Oracle® Financial Services

Administrator Tools User Guide

Release 8.1.2.11.0
G52586-01
February 2026

Oracle Financial Services Administrator Tools User Guide, Release 8.1.2.11.0

G52586-01

Contents

List of Figures

List of Tables

Document Control

This topic lists the changes that have been made to this guide in each release.

Table Revision History

Edition	Date	Description
February 2026	First edition of 8.1.2.11.0	There are no content changes to this guide in this release. The look and feel of the document has been updated.
August 2025	First edition of 8.1.2.10.0	There are no content changes to this guide in this release. The look and feel of the document has been updated.
February 2025	First edition of 8.1.2.9.0	There are no content changes to this guide in this release. The look and feel of the document has been updated.
August 2024	First edition of 8.1.2.8.0	There are no content changes to this guide in this release.
February 2024	First edition of 8.1.2.7.0	There are no content changes to this guide in this release.
October 2023	First edition of 8.1.2.6.0	Removed references and content related to the Scenario Wizard utility.
June 2023	First edition of 8.1.2.5.0	There are no content changes to this guide in this release.
March 2023	First edition of 8.1.2.4.0	Added note to Chapter 3, *Scenario Threshold Editor* to provide guidance on testing scenarios in the threshold editor.
December 2022	First edition of 8.1.2.3.0	There are no content changes to this guide in this release.
September 2022	First edition of 8.1.2.2.0	There are no content changes to this guide in this release.
June 2022	First edition of 8.1.2.1.0	Added note to Chapter 7, *Alert Assigner Editor* to provide configuration steps for parameters which may not load automatically during installation.
March 2022	First edition of 8.1.2.0.0	There are no content changes to this guide in this release. Only the version and the release month is updated.

About This Guide

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

Audience

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Resources

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

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

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

About Financial Crimes and Compliance Management

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.

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.

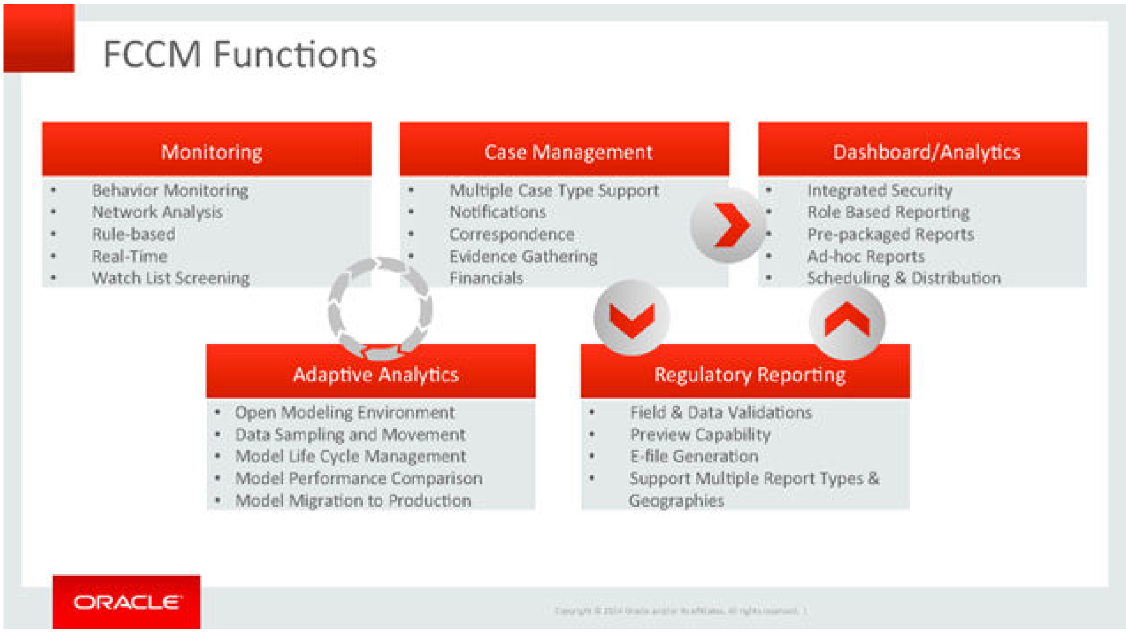
- Oracle Financial Services Currency Transaction Reporting (CTR) analyzes transaction data from the organization and identifies any suspicious activities within the institution that may lead to fraud or money laundering and must be reported to the regulatory authorities. Currency Transaction Reports (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 and Fraud 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).
- 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 Behavior Detection and Know Your Customer, 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.

Figure 1-1 Functions



FCCM Functions

Monitoring
- Behavior Monitoring
- Network Analysis
- Rule-based
- Real-Time
- Watch List Screening

Case Management
- Multiple Case Type Support
- Notifications
- Correspondence
- Evidence Gathering
- Financials

Dashboard/Analytics
- Integrated Security
- Role Based Reporting
- Pre-packaged Reports
- Ad-hoc Reports
- Scheduling & Distribution

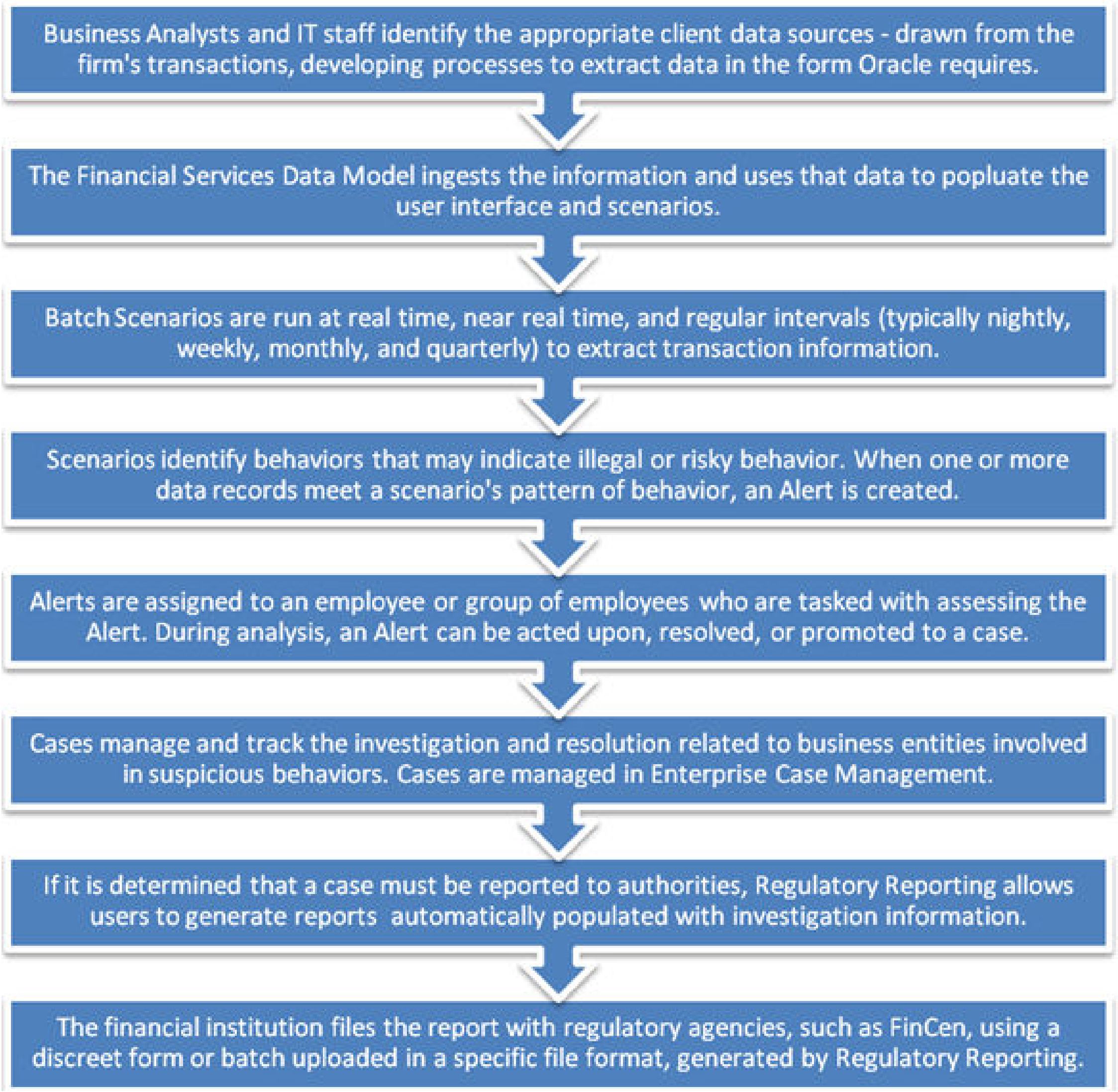
Adaptive Analytics
- Open Modeling Environment
- Data Sampling and Movement
- Model Life Cycle Management
- Model Performance Comparison
- Model Migration to Production

Regulatory Reporting
- Field & Data Validations
- Preview Capability
- E-file Generation
- Support Multiple Report Types & Geographies

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.

Figure 1-2 Workflow



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.

2 About the Administration Tools

Administration Tools are used to configure alert and case generation.

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.
- 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.
- Alert Scoring Editor: This tool is used for creating new rules or modify the logic behind existing rules that prioritize alerts automatically.
- Alert Assigner Editor: This tool is used for assigning ownership of alerts.
- 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.

This topic details the following actions:

- Accessing the Administration Tools
- Using Common Screen Elements
- Logging off of the Administration Tools
- Saving Changes to a Log File

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
- Users assigned to the Administrator role can access the following:
  - User Administration
  - Security Attribute
  - Administration
  - Alert Creator Editor
  - Alert Scoring Editor
  - Alert Assigner Editor

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

2.1 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.

3

Scenario Threshold Editor

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:

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

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. 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:

For more information about scenarios, refer to the respective *Technical Scenario Description* document (for example, for anti-money laundering scenario information, refer to the Anti-Money Laundering Technical Scenario Descriptions).

> **Note**
>
> To test the scenario in the Threshold Editor, run the AAI server using the following command:
>
> ```
> Path:"$FIC_HOME/ficdb/bin" ./agentstartup.sh
> ```

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 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 Mutually Exclusive Thresholds and Additional Scenario Thresholds groups of thresholds can have values set to *Inactive*.

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. The following table shows how mutually exclusive thresholds work in two different situations.

Table 3-1 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.

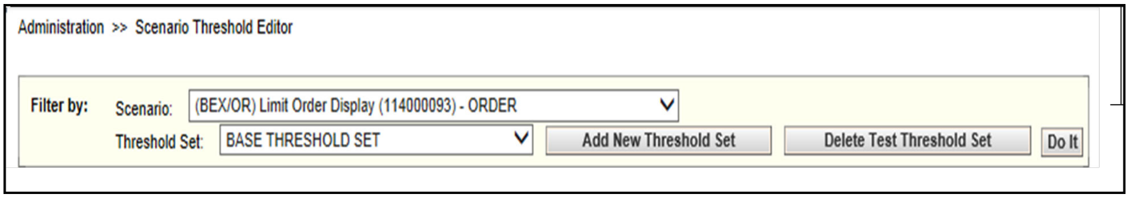
3.1 Scenario Threshold Editor Screen Elements

The Search Bar and <Scenario–Threshold Set> Area screen elements display in the Scenario Threshold Editor.

Search Bar

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

Figure 3-1 Search Bar



Administration >> Scenario Threshold Editor

Filter by: Scenario: (BEX/OR) Limit Order Display (114000093) - ORDER

Threshold Set: BASE THRESHOLD SET

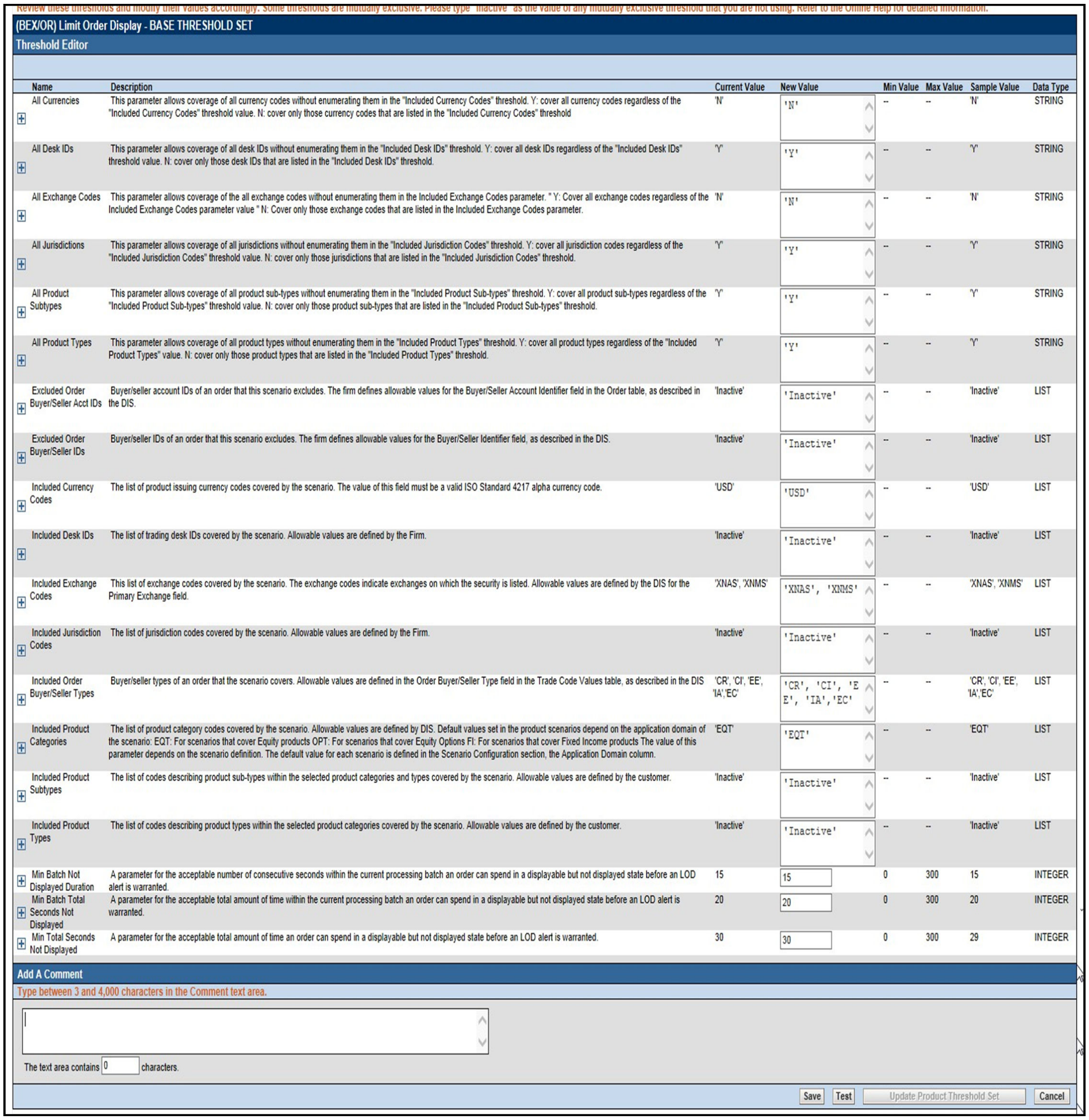
The components of the search bar includes the following:

- **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. This list displays after you select a scenario and threshold set in the search bar and click **Do It**.

