each binding must be attributed as mandatory (!) or conditional (?). If a binding is specified as mandatory, all matches grouped together must have the same binding and the same value for that binding. If a binding is specified as conditional, matches that have that binding and have the same value for that binding is grouped together; matches that do not have this binding is grouped together.

For example, !FIRM ?ISSUE, wherein FIRM is the mandatory binding and ISSUE is conditional binding. In other words, for an alert to be created, each group must have a FIRM binding in which the values for that binding must match. In addition to FIRM binding, each group must either have an ISSUE binding in which the values match or each must be missing the ISSUE binding.

Note: You can select only those bindings that represent focal entities.

● One of three strategies must be selected for each Alert Creation rule. The strategies specify whether the same pattern, scenario, or scenario class must have generated all matches.

When you have finished using the Alert Creator Editor, you need to adjust the sequencing of the associated jobs. The following guidelines apply to job sequencing:

● To adjust the sequencing of the jobs, refer to your scheduling tool's documentation (for example, Control-M) to resequence the associated jobs. The Job ID and Job Template ID's associated with each rule are identified in both the Alert Creator Rule List and the Alert Creator Editor pages.

● Alert Creation jobs must run in a specified order (most specific to most general). If general jobs are run first, the matches would be grouped into one large (general group) alert as opposed to multiple (specific group) alerts.

● The system job must run after all other grouping jobs to create alerts for each match that could not be grouped, based on the defined grouping rules.

Note: Job Template IDs for all jobs are provided at deployment.

About the Alert Creator Editor Screen Elements

There are two pages associated with the Alert Creator Editor:

● **Alert Creator Rule List:** This is the first page displayed when you access the Alert Creator Editor. You can add or delete a rule from this page, or navigate to the Alert Creator Rule Editor to add or modify a rule. Refer to the *Alert Creator Rule List,* on page 59 for more information.

● **Alert Creator Rule Editor:** This page enables you to add or modify a rule. Refer to the *Alert Creator Rule Editor,* on page 60 for more information.

Alert Creator Rule List

The Alert Creator Rule List displays all rules sorted by Focus, Elements, and then Group Matches (Figure 21).

Figure 21. Alert Creator Rule List

The components of the Alert Creator Editor include the following:

- **Alert Creator Rule List:** Displays all rules with the following columns of information:
    - The Focus column displays the focus (first binding) of the rule.
    - The Elements column displays the bindings, other than focus, of the rule. A space (" ") displays between each set of operator and focus type values, for example, !SECURITY !EMPLOYEE ?FIRM.
    - The Group Matches column displays the Alert Creation Rule strategy. For example, Pattern, Scenario or Scenario Class.
    - The Job ID column displays the job number of the rule.
    - The Job Template ID displays the job ID template used to create the job referenced in the Job ID column.
- **Add button**: Navigates you to the Alert Creator Rule Editor to create a new rule.
- **Update button**: Navigates you to the Alert Creator Rule Editor to modify the selected rule.
- **Delete button**: Deletes the selected rule.

Alert Creator Rule Editor

From the Alert Creator Rule Editor, you can create a new rule or update an existing rule (Figure 22)
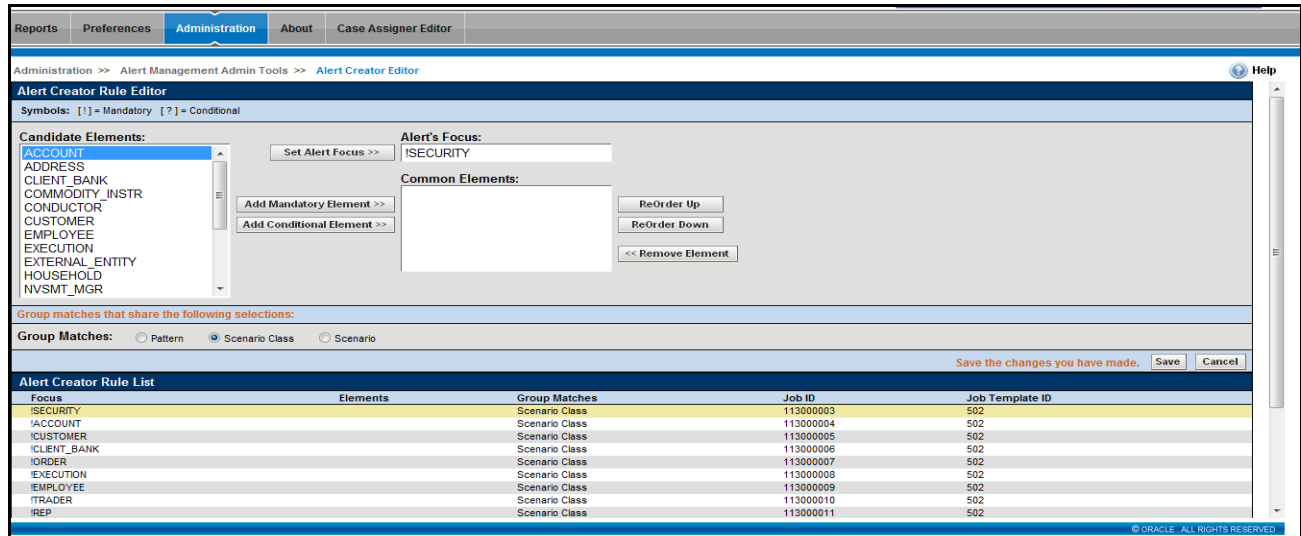

Figure 22. Alert Creator Rule Editor

The basic screen elements on the Alert Creator Rule Editor page are categorized into two areas:

- The Alert Creator Rule Editor area where you can create or update a rule.

- The Alert Creator Rule List that displays the rule's Focus, Elements, Group Matches, Job IDs, and Job Template IDs (but does not contain the Update or Delete buttons). Refer to the *Alert Creator Rule List,* on page 59 for more information.

The components of the Alert Creator Rule Editor include the following:

- **Candidate Elements** list box: Displays available elements in ascending alphabetical order.

  - When you select **Add**, the Candidate Elements list box is populated with a value for the full name of each focus.

  - When you select **Update**, the Candidate Elements list box is populated with a value for the full name of each focus type that is not associated with the rule being updated as either the Alert's focus or a common element.

- **Alert's Focus** text box: The focus of the resulting alert.

  - When you select **Add**, the **Alert's Focus** text box displays as blank (" ").

  - When you select **Update**, the **Alert's Focus** text box displays with the value representing the focus of the selected rule.

- **Common Elements** list box: Displays elements in the sequence in which they are associated to the rule. Common elements are the additional bindings that must be shared by matches to be grouped.

- When you select **Add**, the Common Elements list box displays as blank (" ").

- When you select **Update**, the Common Elements list box displays a value representing the common elements of the selected rule.

● **Group Matches** options: Displays options to group matches that share the same **Pattern**, **Scenario**, or **Scenario Class**.

- When you select **Add**, a Group Matches option is not selected.

- When you select **Update**, the Group Matches displays the translation of the Alert Creation Rule strategy of the associated rule.

● **Set Alert Focus button**:

- Replaces any existing value in the Alert's Focus box with the value selected in the Candidate Elements list box.

- Resets the Common Elements list box by removing any values in the Common Elements list box.

- Resets the Candidate Elements list box by displaying a value for every focus type, except the value selected as the Alert's focus.

● **Add Mandatory Element button**:

- Adds the value selected in the Candidate Elements list box as the last value listed in the Common Elements list box.

- Prepends an exclamation point (!) to the value added to the Common Elements list box.

- Removes the selected value from the Candidate Elements list box.

● **Add Conditional Element button**:

- Adds the value selected in the Candidate Elements list box as the last value listed in the Common Elements list box.

- Prepends a question mark (?) to the value added to the Common Elements list box.

- Removes the selected value from the Candidate Elements list box.

● **ReOrder Up button**: Reorders the sequence of the displayed common elements by shifting the selected value above the preceding value.

● **ReOrder Down button**: Reorders the sequence of the displayed common elements by shifting the selected value below the following value.

● **Remove Element button**:

- Removes the selected element value from the Common Elements list box.

- Adds the selected value without the exclamation point (!) or question mark (?) to the Candidate Elements list box.

● **Save button**: Saves the rule.

● **Cancel button**: Navigates to the Alert Creator Rule List and does not create the rule or update the existing rule.

Using the Alert Creator Editor

This section explains how to perform the following functions using the Alert Creator Editor:

- Adding a Rule

- Modifying a Rule

- Deleting a Rule

Adding a Rule

To add a new rule to the Alert Creator Rule List, follow these steps:

1. Click **Add**.

   The Alert Creator Rule Editor displays.

2. Select an element in the Candidate Elements list that you want to use as the focus for the rule.

3. Click **Set Alert Focus** to move the element you selected in the Candidate Elements list box to the **Alert's Focus** text box.

   The element is removed from the Candidate Elements list box and displays in the **Alert's Focus** text box, preceded by a !.

4. Select an element in the Candidate Elements list box that you want to assign as a mandatory element.

5. Click **Add Mandatory Element** to add the selected element to the Common Elements list box.

   The element is removed from the Candidate Elements list box and displays in the Common Elements list box, preceded by a !.

6. Select an element in the Candidate Elements list box that you want to assign as a conditional element.

   Selecting a conditional element is optional. Proceed to Step 9, if you do not add a conditional element.

7. Click **Add Conditional Element** to add the selected element to the Common Elements list box.

   The element is removed from the Candidate Elements list box and displays in the Common Elements list box, preceded by a ?.

8. Click the desired **Group Matches** option.

9. Click **Save**.

   The Confirmation dialog box displays.

10. Click **OK**.

    The system creates a new alert creation job template and creates and associates a new job based on the new job template to the new rule

Note: It is not important whether you specify mandatory elements before conditional elements. You should add elements to the Common Elements list box in the order in which you want the application to evaluate the elements. Use the **ReOrder Up** and **ReOrder Down** buttons to make those adjustments. In addition, you can repeat Step 4 through Step 7 as needed for your rule.

Modifying a Rule

To modify an existing rule in the Alert Creator Rule List, follow these steps:

1. Select the rule and click **Update**.

   The Alert Creator Rule Editor displays.

2. Update the **Candidate Elements**, **Alert's Focus**, and **Common Elements** values.

   Changing the focus of a rule, in the **Alert's Focus** text box, returns all elements in the Common Elements list to the Candidate Elements list, which requires you to specify new common elements for the new focus.

3. Click the desired **Group Matches** option, if applicable.

4. Click **Save**.

   The Confirmation dialog box displays.

5. Click **OK**.

   The system updates the strategy of the existing alert creation rule to the option selected in **Group Matches**.

   Also, the system updates the binding of the existing alert creation rule by concatenating the following:

   ● An exclamation point with the value selected in the **Alert's Focus** field.

   ● The symbol (that is, ! or ?).

   ● Value for each value listed in the Common Elements list box.

Deleting a Rule

To delete an existing rule from the Alert Creator Rule List, follow these steps:

1. Select the rule and click **Delete**.

   The system displays a Confirmation dialog box with a message: *Do You want to delete the selected Alert Creation Rule?*.

2. Click **OK**.

   The system deletes the job associated to the rule and deletes the job template associated with the job for the selected rule.

CHAPTER 6 *Alert Scoring Editor*

This chapter describes how to use the Alert Scoring Editor administration tool to create new rules or modify the logic behind existing rules that prioritize alerts automatically:

- About the Alert Scoring Editor
- Scoring Match Strategies
- About the Alert Scoring Editor Screen Elements
- Using the Alert Scoring Editor
- Using the Scoring Editors

About the Alert Scoring Editor

The score of an alert is a measure of priority or risk that an analyst can use to determine the appropriate sequence in which to investigate alerts. Depending upon the configuration of your specific installation, the alert score may also determine whether the system closes the alert automatically. The system bases the score of an alert on the score of the matches that compose it. Match scoring computes the score for individual matches to provide an initial prioritization. This dependency implies that scoring of matches must occur *before* the determination of an alert's score.

The Alert Scoring Editor allows you, the application Administrator, to view, modify, or delete the rules that the system uses to determine the score for matches and alerts. You can also create or modify existing match scoring rules for each Scenario, and variations of each rule for each Threshold Set in a Scenario. In the Alert Scoring Editor, you can view a history of changes to each rule and its variations.

Scoring Match Strategies

Scoring of matches can occur using any combination of the following strategies:

- **Simple Lookup:** Criteria can be established that increment a match's score by a pre-defined value (when satisfied in match information). It supports adding multiple filters for a rule.

  For example, if the match focuses on high-risk entity and the entity has wire transactions of more than 100, increment the score by 25.

- **Graduated Value:** Criteria can be established that increment a score based on the value of a match's attributes as compared to a graduated scale. Determination of the graduated scale establishes a minimum value, a minimum score, a maximum value, and a maximum score. The system determines the relative score for all values between the minimum and maximum values. It supports adding multiple filters for a rule.

  For example, if the number of transactions of a match is less than or equal to 10, increment the score by 20. If the number of transactions of a match is greater than or equal to 30, increment the score by 40. Where 5 or more of the transactions are wire transaction and the transaction amount is greater than USD 20,000.

  The system determines the appropriate score between 20 and 40 for any match which satisfies the rule but not the filter. if the match satisfies the filters then the score is increased by 40.

● **Prior Matches:** Criteria can be established that increment a match's score based not on attributes of the match, but on the quantity of matches focused on the same entity as the match and generated by the same scenario or scenario class as the match. A look back period limits the strategy to count only matches generated in the last *N* days.

For example, for each match on an entity and scenario AA within the last 10 days, increment the score by five (5).

The Prior Matches scoring strategy also supports scoring in which the score of an alert increases by a greater amount when the number of occurrences nears or exceeds the minimum value, rather than the maximum value.

● **Simple Scenario:** Criteria can be established that increment the score if a specific scenario generated the match.

For example, if an Account scenario (AC) generated the match, increment the score by 10.

● **Scoring Rule Set:** Criteria can be established to provide different scores for a matches if the match satisfies multiple rules defined.

For example, if the rules defined are as follows:

Scoring Tier 1, Number of Transactions = 40, Score 20, Next Scoring Tier is 2

Scoring Tier 2, Customer age between 20 to 40, Score 30, Next Scoring Tier is 3

Scoring Tier 3, Transaction Amount is between 10,0000 USD to USD 20,000 score is 40

The system initially checks for which rule attribute there is a match and then moves to the next scoring tier. If the match does not satisfy the values of a next scoring tier the system assigns a score as of the previous scoring tiers matched by summing up those and max it to 100 if it exceeds.

About the Alert Scoring Editor Screen Elements

The Alert Scoring Editor provides information in two areas:

● **Alert Scoring Editor:** Displays when accessing the Alert Scoring Editor Administration Tool. You can navigate to a Scoring Rule Editor List page to add, modify, or delete a rule. In addition, you can change the Alert Scoring Strategy. Refer to *Alert Scoring Editor,* on page 67 for more information.

● **Alert Scoring Strategy Selector with Match Scoring Rule List:** Enables you to add, modify, or delete a rule using one of the following match scoring rule editors:

■ Simple Lookup Scoring Editor (Refer to *Simple Lookup Scoring Rule Editor,* on page 71 for more information.)

■ Graduated Value Scoring Editor (Refer to *Graduated Value Scoring Rule Editor,* on page 74 for more information.)

■ Prior Matches Scoring Editor (Refer to *Prior Matches Scoring Rule Editor,* on page 78 for more information.)

■ Simple Scenario Scoring Editor (Refer to *Simple Scenario Scoring Rule Editor,* on page 81 for more information.)

■ Scoring Rule Set (Refer to *Scoring Rule Set List,* on page 84 for more information.)

Note: For a Scenario Class, you can modify or delete an existing rule. For a Scenario, you can create a new rule, or modify or delete an existing rule.

Alert Scoring Editor

Select a Scenario Class or a Scenario in the Alert Scoring Editor (Figure 23) to display all alert scoring rules that relate to that Scenario Class or Scenario.
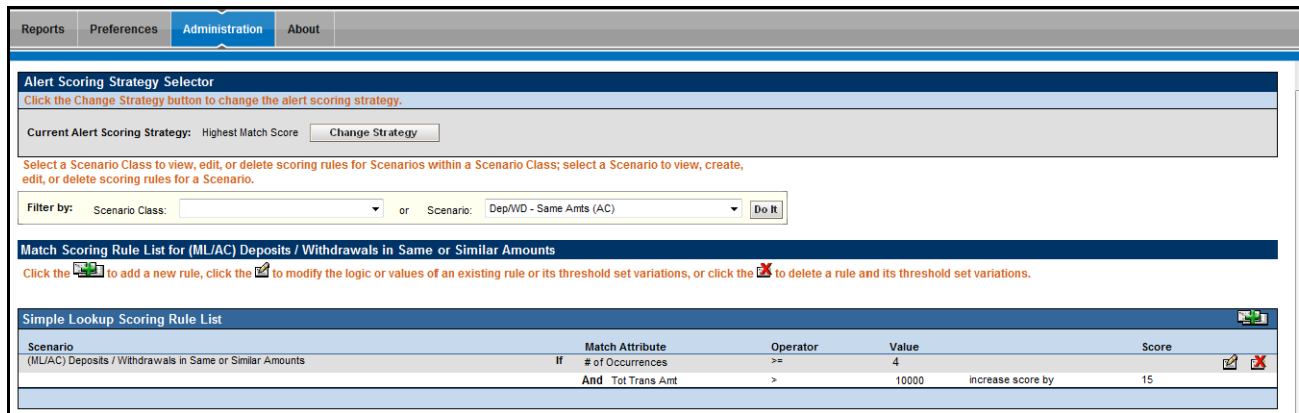

Figure 23. Alert Scoring Editor

The Alert Scoring Editor includes the following components:

- Alert Scoring Strategy Selector

- Search Bar

- Alert Scoring Strategy Selector with Match Scoring Rule Lists

Alert Scoring Strategy Selector

The Alert Scoring Strategy Selector allows you to view and change the strategy for alert scoring (Figure 24)..
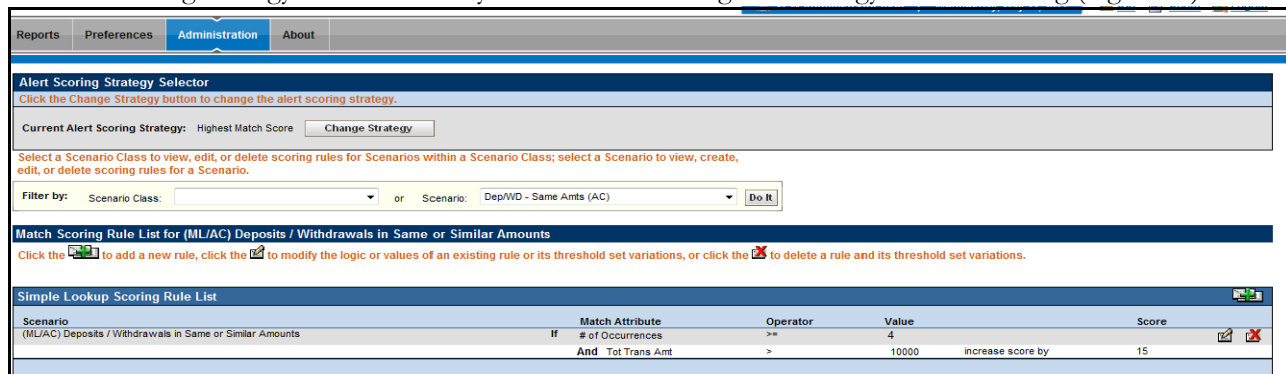
Figure 24. Alert Scoring Strategy Selector

Click **Change Strategy** to display the following screen elements in the Alert Scoring Strategy Selector:

- **Current Alert Scoring Strategy:** Displays the name of the currently set alert scoring strategy.

- **New Alert Scoring Strategy** option buttons: Enables you to select an alert scoring strategy of Highest Match Score or Average Match Score.

    - **Highest Match Score:** Bases the score of an alert on the most critical match associated with the alert. The system assigns the alert a score equal to the highest score of any of the associated matches.

For example:

Match 1	Score = 40
Match 2	Score = 80
Match 3	Score = 60
Alert	Score = 80

■ **Average Match Score:** Assigns an alert a score equal to the average of the scores of the associated matches. The system sums each of the score's associated matches and divides the total by the quantity of related matches.

For example:

Match 1	Score = 40
Match 2	Score = 80
Match 3	Score = 60
Alert	Score = 60 ((40+80+60)/3)

● **Save** button: Saves the new alert scoring strategy.

Note: If you change the scoring strategy, a confirmation dialog box displays prompting you to confirm the change. Click **OK** to continue and save the new strategy.

● **Cancel** button: Redisplays the Alert Scoring Editor without a change to the alert scoring strategy.

Search Bar

The search bar allows you to filter the list of match scoring rules by Scenario Class or Scenario (Figure 25).

Figure 25. Alert Scoring Editor Search Bar

Components of the search bar include the following:

● **Filter by: Scenario Class** drop-down list: Provides all installed Scenario Classes. The values in the Scenario Class drop-down list display in alphabetically ascending order.

If you select a Scenario Class, you cannot select a Scenario from the **Scenario** drop-down list.

● **Filter by: Scenario** drop-down list: Provides valid long names of all installed Scenarios. Values in the Scenario drop-down list display in alphabetically ascending order by scenario long name.

If you select a Scenario, you cannot select a Scenario Class from the Scenario Class drop-down list.

● **Do It** button: Displays all match scoring rules that relate to the selected Scenario Class or Scenario.

Alert Scoring Strategy Selector with Match Scoring Rule Lists

The Match Scoring Rule List displays below the Alert Scoring Search Bar after you select a Scenario Class or Scenario and click **Do It**. Within the Match Scoring Rule List, each match scoring strategy displays for the selected Scenario Class or Scenario
(Figure 26).

