Alert Management User Guide

Release 8.0.6.0.0
May 2018

ORACLE®
FINANCIAL SERVICES

ORACLE®

Alert Management User Guide

Release 8.0.6.0.0
May 2018

Part Number: **F33033-01**

Contents

List of Figures

List of Figures

List of Tables

List of Tables

About this Guide

This guide explains the concepts of Oracle Financial Services Alert Management application and provides step-by-step instructions for navigating the Oracle Financial Services web pages, analyzing alerts, acting on alerts, and researching the business information.

This chapter focuses on the following topics:

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

Who Should Use this Guide

This guide is designed for the following users:

- **Analyst:** This user works on the alerts within the application frequently. This user's specific role (that is, Analyst I, Analyst II, or Analyst III) determines what they can view and perform within the application.

- **Supervisor:** This user works on the alerts within the application on a daily basis and is typically a higher level Analyst or Compliance Officer.

- **Executive:** This user can not be involved in the day-to-day analysis of alerts. However, they can view many areas within the application and can perform only a limited set of actions.

- **Auditor:** This user has broad viewing rights within the application. However, user can perform a limited set of actions based on their role (that is, Internal Auditor or External Auditor).

  For more informatin on user roles and actions, see *Appendix A, User Privileges.*

How this Guide is Organized

The *Alert Management User Guide* includes the following chapters:

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

- *Chapter 2, About Alert Management,* provides an overview of the Alert Management application, how it works, and what it does.

- *Chapter 3, Getting Started,* explains common elements of the interface. includes instructions on how to configure your system, access Alert Management, and exit the application.

- *Chapter 4, Investigating Alerts,* explains the Alerts workflow, how to search for business data and create alerts, and the actions you can take on alerts.

- *Chapter 5, Managing Suppression Rules,* provides instructions for managing suppression rules.

- *Chapter 6, Managing Trusted Pairs,* provides instructions for managing trusted pairs.

- *Chapter 7, Managing Trade Blotter,* provides instructions on managing trades, primarily for suitability issues.

- *Chapter 8, Managing Controlling Customers,* describes how to view existing or historical data, update certain components of the controlling customer, and delete existing controlling customers.

- *Chapter 9, Managing Security Restrictions,* explains securities restriction features providing a way to search for existing trading restrictions on different securities based on user-specified search parameters.

- *Chapter 10, Researching Business Data,* describes how to use the Oracle Financial Services Research workflow to search for and inquire about a specific focus type and its related information.

- *Chapter 11, Managing Compliance Regulatory Reporting,* explains the high-level information on Compliance Regulatory Reporting application.

- *Chapter 12, Managing Watch List Management,* describes the Oracle Financial Services Watch List Management feature.

- *Chapter 13, Setting User Preferences,* explains how to setup Oracle Financial Services Alert Management preferences.

- *Appendix A, User Privileges,* provides complete information on the user roles and action they can perform.

- *Appendix B, Alert Components and Tables,* provides the additional information on various components and tables of Alert Management.

- *Appendix C, Results from Updating Trusted Pairs Relationships,* provides the results from updating trusted pairs relationships.

- *Appendix D, Business Tabs,* identifies the possible business tab pages that the Oracle Financial Services application displays for a specific scenario class and focus type.

- *Appendix E, Using Alert Management Web pages,* explains common elements of the interface.

- *Appendix F, Message Pages,* explains error and status pages that are not directly related to the business function of the application.

- *Appendix G, Security within Oracle Financial Services Alert Management,* explains how Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) security is used.

- *Appendix H, Calculating Risk,* describes how Oracle Financial Services Alert Management application uses risk calculations as part of managing sensitivity when detecting behaviors of interest.

- *Appendix I, Trade Blotter List Component Matrix,* lists trade blotter components in the Oracle Financial Services Alert Management application.

- The *Index* provides an alphabetized cross-reference list that helps you to locate information quickly.

Where to Find More Information

For more information about Oracle Financial Services Alert Management, refer to the following documents:

- *Administration Guide*
- *Administration Tools User Guide*
- *Configuration Guide*
- *Data Interface Specification (DIS)*
- *Reference Guides*
- *Scenario Manager User Guide*
- *Scenario Wizard Configuration Guide*
- *Installation Guide*
- *Anti-Money Laundering Technical Scenario Descriptions*
- *Trading Compliance Technical Scenario Descriptions*
- *Fraud Technical Scenario Descriptions*
- *Broker Compliance Technical Scenario Descriptions*
- *Energy and Commodity Trading Technical Scenario Descriptions*
- *Glossary*
- *Release Notes*
- *Read me*

These documents are available at the following link:
http://docs.oracle.com/cd/E60570_01/homepage.htm

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

Conventions Used in this Guide

Table 1 provides the conventions used in this guide.

Table 1. Conventions Used in this Guide

This convention. . .	Stands for . . .
Italics	● Names of books as references ● Emphasis ● Substitute input values
Bold	● Menu names, field names, options, button names ● Commands typed at a prompt ● User input
Monospace	● Directories and subdirectories ● File names and extensions ● Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<Variable>	● Substitute input value

CHAPTER 1 · *Overview of FCCM*

This chapter describes Oracle Financial Services Financial Crimes and Compliance Management (FCCM) applications, the workflow and the usage by financial institutions.

It contains the following topics:

- About Financial Crimes and Compliance Management
- Functions
- FCCM Workflow

About Financial Crimes and Compliance Management

In today's complex banking environment, there are many different factors that financial institutions must address to deter crime, safeguard their reputation, increase efficiency, minimize risk, and comply with regulatory agencies. Oracle Financial Services Financial Crimes and Compliance Management (FCCM) applications 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.

The FCCM application is a common platform that supports the following OFSAA products:

- Anti-Money Laundering Enterprise Edition
- Know Your Customer (KYC)
- Enterprise Fraud Management (EFM)
- Oracle Financial Services Currency Transaction Reporting (CTR)
- Foreign Account Tax Compliance Act (FATCA) Management
- Trading Compliance (TC)
- Oracle Financial Services Personal Trading Approval
- Trade Blotter (TB)
- Broker Compliance (BC)
- Energy and Commodity Trading Compliance (ECTC)
- Enterprise Case Management (ECM)
- Compliance Regulatory Reporting

Anti-Money Laundering Enterprise Edition

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 can 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)

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 the cases are resolved or reported to the appropriate regulatory authorities.

For more information on KYC related documents, see *OTN* page.

Enterprise Fraud Management (EFM)

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 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 can indicate money laundering, terrorist financing, or an account takeover.

Oracle Financial Services Currency Transaction Reporting (CTR)

Oracle Financial Services Currency Transaction Reporting (CTR) analyzes currency transaction data from the organization and identifies any suspicious activities within the institution that can 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) uploading in a batch form in a specific text file format.

Unlike alerts for other Oracle Financial Services products such as Anti-Money Laundering, Fraud, Trading Compliance, Broker Compliance, or Energy and Commodity Trading Compliance which appear in an Alert

Management user interface, CTR alerts are automatically processed and converted into CTR reports or Monetary Instrument Log reports managed through the CTR user interface.

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

Foreign Account Tax Compliance Act (FATCA) Management

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

Trading Compliance (TC)

Trading Compliance (TC) examines prices and timing of orders and executions by comparing them to market conditions and detect behaviors or situations that violate exchange, market center, and individual broker or dealer policies and procedures, including behaviors that violate the Chinese Wall policies and procedures established by the Firm or those with confidential information held by the Firm about security.

For example, the Trading Ahead of Material Events scenario detects possible insider trading by analyzing trades which occur prior to "events", which can be defined by the Oracle client. The type and volume of trades which occur prior to an event indicate that an employee, customer, trader, or trading desk was in possession of material non-public information. As there can also be non-fraudulent reasons for this trading activity, this scenario minimizes false alerts by excluding accepted hedging or trading strategies.

Oracle Financial Services Personal Trading Approval

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

Trade Blotter (TB)

Trade Blotter (TB) allows trades to be viewed and reviewed, primarily for suitability issues within the wealth management sector, by compliance analysts and business supervisors after a trade is executed. Trade Blotter is a list of trades returned after a search based on specified criteria. Users can view trade details, view related trade documents, enter a comment on a specific trade, and then mark the trade as reviewed or requiring follow-up.

Broker Compliance (BC)

Broker Compliance (BC) identifies activities or situations in customer accounts that involve either a significant amount of risk and therefore can be unsuitable for the customer or can violate trading rules set by the exchanges or regulators; trades in mutual fund securities that can violate regulatory trading guidelines, Commission policies, or are unsuitable for a particular customer; and activities performed by employees that can violate regulatory conduct rules or can be prohibited by firm policies. These scenarios also detect instances in which an investment advisor can be managing client accounts in a manner that is unsuitable for their customers, giving preferential treatment to particular customers, or manipulating transactions between accounts; and instances in which a portfolio manager can be placing orders on material, non-public information, misrepresenting portfolio performance, or unfairly allocating orders to accounts they manage.

For example, the Reps Concentrating Solicitations in Too Few Securities scenario verifies that Registered Representatives are not exposing their clients to undue risk by recommending a significant percentage of buy solicitations in a single security, which can result in an unbalanced and volatile portfolio.

Energy and Commodity Trading Compliance (ECTC)

Energy and Commodity Trading Compliance (ECTC) monitors trading activities that involve the financial institution as the buyer or seller on energy and commodity related trades, including commodities, options, futures, and swaps.

For example, the Energy Trading Limits scenario monitors trading of energy instruments to detect excessive hourly amounts of energy traded, based on internal limits which consider physical power, financial power, and Financial Transmission Rights (FTR). The scenario generates alerts when the amount of energy approaches or exceeds these internal limits. This behavior can indicate an attempt to manipulate the market by knowingly creating congestion with the purpose of benefiting from the creation of that congestion.

Compliance Regulatory Reporting

Compliance 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 can lead to fraud or money laundering within the institution to regulatory authorities. This application can be integrated with Alert Management and Case Management.

Functions

The following figure depicts the functionality of FCCM.
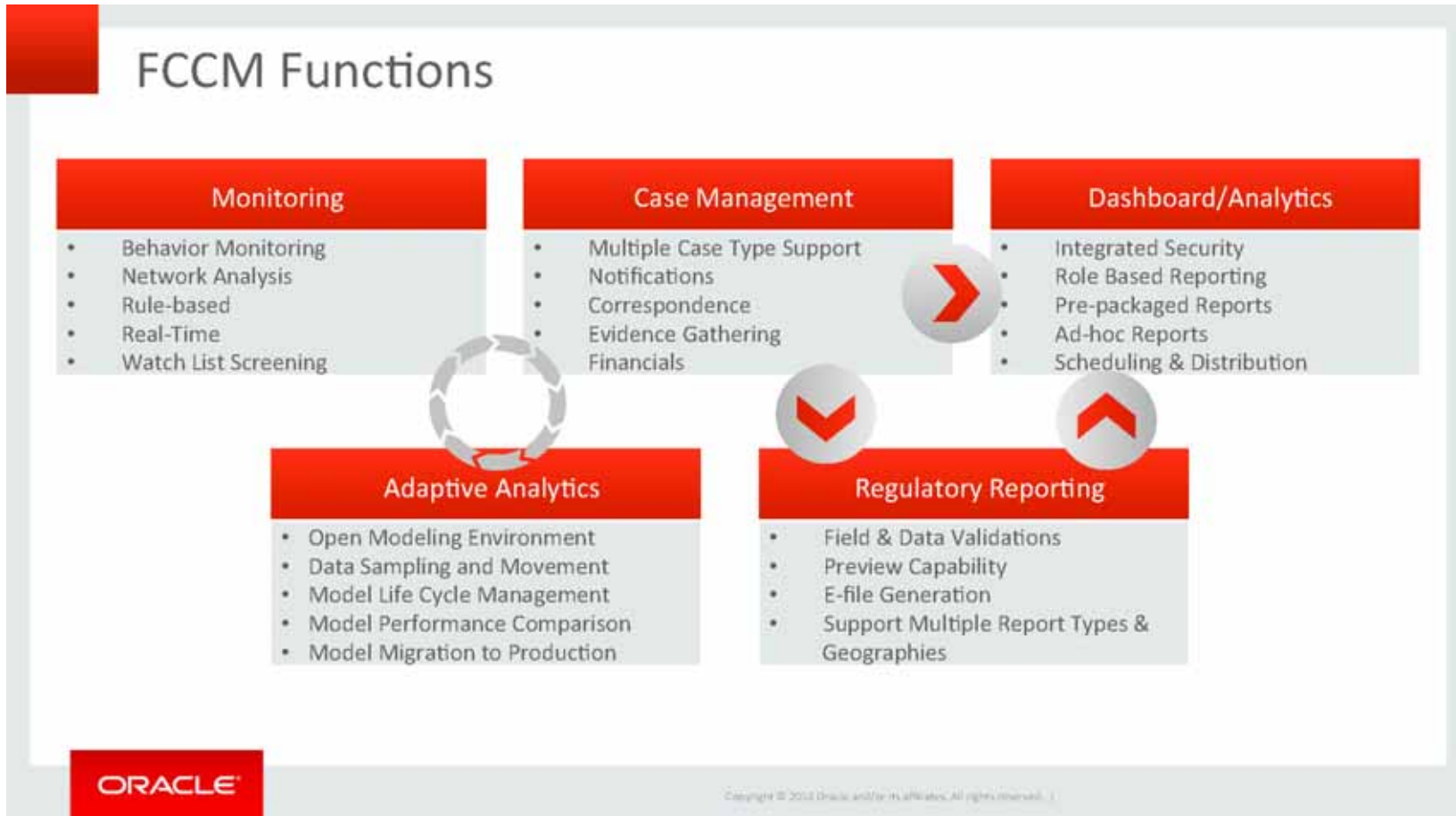
FCCM Workflow

The following figure shows the FCCM process flow.
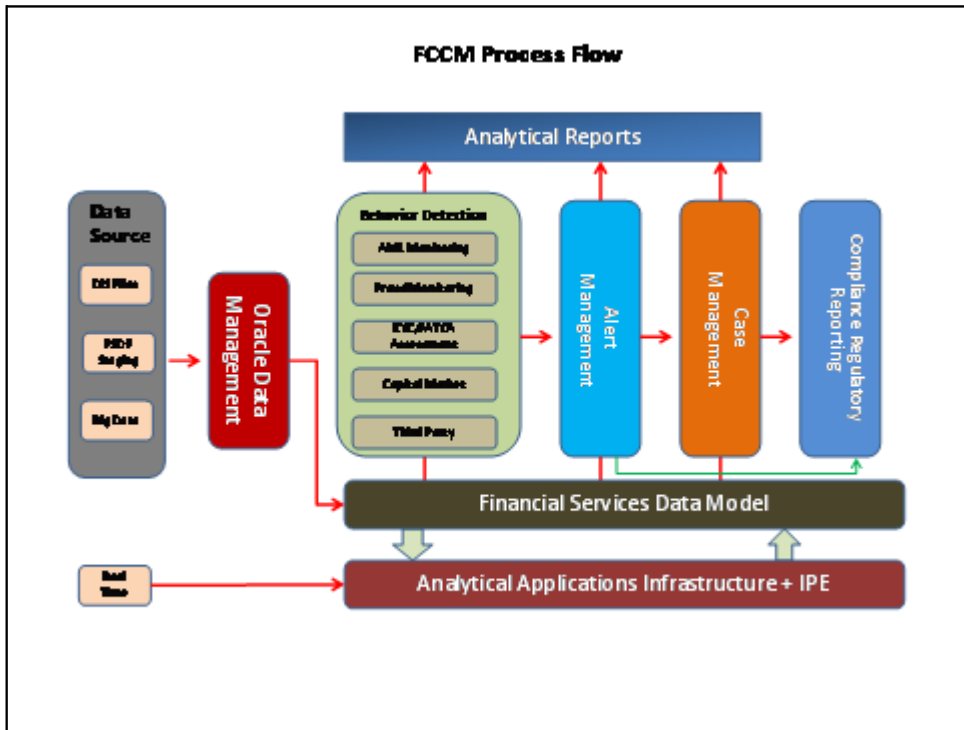
Figure 1. FCCM Process Flow

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

 Figure 2. FCCM Workflow

Detailed information about these processes is available in the following chapters.

CHAPTER 2 *About Alert Management*

This chapter gives an overview of Alert Management application and discusses the following topics:.

- Overview of Alert Management
- Alert Management Workflow
- Data Loading and Processing
- Behavior Detection (BD)
- Post Processing
- Oracle Financial Services Behavior Detection UI
- Correlation
- Suppression Rules
- Four - Eyes Approval
- Trusted Pairs
- Trade Blotter
- Controlling Customer
- Security Restriction
- Watch List Management
- User Privileges

Overview of Alert Management

Oracle Financial Services Alert Management application detects potentially problematic behaviors by identifying patterns in data and generating alerts. An alert is a unit of work in which a focus appears to have exhibited a behavior of interest, along with the supporting information. A focus represents a business entity or business unit around which activity is reviewed and aggregated. There are many supported types of focus, ranging from Account or Customer to Order, Execution or Trade, depending on the behavior of interest. Alerts can be generated from a pattern matching specific source events, a sequence of events, trends, conditions, or context. An alert is not necessarily tied to an event, but rather to the behavior of a focus. An alert is a record of one or more pattern matches in a detection run, which is a signal for further investigation.

Alert Management Workflow

The following figure illustrates the workflow of Oracle Financial Services Alert Management.
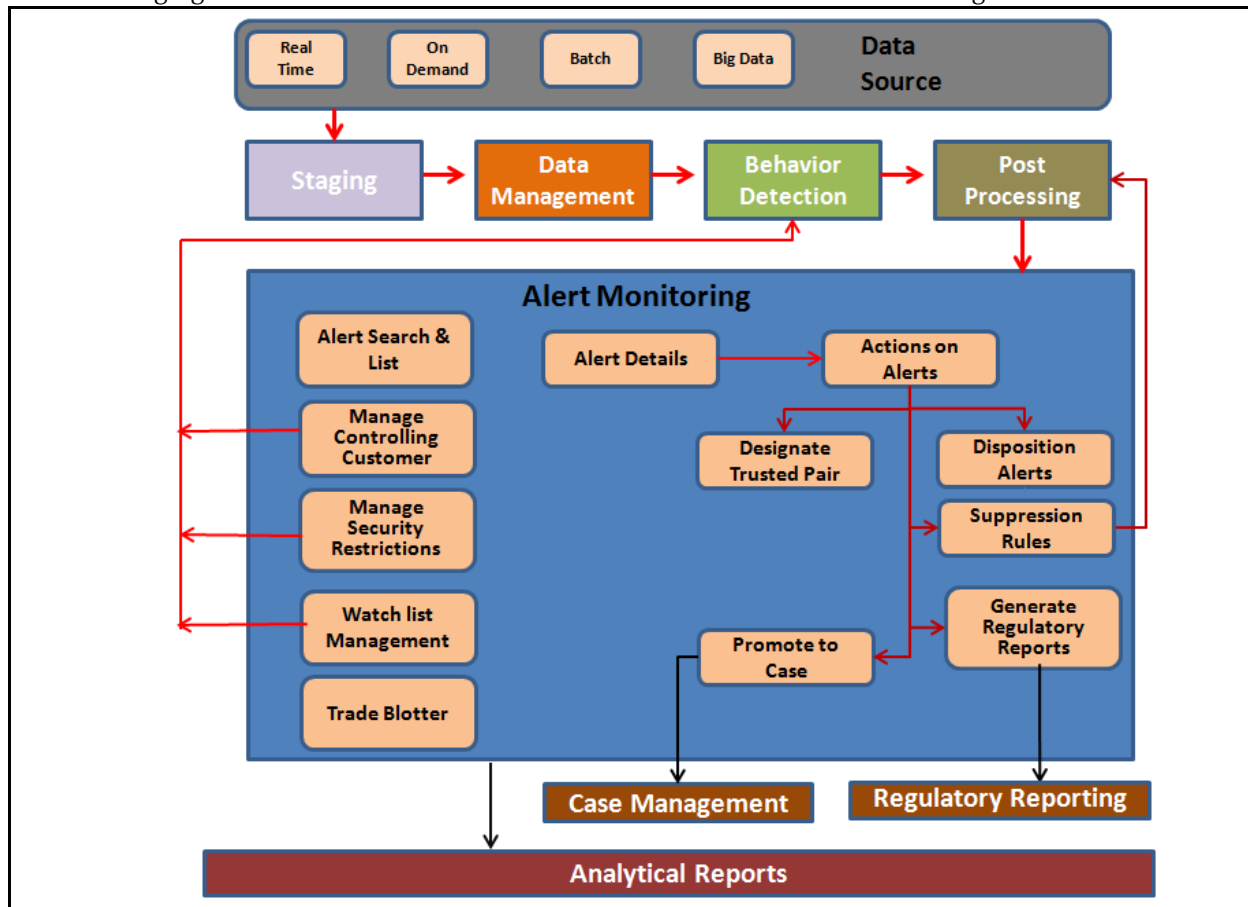
Figure 3. Alert Management Workflow

Data Loading and Processing

The Oracle Financial Services Ingestion Manager receives, transforms, and loads Market data, Business data (such as, Transactions or Orders and Trades), and Reference data (such as Account, Customer, and Employee information) from Common Staging Area or Flat File Interface that alert detection processing requires. The Data Ingestion subsystem transforms Market, Business, and Reference data to create derived attributes that the detection algorithms require (much of the loaded data is as is). The system extracts and transforms data and subsequently loads the data into the Financial Services Data Model (FSDM). After loading the base tables, the Oracle client's job scheduling system invokes Behavior Detection (BD) datamap XML to derive and aggregate data. The Data Ingestion component also uses the Fuzzy Name Matcher Utility to compare names found in the source data with names in the Watch List.

An Oracle client implements the Ingestion Manager by setting up a batch process that conforms to the general flow that this chapter describes. Typically, the system uses a job scheduling tool such as Analytical Application Infrastructure (AAI) Scheduler to control the batch processing of the Ingestion Manager.

Behavior Detection (BD)

The Oracle Financial Services Behavior Detection uses sophisticated pattern recognition techniques to identify behaviors of interest, or scenarios, that are indicative of potentially interesting behavior. A pattern is a specific set of detection logic and match generation criteria for a particular type of behavior. These behaviors can take multiple representations in a firm's data.

The software detects behavior that matches the logic and criteria defined by specific patterns. When one or more data records equal a scenario's pattern of behavior, a match is created. Records that contribute to the exhibition of the behavior are associated to the match as matched records are displayed in the Oracle Financial Services Alert Management as building blocks. The entity that is responsible for the behavior of interest is considered the focus of the match. Examples of focus types are account, execution, correspondent bank, and employee.

The Oracle Financial Services Alert Management generates an alert to package one or more matches for analysis and action. If multiple matches are found that are closely related to the same focus (that is, instances of similar behaviors by the same entity), the matches can be combined to create a single alert, herein referred to as a multi-match alert, to help the analysis of the found behaviors.

Scenarios representing related business problems are grouped into scenario classes. Scenario classes are categories of behaviors or situations that have common underlying characteristics.

Depending on your deployment, one or more of the following solution sets are available: Anti-Money Laundering (AML) and Fraud (FR), Trading Compliance (TC), Broker Compliance (BC), and Energy and Commodity Trading Compliance (ECTC).

Scenarios

The Oracle Financial Services Alert Management detection modules are divided into scenarios that typify specific types of business problems or activities of interest. The scenarios within Oracle Financial Services Alert Management are grouped into scenario classes that represent categories of behaviors or situations that have common underlying characteristics.

Post Processing

During post-processing of detection results, Behavior Detection prepares the detection results for presentation to users depending on the following processes:

- **Augmentation**: Collects additional information related to the matched behavior and focus for pattern detection, which enables proper display or analysis of the generated matches.

- **Match Scoring**: Computes a ranking for scenario matches indicating a degree of risk associated with the detected event or behavior.

- **Alert Creation**: Packages the scenario matches as units of work (alerts), potentially grouping similar matches together, for disposition by end users. This is applicable when multiple matches with distinct scores are grouped into a single alert.

- **Update Alert Financial Data**: Records additional data for alerts such as the related Investment Advisor or Security involved in the alert which can be useful for display and analysis.

- **Alert Scoring**: Ranks the alerts (including each match within the alerts) to indicate the degree of risk associated with the detected event or behavior.

- **Alert Assignment**: Determines the user or group of users responsible for handling each alert.

- **Auto-Close**: Based on configurable rules, closes alerts based on attributes of the alert or the alert focus.