Figure 3-2 <Scenario-Threshold Set> Area



Review these thresholds and modify their values accordingly. Some thresholds are mutually exclusive. Please type "Inactive" as the value of any mutually exclusive threshold that you are not using. Refer to the Online Help for detailed information.

(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.

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

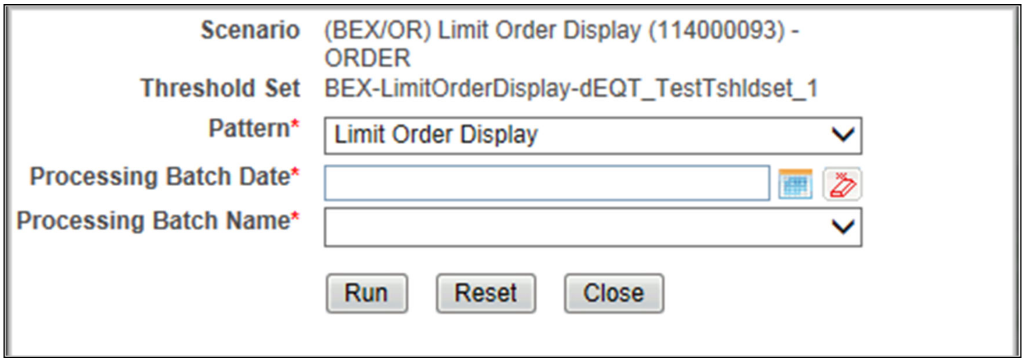
- Long name of the scenario and the name of the threshold set in the title of the <Scenario-Threshold Set> bar.
- List of scenario thresholds by threshold name, sorted in ascending alphabetical order.
- Threshold information as follows:
  - **Threshold History Icon**: Expands or contracts the Threshold 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, 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 *ScenarioTest Execution* pop-up window is displayed.

Figure 3-3 Scenario Test Execution window



Scenario (BEX/OR) Limit Order Display (114000093) - ORDER
Threshold Set BEX-LimitOrderDisplay-dEQT_TestTshldset_1
Pattern* Limit Order Display
Processing Batch Date*
Processing Batch Name*

The Scenario Test Execution window displays the following fields:

Table 3-2 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.

3.2 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, and 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

3.2.1 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**. The Add New Threshold Set pop-up window is displayed.
4. Enter the required details in the following fields:

Table 3-3 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 drop-down list 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 drop-down 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.*
Test Threshold Set	Select this checkbox if the threshold set created is a test threshold set or not. The threshold set name is available thresholdset name + _TST_datetimestamp.
New Threshold Set Name	By default, this field is kept blank. You can enter the threshold set name only when the *CreateTest Threshold Set* checkbox is not selected. When the user has selected the Test Threshold Set checkbox, then this text box is pre- populated with a value that has been selected from the available threshold sets along with a time stamp.

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

3.2.2 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**. The Threshold Set is deleted.

3.2.3 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.
5. **Optional:** Enter any comments in the **Add A Comment** text box.
6. Click **Save**. The new threshold values display in the Threshold List for <Scenario-Threshold Set>.

3.2.4 Bugs Fixed

This section describes the issues which were resolved in this release.

The following bugs have been addressed in OFS Behavior Detection Release 8.1.2.11.0.

Table 3-4 Resolved Issues

Component	Bug ID	Description
Scenario	38799071	Functional Currency highlights were added to ML-CIBPreviousAverageActivity-CU.
Scenario	38079181	Standard Deviation highlights were added to ML-CIBPreviousAverageActivity-CB
BD	37305606	Add missing BDF for ACCOUNTBALANCE.STG_MM_CONTRACTS.

3.2.5 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.

3.2.6 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.
2. Click **X** (Close button) on the top right corner to close the dialog box.

3.3 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.

The review scenario details page contains the following screen elements:

- Search Bar

- Search and List Grid

Search Bar

Table 3-5 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 • Canceled

Search and List Grid

The search results are displayed in the Search and List grid. This grid displays the following columns:

Table 3-6 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.

Table 3-6 (Cont.) Search and List Grid Components

Field	Description
Batch Status	This field displays the batch status. Following is the batch status: • Running • Finished • Error • Canceled
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>_MatchedDetails.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.

The **Purge** action button is available on the *Search and List* grid. When clicked, this button purges all the matches that are generated for the selected scenario and threshold set combination.

4

Alert Creator Editor

The Alert Creator Editor administration tool is used 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

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.

4.1 Alert Creator Editor Screen Elements

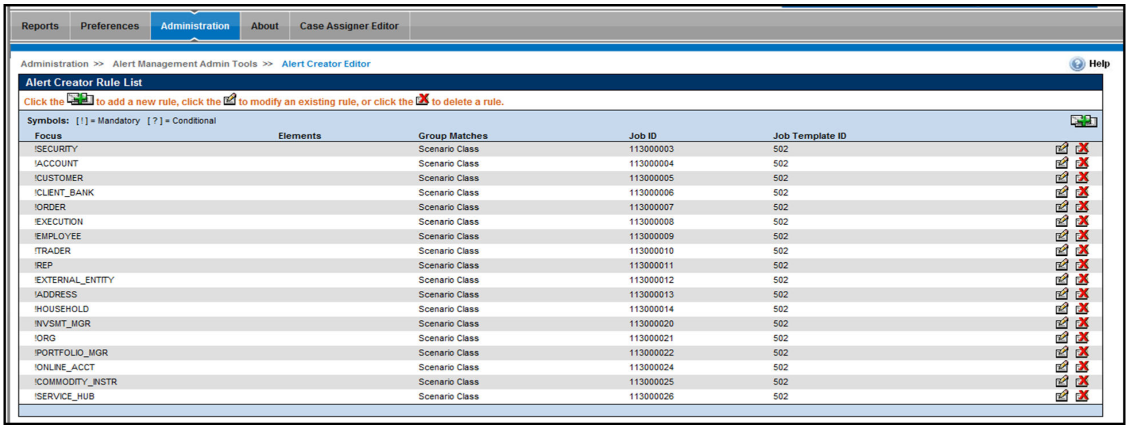
The Alert Creator Editor contains the Alert Creator Rule List, which displays when you access the Alert Creator Editor and the Alert Creator Rule Editor.

This topic describes the 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.
- Alert Creator Rule Editor: This page enables you to add or modify a rule.

Alert Creator Rule List

Figure 4-1 Alert Creator Rule List



Reports
Preferences
Administration
About
Case Assigner Editor
Administration >> Alert Management Admin Tools >> Alert Creator Editor
Help

Alert Creator Rule List

Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule.

Symbols: [!] = Mandatory [?] = Conditional

Focus	Elements	Group Matches	Job ID	Job Template ID
!SECURITY		Scenario Class	113000003	502
!ACCOUNT		Scenario Class	113000004	502
!CUSTOMER		Scenario Class	113000005	502
!CLIENT_BANK		Scenario Class	113000006	502
!ORDER		Scenario Class	113000007	502
!EXECUTION		Scenario Class	113000008	502
!EMPLOYEE		Scenario Class	113000009	502
!TRADER		Scenario Class	113000010	502
!REP		Scenario Class	113000011	502
!EXTERNAL_ENTITY		Scenario Class	113000012	502
!ADDRESS		Scenario Class	113000013	502
!HOUSEHOLD		Scenario Class	113000014	502
!NVSMT_MGR		Scenario Class	113000020	502
!ORG		Scenario Class	113000021	502
!PORTFOLIO_MGR		Scenario Class	113000022	502
!ONLINE_ACCT		Scenario Class	113000024	502
!COMMODITY_INSTR		Scenario Class	113000025	502
!SERVICE_HUB		Scenario Class	113000026	502

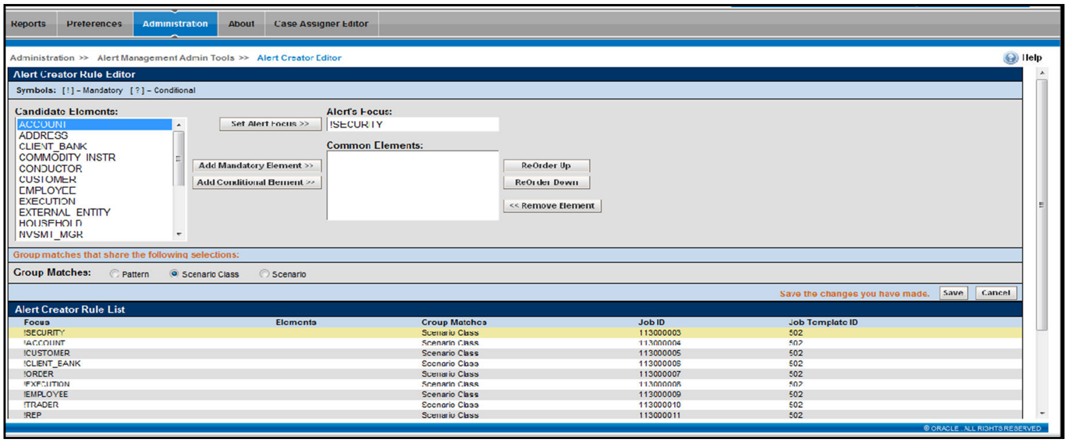
The Alert Creator Rule List displays all rules sorted by Focus, Elements, and then Group Matches, with the following columns of information:

- 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.

Alert Creator Rule Editor

From the Alert Creator Rule Editor, you can create a new rule or update an existing rule.

Figure 4-2   Alert Creator Rule Editor



Symbols: [!] – Mandatory [?] – Conditional

Candidate Elements: ACCOUNT, ADDRESS, CLIENT_BANK, COMMODITY_INSTR, CONDUCTOR, CUSTOMER, EMPLOYEE, EXECUTION, EXTERNAL_ENTITY, HOUSEHOLD, INVSMT_MGR

Alert's Focus: !SECURITY

Common Elements:

Group matches that share the following selections:

Group Matches: ○ Pattern ● Scenario Class ○ Scenario

Save the changes you have made.

Alert Creator Rule List

Focus	Elements	Group Matches	Job ID	Job Template ID
!SECURITY		Scenario Class	113000003	502
!ACCOUNT		Scenario Class	113000004	502
!CUSTOMER		Scenario Class	113000005	502
!CLIENT_BANK		Scenario Class	113000006	502
!ORDER		Scenario Class	113000007	502
!EXECUTION		Scenario Class	113000008	502
!EMPLOYEE		Scenario Class	113000009	502
!TRADER		Scenario Class	113000010	502
!REP		Scenario Class	113000011	502

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).

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: This button does the following actions.
  - 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: This button does the following actions.
  - 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: This button does the following actions.
  - 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.
- **ReOrderUp** button: Reorders the sequence of the displayed common elements by shifting the selected value above the preceding value.
- **ReOrderDown** button: Reorders the sequence of the displayed common elements by shifting the selected value below the following value.
- **Remove Element** button: This button does the following actions.
  - 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.

4.2 Using the Alert Creator Editor

You can perform the following functions using the Alert Creator Editor: Adding a Rule, Modifying a Rule, and Deleting a Rule.

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

- Adding a Rule
- Modifying a Rule
- Deleting a Rule

4.2.1 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.

4.2.2 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.

4.2.3 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.

5

Alert Scoring Editor

Use the Alert Scoring Editor administration tool to create new rules or modify the logic behind existing rules that prioritize alerts automatically.

This chapter contains the following topics :

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.

5.1 Scoring Match Strategies

Match scoring computes the score for individual matches to provide an initial prioritization.

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

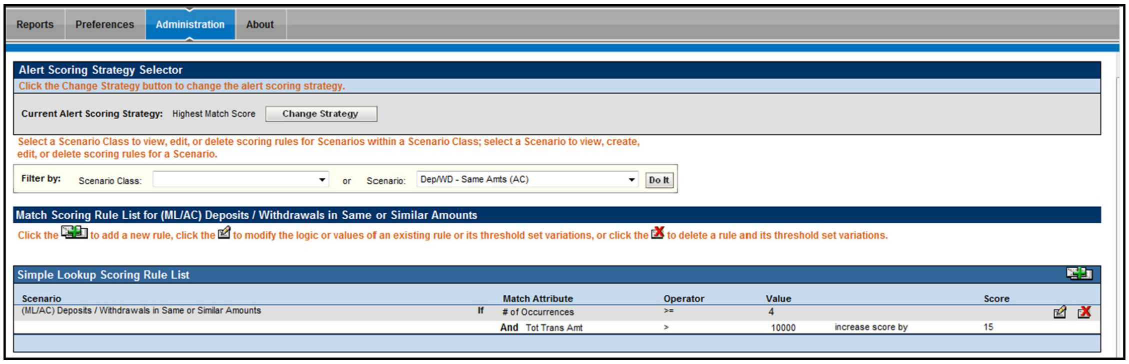
  Scoring Tier 3, Transaction Amount is between 10,0000 USD to USD 20,000 score is 40

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.

5.2 Alert Scoring Editor

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

Figure 5-1 Alert Scoring Editor



Alert Scoring Strategy Selector

Click the Change Strategy button to change the alert scoring strategy.

Current Alert Scoring Strategy: Highest Match Score

Select a Scenario Class to view, edit, or delete scoring rules for Scenarios within a Scenario Class; select a Scenario to view, create, edit, or delete scoring rules for a Scenario.