Figure 26. Alert Scoring Strategy Selector - Match Scoring Rule List

The Match Scoring Rule List includes the following components:

- Areas that contain the list of rules for each of the various match scoring strategies:

  - **Simple Lookup Scoring Rule List:** Displays the Scenario, Match Binding, Operator, Value, and Score columns for each base scoring rule. Refer to *Simple Scoring Rule Editor Components,* on page 72 for column descriptions.

  - **Graduated Value Scoring Rule List:** Displays the Scenario, Match Binding, Min Value, Min Score, Max Value, and Max Score columns for each base scoring rule. Refer to *Graduated Value Scoring Rule Editor Components,* on page 76 for column descriptions.

  - **Prior Matches Scoring Rule List:** Displays the Scenario, Min Number Matches, Min Score, Max Number Matches, Max Score, Look Back, and Within columns for each base scoring rule. Refer to *Prior Matches Scoring Rule Editor Components,* on page 79 for column descriptions.

- ■ **Simple Scenario Scoring Rule List**: Displays the Scenario (within rule text) and Score columns for each base scoring rule. Refer to the *Simple Scenario Scoring Rule Editor Components,* on page 82 for column descriptions.

- ■ **Scoring Rule Set:** Displays the scoring rule set for a particular scenario (Refer to *Scoring Rule Set List,* **on page 84** for more information.)

- **Add** button: Navigates you to the associated Match Scoring Rule Editor.

  Note: The **Add** button is available only if you select an option in the **Scenario** drop-down list.

- **Update** button: Navigates you to the associated Alert Scoring Editor.

- **Delete** button: Deletes the match scoring rule.

Scoring Rule Variation List

The Scoring Rule Variation List displays after clicking either the **Add** or **Update** button in any scoring rule list (Figure 27 illustrates the Simple Lookup Scoring Rule Variation List). This list contains attributes of Threshold rule variations, which depend on the scoring rule that you use.

Figure 27. Simple Lookup Scoring Rule Editor- Scenario Filtering

The variation list contains the same components as those in the Scoring Rule Editor as well as the following:

- **+ Icon (Threshold History):** Opens a window below the selected Threshold that contains a scrollable list of modifications to a rule variation for a Threshold (Figure 28).

Figure 28. Expanded Rule Modification History

Threshold history includes modification date, user who updated the rule, modified rule attributes, and any comment(s) about the update.

When the history window is open, clicking the orange - icon closes it.

- **Threshold Set** label: Displays the names of individual Thresholds that compose the Threshold Set, including the Base Threshold Set.

- **Inherit** label: Determines whether a Threshold inherits the rule attributes for the Base Threshold Set.

This applies only to rule variations for a Scenario.

- **Add a Comment** field: Allows you to type comments (from 3 to 4,000 characters) about new rules or changes that a user made to a current rule.

Comments also display as part of scoring rule history.

- **The text area contains _ characters** text box: Numeric field that provides the current number of characters in the **Add a Comment** field.

- **Save** button: Saves any changes that you made and displays the previous screen.

- **Revert** button: Reverts to previous values without saving any modifications and displays the previous screen.

Simple Lookup Scoring Rule Editor

When you click **Add** or **Update** in the Simple Lookup Scoring Rule List and filter by Scenario, or click **Update** when filtering by Scenario Class, the Simple Lookup Scoring Rule Editor with Scoring Rule Variation List displays (Figure 27).

The Simple Lookup Scoring Rule Editor allows you to add and update rules (depending on filtering by Scenario Class or Scenario) that, when in a match's information, result in incrementing a match's score by a standard value.

The Scoring Rule Variation List, provides a history of changes or updates for the match binding associated within each pattern and other scoring parameters for the selected Scenario Class or Scenario.

The following sections describe the components of the Simple Lookup Scoring Rule Editor, and the components in the Rule Editor when you modify a rule:

- Simple Scoring Rule Editor Components (refer to *Simple Scoring Rule Editor Components,* on page 72 for more information).

- Simple Lookup Scoring Rule Modification (refer to *Simple Lookup Scoring Rule Modification,* on page 73 for more information).

Simple Scoring Rule Editor Components

The Simple Lookup Scoring Rule Editor includes the following components:

- **Scenario Class** label: Displays (not editable) the name of the Scenario Class when you select this editor to create a scoring rule for a Scenario Class.

    Or

- **Scenario** label: Displays (not editable) the name of the Scenario when you select this editor to create a scoring rule for a Scenario.

- **Match Attribute** drop-down list: Contains a value for each binding description associated within each pattern and a matched record within the selected Scenario Class (if you are updating a rule for a Scenario Class), or a value for each binding description and matched record (displays in table.column format) associated with patterns within the selected Scenario (if you are adding or updating a rule for a single Scenario). The values display in ascending alphabetic order.

    - If you select **Add**, the first option in the Match Attribute drop-down list displays as the sample value.

    - If you select **Update**, the current match attribute for the selected rule displays in the Match Attribute drop-down list field.

- **Match Record Strategy** drop-down list: Displays Min, Max and Sum. This is enabled only if you choose a matched record from the Match Attribute drop-down list. The value of the match record strategy is displayed in Parenthesis beside the matched record after selection of the value. This is mandatory to be selected for any matched record being selected in the Match Attribute drop-down list.

- **Operator** drop-down list: Contains the values <, <=, >, >=, =, and !=.

    - If you select **Add**, the Operator drop-down list displays = as the default.

    - If you select **Update**, the Operator drop-down list displays the current Operator for the selected rule.

- **Value** text box: Displays a value as an enumerated figure or range to associate to the selected value in the Match Attribute drop-down list.

    - If you select **Add**, the **Value** text box displays the text *Value*.

    - If you select **Update**, the **Value** text box displays the current value entry for the selected rule.

- **Score** text box: Displays a value assigned to matches that meet all rule criteria.

    - If you select **Add**, the **Score** text box displays the text *Score*.

    - If you select **Update**, the **Score** text box displays the current score entry for the selected rule.

    - The score can be any numeric value, less than, greater than, or equal to zero (0) and less than or equal to the application's Maximum Match Score.

    For example, you can create range-based scoring rules using negative values in the **Score** field: To get 10 points for a value between 100 and 500, use:

    Rule 1: If the value is greater than or equal to 100, then add 10 points to the **Score** field.

    Rule 2: If the value is greater than 500, then add negative 10 (-10) points to the **Score** field.

    To reduce the score when high amounts are involved, use:

Rule 1: If the value is greater than 10,000,000, then add negative 50 (-50) to the **Score** field.

You can also combine this with the Graduated Lookups to get a *below minimum* that adds nothing to the alert, but you do not have to start the range at zero (0).

- **And** button: Allows you to add multiple filters for a rule using. This is optional for a rule definition. You can add *x* number of filters for a rule, where x is a configurable parameter in config.xml.

Simple Lookup Scoring Rule Modification

For a Scenario, you can modify the scoring rule for each attribute that you select in the Match Attribute drop-down list (Figure 29).

Figure 29. Match Attribute Scoring Rule Modification

When you enter values in the **Value** and **Score** fields and click **Save**, the Scoring Rule Variation List displays (Figure 30).

Figure 30. Scoring Rule Variation List by Scenario

For each rule variation for a Threshold Set, you can do the following:

- Enter new values

- View a history of changes to a rule

- Enter comments that describe the value of, or changes to a rule

Note: You can enter negative values by changing the scoring increment to a negative value. For example you would have two simple lookup rules as follows:
If <binding name 1> = 50, increase score by 10
If <binding name 2> = 100 increase score by -5
If for a particular match, "binding name 1" had a value of 50 and "binding name 2" had a value of 100, the final score would be 5.

Scoring Rule Variation List, on page 70 and *Simple Scoring Rule Editor Components,* on page 72 provide description of most components in the Scoring Rule Variation List. The Simple Lookup Scoring Rule Editor also contains the following buttons:

- **And:** Allows you to add new filters for a rule. If at any time you want to remove a filter already associated to a rule, click the Remove button available for each of the filter rows.

- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which the Inherit check box is selected).

- **Save**: Saves your changes to the rules and displays the previous screen.

- **Revert**: Exits the area without saving any changes and displays the previous screen.

Graduated Value Scoring Rule Editor

The Graduated Value Scoring Rule Editor displays after clicking **Add** or **Update** in the Graduated Value Scoring Rule List (Figure 31). The Graduated Value Scoring Rule Editor allows you to create and edit rules that increment scores based on the value of a match's attributes as compared to a graduated scale.

Figure 31. Graduated Value Scoring Rule Editor

The following sections describe the components of the Graduate Value Scoring Rule Editor, and the components in the Rule Editor when you modify a rule:

- Graduated Value Scoring Rule Editor Components (refer to *Graduated Value Scoring Rule Editor Components,* on page 76 for more information).

- Graduated Value Scoring Rule Modification (refer to *Graduated Value Scoring Rule Modification,* on page 77 for more information).

Graduated Value Scoring Rule Editor Components

Components of the Graduated Value Scoring Rule Editor include the following:

- **Scenario Class** label: Displays (but is not editable) the name of the Scenario Class when you select this editor to create a scoring rule for a Scenario Class.

  Or:

- **Scenario** label: Displays (but is not editable) the name of the Scenario when you select this editor to create a scoring rule for a Scenario.

- **Match Attribute** drop-down list: Contains a value for each binding description associated within each pattern and matched record within the selected Scenario Class (if you are updating a rule to a Scenario Class), or a value for each binding description and matched record (displays in table.column format) associated with patterns within the selected Scenario (if you are adding or updating a rule to a single Scenario). The values display in ascending alphabetic order.

  - If you select **Add**, the Match Attribute drop-down list displays the first option in the list as the default value.

  - If you select **Update**, the Match Attribute drop-down list field displays the current match attribute for the selected rule.

- **Match Record Strategy** drop-down list: Displays Min, Max and Sum. This is enabled only if you choose a matched record from the Match Attribute drop-down list. The value of the match record strategy is displayed in Parenthesis beside the matched record after selection of the value. This is mandatory to be selected for any matched record being selected in the Match Attribute drop-down list.

- **Min Value** text box: Must contain the minimum value for the selected binding description in the Match Attribute drop-down menu for the rule to apply.

  - If you select **Add**, the **Min Value** text box displays the text *Min Value*.

  - If you select **Update**, the **Min Value** text box displays the current minimum value entry for the selected rule.

  - Accepts a numeric value that is greater than or equal to zero (0) and less than the maximum value.

- **Min Score** text box: Must contain the score value that applies to the minimum value for the selected binding description in the Match Attribute drop-down menu for the rule to apply.

  - If you select **Add**, the **Min Score** text box displays the text *Min Score*.

  - If you select **Update**, the **Min Score** text box displays the current minimum score entry for the selected rule.

  - Accepts a minimum score of a numeric value greater or equal to zero (0) and less than or equal to the maximum score.

- **Max Value** text box: Must contain the maximum value for the selected binding description selected in the Match Attribute drop-down menu for the rule to apply.

  - If you select **Add**, the **Max Value** text box displays the text *Max Value*.

  - If you select **Update**, the **Max Value** text box displays the current maximum value entry for the selected rule.

  - Accepts a numeric value that is greater than or equal to zero (0) and greater than the minimum value.

- **Max Score** text box: Must contain the score value that would apply to the maximum value for the binding description selected from the Match Attribute drop-down menu for the rule to apply.

  - If you select **Add**, the **Max Score** text box displays the text *Max Score*.

  - If you select **Update**, the **Max Score** text box displays the current maximum score entry for the selected rule.

  - Maximum score must be a numeric value greater or equal to the minimum score and less than or equal to the application's Maximum Match Score set during installation.

  - Click the **And** button if you wish to add multiple filters for a rule.

Graduated Value Scoring Rule Modification

For a particular Scenario, you can modify the graduated value scoring rule for each attribute that you select in the Match Attribute drop-down list (Figure 32).

Figure 32. Match Attribute Scoring Rule Modification

When you enter values in the **Min Value**, **Min Score**, **Max Value**, and **Max Score** fields and click **Save**, the Scoring Rule Variation List displays (Figure 33).

Figure 33. Graduated Value Scoring Rule Variation List by Scenario

For each rule variation for a Threshold Set, you can do the following:

- Enter new values

- View a history of changes to a rule

- Enter comments that describe the value of, or changes to, a rule

Scoring Rule Variation List, on page 70 and *Graduated Value Scoring Rule Editor,* on page 74 provides description of most components in the Scoring Rule Variation List. The Graduated Value Scoring Rule Editor also contains the following buttons:

- **And:** Allows you to add new filters for a rule. If at any time you want to remove a filter already associated to a rule, click the Remove button available for each of the filter rows.

- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which the **Inherit** check box is selected).

- **Save**: Saves your changes to the rules and displays the previous screen.

- **Revert**: Exits the area without saving any changes and displays the previous screen.

Prior Matches Scoring Rule Editor

The Prior Matches Scoring Rule Editor (Figure 34) displays after you click **Add** or **Update** in the Prior Matches Scoring Rule List. The Prior Matches Scoring Rule Editor allows you to create and edit rules based not on attributes of the match, but based on the quantity of matches focused on the same entity as the match and generated by the same scenario or scenario class as the match. A look back period also constrains the strategy to count only matches that the system generated in the last N days.

Figure 34. Prior Matches Scoring Rule Editor

The following sections describe the components of the Prior Matches Scoring Rule Editor, and the components in the Rule Editor when you modify a rule:

- Prior Matches Scoring Rule Editor Components (refer to *Graduated Value Scoring Rule Editor Components,* on page 76 for more information).

● Prior Matches Scoring Rule Modification (refer to *Graduated Value Scoring Rule Modification,* on page 77 for more information).

Prior Matches Scoring Rule Editor Components

The Prior Matches Scoring Rule Editor includes the following components:

● **Scenario Class** label: Displays (but is not editable) the name of the Scenario Class when you select this editor to create a scoring rule for a Scenario Class.

Or:

● **Scenario** label: Displays (but is not editable) the name of the Scenario when you select this editor to create a scoring rule for a Scenario.

● **Min Number Matches** text box: Must contain the minimum number of matches that meet the Same Scenario criteria for the rule to apply.

   ■ If you select **Add**, the **Min Number** text box displays the text *Min Number*.

   ■ If you select **Update**, the **Min Number** text box displays the current minimum number entry for the selected rule.

   ■ Accepts a numeric value that is greater than or equal to zero (0) and less than or equal to the maximum number.

● **Same Scenario** drop-down list: Designates that you select matches that are focused on the same entity, focused on the same entity and generated by the same scenario, or focused on the same entity and generated by the same scenario class.

   ■ If you select **Add**, the Same Scenario drop-down list displays the default value of *focused on the same entity*.

   ■ If you select **Update**, the Same **Scenario** text box displays the current entity or scenario entry for the selected rule.

● **Alert Closing Classification** list box: Designates that you select matches that are closed with Actionable, Indeterminate, or Non-actionable classification. You can configure the list of Alert Closing Classification names at the time of installation (Refer to the *Installation Guide* for more information).

   ■ If you select **Add**, all classifications in the Alert Closing Classification list box are selected.

   ■ If you select **Update**, the Alert Closing Classification list box displays the current classification for the selected rule.

   Note: If you do not want to search matches on Alert Closing Classification, select all options in the list box.

● **Look Back Days** text box: Must contain the number of days prior to the current date that the rule searches for matches that meet all other prior match scoring rule criteria.

   ■ If you select **Add**, the **Look Back Days** text box displays the text *Look Back Days*.

   ■ If you select **Update**, the **Look Back Days** text box displays the current look back days entry for the selected rule.

   ■ Enter a numeric value in this text box that is greater than or equal to zero (0).

● **Min Score** text box: Must contain the score value to be assigned to matches that meet the minimum value for the selected attribute in the **Same Scenario** drop-down list for the rule to apply.

- ■ If you select **Add**, the **Min Score** text box displays the text *Min Score*.

- ■ If you select **Update**, the **Min Score** text box displays the current minimum score entry for the selected rule.

- ■ Minimum score must be a numeric value greater or equal to zero (0) and less than or equal to the maximum score.

- ● **Max Number Matches** text box: Must contain the maximum number of matches that meet the Same Scenario criteria for the rule to apply.

  - ■ If you select **Add**, the **Max Number** text box displays the text *Max Number*.

  - ■ If you select **Update**, the **Max Number** text box displays the current maximum number entry for the selected rule.

  - ■ Enter a numeric value in this text box that is greater than or equal to zero (0) and greater than or equal to the minimum number.

- ● **Max Score** text box: Must contain the score value to be assigned to matches that meet the maximum value for the attribute selected from the Same Scenario drop-down list for the rule to apply.

  - ■ If you select **Add**, the **Max Score** text box displays the text *Max Score*.

  - ■ If you select **Update**, the **Max Score** text box displays the current maximum score entry for the selected rule.

  - ■ Maximum score must be a numeric value greater or equal to the minimum score and less than or equal to the application's Maximum Match Score set during installation.

Prior Matches Scoring Rule Modification

For a particular Scenario, you can modify the prior matches scoring rule for the same Scenario criteria that you select in the Same Scenario drop-down list (Figure 35).
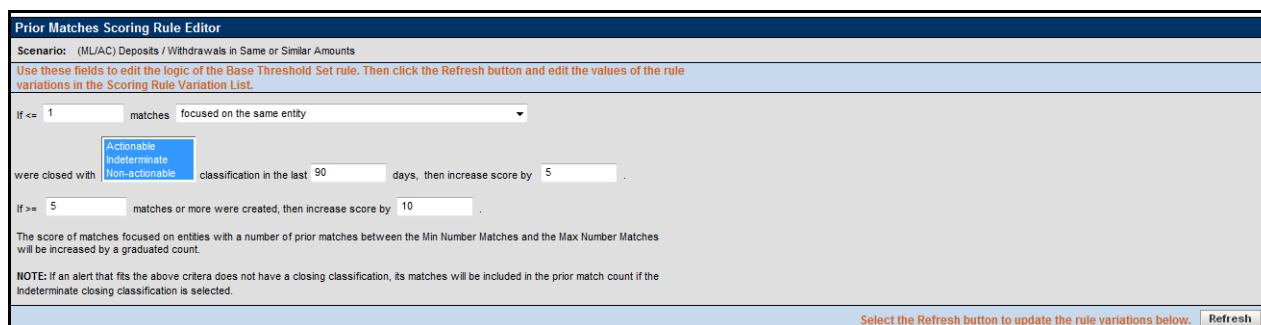

Figure 35. Prior Matches Scoring Rule Modification

When you enter values in the Rule Editor fields (**Min Number Matches**, **Same Scenario**, **Alert Closing Classification**, **Look Back Days**, **Min Score**, **Max Number Matches**, and **Max Score**) and click **Save**, the Prior Matches Scoring Rule Variation List displays (Figure 36).

Threshold Set	Min Number Matches	Min Score	Max Number Matches	Max Score	Look Back	Within	Closing Classification	Inherit
BASE THRESHOLD SET	1	5	5	10	90	All		
Cash-Credit	1	5	5	10	90	All		☑
Cash-Debit	1	5	5	10	90	All		☑
EFT-Credit	1	5	5	10	90	All		☑
EFT-Debit	1	5	5	10	90	All		☑
MI-Credit	1	5	5	10	90	All		☑
MI-Debit	1	5	5	10	90	All		☑
ML-DepWDSameAmts_TestTshldset_1	1	5	5	10	90	All		☑

Figure 36. Prior Matches Scoring Rule Variation List by Scenario

For each rule variation for a Threshold Set, you can perform the following:

- Enter new values.

- View a history of changes to a rule.

- Enter comments that describe the value of, or changes to, a rule.

Scoring Rule Variation List, on page 70 and *Prior Matches Scoring Rule Editor,* on page 78 provides description of most components in the Scoring Rule Variation List. The Prior Match Scoring Rule Editor also contains the following buttons:

- **And:** Allows you to add new filters for a rule. If at any time you want to remove a filter already associated to a rule, click the Remove button available for each of the filter rows.

- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which the Inherit check box is selected).

- **Save**: Saves your changes to the rules and displays the previous screen.

- **Revert**: Exits the area without saving any changes and displays the previous screen.

Simple Scenario Scoring Rule Editor

The Simple Scenario Scoring Rule Editor displays after clicking **Add** or **Update** in the Simple Scenario Scoring Rule List (Figure 37) when you filter by scenario. The Simple Scenario Scoring Rule Editor allows you to create and edit a rule that increments the score of matches that a specific scenario generates.