- **Automatic Alert Suppression**: Suppresses alerts that share specific scenario and focal entity attributes for a particular time frame. This process only impacts alerts which match suppression logic defined for a specific scenario and focal entity combination.

- **Highlight Generation**: Generates highlights for alerts that appear in the alert list of the Alert Management subsystem and stores them in the database.

- **Augment Trade Blotter**: Provides the ability to differentiate between various types of trades using text-based codes. It also provides the ability to flag trades that require additional analysis before an analyst can mark trade as Reviewed or Reviewed with Follow up.

- **Score Trade Blotter**: Determines the maximum score of alerts generated in the same batch cycle associated with a trade; also determines the alert/trade mappings.

- **Historical Data Copy**: Identifies the records against which the current batch's scenario runs generated alerts and copies them to archive tables. This displays a snapshot of information as of the time the alert behavior was detected.

- **Alert Correlation:** Uncovers relationships among alerts by correlating alerts to business entities and subsequently correlating alerts to each other based on these business entities. The relationships are discovered based on configurable correlation rule sets.

Oracle Financial Services Behavior Detection UI

The pages that are available within the Oracle Financial Services Alert Management User Interface (UI), the fields on those pages, and the actions you can take are based on your firm's deployment of the product. There is a base set of pages that appears for all alerts (for example, the Alert Data tab pages).

The Alert Data tabs consist of Details, Disposition, Financials, Correlations, Relationships, Narrative, Evidence, and Audit tabs. These tabs display information pertaining to the focus of the alert and the entities related to the focus in relation to the firm's most recent data submission.

In addition to the Alert Data tab pages, Business Data tab pages are conditionally displayed, based on the focus and scenario class of the alert class. In some instances, the content of the Business Data tab page can also be affected by attributes of the business entity that is being displayed. For example, the Customer business data page for an Individual type customer displays different information than the Customer tab page for a Customer which is a legal entity or business.

Oracle Financial Services Behavior Detection (OFSBD) routinely generates alerts as determined by the configuration of the application in your environment, typically nightly, weekly, monthly, and quarterly. Alerts can be automatically assigned to an individual or group of users and can be reassigned by a user.

Once matches are generated and alerts created and assigned, OFSBD provides a User Interface (UI) for the investigation and disposition of those alerts. The Alert Management UI allows users to review details of the behavior which led to the alert, information about the focus of the alert, and a history of behavior related to the focus.

Users can take actions on an alert using OFSBD, and move it through a series of statuses to a final disposition.

Alert Statuses

An alert's status can change in the following ways:

- An eligible user views the alert
- An action is taken on the alert

While some actions can be taken automatically by the application that changes status, this section focuses on the manual actions you take that cause an alert's status to change.

If you access the Alert Details page of an alert with the status of New, and the alert is owned by a user group of which you are a member, the alert status is changed to Open through the Alerts workflow. However, ownership of the alert is transferred to you if your firm's installation is configured to allow for Alert Inheritance (the transfer of ownership of a New alert to an authorized user on the viewing of the alert).

During the process of closing an alert, several actions can be taken on the alert. See Chapter 4, *Investigating Alerts*, for details on how to take these actions.

Note: You can only take actions on alerts that you are authorized to view. Oracle Financial Services Alert Management determines your ability to take action on alerts based on your role.

The following table lists alert statuses and the events that can cause the status to change.

Table 1. Alert Status Descriptions

Status	Description
New	The application has generated an alert, and the owner has not yet viewed the alert detail information. An alert is newly generated, either from detection, posting from a third party system or manually created by a user.
Open	An owner has viewed the alert detail information.
Follow-up	An authorized user has set a date when additional information needed to aid in the analysis of the alert must be received.
Reassigned	An authorized user has assigned the alert to another owner, and the new owner has not yet viewed the details information.
Closed	An authorized user has taken a closing action, or the alert is auto-closed or auto-suppressed by the application because it meets your firm's criteria for auto-closing or auto-suppression.
Reopened	An authorized user has opened an alert that was previously closed, and the owner has not yet viewed the reopened alert.

Figure 4 identifies the events that can change the status of an alert in Alert life cycle.
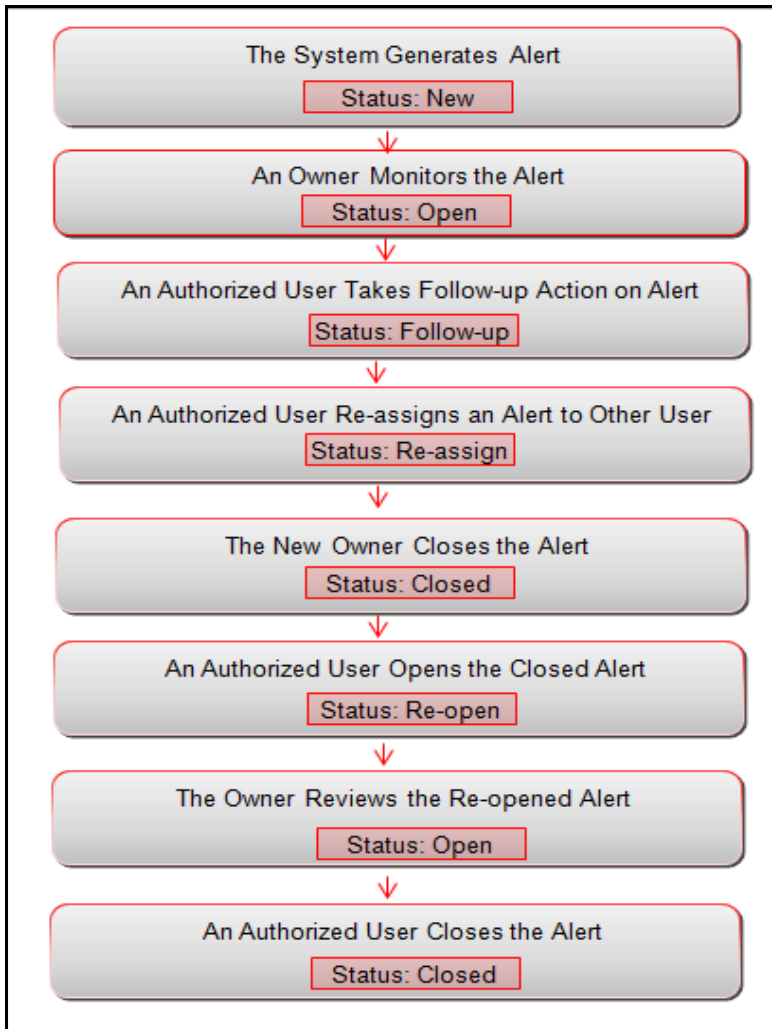
Figure 4. Potential Life Cycle of an Alert

Related Alerts

The UI displays the alerts related to the focal entity of the alert. Related alerts are alerts with the same focal entity as the current alert or alerts whose focal entities share a business relationship with the focal entity of the current alert under investigation. Additionally, related alerts can be alerts related to the focal entity of the current alert based on matching one or more business entities to alert correlation rules. See section *Correlation* for more information on alert correlation.

Related Alerts display on the Relationship tab.

Related Cases

If your firm has implemented Oracle Financial Services Enterprise Case Management, the UI displays the cases related to the focal entity of the alert under investigation where the focal entity is included as a business entity or involved party on the case. The Linked Cases display on the Relationship tab.

Correlation

Alert Correlation is an Oracle Financial Services Alert Management module that automatically uncovers relationships among alerts based on configurable rule sets. It is executed on-demand by the Alert Management Supervisor Web Service as alerts are posted or as part of the behavior detection batch process. Its purpose is to find relationships between individual posted alerts and other existing alerts, to correlate alerts generated as part of a nightly batch process with other alerts generated in the same or prior batches, and to periodically identify relationships across alerts generated within a certain time period. If your firm has implemented Oracle Financial Services Enterprise Case Management, Alert Correlations can automatically be promoted to a case based on configurable actions.

Business Entity correlations and alert correlations are displayed on the Correlation Tab in the Alert Management UI as additional information within the context of an alert.

Alert correlation occurs either as part of processing a posted alert (alerts which can be posted directly into the Alert Management subsystem from an external source) or during batch alert processing. Alert correlation derives the Alert-to-Business Entity Correlation and stores the resulting relationships in the FSDM (Financial Services Data Model). After the Alert-to-Business Entity Correlation, alerts are correlated to other alerts (Alert-to-Alert Correlation) and a set of action rules are instituted to process the resulting correlation.
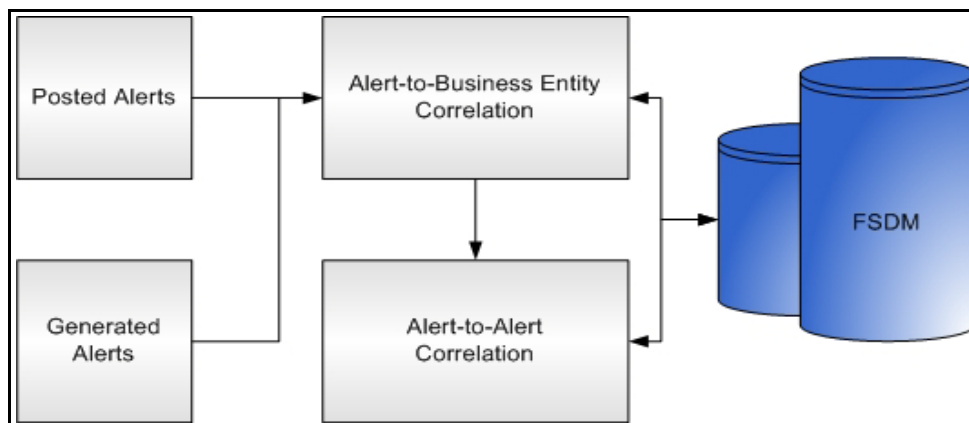
Figure 5. Alert Correlation – Process Flow

Correlation Rules

Alerts are correlated to other alerts based on the common business entities and correlation rules that are applied on the alerts. Multiple correlation rules are defined to correlate alerts for different business purposes. For example, you can set a correlation rule to link alerts generated over a specific time period that share the business entity. These correlation rules are version controlled with an audit trail to identify any changes made by the user.

Correlation Scoring Rule

Similar to alert scoring rules, a correlation can also be scored. The correlation scoring rule, which is defined within the correlation rule, is driven by the alerts that are part of the correlation.

Alert Correlation in the Oracle Financial Services Alert Management UI

The Oracle Financial Services Alert Management UI displays detected Alert-to-Business Entity Correlations within the context of alerts. The UI also displays discovered Alert Correlations (that is, Alert-to-Alert Correlations) within the context of alerts. Correlation relationships and memberships displays on the Correlation tab.

Suppression Rules

Users can choose to take an action on an alert that results in future alerts for that particular entity and scenario combination to be automatically closed for a user specified period of time. Closing by reason of suppression helps to eliminate false positives where behavior for an entity is deemed to not suspicious or is a normal business practice.

The Manage Suppression Rules feature provides a way to search for existing suppression rules based on a set of user-specified parameters. Manage Suppression Rules also enables you to modify certain components of rules, in particular, to Update or to End an existing suppression rule and to track all the actions performed on that rule.

An alert suppression rule enables the system to automatically suppress a particular entity's newly-generated alerts based on criteria such as highlight, scenario, and suppression rule begin and end date. The rule captures information such as the creation date, the status, the generating scenario, the focal entity (focus type and focal entity ID) and the links to user comments associated with the suppression rule. Suppression rules are automatically created when you save a Close and Suppress action on an alert from within the Monitoring workflow.

See *Chapter 5, Managing Suppression Rules*, for information on Four - Eyes Approval for suppression where the recommendation is done at the alert level and the approval/rejection is done at the Manage Suppression UI.

Four - Eyes Approval

Four-Eyes Approval is a dual control or approval process that requires an authorized user (for example, a Supervisor) to approve actions of other users prior to those actions taking full effect on the alert (for example, closing the alert or creating a suppression instruction). This process also enables users of specified roles to acknowledge approved or rejected changes proposed and to annotate an acknowledgement with comments. The system must be configured for Four - Eyes Approval.

Trusted Pairs

The Manage Trusted Pairs workflow is intended only for the management of existing trusted pairs, not the designation of trusted pairs. Through the Manage Trusted Pairs workflow, you can search, view, approve, reject, and modify existing trusted pairs based on your user privileges. Trusted Pairs can be designated by users during the course of investigating an alert or by the client providing trusted pairs via the Data Interface Specification (DIS) file. These options are mutually exclusive. See Chapter 6, *Managing Trusted Pairs* for more information.

Designating pairs of entities as trusted helps to decrease the number of false positive alerts that are generated when the alerting activity is between entities that an institution considers to have a trusted relationship. During the process of ingesting transactional information (Wires, Checks and Monetary Instruments, Back Office Transactions and Insurance Transactions), Oracle Financial Services Behavior Detection ingestion process flags a transaction as trusted if at least one party/counterparty pair on the transaction is considered to be a trusted pairs. These transactions can be optionally excluded from detection for many ML, IML, and FR class scenarios (through the use of a threshold parameter), thus reducing the number of false positives where alerts are generated on activity between parties trusted to do business with one another. As the relationship between a pair of entities is marked trusted for some period of time and is excluded from the process of behavior detection, the workload of an analyst can be greatly reduced. If the decision is made to not exclude trusted transactions from detection, alerts involving trusted transactions display information regarding the percent of the alert's transactions that involve trusted pairs versus transactions that do not involve trusted pairs.

Trade Blotter

The Trade Blotter functionality allows trades to be viewed and reviewed, primarily for suitability issues within the wealth management sector, by compliance analysts and/or business supervisors after a trade is executed. Trade Blotter trades can or can not are associated with an alert. You can access Trade Blotter only if the Trade Blotter functionality is enabled at installation and you have the appropriate permissions to do so.

Trade Blotter provides a list of trades returned after a search based on specified criteria. An analyst or supervisor can view various trade details, view related trade documents, enter a comment on a specific trade, and then mark the trade as Reviewed or Reviewed with Follow-up. See Chapter 7, *Managing Trade Blotter* for more information.

Controlling Customer

The Manage Controlling Customers provides a way to search and manage customer relationships. A Controlling Customer is a customer in a company represented by a specific security. A customer can have a controlling position in more than one security. Controlling customer relationships are considered by some Oracle Financial Services Behavior Detection scenarios during alert generation.

Through the Manage Controlling Customers UI, you can view existing or historical controlling customers, update certain components or delete the controlling customer. In addition, it enables you to establish new controlling customers. This UI is only available if your firm has enabled Manage Controlling Customers during installation. See Chapter 8, *Managing Controlling Customers* for more information.

Security Restriction

The Manage Securities Restriction provides a way to search for existing trading restrictions on different securities based on user-specified search parameters. It also enables you to view existing or historical data, update certain components of the restriction, and delete existing restrictions and establish new security trading restriction conditions.

A security restriction sets the conditions related to restriction on trading of specific securities. Oracle Financial Services Alert Management uses this information to generate alerts on suspicious trading behavior involving these restricted securities. This UI is only available if your firm has enabled Manage Security Restriction during installation. See Chapter 9, *Managing Security Restrictions* for more information.

Watch List Management

The Watch List Management feature allows watch lists to be added, updated and deactivated. You can also add and deactivate watch list members. A watch list is a list of entries that have known risk characteristics. Watch lists can represent public sources or can be created and managed internally by the institution. Common public sources for watch lists include Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF). Watch lists are associated with a score. See Chapter 12, *Managing Watch List Management* for more information.

For watch lists that can be categorized as risk lists (lists that contain entries considered to pose a risk to your firm), a risk score is assigned based on increasing risk, usually on a scale of 1 to 10. Watch lists can also be used to designate trusted or exempted entities. Watch lists play an important role in behavior detection for Anti-Money Laundering and Fraud behaviors. See *Appendix H, Calculating Risk*.

User Privileges

Oracle Financial Services Alert Management allows different types of roles to access the Alert Management UI. The various roles are: Analyst I, Analyst II, Analyst III, Supervisor, Executive, Internal Auditor, External Auditor, Data Miner, Oracle Administrator, and WLM Supervisor.

For more information on User privileges, see *Appendix A, User Privileges.*

Getting Started

This chapter provides step-by-step instruction to login to the Alert Management System and different features of the Oracle Financial Services Analytical Applications (OFSAA) Application page.

This chapter discusses the following topics:

- System Requirements
- Accessing OFSAA Applications
- Managing OFSAA Application page
- Troubleshooting Your Display

System Requirements

The following applications are required to run Oracle Financial Services Alert Management system:

- Microsoft Internet Explorer (IE) version 9 or later.

  Earlier versions and other browsers are not supported and can produce errors, inaccurate data and display failures. For users of IE version 8.0, the browser should be run in compatibility mode.

- Adobe Acrobat Reader version 9.0, or later.

  You can download a free copy of the latest version of the Reader at www.adobe.com.

- Java must be installed. JDK 1.6 (version 6) or above.

- The screen resolution of the system should be set to 1280×1024 or higher for proper display of the user interface (UI).

  For more information, refer to the *OFSBD Installation Guide*.

Accessing OFSAA Applications

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

Your system administrator provides you with a User ID and Password. Login to the application through the Login page. You are prompted to change your password on your first login. You can change your password whenever required by logging in. For more information, see the *Change Password* section.

To access the Oracle Financial Services Analytical Applications, follow these steps:

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

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

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

   The OFSAA Login page is displayed.

Figure 6. OFSAA Login page

2. Select the Language from the Language drop-down list. This allows you to use the application in the language of your selection.

3. Enter your User ID and Password in the respective fields.

4. Click **Login**. The Oracle Financial Services Analytical Applications page is displayed.

Figure 7. OFSAA Main Page

The Oracle Financial Services Analytical Applications page is a common landing page for all users until a preferred application page is set. For more information about how to set your preferred application page, see *Chapter 13, Setting User Preferences*. You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

Managing OFSAA Application page

This section describes the different panes and tabs in the OFSAA Application page.
The OFSAA Application page has the following tabs:

- Applications Tab
- Object Administration Tab
- Change Password
- Copyright Information

Applications Tab

The Applications tab lists the various OFSAA Applications that are installed in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups.
For example, to access the OFSAA Applications, select the required Application from the Select Application drop-down list. For Alert Management, select Financial Services Anti-Money Laundering. Based on your selection, the page refreshes the menus and links across the panes.

Figure 8. Applications Tab

Object Administration Tab

Object Administration is an integral part of the Infrastructure system and allows system administrators to define the security framework with the capacity to restrict access to the data and metadata in the warehouse, based on a flexible, fine-grained access control mechanism. These activities are mainly done at the initial stage, and then as needed. This tab includes information related to the workflow of the Infrastructure Administration process with related procedures to assist, configure, and manage administrative tasks.

The Object Administration tab lists the various OFSAA Information Domains created in the OFSAA setup based on the logged in user and mapped OFSAA Application User Groups. For more information about managing Information Domains, see *Administration Guide*.

To define or maintain access for an Information Domain, follow these steps:

1. Navigate to the OFSAA Applications page.

2. Click **Object Administration** tab. The Object Administration page is displayed.

3. Select the required Information Domain from the Select Information Domain drop-down list. Based on your selection, the page refreshes the menus and links across the panes.

Figure 9. Object Administration Tab

Change Password

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

To change the password, follow these steps:

1. Navigate to the OFSAA Applications page.

Figure 10. Change Password

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

Figure 11. Change Password

3. Enter your old and new password in the respective fields.

4. Click **OK**. Your password is changed successfully. The application navigates back to the Login page where you can login with the new password.

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

Copyright Information

To access copyright information, follow these steps:

1. Navigate to the OFSAA Applications page.

2. Click the **About** hyperlink in the OFSAA Login page. The Copyright text is displayed in a new window.

Figure 12. Copyright Information

Selecting Applications

This section explains how to access required applications.

The OFSAA Application page has multiple tabs and each tab has specific links to OFSAA Infrastructure and Application modules. The modules, tabs, and links are enabled depending on your user role and the OFSAA Application you select.

This page is divided into two panes:

- **Left Pane**: displays menus and links to modules in a tree format based on the application selected in the Select Application drop-down list.

- **Right Pane**: displays menus and links to modules in a navigational panel format based on the selection of the menu in the Left pane. It also provides a brief description of each menu or link.

To access required applications, follow these steps:

1. Navigate to the OFSAA Applications home page.

2. Select **Financial Services Anti-Money Laundering**.

Figure 13. Behavior Detection- Anti-Money Laundering page

3. Click **Alert Investigation** in the RHS. The *Alert Search and List Page* is displayed.

Troubleshooting Your Display

If you experience problems logging into Oracle Financial Services Behavior Detection or with your display, the browser settings can be incompatible with running OFSAA applications. The following sections provide instructions for setting your Web display options for OFSAA applications within IE.

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

This section covers the following topics:

- Enabling JavaScript
- Enabling Cookies
- Enabling Temporary Internet Files
- Enabling File Downloads
- Setting Printing Options
- Enabling Pop-Blocker
- Setting Preferences

Enabling JavaScript

This section describes how to enable JavaScript.

To enable JavaScript, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. Click the **Security** tab and click the **Local Intranet** icon as your Web content zone.

3. Click **Custom Level**. The Security Settings dialog box is displayed.

4. In the Settings list and under the Scripting setting, enable all options.

5. Click **OK,** then click **OK** again to exit the Internet Options dialog box.

Enabling Cookies

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

Enabling Temporary Internet Files

Temporary Internet files are pages that you view on the Internet and store in a folder for quick viewing later. You must adjust this setting to always check for new versions of a stored page.

To adjust your Temporary Internet File settings, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. On the General tab, click **Settings**. The Settings dialog box is displayed.

3. Click the **Every visit to the page** option.

4. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. Click the **Security** tab and then click the **Local Intranet** icon as your Web content zone.

3. Click **Custom Level**. The Security Settings dialog box is displayed.

4. Under the Downloads section, ensure that **Enable** is selected for all options.

5. Click **OK**, then click **OK** again to exit the Internet Options dialog box.

Setting Printing Options

This section explains the how to enable printing background colors and images must be enabled.

To enable this option, follow these steps:

1. Navigate to the Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

2. Click the **Advanced** tab. In the Settings list, under the Printing setting, click **Print background colors and images**.

3. Click **OK** to exit the Internet Options dialog box.

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

Enabling Pop-Blocker

You can experience difficulty running the Oracle Financial Services Behavior Detection application when the IE Pop-up Blocker is enabled. It is recommended to add the URL of the application to the Allowed Sites in the Pop-up Blocker Settings in the IE Internet Options.

To enable Pop-up Blocker, follow these steps:

1. Navigate to Tools menu, click **Internet Options**. The Internet Options dialog box is displayed.

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

3. Click **Settings** to open the Pop-up Blocker Settings dialog box.

4. In the Pop-up Blocker Settings dialog box, enter the URL of the application in the text area.

5. Click **Add**. The URL appears in the Allowed site list.

6. Click **Close**, then click **Apply** to save the settings.

7. Click **OK** to exit the Internet Options dialog box.

Setting Preferences

The Preferences section enables you to set your OFSAA Applications Home page.

To access this section, follow these steps:

1. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed. The Preferences page is displayed.
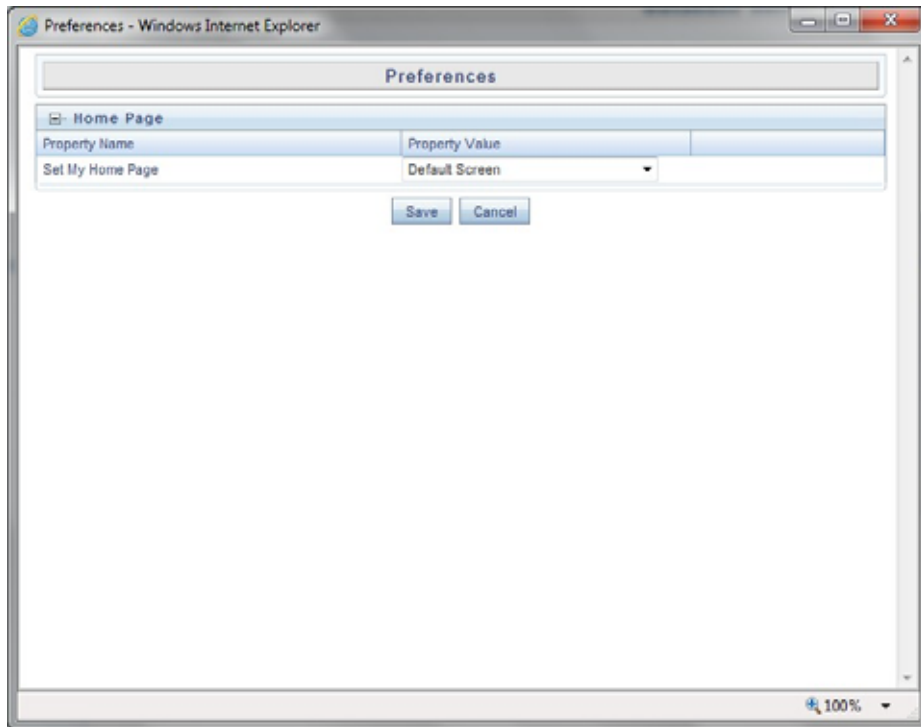
Figure 14. Preference screen

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

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

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

Investigating Alerts

This chapter describes the concept and process of managing Alerts in the Monitoring workflow of the Alert Management system. It provides systematic instructions to carry out various actions according to the workflow and user roles. This helps you to understand how to use various components to accomplish each task.