Filter by: Scenario Class: or Scenario: Dep/WD - Same Amts (AC)

Match Scoring Rule List for (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Click the to add a new rule, click the to modify the logic or values of an existing rule or its threshold set variations, or click the to delete a rule and its threshold set variations.

Simple Lookup Scoring Rule List

Scenario		Match Attribute	Operator	Value		Score
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If	# of Occurrences	>=	4		
	And	Tot Trans Amt	>	10000	increase score by	15

The Alert Scoring Editor includes the following components:

- Alert Scoring Strategy Selector
- Search Bar

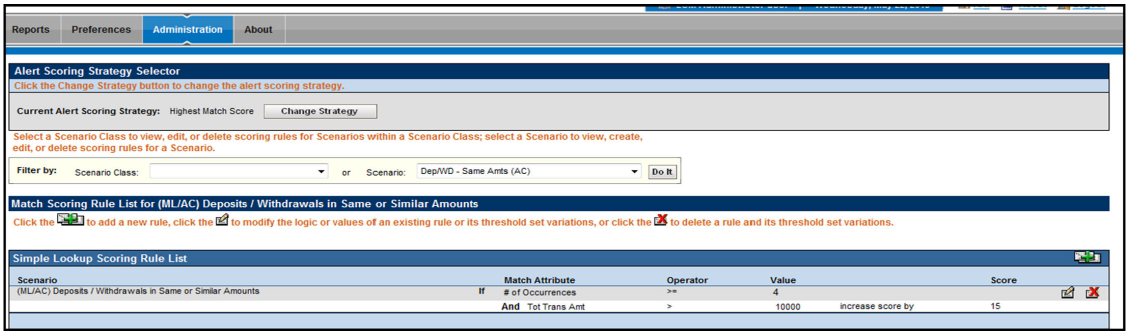
- Alert Scoring Strategy Selector with Match Scoring Rule Lists

The following sections describe these components.

Alert Scoring Strategy Selector

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

Figure 5-2 Alert Scoring Strategy Selector



Alert Scoring Strategy Selector

Click the Change Strategy button to change the alert scoring strategy.

Current Alert Scoring Strategy: Highest Match Score [Change Strategy]

Select a Scenario Class to view, edit, or delete scoring rules for Scenarios within a Scenario Class; select a Scenario to view, create, edit, or delete scoring rules for a Scenario.

Filter by: Scenario Class: or Scenario: Dep/WD - Same Amts (AC) [Do It]

Match Scoring Rule List for (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Click the to add a new rule, click the to modify the logic or values of an existing rule or its threshold set variations, or click the to delete a rule and its threshold set variations.

Simple Lookup Scoring Rule List

Scenario		Match Attribute	Operator	Value		Score
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If	# of Occurrences	>=	4		
	And	Tot Trans Amt	>	10000	increase score by	15

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.

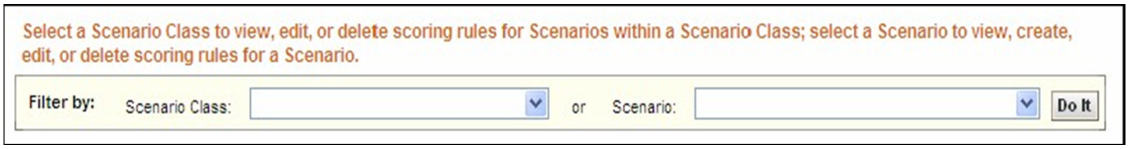
> **Note**
>
> If you change the scoring strategy, a confirmation dialog box displays prompting you to confirm the change. Click **OK** to continue and save the new strategy.

- **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 5-3 Alert Scoring Editor Search Bar



Select a Scenario Class to view, edit, or delete scoring rules for Scenarios within a Scenario Class; select a Scenario to view, create, edit, or delete scoring rules for a Scenario.

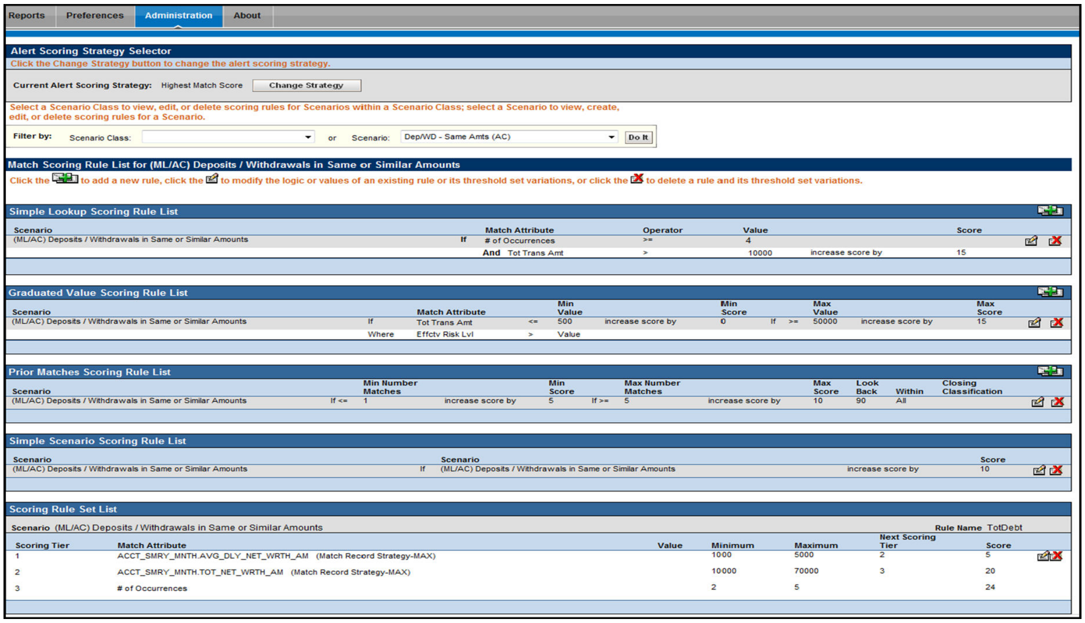
Components of the search bar include the following:

- **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 5-4 Alert Scoring Strategy Selector - Match Scoring Rule List



Alert Scoring Strategy Selector

Click the Change Strategy button to change the alert scoring strategy.

Current Alert Scoring Strategy: Highest Match Score

Select a Scenario Class to view, edit, or delete scoring rules for Scenarios within a Scenario Class; select a Scenario to view, create, edit, or delete scoring rules for a Scenario.

Filter by: Scenario Class: or Scenario: Dep/WD - Same Amts (AC)

Match Scoring Rule List for (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Click the to add a new rule, click the to modify the logic or values of an existing rule or its threshold set variations, or click the to delete a rule and its threshold set variations.

Simple Lookup Scoring Rule List

Scenario		Match Attribute	Operator	Value		Score
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If	# of Occurrences	>=	4		
	And	Tot Trans Amt	>	10000	increase score by	15

Graduated Value Scoring Rule List

Scenario		Match Attribute		Min Value		Min Score			Max Value		Max Score
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If	Tot Trans Amt	<=	500	increase score by	0	If	>=	50000	increase score by	15
	Where	Effctv Risk Lvl	>	Value							

Prior Matches Scoring Rule List

Scenario		Min Number Matches		Min Score		Max Number Matches		Max Score	Look Back	Within	Closing Classification
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If <=	1	increase score by	5	If >=	5	increase score by	10	90	All	

Simple Scenario Scoring Rule List

Scenario		Scenario		Score
(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	If	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	increase score by	10

Scoring Rule Set List

Scenario (ML/AC) Deposits / Withdrawals in Same or Similar Amounts Rule Name TotDebt

Scoring Tier	Match Attribute	Value	Minimum	Maximum	Next Scoring Tier	Score
1	ACCT_SMRY_MNTH.AVG_DLY_NET_WRTH_AM (Match Record Strategy-MAX)		1000	5000	2	5
2	ACCT_SMRY_MNTH.TOT_NET_WRTH_AM (Match Record Strategy-MAX)		10000	70000	3	20
3	# of Occurrences		2	5		24

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.
  - 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.
  - 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.
  - Simple Scenario Scoring Rule List: Displays the Scenario (within rule text) and Score columns for each base scoring rule.
  - Scoring Rule Set: Displays the scoring rule set for a particular scenario.
- **Add** button: Navigates you to the associated Match Scoring Rule Editor.

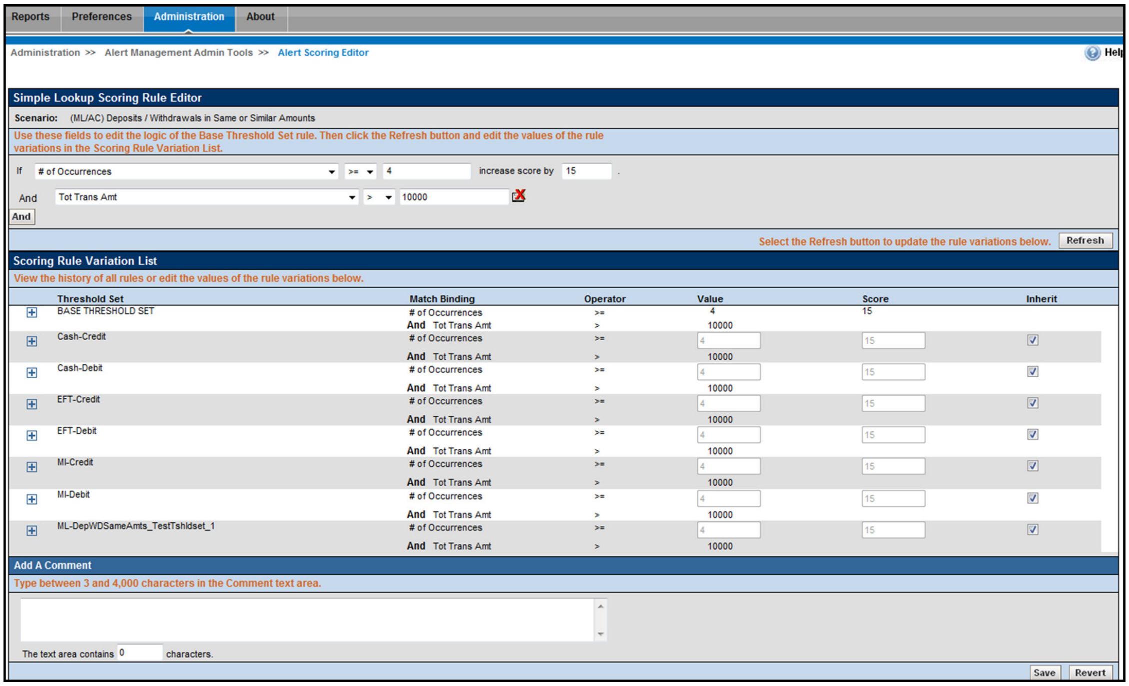
> **Note**
>
> The Add button is available only if you select an option in the Scenario drop-down list.

- **Update** button: Navigates you to the associated Alert Scoring Editor.
- **Delete** button:Deletes the match scoring rule

5.2.1 Scoring Rule Variation List

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

Figure 5-5   Expanded Rule Modification History



Administration >> Alert Management Admin Tools >> Alert Scoring Editor

Simple Lookup Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.

If # of Occurrences >= 4 increase score by 15 .

And Tot Trans Amt > 10000

Select the Refresh button to update the rule variations below.

Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

	Threshold Set	Match Binding	Operator	Value	Score	Inherit
⊞	BASE THRESHOLD SET	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	
⊞	Cash-Credit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	Cash-Debit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	EFT-Credit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	EFT-Debit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	MI-Credit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	MI-Debit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	ML-DepWDSameAmts_TestTshldset_1	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑

Add A Comment

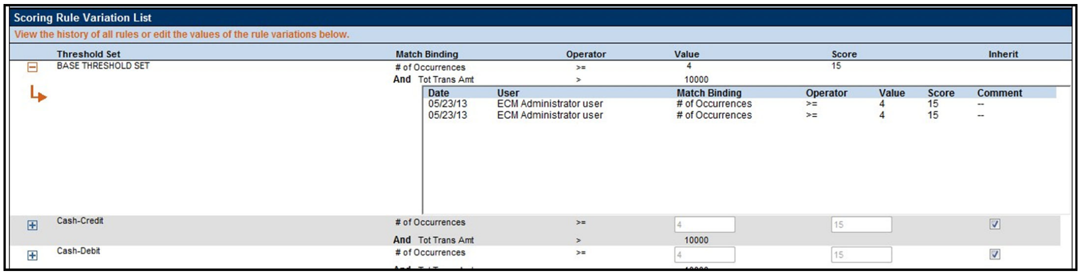
Type between 3 and 4,000 characters in the Comment text area.

The text area contains 0 characters.

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 5-6   Expanded Rule Modification History

  Scoring Rule Variation List

  View the history of all rules or edit the values of the rule variations below.

	Threshold Set	Match Binding	Operator	Value	Score	Inherit
⊟	BASE THRESHOLD SET	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	
⊞	Cash-Credit	# of Occurrences And Tot Trans Amt	>= >	4 10000	15	☑
⊞	Cash-Debit	# of Occurrences	>=	4	15	☑

Date	User	Match Binding	Operator	Value	Score	Comment
05/23/13	ECM Administrator user	# of Occurrences	>=	4	15	--
05/23/13	ECM Administrator user	# of Occurrences	>=	4	15	--

  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.

5.3 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.

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

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:

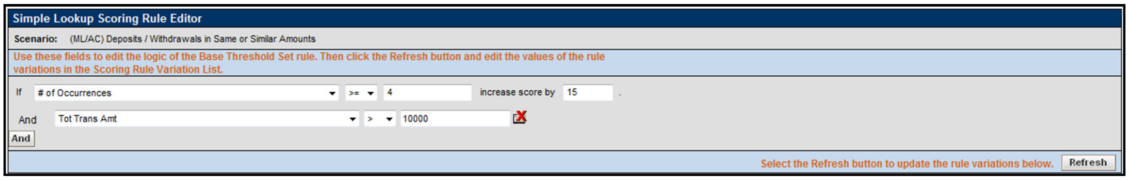
  Rule1: If the value is greater than 10,000,000, then add negative 50 (-50) to the **Score**field.

  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 5-7 Match Attribute Scoring Rule Modification



Simple Lookup Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.

If # of Occurrences >= 4 increase score by 15 .