Note: Users cannot create Simple Scenario scoring rules for Scenario Classes. However, users can modify and delete existing scenario scoring rules from within the Simple Scenario Scoring Rules List when viewing scoring rules for a Scenario Class.
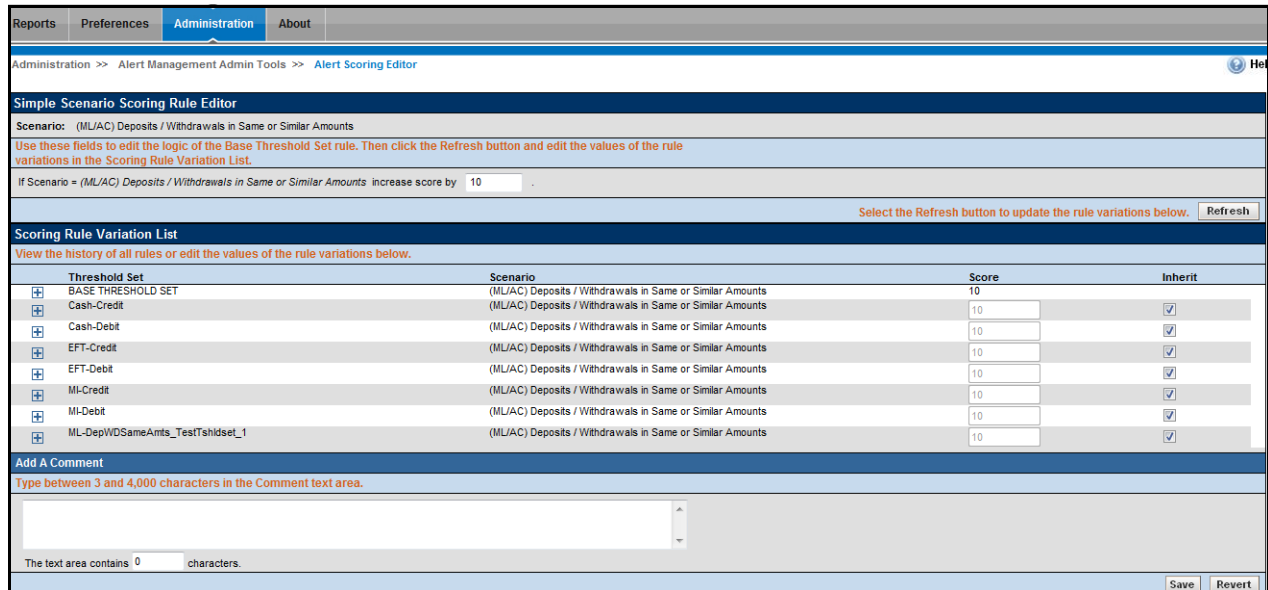
Figure 37. Simple Scenario Scoring Rule Editor

The following sections describe the components of the Simple Scenario Scoring Rule Editor, and the components in the Rule Editor when you modify a rule:

- Simple Scenario Scoring Rule Editor Components (refer to *Graduated Value Scoring Rule Editor Components,* on page 76 for more information).

- Simple Scenario Scoring Rule Modification (refer to *Graduated Value Scoring Rule Modification,* on page 77 for more information).

Simple Scenario Scoring Rule Editor Components

The Simple Scenario Scoring Rule Editor includes the following components:

- **Scenario** label: Displays (but is not editable) the name of the Scenario for which you are creating a scoring rule.

- **Score** text box: Assign the score to all matches that the selected Scenario generates.

  - If you select **Add**, the **Score** text box displays the text *Score.*

  - If you select **Update**, the **Score** text box displays the current score entry for the selected rule.

  - Accepts a numeric value greater or equal to zero (0) and less than or equal to the Maximum Match Score.

Simple Scenario Scoring Rule Modification

Figure 38. Simple Scenario Scoring Rule Variation List by Scenario

For each rule variation for a Threshold Set, you can perform the following:

- Enter new values.

- View a history of changes to a rule.

- Enter comments that describe the value of, or changes to, a rule.

Scoring Rule Variation List, on page 70 and *Simple Scenario Scoring Rule Editor,* on page 81, provides description of most components in the Scoring Rule Variation List. The Simple Scenario Scoring Rule Editor also contains the following buttons:

- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which the Inherit check box is selected).

- **Save**: Saves your changes to the rules and displays the previous screen.

- **Revert**: Exits the area without saving any changes and displays the previous screen.

Scoring Rule Set List

The Scoring Rule Set List displays below the Simple Scenario Scoring Rule List after you select a Scenario and click **Do It**. Within the Scoring Rule Set List, each match scoring strategy displays for the selected Scenario (Figure 39)

Figure 39. Scoring Rule Set List

The following sections describe the components of the Scoring Rule Set List, and the components in the Rule Editor when you modify a rule:

- Simple Scenario Scoring Rule Editor Components (refer to *Graduated Value Scoring Rule Editor Components,* on page 76 for more information).

- Simple Scenario Scoring Rule Modification (refer to *Graduated Value Scoring Rule Modification,* on page 77 for more information).

Scoring Rule Set List Editor Components

Figure 40. Scoring Rule Set List Editor

The Scoring Rule Set List Editor includes the following components:

- **Scenario** label: Displays (not editable) the name of the Scenario when you select this editor to create a scoring rule for a Scenario.

- Rule Name textbox: Displays the name of the rule.

- **Scoring Tier** textbox: Displays the scoring tier which should be the same number as for the match attribute selected.

- **Match Attribute** drop-down list: Contains a value for each binding description associated within each pattern and a matched record within the selected Scenario Class (if you are updating a rule for a Scenario Class), or a value for each binding description and matched record (displays in table.column format) associated with patterns within the selected Scenario (if you are adding or updating a rule for a single Scenario). The values display in ascending alphabetic order.

  - If you select **Add**, the first option in the Match Attribute drop-down list displays as the sample value.

  - If you select **Update**, the current match attribute for the selected rule displays in the Match Attribute drop-down list field.

- **Match Record Strategy** drop-down list: Displays Min, Max and Sum. This is enabled only if you choose a matched record from the Match Attribute drop-down list. The value of the match record strategy is displayed in Parenthesis beside the matched record after selection of the value. This is mandatory to be selected for any matched record being selected in the Match Attribute drop-down list.

- **Value** text box: Displays a value as an enumerated figure or range to associate to the selected value in the Match Attribute drop-down list.

  - If you select **Add**, the **Value** text box displays the text *Value*.

  - If you select **Update**, the **Value** text box displays the current value entry for the selected rule.

- **Minimum** text box: Must contain the minimum number of matches that meet the Same Scenario criteria for the rule to apply.

  - Minimum value must be a numeric value greater or equal to zero (0) and less than or equal to the maximum value.

- **Maximum** text box: Must contain the maximum number of matches that meet the Same Scenario criteria for the rule to apply.

  - Maximum must be a numeric value greater or equal to the minimum.

- **Next Scoring Tier** text box: Displays the scoring tier number looking at the Rule Set Scoring Tier list.

- **Score** text box: Displays a value assigned to matches that meet all rule criteria.

  - If you select **Add**, the **Score** text box displays the text *Score*.

  - If you select **Update**, the **Score** text box displays the current score entry for the selected rule.

  - The score can be any numeric value, less than, greater than, or equal to zero (0) and less than or equal to the application's Maximum Match Score.

For example, you can create range-based scoring rules using negative values in the **Score** field: To get 10 points for a value between 100 and 500, use:

Rule 1: If the value is greater than or equal to 100, then add 10 points to the **Score** field.

Rule 2: If the value is greater than 500, then add negative 10 (-10) points to the **Score** field.

To reduce the score when high amounts are involved, use:

Rule 1: If the value is greater than 10,000,000, then add negative 50 (-50) to the **Score** field.

You can also combine this with the Graduated Lookups to get a *below minimum* that adds nothing to the alert, but you do not have to start the range at zero (0).
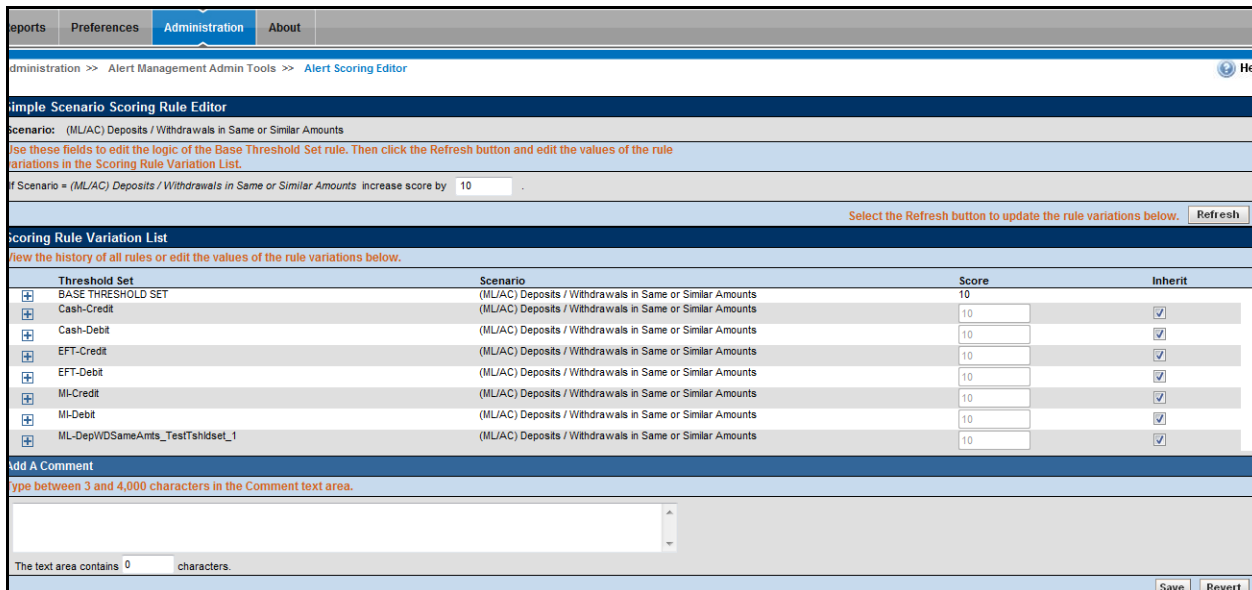
Scoring Rule Set List Modification

Figure 41. Scoring Rule Set List Variation List by Scenario

For each rule variation for a Threshold Set, you can perform the following:

- Enter new values.

- View a history of changes to a rule.

- Enter comments that describe the value of, or changes to, a rule.

Scoring Rule Variation List, on page 70 and *Scoring Rule Set List,* on page 84, provides description of most components in the Scoring Rule Variation List. The Simple Scenario Scoring Rule Editor also contains the following buttons:

- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which the Inherit check box is selected).

- **Save**: Saves your changes to the rules and displays the previous screen.

- **Revert**: Exits the area without saving any changes and displays the previous screen.

Using the Alert Scoring Editor

The Alert Scoring Editor enables you to view and modify the logic that the system uses to determine the score for matches and alerts.

Access the match scoring rules by using the search bar in the Alert Scoring Rule Editor. When the rules display, you can use the following Scoring Rule Editors to add, modify, and delete scoring rules:

- Simple Lookup Scoring Rule Editor

- Graduated Value Scoring Rule Editor

- Prior Matches Scoring Rule Editor

- Simple Scenario Scoring Rule Editor

- Scoring Rule Set

Using the Alert Scoring Strategy Selector, you can also view and change the alert scoring strategy for your deployment.

This section explains the following functions of the Alert Scoring Editor:

- Displaying the Match Scoring Rules for a Scenario Class or Scenario

- Using the Scoring Editors

- Changing the Alert Scoring Logic

Displaying the Match Scoring Rules for a Scenario Class or Scenario

To display the match scoring rules for a particular Scenario Class or Scenario, follow these steps:

1. In the Alert Scoring Editor search bar, select either a **Scenario Class** in the Scenario Class drop-down list or a single **Scenario** in the Scenario drop-down list.

2. Click **Do It**.

   The system displays all match scoring rules for the selected Scenario Class or Scenario.

   If the Scenario Class or Scenario does not have match scoring rules, the system displays the following message: *No scoring rules of this type currently exist for the selected scenario or scenario class.*

Using the Scoring Editors

This section lists the types of scoring editors and how to use the various scoring editors for scenario and scenario class.

- Simple Lookup Scoring Editor:

  - Using the Simple Lookup Scoring Editor for a Scenario Class

  - Using the Simple Lookup Scoring Editor for a Scenario

- Graduated Value Scoring Editor:

  - Using the Graduated Value Scoring Editor for a Scenario Class

  - Using the Graduated Value Scoring Editor for a Scenario

- Prior Matches Scoring Editor:

  - Using the Prior Matches Scoring Editor for a Scenario Class

  - Using the Prior Matches Scoring Editor for a Scenario

- Simple Scenario Scoring Editor:

  - Using the Simple Scenario Scoring Editor for a Scenario Class

  - Using the Simple Scenario Scoring Editor for a Scenario

- Scoring Rule Set Editor

  - Using the Scoring Rule Set Editor for a Scenario

This section also describes procedures that apply to all Alert Scoring Editors:

● Changing the Alert Scoring Logic

● Specifying a Variation for a Threshold Set Within a Scenario

● Deleting a Scoring Rule for a Scenario Class or Scenario

Using the Simple Lookup Scoring Editor for a Scenario Class

In the Simple Lookup Scoring Editor, you can modify or delete a rule for a Scenario Class. Use either of the following procedures:

● Modifying a Simple Lookup Scoring Rule for a Scenario Class

● Deleting a Scoring Rule for a Scenario Class or Scenario

Modifying a Simple Lookup Scoring Rule for a Scenario Class

To modify an existing Simple Lookup scoring rule for a Scenario Class, follow these steps:

1. In the Simple Lookup Scoring Rules List, click **Update Rule** next to the selected rule.

   The Simple Lookup Scoring Rule Editor displays with the rule's current values in the text boxes.

2. Do one or more of the following:

   ● Modify the binding description or matched record in the Match Attribute drop-down list.

   ● Modify the Match Record Strategy, if required.

   ● Modify the operator in the Operator drop-down list.

   ● Modify the value in the **Value** text box.

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

   ● Modify the value in the **Score** text box.

   ● Click the **And** button if you wish to add multiple filters for a rule.

3. Click **Refresh**.

   The system updates the rule and redisplays the Simple Lookup Alert Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

   ● Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

   ● Click the orange **-** icon to close the history window.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

   If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

Using the Simple Lookup Scoring Editor for a Scenario

In the Simple Lookup Scoring Editor, you can modify or delete a rule for an individual Scenario as you would for a Scenario Class (refer to *Using the Simple Lookup Scoring Editor for a Scenario Class,* on page 88 for more information). You can also add a new rule. Doing so establishes the conditions of the match scoring in a Scenario.

Within a Threshold Set for a Scenario, you can establish a rule variation. that is independent of the associated rule(s) for a Base Threshold Set.

Procedures in the following sections apply to rules for a Scenario:

- Adding a Simple Lookup Scoring Rule for a Scenario

- Modifying a Simple Lookup Scoring Rule for a Scenario

- Deleting a Scoring Rule for a Scenario Class or Scenario

- Specifying a Variation for a Threshold Set Within a Scenario

Adding a Simple Lookup Scoring Rule for a Scenario

To add a new Simple Lookup scoring rule for a Scenario, follow these steps:

1. In the Simple Lookup Scoring Rule List, click **Add**.

   The Simple Lookup Scoring Rule Editor displays.

2. Select a binding description or matched record in the Match Attribute drop-down list.

3. Modify the Match Record Strategy, if required.

4. Type a value in the **Value** text box.

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

5. Click the **And** button if you wish to add multiple filters for a rule.

6. Type a value in the **Score** text box.

7. Click **Save** to save your changes.

   The system creates the rule and redisplays it in the Alert Scoring Editor and Scoring Rule Variation List.

Note: If you select a Match Binding, Operator, and Value combination that exists in an existing rule for the same Scenario, the system displays an error dialog box. Click **OK** to modify any values.

Modifying a Simple Lookup Scoring Rule for a Scenario

To modify an existing Simple Lookup scoring rule for a Scenario, follow these steps:

1. In the Simple Lookup Scoring Rules List, click **Update Rule** next to the selected rule.

   The Simple Lookup Scoring Editor displays with the rule's current values in the text boxes.

2. Modify the binding description in the Match Attribute drop-down list.

3. Click **Refresh**.

   The system updates the rule and redisplays the Simple Lookup Alert Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

   a. Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

   b. Click the orange **-** icon to close the history window.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

   If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

5. To modify a rule for a particular Threshold Set in the Scoring Rule Variation List, refer to *Specifying a Variation for a Threshold Set Within a Scenario,* on page 97.

6. Click **Save** to save your changes.

   The system updates the rule values in the Simple Lookup Alert Scoring Editor and the Scoring Rule Variation List. The system then displays the previous screen.

Using the Graduated Value Scoring Editor for a Scenario Class

In the Graduated Value Scoring Editor, you can modify or delete a rule for a Scenario Class. Use either of the following procedures:

● Modifying a Graduated Value Scoring Rule for a Scenario Class

● Deleting a Scoring Rule for a Scenario Class or Scenario

Modifying a Graduated Value Scoring Rule for a Scenario Class

To modify an existing Graduated Value scoring rule for a Scenario Class, follow these steps:

1. In the Graduated Value Scoring Rules List, click **Update Rule** next to the selected rule.

   The Graduated Value Scoring Editor displays with the rule's current values in the text boxes.

2. Do one or more of the following:

   ● Modify the binding description in the Match Attribute drop-down list.

- Modify the numeric values in the **Min Value, Max Value, Min Score, and Max Score** text boxes.

- Click the **And** button if you wish to add multiple filters for a rule.

3. Click **Refresh**.

   The system updates the rule and redisplays the Graduated Value Alert Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

   a. Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

   b. Click the orange **-** icon to close the history window.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

   If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

   The system updates the values and displays the modified rule in the Graduated Value Alert Scoring Editor and Scoring Rule Variation List. The system then displays the previous screen.

Using the Graduated Value Scoring Editor for a Scenario

In the Graduated Value Scoring Editor, you can modify or delete a rule for an individual Scenario as you would for a Scenario Class (refer to *Using the Graduated Value Scoring Editor for a Scenario Class,* on page 90 for more information). You can also add a new rule. Doing so establishes the conditions of the match scoring in a Scenario.

Within a Threshold Set for a Scenario, you can establish an independent rule variation for a Threshold Set that does not inherit attributes of the rule for a Base Threshold Set.

Procedures in the following sections apply to rules for a Scenario:

- Adding a Graduated Value Scoring Rule for a Scenario

- Modifying a Graduated Value Scoring Rule for a Scenario

- Deleting a Scoring Rule for a Scenario Class or Scenario

Adding a Graduated Value Scoring Rule for a Scenario
To add a new Graduated Value scoring rule for a Scenario, follow these steps:

1. In the Graduated Value Scoring Rules List, click **Add**.

   The Graduated Value Scoring Rule Editor displays.

2. Select the desired binding description in the Match Attribute drop-down list.

3. Type numeric values in the **Min Value**, **Max Value**, **Min Score**, and **Max Score** text boxes.

4. Click the **And** button if you wish to add multiple filters for a rule.

5. Click **Save** to save your changes.

   The system creates the rule and redisplays the rule's attributes in the Graduated Value Scoring Editor and the Scoring Rule Variation List.

   Refer to *Specifying a Variation for a Threshold Set Within a Scenario,* on page 97 for information about using the Scoring Rule Variation List.

Note: If you select an attribute equal to the attribute of the selected Scenario, the system displays an error dialog box. Click **OK** to modify the values.

Modifying a Graduated Value Scoring Rule for a Scenario

To modify an existing Graduated Value scoring rule for a Scenario, follow these steps:

1. Modify the scoring rule by using the procedure for a Scenario Class (refer to *Modifying a Graduated Value Scoring Rule for a Scenario Class,* on page 90 for more information).

2. Modify a rule for a particular Threshold Set in the Scoring Rule Variation List by using the defined procedure. Refer to *Specifying a Variation for a Threshold Set Within a Scenario,* on page 97 for information about using the Scoring Rule Variation List.

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

   The system updates the rule values in the Graduated Value Scoring Editor and the Scoring Rule Variation List. The system then displays the previous screen.

Using the Prior Matches Scoring Editor for a Scenario Class

In the Prior Matches Scoring Editor, you can modify or delete a rule for a Scenario Class. Use either of the following procedures:

- Modifying a Prior Matches Scoring Rule for a Scenario Class
- Deleting a Scoring Rule for a Scenario Class or Scenario

Modifying a Prior Matches Scoring Rule for a Scenario Class

To modify an existing Prior Matches scoring rule for a Scenario Class, follow these steps:

1. From the Prior Matches Scoring Rules List, click **Update Rule** next to the selected rule.

   The rule attributes display in the Prior Matches Scoring Editor.

2. Do one or more of the following:

   - Modify the numeric value in the **Min Number Matches** text box.
   - Modify the value in the Same Scenario drop-down list.
   - Modify the numeric value in the Look Back Days, Min Score, Max Number Matches, and **Max Score** text boxes.

3. Click **Refresh**.

   The system updates the rule and redisplays the Prior Matches Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

a. Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

b. Click the orange **-** icon to close the history window.

Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

The system updates the values and displays the modified rule in the Prior Matches Scoring Editor and Scoring Rule Variation List. The system then displays the previous screen.

Using the Prior Matches Scoring Editor for a Scenario

In the Prior Matches Scoring Editor, you can modify or delete a rule for an individual Scenario as you would for a Scenario Class (refer to *Using the Prior Matches Scoring Editor for a Scenario Class,* on page 92 for more information). You can also add a new rule. Doing so establishes the conditions of the match scoring in a Scenario.

Within a Threshold Set for a Scenario, you can establish an independent rule variation for a Threshold that does not inherit attributes of the rule for a Base Threshold Set.

Procedures in the following sections apply to rules for a Scenario:

- Adding a Prior Matches Scoring Rule for a Scenario

- Modifying a Prior Matches Scoring Rule for a Scenario

- Deleting a Scoring Rule for a Scenario Class or Scenario

Adding a Prior Matches Scoring Rule for a Scenario

To add a new Prior Matches scoring rule for a Scenario, follow these steps:

1. In the Prior Matches Scoring Rules List, click **Add**.

   The Prior Matches Scoring Editor displays.

2. Type a numeric value in the **Min Number Matches** text box.

3. Select the desired attribute in the Same Scenario drop-down list.

4. Type a numeric value in the **Look Back Days**, **Min Score**, **Max Number Matches**, and **Max Score** text boxes.

5. Click **Save** to save your changes.

   The system creates the rule and redisplays the rule's attributes in the Prior Matches Scoring Editor and Scoring Rule Variation List.

Note: If you select a value in the Same Scenario drop-down list that is the same as an existing rule for the same scenario, the system displays an error dialog box. Click **OK** to modify values.

Modifying a Prior Matches Scoring Rule for a Scenario

To modify an existing Prior Matches scoring rule for a Scenario, follow these steps:

1. Modify the scoring rule by using the procedure for a Scenario Class (refer to the *Modifying a Prior Matches Scoring Rule for a Scenario Class,* on page 92, for more information).