This chapter covers the following topics:

- About Alerts
- User Roles and Actions
- Alert Workflow
- Analyzing Alerts
- Searching for Alerts
- Acting on Alerts
- Closing Alerts
- Reopening Alerts

About Alerts

OFSBD routinely generates alerts as determined by the configuration of the application in your environment, typically nightly, weekly, monthly, and quarterly. Alerts can be automatically assigned to an individual or group of users and can be reassigned by a user.

Once matches are generated and alerts are created and assigned, OFSBD provides a User Interface (UI) for the investigation and disposition of those alerts. The Alert Management UI allows users to review details of the behavior which led to the alert, information about the focus of the alert, and a history of behavior related to the focus.

Users can take actions on an alert using OFSBD, and move it through a series of statuses to a final disposition.

The following are the tasks you can perform using the Alert Management UI:

- Monitor and analyze system-generated alerts using dashboard
- View detailed information about alerts
- Reassign alerts are reassigned to the appropriate individual or group for a thorough review
- Email and Print Alerts
- Add comments and attach related documents to alerts for further verification
- Designate two parties as trusted pairs
- Identify associated alerts by correlation rules
- Analyze cases related to alerts, and link/unlink cases related to alerts
- Narrate complete analysis of an alert
- Analyze total loss and recovery amount due to specific alert
- Promote alerts to case for further investigation

● Audit all actions that are previously performed on the current alert

User Roles and Actions

This section describes various user roles and actions they can perform in the Managing Alerts workflow.

The following table details the user roles and actions in the Managing Alerts workflow.

Table 2. Alert Management User Roles and Actions

User Actions	User Roles						
Privileges	**Analyst I**	**Analyst II**	**Analyst III**	**Supervisor**	**Executive**	**Internal Auditor**	**External Auditor**
Access to Tabs							
Access to Relationships Tab	X	X	X	X	X	X	X
Access to Narrative Tab	X	X	X	X	X	X	X
Access to Disposition Tab		X	X	X			
Access to Audit Tab	X	X	X	X	X	X	X
Access to Evidence Tab	X	X	X	X	X	X	X
Access to Correlations Tab	X	X	X	X		X	X
Access to Financials Tab	X	X	X	X	X	X	X
Access to Alert Actions							
Access to Add/Modify narrative		X	X	X			
Access to Print Alert Investigative reports (detailed and summary level)		X	X	X	X	X	
Access to Create Alerts		X	X	X			
Access to add Comments	X	X	X	X		X	
Access to remove Attachments	X	X	X	X			
Access to Follow-up or Closing actions (additional restrictions can apply)		X	X	X			
Access to the Reassign action	X	X	X	X			
Ability to Reassign to owners in all organizations (additional access control restrictions can apply)	X	X	X	X			
Access to email actions		X	X	X			
Access to suppression actions			X	X			
Ability to modify the highlight value while creating a suppression rule.			X	X			
Access to reopen actions		X	X	X			
Access to add attachments	X	X	X	X		X	
Access to Financials Functionality							
Access to enter data in Financials data entry sections		X	X	X			
Access to view history in the Financials tab		X	X	X	X	X	

Table 2. Alert Management User Roles and Actions

User Actions	User Roles						
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor
Access to edit existing data on Financials tab		X	X	X			
Access to delete existing data on Financials tab		X	X	X			

Alert Workflow

The following figure shows the potential workflow for managing alerts.
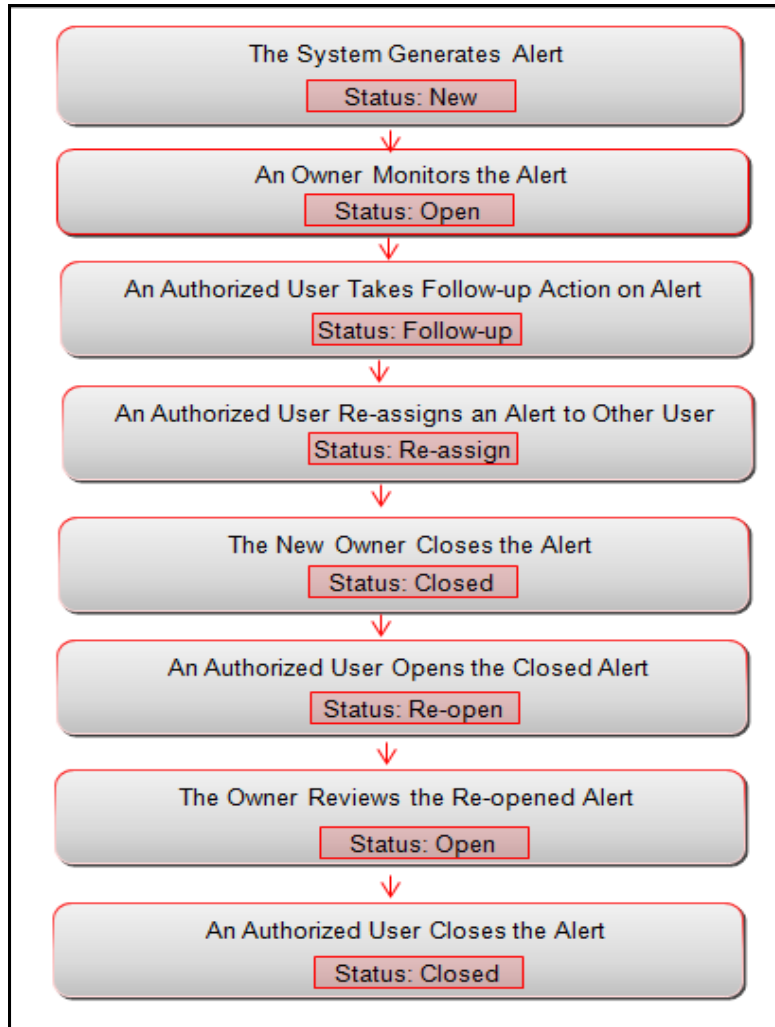
Figure 15. Potential alerts workflow

The following table describes the primary activities associated with managing alerts.

Table 3. Managing Alerts Workflow Table

Action	Description	Roles
Analyzing Alerts	Users monitor and analyze system generated alerts to determine to take various kind of actions.	Analysts I, II, III, and Supervisors
Acting on Alerts	Users can reassign alerts to the most appropriate individual or group, if an alert's initial analysis reveals an issue that should be reviewed by another user. Users can also email, comment, and take addition actions on alerts.	Analysts II, III, and Supervisors

Table 3. Managing Alerts Workflow Table

Action	Description	Roles
Closing Alerts	Alert Management system regularly evaluates all alerts and closes each alert that satisfies the auto close and auto suppress criteria. Users can close alerts manually and by promoting them to case with or without Four-Eyes approval.	Analysts II, III, and Supervisors
Reopening Alerts	Users can reopen closed alerts that require further investigation.	Analysts II, III, and Supervisors

Analyzing Alerts

This section explains how to monitor and analyze system-generated alerts based on your roles. System-generated alerts are in *New* status. To monitor these alerts, you can use the Alert Search and List page, and for in depth analysis, you can use the Details tabs.

Using Alert Details Tabs

The Details tabs in the Alert Management workflow display detailed information about an alert to assist you in your analysis and resolution of the alert.

Details tabs display information according to the focus and entities related to the focus of the alert in accordance with the access permissions appropriate for your role.

The following are two types of details tabs:

- **Alert Details tabs:** These are common tabs that display for all alerts in Alert Details page. For example, Details, Disposition, Correlation, Relationship, Narrative, Evidence, Audit, and Network Analysis.

- **Business Details tabs**: These are unique tabs which display conditionally based on the focus type and scenario class of the alert under investigation.

This section covers the following topics:

- Accessing Alert Details page
- Using Operational Tabs
- Managing Business Tabs

Accessing Alert Details page

This section describes how to access the Alert Details page in the Alert Management workflow to view Alert Details tabs and Business Details tabs.

To access the Alert Details page, follow these steps:

1. Navigate to the OFSAA applications Home page. For more information, see *Chapter 3, Getting Started.*

Note: For more information on searching alerts, see *Searching for Alerts using Views and Searching for Alerts using Alert IDs.*

2. Click **Alert Investigation** in the RHS menu. The Alert Search and List page is displayed.

Figure 16. Alert Search and List Page

For any alert mentioned in the Alert List, you can add an evidence, which can be in the form of an attachment or a comment.

To add a comment, follow these steps:

    a. Select the Comment radio button.

Figure 17. Add Evidence link - Add a comment

    b. Select a standard comment from the Standard Comments field.

    c. Enter any other comments in the Comments field.

    d. Click **Save**.

To add an attachment, follow these steps:

a. Select the Attachment radio button.

Figure 18. Add Evidence link - Add an attachment

b. Click **Attach** and select a file.

c. Click **Upload**.

You can also add comments for the attachment using the Attach Comments field.

3. Click the number in the **Alert ID** column. The Alerts Details page is displayed.

Figure 19. Alerts Details page

Using Operational Tabs

This section explains the various operational tabs which are enabled to all users to monitor and carry out comprehensive analysis to take appropriate action on an alert.

This section covers the following topics:

- Using Details Tab
- Using Disposition Tab
- Using Correlation Tab
- Using Relationship Tab
- Using Narrative Tab
- Using Evidence Tab
- Using Audit History Tab

Using Details Tab

The Alert Details tab gives you access to detailed information regarding each match associated with an alert and the information that triggered each match.

When an Analyst I, II, III, or Supervisor views the alert details, the alert's status changes from New, Reassigned, or Reopened to Open if the user is an owner of an alert. For more information, see *Additional Information* section. If your firm configured your deployment to use the Alert Inheritance feature, and an organization or group owns the alerts, an Analyst I, II, III, or Supervisor takes ownership of the alert when the user views the alert details. Internal and External Auditors can view the alert details, but the application does not assign the alert to them or change the status.

Within the Alert Details tab, you can access additional information related to the alert by selecting one of the tabs on the page.

Note: When you navigate to the Alert Details tab for an alert, the alert gets locked and the system allows other users *view only* access to the alert. If other users attempt to access the same alert they receive a message informing them that the alert is locked by another user and granted only view rights (they cannot take any action on the alert).

This section covers the following topics:

- Viewing Alert Context Information
- Viewing Matched Information

Viewing Alert Context Information

This section provides a brief description of the alert and the context for determining what actions need to be taken to dispose the alert. This area is displayed on top of every tab. The fields that display in the Alert Context are based on the solution set associated with the class of the scenario generating the alert.

The alert context initially displays in a contracted mode. Only the Alert ID, Focus, Status, and Score are visible.

To view the complete details of the context you can click the **Expand** icon to expand the context section for additional information on the alert.

For more information on the list of fields that display in the Alert Context information based on your scenario class of the alert, see .

Viewing Matched Information

This section provides the matched information that triggered the alert as a function of the scenario. The matched information can show a single match or multiple matches, if it is a multi-match alert. Detailed information is displayed in the form of building blocks. The building blocks display when you click the match in the Matched Information section. The LHS (Left Hand Side) menu helps you navigate through the detailed information in the building blocks. The information corresponding to the LHS menu refreshes for each selection of match from the Matched Information section. The information in this area is a snapshot in time of when the application created the alert and does not get updated. This contrasts with data on Business tabs that display the most recent submitted data. The **Excel** icon is displayed next to the building block name if the data that the matched information contains qualifies for Excel Upload functionality.

This section covers the following topics:

- Viewing Thresholds Details
- Viewing Score Details
- Viewing All Transactions Details Page

- [Viewing Summary Details Page](#)
- [Designating Trusted Pairs](#)

Viewing Thresholds Details

If your role permits, you can view the thresholds that are defined at the time the alert was generated. If you are viewing a multi-match alert, each match displays a separate Thresholds link. The layout of the information that this area contains varies based on the focus type, entity type, and scenario class of the alert.

To view threshold details, follow these steps:

1. Navigate to the Matched Information section in the Alert Details page.

2. Click the **Thresholds** link. The Threshold Details window is displayed with Threshold details and values.

Viewing Score Details

If your role permits, you can view scoring rules defined for the scenario that generated the match, and the match's actual value of each scoring variable associated with the scenario's scoring rule. In addition, it displays how the individual scoring values are added up to the total and final score of the match. If you are viewing a multi-match alert, each match displays a separate scoring link. The layout of the information that this area contains varies based on the focus type, entity type, and scenario class of the alert.

To view score details, follow these steps:

1. Navigate to Matched Information section in Alert Details page.

2. Click the **Score** link. The Score Details window is displayed with score details and values.

Viewing All Transactions Details Page

The Transaction Details page provides detailed information of the transactions that occurred between the beneficiary and remitter on an alert.

Note: The Transaction Details icon is displayed in the Electronic Funds Transfer Transactions, Check, Monetary Instrument Transactions, and Back Office Transactions building blocks of the Alert Details tab.

To view transaction details, follow these steps.

1. Navigate to the Matched Information section in the Alert Details page. Click the **Details Show All Transactions** icon available on each row in the Transaction building blocks. The Transaction Details window is displayed.

Viewing Summary Details Page

The Summary details page allows you to view the focal entity-related information in the form of a section for an alert. The section provides the detailed information that is specific to a focal entity summary.

For example, for an Account Summary building block in an Alert Details tab, the Summary Details tab displays detailed information regarding the account's deposits and disbursements across a rolling twelve month period.

To view transaction details, follow these steps.

1. Navigate to the Matched Information section in the Alert Details page.

2. Click the **Summary** icon in the Summary building blocks. The Summary link window displays a thirteen-month summary.

   Or, in the Business tabs, a three-month summary is displayed on the tab. Click **Summary**. The Summary link window displays a twelve-month summary.

Or, in the Correspondent Bank tab, for Correspondent Bank Peer Group Summary, click **Summary**. The Summary link window displays a twelve-month summary.

Designating Trusted Pairs

If your role permits, your application is configured to allow designation of trusted pairs via the user interface. If an alert has one or more matched transactions records, a Designate Trusted Pairs link appears on the Matched Information section.

To designate trusted pairs, follow these steps:

1. Navigate to the Matched Information section in the Alert Details page.

2. Click **Designate Trusted Pairs**. The Designate Trusted Pairs window is displayed with a list of potential trusted pairings for the selected alert with a check box against each pair.

    For more information, see *Chapter 6, Managing Trusted Pairs* for instructions on how to designate trusted pairs.

    Note: User-initiated alerts do not provide matched information.

Using Disposition Tab

The Disposition tab is used to select an action for disposition of the alert. This helps you to complete your analysis of the alert. The Disposition tab contains actions which, when taken, result in the closure of the alert. Once a closing action or actions is taken, the history of the closing actions shows on this tab.

Key features of disposition are as follows:

● Choosing an action for alert disposition, such as close and suppress the alert or move the alert status to closed

● Reassign the alert to another user

● Provide a due date for the alert for suppression actions

● Provide comments for the alert

Note: The Audit tab provides a complete view of all actions and the associated modifications and changes taken on the alert, whereas the Disposition tab provides a concise view of the action or actions taken to resolve or dispose the alert.

Taking an Action on the Alert

The Take Action section allows you to choose an action to take on the alert. Some of the actions are listed below:

Note: You can select one or more of the actions using the Choose Action field. If you cannot select a particular combination of actions, an error message is displayed

● **Close and Suppress-Enter Date**: To close a suppressed alert until a particular date, select this action. You cannot select this action with any other suppression actions.

● **Close and Suppress 1 Year**: To close a suppressed alert for a year, select this action.

● **Close and Suppress 6 Months**: To close a suppressed for 6 months, select this action.

● **Close and Suppress 3 Months**: To close a suppressed alert for 3 months, select this action.

● **Close and Suppress 1 Month**: To close a suppressed alert for 1 month, select this action.

● **Invalid Alert**: To move the alert status to closed, select this action.

- **Withheld Action**: To move the alert status to closed, select this action.

- **Promote to Case**: To promote the alert to a case, select this action.

To take an action on the alert, follow these steps:

1. Navigate to the Take Action section in the Disposition Tab.

2. In the Choose Action field, select an action to be taken on the alert.

Figure 20. Disposition Tab

After you select an action, you can perform other actions in the Action Information field. These actions are described below:

Field	Description
Choose Action	Select an action taken to resolve or dispose the alert. The below fields are editable only if you select one or more actions.
Reassign	Select the user to whom you want to reassign the alert. This field is read-only if you select the Auto Assignment check box.
Auto Assignment check box	To auto-assign the alert to the selected user, select this check box.
Set Due Date	Select a due date for the alert.
Suppression End Date	Select the date until when the alert is suppressed. This action is editable only if you select **Close and Suppress-Enter Date** as a suppression action.
Suppression Highlight	Select a name for the suppression condition. This action is editable only if you select a suppression action.
Suppression Operato	Select an operator for the suppression condition. This action is editable only if you select a suppression action.
Suppression Value	Select a value for the suppression condition. This action is editable only if you select a suppression action.
Standard Comments	Select a comment from the list. You can select more than one comment.
Comments	Enter any other comments that you have.

Once you select the required actions, you can save the selection and attach documents.

If you select Promote to Case, the Next button is displayed. Once you click **Next**, you must select the required values in the Promote to Case section and click **Save**.

Using Correlation Tab

A Correlation is defined as a group of alerts that are associated to one another based on matching a set of criteria as defined by a correlation rule.

Key features of correlation are as follows:

- The establishment of business relationships between the entity or entities associated with an alert to other business entities, which can exist in your firm's data.

- Using these business relationships and the criteria specified for a correlation rule, an Alert Correlation can be created.

- An alert can be a part of more than one correlation.

- The Correlation rules are defined by organization.

  Note: Contact with your system administrator for more information on correlation rules, which your firm can use.

The Alert Correlation tab provides detailed information regarding the business associations of the current alert. In the context of an alert, the tab enables you to view a list of all correlations of which the current alert is a member as well as a list of the business entities associated with the current alert, regardless of whether those entities become part of a correlation.

This section covers the following topics:

- Viewing Correlation Summary
- Viewing Correlation Memberships
- Viewing Correlation Business Entities

Viewing Correlation Summary

The Correlation Summary section displays a list of correlations for which the alert is a member. By default, the section includes up to five of the most recent correlations. If the alert is a member of more than five correlations, then you can use the pagination options in the Summary section to navigate to the additional correlations.

The Correlation Summary section displays the correlations in chronologically descending order based on the update date associated with the correlation, and then by numerically ascending order by Correlation ID.

If your firm has implemented Oracle Financial Services Enterprise Case Management and the correlation is promoted automatically to a case, then the summary record contains a Case ID. If your role permits access to the case, then the section displays the Case ID as a link.

To view correlation summary information, follow these steps:

1. Navigate to the Correlation Summary section in the Correlation Tab.
2. Click **Correlation ID**. The Alert Details page is displayed.

Figure 21. Correlation Tab

Table 10 describes fields in the Correlation Summary section.

If the alert has one or more correlations associated with it, then by default the first correlation from the Correlation Summary section displays records in the Correlation Memberships section corresponding to the selected summary.

Viewing Correlation Business Entities

The Correlation Business Entities section calculates and displays a distinct list of business entities to which the currently selected alert is associated. In addition, it displays the total number of distinct alerts to which each displayed business entity is correlated. These correlated business entities display in the alphanumeric ascending order based on the Entity field.

To view business entity information, follow these steps:

1. Navigate to the Correlation Business Entities section in the Correlation Tab.

2. Click **Entity**. The Business Entity information window is displayed.

   By default, the section includes up to ten of the most recent correlated business entities. If there are more than ten correlation business entities, you can use the pagination options to navigate to additional records.

   Note: If your role permits, the Correlation Business Entities section displays each entity as a link to the new window.

   Table 4 describes the fields for the Correlated Business Entities section.

Table 4. Fields for the Correlated Business Entities for Alert [ID]

Field	Description
Entity	Displays the concatenated value of the two character, that is, business entity type code and the business entity identifier.
Relationship	Displays a translated data path name for each business entity to alert correlation.
Total # of correlated Alerts	Displays the total count, including the current alert (distinct alerts) to which the business entity is correlated.

Using Relationship Tab

The Relationship tab provides information regarding other alerts related to the current alert being analyzed. In context of an alert, the tab enables you to view the list of alerts related through entities and correlations. If your firm has implemented Oracle Financial Services Enterprise Case Management, the Relationship tab also display cases related to the current alert. Cases can be related to the current alert either through a common business entity association or by virtue of the current alert being linked to a case. If your firm has implemented Oracle Financial Services Enterprise Case Management, and your role permits, then you can link, unlink, and add more links in the Related Cases section.

This section covers the following topics:

- Viewing Related Alerts
- Managing Related Cases

Viewing Related Alerts

The Relationship tab displays up to eleven of the most recent alerts related to the focus of the alert, where the related alert can be focused on the same entity as the current alert or can be focused on entities related to the focus of the current alert. This can include alerts considered related to the focal entity of the current alert based on matching one or more business entities to alert correlation rules. If the number of alerts exceeds the default, you can use the pagination option in the Related Alerts section to view additional records.

To view related alerts, follow these steps:

1. Navigate to the Alert Details page.

2. Select the **Relationship** tab. The Relationship page is displayed.
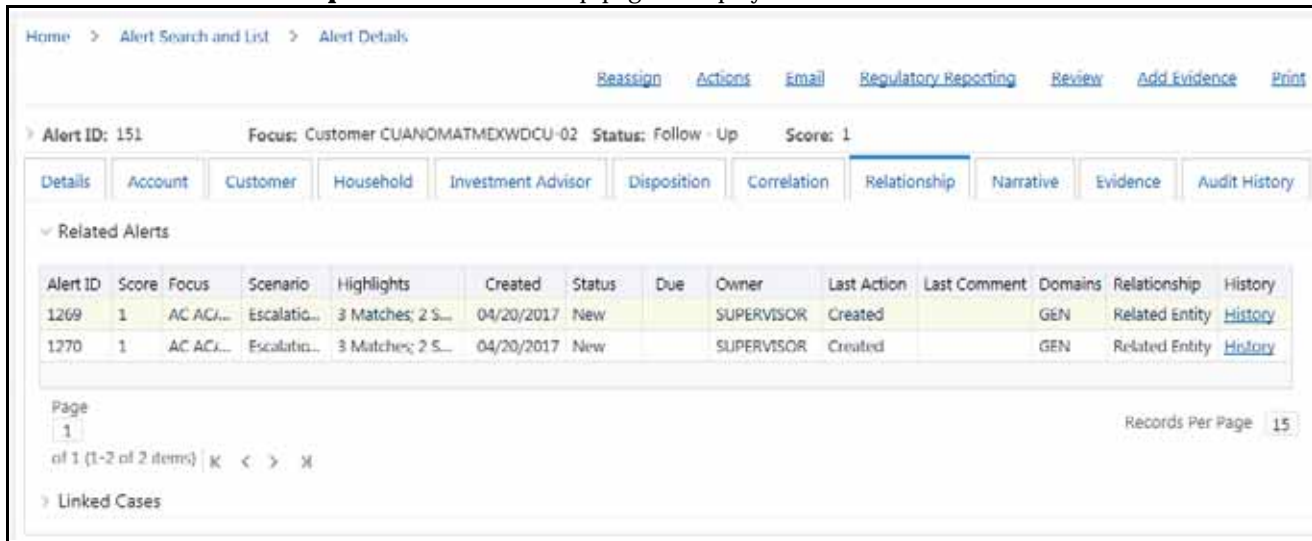
Figure 22. Relationship Page

The following table lists the possible related focus types that can appear in the Related Alerts section.