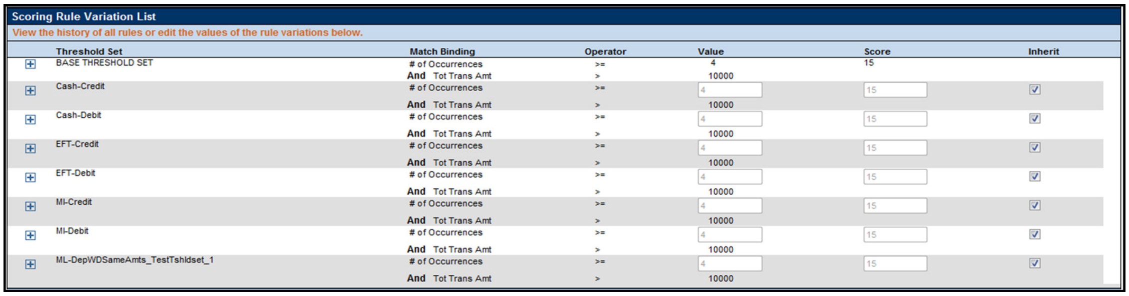
And Tot Trans Amt > 10000

And

Select the Refresh button to update the rule variations below. Refresh

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

Figure 5-8 Scoring Rule Variation List by Scenario



Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

	Threshold Set	Match Binding	Operator	Value	Score	Inherit
⊞	BASE THRESHOLD SET	# of Occurrences	>=	4	15	
		And Tot Trans Amt	>	10000		
⊞	Cash-Credit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	Cash-Debit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	EFT-Credit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	EFT-Debit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	MI-Credit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	MI-Debit	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		
⊞	ML-DepWDSameAmts_TestTshldset_1	# of Occurrences	>=	4	15	☑
		And Tot Trans Amt	>	10000		

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 and Simple Scoring Rule Editor Components 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.

5.4 Graduated Value Scoring Rule Editor

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.

The Graduated Value Scoring Rule Editor displays after clicking Add or Update in the Graduated Value Scoring Rule List.

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

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.

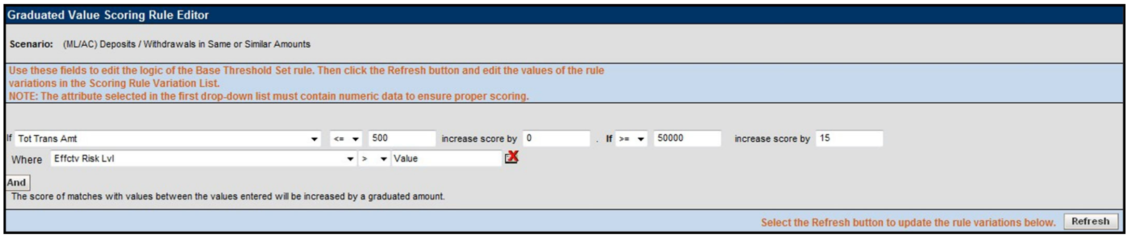
  If you select **Update**, the Max Score text box displays the current maximum score entry for the selected rule.

  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 5-9 Match Attribute Scoring Rule Modification



Graduated Value Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.
NOTE: The attribute selected in the first drop-down list must contain numeric data to ensure proper scoring.

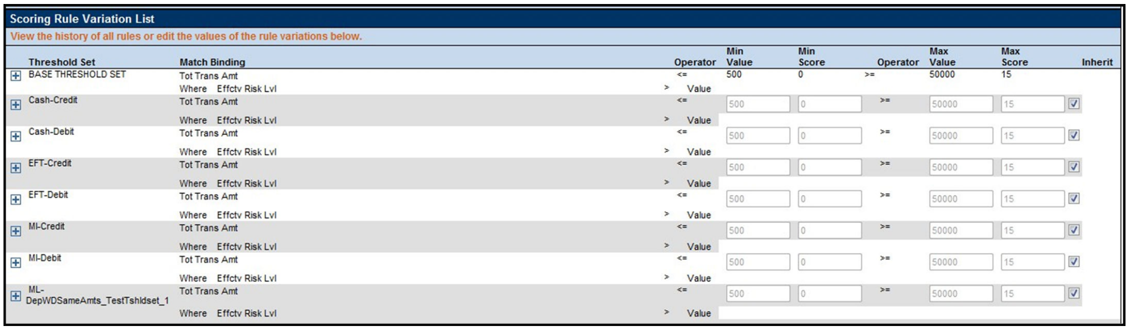
If Tot Trans Amt <= 500 increase score by 0 . If >= 50000 increase score by 15
Where Effctv Risk Lvl > Value

The score of matches with values between the values entered will be increased by a graduated amount.

Select the Refresh button to update the rule variations below.

When you enter values in the **MinValue**, **MinScore**, **MaxValue**, and **Max Score** fields and click **Save**, the Scoring Rule Variation List displays.

Figure 5-10 Graduated Value Scoring Rule Variation List by Scenario



Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

Threshold Set	Match Binding	Operator	Min Value	Min Score	Operator	Max Value	Max Score	Inherit
BASE THRESHOLD SET	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	
Cash-Credit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
Cash-Debit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
EFT-Credit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
EFT-Debit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
MI-Credit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
MI-Debit	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑
ML-DepWDSameAmts_TestTshldset_1	Tot Trans Amt Where Effctv Risk Lvl	<= >	500 Value	0	>=	50000	15	☑

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 and Graduated Value Scoring Rule Editor provides description of most components in the Scoring Rule Variation List. The Graduated Value Scoring Rule Editor also contains the following buttons:

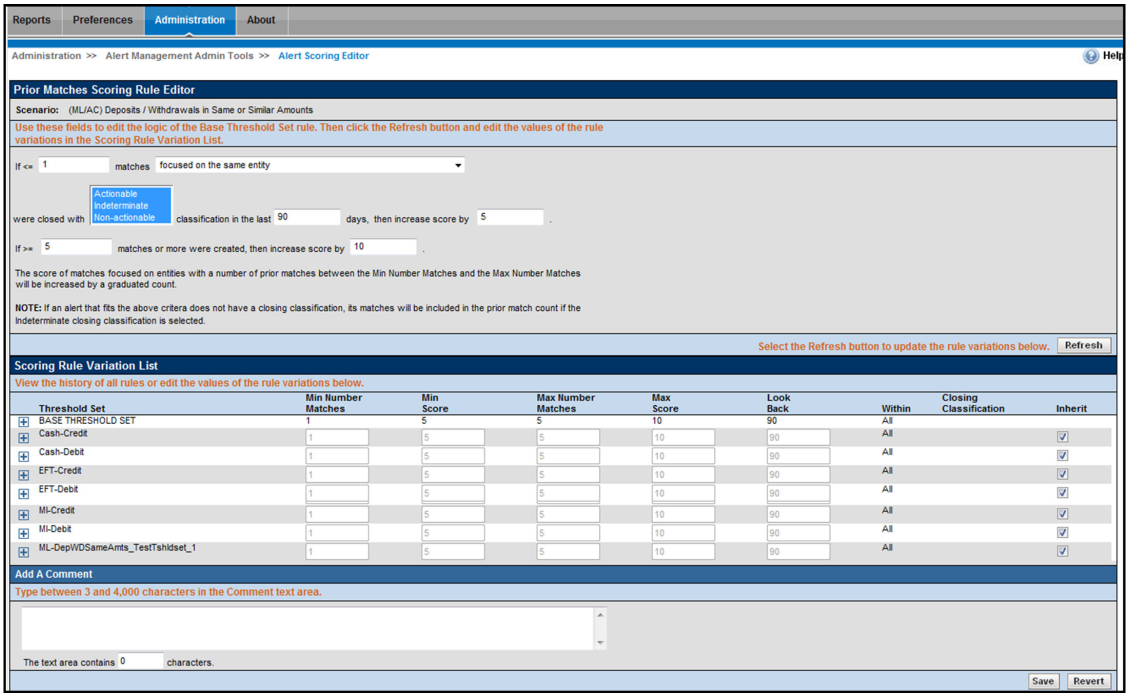
- **And:**Allows you to add new filters for a rule. If at any time you want to remove a filter already associated to a rule, click the Remove button available for each of the filter rows.
- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which 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.

5.5 Prior Matches Scoring Rule Editor

The Prior Matches Scoring Rule Editor 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 5-11   Prior Matches Scoring Rule Editor


Reports
Preferences
Administration
About
Administration >> Alert Management Admin Tools >> Alert Scoring Editor
Help
Refresh
Save
Revert

Prior Matches Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.

If <= 1 matches focused on the same entity

were closed with Actionable / Indeterminate / Non-actionable classification in the last 90 days, then increase score by 5 .

If >= 5 matches or more were created, then increase score by 10 .

The score of matches focused on entities with a number of prior matches between the Min Number Matches and the Max Number Matches will be increased by a graduated count.

NOTE: If an alert that fits the above critera does not have a closing classification, its matches will be included in the prior match count if the Indeterminate closing classification is selected.

Select the Refresh button to update the rule variations below.

Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

	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		☑

Add A Comment

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

The text area contains 0 characters.

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

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.

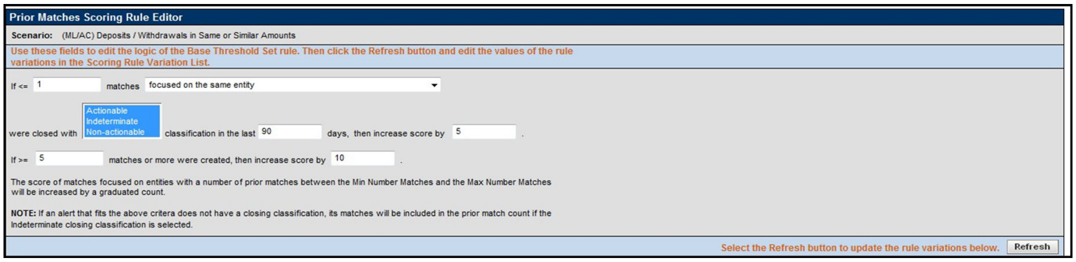
  If you select **Update**, the Max Score text box displays the current maximum score entry for the selected rule.

  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 5-12   Prior Matches Scoring Rule Modification



Prior Matches Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.

If <= 1 matches focused on the same entity

were closed with Actionable Indeterminate Non-actionable classification in the last 90 days, then increase score by 5 .

If >= 5 matches or more were created, then increase score by 10 .

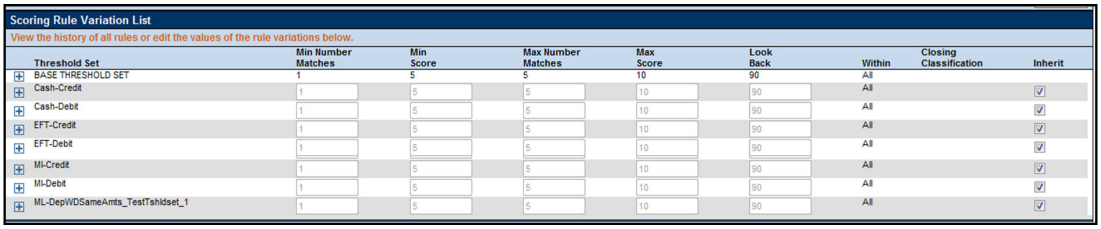
The score of matches focused on entities with a number of prior matches between the Min Number Matches and the Max Number Matches will be increased by a graduated count.

NOTE: If an alert that fits the above critera does not have a closing classification, its matches will be included in the prior match count if the Indeterminate closing classification is selected.

Select the Refresh button to update the rule variations below.

When you enter values in the Rule Editor fields (**Min Number Matches**, **Same Scenario**, **Alert ClosingClassification**, **LookBack Days**, **MinScore**, **MaxNumber Matches**, and **MaxScore**) and click **Save**, the Prior Matches Scoring Rule Variation List displays.

Figure 5-13   Prior Matches Scoring Rule Variation List by Scenario



Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

	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		☑

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

- 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 and Prior Matches Scoring Rule Editor provides description of most components in the Scoring Rule Variation List. The Prior Match Scoring Rule Editor also contains the following buttons:

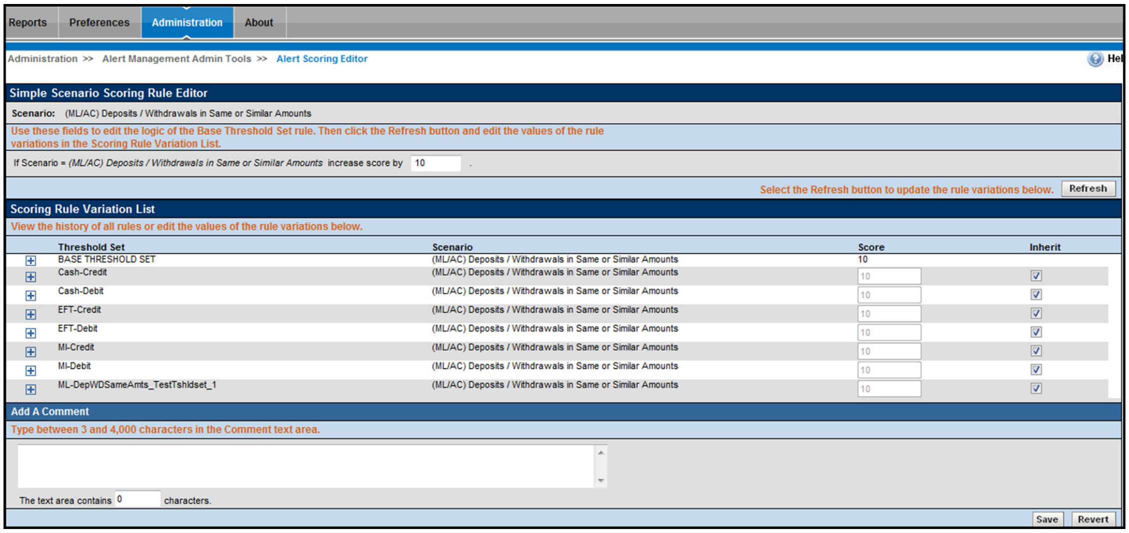
- **And:**Allows you to add new filters for a rule. If at any time you want to remove a filter already associated to a rule, click the Remove button available for each of the filter rows.
- **Refresh**: Updates changes to rules in the Scoring Rule Variation List based on the base rule (and for which 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.