2. Modify a rule for a particular Threshold Set in the Scoring Rule Variation List. Refer to *Specifying a Variation for a Threshold Set Within a Scenario,* on page 97 for more information about using the Scoring Rule Variation List.

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

   The system updates the rule values in the Prior Matches Scoring Editor and the Scoring Rule Variation List. The system then displays the previous screen.

Using the Simple Scenario Scoring Editor for a Scenario Class

In the Simple Scenario Scoring Editor, you can modify or delete a rule for a Scenario Class. Use either of the following procedures:

- Modifying a Simple Lookup Scoring Rule for a Scenario Class
- Deleting a Scoring Rule for a Scenario Class or Scenario

Modifying a Simple Scenario Scoring Rule for a Scenario Class

To modify an existing Simple Scenario scoring rule for a Scenario Class, follow these steps:

1. From the Simple Scenario Scoring Rules List for a single Scenario, click **Update Rule** for the desired rule.

   The Simple Scenario Scoring Editor displays with the associated rule highlighted in the display.

2. Modify the numeric value in the **Score** text box.

3. Click **Refresh**.

   The system updates the rule and redisplays the Simple Scenario Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

   a. Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

   b. Click the orange **-** icon to close the history window.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

5. The system updates the values and displays the modified rule in the Simple Scenario Scoring Editor and Scoring Rule Variation List. The system then displays the previous screen.

Using the Simple Scenario Scoring Editor for a Scenario

In the Simple Scenario Scoring Editor, you can modify or delete a rule for an individual Scenario as you would for a Scenario Class (refer to *Using the Simple Scenario Scoring Editor for a Scenario Class,* on page 94, for more information). You can also add a new rule. Doing so establishes the conditions of the match scoring in each Scenario.

Within a Threshold Set for a Scenario, you can establish an independent rule variation for a Threshold Set that does not inherit attributes of the rule for a Base Threshold Set.

Procedures in the following sections apply to rules for a Scenario:

- Adding a Simple Scenario Scoring Rule for a Scenario

- Modifying a Simple Scenario Scoring Rule for a Scenario

- Deleting a Scoring Rule for a Scenario Class or Scenario

Adding a Simple Scenario Scoring Rule for a Scenario
To add a new Simple Scenario scoring rule for a Scenario, follow these steps:

1. From the Simple Scenario Scoring Rules List for a single Scenario, click **Add**.

   The Simple Scenario Scoring Editor displays.

2. Type a numeric value in the **Score** text box.

3. Click **Save**.

   The system creates the rule and redisplays the rule's attributes in the Alert Scoring Editor and the Scoring Rule Variation List.

Modifying a Simple Scenario Scoring Rule for a Scenario
To modify an existing Simple Scenario scoring rule for a Scenario, follow these steps:

1. Modify the scoring rule by using the procedure for a Scenario Class (refer to *Modifying a Simple Scenario Scoring Rule for a Scenario Class,* on page 94, for more information).

2. Modify a rule for a particular Threshold Set in the Scoring Rule Variation List. Refer to *Specifying a Variation for a Threshold Set Within a Scenario,* on page 97 for information about using the Scoring Rule Variation List.

3. Click **Save**.

Using the Scoring Rule Set Editor for a Scenario

In the Scoring Rule Set Editor, you can modify or delete a rule set for an individual Scenario. Doing so establishes the conditions of the match scoring in each Scenario.

Procedures in the following sections apply to rules for a Scenario:

- Adding a Simple Scenario Scoring Rule for a Scenario

● Modifying a Simple Scenario Scoring Rule for a Scenario

● Deleting a Scoring Rule for a Scenario Class or Scenario

Adding a Scoring Rule Set for a Scenario

To add a new Scoring Rule Set for a Scenario, follow these steps:

1. From the Scoring Rule Set for a single Scenario, click **Add**.

   The Scoring Rule Set Editor displays.

2. Type a numeric value in the **Score** text box.

3. Click **Save**.

   The system creates the rule and redisplays the rule's attributes in the Alert Scoring Editor and the Scoring Rule Variation List.

Modifying a Scoring Rule Set for a Scenario

To modify an existing Scoring Rule Set for a Scenario, follow these steps:

1. From the Scoring Rule Set List, click **Update Rule** next to the selected rule.

   The rule attributes display in the Prior Matches Scoring Editor.

2. Do one or more of the following:

   ● Modify the value in the **Scoring Tier** text box.

   ● Modify the value in the **Match Attribute** drop-down list.

   ● Modify the value in the **Match Record Strategy** drop-down list.

   ● Modify the numeric value in the **Value, Minimum, Maximum, Next Scoring Tier** and **Score** text boxes.

3. Click **Refresh**.

   The system updates the rule and redisplays the Prior Matches Scoring Editor with the changes. The updated rule logic also displays in the Scoring Rule Variation List.

   Optional: In the Scoring Rule Variation List:

   a. Click the blue **+** icon next to a rule to open a scrollable window that contains a history of changes to the rule (including modification date, user who modified a rule variation, rule attributes, and comments about the update).

   b. Click the orange **-** icon to close the history window.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

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

   If you did not previously click **Refresh** to save your updates to the rule logic, a dialog box displays and prompts you to click **Refresh** before clicking **Save**.

   The system updates the values and displays the modified rule set in the Scoring Rule Set Editor and Scoring Rule Variation List. The system then displays the previous screen.

Changing the Alert Scoring Logic

To change the alert scoring logic, follow these steps:

1. From the Alert Scoring Editor, click **Change Strategy**.

   The Alert Scoring Strategy Selector dialog box displays.

2. Select the desired **Alert Scoring Strategy** option button.

3. Click **Save**.

   A Confirmation dialog box displays.

4. Click **OK** to close the dialog box and continue.

   The system updates the alert scoring strategy with the selected value. It redisplays the Alert Scoring Editor with only the search bar and updated Alert Scoring Strategy Selector window.

Specifying a Variation for a Threshold Set Within a Scenario

You can specify a rule variation for a Threshold Set that is independent of the rule for the Base Threshold Set. Use the following procedure.

Specifying a Variation for a Threshold Set within a Scenario

To specify a variation for a Threshold Set within a Scenario, follow these steps:

1. In the Scoring Rule Variation List, deselect the Inherit check box next to the rule that you want to modify. (A selected check box next to a rule implies that the system associates it with the rule for the Base Threshold Set.)

2. Do either of the following:

   ● Leave the values in the modifiable text boxes unchanged.

   ● Modify an entry in any modifiable text box.

   Optional: Type a comment about a rule logic update in the **Add a Comment** text box. Enter from 3 to 4,000 characters.

   A count in the numeric field below the Add a Comment field tracks the number of characters you have entered in the comment area.

3. Click **Save**.

Deleting a Scoring Rule for a Scenario Class or Scenario

Deleting a scoring rule eliminates the rule and any related variations for Threshold Sets. You can delete a rule that applies to a Scenario Class or Scenario. Use the following procedure.

Deleting a Scoring Rule for a Scenario Class or Scenario

To delete an existing scoring rule for a Scenario Class or Scenario, follow these steps:

1. From the desired match scoring rule list, click **Delete** adjacent to the selected rule.

   The Confirmation dialog box displays the following message:

Deleting this rule will also delete any variations for Threshold Sets within this Scenario. Are you sure you want to delete the selected rule?

2. Click **OK** to close the dialog box and continue.

The system redisplays the Alert Scoring Editor without the rule.

CHAPTER 7 — *Alert Assigner Editor*

This chapter describes how you can assign ownership of alerts:

- About the Alert Assigner Editor

- Alert Assigner Screen Elements

- Using the Alert Assigner Editor

About the Alert Assigner Editor

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

- Select a focus and then create, modify, or delete a rule

- Change the Default Owner

- Define Role-Based Assignment Limits

Each alert generated within the application is assigned an initial owner before it is available for analysis. The application automatically determines an appropriate owner (a user or group of users) for each alert based on the initial assignment logic you configured or configured for your firm. Initial assignment logic is composed in a set of operations that evaluate various attributes of the alert or its focal entity. For example, scenario, score, focal entity, or related entities.

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

- Each assignment rule is defined as an attribute (either an attribute of an alert, or an attribute of the focal entity), an operator, and a value.

Table 13 shows a sample of an alert assignment rule.

Table 13. Sample of an Alert Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
1	Focus	- Alerts with focus domain code **c** only are assigned to the Brokerage pool. - Alerts with focus domain code **d**, **e**, or **de** are assigned to the Banking pool.

Table 13. Sample of an Alert Assignment Rule

Precedence	Assignment Rule Type	Assignment Rule
2	Focus and Scenario	● Alerts with focus domain code **d**, **e**, or **de** and generated by scenario High Risk Transactions – High Risk Counter Party (AC) to the Wires pool. ● Alerts with focus domain code **d**, **e**, or **de** and generated by scenario Single or Multiple Cash Transaction – Possible CTR (CU) to the Structuring pool. ● Alerts with focus domain code **d**, **e**, or **de** and generated by scenario Networks of Accounts, Entities (AC) or Rapid Movement of Funds – All Activity (CU) to the General pool.
3	Default	● All alerts that do not meet other rules are assigned to the AML Risk Management pool.

- Each assignment rule consists of an operation set that identifies a grouping of rules of which it is a member.

- Operations are logical expressions that can be used to evaluate alerts (for example, alert score > 50). A set of operations based on the same attribute (for example, score) are grouped into an operation set.

- All operations within an operation set must be mutually exclusive and should collectively cover the entire spectrum of values for a given attribute.

- Each operation specifies the next step that is applied to alerts that satisfy the operation. This next step is either an owner for the alert, or the next operation set, or branch, to further evaluate the alerts.

- Each alert is evaluated against the operations within operation set one (1). Each alert then branches out based upon the next operation set specified for the operation within Operation Set one (1) that they satisfy. Each alert continues through a chain of operation sets until it satisfies an operation for which an owner has been specified. Alerts that do not reach an operation that they satisfy and for which an owner has been specified, will be assigned to the Default Owner.

Note: Manually posted alerts, generated by the alert correlation process, are not assigned to the default owner that is specified through the assignment editor (see Figure 46). Refer to the *Administration Guide,* for more information.

Accessing the Alert Assigner Editor

Navigate to the Alert Assigner Editor by selecting **Alert Management Configuration** in the Administration menu, then selecting the **Alert Assigner Editor** option.
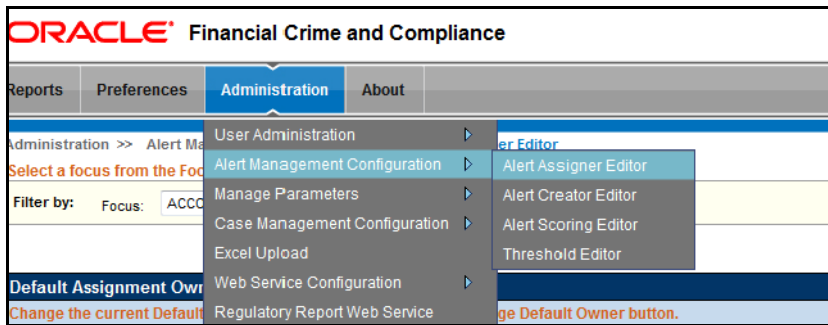
Figure 42. Alert Assigner Editor Navigation

Alert Assigner Screen Elements

The following pages are associated with the Alert Assigner Editor:

- **Alert Assigner Editor:** This is the first page displayed when accessing the Alert Assigner Editor Administration Tool. You can navigate to the Assignment Rule Editor to add a new rule or delete or modify an existing rule. Additionally, you can change the Default Owner for unassigned alerts. Refer to *Alert Assigner Editor,* on page 102 for more information.

- **Assignment Rule List for <Focus> Focus:** This page enables you to create a new rule or modify an existing rule. Refer to *Assignment Rule List for <Focus> Focus,* on page 103 for more information.

- **Assignment Rule Editor:** This page allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. Refer to *Assignment Rule Editor,* on page 104 for more information.

Alert Assigner Editor

In the Alert Assigner Editor, you must select a focus to view all of the assignment rules associated to that focus.
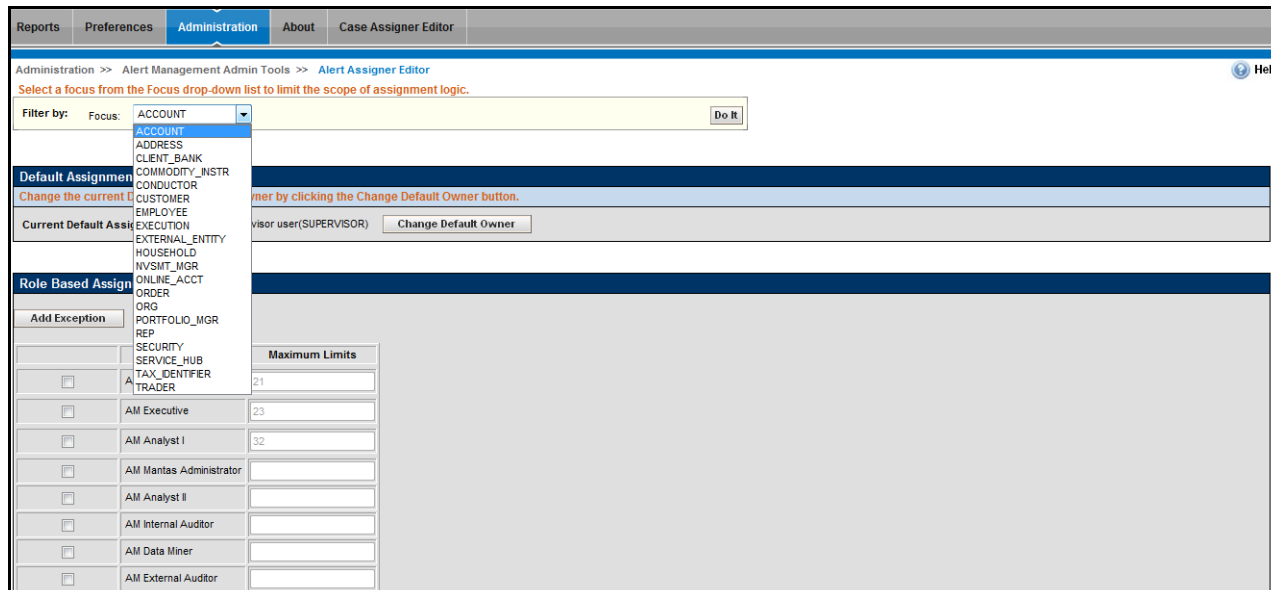
Figure 43. Alert Assigner Editor

The components of the Alert Assigner Editor include the following:

- Search Bar

- Default Assignment Owner Selector

- Assignment Rule List for <Focus> Focus

- Role Based Assignment Limits Editor

Search Bar

The search bar allows you to filter the list of assignment rules by the focus (Figure 44).
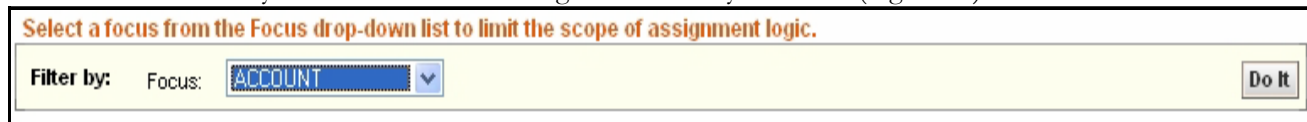
Figure 44. Alert Assigner Editor search Bar

The components of the search bar include the following:

- **Filter by:** Focus drop-down list: Provides a list of focus types. The values in the Focus drop-down list are sorted in ascending alphabetic order.

- **Do It button**: When clicked, displays the assignment rules associated with the selected focus.

Default Assignment Owner Selector

The Default Assignment Owner Selector page allows you to change the default owner for alerts (Figure 45).

Note: Ensure that the new default owner has permission to view *all* alerts.

Figure 45. Default Assignment Owner Selector

The following screen elements appear in the Default Assignment Owner Selector after you click the **Change Default Owner button** from the Alert Assigner Editor page:

- **Current Default Assignment Owner**: Displays the name of the current owner.

Note: To change the default assignment owner, refer to *Changing the Default Assignment Owner,* on page 107.

- **New Default Assignment Owner** drop-down list: Provides a list of owner IDs available to be the Default Owner.

- **Save button**: Saves all modifications to the database.

- **Cancel button**: Redisplays the Assignment Editor without the Assignment Rules list. The New Default Owner value is not saved.

Assignment Rule List for <Focus> Focus

The assignment rule list displays in the Alert Assigner Editor after you select a focus in the search bar and click **Do It**. The rules in the list are sorted in ascending order by operation set number (Figure 46).

Figure 46. Assignment Rule List for <Focus> Focus

The Assignment Rule List for <Focus> Focus includes the following components:

- **Add button**: Navigates you to the Assignment Rule Editor.

- **Update button**: Navigates you to the Assignment Rule Editor.

- **Delete button**: Deletes the assignment rule.

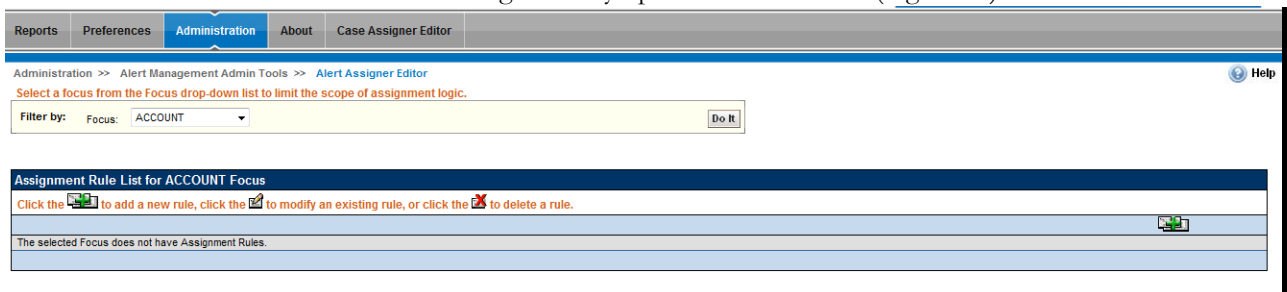- **Assignment Rule List for <Focus> Focus** page displays the column headings: Operation Set, Attribute, Operator, Value, Next Operation Set, Strategy, and Owner. Refer to *Assignment Rule Editor,* on page 104 for more information.

Role Based Assignment Limits Editor

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

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

Figure 47. Role Based Assignment Limits Editor

The Role Based Assignment Limits Editor includes the following components:

- **User Role grid**: When a user role is selected, you can edit the maximum limit. A *Null* value indicates there is no limit for the assignment of alerts.

- **Add Exception button**: Allows you to enter exceptions to the limit assigned to the user role. For example, to set a new limit for a specific user in a role. Refer to *Adding an Exception to a Role Based Assignment Limit,* on page 110 for more information.

- **Save button**: Saves all modifications to the database.

- **Cancel button**: Redisplays the Assignment Editor. The New Maximum Limits value is not saved.

Assignment Rule Editor

The Assignment Rule Editor displays after you click **Add** or **Update** (Figure 48). This editor allows you to create or edit a series of rules, or operations, that are chained together to form a decision tree. A decision tree is created for each focus type. The decision trees are used to determine the owner (an individual or group of users) of each alert generated by the system.

Figure 48. Assignment Rule Editor

The components of the Assignment Rule Editor include the following:

- **Focus** label: Displays (but is not editable) the name of the selected focus.

- **Operation Set** text box: Specifies a grouping of mutually exclusive rules based on an attribute.

    - If you select **Add**, the **Operation Set** text box displays as blank.

    - If you select **Update**, the **Operation Set** text box field is populated with the current data for the selected rule.

    - You must create rules within Operation Set 1 before creating any additional rules. Any condition not covered by Operation Set 1 is assigned to the default assignment owner, as are all other operation sets when alerts are added to them.

- **Investigation Attribute** drop-down list: Populates alphabetically with values for each attribute of the alert. For example, scenario class, scenario, pattern ID, score, match count, and scenario count, of which to base the rule.

    - If you select **Add**, the **Investigation Attribute** drop-down list displays a blank value (" ") (the default).

    - If you select **Update**, the **Investigation Attribute** drop-down list displays the current value of the selected rule, if the rule is based on an investigation attribute, rather than a business attribute.

    - If you base your rule on an investigation attribute, you cannot select a business attribute.

- **Business Attribute** drop-down list: Displays values for each attribute, excluding artificial keys (for example, sequence IDs), of the focus type, of which to base the rule.

    - If you select **Add**, the **Business Attribute** drop-down list displays a blank value (" ") (the default).

    - If you select **Update**, the **Business Attribute** drop-down list displays the current value of the selected rule, if the rule is based on an business attribute, rather than an investigation attribute.

    - If you base your rule on an business attribute, you cannot select an investigation attribute.

- **Operator** drop-down list: Contains the following values =, !=, >, <, <=, >=, in, contains, blanks (" "), and else.

  - If you select **Add**, the **Operator** drop-down list displays a blank value (" ") (the default).

  - If you select **Update**, the **Operator** drop-down list displays the current value of the selected rule.

  - If you base your rule on an investigation attribute or business attribute for which an enumerated list of values has been defined, only the values = and != are available in the **Operator** drop-down list.

  - If you have a list of values and you want to check if the database field is one of the values in the list, select the *in* operator in the **Operator** drop-down list.

  - If you want to check a database field that contains a comma-delimited list of values for a specific value, select the **contains** operator in the **Operator** drop-down list.

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

  - If you select the *else* operator, the *value* must be NULL; followed by a subsequent operation or alert owner recipient specification.

Note: The system evaluates the *else* operation after evaluating all other operations.

- **Value** text box or drop-down: Within the rule, the value of the investigation or business attribute is compared to the **Value** field. If you have selected an attribute in the **Investigation Attribute** drop-down list with defined values (Jurisdiction, Domain, Pattern ID, Scenario Name, and Scenario Class Name), the **Value** drop-down list will contains those values. The **Value** field displays as a text box for all other attributes (for example, score or account balance).