Table 5. Related Alerts by Focus Type

Current Alert Focus Type	Related Focus Types
Employee	Account and Customer
Account	Employee, Household, Customer, and Correspondent Bank
Customer	Account, Related Customer, Correspondent Bank, and Employee
Household	Account, Customer, and Employee
Correspondent Bank	Customer
Representative	Employee
Portfolio Manager	Employee and Account

The following table lists the fields displayed for the Related Alerts section.

Table 6. Related Alerts

Columns Displayed	Description
Alert ID	Displays the unique identification number of an alert. It also serves as a link to the Alert Details tab.
Score	Displays the score that alert has received.
Focus	Displays the focus on which the alert is based. Both the focus type abbreviation and the focus name are displayed.
Scenario	Displays the scenario name of the behavior or activity that generated the alert.
Highlights	Displays the pertinent information related to the alert. The Highlights column display "- -", when no highlights are found for an alert.
Created	Displays the date of alert creation.
Status	Displays the current state of alert relative to its analysis and closure.

Table 6. Related Alerts (Continued)

Columns Displayed	Description
Due	Displays the date an action associated to an investigation record is to be completed. Blank value indicates a due date is not set.
Owner	Displays the name of an individual or group of users to whom the alert is assigned.
Last Action	Displays the action representing the last action recorded for an alert.
Last Comment	Displays the comment associated with the last action recorded for an alert.
Domains	Displays the business domains associated with the alert focus.
Relationship	Displays the translated data path name for each business entity to alert correlation.
History	Click **History** to view the history of the related alert in a window.

Managing Related Cases

The Related Cases section displays up to five of the most recent cases to which the current alert is either linked or related. The list is sorted in descending chronological order by Created Date. If the number of cases exceeds the default, you can use the pagination option in the Related Cases section to view additional records.

Note: The following section on Related Cases is only applicable if your firm has implemented Oracle Financial Services Enterprise Case Management. For more information on case management, see *Oracle Financial Services Enterprise Case Management User Guide*.

This section covers the following topics:

- Viewing Related Cases
- Linking Cases
- Unlinking Cases
- Adding More Cases

Viewing Related Cases

Related cases are displayed for an alert based on the case having a business entity that is either the focus of the current alert or has one of the mentioned business relationships with the focus of the current alert.

To view related cases, follow these steps:

1. Navigate to the Alerts Details page. Select the **Relationship** tab.

2. Go to the Related Cases section. Click the **Case ID**, the page navigates you to the Case Details tab.

The following table describes the fields of Related Cases.

Table 7. Related Cases Fields

Columns Displayed	Description
Check box	Displays a check box to link or unlink actions.
Linked	Displays whether the case is linked or not. *Yes* referred as linked and *No* referred as not linked.
Case ID	Displays unique identification Case number. Click the link to view the Case Details page.
Title	Displays the name of the case displayed in the case list section.
Type	Displays the type of the case displayed in the case list section. For example, AML.
Subtype	Displays the subtype of the case displayed in the case section. For example, AML Surveillance.
Subclass 1	Displays the type code of the case Subclass 1 associated with this case subclass.
Subclass 2	Displays the type code of the case Subclass 2 associated with this case subclass.

Table 7. Related Cases (Continued)Fields

Columns Displayed	Description
Created [Date]	Displays the date on which the case was created.
Alerts Due [Date and Time]	Displays the date and time by which an action should be taken on the case. **Note:** The definition of nearly due is a value that is configurable by your firm.
Owner	Displays the name or unique identification number of an individual or group of users who own the case.
Assigned To	Displays the name or unique identification number of an individual or group of users who are assigned to the case.
Priority	Displays the priority given to the case under investigation.
Organization	Displays the organization or group that owns the cases.
Status	Displays the current state of the case relative to its analysis and closure. The New, Reopened, and Reassigned statuses display in bold text.
Regulatory Reporting Status	Displays the case list by the current status of a case that is recommended for Regulatory Reporting, an optional Oracle Financial Services application.
Last Action	Displays the case list by one or more selected last actions that are taken on the case. If you filter by Last Action, you cannot filter by Resolution and Action.
Last Comment	Displays the comment associated with the last action recorded for a case.
Linked Alerts	Displays the case list by count of alerts that are linked to the case. Alert Management retrieves cases, which are either greater than or equal to, equal to, or less than or equal to the count you enter in the text box. This search option is only be available if your firm has implemented Behavior Detection framework.
User Linked	Displays whether the relationship is based on user-defined link or system-defined link. It displays *Yes* when user manually links an alert/case and *No* when system linked an alert/case (as part of alert promotion and correlation promotion to a case).
History	Displays the history of the related case in a window.

Adding More Cases

If you analyze and determine that an alert has association with many more cases and they are not part of the list, then you can search such cases and you are allowed to link those cases with the selected alert. This section describes how to add more cases to an alert.

The Add More Cases option allows you to search for any case record by Case ID for the purpose of adding additional case links to the current alert.

To add more cases to an alert, follow these steps:

1. Navigate to the Alerts Details page. Select the **Relationship** tab.

2. Go to the Related Cases section. Click **Add More Links**. The Add More Links dialog box is displayed.

3. Enter the required Case IDs to search for additional cases. Click **Go**. The required additional cases are displayed in the list.

4. Select one or more check boxes against each case to link to an alert. The Add Comments dialog box is displayed.

5. Select the Transfer Alert Information from drop-down list. For example, Account, Customer, and so on.

6. Enter your justification in Comment box to link cases. The confirmation dialog box is displayed with the following message: *The selected cases will be linked. Click OK to save the changes.*

7. Click **OK**. The confirmation dialog box is displayed with the following message: *Selected alerts and cases were linked and requested transfer of alert information is also completed.* The Alert Management system records the action, updates the alert information, and returns you to the refreshed Relationship tab.

Note:

For more information on the modes for transfer of alert information, see *Promoting Alerts to Cases with Four-Eyes Approval.*

When the transfer alert information is in asynchronous mode, the system processes the data transfer in the background, allowing you to continue to work. Notification of failure of the data transfer is made through the Notifications section on your Home page.

- If you do not make a selection of at least one data type of information to be transferred, the system will default to transferring all possible alert data during the link (that is, not making a selection is equivalent to selecting all).

- The data transferred to the case is the data available as of the date of link action.

- The alert information that is already associated with the case as a result of previous promotion or link actions will not be transferred again during the current link action.

- During unlink action, when one or more alerts are unlinked from the case, the alert information, which is transferred during link action will not be removed by the system. If required, you can manually remove the alert information from the appropriate Enterprise Case Management tabs through the remove action.

- For link or unlink actions, the case must be in a non-closed status.

Using Narrative Tab

The Narrative tab allows you to capture and modify any narrative surrounding the analysis of an alert that has helped you decide how to dispose of the alert. This allows you to format text using Rich Text Format (RTF). The narrative exists as a single data element on an alert, which allows you to add and maintain narrative.

This section covers the following topics:

- Creating Narrative
- Editing Narrative
- Deleting Narrative

Creating Narrative

This section explains how to create a narrative analysis for a selected alert.

To create a narrative for a selected alert, follow these steps:

1. Navigate to the Alerts Details page.

2. Click the **Narrative** tab. The Narrative page is displayed.
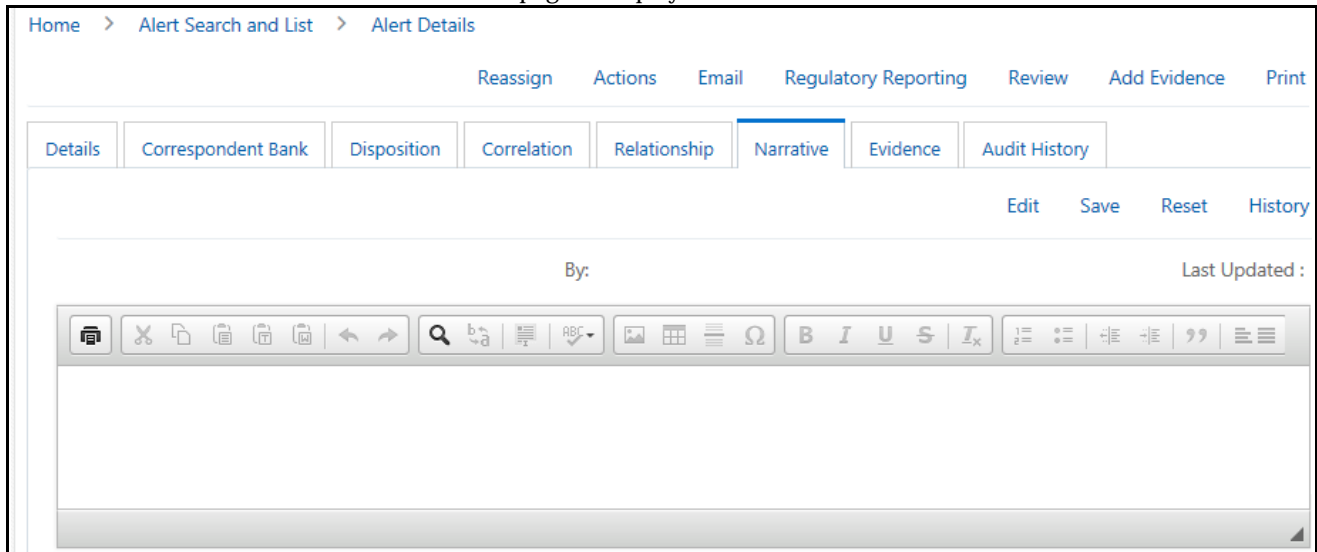
Figure 23. Narrative Page

3. Click **Edit.** The Alert Narrative box is enabled to enter your analysis using RTF.

4. Enter the required narrative analysis for an alert in the text box.

5. Click **Save**. The application saves your changes, adds the current date to the Last Updated field and adds your name to the By field in the Narrative section.

Editing Narrative

This section explains how to edit an existing narrative analysis for a selected alert.

To edit a narrative for a selected alert, follow these steps:

1. Navigate to the Alerts Details page. Select the **Narrative** tab. The Narrative page is displayed.

    If the narrative analysis is already created, the Narrative tab displays last updated details, date, and the user who has created the narrative.

2. Click **Edit.** The Alert Narrative box is enabled to modify the analysis.

3. Modify the necessary changes in the text box.

4. Click **Save**. The application saves your changes, adds the current date to the Last Updated field and adds your name to the By field in the Narrative section.

Deleting Narrative

To delete a narrative for a selected alert, follow these steps:

1. Navigate to the Alerts Details page. Select the **Narrative** tab. The Narrative page is displayed.

2. Select the text and press **Delete**. This can only be done when you have selected to edit the narrative.

3. Click **Save**. The application saves your changes, adds the current date to the Last Updated field and adds your name to the By field in the Narrative section.

Using Evidence Tab

The Evidence tab allows you to view, add, and remove comments or attachments to the alert under investigation.

Viewing Comments and Attachments

This section allows you to view various comments and attachments related to the selected alert.

To view comments and attachments, follow these steps:

1. Navigate to the Alerts Details page.

2. Click the **Evidence** tab. The Evidence page is displayed.

Figure 24. Evidence Page

3. Go to the Comments section to view the following details.

Table 8. Comment section

Headings	Description
Date	Displays creation date and time of the comment.
By	Displays the name of person who carried out this action.
Status	Displays the status of alert.
Comments	Displays the comments provided by the last person.

4. Go to the Attachment section to view the following details.

Table 9. Attachment section

Headings	Description
Date	Displays creation date and time of the attachment.
By	Displays the name of person who carried out this action.
Status	Displays the status of alert.
Comments	Displays the comments provided by the last person while attaching.
Attachment Name	Displays the name of attachments.
Attachment	Displays the number of attachments.

To add comments or attachments for an evidence, use the **Add Evidence** link. For more information, see the *Accessing Alert Details page* section.

Using Audit History Tab

The Audit History tab allows you to view all actions that are previously performed on the current alert.
This tab includes the following details:

- Date and time of the alert action

- Types of action taken on alert

- Owner of the alert at the time of the action

- User who took the action

- Alert status at the time of the action or resulting from the action

- Comments associated with the action

- Attachment name

The Audit History tab also allows you to view a history of the current alert when it was viewed by the owner or other users, regardless of any action being taken. These entries are recorded in situations when a user navigates to the details of an alert from the Alert List page link or any alert link where it appears within Alert Management. The system records Viewed Alert Details as an action regardless of the current status of the alert. This action does not result in any status change for the viewed alert.

This section covers the following topics:

- Filtering View Only Action

- Filtering Status Changing Actions

- Filtering Alerts with Attachments

- Viewing Attachments and Comments

Filtering View Only Action

As the number of Viewed Alert Details entries can become numerous over the course of working on an alert, you can modify the Display View Only Action option to filter this action out of the audit list for the current alert.

To view only those alerts that are viewed by users in the Alert List, follow these steps:

1. Navigate to the Alerts Details page.

2. Click the **Audit History** tab. The Audit History page is displayed,
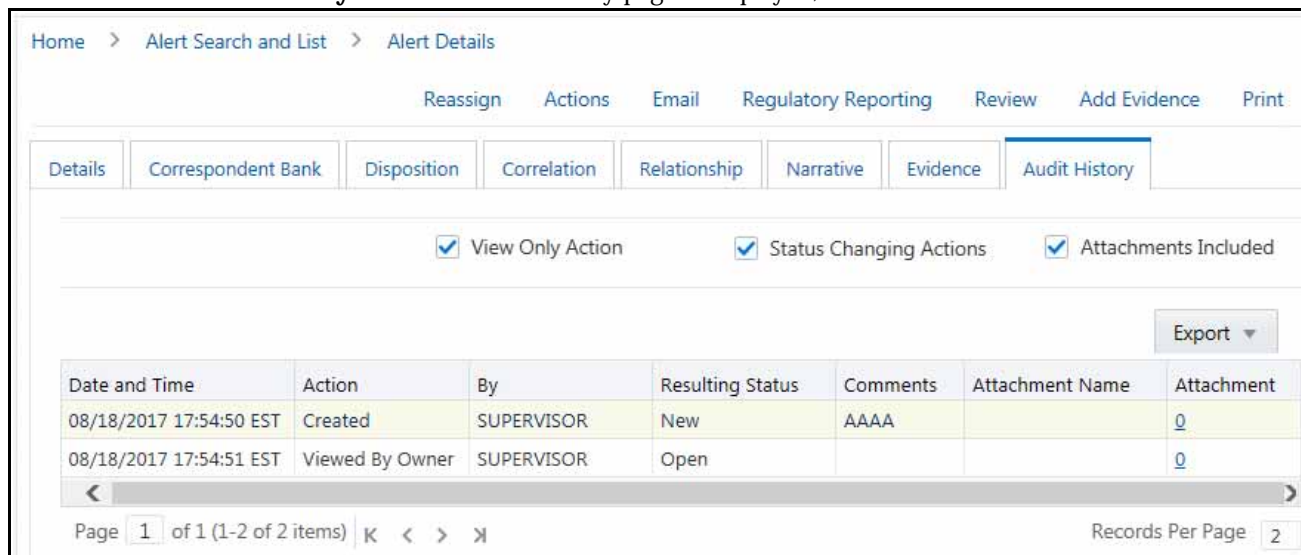
Figure 25. Audit History Page

3. Go to the Set Option for Audit Display section and select the check box against **View Only Action**.

When the check box is selected, the Audit list displays the Viewed Alert Details in the current appropriate sort order for the list. If the check box option is deselected, then the Viewed Alert Details actions are filtered out of the list display.

Filtering Status Changing Actions

Use the Status Changing Actions option to view all the different statuses assigned to an alert.

To view the statuses of the alert, follow these steps:

1. Navigate to the Alerts Details page. Select the **Audit History** tab.

2. Go to the Set Option for Audit Display section and select the check box against **Status Changing Actions**.

When the check box is selected, the Audit list displays the different statuses for the alert chronologically. If the check box option is deselected, then the Status Changing Actions are filtered out of the list display.

Filtering Alerts with Attachments

Use the Attachments Included option to view all the alerts that have attachments. You can also view the attachment name by clicking the hyperlink in the Attachment column.

To view the alerts that have attachments, follow these steps:

1. Navigate to the Alerts Details page. Select the **Audit History** tab.

2. Go to the Set Option for Audit Display section and select the check box against **Attachments Included**.

When the check box is selected, the Audit list displays the different alerts that have attahcments. If the check box option is deselected, then these alerts are filtered out of the list display.

Viewing Attachments and Comments

Attachments and comments by various users helps you to take appropriate action on alerts.

To view attachments and comments related to the alert, follow these steps:

1. Navigate to the Alerts Details page. Select the **Audit** tab. The Audit page is displayed.

2. Go to the Actions Taken on Alert section and click the **Attachment** icon in the Attachment column. The Attachment dialog box is displayed.

3. To add comments, go to the Comments column, click **Expand** to view the full text of the comment that exceeds the width of the column. The **Expand All/Collapse All** is also available on the header.

   When both standard comments (comments selected from a preset list of comments) and free text comments display with an action, the free text comments appear appended with the selected standard comments.

   If your firm has implemented Oracle Financial Services Enterprise Case Management and the alert is, or is, associated with a case, you can see actions related to the linking and unlinking of the alert from a case. In the Comments column, for Link and Unlink actions, the Case ID(s) of the linked or unlinked cases are appended with the user-entered comments.

Managing Business Tabs

The Business tabs are displayed conditionally based on the focus type and scenario class of the alert under investigation.

Business tabs correspond to similarly named information blocks that display within the Matched Information area on the Details tab. However, the information displayed on the Business tab updates each time your firm submits data, whereas the information contained with the Matched Information section is static. When viewing a Business tab, it displays *Updated On*, indicating the date of the last data submission.

For example, if an account-focused alert is generated within the Money Laundering scenario class, Oracle Financial Services Behavior Detection Framework displays the Account, Account Balance, Account Summary, Account Peer Group Summary, Customer, Employee, Household, Network, and Investment Advisor business tabs in addition to the Details tabs described in *Using Operational Tabs*.

By default, the Business Entities section displays five records. The lists of Business Entities have buttons for the following view options.

- Related to Alert filters the data that is being displayed on the business tab based on an entity's involvement in an alert.

- Related to Focus presents all business data associated with the focal entity of the alert, regardless of their involvement in the current alert.

  For example, if the current alert is Customer-focused and you select the Account tab, Related to Alert shows you the information only about those customer's accounts that are directly involved in the alerting behavior. Selecting Related to Focus shows you information about all customer's accounts, even if they are not involved in the current alert.

By default, the Related to Alert data is displayed. Not every Business tab displays both Related to Alert and Related to Focus. To use an previous example, for a Customer-focused alert, the Customer tab does not display Related to Focus, as there is no additional information it offers about the focal customer.

This section covers the following topics:

- Viewing Business Tabs
- Managing Financials Tab
- Replay Tab

Viewing Business Tabs

Appendix D, *Business Tabs* lists the possible Business tabs that display relative to the workflow (alert) of an application and based on a specific focus type and scenario class.

Managing Financials Tab

In the course of investigating fraudulent activity, it is necessary to track data pertaining to potential and actual losses (which can result from the activity identified), as well as to track any amounts that can be recovered during the course of the investigation. The Financials business tab is designed to manage loss and recovery data, provide a mechanism to enter, edit and audit the data. This tab is visible based on user roles. For more information on User privileges, see Appendix A, *User Privileges.*

This section covers the following topics:

- Accessing Financials Tab
- Managing Current Loss and Recovery
- Managing Loss and Recovery

Accessing Financials Tab

This section explains how to access the Financials tab.

To access the Financials tab, follow these steps:

1. Navigate to the Alert Search and List page.

2. Click **Search** or **Advanced Search**. The respective Search page is displayed.

3. Select **Fraud** from the Scenario Class drop-down list. The list of Fraud Scenario alerts is displayed.

4. Click the required **Alert ID**. The Alert Details page is displayed.

5. Click **Financials** Tab. The Financials Tab is displayed.

This tab is visible based on the user-role as defined in Appendix A, *User Privileges*.

Figure 26. Financials Page

Managing Current Loss and Recovery

This section provides information for total loss and recovery values, primary general ledger, cost center, and offset account information.

This section covers the following topics:

- Viewing Current Loss and Recovery Details

- Adding Current Loss and Recovery Details

- Editing Current Loss and Recovery Details

- Removing Current Loss and Recovery Details

Viewing Current Loss and Recovery Details

This section allows you to view information pertaining to the cost center and general ledger financial details.

To view current loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Go to the Current Loss and Recovery Summary section to view cost center and general ledger financial details.

The following table lists and describes the individual information fields for the Current Loss and Recovery section.

Table 10. Current Loss and Recovery Information Fields

Field	Description
Total Potential Loss Amount	Displays the total potential financial loss that the institution can experience as a result of the fraudulent activity identified by the alert. This value is calculated as an aggregate of all active Potential Loss data items for the alert.
Total Averted Loss Amount	Displays the total financial loss amounts that the institution can be able to prevent based on actions taken during the course of the investigation into the fraudulent activity identified by the alert. This value is calculated as an aggregate of all active Averted Loss data items for the alert.
Total Recovered Amount	Displays the total financial losses that are recovered during the course of the investigation into the fraudulent activity identified by the alert. This value is calculated as an aggregate of all active Recovery data items for the alert.
Total/Net Loss Amount	Displays the total loss remaining after Averted Loss and Recovery Amounts are subtracted from the Potential Loss. It is calculated as: Potential Loss – Averted Loss – Recovery Amounts = Total/Net Loss Amount
Primary GL Account	Displays the primary general ledger (GL) account to which the total net loss amount for this investigation is associated.
Primary Cost Center	Displays the primary cost center to which the total net loss amount for this investigation is associated.
Offset Account	Displays the offset account associated with loss and recovery financial for this investigation.
Offset Cost Center	Displays the offset account's cost center associated with loss and recovery financials for this investigation.
Charge Off Date	Displays the date on which the loss was charged off.
Last Updated Date	Displays the date and time at which loss and recovery data was last updated.
Last Updated By	Displays the last user who update loss and recovery data.

Note: The total loss and recovery summary values are displayed with the current information on entry into this page and are refreshed only when you enter or edit the relevant data in the Loss and Recovery Data Entry section and save it.

Adding Current Loss and Recovery Details

This section allows you to add information pertaining to cost center and general ledger financial details.

To add current loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.
2. Go to the Current Loss and Recovery Summary section.
3. Click **Add/Edit**. The Cost Center and General Ledger Financials dialog box is displayed.

Figure 27. Cost Center and General Ledger Financials Dialog Box

4. Enter the following information in the respective fields.

Table 11. Cost Center and General Ledger Financials

Fields	Description
Total Potential Loss Amount	Enter the total possible loss amount in USD. For example, USD 35,00,000.
Total Averted Loss Amount	Enter the total averted loss amount in USD.
Total Recovered Amount	Enter the total recovered loss amount in USD.
Total/Net Loss Amount	Enter the net operating loss in USD.
Primary GL Account	Enter the primary general ledger account. The primary General Ledger (GL) account to which the total net loss amount for this investigation is associated.
Primary Cost Center	Displays the primary cost center to which the total net loss amount for this investigation is associated with.
Offset Account	Enter the offset account. The Offset account associated with loss and recovery financials for this investigation.
Offset Cost Center	Displays the Offset account's cost center associated with loss and recovery financials for this investigation.
Charge off Date	Displays the date on which the loss was charged off.
Last Updated Date	Displays the date on which the above details were last updated.
Last Updated By	Displays the name of the user who last updated the above details.

5. Click **Save**. The following message is displayed: *Would you like to save these actions?*

6. Click **OK**. The Current Loss and Recovery Summary information is updated.

Editing Current Loss and Recovery Details

This section allows you to modify information pertaining to the existing cost center and general ledger financial details.

To modify current loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Go to the Current Loss and Recovery Summary section. Click **Add/Edit**. The Cost Center and General Ledger Financials dialog box is displayed with existing information.

3. Modify the necessary information in the respective fields. For more information on the fields, see *Adding Current Loss and Recovery Details* section.

4. Click **Save**. The following message is displayed: *Would you like to save these actions?*

5. Click **OK**. The Current Loss and Recovery Summary information is updated.

Removing Current Loss and Recovery Details

This section allows you to delete information pertaining to cost center and general ledger financial details.