5.6 Simple Scenario Scoring Rule Editor

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.

The Simple Scenario Scoring Rule Editor displays after clicking Add or Update in the Simple Scenario Scoring Rule List when you filter by scenario.

Figure 5-14 Simple Scenario Scoring Rule Editor



Administration >> Alert Management Admin Tools >> Alert Scoring Editor

Simple Scenario Scoring Rule Editor

Scenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

Use these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule variations in the Scoring Rule Variation List.

If Scenario = *(ML/AC) Deposits / Withdrawals in Same or Similar Amounts* increase score by 10 .

Select the Refresh button to update the rule variations below. Refresh

Scoring Rule Variation List

View the history of all rules or edit the values of the rule variations below.

	Threshold Set	Scenario	Score	Inherit
⊞	BASE THRESHOLD SET	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	
⊞	Cash-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	Cash-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	EFT-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	EFT-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	MI-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	MI-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	ML-DepWDSameAmts_TestTshldset_1	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑

Add A Comment

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

The text area contains 0 characters.

Save Revert

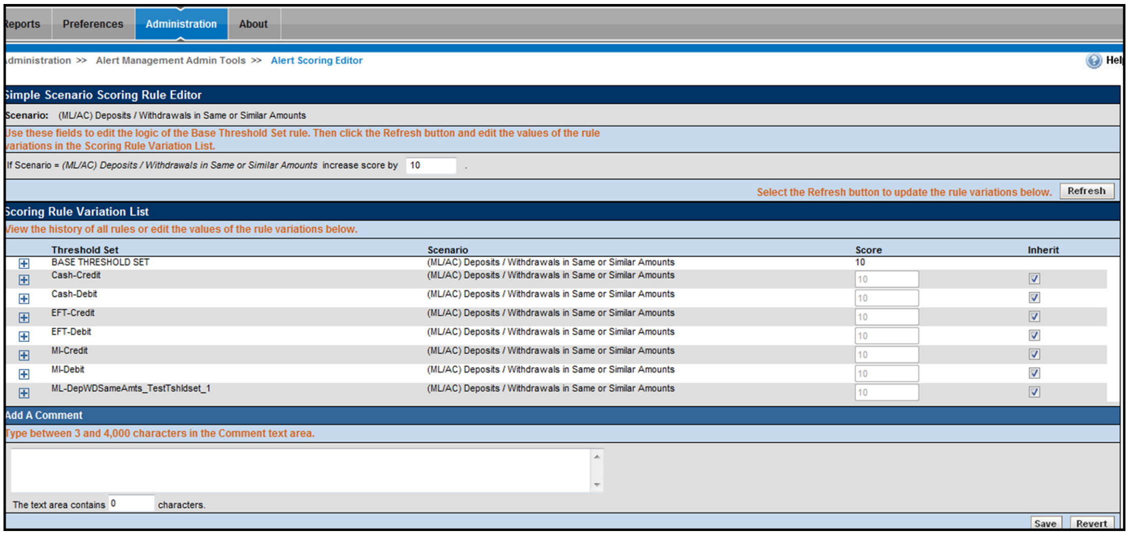
Note

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.

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

Figure 5-15 Simple Scenario Scoring Rule Variation List by Scenario



dministration >> Alert Management Admin Tools >> Alert Scoring Editor

imple Scenario Scoring Rule Editor

cenario: (ML/AC) Deposits / Withdrawals in Same or Similar Amounts

se these fields to edit the logic of the Base Threshold Set rule. Then click the Refresh button and edit the values of the rule ariations in the Scoring Rule Variation List.

If Scenario = *(ML/AC) Deposits / Withdrawals in Same or Similar Amounts* increase score by 10 .

Select the Refresh button to update the rule variations below. Refresh

coring Rule Variation List

iew the history of all rules or edit the values of the rule variations below.

	Threshold Set	Scenario	Score	Inherit
⊞	BASE THRESHOLD SET	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	
⊞	Cash-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	Cash-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	EFT-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	EFT-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	MI-Credit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	MI-Debit	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑
⊞	ML-DepWDSameAmts_TestTshldset_1	(ML/AC) Deposits / Withdrawals in Same or Similar Amounts	10	☑

dd A Comment

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

The text area contains 0 characters.

Save Revert

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

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 and Simple Scenario Scoring Rule Editor 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.

5.7 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
  - Using the Simple Lookup Scoring Editor for a Scenario Class
  - Using the Simple Lookup Scoring Editor for a Scenario
- Graduated Value Scoring Rule Editor
  - Using the Graduated Value Scoring Editor for a Scenario Class
  - Using the Graduated Value Scoring Editor for a Scenario
- Prior Matches Scoring Rule Editor
  - Using the Prior Matches Scoring Editor for a Scenario Class
  - Using the Prior Matches Scoring Editor for a Scenario
- Simple Scenario Scoring Rule Editor
  - Using the Simple Scenario Scoring Editor for a Scenario Class
  - Using the Simple Scenario Scoring Editor for a Scenario
- Scoring Rule Set

  - Using the Scoring Rule Set Editor for a Scenario

Using the Alert Scoring Strategy Selector, you can also view and change the alert scoring strategy for your deployment.

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 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

5.7.1 Modifying a Simple Lookup Scoring Rule for a Scenario Class

In the Simple Lookup Scoring Editor, you can modify or delete a 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.
3. Click the **And** button if you wish to add multiple filters for a rule.
4. 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.
5. **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.

6. **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.
7. 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.

5.7.2 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. 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

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 **UpdateRule** next to the selected rule.
2. The Simple Lookup Scoring Editor displays with the rule's current values in the text boxes.
3. Modify the binding description in the Match Attribute drop-down list.

4. 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.
5. *Optional:*Inthe 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.
6. *Optional:*Type a comment about a rule logic update in the **Adda 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.
7. 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**.
   - 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
   - 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

5.7.3 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.

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 **UpdateRule** 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 **MinValue, Max Value, Min Score, and Max Score** text boxes.
3. Click the **And**button if you wish to add multiple filters for a rule.
4. 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.
5. *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.
6. *Optional:*Type a comment about a rule logic update in the **Adda 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.
7. 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.

5.7.4 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.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

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 **MinValue**, **MaxValue**, **MinScore**, and **MaxScore** 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 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.
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 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.

5.7.5 Using the Prior Matches Scoring Editor for a Scenario Class

In the Prior Matches Scoring Editor, you can modify a rule for a Scenario Class.

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 **UpdateRule** 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 **MinNumber 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 **MaxScore** 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.
4. *Optional:*Inthe 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.
5. *Optional:*Type a comment about a rule logic update in the **Adda 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.
6. 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.

5.7.6 Using the Prior Matches Scoring Editor for a Scenario

In the Prior Matches Scoring Editor, you can modify a rule for an individual Scenario as you would for a Scenario Class. 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

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 **MinNumber Matches** text box.
3. Select the desired attribute in the Same Scenario drop-down list.
4. Type a numeric value in the **LookBack Days**, **MinScore**, **MaxNumber Matches**, and **MaxScore** 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.
2. Modify a rule for a particular Threshold Set in the Scoring Rule Variation List. Refer to Specifying a Variation for Threshold Set Within a Scenariofor 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.

5.7.7 Using the Simple Scenario Scoring Editor for a Scenario Class

In the Simple Scenario Scoring Editor, you can modify a rule for a Scenario Class.

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.
4. *Optional:*Inthe 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.
5. *Optional:*Type a comment about a rule logic update in the **Adda Comment** text box. Enter from 3 to 4,000 characters. Acount in the numeric field below the Add a Comment field tracks the current number of characters in the comment area.

6. 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**.
7. 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.

5.7.8 Using the Simple Scenario Scoring Editor for a Scenario

In the Simple Scenario Scoring Editor, you can modify a rule for an individual Scenario as you would for a Scenario Class. 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

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.
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 for information about using the Scoring Rule Variation List.
3. Click **Save**.

5.7.9 Using the Scoring Rule Set Editor for a Scenario

In the Scoring Rule Set Editor, you can modify 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

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 **UpdateRule** 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 **ScoringTier** text box.
   - Modify the value in the **MatchAttribute** drop-down list.
   - Modify the value in the **MatchRecord 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.
4. *Optional:*Inthe 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.
5. *Optional:*Type a comment about a rule logic update in the **Adda 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.
6. Click **Save**to save your changes. Ifyou 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.

5.7.10 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.

5.7.11 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.

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.
3. *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.
4. Click **Save**.

5.7.12 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.

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.

6 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.

Yo ucan 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.
  The following table shows a sample of an alert assignment rule.

Table 6-1 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 6-1 (Cont.) 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**
>
> 1. Manually posted alerts, generated by the alert correlation process, are not assigned to the default owner that is specified through the assignment editor. Refer to the *Behavior Detection Administration Guide*, for more information.
> 2. The following attributes of the Admin Tools and Alert Owner Parameters fail to load automatically during installation and must be manually updated:
>   - Attribute 1 Value
>   - Attribute 4 Value
>   - Attribute 5 Value
>   - Attribute 8 Value
>   To update the Attribute 1 Alert Owner parameter in the Manage Common Parameters page, select the Used for Design parameter category and the Alert Owner parameter name.
>
>   To update the Attribute 4, Attribute 5, and Attribute 8 Admin Tools parameters in the Manage Common Parameters page, select the Used for Design parameter category and the Admin Tools parameter name

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.

6.1 Alert Assigner Screen Elements

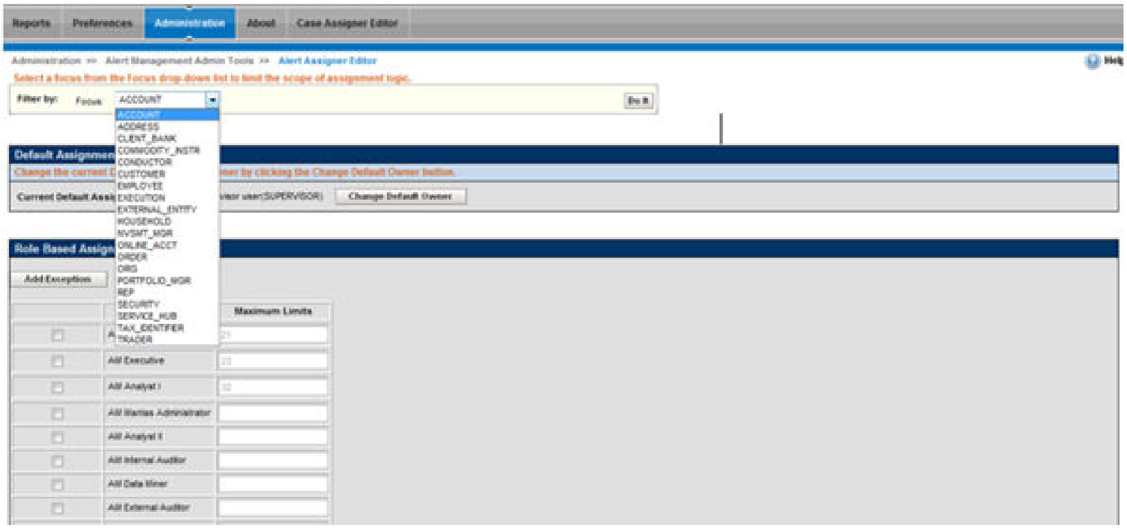
The following pages are associated with the Alert Assigner Editor:

- **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.
- **Assignment Rule List for <Focus> Focus:** This page enables you to create a new rule or modify an existing rule.
- **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.

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 6-1   Alert Assigner Editor



Select a focus from the Focus drop-down list to limit the scope of assignment logic.

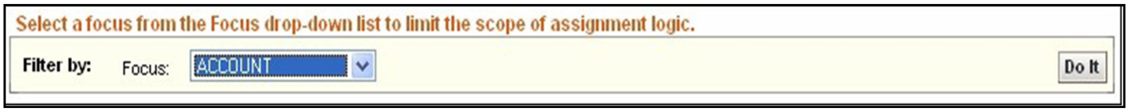
The components of the Alert Assigner Editor include the following:

- 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 6-2   Alert Assigner Editor Search Bar



Select a focus from the Focus drop-down list to limit the scope of assignment logic.

The components of the search bar include the following:

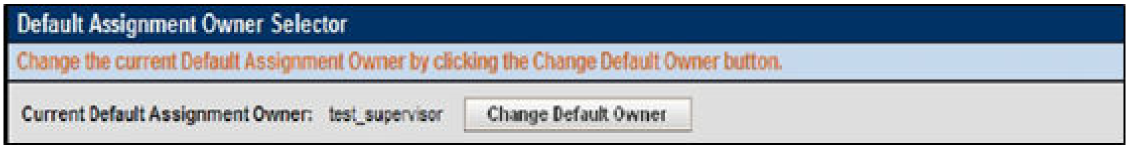
- **Filter by:** Focus drop-down list: Provides a list of focus types. The values in the Focus drop-down list are sorted in ascending alphabetic order.
- **Do It button**: When clicked, displays the assignment rules associated with the selected focus.

Default Assignment Owner Selector

The Default Assignment Owner Selector page allows you to change the default owner for alerts.

> **Note**
>
> Ensure that the new default owner has permission to view all alerts.

Figure 6-3 Default Assignment Owner Selector



Default Assignment Owner Selector

Change the current Default Assignment Owner by clicking the Change Default Owner button.

Current Default Assignment Owner: test_supervisor

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.

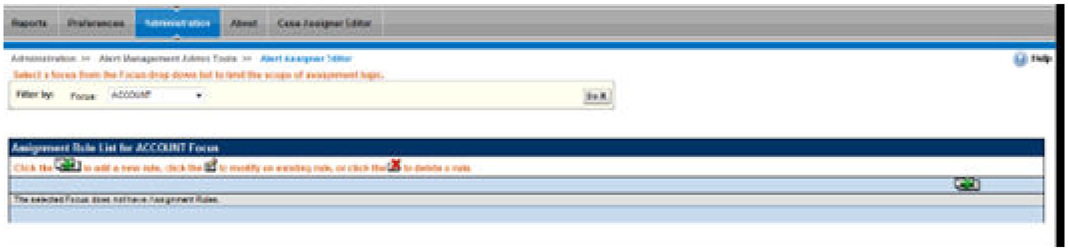
> **Note**
>
> To change the default assignment owner, refer to Changing the Default Assignment Owner.