  - If you select **Add** , the **Value** text box displays a blank value (" ").

  - If you select **Update**, the **Value** text box displays the current value of the selected rule.

  - If you enter multiple values in the **Value** text box after having selected *IN* as the operator, separate the values with pipe (|).

  - If you select the *else* operator, the **Value** must be NULL therefore, the system disables the Value text box or drop-down list.

- **Next Operation Set** text box: The number of the next operation set, or branch, to further evaluate the alert or assign to an owner.

  - If you select **Add**, the **Next Operation Set** text box displays a blank value (" ") (the default).

  - If you select **Update**, the **Next Operation Set** text box displays the current value of the selected rule.

  - If the result of your rule is to continue to the next operation set, you must not select an owner to assign the alert.

- **Owner** drop-down list: Displays available owners for both alerts.

- ■ If you select **Add**, the **Owner** drop-down list displays a blank value (" ") (the default).

- ■ If you select **Update**, the **Owner** drop-down list displays the current value of the selected rule.

- ■ If the result of your rule is to assign the alert, you must not select to continue to the next operation set.

- ● **Strategy** drop-down list (*Optional:*): Displays available strategies for the assignment rule. This drop-down list is disabled unless an owner is selected and that owner is a pool and not an individual user.

  - ■ If you select **Round Robin**, alerts are assigned to the members of a pool in a circular order until all the alerts have been assigned.

  - ■ If you select **Load Leveling**, the pool member's current load is taken into consideration when assigning alerts.

  - ■ If a strategy is selected and then an individual user is selected in the **Owner** drop-down list, then the value in the Strategy drop-down list is made blank.

Using the Alert Assigner Editor

This section explains the following functions of the Assignment Editor:

- ● Displaying Assignment Rules for a Focus
- ● Changing the Default Assignment Owner
- ● Adding a New Rule
- ● Modifying a Rule
- ● Deleting a Rule
- ● Adding a Role Based Assignment Limit
- ● Adding an Exception to a Role Based Assignment Limit

Displaying Assignment Rules for a Focus

To display the assignment rules for a particular focus from the search bar, follow these steps:

1. Select a focus from the **Focus** drop-down list.

2. Click **Do It**.

   The Administration Tool displays all Assignment Rules for the selected focus.

   If the focus type selected does not have Assignment Rules, Administration Tool displays the message: *The selected focus does not have assignment rules.*

Changing the Default Assignment Owner

To change the default owner from the Default Assignment Owner Selector, follow these steps:

1. Click **Change Default Owner**.

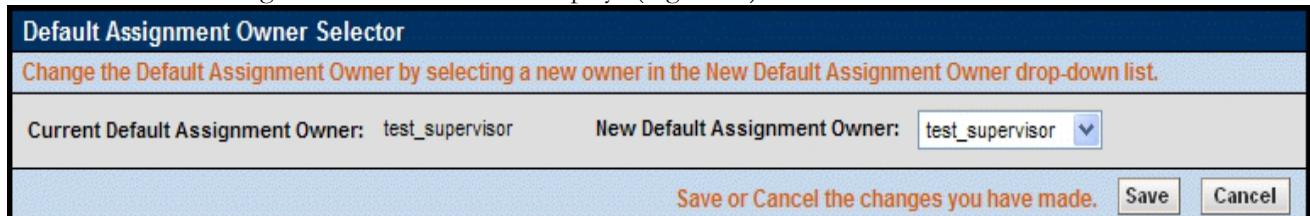The Default Assignment Owner Selector displays (Figure 49).

Figure 49. Default Assignment Owner Selector

2. Click the desired owner in the **New Default Assignment Owner** drop-down list.

   Note: Ensure the new default assignment owner has permission to view *all* alerts.

3. Click **Save**. The Administration Tool displays a Confirmation dialog box with the message: *Do you want to update the default alert owner?*

4. Click **OK**.

   The Administration Tool updates the default owner with the owner ID of the selected value and redisplays the Alert Assigner Editor with only the Focus sections and the updated Default Owner section.

Adding a New Rule

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

1. Click **Add**.

   The Assignment Rule Editor displays.

2. Type an operation set number in the **Operation Set** text box.

   You can add to an existing operation set based on the same attribute by entering the same number as the other rules in that set or you can start a new set by entering the next sequential number.

3. Select either an investigation attribute or a business attribute on which to base the rule in the **Investigation Attribute** or **Business Attribute** drop-down lists.

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

4. Select an operator in the **Operator** drop-down list. If you select the *else* operation, skip to Step #6 since no value is required for this operand.

5. Type a value in the **Value** text box.

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

6. Select either the next operation set to attach additional rules to this rule in the **Next Operation Set** text box, or select an owner to assign alerts to in the **Owner** drop-down list.

   Note: Ensure that the new owner has permission to view alerts with the attributes specified in the rule.

7. If you selected a pool in the **Owner** drop-down list, select a strategy for alert assignment from the **Strategy** drop-down list.

8. Click **Save**.

The system creates the new rule and redisplays the Alert Assigner Editor with the new rule.

To ensure that all alerts are appropriately assigned, rules within an operation set should cover the complete range of values for a given attribute. For example, in the following rules, the assignment logic does not cover alerts with score values between 50 and 60 and would thus assign alerts with scores in this range to the Default Owner.

- Operation Set 2, Attribute REVIEW.score, Operator <, Value 50, Owner JonesRJ.

- Operation Set 2, Attribute REVIEW.score, Operator >, Value 60, Owner SmithJB.

Modifying a Rule

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

1. Click **Update** for the desired rule.

   The Assignment Rule Editor displays.

2. Do one or more of the following:

   - Modify the operation set number in the **Operation Set** text box.

   - Modify the investigation attribute or a business attribute on which to base the rule from the **Investigation Attribute** or **Business Attribute** drop-down lists.

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

   - Modify the operator in the **Operator** drop-down list.

   - Modify the value in the **Value** text box.

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

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

- Modify the strategy selected to assign alerts to the pool in the **Strategy** drop-down list.

3. Click **Save**.

   The system updates the rule and redisplays the Alert Assigner Editor with the rule's updates.

Rules within an operation set should cover the complete range of values for a given attribute, to ensure that all alerts are appropriately assigned. For example, assume you specify the following rules:

- Operation Set 2, Attribute REVIEW.score, Operator <, Value 50, Owner JonesRJ.

- Operation Set 2, Attribute REVIEW.score, Operator >, Value 60, Owner SmithJB.

This assignment logic does not cover alerts with score values between 50 and 60 and would assign alerts with scores in this range to the Default Owner.

Deleting a Rule

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

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

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

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

   The system removes the rule and redisplays the Alert Assigner Editor.

Adding a Role Based Assignment Limit

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

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

2. Enter the Maximum Limit for this user role.

3. Click **Save**.

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

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

   The system sets the limit and redisplays the Alert Assigner Editor.

Adding an Exception to a Role Based Assignment Limit

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

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

2. Click **Add Exception**.

3. Select the user you want to add the exception for from the dropdown list.

4. Enter the Maximum Limit.

5. Click **Save**.

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

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

   The system sets the limit and redisplays the Alert Assigner Editor.

Modifying an Exception

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

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

2. Click **Add Exception**.

3. Select the user you want to modify the exception for from the drop-down list.

4. Click **Edit**.

5. Modify the limits.

6. Click **Save**.

    The system updates the rule and redisplays the Alert Assigner Editor with the rule's updates.

Deleting an Exception

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

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

2. Click **Add Exception**.

3. Select the user you want to modify the exception for from the drop-down list.

4. Click **Delete**.

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

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

    The system removes the exception and redisplays the Alert Assigner Editor.

Example of an Alert Assignment

Alert Assignment rules are created in the editor as a series of operation sets that are chained together to form a decision tree. The assignment algorithm will move through the decision tree in ascending order of the defined operation sets until all rules have been processed and alerts assigned.

Example 1

This example demonstrates how rules can be created using multiple operation sets to combine together to form a series of specific conditions to be met to control alert assignment.
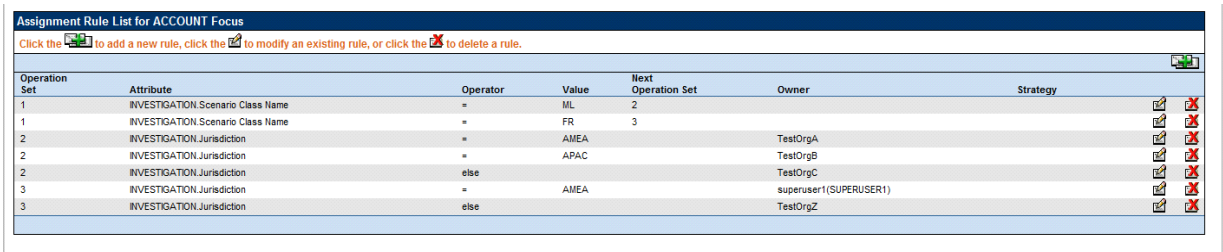

Figure 50. Example 1

The rules set up in this figure reflect the following logic and use of operations sets.

- Per Operation Set 1 all alerts that are created on Scenario Class FR will be routed to Pool TestOrgA.

- If the Scenario Class is not FR the algorithm will look to Next Operation Set 2.

- Per Operation Set 2 if the Jurisdiction of the alert is A then it should be routed to Pool TestOrgB with a Strategy of Round Robin.

- If the Jurisdiction of the alert is not A the algorithm will continue with the next rule that is part of Operation Set 2.

- If the Jurisdiction of the alert is B then it should be routed to Superuser2.

- If, at this point, the algorithm has determined that the alert is not of Scenario Class FR and is not in Jurisdiction A or B, then the algorithm will move to Next Operation Set 3.

- Per Operation Set 3 if the score of the alert is >= 50 then it should be routed to Superuser3.

- If none of the above rules are met the alert will be routed to the default owner defined for alert assignment.

Example 2

This example demonstrates how rules can be created using the Else operator. The goal of this set of rules is to have specific assignment for some alerts within a scenario class based on selected criteria while all other alerts within that class go to the same owner when that criteria is not met.

Figure 51. Example 2

The rules set up in this figure reflect the following logic and use of operations sets.

- Per Operation Set 1 check to see if the Scenario Class is ML. If so proceed to Next Operation Set 2.

- If Scenario Class is not ML but is FR then the algorithm will proceed to Next Operation Set 3.

- Per Operation Set 2, for ML class alerts the algorithm will check if the Jurisdiction matches AMEA. If it does alerts will be assigned to TestOrgA.

- If an ML class alert and the Jurisdiction is not AMEA the algorithm will check to see if the Jurisdiction is APAC. If it is alerts will be assigned to TestOrgB.

- Otherwise, if an ML class alert and the Jurisdiction is other than AMEA or APAC the alert will be assigned to TestOrgC.

- Per Operation Set 3, for FR class alerts the algorithm will check if the Jurisdiction matches AMEA. If it does alerts will be assigned to Superuser1.

- If a FR class alert and the Jurisdiction is other than AMEA the alert will be assigned to TestOrgZ.

- If none of the above rules are met the alert will be routed to the default owner defined for alert assignment.

CHAPTER 8   *Threshold Analyzer*

This chapter introduces you to the Threshold Analyzer utility and describes how you can view and operate the source business and Threshold Analyzer data. It also explains how the user interface is organized, how the application uses the data, and how to view reports as per your setting. This chapter focuses on the following topics:

- Introduction to the Threshold Analyzer
- Understanding the Graph Display

Introduction to the Threshold Analyzer

The Threshold Analyzer utility leverages decisions made by analysts on past alerts to help tune the scenarios and their thresholds going forward. The goal is to reduce the number of false positive alerts. Past alerts are analyzed and categorized to identify the quality of the alert. This utility helps to identify correlations between alert attributes and alert quality.

Oracle Financial Services application scenarios calculate *binding* values as part of behavior detection. Many of these can be used to *simulate* thresholds. The Threshold Analyzer allows users to plot the actual values of those bindings for alerts on a graph relative to the determined quality of those alerts. For example, analysis of the graph might reveal that when the binding value for the Total Transaction Amount associated with an alert was below a certain level, most alerts were considered to be non-productive or representing a false positive. This would suggest that raising thresholds based on the Total Transaction Amount for the selected scenario could eliminate some false positives.

The Threshold Analyzer utility is a component that utilizes Oracle Business Intelligence Enterprise Edition (OBIEE) software. This utility operates as a standalone utility meaning that, while it falls within the category of administrative tools, it is not actually accessible via the Oracle Financial Services Administration Tools user interface. The Threshold Analyzer is accessed via a separate URL. Contact your System Administrator for the exact Web address to be used.

Getting Started

Note: To access the Threshold Analyzer via Reports, OBIEE software must be installed and you need to have a valid user name and password.

To login, follow these steps:

1. Navigate to the Login page for the application alert administration or case administration application.
2. Enter your **User ID**.
3. Enter your **Password**.
4. Click **Log In,** in the application page.

Note: The language selected is reflected only in the product-related titles and messages. The reports are displayed in English.
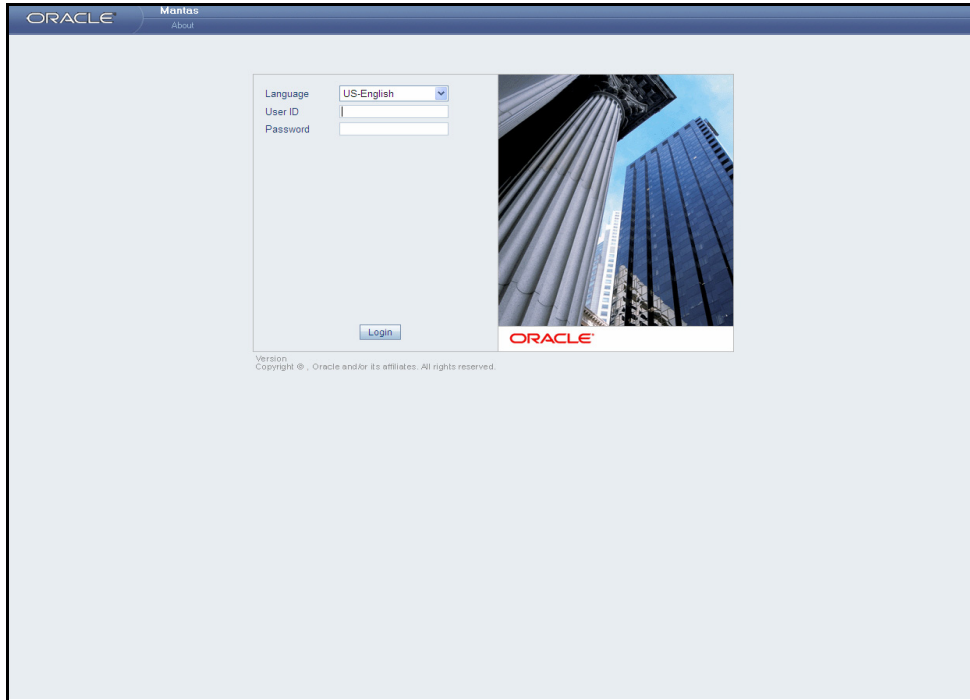
Figure 52. Application Login

Homepage

To navigate to the Threshold Analyzer application, select the Threshold Analyzer option from the Reports primary navigation menu. On successful login, the homepage is displayed with Reports menu option. On clicking the Reports option, the OBIEE Dashboard page is displayed (Figure 53).

When the User is an Administrator
Users with administrator or data miner roles will default to the Threshold Analyzer Report. (Figure 53).
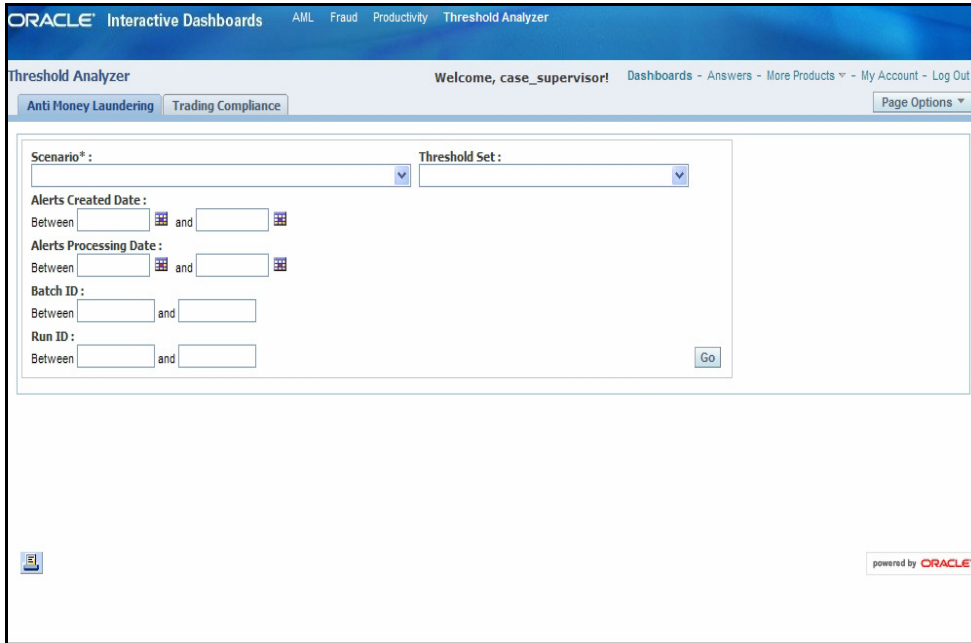
Figure 53. Dashboard Page

If you have logged out from the Answers page, the next time you login you are directly taken to the Answers page (Figure 54).
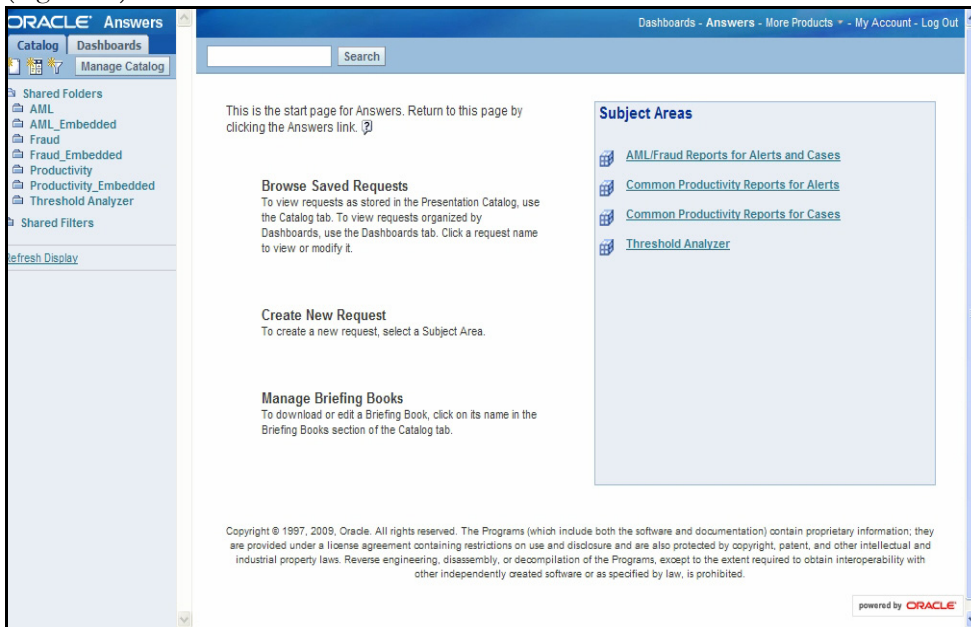
Figure 54. Answers Page

When the User is not an Administrator

If you are not an Administrator, the Homepage is always the dashboard.

On login, if dashboard is displayed as home page, you can see four dashboards—AML, Fraud, Productivity, and Threshold Analyzer. By default, the dashboard seen is AML. Click **Threshold Analyzer** to view the Threshold Analyzer dashboard (Figure 55).

Figure 55. Threshold Analyzer Dashboard

Here, you can see a tab for each scenario class for which scenarios have been installed. For example, as shown in Figure 55, Anti Money Laundering and Trading Compliance scenarios have been installed.