To remove current loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Go to the Current Loss and Recovery Summary section. Click **Remove**. The following message is displayed: *You have selected to remove the Primary GL Account and Cost Center information associated with this investigation. Select OK to continue and save the changes.*

3. Click **OK**. The Current Loss and Recovery Summary information is updated.

Viewing History of Current Loss and Recovery Details

This section allows you to view the details of an alert.

To view the details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Go to the Current Loss and Recovery Summary section.

3. Click **History**. The Cost Center and GL Financials Data Entry History dialog box is displayed.

Figure 28. Cost Center and GL Financials Data Entry History

Managing Loss and Recovery

This section provides information for individual loss and recovery values.

This section covers the following topics:

- Adding Loss and Recovery Details
- Editing Loss and Recovery Details
- Removing Loss and Recovery Details

Adding Loss and Recovery Details

This section allows you to add information pertaining to potential loss, averted loss, and recovery details.

To add loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Go to the one of the Potential Loss, Averted Loss, or Recovery sections andclick **Add**. The Loss and Recovery Data Entry dialog box is displayed.

Figure 29. Loss and Recovery Data Entry Dialog Box

3. Enter the following information in the respective fields.

Table 12. Loss and Recovery Data Entry Fields

Field	Description
Data Entry Type	Displays a pre-populated type as per the data entry type selected (for both add/edit), that is, Potential Loss, Averted Loss, or Recovery.
Cost Center	Select the cost center to which this loss or recovery item should be associated from the drop-down list. This field associates this cost center to the current item being entered only and not the overall alert, appropriate for the entire alert. It allows you to associate a different cost center to an individual item than can be appropriate for the entire alert. **Note:** This drop-down list is populated with available cost centers as defined by your firm. If you require additional values, contact your System Administrator.
Date	Enter the date on which this loss or recovery item was incurred.
Loss Payee (if applicable)	Enter the loss payee details.This is payee identified for the loss amount represented by this record.
Amount	Enter the respective amount of the loss or recovery record. **Note:** The system accepts values in base currency only. You must enter the amount in the correct base currency format.
Loss Averted Type (if applicable)	Select the loss averted type from the drop-down list. The specification of Averted Loss Types is optionally provided by your firm. If no averted loss types are defined, then this drop-down list provides no entries for selection.
GL Account	Enter the general ledger account to which this loss or recovery item is associated. This data item associates this GL account to the current item being entered only and not to the overall alert. This field allows you to associate a different GL account to an individual item than can be appropriate for the entire alert.
Description	Enter comments regarding the current item being entered in the row.

4. Click **Save**. The following message is displayed: *Would you like to save these actions?*

5. Click **OK**. The Loss and Recovery Summary information is updated.

Editing Loss and Recovery Details

This section allows you to modify existing information pertaining to potential loss, averted loss, and recovery details.

To modify loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Click **Potential Loss, Averted Loss,** or **Recovery**. Click **Edit**. The Loss and Recovery Data Entry dialog box is displayed.

3. Modify necessary information in the respective fields. For more information on the fields, see *Adding Loss and Recovery Details* section.

4. Click **Save**. The following message is displayed: *Would you like to save these actions?*

5. Click **OK**. The Loss and Recovery Summary information is updated.

Removing Loss and Recovery Details

This section allows you to delete information pertaining to potential loss, averted loss, and recovery details.

To remove loss and recovery details, follow these steps:

1. Navigate to the Financials tab Details page.

2. Click **Potential Loss, Averted Loss,** or **Recovery**. The list of records is displayed.

3. Select the required record. Click **Remove**. The following message is displayed: Y*ou have selected to remove the Primary GL Account and Cost Center information associated with this investigation. Select OK to continue and save the changes.*

4. Click **OK**. The Loss and Recovery Summary information is updated.

Replay Tab

The Trading Compliance Solution enables you to replay the market and trade events for a match associated with the alert you are reviewing or for an activity during a specified time frame.

When you access the Replay page through the Monitoring workflow, the page presents the trade events associated with the match, interlaced with the market events in the market at the time the application generated the match. For multi-match alerts, the Replay page displays only information for the match you selected on the Details page. To display information for another match involved in the alert, you must select a different match on the Alert Details page.

This section covers the following topics:

- Accessing Replay Tab
- Searching Replay Details
- Replaying Market and Trade Activity for a Match

Accessing Replay Tab

This section explains how to access the Replay tab.

1. Navigate to the Alert Search and List page.

2. Click **Search** or **Advanced Search**. The Simple Search or Advanced Search page is displayed.

3. Select **Trading Compliance (TC)** from the Scenario Class drop-down list. The list of Trading Compliance Scenario alerts is displayed.

4. Click the required **Alert ID**. The Alert Details page is displayed.

5. Click the **Replay** Tab. The Replay page is displayed.

   This page displays trade events associated with the match, interlaced with the market events in the market at the time the application generated the match.

   The Replay section enables you to maximize the usability of the Replay page. It enable you to sort replay columns according to the date and time stamp associated with the entity expressed in Coordinated Universal Time (UTC) while replaying the match event.

Figure 30. Replay Page

Searching Replay Details

This section allows you to filter details pertaining to Trading Compliance scenarios.

To search replay details, follow these steps:

1. Navigate to the Replay tab Details page.

2. Go to the Search section.

3. Enter the following information in the respective fields.

Table 13. Replay Tab Search page

Fields	Description
Market Center	Enter the name of the market center for the involved security. By default, this field is populated with the matched market center. **Note:** You need to enter market center name only if you select the Market Center Quote check box under the View search bar.
Security	Select the security from drop-down list of distinct security for the involved replay match for trading compliance.

Table 13. Replay Tab Search page

Fields	Description
Security Group	Select the security group from the drop-down list of which the security is matched or bound to the alert. **Note:** The Replay Search bar displays the Security Group list box for only Trading Compliance solution Sets and if Security Group option is Enabled from the Preference page.
Expand by ISIN	The search filter is used to query MiFID-based records. It searches for the securities that come under the same ISIN in the Security list box of the security matched or bound to the alert. The following message is displayed: *Add securities to the Security selection box that share the same ISIN.*
Security	Default populated by distinct list of ISIN. When the Security Group list box is set on the Enabled option, the ISIN list contains the following: ● ISIN of the securities matched to the Alert ● All securities that are members of the security groups of which the matched security is a member. When the Security Group drop-down list is set on Disabled option, the ISIN list contains ISIN of the securities matched or bound to the Alert with the following functionality: ■ If you select the Expand by ISIN check box, the security selection box repopulates with a distinct list by ISIN of all the securities that have the same ISIN as the security matched or bound to the alert. The page, by default, selects the security that have the same ISIN as the security matched or bound to the alert. ■ If you clear the Expand by ISIN check box and click Search, the page restores the initial population of the Security list box.
Start Date	Enter the start date or default populated by the date of the earliest event matched or otherwise associated with the alert replayed in the section expressed in the time zone local to the event.
End Date	Enter the end date or default populated by the date of the latest event matched or otherwise associated with the alert replayed in the section expressed in the time zone local to the event.
Time From	Enter the time from or default populated by the time of the earliest event matched or otherwise associated with the alert replayed in the section expressed in the time zone local to the event.
Time To	Enter the time to or default populated by the time of the latest event matched or otherwise associated with the alert replayed in the section expressed in the time zone local to the event. If the time zones of the earliest event and the latest event are different, then by default this field will display the time of the latest event by converting it into the time zone of the earliest event. **Note:** The Time From value must be earlier than the Time To value, if using the same dates. When entering times, use the 24-hour standard of HH:MM:SS:MMM.You can change Date and Time filters as required. When entering times, enter the Time filters with the time values expressed in the Time Zone drop-down list.

Table 13. Replay Tab Search page

Fields	Description
Time Zone	Shows a distinct list of time zones (configurable). Application displays time zone values as the time zone displays text followed by a space and the UTC offset in parenthesis (for example, EST(-05:00)) sorted by UTC offset. The Time Zone drop-down list displays value as both negative and positive by UTC offset. The default values for the time zone are the events matched to the alert. However, if the matched events occur in more than one time zone, then the time zone of the earliest event is considered. Select the Time Zone filter either in Local or Selected mode. By default, the Replay page displays a Local option. However, you can change to a Selected option depending on your search criteria. Select the time zone as **Local**, the replay page displays the date and time value for each record in the time zone local to the record's event. Select the time zone as **Selected**, the replay page displays the date and time value for each record in the time zone selected in the Time Zone filter. For example, consider the following information shown on the Replay page: ● **Case #1 (Default Case):** Search and display replay data in Local time zone.The time in the Search bar and resultant section is expressed in the EST time zone. ● **Case #2**: Search replay data in GMT time zone. However, display replay data in Local time zone. The time in the Search bar is expressed in the GMT time zone, whereas, time in the resultant section is expressed in the EST time zone, which is local to an alert. ● **Case #3**: Search and display replay data in the GMT time zone. The time in Search bar and resultant section is expressed in the GMT time zone, which is selected by the user.

Table 13. Replay Tab Search page

Fields	Description
View	Select the check box to view columns of data in the match replay. You can select one or more of the following option: ● **Inside Quotes**: Matched events of inside quote or framing records in the match, in case, order and execution are involved in the match. ● **Market Center Quotes**: Matched events of Market Center quote records that were involved in the match. ● **Automated Quotes**: Automated quote records that were either involved in the match or provided context for the events involved in the match. ● **Trades**: Trade information during the time frame for the involved security. ● **Orders**: Order records that were either involved in the match or the executions involved in the match. ● **Order Events**: Event records for the chosen securities, which are within date and time range. These event types are Route, Modification, Cancellation, Cancellation and Replacement, and Desk Transfer if Security Group is enabled. **Note :** Event records for the chosen securities, which are within date and time range. These event types are New or Routed if Security Group is disabled. ● **Executions**: Execution records that were involved in the match. ● **Reported Sales**: Matched Reported Sales and Framing Records in case trade is matched.
Expand	Select a check box to expand the display of the corresponding column you selected in the View option. You can select one of the following: Inside Quotes, Market Center Quotes, Automated Quotes, Trades, Orders, Order Events, Executions, or Reported Sales. By default, Replay displays only those events associated with the match. You can view these events in the context of other events during the same time frame by selecting an Expand option. Selecting an Expand option for an event type displays all records of the selected event type within the time frame between the first and last events associated with the match, not the events associated with the match. The expanded context information is displayed in gray text. If you select an Expand option without having selected its corresponding View option, the View option is selected by default, and the market data for that option is displayed. By default, Alert Management system displays a set of related events in the replay section. These events are associated with the default event or event that you select from the View and the Expand options in the search bar. **Note:** If the default event is selected as Automated Quotes, then events Inside Quotes and Market Center Quotes must be deselected.

4. Click **Go**. The relevant search list is displayed.

Note: If the number of retrieved records, based on the search bar criteria exceeds the allowable number for an event type, then the application displays only the default number of records that was set at the time of installation of the Alert Management UI.

The following table displays the related events and default events in the replay section.

Table 14. Related Events and Default Events

Related Events vs. Default Events	Inside Quotes	Market Center Quotes	Automated Quotes	Trades	Orders	Order Events	Executions	Reported Sales
Inside Quotes	x							
Market Center Quotes		x						
Automated Quotes			x					
Trades				x				x
Orders	x				x			
Order Events	x				x	x		
Executions	x						x	
Reported Sales								x

The following table displays the related events and user-selected events in the replay section.

Table 15. Related Events and User-defined Events

Related Events vs. User-Selected Events	Inside Quotes	Market Center Quotes	Automated Quotes	Trades	Orders	Order Events	Executions	Reported Sales
Inside Quotes	x							
Market Center Quotes		x[*]						
Automated Quotes			x					
Trades				x				x
Orders	x							
Order Events	x				x	x		
Executions	x				x		x	
Reported Sales								x

* To view records for the Market Center Quotes, enter a valid Market Center value.

Replaying Market and Trade Activity for a Match

You can use the View and Expand options on the Replay search bar to replay the market and trade activity for a match included in an alert you are reviewing.

To see order information and expanded execution information, follow these steps:

1. Navigate to the Alerts Details page. Click the **Replay** tab.

If the alert is a multi-match alert, select a match in the **Matched Information** section, then click the **Replay** tab.

2. Select check boxes for the additional events you want to view in the **View** row. By default, the system selects the events matched to the current alert. All details are selected in the search bar and the resultant section is displayed accordingly.

3. Select check boxes for the events for which you want more details in the **Expand** row.

4. Click **Go**. The application refreshes and displays the data based on these selections.

Searching for Alerts

This section describes the different ways of searching for an alert and the steps involved in filtering alerts based on the search mode. You can search for alerts using the Alert Search and List page. The Alert Search and List page allows you to filter alerts that you want to view and analyze.

You can filter alerts in the following ways:

- Searching for Alerts using Views
- Searching for Alerts using Alert IDs
- Searching for Alerts using Search Criteria

Note: At a time, you can search for an alert using either Views, Alerts IDs, or Search Criteria.

Searching for Alerts using Views

Views represent pre-populated search queries. The View for searching allows a single-click option for returning a filtered alert list based on the view's preset search criteria. Using the Views field, you can select a particular View and the fields in the **Alert Search** section change based on the search criteria.

To search for alerts using the Views search, follow these steps:

1. Navigate to the Alert Search and List page.

2. Select a view type from the Views drop-down list. The relevant alerts are displayed in the Alert List section.

For information on the options available, see the table below:

Table 16. Views Search Options

Option	Description
My New Alerts	Displays alerts for which the owner is the logged in user or the pool to which user belongs. Alert Status is *New*.
My Open Alerts	Displays alerts for which the owner is the logged in user or the pool to which user belongs. Alert status can be any status except *Closed*.
My Overdue Alerts	Displays alerts for which the owner is the logged in user or the pool to which user belongs. For an alert to be overdue, the due date must be equal to or less than the current date.

Searching for Alerts using Alert IDs

Using the alert ID, you can search for one or more alerts by entering the alert IDs.

Note: If you attempt to search by a combination of the alert ID and other search criteria, the search results display based on the alert ID and ignores the other criteria.

To search for alerts using the alert IDs, follow these steps:

1. Navigate to the Alert Search and List page.

2. Enter one or more unique alert IDs in the alert ID field.

    Note: To search for multiple IDs, separate the Alert IDs with commas.

3. Click **Search** or **Enter** on the keyboard. The Alert List page displays information about the alerts with the alert IDs that exactly matches the values that you enter.

Searching for Alerts using Search Criteria

Using the search criteria, you can view specific data related to those alerts which you are authorized to view based on the selected data.

There are two types of search criteria: Less Search Criteria and More Search Criteria.

Less Search Criteria is a simple search criteria based on the limited set of search fields. More Search Criteria is an advanced search criteria based on the Less Search Criteria.

Note: The Alert List is dynamically populated based on the different sets of input criteria.

To search for alerts using search criteria, follow these steps:

1. Navigate to the Alert Search and List page. By default, the *More Search Criteria* fields are displayed.

2. Enter the following search criteria in the respective fields.

Table 17. More Search Criteria

Fields	Description
Created From	Select the From date. All alerts created from this date appear.
To	Select the To date. All alerts created until this date appear.
Status	Select the alert status from the drop-down list. This filters the alert list based on the current status of the alert.
Organization	Select the organization from where the alert originated. This filters alert list by the ID of the organization associated with the owner of an alert.
Owner	Select the alert owner from the drop-down list. This filters the alert list by a user or user group to whom an alert is assigned.
Closing Action	Select the closing action from the drop-down list. This filters the alert list by one or more selected. closing actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.
Focus Type	Select the focus type from the drop-down list. This filters the alert list by the type of business object that exhibits the behavior of interest.
Scenario	Select the alert scenario from the drop-down list. This filters the alert list by the scenarios name of the behavior or activity that generated the alert.

Table 17. More Search Criteria

Fields	Description
Scenario Class	Select the alert scenario class from the drop-down list. This filters the alert list by the scenario class associated with an alert. The Scenario Class is listed by its abbreviation.
Score	Select the alert score from the drop-down list. This filters the alert list by the score the alert received against the criteria selected by your firm.
Jurisdiction	Select the jurisdiction from the drop-down list. This filters the alert list by the business jurisdiction associated with an alert. The drop-down list contains only the jurisdictions with which you are authorized to view.
Business From	Select the From processing date. All alerts created from this date appear.
Business To	Select the To processing date. All alerts created until this date appear.
Business Domain	Select the domain from the drop-down list. This filters the alert list by the business domain associated with an alert. The drop-down list contains only the business domains which you are authorized to view.
Entity Type	Select the entity type from the drop-down list. This filters the alert by the type of business entity. It is distinct from the Focus search filter. The Entity Type drop-down list refreshes according to the option that you selected through the Limit to Focus check box.
Entity ID	Enter the entity ID. This filters the alert entity ID that is associated with alerts you want to view.
Entity Name	Enter the entity name. This filters the alert entity ID that is associated with alerts you want to view.
Regulatory Report Type	Select the regulatory reporting type from the drop-down list. This filters the alert list by the Regulatory Reporting types that are available to you. Regulatory Reporting is an optional application.
Regulatory Report Status	Select the regulatory reporting status from the drop-down list. This filters the alert list by the current status of an alert that is recommended for Regulatory Reporting, Regulatory Reporting is an optional application.
Action	Select the action from the drop-down list. This filters the alert list by one or more actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.
Action From	Select the Action From date. All actions created from this date appear.
Action To	Select the Action To date. All actions created until this date appear.
Last Action	Select the last action from the drop-down list. This filters the alert list by one or more selected last actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.
Linked Cases	Select the linked cases parameter from the drop-down list. This filters the alert list by the number of cases that are linked to the alert. Oracle Financial Services Alert Management retrieves alerts, which are either greater than or equal to, equal to, or less than or equal to the count you enter in the text box. This option is available only if you have implemented *Oracle Financial Services Case Management*.
Limit to Focus	Select the Limit to Focus check box. This filters the alert focused on specified entities with a business relationship. **Note:** Searching for alerts using Limit to Focus check box is applicable only to the entity filter options. Hovering over the check box displays the following message: "Selecting this check box will limit your results to where the specified entity is the focus. Deselecting this check box will return results where the specified entity is the focus as well as include results focused on entities related to the specified entity".
Age	Select the age parameter from the drop-down list and enter the age in the next field. This filters the alert list by the number of calendar or business days, and any number greater, since the creation of an Active alert.

Table 17. More Search Criteria

Fields	Description
Due Date	Select the due date from the drop-down list. This filters the alert list by past and up to the date you enter by which an action should be taken on the alert.
Security Name	Enter the security name. This filters the alert list by the name of security involved in the alert.
Security ID	Enter the security ID. This filters the alert list by the identification number of the security involved in the alert.
Investment Advisor Firm Name	Enter the investment advisor firm name. This filters the alert list by the name of the firm associated with the investment advisor.
Investment Advisor Firm ID	Enter the investment advisor firm ID. This filters the alert list by the identification of the firm associated with the investment advisor.
Service Team ID	Enter the service team ID. This filters the alert list by the identification of the primary service team of which this employee is a member.
Representative Name	Enter the representative name. This filters the alert list by name of the employee or contractor who is the registered representative.
Representative ID	Enter the registered representative ID. This filters the alert list by identification number of the employee or contractor who is the registered representative.
Supervisory Organization Name	Enter the supervisory organization name. This filters the alert list by the name of the organization where the registered representative is employed.
Supervisory Organization ID	Enter the supervisory organization ID. This filters the alert list by unique identification number of the organization where the registered representative is employed.
Primary Cost Center	Select the primary cost center value from the drop-down list. This filters the alert list by the primary cost center to which the total net loss amount for an alert is associated.
Total/Net Loss Amount	Select the total/net loss amount value. This filters the alert list by the total net loss amount associated with the alert.
Trader ID	Enter the trader ID. This filters the alert list by the identification number of the trader involved in the alert.
Trader Name	Enter the trader name. This filters the alert list by the name of the trader involved in the alert.

3. Click Search. The Alert List section displays the list of alerts that meet the search criteria.

You can also search for alerts using the Less Search Criteria fields. To view these fields, click **Less Search Criteria**. Some of the fields are hidden.

Note: The Alert List section enables you to view details about the alerts and take various actions, depending on the user privileges.

Acting on Alerts

After monitoring the system generated alerts, you can analyze and determine to take appropriate action on alerts. This section explains various types of actions and how to take ideal action on alerts. For example, reassign, close, and so on.

This section covers the following topics:

- About Alert Actions
- Taking Follow-up Actions on Alerts
- Reassigning Alerts
- Taking Additional Actions on Alerts

About Alert Actions

This section explains different types of action in the Alert Management system and who can perform these actions in what status.

This section covers the following topics:

- Types of Actions
- Action Categories
- Taking Action on Alerts

Types of Actions

The Alert Management system provides the following types of actions to document your analysis:

- Taking Follow-up Actions on Alerts
- Reassigning Alerts
- Emailing Alerts
- Reviewing Alerts
- Adding attachments and comments to Alerts

Action Categories

Action categories represent logical groupings of individual actions, which have similarities, either in the line of investigation or in the resulting status of the action. Each of these action categories are represented by buttons, which on click display a window corresponding to the category. Some actions represent definitive progress in analysis and can therefore update the status of the alert.

The Alert Management system classifies the actions available on alerts into eight distinct categories:

- **Reassign**: This option allows you to reassign the selected alerts to another user. It is available for only certain roles. For more information, see *Reassigning Alerts* section.

- **Actions**: This option includes a list of actions that can require follow-up analysis or can require an alert to be reopened. In addition, some actions can not alter the alert status, but serve to indicate steps taken in the course of investigation. Some actions within the Action category can require you to enter a due-date, which

takes the alert to the Follow-up status. The section *Taking Follow-up Actions on Alerts* on an Alert explains Follow-up actions on alerts in detail. For more information on reopening an alert, see *Reopening Alerts* section.

Note: The Reopen action displays when you are taking an action on alerts in a Closed status.

- **Disposition**: This option includes a list of actions that complete your analysis of alert, and in most instances, results in closure of the alert. This list varies based on the scenario class that generated the alert. The section Closing Alerts explains closing an alert in detail. For more information, see *Closing Alerts* section.

- **Email**: This option allow you to email the alert details in HTML format. For more information, see *Emailing Alerts* section.

- **Regulatory Reporting**: This option includes a list of actions that can require follow-up analysis or can complete your analysis of the alert. These are the actions which generate reports. Additionally, some actions in this section can not alter the alert status, but can serve to indicate actions taken in the course of investigation.

- **Review**: This option includes a list of actions that can require follow-up analysis or can complete your analysis of the alert. If you enter a due date when selecting an action from this area, Alert Management system changes the alert status to Follow-up. If you do not enter a due date, Alert Management system changes the alert status to Closed. For more information, see *Reviewing Alerts* section.

- **Add Evidence**: This option allows you to add attachments and make comments to the selected alerts from the alert list section. For more information, see *Accessing Alert Details page* section.

The Alert Management system enables you to take multiple actions simultaneously, whether you apply them to a single alert or to a batch of alerts through the action category. For example, you can simultaneously close and suppress the alert for one-month and promote it to a Case from the Disposition category. However, there are some actions, which you cannot take simultaneously. For example, you cannot reassign and close an alert simultaneously. The Alert Management's Four-Eyes Approval feature enables you to propose the closing of an alert, but requires authorized users to look at that alert before it can actually be closed.

The Alert Management system displays warning messages to help you in the appropriate way to use actions. See Appendix *Message pages* explains error messages in detail. In addition, some actions can are configured to automatically assign a due date.

Note: This topic includes instructions in optional steps that indicate additional functionality and alternative steps that indicate other methods to perform the operation successfully.

Taking Action on Alerts

During analysis you can take various actions on an alert, such as reassigning, reviewing, adding comments and attachments, and setting due-dates for the following up on an investigative step. You can also take disposition actions that closes the alert for a specified reason.
You can take actions in the following ways:

- You can take one or more actions specific to that alert by selecting any of the action buttons. These action buttons represent action categories (that is, Reassign, Evidence, Actions, Disposition, email, Regulatory Reporting, and Review). The action window displays within a context of the current alert and any actions taken apply to the current alert.

- You can take actions simultaneously on multiple alerts by selecting any of the action buttons which represent an action category (that is, Evidence, Reassign, Actions, email, Regulatory Reporting, and Review). The

action window displays with a context of all of selected alerts and any actions taken apply to each of the selected alerts.

Note: If you select one or more alerts from the list, and click the **Action** button, the system locks the selected alerts and make them unavailable by action for other users. If another user attempts to access the same alert (either by selecting the alert and taking an action or by navigating to the Alert Details), the user receives a message informing that the alert is locked by another user and the system grants only view rights (user can take no action on the alert).