- **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 6-4 Assignment Rule List for <Focus> Focus



Reports
Preferences
Administration
About
Case Assigner Editor
Administration >> Alert Management Admin Tools >> Alert Assigner Editor
Help

Select a focus from the Focus drop down list to limit the scope of assignment logic.

Filter by: Focus: ACCOUNT

Assignment Rule List for ACCOUNT Focus

Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule.

The selected Focus does not have Assignment Rules.

The Assignment Rule List for <Focus> Focus includes the following components:

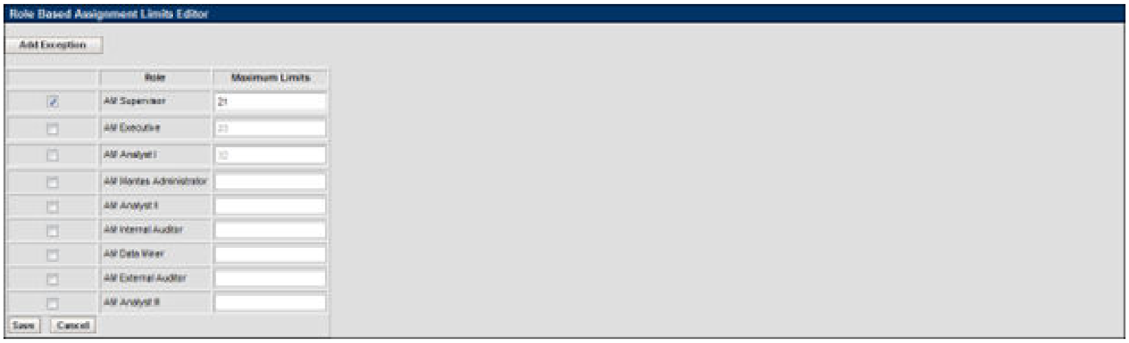
- **Addbutton**: Navigates you to the Assignment Rule Editor.
- **Updatebutton**: Navigates you to the Assignment Rule Editor.
- **Deletebutton**: Deletes the assignment rule.
- **Assignment Rule List for <Focus> Focus** page displays the column headings: Operation Set, Attribute, Operator, Value, Next Operation Set, Strategy, and Owner. Refer to Assignment Rule Editor 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 assignedonly 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 6-5 Role Based Assignment Limits Editor



	Role	Maximum Limits
☑	AM Supervisor	21
□	AM Executive	23
□	AM Analyst I	32
□	AM Mantas Administrator	
□	AM Analyst II	
□	AM Internal Auditor	
□	AM Data Miner	
□	AM External Auditor	
□	AM Analyst III	

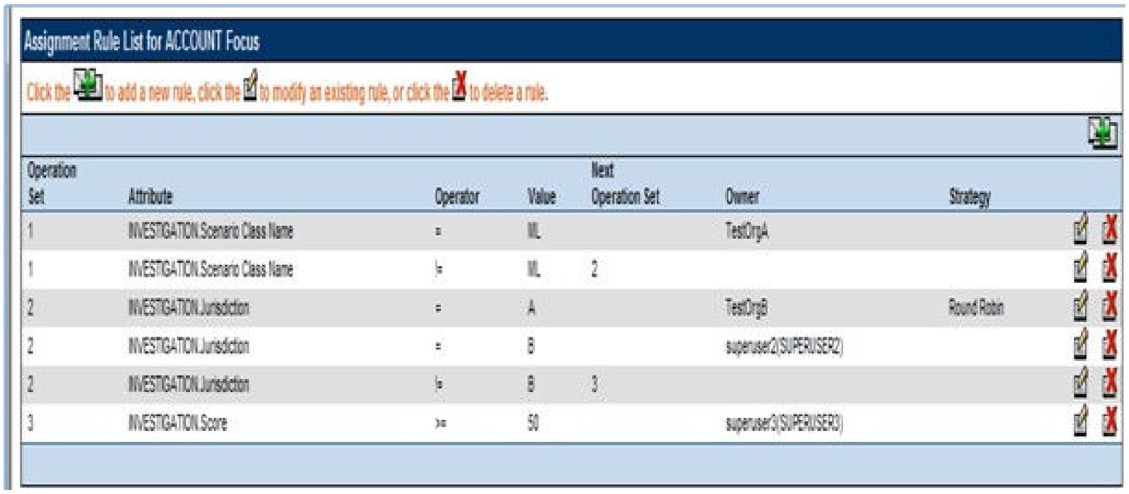
The Role Based Assignment Limits Editor includes the following components:

- **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 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**. 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 6-6 Assignment Rule Editor



Assignment Rule List for ACCOUNT Focus

Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule.

Operation Set	Attribute	Operator	Value	Next Operation Set	Owner	Strategy
1	INVESTIGATION.Scenario Class Name	=	ML		TestOrgA	
1	INVESTIGATION.Scenario Class Name	!=	ML	2		
2	INVESTIGATION.Jurisdiction	=	A		TestOrgB	Round Robin
2	INVESTIGATION.Jurisdiction	=	B		superuser2(SUPERUSER2)	
2	INVESTIGATION.Jurisdiction	!=	B	3		
3	INVESTIGATION.Score	>=	50		superuser3(SUPERUSER3)	

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 **InvestigationAttribute** 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.
  - **NextOperation 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 **NextOperation Set** text box displays a blank value (“ ”) (the default).

  - If you select **Update**, the **NextOperation 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 **RoundRobin**, alerts are assigned to the members of a pool in a circular order until all the alerts have been assigned.
  - If you select **LoadLeveling**, 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.

6.2 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
- Modifying an Exception
- Deleting an Exception

6.2.1 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.*

6.2.2 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.
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.

6.2.3 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.
3. 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.
4. 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.
5. 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.
6. Type a value in the **Value** text box. Depending on the attribute, this value can be a numeric or a text string.
7. 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.

8. If you selected a pool in the Owner drop-down list, select a strategy for alert assignment from the Strategy drop-down list.
9. 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.

6.2.4 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**.

   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.

6.2.5 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.

6.2.6 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.

6.2.7 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 drop-down 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.
7. (Required) <Enter the first step.>

   (Optional) <Enter a step example.>
8. <Enter the next step.>

   (Optional) <Enter additional information about the step.>
9. <Enter the next step.>
   - (Optional) <Enter one of the user's choices while performing this step.>
   - (Optional) <Enter another of the user's choices while performing this step.>
10. <Enter the next step.>
    a. (Optional) <Enter a substep.>
    b. (Optional) <Enter a substep.>

6.2.8 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.

6.2.9 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.

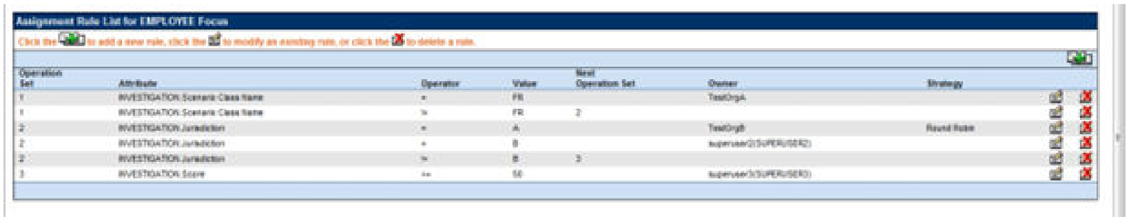
6.3 Example of an Alert Assignment

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 6-7 Example 1



Assignment Rule List for EMPLOYEE Focus

Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule.

Operation Set	Attribute	Operator	Value	Next Operation Set	Owner	Strategy
1	INVESTIGATION.Scenario Class Name	=	FR		TestOrgA	
1	INVESTIGATION.Scenario Class Name	!=	FR	2		
2	INVESTIGATION.Jurisdiction	=	A		TestOrgB	Round Robin
2	INVESTIGATION.Jurisdiction	=	B		superuser2(SUPERUSER2)	
2	INVESTIGATION.Jurisdiction	!=	B	3		
3	INVESTIGATION.Score	>=	50		superuser3(SUPERUSER3)	

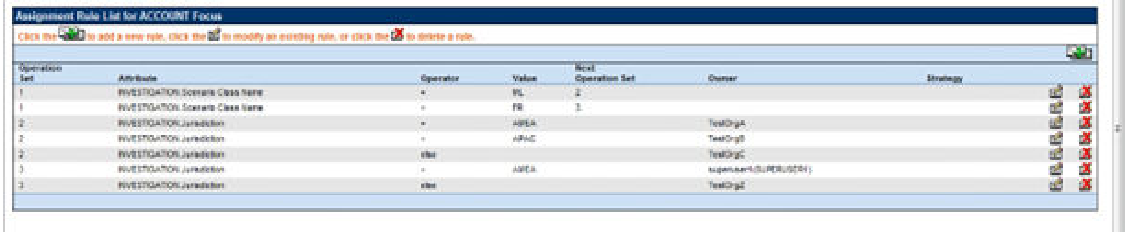
The rules set up in this figure reflect the following logic and use of operations sets.

- 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 6-8   Example 2



Assignment Rule List for ACCOUNT Focus

Click the to add a new rule, click the to modify an existing rule, or click the to delete a rule.

Operation Set	Attribute	Operator	Value	Next Operation Set	Owner	Strategy		
1	INVESTIGATION.Scenario Class Name	=	ML	2				
1	INVESTIGATION.Scenario Class Name	=	FR	3				
2	INVESTIGATION.Jurisdiction	=	AMEA		TestOrgA			
2	INVESTIGATION.Jurisdiction	=	APAC		TestOrgB			
2	INVESTIGATION.Jurisdiction	else			TestOrgC			
3	INVESTIGATION.Jurisdiction	=	AMEA		superuser1(SUPERUSER1)			
3	INVESTIGATION.Jurisdiction	else			TestOrgZ			

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.

7

Scenario Tuning

The Scenario Tuning utility leverages decisions made by analysts on past alerts to help tune the scenarios and their thresholds going forward.

This chapter introduces you to the Scenario Tuning utility and describes how you can view and operate the source business and Scenario Tuning 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.

The Scenario Tuning utility leverages decisions made by analysts on past alerts to help tune the scenarios andtheir 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 Scenario Tuning 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 Scenario Tuning 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 Scenario Tuning utility is accessed via a separate URL. Contact your System Administrator for the exact Web address to be used.

7.1 Getting Started

To access Scenario Tuning 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.

7.2 Homepage Options

The default Hompage which displays upon login is dependent on your user role.

To navigate to the Scenario Tuning application, select the **Scenario Tuning** 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.

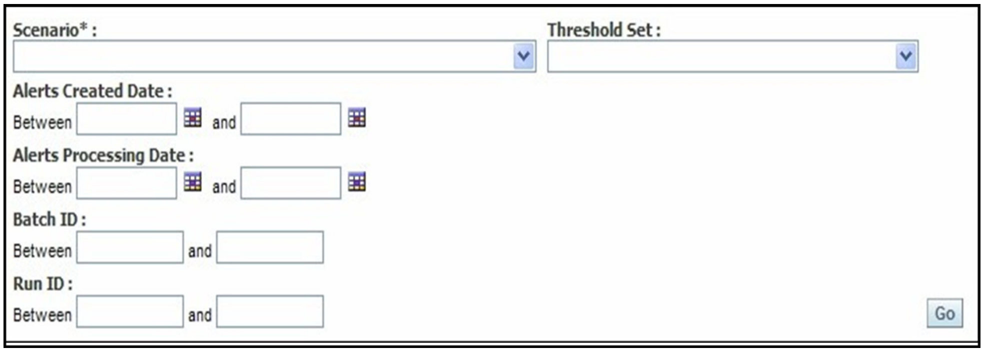
- When the User is an Administrator: Users with administrator or data miner roles will default to the Scenario Tuning Report. If you have logged out from the Answers page, the next time you login you are directly taken to the Answers page.
- When the User is not an Administrator: If you are not an Administrator, the Homepage is always the dashboard.
  On login, if dashboard is displayed as home page, you can see four dashboards–AML, Fraud, Productivity, and Scenario Tuning. By default, the dashboard seen is AML.

  Click **Scenario Tuning** to view the Scenario Tuning dashboard. Here, you can see a tab for each scenario class for which scenarios have been installed. For example, 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 Scenario Tuning 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 7-1 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.

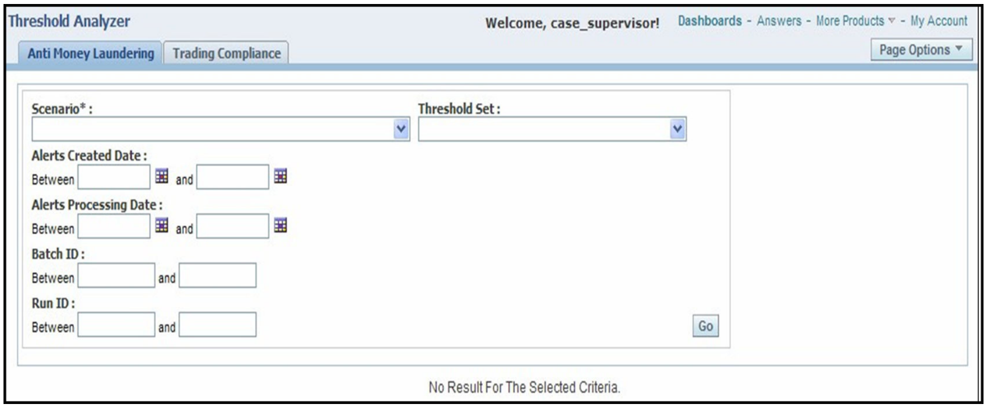
The from date should always be less than the to date. Data must be in the MM/DD/YYYY format. By default, the date fields are blank.
If you enter only a from date, keeping the to date blank, the system fetches the data based on where the alert created date is greater than or equal to the given date. Similarly, 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 Scenario Tuning Report

By default, the Scenario Tuning reports are not displayed upon login and the page shows the *No Result For The Selected Criteria* message.