Initial Report Filters

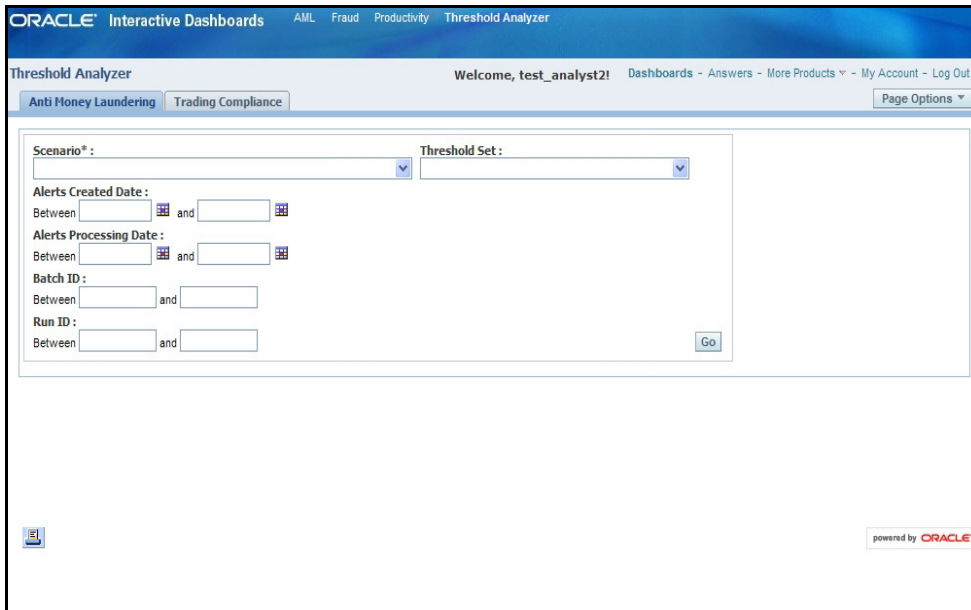Initial Report Filters are those filters that are always available, regardless of the scenario class or scenario selected for analysis. This section displays when you log into the Threshold Analyzer dashboard and select a scenario class tab. These filters can be used to filter your analysis based upon a Scenario and Threshold Set, as well as alert create dates or processing dates, or filtering based on a particular processing job run ID or a processing batch ID (Figure 56).
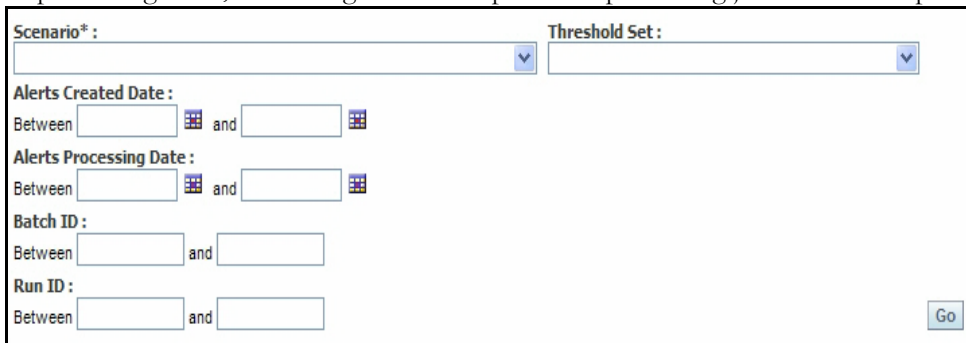
Figure 56. Initial Report Filters

- **Scenario**: This field is mandatory to specify and lists scenarios associated to the corresponding scenario class. The values in the Scenario drop-down contain the scenario name concatenated with the focus type in parenthesis.

- **Threshold Set**: Values in this field are populated depending on the scenario selected. If the scenario is changed, the Threshold Set values corresponding to that scenario are populated. Initially, when no scenario is selected, the drop-down lists all possible threshold sets associated with your set of scenarios.

- **Alerts Created Date**: The alert created date represents the system date of the creation of the alert. In this date filter, you can specify the date range by entering a *from* and *to* date (represented by the *Between* and fields) or selecting the dates using the calendar control. The *from* date should always be less than the *to* date. Data must be in the MM/DD/YYYY format. By default, the date fields are blank.

  If you enter only a *from* date, keeping the *to* date blank, the system fetches the data based on where the alert created date is greater than or equal to the given date. Similarly, if you enter only a *to* date then the system fetches data based on where the alert created date is less than or equal to the given date.

- **Alerts Processing Date**: The alert processing date represents the business date associated with the creation of the alert. In this date filter, you can specify the date range by entering a *from* and *to* date (represented by the *Between* and *and* fields) or selecting the dates using the calendar control. The *from* date should always be less than the *to* date. Data must be in the MM/DD/YYYY format. By default, the date fields are blank.

  If you enter only a *from* date, keeping the *to* date blank, the system fetches the data based on where the alert processing date is greater than or equal to the given date. Similarly, if you enter only a *to* date then the system fetches data based on where the alert processing date is less than or equal to the given date.

- **Batch ID**: Behavior detection cycles are associated with a processing batch, which is assigned a unique identifier for each execution of the detection batch cycle. Using this filter you can specify a range of batch identifiers by entering *from* and *to* batch identifier values (represented by the *Between* and *and* fields) in the text box. Only positive values can be entered in these text boxes. The *from* Batch ID value should always be less than the *to* Batch ID value. You are allowed to enter only numeric values in these fields.

  If only a *from* Batch ID is entered then the report fetches data based on where the batch identifier is greater than or equal to the given batch ID. Similarly, if you enter only a *to* Batch ID then the report fetches data based on where the batch identifier is less than or equal to the given value.

- **Run ID**: Within a behavior detection batch cycle, detection jobs are associated with job runs. Each job run receives a unique run identifier. Using this filter you can specify a range of run identifiers, or individual identifiers in a similar manner as described for the Batch ID filter. As for the Batch ID filter, the Run ID filter accepts only positive values and the *from* Run ID value should always be less than the *to* Run ID value and the filter accepts only numeric values.

  If only a *from* Run ID is entered then the report fetches data based on where the run identifier is greater than or equal to the given run ID. Similarly, if you enter only a *to* Run ID then the report fetches data based on where the run identifier is less than or equal to the given value.

Executing a Threshold Analyzer Report

By default, the Threshold Analyzer reports are not displayed upon login and the page shows the *No Result For The Selected Criteria* message as shown in Figure 57. To view the report, enter search values in your desired filters and click **Go**. The Additional Filters selection section opens (see *Using Additional Filters,* on page 118) and the Threshold Analyzer scatter graph statistical reports and their associated graphs open. For information about understanding graph display, see *Understanding the Graph Display,* on page 120.
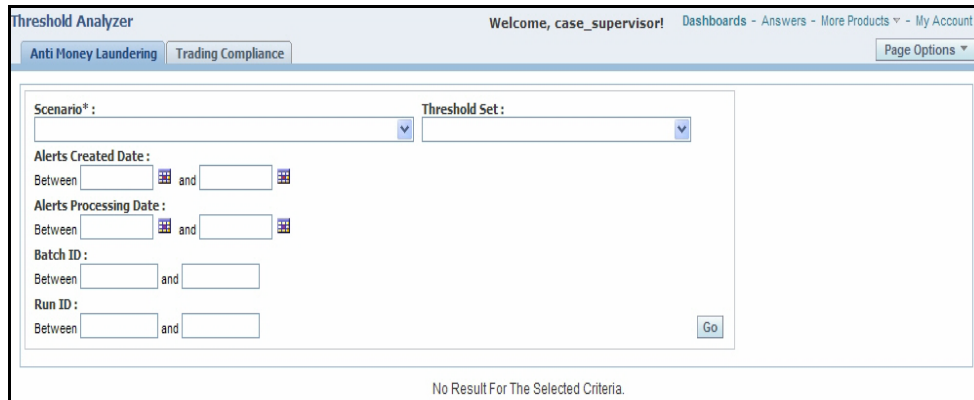
Figure 57. Default Page

Using Additional Filters

Additional filters can be optionally specified, where the additional filter options are driven by the selection of a scenario and the subsequent identification of scenario specific binding variables. The number and type of additional filters depends on the scenario selected. The Additional Filters section does not appear until you have clicked **Go** in the initial report filters section to generate the initial graph. The Additional Filters section appears below the initial report filters section but above the resulting graph. By default, additional filters are not applied to the initial results (Figure 58).
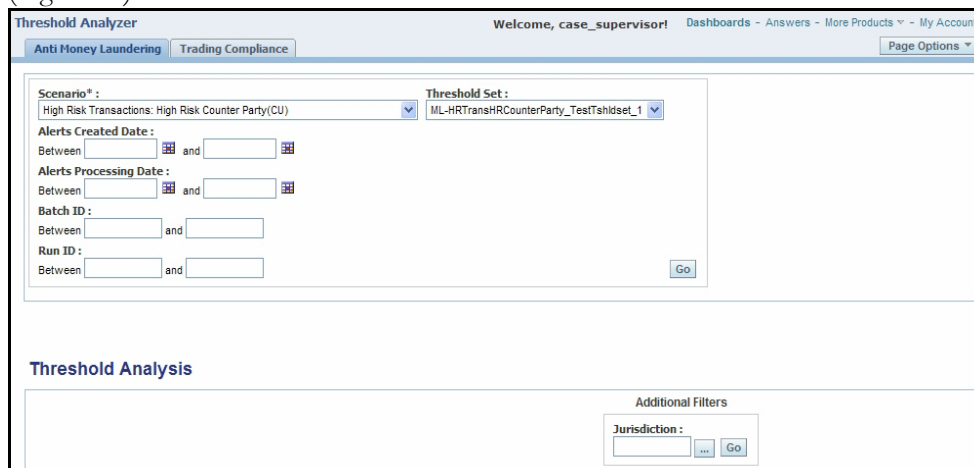

Figure 58. Additional Filter

To specify a value for use as an additional filter, you need to click on the ellipsis icon (...) next to the filter (as shown in Figure 58) to open a multi-select box (Figure 59)
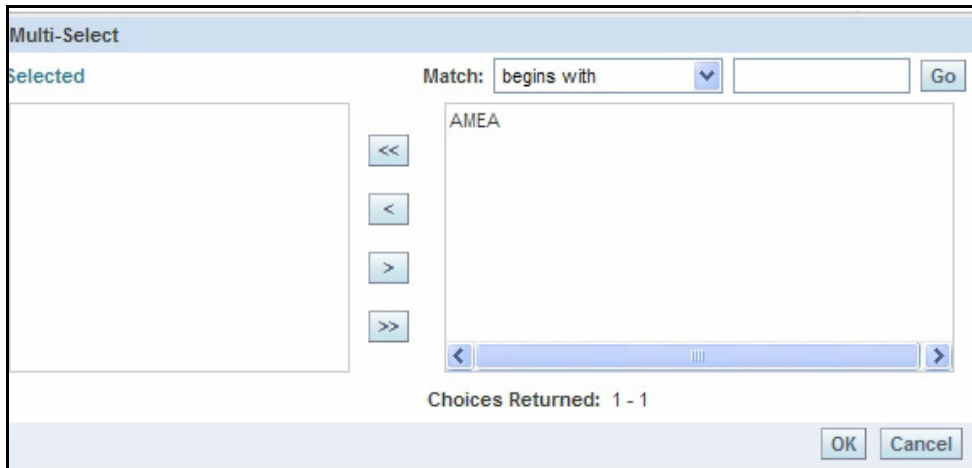
.

Figure 59. Additional Filter with Value

Follow these steps:

1. Select one or more desired filter values from the list of available values in the right hand list of the selection box. Move the selected filter values from the right hand list to the left using ⟨ .

2. To filter by all possible values, click ⟨⟨ to move all values into the Selected list.

3. To remove a filter value from the Selected list, select the filter value and click ⟩ . To remove all values from the Selected list click ⟩⟩ .

4. If the list of possible values for use as filters is lengthy then you can narrow the list by using the Match filter drop-down to bring back a subset of values to be displayed in the right hand list.

5. Once you are satisfied with your selection of additional filters, click **OK** to save these as searchable values or click **Cancel** to cancel your selections.

6. Once you have finished selecting any additional filters you would like to apply. Click **Go**. The scatter graph and the report statistics refreshes to show the result of applying the additional filters.

Modifying Axis Selections

The scatter graph is dependent on the values selected in the Axis drop-downs. Values in the Axis selection drop-downs represent bindings that are calculated for a scenario during the detection process and are specific to the scenario that has been selected in the Initial Filters section. These bindings often represent the values that are compared to the scenario's threshold parameters in order to determine whether or not to trigger an alert. For example, if a scenario has a threshold parameter for Minimum Total Transaction Amount, the value calculated and captured in the binding Tot Trans Amt is what is compared to the threshold value. Selecting Tot Trans Amt for use on an axis allows you to graphically plot the actual total transaction amounts that met or exceeded the scenario's Minimum Total Transaction Amount threshold. Additionally, axis selections may represent bindings that are calculated and captured for the purpose of providing parameters for use in setting up scoring rules. Being able to specify a scoring variable for a graph axis allows you to see what bindings might be useful for establishing scoring rules, based upon where on the axis the productive versus non-productive alerts fall. Being able to select and

graphically display two different variables will allow you to experiment with combinations of bindings to get an understanding of how to effectively set your thresholds to work together to eliminate false positive alerts.

The graph is initially generated using the first value as shown in the X axis selection drop-down and the second value as shown in the Y axis drop-down upon selection of **Go** in the initial report filters section. You have the option to select a different value for the vertical (Y) and the horizontal (X) axis of the scatter graph. The graph refreshes upon the selection of a value in either axis. To change both axis variables it is necessary to select one and allow the graph to refresh before selecting a different value for the second axis. Figure 60 shows the axis selection drop-down.
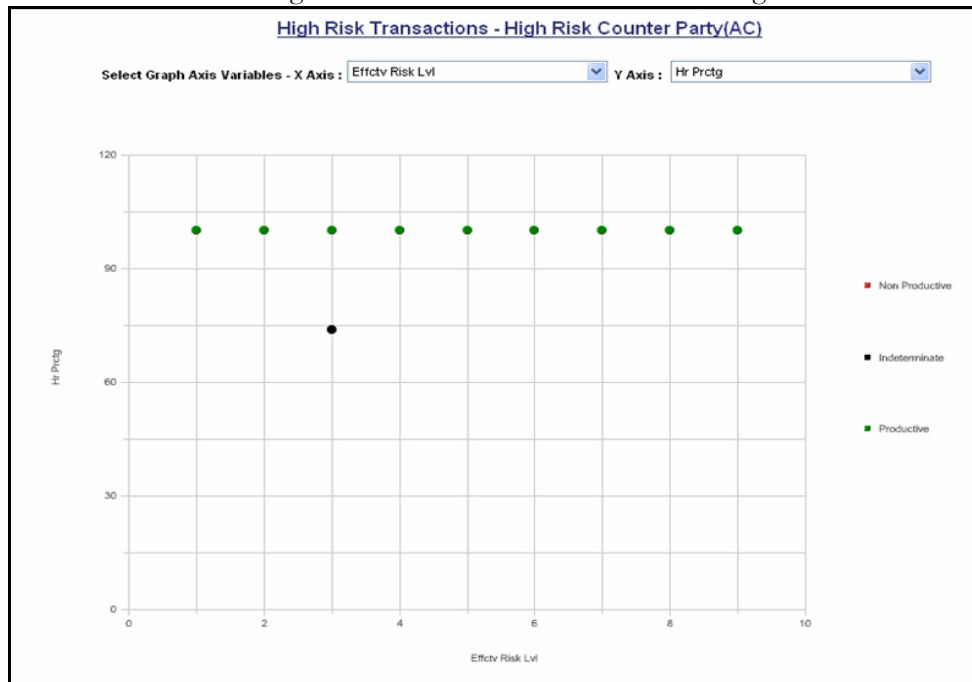

Figure 60. Axis Selection

Understanding the Graph Display

Each dot on the graph represents a match. By definition a match is the collection of records that satisfy the logic and criteria of a scenario pattern. An alert is generated during post-processing and is defined as one or more matches packaged and presented on the Oracle Financial Services application user interface for analysis and action. If multiple matches are found that are closely related for the same focus (that is, instances of the similar behaviors by the same entity), the matches can be combined to create a single alert, called a multi-match alert. So a single alert may be represented by multiple dots (matches) on the graph if that alert was a multi-match alert.

The scatter graph uses dots of differing colors to represent the quality rating of individual matches. By default, the Threshold Analyzer uses three categories of quality rating. By default, match quality rating is classified based upon the closing classification associated with a closing action on the alert, where possible classifications include Productive, Non Productive, and Indeterminate. For a multi-match alert, the closing classification for that alert is applied to each match that is part of that alert. Each match is plotted positionally on the graph based upon the match's actual binding value that is associated with the binding variables represented by the X and Y axis.

For example, if the X axis is the variable *Tot Trans Amt* and the Y axis is the variable *Tot Trans Ct*, the match is displayed on the graph relative to the *Tot Trans Amt* and the *Tot Trans Ct* actually involved in, and bound by, the match. Figure 61 shows an example of a scatter graph.
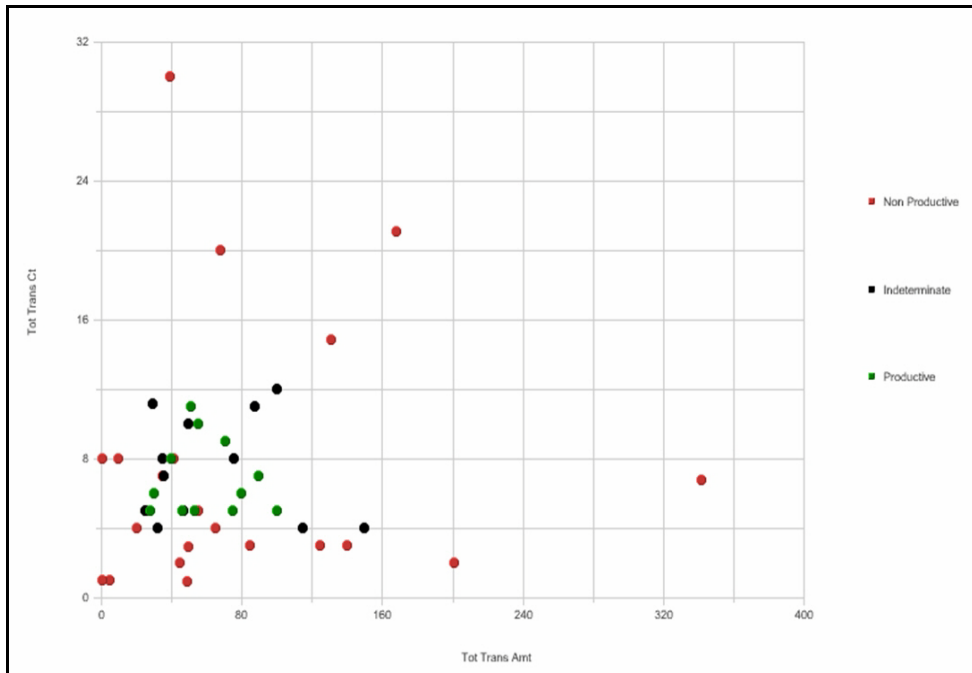
Figure 61. Scatter Graph

The closing classifications associated with the alert closing actions are configurable per implementation (refer to the *Configuration Guide* for information on how to modify closing classifications). Additionally, the logic used to determine what attribute of an alert is used to rate the quality (does not have to be the closing classification code) is configurable per implementation.

How to Interpret Results

There are the following three types of alerts:

- **Productive**: green dots on the graph show the alerts that are Productive

- **Non-Productive**: red dots on the graph show the alerts that are Non-Productive

- **Indeterminate**: black dots on the graph show the alerts that have been closed with a reason considered to be Indeterminate (action does not indicate definitively whether the alert was of quality or a false positive)

The location and concentration of the Productive, Indeterminate, and Non-Productive alerts on the scatter graph can represent at what value ranges or boundaries the thresholds associated with the X and Y axis variables are most effective. Refreshing the graph using various combinations of axis variables can provide a comprehensive view of what settings are likely to produce the most effective and quality alerts.

For example, using the graph results shown in Figure 61, you can review the results and draw the following conclusions:

- Productive alerts for this scenario have a total transaction count between 5 and 11

- Productive alerts for this scenario have a total transaction amount between approximately $20K and $100K

- You can eliminate false positives without losing any Productive or Indeterminate alerts by raising the *Min Total Trans Amt* threshold for this scenario to $15K

- You can eliminate false positives without losing any Productive or Indeterminate alerts by raising the *Min Total Trans Ct* threshold for this scenario to 4

- You can use scoring to reflect that the alerts with an amount > $100K are less likely to be Productive

- You can use scoring to reflect that alerts with a count > 12 are less likely to be productive

Understanding Report Statistics

The Report Statistics section shows two sets of matrices and graphs. The first set of statistics displays the percentage of alerts returned by your search as they breakdown across the quality rating categories. The second set of statistics displays the minimum, maximum, median, and average values across certain binding variables associated with the scenario and the alerts returned as a result of your search.

Summary Counts

The summary counts display results in a tabular and line-bar combo graph. The tabular report shows the total number of matches, total number of alerts, and the percentage of the total number of alerts that is represented in each quality category. The Grand Total is calculated as the sum of matches across all categories and the sum of alerts across all quality categories. The sums returned are irrespective of the axis variables used and represent primarily a count of alerts/matches by quality category. The percentage of alerts represented in each category is calculated by the formula:

(Total count of alerts for individual category / Grand Total of alerts) × 100

In the line-bar combo graph (Figure 62), the clustered bar graph shows the total number of matches in blue and total number of alerts in red over the three default quality categories - productive, non-productive, and indeterminate. The green colored line shows the percentage of alerts distributed over each category.

These statistics should provide you a high level understanding of how your alerts have been ranking, in terms of quality.

Category	Total # of Matches	Total # of Alerts	% of Alerts
Indeterminate	8	8	53.33%
Non Productive	2	2	13.33%
Productive	5	5	33.33%
Grand Total	**15**	**15**	**100.00%**

Figure 62. Summary Counts

Understanding the Minimum, Maximum, Average and Median Statistics

This statistical graph shows minimum, maximum, average, and median value of certain binding variables for each category of alerts. The binding variables represented in the report statistics are pre-defined based upon the current scenario being analyzed and are not driven by the X and Y axis variables selected for the scatter graph. These variables may differ from scenario to scenario and are meant to represent those variables likely to be most influential in the generation of an alert. Understanding the minimum and maximum values represented in the results, as well as the average and median values being returned for bindings representing some of the more impactful thresholds, provides a better view of the alerts represented in the search results and gives greater context to your analysis.

In the report, Minimum columns show the minimum value of the relevant binding variable returned for all alerts in the current search, by quality category. Maximum columns show the highest value of the relevant binding variable returned for all alerts in the current search, by quality category. Average columns show the average amount of the relevant binding variable returned for all alerts in the current search, by quality category. Median columns show the middle value of the relevant binding variable returned for all alerts in the current search, by quality category.

This statistical report utilizes a tabular representation as well as two vertical bar graphs. The tabular view basically shows the min, max, average and median amount and count of alerts for each quality category. The graphical view gives clustered bar graph min, max, average and median amount and count for each category. For productive alerts the bar comes in green, non-productive comes in red, and indeterminate comes in black color, by default (Figure 63).