- You can select an alert, view Alert Details, Alert Management system tabs or Business tabs and select any of the action buttons (Evidence, Reassign, Actions, email, Regulatory Reporting, and Review). The action window is displayed and any actions taken apply to the current alert.

- You can select an alert, view the Alert Details, and navigate to the Disposition tab. Any Disposition actions taken apply to the current alert.

- You can select an alert, view Alert Details, and navigate to the Evidence tab. Any comment and/or attachment actions taken apply to the current alert.

Taking Follow-up Actions on Alerts

You can do follow-up analysis by setting due-dates for further investigation and choose actions on alerts such as reopen, reassign, awaiting response, further analysis required, and so on.

If you are an Analyst II, III, or Supervisor, you can take actions that indicate that additional analysis is required.

To take follow up actions on alerts, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to update

   Or, navigate to the Alert Details tab of the alert that you want to update.

2. Click **Reassign**, **Actions**, **Disposition, Regulatory Reporting**, or **Review** to view the Take Action dialog box. Click **Email** to view the Monitoring Actions dialog box.

Note: If you take one or more actions with post follow-up without entering a Due Date, the alert will close. However, if you enter a Due Date, these actions place the alert into a Follow-up status.

3. Enter the following information in the respective fields.

Table 18. Follow up Actions

Fields	Description
Selected Alerts	Displays only those alerts on which you can perform the action, that is, alerts which are in unlocked status during the selection (not currently opened by another user).
Choose Action	Select the actions from Choose Action drop-down list. For example, Awaiting Response, Further Analysis Required, and so on.This allows you to take one or multiple actions pertaining to the action category on the selected alerts. Possible actions can vary based on the scenario class, status of the alert, and your role. **Note:** If you are taking action on multiple alerts, system displays only actions and comments that are common to all selected alerts.
Note: The following fields display based on the selection of actions, the fields are enabled or disabled for your inputs.	

Table 18. Follow up Actions

Fields	Description
Reassign	Select the owner from Reassign drop-down list. This includes a list of owners (that is, users and groups of users) to whom you can assign alerts. This action is only available for certain roles. The list of owners only displays users who are allowed to own alerts and who have access rights to the current alert or alerts being acted on. For more information, see *Reassigning Alerts*. **Note:** You can automate the assignment of ownership of the alert by selecting the Auto Assignment check box.
Auto Assignment check box	Select the Auto Assignment check box. While performing actions on alerts and creating manual alerts, an Analyst I, II, or Supervisor user can automate the assignment of ownership of the alert. Selecting this check box disables the *Reassign Ownership To* field and the system automatically assigns the owner as per rules defined in Alert Assigner Editor under Alert Management Configuration settings set by an Administrator. For more information, contact your System Administrator. **Note:** Deselect the Auto Assignment check box to enable the *Reassign Ownership To* field. Auto Assignment is a feature which enables the user to allow the system to select the owner based on pre-defined assignment rules. The pre-defined rules are set under Alert Assigner Editor (parameters such as Alert Type and so on). If the system is unable to find an owner based on the rules defined then the alert are auto-assigned to the default owner set in Default Alert Owner attribute under the Installation Parameters table.
Set Due Date	Select the due date from calendar icon. This provides an ability to select a date by which the selected action should complete. **Note:** ● If your system is configured with default due-dates for some actions, then the default due shall be applied to the alert when those actions are taken, provided you do not enter any date in the Due Date calendar control. ● If multiple actions with default due-dates are taken on the alert then the nearest default due-date is applied to the alert. ● However, if you explicitly enter a due-date in the control, it gives the highest priority irrespective of the default due configured for the actions.
Suppression End Date	This option is enabled when you want to take Disposition action on alerts. Select suppression end date from the calendar. This provides the ability to select an end date for the suppression rule. When this date is reached, the suppression rule expires. **Note:** It is enabled only when you select an action that is designated to trigger the suppression of future alerts based on a user-entered suppression time frame.
Suppression Condition	This option is enabled when you want to take disposition action on alerts. Select the suppression condition from the drop-down list. This provides the ability to select binding information used in creating a suppression rule for an alert. Suppression conditions are enabled only when you select an action that is designated to trigger the suppression of future alerts. Enter the following information: ● **Binding Name**: Select the binding name from the Binding Name drop-down list. ● **Binding Operator**: Select the binding operator from the Binding Operator from drop-down list which contains comparison operators. They are: equal to (=), greater than or equal to (>=), less than or equal to (<=), greater than (>), less than (<), and not equal to (!=). **Binding Value**: This is blank by default, but populates with the selected alert's highlight value associated with a selected binding name. If your role permits, the value is editable. Otherwise, this value appears as an un editable text. For more information on User privileges, see *Appendix A, User Privileges.*Bindings are variables captured in a scenario pattern that are used for defining highlights. The bindings displayed in the binding name drop-down list reflects the highlights associated with the current alert.

Table 18. Follow up Actions

Fields	Description
Standard Comments	Select the standard comments from the drop-down list. This provides a quick means of entering comments that are relevant to the analysis and closing of the selected alerts. The scenario class of the alerts on which you are taking action determines which standard comments display.
Comments	Enter remarks relevant to the analysis and closure of the selected alerts. Use this text area if none of the standard comments applies to your action or if you want to include additional information. The number of characters you can enter display below the box.

Note: Once you select an action, the **Save**, **Save and Attach**, and **Reset** buttons are displayed.

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

   Or, click **Save and Attach**.

5. Click **OK**. The Alert Management system records the action, updates the alert information, and returns you to the refreshed Alert Search and List page or Alert Details tab depending on from where the action was taken.

Reassigning Alerts

If an alert's initial analysis reveals an issue that should be reviewed by another user, you can reassign alerts to the most appropriate individual or group. If you are an Analyst I, II, III, or Supervisor, you can reassign alerts to different users or groups of users. When you save a reassignment action, The Alert Management system immediately reflects the new ownership of the alert.

To reassign alerts, follow these steps:

1. Navigate to Alert Search and List page. Select one or more check boxes against each alert that you want to reassign.

   Or, navigate to the Alert Details tab of the alert that you want to reassign.

2. Click **Reassign**. The Monitoring Actions dialog box is displayed.

3. Enter the required information in the respective fields. For more information on fields, see *Table 18*.

   Note: Once you select an action, **Save, Save and Attach**, and **Reset** buttons are displayed.

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

   Or, click **Save and Attach**.

5. Click **OK**. The Alert Management system reassigns the alert, records the action, updates the alert information, and returns you to the refreshed Alert List page or Alert Details tab depending on from where the action was taken.

Taking Additional Actions on Alerts

This section explains various other action that can be taken on alerts. When you take these actions on alerts, they do not impact the status of alerts.

This section covers the following topics

- Emailing Alerts
- Printing Alerts

- [Adding Comments to Alerts](#)
- [Managing Attachments](#)
- [Generating Regulatory Reports](#)
- [Reviewing Alerts](#)
- [Designating Trusted Pairs](#)

Note:

Emailing Alerts

The Alert Management system enables you to email alert attachments in the form of an eXtensible Markup Language (XML). Analyst II, III, or Supervisor can email alerts.

The Alert Management system sends a single email with each alert as a separate attachment. Each attached file follows the naming convention as `<Alert ID>.HTML` or `<Alert ID>.XML` according to the action performed.

By default, a footer is added to the email, which can be configured at the time of installation. For more information, see *Configuration Guide*.

To email alerts, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to email.

   Or, navigate to the Alert Details tab of the alert that you want to email.

2. Click **Email**. The Email window is displayed.

3. Enter the following information in the respective fields.

Table 19. Email Alerts

Fields	Description
Associated Alert ID(s)	Displays only those alerts on which you can perform the action, that is, those alerts which are in unlocked status during the selection (not currently opened by another user).
From	Displays the name of user who is sending an email.
To	Enter the names of users to whom you want to send the email.
Subject	Displays the alerts details, you can also modify the subject details.
Body	Enter the details of select alerts.
Select Action	Select the action on the email from the drop-down list. You can select from the following actions: ● Email Alert Details ● Email with Response Request ● Email Alert Details with Response Request ● Send Email
Reassign	Select the owner from Reassign drop-down list. This includes a list of owners (that is, users and groups of users) to whom you can assign alerts. This action is only available for certain roles. The list of owners only displays users who are allowed to own alerts and who have access rights to the current alert or alerts being acted on. For more information, see *Reassigning Alerts*. **Note:** You can automate the assignment of ownership of the alert by selecting the Auto Assignment check box.

Table 19. Email Alerts

Fields	Description
Auto Assignment check box	Select the Auto Assignment check box. While performing actions on alerts and creating manual alerts, an Analyst I, II, or Supervisor user can automate the assignment of ownership of the alert. Selecting this check box disables the *Reassign Ownership To* field and the system automatically assigns the owner as per rules defined in Alert Assigner Editor under Alert Management Configuration settings set by an Administrator. For more information, contact your System Administrator. **Note:** Deselect the Auto Assignment check box to enable the *Reassign Ownership To* field. Auto Assignment is a feature which enables the user to allow the system to select the owner based on pre-defined assignment rules. The pre-defined rules are set under Alert Assigner Editor (parameters such as Alert Type and so on). If the system is unable to find an owner based on the rules defined then the alert are auto-assigned to the default owner set in Default Alert Owner attribute under the Installation Parameters table.
Set Due Date	Select the due date from calendar icon. This provides an ability to select a date by which the selected action should complete. **Note:** ● If your system is configured with default due-dates for some actions, then the default due shall be applied to the alert when those actions are taken, provided you do not enter any date in the Due Date calendar control. ● If multiple actions with default due-dates are taken on the alert then the nearest default due-date is applied to the alert. ● However, if you explicitly enter a due-date in the control, it gives the highest priority irrespective of the default due configured for the actions.
Standard Comments	Select the standard comments from the drop-down list. This provides a quick means of entering comments that are relevant to the analysis and closing of the selected alerts. The scenario class of the alerts on which you are taking action determines which standard comments display.
Comments	Enter comments for sending an email. This enables you to enter free-form text characters relevant to the analysis of the selected alerts. The number of characters you can enter display below the box. **Note:** If the comments exceed 4000 characters, the system prints only the first 4000 characters. Comments added to an email attachment are not secure.

4. Click **Save**. The Send email window closes.

The Alert Management system sends the email, records the action, and returns you to the Alert Search and List page or Alert Details tab depending on from where the action was taken.

Generating Regulatory Reports

When it is determined that an alert requires filing of a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR), institutions must file the report with their applicable regulatory authority.

When you determine that an alert requires reporting, you can take an action to generate the regulatory report.

To generate reports, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to report.

   Or, navigate to the Alert Details tab of the alert that you want to generate report.

2. Click **Regulatory Reporting**. The Monitoring Actions dialog box displays.

3. Select relevant Suspicious Transaction Reports (STRs) or Suspicious Activity Report (SAR) from the Choose Action drop-down list.

4. Enter other required information in the respective fields. For more information on the fields, see *Table 18.*

5. Click **Save**. The confirmation dialog box displays the following message: *SAR or STR Successful.*

   Or, click **Save and Attach**.

6. Click **OK**. The Alert Management system records the action, updates the alert information, and returns you to the refreshed Alert Search and List page or Alert Details tab depending on from where the action was taken.

Reviewing Alerts

When you determine that alerts require additional reviews internally, such as review with manager, you can opt to take this action.

To review alerts, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to review.

   Or, navigate to the Alert Details tab of the alert that you want to review.

2. Click **Review**. The Monitoring Actions dialog box displays.

3. Select one or more review type from the Choose Action drop-down list. For example, Internally, with manager, and so on.

4. Enter other required information in the respective fields. For more information on the fields, see *Table 18.*

5. Click **Save**. The confirmation dialog box displays the following message: *Would you like to save this actions?*

   Or, click **Save and Attach.**

6. Click **OK**. The Alert Management system records the action, updates the alert information, and returns you to the refreshed Alert Search and List page or Alert Details tab depending on from where the action was taken.

Designating Trusted Pairs

In the course of reviewing and analyzing alerts, you can determine that the activity between two parties on a transaction constitutes acceptable business practice and poses little risk to your institution. If your role permits, you can mark the relationship between these parties as trusted, using a combination of multiple attributes and factors to identify the exact format of the relationship that is to be trusted and therefore, potentially, excluded in behavior detection. Having this ability to exclude selected parties from consideration in behavior detection over a period of time can greatly reduce your workload. This is applicable to ML and FR class alerts only and only to Wires, MI's, Back Office, and Insurance Transactions.

You can designate a trusted relationship from the Matched Information area. For more information on Designating Trusted Pairs, see *Chapter 6, Managing Trusted Pairs.*

Closing Alerts

Only an Alert Management user with the role of Supervisor, Analyst II, or Analyst III can close an alert.

The Alert Management system recommends that your firm determines a standard practice for closing an alert.

This section covers the following topics:

- Auto-closing System Alerts

- Auto-suppressing System Alerts

- Reopening Alerts Closed by Suppression

- Creating a Tailored Suppression Rule

- Manually Closing Alerts with Four-Eyes Approval

- If you are an Analyst II, III, or Supervisor, you can take an action to close an alert with the status of New, Open, Follow-up, or Reassigned.

- Promoting Alerts to Cases with Four-Eyes Approval

- Promoting Alerts to Cases without Four-Eyes Approval

Auto-closing System Alerts

Your firm establishes the criteria that determines when an alert should be auto-closed. This criteria defines one or more attributes of the alert to be evaluated in determining whether Alert Management system should automatically close the alert. For example, alerts can be closed based on their age, status, score, focus type, generating scenario, or any combination of these attributes.

This section covers the following topics:

- Defining Auto-Close Alert Algorithm

- Reopening Automatically Closed Alerts

Defining Auto-Close Alert Algorithm

The auto-close function cannot be set by typical users. Auto-close is configured by the System Administrator, and is handled transparently by the application.

To define auto-close alert algorithm, see *Administration Guide*, *Auto Close* section.

Reopening Automatically Closed Alerts

Once your firm's autoclose parameters are established, Alert Management system regularly evaluates all candidate alerts and closes each alert that satisfies the auto-close criteria. However, the closed alerts are maintained for viewing purposes and are still available for reopening.

The procedure for reopening a closed alert is the same whether the alert was closed by a user or by the application's auto-close process. For information on how to reopen an alert that was closed, see *Reopening Alerts* section.

Auto-suppressing System Alerts

The Alert Management system regularly runs an auto-suppression process to determine if there are alerts that meet the suppression criteria. Alerts that the scenario generates for the specific focus and that meet the suppression criteria do not display for a user's action. Instead, Alert Management system automatically closes them.

This section covers the following topics:

- Defining Auto-suppress Alert Algorithm

- Reopening Automatically Suppressed Alerts

- Suppressing a Scenario for a Specific Focus

Defining Auto-suppress Alert Algorithm

The auto-suppress function cannot be set by typical users. Auto-suppress is configured by the System Administrator, and is handled transparently by the application.

To define auto-suppress alert algorithm, see *Administration Guide*, *Auto Close* section.

Reopening Automatically Suppressed Alerts

Even though the Alert Management system closes the alerts that meet the appropriate suppression criteria, it still maintains the alerts for viewing and tracking purposes, and the alerts are still available for reopening at any time through the Actions page. see *Reopening Alerts*.

Suppressing a Scenario for a Specific Focus

The Alert Management system suppresses alerts for the same focal entity and scenario for the designated time. To suppress a scenario for a specific focus, perform a Close and Suppress action (for example, Close and Suppress 3 Months) on an alert focused on the entity and generated by the scenario.

To suppress alerts for a specific period, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to close.

   Or, navigate to the Alert Details tab of the alert that you want to close.

2. Click **Disposition**. The Take Action dialog box is displayed.

3. Select an action from Choose Action drop-down list.

   For more information on the other fields, see *Table 18.*

   Therefore, the only time that the system enables and pre-populates the **Suppression End Date** field with a blank value is when you select one or more suppression triggering actions that are not associated with a duration

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

   Or, click **Save and Attach**.

   The system automatically generates a suppression rule for auto-suppressing future alerts that match the rule criteria you created and changes the status of the alert to *Closed*.

   Note: The **Close and Suppress** options are not available in the Disposition action category or Disposition tab for multi-match alerts with multiple scenarios or for user-initiated alerts.

Reopening Alerts Closed by Suppression

The procedure for reopening a closed alert is the same whether the alert was closed by an Analyst or Supervisor or by an Alert Management auto-suppression action.

For information on how to reopen an alert that was closed by auto-suppression, see *Reopening Alerts* section.

Creating a Tailored Suppression Rule

If your role permits, you can create a tailored suppression rule for an alert by adding a highlight binding name and value pair, and a suppression end date.

To create a tailored suppression rule, follow these steps:

1. Navigate to the Alert Search and List page. Select one or more check boxes against each alert that you want to close.

   Or, navigate to the Alert Details tab of the alert that you want to close.

2. Click **Disposition**. The Take Action dialog box is displayed.

3. Enter the required information in the respective fields.

   For more information on the fields, see *Table 18.*

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

   Or, click **Save and Attach**.

   The system automatically generates a suppression rule for auto-suppressing future alerts that match the rule criteria you just created and changes the status of the alert to Closed.

   Note: If your access privileges permit, you can edit the binding value of an existing suppression rule by changing the value in the **Suppression Condition Value** text box.

   For more information on updating Suppression Rules, see *Chapter 5, Managing Suppression Rules.*

Manually Closing Alerts with Four-Eyes Approval

Four-Eyes Approval is a dual control or approval process that requires an authorized user (for example, a Supervisor) to approve actions of other users prior to those actions taking full effect on the alert (for example, closing the alert). This process also enables users of specified roles to acknowledge approved or rejected changes proposed and to annotate an acknowledgement with comments.

Note: The system must be configured for Four-Eyes Approval.

This section covers the following topics:

- Recommending To Close Alerts
- Approving Alerts Recommended for Closure

Recommending To Close Alerts

If you are an Analyst II or III user, Alert Management system enables you to recommend an alert for closure. For users requiring supervisory approval, actions are labeled with *Recommend to* easily identify those actions that require additional oversight.

To recommend alerts to close, follow these steps:

1. Navigate to the Alert List, select the one or more check boxes against each alert that you want to recommend for closure.

   Or, navigate to the Alert Details tab of the alert that you want to close.

2. Click **Disposition**. The Take Action dialog box is displayed.

3. Select one or more recommend to close actions from Choose Action drop-down list. For example, Duplicate Alertand Invalid Alert.

    For more information on other fields, see *Table 18.*

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

    Or, click **Save & Attach**.

5. Click **OK**. Alert Management records the action, updates the alert information, and returns you to the refreshed Alert List page or Alert Details tab depending on from where the action was taken.

Approving Alerts Recommended for Closure

If you are a Supervisor, the Alert Management system enables you to review alerts on which a recommended closure action is taken. To approve a recommended action, you need to take the action to finalize the status change.

If you do not agree with the recommended action and thus do not take the action yourself, the alert will remain in its current status unless you choose to take a different action.

To approve an alert recommended for closure, follow these steps:

1. Navigate to the Alert Search and List page, select the check box against each alert that is reassigned to you for approval and for which you want to approve the closure with the same closing information.

    Or, navigate to the Alert Details tab of the alert that you want to approve.

2. Click **Disposition**. The Monitoring Action dialog box is displayed.

3. Select one or more recommended to close actions from Choose Action drop-down list. For example, Duplicate Alert, Invalid Alert, and so on.

    For more information on other fields, see *Table 18.*

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

    Or, click **Save and Attach**.

5. Click **OK**. Alert Management records the action, updates the alert information, and returns you to the refreshed Alert List page or Alert Details tab depending on from where the action was taken.

If you are an Analyst II, III, or Supervisor, you can take an action to close an alert with the status of New, Open, Follow-up, or Reassigned.

To close an alert, follow these steps:

1. Navigate to the Alert List, select the check box against each alert that is reassigned to you for approval and for which you want to approve the closure with the same closing information.

    Or, navigate to the Alert Details tab of the alert that you want to approve.

2. Click **Disposition**. The Monitoring Action dialog box is displayed.

3. Enter required information in the respective fields.

    For more information on the fields, see *Table 18.*

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

    Or, click **Save & Attach**. For more information.

5. Click **OK**. Alert Management records the action, updates the alert information, and returns you to the refreshed Alert List page or Alert Details tab depending on from where the action was taken.

Reopening Alerts

If you are an Analyst II, III, or Supervisor with enabled user role permissions, then you can reopen closed alerts that require further investigation.

You can also assign the alerts to any user when you reopen an alert. When you save the Reopen action, the selected alert is set to the status of Reopened and assigned to its last owner before it was closed.

To reopen closed alerts, follow these steps:

1. Navigate to Alert Search and List page. Select one or more check boxes against each alert in Closed status that you want to reopen.

    Or, navigate to the Alert Details tab of the alert in Closed status that you want to reopen.

2. Click **Actions**. The Monitoring Actions dialog box is displayed.

3. Select **Reopen** from the Choose Action drop-down list. Enter other required information in the respective fields. For more information on the fields, see *Table 18*.

    Note: Once you select an action, **Save**, **Save and Attach**, and **Reset** buttons are displayed.

4. Click **Save**. The confirmation dialog box displays the following message: *Would you like to Save these actions?*

    Or, click **Save and Attach**.

5. Click **OK**. The Alert Management system reopens alerts, records the action, updates the alert information, and returns you to the refreshed Alert List page or Alert Details tab depending on from where the action was taken.

CHAPTER 5   *Managing Suppression Rules*

This chapter describes the concept and process of managing alerts suppression rules in the Monitoring workflow of the Alert Management system. It provides instructions to carry out various actions according to the workflow and user roles. This helps you to understand how to use various components to accomplish each task.

The following topics are covered in this chapter:

- About Suppression Rules
- Key Features
- User Roles and Actions
- Suppression Rules Workflow
- Accessing Suppression Rules page
- Creating Suppression Rules
- Updating Suppression Rules
- Ending Suppression Rules
- Managing Four-Eyes Approval Process
- Searching Suppression Rules

About Suppression Rules

An alert suppression rule enables the system to automatically suppress a particular entity's newly-generated alerts based on criteria such as highlight, scenario, and suppression rule begin and end date. The rule captures information such as the creation date, the status, the generating scenario, the focal entity (focus type and focal entity ID) and the links to the comments by the user associated with the suppression rule. Suppression rules are automatically created when you save a *Close and Suppress* action on an alert from within the Monitoring workflow.

The Manage Suppression Rules feature provides a way to search for existing suppression rules based on a set of user-specified parameters. The Manage Suppression Rules also enables you to modify certain components of rules, in particular, to update or to end an existing suppression rule as well as to track all actions performed on that rule.

When Four-Eyes functionality is selected, the following action buttons are enabled on the Suppression List section:

- Approve
- Update and Approve
- Reject

These buttons are enabled only when the rule status is *Recommended.*

Key Features

The Alert Management UI allows you to perform the following actions:

- Manually create suppression rules
- Modify suppression rules end date
- Extend suppression end date by 1, 3, 6, or 12 months
- Recommend to update or end suppression rules
- Approve or reject recommended suppression rules using Four-Eyes approval process

User Roles and Actions

This section describes various user roles and actions they can perform in the Alerts Suppression Rules workflow.