Figure 7-2 Default Page



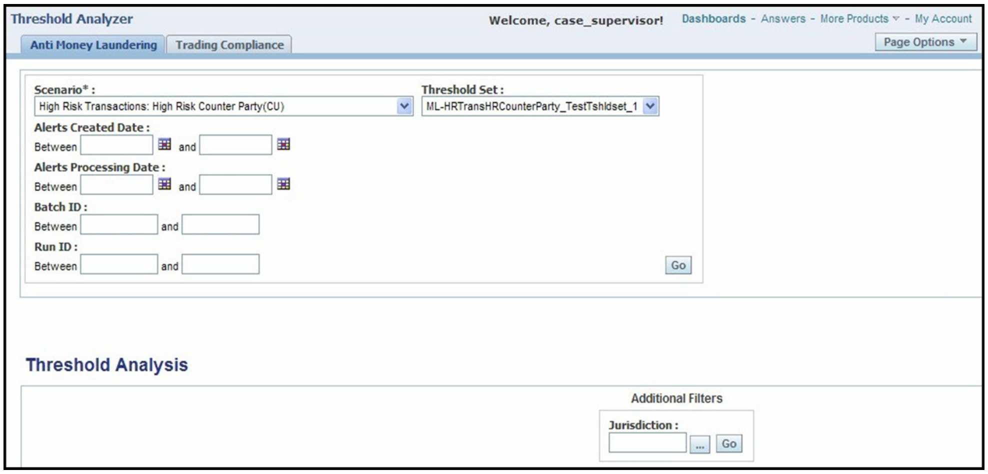
No Result For The Selected Criteria.

To view the report, enter search values in your desired filters and click **Go**. The Additional Filters selection section opens and the Scenario Tuning scatter graph statistical reports and their associated graphs open. For information about understanding graph display, see Understanding the Graph Display.

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 7-3 Additional Filter

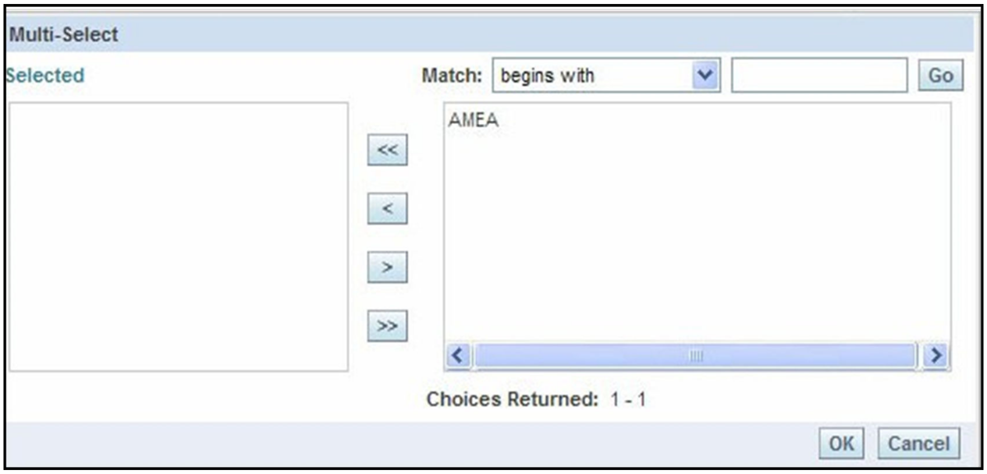


Scenario* : High Risk Transactions: High Risk Counter Party(CU)

Threshold Set : ML-HRTransHRCounterParty_TestTshldset_1

To specify a value for use as an additional filter, click on the ellipsis icon (…) next to the filter to open a multi-select box.

Figure 7-4 Additional Filter with Value



Match: begins with

AMEA

Choices Returned: 1 - 1

Follow these steps:

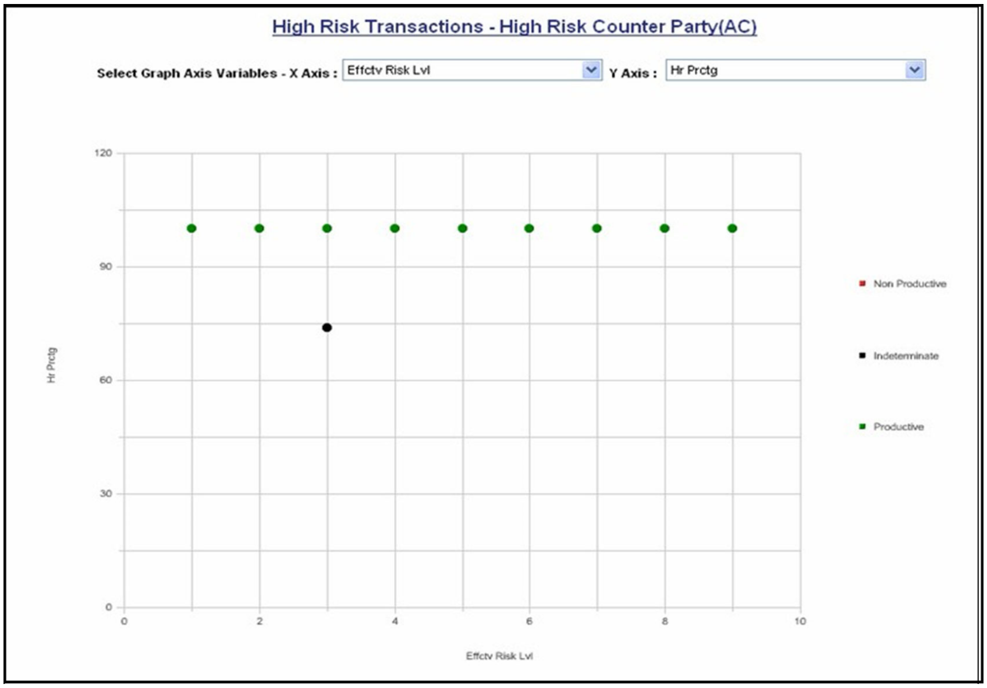
- Select one or more desired filter values from the list of available values in the right hand list of the selection box. Move the selected filter values from the right hand list to the left using .
- To filter by all possible values, click **Move All** to move all values into the Selected list.
- To remove a filter value from the Selected list, select the filter value and click **Move**. To remove all values from the Selected list click **Move All**.
- 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.
- 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.
- 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

Thescatter 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. The following figure shows the axis selection drop-down.

Figure 7-5 Axis Selection


High Risk Transactions - High Risk Counter Party(AC)
Select Graph Axis Variables - X Axis : Effctv Risk Lvl
Y Axis : Hr Prctg
120
90
60
30
0
Hr Prctg
0
2
4
6
8
10
Effctv Risk Lvl
Non Productive
Indeterminate
Productive

7.3 Understanding the Graph Display

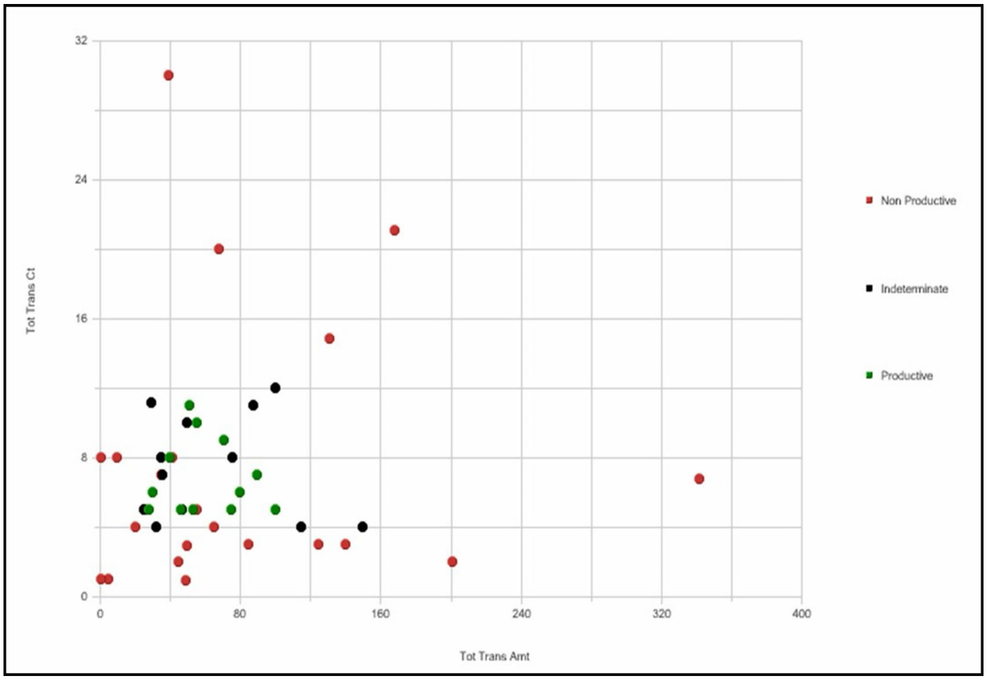
The scatter graph uses dots of differing colors to represent the quality rating of individual matches.

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, Scenario Tuning 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 *TotTrans Amt* and the *TotTrans Ct* actually involved in, and bound by, the match. The following figure shows an example of a scatter graph.

Figure 7-6   Scatter Graph



How to Interpret Results

There are 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 the Scatter Graph, 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

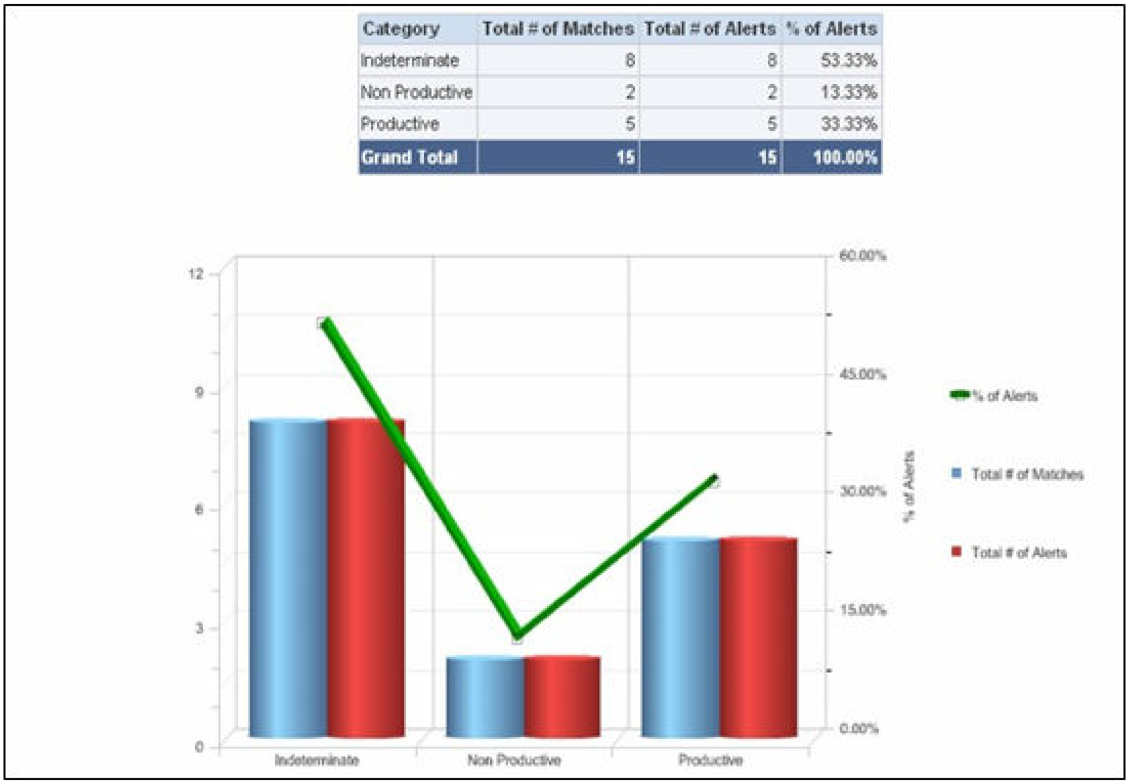
The summary counts display results in a tabular and line-bar combo graph. The tabular report shows the total number of matches, total number of alerts, and the percentage of the total number of alerts that is represented in each quality category. The Grand Total is calculated as the sum of matches across 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 shown below, 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.

Figure 7-7   Summary Counts



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%**

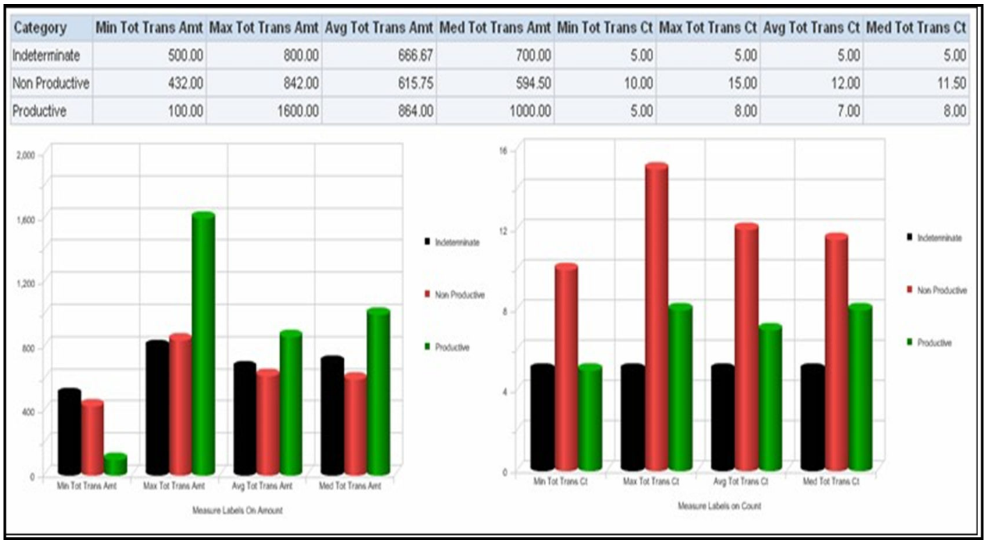
Understanding the Minimum, Maximum, Average and Median Statistics

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 7-8 Minimum, Maximum, Average, and Median Statistics



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

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.

8

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:

8.1 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.

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.

8.2 User Setup

This topic tells how to set up a user and provide the user access.

To set up a user and provide the user access to OFS AM, follow these 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 User Group and User Roles more information on User Roles and User Groups. Refer to the *Oracle Financial Services Analytical Applications Infrastructure User Manual* for further information.