Note: All scenarios may not report on two distinct sets of bindings. As available binding variables may vary based on the selected scenario, this statistical graph also varies scenario to scenario and is based on pre-defined columns for each scenario. The results refresh only with application of new static filters. It is independent of additional filter as well as graph axis filter. For those scenarios the report may only display one graph..
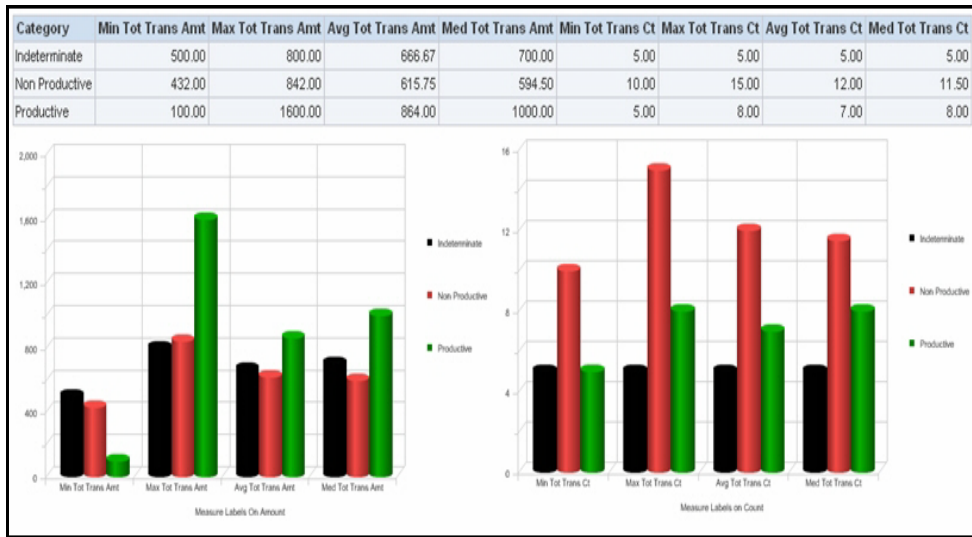
Category	Min Tot Trans Amt	Max Tot Trans Amt	Avg Tot Trans Amt	Med Tot Trans Amt	Min Tot Trans Ct	Max Tot Trans Ct	Avg Tot Trans Ct	Med Tot Trans Ct
Indeterminate	500.00	800.00	666.67	700.00	5.00	5.00	5.00	5.00
Non Productive	432.00	842.00	615.75	594.50	10.00	15.00	12.00	11.50
Productive	100.00	1600.00	864.00	1000.00	5.00	8.00	7.00	8.00

Figure 63. Minimum, Maximum, Average, and Median Statistics

CHAPTER 9 — *Security Configuration*

This chapter provides instructions for setting up and configuring the Security Management System (SMS) to support OFSAAI user authentication and authorization. It also contains instructions for setting up user accounts in the OFSAAI database to access the Scenario Manager.

This chapter focuses on the following topics:

- **About OFS AM User Authentication**
- **About User Setup**
- **About Configuring Access Control Metadata**
- **Mapping Users To Access Control Metadata**
- **About Scenario Manager Login Accounts**
- **About Changing Passwords for System Accounts**
- **About Configuring File Type Extensions**
- **About Configuring File Size**
- **About Configuring Status To User Role Table**

About OFS AM User Authentication

The primary way to access information is through a Web browser that accesses the Alert Management, Case Management, and Administration Tools. The Scenario Manager authenticates use of the OFSAAI database only.

Web server authentication is also available for Oracle clients who want to utilize their own External Authentication Management (EAM) tool.

Accessing OFS AM

A user gains access to OFS AM based on the following:

- Authentication of a unique user ID and password that enables access to Alert Management, Case Management, and Administration Tools.

For accessing Alert Management:

- Set of policies that associate functional role with access to specific system functions in OFS AM.
- One or more associated organizational affiliations that control the user's access to alerts.
- Relationship to one or more scenario groups.
- Access to one or more jurisdictions.
- Access to one or more business domains.

For accessing Case Management:

- Set of policies that associate functional roles with access to specific system functions in OFS AM.

- Access to one or more case types/subtypes.

- 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.

For accessing Watch List Management:

- Set of policies that associate functional roles with access to specific system functions in OFS AM.

- Access to one or more jurisdictions.

- Access to one or more business domains.

For accessing Administration Tool:

- Set of policies that associate admin functional role with access to specific system functions in OFS AM.

About User Setup

To set up a user and provide the user access to OFS AM, perform the following steps:

1. Create a user: Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* for setting up a user.

2. Once the user is created, map the user to the group. This in turn maps the user to the role. With this the user will have access to the privileges as per the role.

Note: You must assign at least one Alert Management or Case Management role and one Administrator role per user.

Refer to section *User Group and User Roles* on page 126 for more information on User Roles and User Groups. Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* for further information.

User Group and User Roles

The OFSBDF User Roles are predefined in the Oracle Financial Services Behavior Detection application. Sample values for User groups are included in the installer but can be modified by clients to meet their specific needs. The corresponding mappings between User Roles and sample User Groups are predefined but can also be modified by clients to either adjust the role to sample user group mapping or to map roles to newly defined user groups.

For creating a new user group and mapping it to en existing role, refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* :

Note: Different solutions have different predefined/preoccupied precedence of User Groups. Therefore, if ECM Admin/System Admin is creating a new User Group make sure while providing precedence value to not use the following precedence:

Table 14. Solution with Predefined Precedence Range

Solution	Precedence Range already occupied
OFS ECM	901 to 1000
OFS OR	1001 to 2000
OFS KYC	2001 to 3000
OFS RR	3001 to 4000

While creating a new User Group, we can give precedence as 5001

- Defining User Group Maintenance Details

- Adding New User Group Details

- Mapping Users to User Group

- Mapping User Group(s) to Domain(s)

- Mapping User Group(s) to Role(s)

Mapping User Group(s) to Domain(s)

To map User Group(s) to Domain(s), map all the Alert Management User Groups to Alert Management Information Domain (Infodom).

For the above sections, refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* for further information.

Actions to Role mappings are done through Database tables. Sample action to role mappings are included in the application. Refer to the following sections of *Configuration Guide*, for changing the mapping of roles to actions.

- Working with Alert Action Settings

Actions are primarily associated with a User Role, not an individual user. However, the ability to Reassign To All when taking a Reassign action is associated at the individual user level. Reassign To All means that a user is allowed to assign to users and organizations that may not be within their normal viewing privileges.

The following table describes the predefined User Roles and corresponding User Groups present in OFS AM.

Table 15. Alert Management Roles and User Groups

Role	Group Name	User group Code
AM Analyst I	AM Analyst I User Group	AMANALYST1GRP
AM Analyst II	AM Analyst II User Group	AMANALYST2GRP
AM Analyst III	AM Analyst III User Group	AMANALYST3GRP
AM Supervisor	AM Supervisor User Group	AMSUPVISRGRP
AM Executive	AM Executive User Group	AMEXCUTIVEGRP
AM Internal Auditor	AM Internal Auditor User Group	AMINAUDITRGRP
AM External Auditor	AM External Auditor User Group	AMEXAUDITRGRP

Table 15. Alert Management Roles and User Groups (Continued)

Role	Group Name	User group Code
AM Scenario group	AM Scenario group User Group	AMDATAMNRGRP
AM Mantas Administrator	Mantas Administrator User Group	AMMANADMNGR

The following table describes the Watch List Roles and corresponding User Groups

Table 16. Watch List Roles and User Groups

Role	Group Name	User group Code
Watch List Supervisor	Watchlist Supervisor Group	WLSUPERVISORUG

Note: If you wish to change the user group mapping for users who are already mapped to one or more groups, you must deselct the preferences for the Home page if it has been set.

Mapping a User to a Single User Group

If a user is to have only one role then that user can be mapped to a single User Group associated with that User Role. Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* to know more about User to User Group mapping.

Mapping a user to multiple User Groups within Alert Management

If a user needs to have more than one role within Alert Management, then the user needs to be mapped to the different User Groups associated with the corresponding role. When the user logs into Alert Management, user access permissions would be the union of access and permissions across all roles.

Mapping a user to multiple User Groups across Alert Management and other applications

If a user needs to have different roles in Alert Management and roles for other platform supported applications, then that user has to be mapped to different user groups.

Mapping a Function to a Role

The followingfunction needs to be mapped to an appropriate Alert User Role through Function-Role Map function, which is, available in Security Management System, by logging in as the System Administrator in OFSAAI toolkit.

AMACCESS

All Alert Management user roles should be mapped to the function AMACCESS in order to access an alert. Users of roles that are not mapped to this function cannot access the details of the Alerts.

Defining the User Access Properties and Relationships

The following types of data compose a user's security configuration:

- **Business Domain(s):** Property that enables an OFS AM client to model client data along operational business lines and practices.

- **Jurisdiction(s):** Property that enables an OFS AM client to model client data across such attributes as geographic location or type or category of a business entity.

- **Organization(s):** Department or organization to which an individual user belongs.

- **Role(s):** Permissions or authorizations assigned to a user in the system (such as, OFS AM administrator or Auditor).

- **Scenario Group(s):** Group of scenarios in Behavior Detection Framework that identifies a set of scenario permissions and to which a user has access rights.

- **Case Type/Subtype(s):** Case type/subtypes combinations to which, a user has access rights.

The following figure illustrates the OFS AM user authorization model.
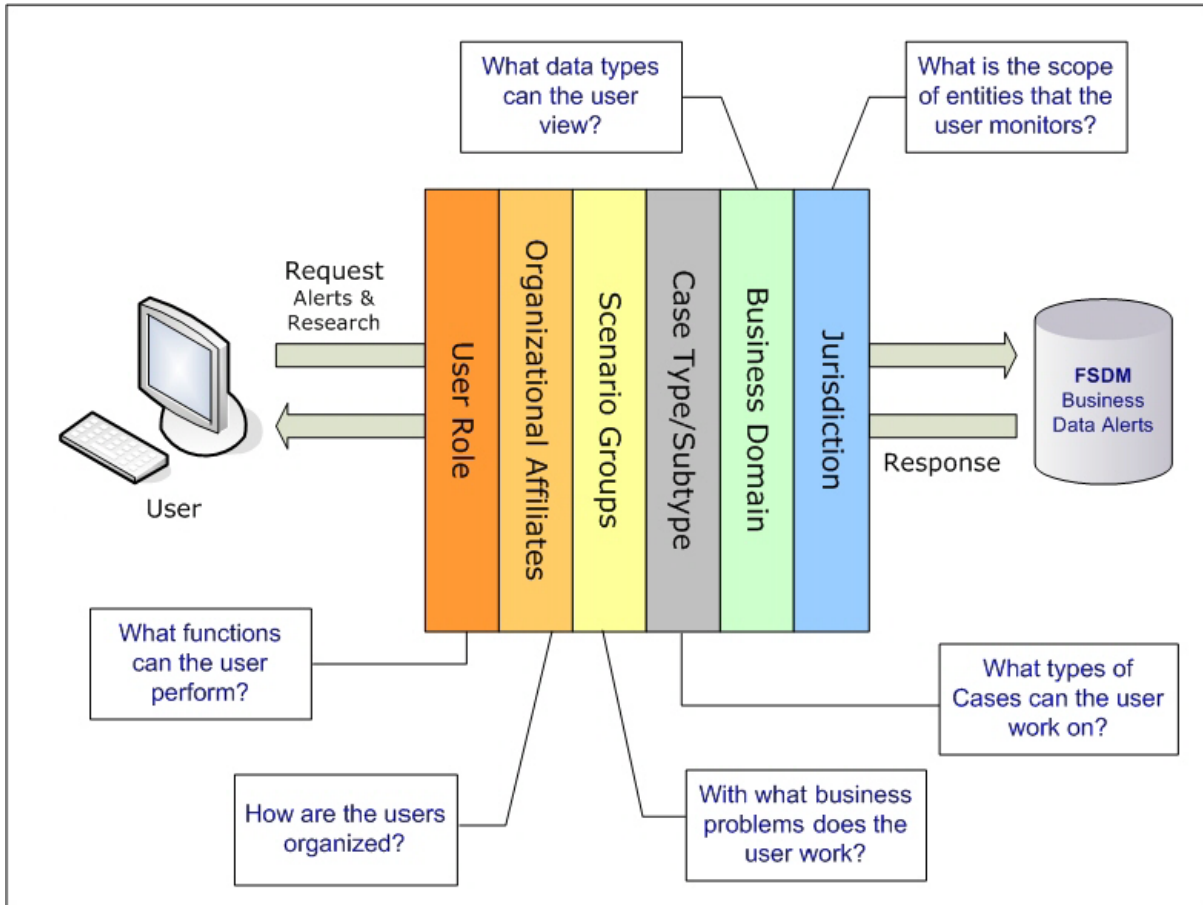
Figure 64. OFS AM User Authorization Model

The following provides the relationships between the data points that Figure 5 illustrates.

Table 17. Relationships between Data Points

Data Point	Relationship
Organization	Root of an OFS AM client's organization hierarchy
	Associated with 0..n users as a line organization
	Associated with 0..n users for view access to the organization
	Associated with 1..n Business Domains
	Associated with 1..n Scenario Groups
	Associated with 1..n Case Type/Subtypes
	Associated with 1..n Jurisdictions
	Has no direct relationship with a Role
Role	Associated with 0..n Users
	Has no direct relationship with an Organization
User	Associated with 1..n Business Domains
	Associated with 1..n Jurisdictions
	Associated with 1..n Roles
	Associated with 1..n Scenario Groups
	Associated with 1..n Case Type/Subtypes
	Associated with 1..n Organizations (as members)
	Associated with one Organization (as `mantasLineOrgMember`)
Users (Admin Tools)	Should be mapped only to mantas Admin Role.
Scenario Group	Associated to 0..n users
	Associated with Scenarios referenced in `KDD_SCNRO` table.
Case Type/Subtype	Associated to 0..n users
	Group name identifies the case type/subtype, matching a case `CASE_TYPE_SUBTYPE_CD` in the `KDD_CASE_TYPE_SUBTYPE` table.
Business Domains	Associated to 0..n users
	Business domain *key* must be in the `KDD_BUS_DMN` table
Jurisdiction	Associated to 0..n users
	Jurisdiction *key* must exist in the `KDD_JRSDCN` table

Obtaining Information Before Configuring Access Control

Before you perform access control activities (for example, adding a group, modifying user information, or deleting a user), contact your system administrator for the following information to add to the locations in Table 11.T

Note: Email ID is mandatory for users who would need to take Email action. The user ID should configured with valid email IDs while configuring the same through the User Maintenance UI.

About Configuring Access Control Metadata

You must first provide the user with access privileges, so the user can perform activities throughout various functional areas in ECM. This enables the user to access at least one of each of the following:

- **Jurisdiction:** Scope of activity monitoring for example, Geographical Jurisdiction or Legal entity (Refer to *Creating a Jurisdiction*, on page 33, for more information).

- **Business Domain:** Operational line of business (Refer to *Creating a Business Domain*, on page 34, for more information).

- **Scenario Group:** Grouping of scenarios to control user access to scenarios.

- **Role:** Permissions or authorizations assigned to a user.

- **Organization:** User group to which a user belongs.

Some data types such as Scenario Group, Role, Business Domain, Case Type, and Case Subtype which compose the user security configuration are predefined with sample values which are available through the installer. Clients can change or add new values for these data types (with the exception of User Role) based on specific requirements. The following section explains how to add or modify these data types.

Creating Jurisdiction in the Database

OFS AM uses Jurisdictions to limit user access to data in the database. Records from the OFS AM client that the Ingestion Manager loads must be identified with a jurisdiction, users of the system must be associated with one or more jurisdictions. In the Alert and Case Management system, users can view only data or alerts or case associated with jurisdictions to which they have access. You can use a jurisdiction to divide data in the database; for example:

- **Geographical:** Division of data based on geographical boundaries, such as countries.

- **Organizational:** Division of data based on different legal entities that compose the client's business.

- **Other:** Combination of geographic and organizational definitions. In addition, it is client driven and can be customized.

In most scenarios, a jurisdiction also implies a threshold that enables use of this data attribute to define separate threshold sets based on jurisdictions.

There can be two approaches to create a jurisdiction in the database:

- Creating Jurisdiction in the Database through Scripts

- Creating Jurisdiction in the Database through Excel Upload

Creating Jurisdiction in the Database through Scripts
You can create jurisdiction in the database using the following steps:

1. Add the appropriate record to the `KDD_JRSDCN` database table, which Table 18 describes.

Table 18. `KDD_JRSDCN` Table Attributes

Column Name	Description
JRSDCN_CD	Code (one to four characters) that represents a jurisdiction (for example, N for North, or S for South).
JRSDCN_NM	Name of the jurisdiction (for example, North or South).

Table 18. `KDD_JRSDCN` **Table Attributes (Continued)**

Column Name	Description
JRSDCN_DSPLY_NM	Display name of the jurisdiction (for example, North or South).
JRSDCN_DESC_TX	Description of the jurisdiction (for example, Northern US or Southern US).

2. Add records to the table by using a SQL script similar to the sample script in Figure 6.

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

Figure 65. Sample SQL Script for Loading KDD_JRSDCN

Note: The `KDD_JRSDCN` table is empty after system initialization and requires populating before the system can operate.

Creating Jurisdiction in the Database through Excel Upload

The Excel upload process inserts the data into the appropriate dimension tables based on the pre-configured Excel upload definitions installed as part of the application installation. Data already existing should not be loaded again, as this would result in failure of upload. When uploading additional records, only the incremental records should be maintained in the Excel template with the correct unique identifier key.

1. All template excel files for excel upload are available in `ftpshare/STAGE/Excelupload/AMCMLookupFiles`.

2. All date values should be provided in `MM/DD/YYYY` format in the Excel worksheet.

3. Whenever a record is deleted from the excel, the complete row should be deleted. In other words, no blank active record should exist in the Excel.

4. After selecting the Excel template, preview it before uploading.

The Excel Upload screen can be accessed by logging in as Admin user.

Creating 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 (for example, Private Client vs. 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. OFS AM tags each data record provided through the Ingestion Manager to one or more business domains. OFS AM also associates users with one or more business domains in a similar fashion. If a user has access to any of the business domains that are on a business record, the user can view that record.

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

● **a:** Private Client

● **b:** Retail Banking

A record for an account that is considered both has BUS_DMN_SET=ab. If a user can view business domain **a** or **b**, the user can view the record. You can use this concept to protect special classes of data, such as data about executives of the firm. For example, you can define a business domain as *e: Executives*.

You can set this business domain with 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 as well, any user who can view Private Client data can view the executive's record. Hence, it is important not to apply too 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.

There can be two approaches to creating a Business Domain in the database:

- Creating Business Domain in the Database through scripts
- Creating Business Domain in the Database through Excel Upload

Creating Business Domain in the Database through scripts

To create a business domain, follow the steps:

1. Add the appropriate user record to the KDD_BUS_DMN database table, which Table 19 describes.

Table 19. KDD_BUS_DMN Table Attributes

Column Name	Description
BUS_DMN_CD	Single-character code that represents a business domain (for example, a, b, or c).
BUS_DMN_DESC_TX	Description of the business domain (for example, Institutional Broker Dealer or Retail Banking).
BUS_DMN_DSPLY_NM	Display name of the business domain (for example, INST or RET).
MANTAS_DMN_FL	Flag that indicates whether Oracle Financial Services Behavior Detection Framework specified the business domain (Y). If an OFS AM client specified the business domain, you should set the flag to N.

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

2. Add more records to the table by using a SQL script similar to the sample script in Figure 8.

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

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

Figure 66. Loading the KDD_BUS_DMN Table

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

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

Creating Business Domain in the Database through Excel Upload

Refer to *Creating Jurisdiction in the Database* to perform the Excel Upload for Business Domain. The excel template to be used is KDD_BUS_DMN.xls.

Creating Scenario Group

There are two approaches to creating a Scenario Group in the database:

- Creating Scenario Group in the Database through scripts

- Creating Scenario Group in the Database through Excel Upload

Creating Scenario Group in the Database through scripts

To create a Scenario Group, follow these steps:

1. Add the appropriate user record to the KDD_SCNRO_GRP database table, which Table 20 describes.

Table 20. KDD_SCNRO_GRP Table Attributes

Column Name	Description
SCNRO_GRP_ID	Scenario group identifier.
SCNRO_GRP_NM	Scenario Group Name

2. Add more records to the table by using a SQL script similar to the sample script in Figure 67.

```
INSERT INTO KDD_SCNRO_GRP(SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES
(66,'BEX');
INSERT INTO KDD_SCNRO_GRP(SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES
(77,'CST');
COMMIT;
```

Figure 67. Loading the KDD_SCNRO_GRP Table

Creating Scenario Group in the Database through Excel Upload

Refer to *Creating Jurisdiction in the Database*, to perform the Excel Upload for Scenario Group. The excel template to be used is KDD_SCNRO_GRP.xls.

Creating Scenario Group Membership

There are two approaches to creating a Scenario Group Membership in the database:

- Creating Scenario Group Membership in the Database through scripts

- Creating Scenario Group Membership in the Database through Excel Upload

Creating Scenario Group Membership in the Database through scripts

To create a Scenario Group Membership, follow these steps:

1. Add the appropriate user record to the KDD_SCNRO_GRP_MEMBERSHIP database table, which Table 21 describes.

Table 21. KDD_SCNRO_GRP_MEMBERSHIP Table Attributes

Column Name	Description
SCNRO_ID	Scenario Identifier.
SCNRO_GRP_ID	Scenario Group Identifier
SCNRO_GRP_NM	Scenario Group Name

2. Add more records to the table by using a SQL script similar to the sample script in Figure 68.

```
INSERT INTO KDD_SCNRO_GRP_MEMBERSHIP
(SCNRO_ID,SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES (113000016,66,'BEX') ;

INSERT INTO KDD_SCNRO_GRP_MEMBERSHIP
(SCNRO_ID,SCNRO_GRP_ID,SCNRO_GRP_NM) VALUES (113000016,77,'CST') ;
```

Figure 68. Loading the KDD_SCNRO_GRP_MEMBERSHIP Table

Creating Scenario Group Membership in the Database through Excel Upload

Refer to *Creating Jurisdiction in the Database*, to perform the Excel Upload for Scenario Group Membership. The excel template to be used is KDD_SCNRO_GRP_MEMBERSHIP.xls.