The following table details the user roles and actions in the Alerts Suppression Rules workflow:

User Actions	User Roles									
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
Access to View Search and List of for Suppression Rules	X	X	X	X	X	X				
Add Suppression Rules			X	X						
Update Suppression Rules			X	X						
Reject Suppression Rules			X	X						
End Suppression Rules			X	X						
View Suppression Rule Action History			X	X	X	X				

Suppression Rules Workflow

The following figure shows the Alert Suppression Rules workflow with and without Four- Eyes Approval.
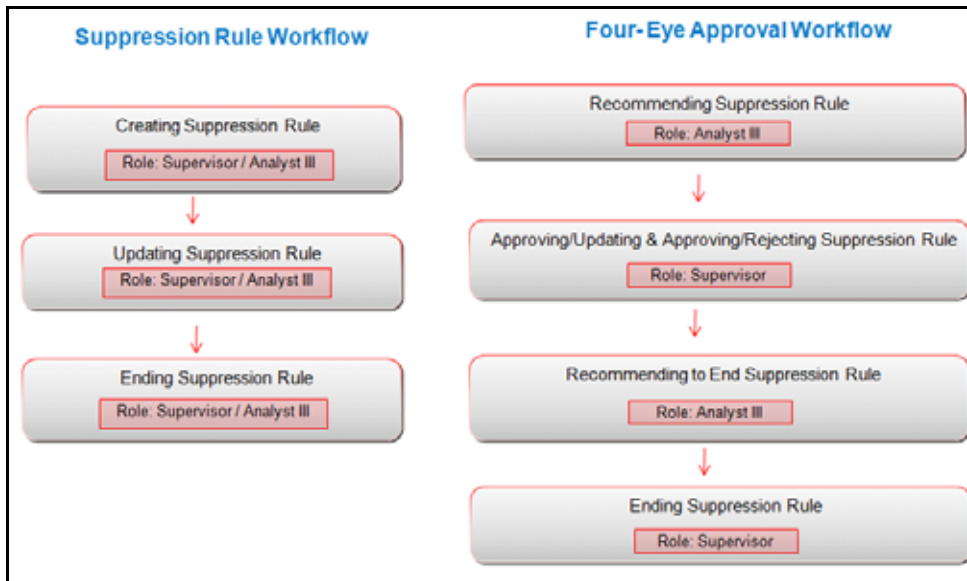
Figure 31. Suppression Rules Workflow

This section covers the following topics:

- Suppression Rules Workflow
- Four- Eyes Approval Process Workflow

Suppression Rules Workflow

The following table details the Suppression Rules workflow.

Table 20. Suppression Rules Workflow

Action	Description	Roles
Creating Suppression Rules	User can create a suppression rule for an alert by adding a highlight binding name and value pair, and a suppression end date.	Analysts I, II, III, and Supervisors
Updating Suppression Rules	User can modify Extend the Suppression By or Suppression End Date by providing appropriate comments.	Analysts II, III, and Supervisors
Ending Suppression Rules	User can end suppression rules by providing appropriate comments.	Analysts II, III, and Supervisors

Four- Eyes Approval Process Workflow

The following table details the Four- Eyes Approval Process workflow.

Table 21. Four- Eye Approval Process Workflow

Action	Description	Roles
Recommending Alert Suppression Rules	Analyst II or III can recommend alert suppression rule. For users requiring supervisory approval, actions are labeled with *Recommend* to easily identify those actions that require additional oversight.	Analysts II and III
Approving Suppression Rules Or Rejecting Suppression Rules	User can approve or reject suppression rules which are Recommended for approval after providing justification in the comment box.	Supervisors
Recommending to End Suppression Rule	User can recommend to end suppression rule.	Analysts II and III
Ending Suppression Rules	User can end suppression rules which are recommended by the analyst by providing appropriate comments.	Supervisors

Accessing Suppression Rules page

This section explains how to access the Alert Suppression page.

To access the Alert Suppression page, follow these steps:

1. Navigate to the OFSAA Applications Home page. For more information, see *Chapter 3, Getting Started.*

2. Click **Administration** in the RHS menu.

3. Hover over the **List Management** menu and click **Alert Suppression**. The Alert Suppression page is displayed.

Creating Suppression Rules

You can create a suppression rule for an alert by adding a highlight binding name and value pair, and a suppression end date.

This section explains how to create an alert suppression rule using the Manage Alert workflow.

For more information on creating alert suppression rule, see *Creating a Tailored Suppression Rule* section in the Managing Alerts chapter.

Updating Suppression Rules

The Update Suppression Rule page allows you to update all selected rules from the Suppression Rule List section.

To update suppression rule, follow these steps:

1. Navigate to the Suppression Rule List page. For more information on how to access the Suppression Rule list page, see *Accessing Suppression Rules page* section.

2. Select one or more check boxes against each rule that you want to update. Click **Update**. The Update Suppression Rule page is displayed.

Figure 32. Update Suppression Rule page

Note:

- If you select one or more *active/inactive* rules with the same expiration date, the Suppression Rule End Date is pre-populated with the common end date. Modify the pre-populated end date to a new date which is prior/subsequent to the existing date or select an Extend Suppression By option.

- If you have selected one or more rules from the Suppression Rules list with different expiration dates. Add the suppression end date that is prior/subsequent to the existing date or select a Extend Suppression By option.

3. Enter the following information in the respective fields.

Table 22. Update Suppression Rule

Column	Description
Extend the Suppression By	Select month or months from the drop-down list. This allows you to extend the suppression rules by a certain time frame of 1, 3, 6, or 12 months. If one of these time frames is selected, the suppression rule for the particular scenario is extended by the chosen period, from the original day it was due to expire.
Suppression End Date	Enter the suppression end date. This allows you to select the suppression rule's end date. You can select the date on which you want the suppression rule to end. For example, see *Table 23*. **Note:** The Extend Suppression By and the Suppression End Date options are mutually exclusive, therefore you can enter only one of them at a time. The Suppression End Date field is pre-populated in the following cases: ● When you have selected only one rule from the List section ● When multiple suppression rules are selected and all of them have the same end date ● The system updates the relevant dates once you have saved your entries and returns you to the Suppression Rules Search and List page, where updates are displayed in the Suppression Rules List section.
Add a Comment	Enter comments in the comments box to justify your changes in the suppression rules. If multiple rules are selected for the update process, these comments are applied to all selected suppression rules. **Note:** If you try to save updates without entering comments, the system displays a warning to remind you to enter comments. The comments text box has no character restrictions and scroll bars can be used for text that exceeds the visible space provided.

The following table provides examples of date changes for Suppression End Date.

Table 23. Examples of Updated Dates for Suppression Rules

Suppression Rule ID	End date (before updating)	Results (after updating) Extend Suppression By 6 months	Results (after updating) Suppression End Date 05/25/2009
SR1	03/16/2009	09/16/2009	05/25/2009
SR2	04/17/2009	10/17/2009	05/25/2009
SR3	04/25/2008	10/25/2008	05/25/2009

4. Click **Save.** The application records the action as Modified and retains the Active status to the rule or rules.

Note:

- If one or more suppression rules expires (reaches the end date), the system records the action as Expired and changes the status to Inactive.

- An expiration end date entered in the Update section applies to all the currently selected suppression rules.

Ending Suppression Rules

A firm can decide that suppressing these alerts results in too few results or missing behaviors of interest. They would then end the suppression rules to allow these alerts to display again.

This section explains how to end suppression rules. The End Suppression Rules feature is available only for active suppression rules.

To end suppression rules, follow these steps:

1. Navigate to the Suppression Rule List page. For more information on how to access the Suppression Rule list page, see *Accessing Suppression Rules page* section.

2. Select one or more check boxes against each active rule that you want to end suppression rule. Click **End**. The End Suppression Rule section is displayed.

3. Enter comments to justify your action to end suppression rule.

4. Click **Save**. The system records the action as *Terminated* and assigns the status as *Inactive.*

    Note: The suppression rule status of *Active* suppression rules changes to *Terminated* when those rules are terminated manually. For all Active suppression rules that reach their expiration date, the system automatically changes their status to *Expired.* This system action is also tracked in the Rule Action History.

Managing Four-Eyes Approval Process

This section explains the Four-Eyes approval process for Suppression Rule. The system must be configured for Four Eyes Approval. An Analyst recommends for alert suppression rule in Alert workflow. The Supervisor can Approve, Update and Approve, and Reject recommended suppression rules. A notification is sent to the analyst based on the action taken by the supervisor.

This section covers the following topics:

- Recommending Alert Suppression Rules
- Approving Suppression Rules
- Updating and Approving Suppression Rules
- Rejecting Suppression Rules
- Recommending to End Suppression Rule
- Ending Suppression Rules

Recommending Alert Suppression Rules

If you are an Analyst II or III user, Alert Management system enables you to recommend alert suppression rules. For users requiring supervisory approval, actions are labeled with *Recommend to* easily identify those actions that require additional oversight.

This section describes how to recommend for alert suppression rule, see *Recommending To Close Alerts* section in Managing Alerts chapter.

Approving Suppression Rules

The Approve Suppression Rule page provides you with the option to approve all the selected rules from the Suppression Rule List section. Based on user roles, you can approve the selected rules which are in *Recommended* status.

To approve suppression rules, follow these steps:

1. Navigate to the Suppression Rule List page. For more information on how to access the Suppression Rule list page, see *Accessing Suppression Rules page* section.

2. Select one or more check boxes against each rule that you want to approve for suppression. Click **Approve**. The Approve Suppression Rule confirmation dialog box is displayed.

3. Click **OK**. The status of the rule (IDs) changes from **Recommended** to **Active**. A notification is sent to the analyst who has recommend for an approval.

   Note: If you select one or more Rule ID (s) which are not in *Recommend* status then the system displays the following message: *The Action could not be completed as the selected rule ID(s) are not in Recommend Status.*

Updating and Approving Suppression Rules

The Update and Approve Suppression Rule page allows you to update and approve all selected rules from the Suppression Rule List section. Based on user roles, you can update and approve the selected rules in *Recommended* status.

To update and approve suppression rules, follow these steps:

1. Navigate to the Suppression Rule List page. For more information on how to access the Suppression Rule list page, see *Accessing Suppression Rules page* section.

2. Select one or more check boxes against each rule that you want to update and approve, which are recommended for suppression. Click **Update** and **Approve**. The Update Suppression Rule page displayed.

Figure 33. Approving Suppression Rules

3. Enter the information in the respective fields. For more information on the fields, see *Table 22*.

4. Click **Save**. The status of the rule (IDs) changes from **Recommended** to **Active**. The triggered alert or alerts are moved to *Closed* status. A notification is sent to the analyst who has recommend for an approval.

Rejecting Suppression Rules

The Reject Suppression Rule page allows you to reject all selected rules from the Suppression Rule List section. Based on user roles, you can reject the selected rules in *Recommended* status.

To reject suppression rules, follow these steps:

1. Navigate to the Suppression Rule List page. For more information on how to access the Suppression Rule list page, see *Accessing Suppression Rules page* section.

2. Select one or more check boxes against each rule that you want to reject, which are recommended for suppression. Click **Reject**. The Reject Recommendation dialog box is displayed.

Figure 34. Comments Box

3. Enter comments to justify your action.

4. Click **Save**. The system records the action as *Terminated* and assigns the status as *Inactive*. The triggered alert status is unchanged and a notification is sent to the recommended analyst and the alert is reassigned to the user.

Recommending to End Suppression Rule

This section explains how you can recommend to end suppression rules. Analyst III can recommend to end suppression rule.

For more information, see *Recommending To Close Alerts* section in the Managing Alerts chapter.

Ending Suppression Rules

This section explains how to end suppression rules. The End Suppression Rules feature is available only for recommended suppression rules.

For more information on how to end recommended suppression rules, see *Ending Suppression Rules.*

Note: The rule status of recommended suppression rules changes to *Inactive.*

Searching Suppression Rules

The Suppression Rules Search page enables you to search for a selected list of suppression rules, based on the criteria that you provide in the search fields. By default, all the search fields are blank. This section explains how to search Alert Suppression rules list.

To the search Alert Suppression list, follow these steps:

1. Navigate to the Alert Suppression page.

Figure 35. Suppression Rules Search page

Note: Blank search is not supported. You must to enter one or more search criteria in order to execute a search.

2. Enter the following information to filter suppression rules.

Table 24. Suppression Rules Search Components

Criteria	Description
Suppression Rule Created From Date (Start Date)	Specify the time frame in which you want to view suppression rules. Enter the start (Suppression Rule Created From) and end (Suppression Rule Created To) dates. Application displays only those rules that are created within the time frame.
Suppression Rule Created To Date (End Date)	• In order to search for suppression rules after the specified date, you must enter only a From search date. • To search for rules before a certain date, you must enter only a To search date. Leaving the date fields blank returns rules regardless of their creation dates.
Expires (in days)	Enter a value in the Expiring (in days). Application displays only those rules that will expire within the specified number of days. **Note:** These filters are mutually exclusive per search. The system does not support searching by both Expires (in days) and Expiring From and Expiring To dates at the same time
Expiring From (Start Date) Expiring To (End Date)	Specify the time frame for searching the suppression rules based on the expiration dates of those rules. Specify the start (Expiring From) and end (Expiring To) dates. When these filters are used. Application displays only those rules that are set to expire within the time frame identified by those dates. You can also opt for the following option to search. • Enter Expiring From (Start Date). This filters the suppression rules list based on the expiration start date. • Enter Expiring From (End Date). This filters the suppression rules list based on the expiration end date.
Focus Type	Select the focus type from the drop-down list. This filters the suppression rules by the focal type of the business entity associated with the suppression rule.
Focus Name	Enter the focus name. This filters the suppression rules by the Focus Name of the business entity associated with the suppression rule.
Focus ID	Enter the focus unique number. This filters the suppression rules by the Focus ID of the business entity associated with the suppression rule.
Scenario Class	Select the scenario class from the drop-down list. This filters the suppression rules by the scenario class associated with a rule, listed by its abbreviation. This drop-down list contains only the scenario classes that you are authorized to view. If you filter by Class, you cannot filter by Scenario.
Scenario	Select the scenario from the drop-down list. This filters the suppression rules by the scenario associated with a rule that is, by the name of the behavior or activity that generated that rule.
Created By	Select the creater from the drop-down list. This filters the results by the user ID of the user who created the rule.
Highlight Name	Select the highlight name from the drop-down list. This filters the suppression rules by the highlight binding used in the suppression rule. (Bindings are variables captured in a scenario pattern that, in this case, are used for defining highlights.)
Triggering Alert ID	Enter the triggering alert ID. This filters the suppression rules based on the alert ID of the alert that was closed with the Close and Suppress action. This filter can accept up to 100 natural numbers and provides comma-separated searching.

Table 24. Suppression Rules Search Components (Continued)

Criteria (Continued)	Description
Suppression Rule ID	Enter the suppression rule ID. This filters the suppression rules based on the Suppression Rule ID you enter. This filter can accept up to 100 natural numbers and provides comma-separated searching. **Note:** Search by Suppression Rule ID will ignore all other search criteria.
Rule Status	Select the rule status from the drop-down list. This filters the suppression rules based on the rule status you select. The following are the options available: ● Active ● Inactive ● Recommend

3. Click **Go**. The relevant suppression rules are displayed.
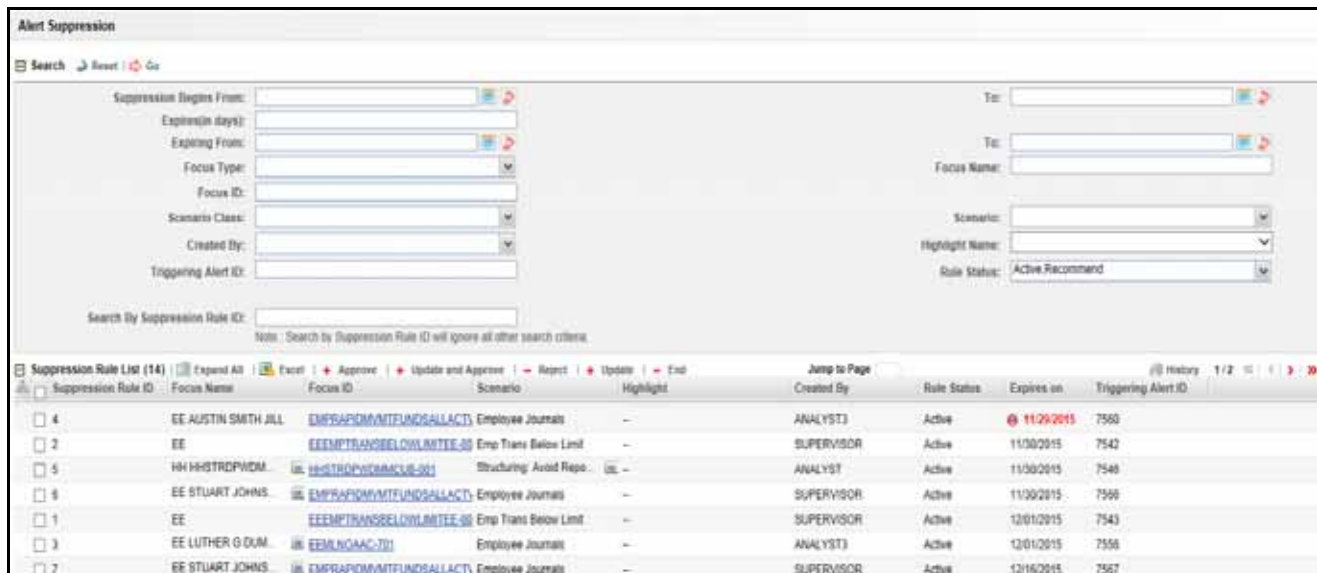
Figure 36. Suppression Rule List

Visual Indicators

The system displays a visual indicator for all rules that are *near expiration*. Starting from the first day (of the X days) until the day before the rule expiration date (for example, if the near expiration duration is set to *5 days* and the suppression rule end date for a suppression rule is can 5th, the system displays the rule end date in the color red from April 31st to can 4th). The system displays a different visual indicator than the *near expiration* indicator when the rule reaches the rule end date (in other words, the system displays the rule end date in a white font with a red background on the date it is set to end. For example, if the suppression end date for a rule is can 5th, the system displays the rule end date in a white font with a red background on can 5th). Visual indicators are system-configurable. Contact your System Administrator if you want to reconfigure these indicators.

Figure 37. Visual Indicators for Suppression Rules Expiration Dates

CHAPTER 6 *Managing Trusted Pairs*

This chapter describes the concept and process of Trusted Pair in the Monitoring workflow of Alert Management. It provides systematic instructions to carry out various actions according to the workflow and user roles. This also helps you to understand the usage of various components to accomplish each task.

This chapter covers the following topics:

- About Trusted Pair
- User Roles and Actions
- Trusted Pair Workflow
- Modifying Trusted Pair
- Cancelling Trusted Pair
- Managing Four-Eyes Approval Process
- Searching Trusted Pair
- Viewing Trusted Pair Action History

About Trusted Pair

Trusted Pair is the concept of reducing the number of false positives alerts by identifying transactions between parties viewed as having a trusted relationship. After analyzing alerts, you can determine two parties are Trusted Pair when the activity between two parties on one or more of the alerting transactions is an acceptable business practice and poses little risk to the institution.

During the process of ingesting transactional information (Wires, Checks and Monetary Instruments, Back Office Transactions, and Insurance Transactions), the application flags a transaction as trusted if at least one party/counter-party pair on the transaction is considered to be a trusted pair. These transactions can be optionally excluded from detection for many Money Laundering (ML) and Fraud (FR) class scenarios through the use of a threshold parameter. As the relationship between a pair of parties is marked trusted for some period of time and is excluded from the process of behavior detection, the workload of an analyst can be greatly reduced. If the decision is made to not exclude trusted transactions from detection, alerts involving trusted transactions display information regarding the percent of the alert's transactions that involve trusted pair versus transactions that do not involve trusted pair. This will allow institutions to potentially score these types of alerts as lower priority or execute automated auto-close rules. Only party identifiers in non-institutional roles can be designated as trusted.

Trusted Pair utilizes a versioning approach for maintaining records of trusted pair to support a Four-Eyes Approval workflow as well as audit changes to records. Versioning means that for each trusted pair that is created, subsequent modifications, cancellations, approvals, or rejections create a new version of that record; reflecting any change in status to the trusted pair as well as tracking the actual change. The trusted pair's ID remains the same from version to version, allowing you to easily identify and track the history of that trusted pair.

Note: The ability to manage trusted pair through the Manage Trusted Pair workflow user interface (UI) is dependent on how an organization chooses to work with trusted pair. If your site has elected to create trusted pairs by passing them into the Oracle Financial Services FSDF during the process of ingesting business and transaction data, then management of those trusted pair is disabled via the UI. The Manage Trusted Pairs tab is suppressed and users will not have the option to designate trusted pair from the alert workflow.

Key Features

- Analyze and determine that two parties are trusted

- Decrease the number of false positive alerts by excluding trusted pairs from the behavior detection process

- Exclude trusted pairs from the behavior detection process

- Define trusted pair activity based on direction of movement of funds to and from designated parties

- Trusted Pairs can be cancelled when two parties are no longer trusted to carry out transactions

- View audit trail of changes to a trusted pairs over time

- Recommend two parties as trusted pair

- Recommend modifications or cancellation for a trusted pair

User Roles and Actions

This section describes various user roles and actions they can perform in the Trusted Pair workflow.

The following table details the user roles and actions in the Trusted Pair workflow.

Table 25. User Roles and Actions-Trusted Pairs

User Actions	User Roles					
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor
Access to Designate Trusted Pairs button on Matched Information section		X	X	X		
Access to View Search and List for Trusted Pairs	X	X	X	X	X	X
Reject Trusted Pairs recommendations				X		
Self-Reject Trusted Pairs recommendations		X	X			
Approve Trusted Pairs recommendations				X		
Cancel Trusted Pairs				X		
Recommend to cancel Trusted Pairs		X	X			
Modify Trusted Pairs				X		
Recommend to modify Trusted Pairs		X	X			
View Trusted Pairs History	X	X	X	X	X	X

Trusted Pair Workflow

The following figure shows the Trusted Pair workflow with and without Four-Eyes approval.
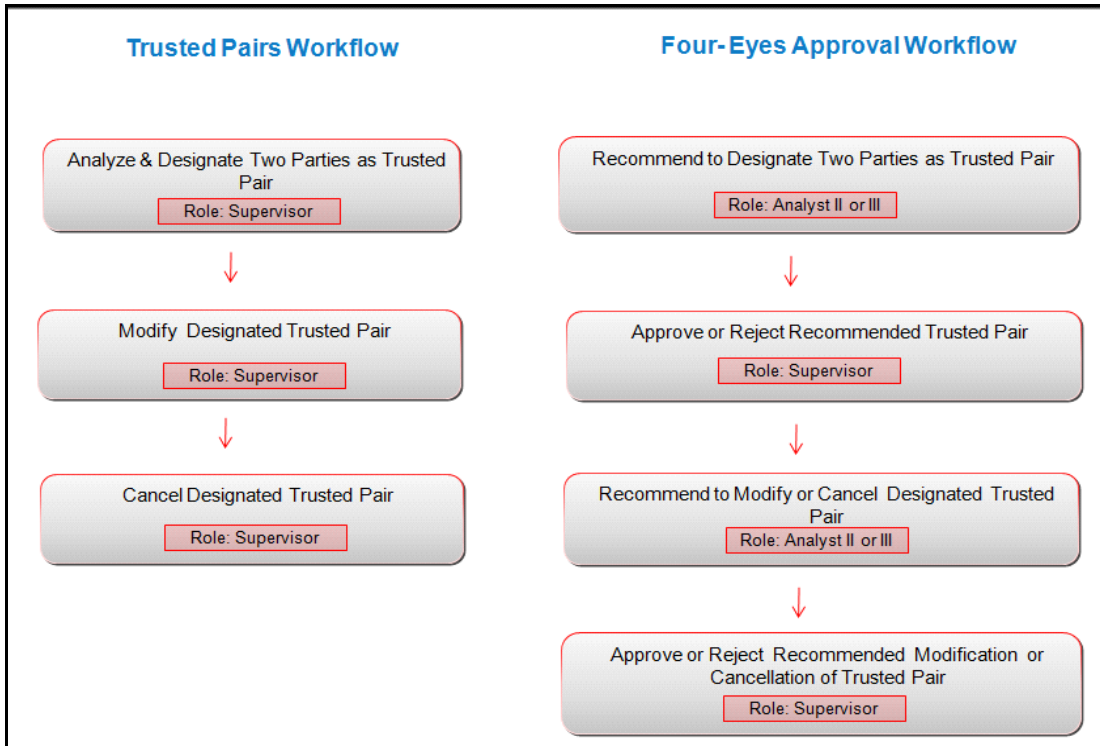
Figure 38. Trusted Pair Workflows

This section covers following topics:

● Trusted Pair without Four-Eyes Approval Workflow

● Trusted Pair with Four-Eyes Approval Workflow

Trusted Pair without Four-Eyes Approval Workflow

The following table describes about the Trusted Pair workflow without Four-Eyes approval.

Table 26. Trusted Pair without Four-Eyes Approval Workflow

Action	Description	Roles
Modifying Trusted Pair	Users can modify the existing trusted pair. You can change the Direction, Trusted Period, and Expiration Date of Trusted Pairs that are mentioned at the time of designating new trusted pair.	Supervisors
Cancelling Trusted Pair	Users can cancel trusted pair when they analyze that two parties are no longer trusted to carry out transactions.	Supervisors

Trusted Pair with Four-Eyes Approval Workflow

The following table details about the Trusted Pair workflow with Four-Eyes approval.