Note

When creating a new User Group, you must set precedence as **5001** or greater. Different solutions have different pre-defined/pre-occupied precedence of User Groups. Therefore, if a BD Admin/System Admin is creating a new User Group, do not use the following precedence while providing precedence value:

Table 8-1 Solution with Pre-defined Precedence Range

Solution	Precedence Range Already Occupied
Oracle Financial Services Enterprise Case Management	901 to 1000
Oracle Financial Services Know Your Customer	2001 to 3000
Oracle Financial Services Enterprise Regulatory Reporting	3001 to 4000

For more information about the pre-defined user groups for each solution, see the appropriate Administration Guide.

8.2.1 Managing User Groups

The following sections describe how to manage User Groups.

Defining User Group Maintenance Details

For more information on defining user group maintenance details, see *Identity Management* in the *Oracle Financial Services Analytical Applications Infrastructure User Guide* .

Adding New User Group Details

For more information on adding new user group details, see *Identity Management* in the *Oracle Financial Services Analytical Applications Infrastructure User Guide* .

Mapping Users to User Groups

When mapping users to user groups, consider the following:

- One user can also be used against multiple roles. If multiple roles are allocated to a single user, then the availability of actions depends on the Four Eyes approval option. If Four Eyes approval is off, then the user can take all actions available by the allocated roles, with no duplicates. If Four Eyes approval is on, then action linked to a role that does not require Four Eyes approval takes precedence if there is a conflict.
- Users will have read-only access to Alert if they have been mapped to the ALERTVIEWERGRP user group. Other user groups such as Supervisor, Analyst, Auditor, Executive groups will not be given access to Alert Viewer.

For more information on mapping users to user group, see *Identity Management* in the *Oracle Financial Services Analytical Applications Infrastructure User Guide* .

Mapping a User to a Single User Group

If a user has only one role then that user can be mapped to a single User Group associated with that User Role. For more information on mapping a user to a single user group, see

Identity Management in the *Oracle Financial Services Analytical Applications Infrastructure User Guide* .

Mapping a User to Multiple User Groups

If a user has more than one role within FCCM (that is, within both Alert Viewer and Enterprise Case Management), then the user must be mapped to the different User Groups associated with the corresponding role. When the user logs into FCCM, the user access permissions are the union of access and permissions across all roles.

Mapping a Function to a Role

Functions must be mapped to appropriate Alert and Case User Roles through Function-Role Map function, which is available in the Security Management System, by logging in as the System Administrator in the OFSAAI toolkit. All Alert Viewer 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.

8.2.1.1 Mapping User Group(s) to Domain(s)

(Required) <Enter a short description here.>

Actions to Role mappings are done through Database tables. Sample action to role mappings are included in the application.

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.

1. Map all Alert Viewer User Groups to the Alert Viewer Information Domain (Infodom).
2. Map all Know Your Customer User Groups to the Alert Viewer Information Domain (Infodom), Case Management Information Domain (Infodom), and Know Your Customer Information Domain (Infodom).
3. Map all FATCA User Groups to the Alert Viewer Information Domain (Infodom) and Case Management Information Domain (Infodom).

> **ⓘ Note**
>
> For more information on mapping user group or groups to domain or domains, see *Identity Management* in the *Oracle Financial Services Analytical Applications Infrastructure User Guide* . For more information on configuring FATCA, see the *FATCA Administration and Configuration Guide*.

8.2.2 Adding Security Attributes

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

This section covers the following topics:

- About Security Attributes
- Loading Security Attributes

About Security Attributes

Security Attributes help an organization classify their users based on their geography, jurisdiction, and business domain, in order to restrict access to the data that they can view. You need to map the roles with access privileges, and since these roles are associated with user groups, the users associated with the user groups can perform activities throughout various functional areas in the BD application.

The following sections describe the security attributes:

- **Jurisdiction:** OFSFCCM solutions use Jurisdictions to limit user access to data in the database. Records from the Oracle client that the Ingestion Manager loads must be identified with a jurisdiction and users of the system must be associated with one or more jurisdictions. In the Alert Viewer system, users can view only data or alerts associated with jurisdictions to which they have access. You can use a jurisdiction to divide data in the database. For example:
  - Geographical: Division of data based on geographical boundaries, such as countries, states, and so on.
  - Organizational: Division of data based on different legal entities that compose the client’s business.
  - Other: Combination of geographic and organizational definitions. In addition, it is client driven and can be customized.

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

  > **Note**
  >
  > BD application supports up to 1000 jurisdictions.

- **Business Domain:** Business domains are used for data access controls similar to jurisdiction but have a different objective. The business domain can be used to identify records of different business types such as Private Client verses Retail customer, or to provide more granular restrictions to data such as employee data. The list of business domains in the system resides in the KDD_BUS_DMN table. The system tags each data record provided through the Ingestion Manager to one or more business domains. It also associates users with one or more business domains in a similar fashion. If a user has access to any of the business domains that are on a business record, the user can view that record. The business domain field for users and data records is a multi-value field. For example, you define two business domains: Private Client and Retail Banking.
  A record for an account that is considered both has BUS_DMN_SET=ab. If a user can view business domain a or b, the user can view the record. You can use this concept to protect special classes of data, such as data about executives of the firm. For example, you can define a business domain as e: Executives. You can assign this business domain to the employee, account and customer records that belong to executives. Thus, only specific users of the system have access to these records. If the executive’s account is identified in the Private Client business domain 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.

- **Scenario Group:** Scenario groups are used for data access controls. A scenario group refers to a group of scenarios in the BD applications that identify a set of scenario permissions and to which a user has access rights. The list of scenario groups in the system resides in the KDD_SCNRO_GRP table.
- **Organization:** Organizations are used for data access controls. Organizations are user group to which a user belongs. The list of Organizations in the system resides in the KDD_ORG table.

Loading Security Attributes

This section covers the following topics:

- Loading Jurisdictions
- Loading Business Domains
- Loading Scenario Groups
- Loading Scenario Group Memberships
- Loading Organizations

8.2.2.1 Loading Business Domains

To load a business domain, follow these steps:

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

   Table 8-2 KDD_BUS_DMN Table Attributes

Column Name	Description
BUS_DMN_CD	Single-character code that represents a business domain such as a, b, or c.
BUS_DMN_DESC_TX	Description of the business domain such as Institutional Broker Dealer or Retail Banking.
BUS_DMN_DSPLY_NM	Display name of the business domain , such as INST or RET.
MANTAS_DMN_FL	Flag that indicates whether Oracle Financial Services Behavior Detection specified the business domain (Y). If a BD 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 records to the table using an SQL script similar to the following sample script.

```
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX, BUS_DMN_DSPLY_NM,
MANTAS_DMN_FL) VALUES (‘a’, ‘Compliance Employees’, ‘COMP’, ‘N’);
INSERT INTO KDD_BUS_DMN (BUS_DMN_CD, BUS_DMN_DESC_TX, BUS_DMN_DSPLY_NM,
MANTAS_DMN_FL) VALUES (‘b’, ‘Executives’
‘EXEC’, ‘N’);
COMMIT;
```

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

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

8.2.2.2 Loading Jurisdictions

(Required) <Enter a short description here.>

To load jurisdictions in the database, follow these steps:

1. Add the appropriate record to the KDD_JRSDCN database table as mentioned in the following table.

   Table 8-3 Loading Jurisdictions

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

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

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

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

   The KDD_JRSDCN table is empty after system initialization and needs to be populated before the system can operate.

8.2.2.3 Loading Organizations

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

1. Add the appropriate record to the KDD_ORG database table as mentioned in the following table.

   Table 8-4 KDD_ORG Table Attributes

Column Name	Description
ORG_CD	Unique identifier for this organization.
ORG_NM	Short name for this organization that is used for display purposes.
ORG_DESC_TX	Description of this organization.

Table 8-4 (Cont.) KDD_ORG Table Attributes

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

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

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

8.2.2.4 Loading Scenario Groups

To load a Scenario Group, follow these steps:

1. Add the appropriate value in the KDD_SCNRO_GRP database table as mentioned in the following table.

Table 8-5 KDD_SCNRO_GRP Table Attributes

Column Name	Description
SCNRO_GRP_ID	Scenario group identifier
SCNRO_GRP_NM	Scenario Group Name.

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

```
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;
```

8.2.2.5 Loading Scenario Group Memberships

To load a Scenario Group Membership, follow these steps:

1. Add the appropriate value in the KDD_SCNRO_GRP_MEMBERSHIP database table as mentioned in the following table.

Table 8-6 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 records to the table using an SQL script similar to the following sample script.

```
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') ;
```

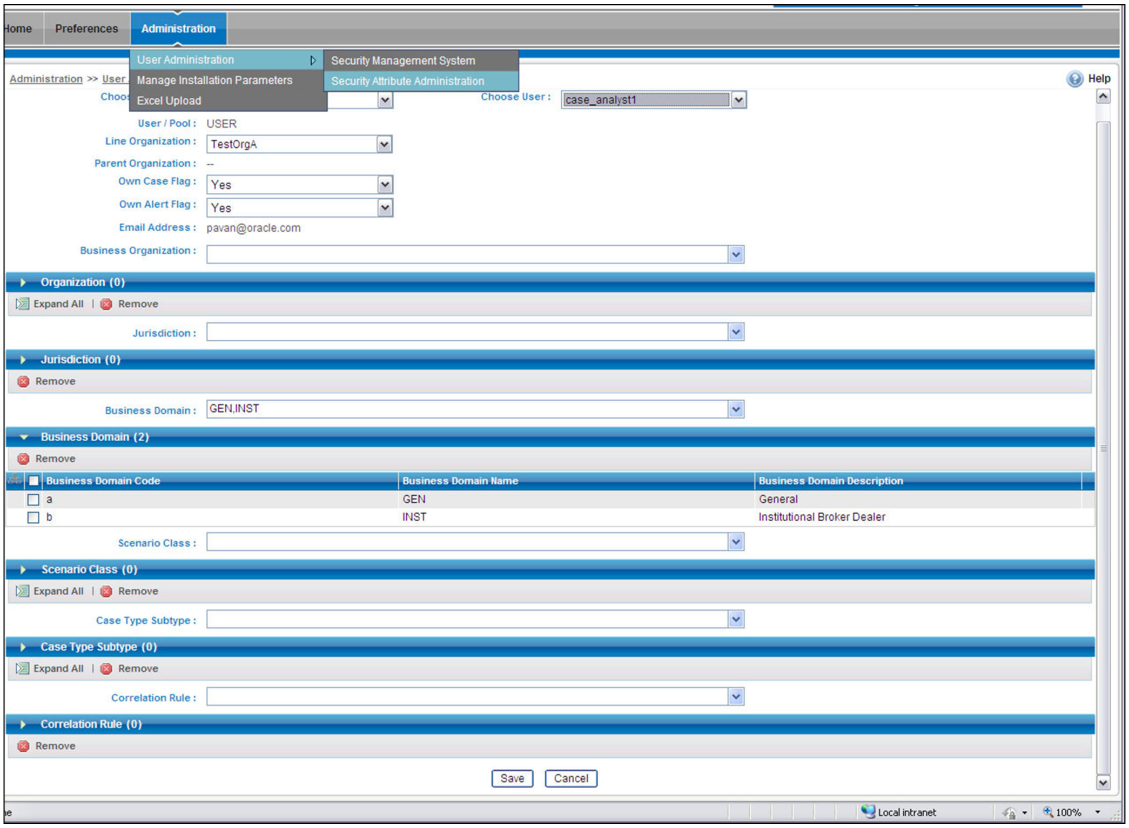
8.2.3 Mapping Users To Access Control Metadata

An Administrator can map each user to Access Control Metadata and Security attributes which will control theuser's access permissions. The Security Attribute Administration can be accessed from the Administration menu.

> **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.

Using this UI an Administrator can map both Organizations and Users to different Security attributes.

Figure 8-1 Components of Security Attribute



Choose User : case_analyst1

User / Pool : USER

Line Organization : TestOrgA

Parent Organization : --

Own Case Flag : Yes

Own Alert Flag : Yes

Email Address : pavan@oracle.com

Business Organization :

Organization (0)

Jurisdiction :

Jurisdiction (0)

Business Domain : GEN,INST

Business Domain (2)

	Business Domain Code	Business Domain Name	Business Domain Description
□	a	GEN	General
□	b	INST	Institutional Broker Dealer

Scenario Class :

Scenario Class (0)

Case Type Subtype :

Case Type Subtype (0)

Correlation Rule :

Correlation Rule (0)

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 **ChooseUser** 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 **UserType** is User; and it shows only organizations, if the **UserType** is Organization.

After selecting the desired user in **ChooseUser** drop-down list, the Administrator can map the following parameters to the selected user:

- 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.

The user should be mapped to any one of the following user groups:

- Case Supervisor
- Case Analyst1
- Case Analyst2
- 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.

8.3 About Scenario Manager Login Accounts

OFS AM users gain access to the Scenario Manager application through User ID and password authentication. 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:

- Create a database login account and password (Refer to Create the Database Login Account for more information).
- 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.

- Grant the database roles that the functional roles require. You can grant the role of data miner, or MNR to an ScenarioManager user.

> **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.

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 setup 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.

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 8-7 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.

d. 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.

e. 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:

```
INSERTINTO KDD_USER VALUES (‘KDD_MNR’, ‘KDD MINER’, ‘MNR’, ‘Y’, ‘FT’);
```

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 8-8 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:

```
INSERTINTO KDD_USER_ROLE values (‘KDD_MNR’, ‘MNR’);
```

8.4 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 8-9 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.

Table 8-9 (Cont.) System Account Passwords

System Account	Subsystem	Instructions
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.
dataminer 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.

Table 8-9 (Cont.) System Account Passwords

System Account	Subsystem	Instructions
RegReporting 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:**Iti s important that the password for RRS WebService and RRS are the same.

8.5 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.

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.

8.6 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 the following table describes.

Table 8-10 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 below.

```
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')
```

> **Note**
>
> The KDD_STATUS_ROLE table is pre populated after system initialization with the following records:

Table 8-11 KDD_STATUS_ROLE

STATUS_CD	USER_ROLE_CD
ACT	AMEXAUDITR
ACT	AMEXCUTIVE
ACT	AMINAUDITR
ACT	WLSUPVISR
DAC	WLSUPVISR

8.7 Configuring Alert and Case Management

The following section describes how to disable and enable Oracle Financial Services Alert Management.

This parameter allows the system to identify whether or not Alert Management Actions and Fields are to bedisplayed 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 user name 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 **Deploymen tBased** in the Parameter category.
4. Select **Alert Management** from the Parameter Name drop-down list.
5. Edit the parameter.

Glossary

Index