Creating Organizations in the Database

There can be two approaches to create an Organization in the database:

- Creating Organization in the Database through scripts
- Creating Organization in the Database through Excel Upload

Creating Organization in the Database through scripts

Add entries directly to the KDD_ORG table using a script.

1. Add the appropriate record to the KDD_ORG database table, which Table 22 describes.

Note: The KDD_ORG table is empty after system initialization and requires populating before the system can operate.

Table 22. KDD_ORG Table Attributes

Business Field	Column Name	Date Type	Definition	Null
Organization	ORG_CD	CHAR(20)	Unique identifier for this organization.	No
Organization Display Name	ORG_NM	CHAR(60)	Short name for the organization that is used for display purposes.	Yes
Organization description	ORG_DESC_TX	CHAR(100)	Description of this organization	Yes
Line Organization	PRNT_ORG_CD	CHAR(20)	Identifies the parent organization of which this organization is considered to be a child	Yes

Table 22. `KDD_ORG` Table Attributes

Business Field	Column Name	Date Type	Definition	Null
Modification Date	`MODFY_DT`	DATE	Identifies the last modified Date and time.	Yes
Modified User	`MODFY_ID`	NUMBER(10)	Identifies the user id of the user who last modified the data	Yes
Comment	`COMMENT_TX`	CHAR(4000)	Comment	

2. Add records to the table by using a SQL script similar to the sample script below.

```
insert into KDD_ORG (ORG_CD, ORG_NM, ORG_DESC_TX,
PRNT_ORG_CD, MODFY_DT, MODFY_ID, COMMENT_TX)
values ('TestOrgA', 'TestOrgA', 'TestOrgA', null, null, null,
null);
insert into KDD_ORG (ORG_CD, ORG_NM, ORG_DESC_TX,
PRNT_ORG_CD, MODFY_DT, MODFY_ID, COMMENT_TX)
values ('TestOrgB', 'TestOrgB', 'TestOrgB', 'TestOrgA', null,
null, null);
insert into KDD_ORG (ORG_CD, ORG_NM, ORG_DESC_TX,
PRNT_ORG_CD,MODFY_DT, MODFY_ID, COMMENT_TX) values
```

Figure 69. Sample SQL Script for Loading `KDD_ORG`

Creating Organization in the Database through Excel Upload

Refer to *Creating Jurisdiction in the Database* to perform the Excel Upload of organization.

The excel template to be used is `KDD_ORG.xls`.

Mapping Users To Access Control Metadata

An Administrator can map each user to Access Control Metadata and Security attributes which will control the user's access permissions. The Security Attribute Administration can be accessed from the Administration menu (Figure 71).

Note: Before proceeding with providing a user access through this UI, all necessary data should be available in the appropriate database tables and the user needs to be created.
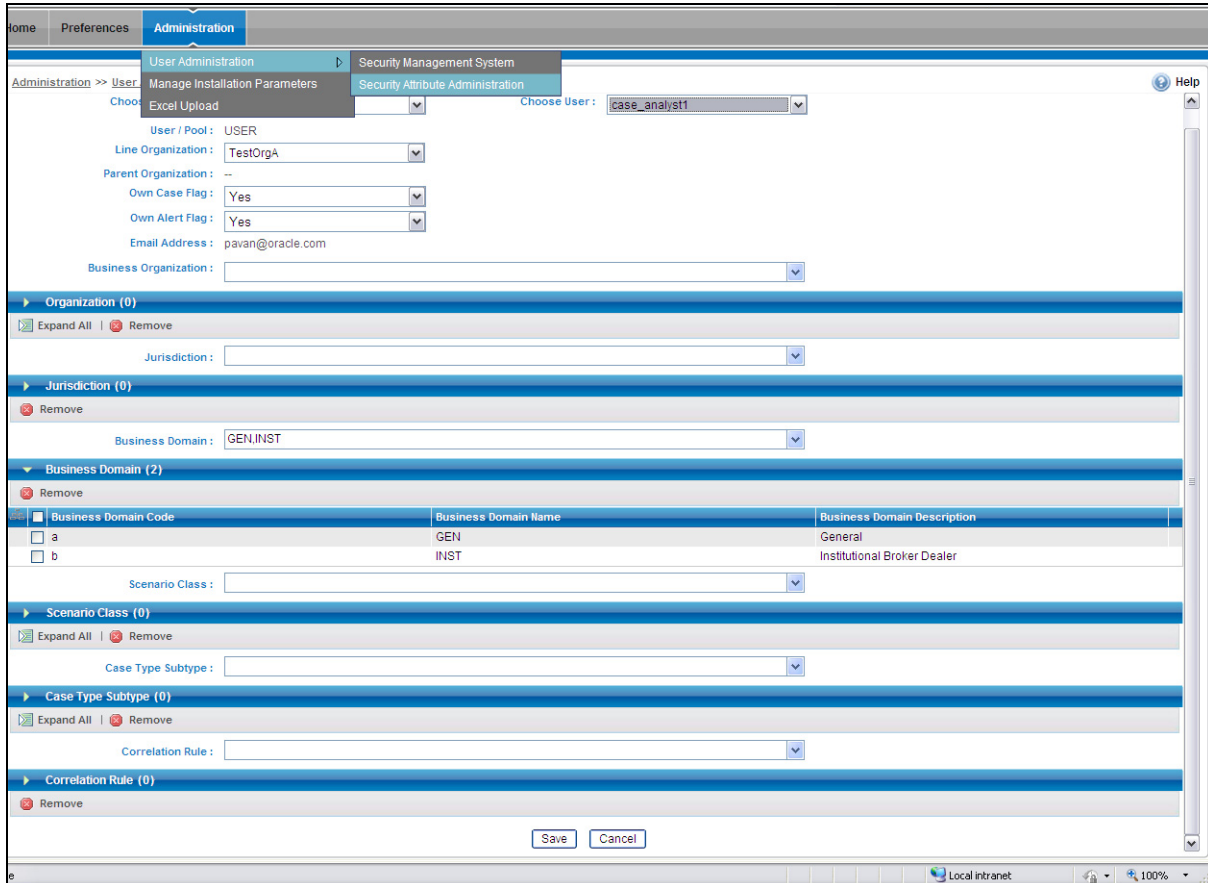
Figure 70. Security Attribute Administration

Using this UI an Administrator can map both Organizations and Users to different Security attributes.
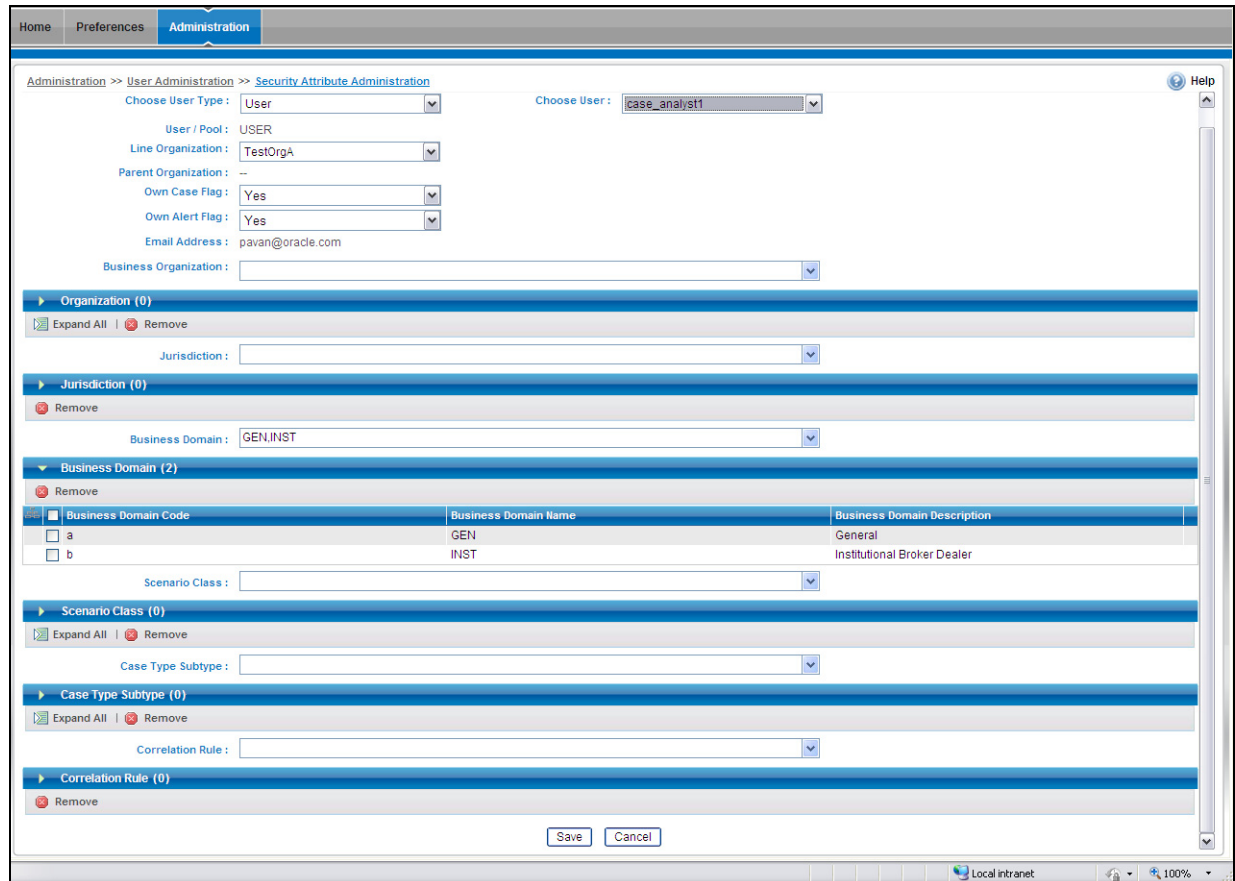
Figure 71. Components of Security Attribute

Note: In order to update the user profiles before proceeding with mapping any security attributes, select the value **User** from the **Choose User Type** drop-down list. When chosen, all the updates made to all the user profiles through User Maintenance UI would be imported from `CSSMS_USER_PROFILE` table of OFSSAAI configuration schema to `KDD_REVIEW_OWNER` table of mantas schema.

This action would not affect the security attributes that might be already mapped.

Once the user details are imported, the security attributes should be mapped/remapped.

The drop-down lists have options for both Organizations and Users. To map an organization, select the organization from the drop-down list and select the corresponding Organization in the **Choose User** drop-down list.

The **Choose User** drop-down list filters its values based on the value selected in the **Choose User Type** selection drop-down list. It shows only users, if the **User Type** is User; and it shows only organizations, if the **User Type** is Organization.

After selecting the desired user in **Choose User** drop-down list, the Administrator can map the following parameters to the selected user:

- Organization

- Jurisdiction

- Business Domain

- Scenario Group

- Correlation Rule

Organization

A User or Organization's access to other Organization depends on the selection(s) made for this organization parameter. For Example, if a user is mapped Org1 and Org2, it implies that, user can access alert/case, which belongs to these two organizations, provided other security attributes are also matching.

Jurisdiction

Mapping of one or more jurisdictions to a user or organization, gives the privilege of accessing cases, alerts, watch lists, and watch list members that belong to the mapped jurisdiction.

Business Domain

Mapping of one or more business domains to a user or organization gives privilege of accessing cases, alerts, watch lists, and watch list members that belong to the mapped business domains.

Scenario Group

Mapping of one or more Scenario Groups to a user or organization gives the privilege of accessing alerts that belong to the mapped scenario Group.

Correlation Rule

Mapping of one or more correlation rules gives the privilege of viewing the correlations generated based on the mapped correlation.

Additional Parameters

Other parameters, such as, Line Organization, Own Case Flag and Own Alert flag can be selected in the corresponding drop-down list mentioned in the screen and can be updated by clicking the **Save** button.

Note: The Own Alert and Case flag is required for taking ownership of the alerts and cases. If an alert user needs to perform a Promote To Case action, then the following pre-requisites should be fulfilled.

---

1. The user should be mapped to any one of the following user groups:

   - Case Supervisor

   - Case Analyst1

   - Case Analyst2

2. The user's 'Case Own' flag should be enabled by setting the value to 'Y'.
   Or
   The user should be mapped to the Case Initiator Role.

Note: You must map the scenario group and case type to all users even if they are not case or alert management users.

About Scenario Manager Login Accounts

OFS AM users gain access to the Scenario Manager application based on the following:

- User ID and password authentication enables access to the Scenario Manager.

- An associated functional role corresponds to particular user tasks and authorities.

Creating Scenario Manager Login Accounts

As administrator, the user setup process requires that you complete the following tasks:

1. Create a database login account and password (Refer to section *To Create the Database Login Account*, on page 38, for more information).

2. Set up an account and functional roles in the Scenario Manager. Before performing any tasks in the Scenario Manager, you must set up a user login account that establishes access and roles in the Scenario Manager. Perform these setups by adding records to the database (Refer to section *To Set Up an Account and Functional Roles,* on page 141, for more information).

3. Grant the database roles that the functional roles require. You can grant the role of data miner, or MNR to an *Scenario Manager* user (Refer to section *To Grant a Database Role,* on page 142, for more information).

   Note: Oracle suggests having only a few generic users in the database to use the Scenario Manager, as most organizations have an extremely small user population to execute these tools.

To Create the Database Login Account
The system instantiates the database as a set of Oracle database tables. Therefore, each user whom the OFS AM client authorizes to use the Scenario Manager must have login access to the Oracle database. As administrator, you must set up an Oracle database login account for each user, and assign the KDD_MNR user role to this account.

Note: OFSBDF does not support external logins (for example, OPS$accounts) in an Oracle database environment. Users must provide an explicit password when logging on.

The assumption is that the Oracle client's system administrator has training and experience in performing such setups, and, therefore, does not require instructions here on how to perform this task. However, for information about setting up Oracle database accounts, Refer to the appropriate Oracle database documentation.

Note: The Solaris and Oracle database login user IDs do not have to be identical. However, the Scenario Manager and Oracle database login user IDs MUST be identical.

To Set Up an Account and Functional Roles
To create a Scenario Manager account and functional role, follow the steps:

1. Access the KDD_USER table.

The following table defines the attributes for the KDD_USER table.

Table 23. KDD_USER Table Attributes

Column Name	Description
USER_ID	User's database login ID.
USER_NM	User's name.
USER_ROLE_CD	User's default database role.
ACTV_FL	Active user indication (Y or N).
WRKLD_CD	Not used by the Scenario Manager.

2. Enter the following information into the table using an SQL script:

   a. User database login ID in the USER_ID column. (The Scenario Manager and Oracle database login user IDs must be identical.)

   b. User name in the USER_NM column.

   c. Default user role in the USER_ROLE_CD column.

      To use the Scenario Manager, the user needs the MNR (data miner) database role. The MNR database role is responsible for adjusting the pattern logic of existing scenarios and employs data mining techniques to create new patterns and scenarios.

   d. Flag of Y(es) or N(o) in the ACTV_FL column to specify whether the user is active.

   A sample SQL insert statement is:

   ```
   INSERT INTO KDD_USER VALUES ('KDD_MNR', 'KDD MINER', 'MNR', 'Y', 'FT');
   ```

To Grant a Database Role

To grant a database role to the Scenario Manager KDD_MNR user, follow the steps:

1. Access the KDD_USER_ROLE table.

   The following table defines the attributes in the KDD_USER_ROLE table.

Table 24. KDD_USER_ROLE Table Attributes

Column Name	Description
USER_ID	User's login ID.
USER_ROLE_CD	User's database role.

2. Enter the following information into the table using an SQL script:

   - User login ID in the USER_ID column.

   - User role MNR in the USER_ROLE_CD column.

   A sample SQL insert statement is:

   ```
   INSERT INTO KDD_USER_ROLE values ('KDD_MNR', 'MNR');
   ```

About Changing Passwords for System Accounts

Throughout the OFSBDF application there are several system accounts that may require changing the password for security purposes.

The following table summarizes the different system account passwords used by Oracle Financial Services Behavior Detection Framework, the subsystems that use those passwords, and instructions on how to change the passwords.

Table 25. System Account Passwords

System Account	Subsystem	Instructions
Data Ingest User (`INGEST_USER`)	Data Ingestion	1. Change the password in the database server for this user. 2. Use the Password Manager Utility to change the password in Oracle Financial Services Behavior Detection Framework to the new password.
Algorithm User (`KDD_ALG`)	Behavior Detection Services	1. Change the password in the database server for this user. 2. Use the Password Manager Utility to change the password in Oracle Financial Services Behavior Detection Framework to the new password.
data miner User (`KDD_MNR`)	Alert & Case Management Data Ingestion	1. Change the password in the database server for this user. 2. Use the Password Manager Utility to change the password in Oracle Financial Services Behavior Detection Framework to the new password.
Web Application User (`KDD_WEB`)	Alert & Case Management Services	1. Change the password in the database server for this user. 2. Use the Password Manager Utility to change the password in OFSBDF to the new password.
Behavior Detection Framework	Bdf	1. Execute `<INSTALL_DIR>/bdf/scripts/changePasswords.sh` to generate an encrypted version of the password. 2. Find the `<INSTALL_DIR>/bdf/config/custom/BDF.xml` with the encrypted password. Refer to the *Installation Guide* for more information. **Note:** Please note that for BDF does not use Password Management utility.
Reports User (`KDD_REPORT`)	OBIEE Reports	Open the `$OracleBI_HOME/server/Repository` and expand the Physical Layer. Open the Connection Pool and change the Password parameter to set a new value of the `KDD_REPORT` schema password. **Note**: OBIEE is an optional application.
Reg Reporting Service User	Alert & Case Management	1. Change the password in the Reg Reporting Service for this user. 2. Use the Password Manager Utility to change the password in OFSBDF to the new password by executing the following command: `<INSTALL_DIR>/changePasswords.sh rrs.password` **Note:** It is important that the password for RRS WebService and RRS are the same.

About 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 `CONFIGURATION` table of `OFSSAAI` configuration schema in its `PARAMVALUE` column where `PARAMNAME` is `DOCUMENT_ALLOWED_EXTENSION`.

About 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 & Attach button, follow these steps:

1. Open file `$FIC_HOME/EXEWebService/<WebSphere or Weblogic or Tomcat>/ROOT/conf/DynamicWSConfig.xml` and update

   From:

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

   To:

   `<PROPERTY NAME="MAXFILESIZE" VALUE="<desired value in bytes up to 10MB>"/>`

2. Then recreate `ExeWebservices ear` file and redeploy it.

3. Restart the web application server.

About Configuring Status To User Role Table

Within Watch List Management, each watch list and watch list entry (referred to as a "Watch List Member" on the Watch List Management UI) is assigned a status. In addition to the rules defined earlier in this chapter for accessing Watch List Management, OFS AM uses this status to limit user access to watch lists and watch list entries within the Watch List Management. For example. a WLM Supervisor user role can view "Active" watch lists and watch list entries only if the user role "WLM Supervisor" is mapped to status "Active". These mappings reside in the Status To User Role table and are applicable only to the Watch List Management. Each mapping of status to user role applies to both watch lists and watch list entries.

Mapping Status to Role in the Database through Scripts

You can create a Status to User Role mapping in the database by following these steps:

1. Add the appropriate record to the KDD_STATUS_ROLE database table, which Table 26 describes..

Table 26. KDD_STATUS_ROLE Table Attributes

Business Field	Column Name	Date Type	Definition	Null
Status Code	STATUS_CD	CHAR(3)	Status that can be accessed by the user role on this record.	Yes
User Role	USER_ROLE_CD	CHAR(50)	User role that is being assigned access to this status.	Yes

2. Add records to the table by using a SQL script similar to the sample script in Figure 72.

```
insert into kdd_status_role (status_cd,user_role_cd) values ('ACT','WLSUPVISR')

insert into kdd_status_role (status_cd,user_role_cd) values ('REJ','WLSUPVISR')
```

Figure 72. Sample SQL Script for Loading KDD_STATUS_ROLE

Note: The KDD_STATUS_ROLE table is pre populated after system initialization with the following records:

Table 27. KDD_STATUS_ROLE

STATUS_CD	USER_ROLE_CD
ACT	AMEXAUDITR
ACT	AMEXCUTIVE
ACT	AMINAUDITR
ACT	WLSUPVISR
DAC	WLSUPVISR

Configuring Alert and Case Management

The following section describes how to disable and enable Oracle Financial Services Alert Management:.

Enabling and Disabling Alert Management

This parameter allows the system to identify whether or not Alert Management Actions and Fields are to be displayed based on the deployment installation. The values to be provided for this parameter are Yes(Y) or No (N).

By default, the parameter is set to Y.

To modify this parameter, follow these steps:

1. Login as an OFS AM Admin User with valid username and password. You are navigated to the Home page.

2. Click **FCCM** and then click the **Administration** Menu and select **Manage Installation Parameter**.

3. Select **Deployment Based** in the Parameter category.

4. Select **Alert Management** from the Parameter Name drop-down list.

5. Edit the parameter.

6.

Index

U

Update button, 70, 103
Update Icon, 9
user authorization, 130
User Group and User Roles, 126
user name, 129
users
    access control, 132
    authorization model, 130
    case type/subtype, 129
    jurisdiction, 129
    KDD_USER table, 141
    name, 129
    organization, 129
    roles, 129
    scenario group, 129

W

wizard pages, 25
    Associated Data, 31
    Focus Selection, 30
    Highlights, 33
    Home, 25
    Review & Save, 50
    Scenario Overview, 27
    Test Scenario, 51
    Threshold Sets, 46
    Thresholds, 40

Index