Table 27. Trusted Pair with Four-Eyes Approval Workflow

Action	Description	Roles
Recommending to Designate Two Parties as Trusted Pair	When users determine that an activity between two parties is an acceptable business practice and poses little risk to the institution, then the users can recommend to designate those parties as a Trusted Pair. This action is available only from within the alert management workflow, Alert Details page.	Analysts II and III
Approving or Rejecting Recommended Trusted Pair	Users can approve or reject a recommendation for designating two parties as a trusted pair.	Supervisors
Recommending to Modify or Cancel Designated Trusted Pair	Users can recommend modifications or cancellations for trusted pairs. Modifications can be made to the direction of trust between the pair, the Trusted Period and the Expiration Date when designating new trusted pair.	Analysts II and III
Approving or Rejecting Trusted Pair Recommended for Modification or Cancellation	Users can approve or reject recommended modification or cancellation for trusted pair.	Supervisors

Accessing Trusted Pairs page

This section explains how to access the Trusted Pairs page to take various actions on trusted pair.

To access the Trusted Pairs page, follow these steps:

1. Navigate to the OFSAA Applications Home page. For more information, see *Chapter 3, Getting Started.*

2. Click **Administration** in the RHS menu.

3. Hover over the **List Management** menu and click **Trusted Pairs**. The Trusted Pairs page is displayed.

Note: Click **Search** to display the **Trusted Pair List** page.

Modifying Trusted Pair

If you are a Supervisor, you can modify the existing trusted pairs. Or, if you are a Analyst II or III, you can recommend to modify trusted pairs. You can change the direction, Trusted Period, and Expiration Date of Trusted Pairs that are mentioned at the time of designating new trusted pair.

To modify designated trusted pair, follow these steps:

1. Hover over the **List Management** menu, select **Trusted Pairs**. The Trusted Pairs Search page is displayed.

Figure 39. Trusted Pairs Search page

2. Search for trusted pairs that you want to modify.

    For more information on searching trusted pairs, see *Searching Trusted Pair* section.

    The Trusted Pairs List page is displayed according to your search criteria. This matrix is sorted on the Trusted Pairs ID column in ascending order.

Figure 40. Trusted Pairs List page

3. Select one or more check boxes against each Trusted Pairs IDs and click **Update**. The Update Trusted Pairs page is displayed.

    Note: If you select Trusted Pair IDs with different statuses or trusted pair in Inactive status. The confirmation dialog box displays the following message: *You are attempting to update the selected trusted pair(s), but one or more of the selected pairs have different versions available. Select only trusted pair(s) that have the value as Yes in the Editable field column to proceed with Updated action.*
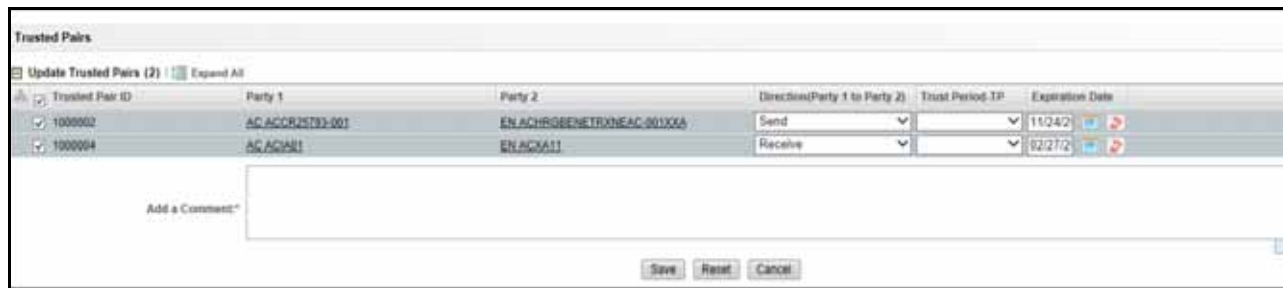
Figure 41. Update Trusted Pairs page

4. Select one or more check boxes against each Trusted Pairs IDs to modify trusted pair. All fields are enabled.

5. Modify the necessary information.

   For more information on the fields, see *Designating Trusted Pair* section.

6. Click **Save** to update the information. The confirmation dialog box displays the following message: *The Selected pair IDs will be updated, click OK to save the changes.*

7. Click **OK** to save the updates. The Trusted Pairs Search and List page is displayed with latest updates.

   For more information on Results from Updating Trusted Pairs Relationships, see *Appendix C, Results from Updating Trusted Pairs Relationships*

Cancelling Trusted Pair

If you are a Supervisor, you can cancel the existing trusted pair. Or, if you are a Analyst II or III, you can recommend to cancel trusted pair. You can cancel trusted pairs when you analyze that two parties are no longer trusted to do further transactions.

Risk Escalation Recommend Cancel: One or more members of the trusted pair has experienced an increase in their effective risk that can affect whether or not you want to continue to let them be a member of a trusted pair. The risk increase was sufficient enough to cause the system to flag the trusted pair as needing review due to risk escalation, with a system recommendation to cancel the trust.

Trusted pair with a Risk Esc Rec Cancel recommendation are still considered to be active and will continue to be used to flag transactions until such time as the recommendation to cancel is approved. A search for Risk Esc Rec Cancel trusted pair returns only those trusted pair currently in Risk Esc Rec Cancel status.

To cancel designated trusted pair, follow these steps:

1. Hover over the **List Management** menu, select **Trusted Pairs**. The Trusted Pairs Search page is displayed.

Figure 42. Trusted Pairs Search page

2. Search for trusted pair that you want to cancel.

   For more information on searching trusted pair, see *Searching Trusted Pair* section.

   The Trusted Pairs List page is displayed according to your search criteria. This matrix is sorted on the Trusted Pairs ID column in ascending order.

Figure 43. Trusted Pairs List page

3. Select one or more check boxes against each Trusted Pairs IDs and select **Cancel** from the Action drop-down list.

4. Enter the justification for cancelling trusted pair in the Comment box.

5. Click **Save**. The confirmation dialog box displays the following message: *The Selected pair IDs will be updated. click OK to save the changes.*

6. Click **OK**. The Trusted Pairs Search and List page is displayed with latest updates.

Managing Four-Eyes Approval Process

This section explains the Four-Eyes approval process for Trusted Pair. The system must be configured for the Four- Eyes Approval. An Analyst II or III recommends to designate two parties as trusted pair in the Alert workflow. The Supervisor can approve, reject, or cancel recommended trusted pair. A notification is sent to the analyst based on the action taken by the supervisor.

This section covers following topics:

- Recommending to Designate Two Parties as Trusted Pair
- Approving or Rejecting Recommended Trusted Pair
- Recommending to Modify or Cancel Designated Trusted Pair
- Approving or Rejecting Trusted Pair Recommended for Modification or Cancellation

Recommending to Designate Two Parties as Trusted Pair

If your analysis suggests that parties involved in the alerted transactions have a trusted business relationship, then you can recommend to designate those parties as being trusted pair. You should be have Analyst II or III role to recommend to designate two parties as trusted pair.

To recommend two parties as designate trusted pair, follow these steps:

For more information on steps, see *Designating Trusted Pair* section.

Approving or Rejecting Recommended Trusted Pair

If you are a Supervisor, the Trusted Pairs Details page allows you to approve or reject trusted pair which are recommended for designating two parties as trusted pair.

To approve or reject recommended trusted pair, follow these steps:

1. Hover over the **List Management** menu, select **Trusted Pairs**. The Trusted Pairs Search page is displayed.

Figure 44. Trusted Pairs Search page

2. Search for Trusted Pairs IDs with *Pending* status or use more search criteria.

   For more information on searching trusted pair, see *Searching Trusted Pair* section.

According to your search criteria, the Trusted Pairs List page is displayed. This matrix is sorted on the Trusted Pairs ID column in ascending order.

Editable	Trusted Pair ID	Party 1	Party 2	Direction	Status	Created Date	By	Expiration Date	Cancelled Date	Review Date	Review Reason	Action
No	1000003	AC ACIA01	EN ACXA01	Receive	Inactive	02/24/2016	SUPERVISOR	02/24/2017	02/24/2016	--	--	
Yes	1000002	AC ACCR25793-001	EN ACHRGBENETRXNEAC-001XX,	Send	Active	02/24/2016	SUPERVISOR	11/24/2016	--	--	--	
Yes	1000004	AC ACIA01	EN ACXA11	Receive	Pending	02/25/2016	AMANALYST2	🔴 02/27/2016				Reject / Approve

Comment:*

Save   Clear

Figure 45. Trusted Pairs List

3. Select one or more check boxes against each Trusted Pairs ID. The Action drop-down list is enabled.

   Note: You can select only Editable Trusted Pairs IDs.

4. Select Approve, Reject, or Cancel from the Action drop-down list.

5. Enter the justification for your action in the Comment box.

6. Click **Save** to confirm the action. The confirmation dialog box displays the following message: *The Selected pair IDs will be updated, click OK to save the changes.*

7. Click **OK** to save the changes. The Trusted Pairs Search and List page is displayed with latest updates.

Recommending to Modify or Cancel Designated Trusted Pair

Analysts II and III are allowed to recommend modifications or cancellation for a trusted pair.

To recommend modifications, see *Modifying Trusted Pair* section.

To recommend to cancellation, see *Cancelling Trusted Pair* section.

Note: If you cancel the recommended trusted pair, the trusted pair status becomes Inactive.

Approving or Rejecting Trusted Pair Recommended for Modification or Cancellation

If you are a Supervisor, the Trusted Pairs Details page allows you to approve or reject trusted pair which are recommended for modification or cancellation.

To approve or reject recommended trusted pair for modification or cancellation, follow these steps:

For more information steps, see *Approving or Rejecting Recommended Trusted Pair* section.

Note:

- If you approve or reject the recommended modifications, the modified trusted pair status becomes *Active*.

- If you cancel the recommended trusted pair, the trusted relation ends for two parties and trusted pair becomes *Inactive*.

Searching Trusted Pair

This section allows you to filter trusted pair that you want to view, analyze, and take various actions.

Note: Blank search is not supported. You need to enter one or more search criteria in order to execute a search.

To search trusted pair, follow these steps:

1. the **List Management** menu, select **Trusted Pairs**. The Trusted Pairs Search page is displayed.

Figure 46. Trusted Pairs Search page

2. Enter the following information in the respective fields.

Table 28. Trusted Pairs Search

Fields	Description
Trusted Pairs Created From and To	Specify the start (Trusted Pairs Created From) and end (To) dates using calendar. You can view only those trusted pairs that are created within the specified time frame. You can also choose to search by specifying only the From or To date. It is not required to enter both.
Expires (in days)	Specify the number of days in which the trust expires by entering a value in the Expiring (in days) filter. You can view only those trusted pairs that are set to expire within the specified number of days.
Expiration From and To	Specify the start (Expiring From) and end (To) dates using calendar. You can view only those trusted pairs that will expire within the specified time frame. You can also choose to search by specifying only the From or To date. It is not required to enter both. **Note:** The system does not support searching by both Expires (in days) and Expiring From and To dates, simultaneously.
Cancellation Date From and To	Specify the start (Cancellation Date From) and end (To) dates using calendar. You can view only those trusted pairs that are cancelled within the specified time frame. You can also choose to search by specifying only the From or To date. It is not required to enter both.

Table 28. Trusted Pairs Search (Continued)

Fields	Description
Review Date From and To	Specify the start (Review Date From) and end (To) dates using calendar. You can view only those trusted pairs that are reviewed within the specified time frame. Review search date filters allow you to search for trusted pairs that are flagged by the system as requiring review based on an escalation in effective risk of one or more of the members of the trusted pair. The review date represents the date the system flagged the pair as it requires the review. When you specify the start (Review Date From) and end (To) dates. You can also choose to search by specifying only the From or only the To date. It is not required to enter both.
Status	Select the status of the trusted pair from the drop-down list. The following is the list of statuses: ● **Active**: The trusted pair is in an active status. In this status you can modify and cancel trusted pairs. ● **Inactive**: The trusted pair is inactive. A Trusted Pair record is inactive if the trusted pair is modified in some way resulting in the currently active version of the record becoming inactive. A trusted pair is considered to be completely inactive only if all versions of the trusted pairs are in an Inactive status. A search for inactive trusted pair records returns only those trusted pairs that are completely inactive. If a trusted pair is currently active but has inactive records associated with it due to modifications and updates, that trusted pair is not returned in the results. ● **Pending**: A trusted pair has either been newly recommended, or a recommendation is made for a modification which requires supervisory approval. Until the recommendation is either accepted or rejected, the record remains in a Pending status. An active trusted pair in Pending status is considered to be Active. **Note:** Active trusted pairs with a Pending recommendation are still considered to be active and will continue to be used to flag transactions based on the Trust Pairs attributes as they were before any modifications. A search for pending trusted pair records returns those trusted pair records in a Pending status. ● **Expired**: The trusted pair has reached its expiration date and the system has set the status to Expired. A search for expired trusted pairs records returns only those trusted pairs records in an Expired status. ● **Risk Esc Rec Cancel**: (Risk Escalation Recommend Cancel) One or more members of the trusted pair has experienced an increase in their effective risk that can affect whether or not you want to continue to let them be a member of a trusted pair. The risk increase was sufficient enough to cause the system to flag the trusted pair as needing review due to risk escalation, with a system recommendation to cancel the trust. **Note:** Trusted Pairs with a Risk Esc Rec Cancel recommendation are still considered to be active and will continue to be used to flag transactions until such time as the recommendation to cancel is approved. A search for Risk Esc Rec Cancel Trusted Pairs returns only those trusted pairs currently in Risk Esc Rec Cancel status. ● **User Rec Cancel**: (User Recommend Cancel) A user has recommended that this trusted pair be cancelled. Records in a User Rec Cancel status require supervisory approval of the cancel recommendation. **Note:** Trusted Pairs with a User Rec Cancel recommendation are still considered to be active and will continue to be used to flag transactions until such time as the recommendation to cancel is approved. A search for User Rec Cancel Trusted Pairs returns only those trusted pairs currently in User Rec Cancel status.

Table 28. Trusted Pairs Search (Continued)

Fields	Description
Direction	When you filter for a specific direction of a trusted relationship, you can view only those trusted pairs whose trust direction matches the filter value specified. Possible directions are Send, Receive, and Both. A search on a Direction of Send will return all trusted pairs where party 1 is trusted to Send to party 2. A direction of Both means that the two parties are allowed to both send and receive funds from one another.
Focus Type	Select one or more focus type from the drop-down list. You can view trusted pair where one or both members of the pair match the focus type. You can also combine a search by Focus Type with a specified Focus ID. You can search by only a Focus ID, without specifying a Focus Type. You can also search by specifying only a Focus Type with no accompanying Focus ID.
Focus ID	Enter Focus ID. You can view trusted pair where a pair matches on the party identifier. You can also search by Focus ID using the percent sign (%) as a wildcard. For example, ● All parties whose Focus ID begins with AC1 enter AC1% in the Focus ID search field. ● All parties whose Focus ID ends in AC1 enter %AC1 in the Focus ID search field. **Note:** You can also use the wildcard anywhere in the middle of the identifier if you know the beginning and end but are unsure of the middle values.
Created By	Select Trusted Pairs Creator from the drop-down list, for example, Analyst or Supervisor. You can view only those trusted pairs that are created by the specified user.
Triggering Alert ID	Enter the Triggering Alert ID. You can view those trusted pairs that are created during the investigation of the specified alert (in other words, the Create trusted pairs action was taken while investigating this alert).
Trusted Pairs ID	Enter the Trusted Pairs ID. You can view those IDs for information about the trusted pair. You can also search for multiple IDs by separating IDs with commas.

Note: The From date must be earlier than the To date.

3. Click **Go**. The relevant List page is displayed.

   Note: Searches by Trusted Pairs ID and other search criteria are mutually exclusive. If you attempt to search by Trusted Pairs ID and any other filters, the other filters are ignored.

Viewing Trusted Pair Action History

The Trusted Pair Action History displays a history matrix which provides an audit trail of changes to a trusted pair over time. Changes include actions such as when it was created, modified or canceled, along with the reason and comments for each action.

To view trusted pair action history, follow these steps:

1. Navigate to the Trusted Pair List page or the Update Trusted Pair page.

2. Click **History**. The Trusted Pair Action History page is displayed.
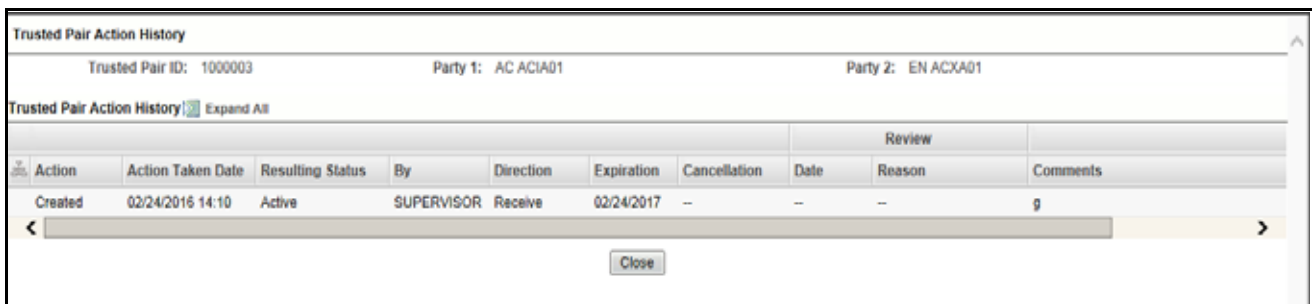
Figure 47. Trusted Pair Action History window

The following table displays the history for the trusted pair:

Table 29. Trusted Pair List Matrix

Column	Description
Trusted Pair ID	Displays the unique identification of the trusted pair.
Party 1	Display the other party that belongs to the trusted pair. The party identifier displays as a link that, when clicked, generates a window providing detailed business information about the entity. **Note:** If your access privileges do not give you rights to see information about this entity, the link is disabled.
Party 2	Displays the other party that belongs to the trusted pair. The party identifier displays as a link that, when clicked, generates a window providing detailed business information about the entity. **Note:** If your access privileges do not give you rights to see information about this entity, the link is disabled.
Action	Displays the action taken on the selected trusted pair. The following are types of actions: ● Modified ● Cancelled ● Created ● Approved ● Rejected ● Risk Review Required
Action Taken Date	Displays the date and time on which the action is taken.

Table 29. Trusted Pair List Matrix (Continued)

Column (Continued)	Description
Resulting Status	Displays the status resulting from taking an action on the selected trusted pair. For example, Active, Inactivate, and Pending.
By	Displays the ID of the user who created the trusted pair.
Direction	Displays any one of the values Send, Receive, or Both based on the direction of the selected trusted pair. Direction displays relative to the direction of trust from Party 1 to Party 2.
Status	Displays the status of the trusted pair. Possible statuses are Active, Inactive, Pending, Expired, Risk Esc Rec Cancel, and User Rec Cancel.
Expiration Date	Displays the expiration date of the trust relationship.
Cancelled Date	Displays the cancellation date of the trust relationship.
Review Date	Displays the date on which the trusted pair was flagged for review.
Review Reason	Displays the reason the trusted pair was flagged for review.
Comments	Displays the comments associated with the action that was taken. If a comment exceeds the width of the Comments column you can click on the ellipses (...) to display a separate pop-up window which displays the complete text.

CHAPTER 7   *Managing Trade Blotter*

This chapter describes the Trade Blotter functionality and gives step-by-step instructions for using it.
The following topics are covered in this chapter:

About Trade Blotter

The Trade Blotter functionality allows trades to be viewed and reviewed, primarily for suitability issues within the wealth management sector, by compliance analysts and business supervisors after a trade is executed. The Trade Blotter is a list of trades returned after a search based on specified criteria. An analyst or supervisor can view various trade details, view related trade documents, enter a comment on a specific trade, and then mark the trade as reviewed or reviewed with follow-up.

Key Features

The Alert Management UI allows you to perform the following actions:

- Search for trades using the specified criteria
- View the trade details
- Enter comments on the specified trade and mark the trade as reviewed or reviewed w/follow-up.
- Export and email trades

User Roles and Actions

This section describes various user roles and actions they can perform in the Trade Blotter workflow.

The following table details the user roles and actions in the Trade Blotter workflow:

User Actions	User Roles									
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
Access to View Trades in "Reviewed" status (This controls user's access to trades that are in the Reviewed status)			X	X	X	X				
Access to View Trades in "New- Un reviewed" status (This controls user's access to trades that are in the Pending status)			X	X	X	X				
Access to View Trades in "Reviewed with Follow-Up" status (This controls user's access to trades that are in the Reviewed with Follow-Up status)			X	X	X	X				
Access to mark a trade as a "Reviewed" Trade (when the existing trade review status is "New- Un reviewed")			X	X						
Access to mark a trade as a "Reviewed with Follow-Up" Trade (when the existing trade review status is "New- Un reviewed")			X	X						
Access to Add Attachments to Trades			X	X						
Access to Add Comments to Trades			X	X						
Access to View Trade Attachments Audit History, Comment Audit History and Trade Action History			X	X		X				
Access to mark a trade as a Reviewed Trade (when the existing trade review status is Reviewed with Follow-Up)				X						
Access to mark a trade as a Reviewed with Follow-Up Trade (when the existing trade review status is Reviewed)				X						
Access to Send email via Trade Blotter			X	X						
Access to Send email and Request a Response via Trade Blotter			X	X						

Trade Blotter Workflow

The following figure shows the Trade Blotter workflow:
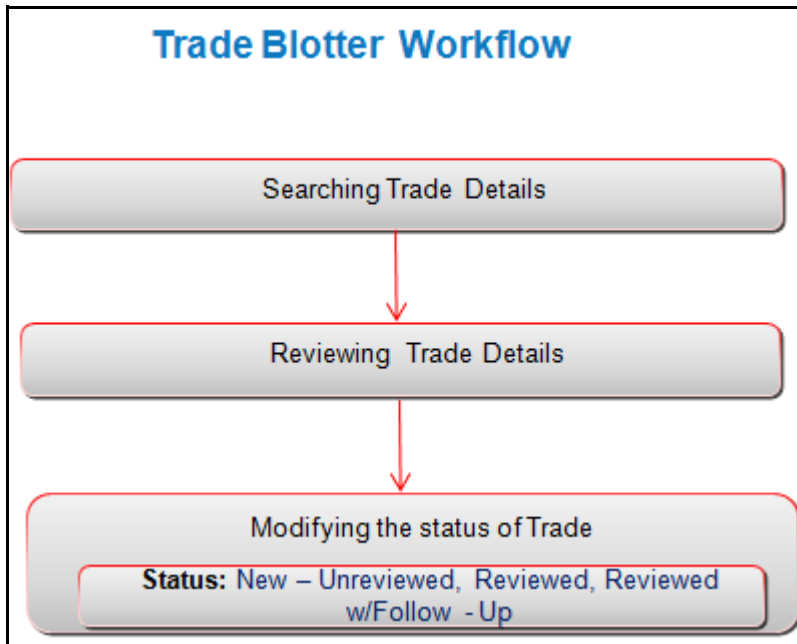
Figure 48. Trade Blotter Workflow

Accessing Trade Blotter

This section explains how to access the Trade Blotter page. The page is available only if the Trade Blotter functionality is enabled at installation and you have the appropriate permissions to view it. You can set the Trade Blotter default search page from your Oracle Financial Services Alert Management UI.

To access the Trade Blotter page, follow these steps:

1. Navigate to the OFSAA Applications Home page. For more information, see *Chapter 3, Getting Started.*

2. Click **Trade Blotter** in the RHS menu. The **Trade Blotter** page is displayed.

Searching Trades

The Trade Blotter page contains the Simple Search section and the Advanced Search section.

Searching Trades using Simple Search

Simple search enables you to search for information about a trade based on the criteria that you have selected within this search bar. This search is based on a limited set of search components.

Figure 49. Trade Blotter Simple Search

Simple search is set as a default search. When the user navigates to the Preferences page for the first time, Simple search will be selected. This search supports a wildcard search.

You can access Simple Search from the Trade Blotter Home page.

Note: You can navigate back to Simple search from the Advanced Search page by clicking the **Search** icon.

To search for trades using the Simple search components, follow these steps:

1. Navigate to the Trade Blotter Search and List page.

2. Enter the following information:

Table 30. Simple Search Components

Criteria	Description
Review Status	This is a default search. Filters the Trade List by the trade review status. Following are the options available: ● New - Unreviewed: Displays trades that are in New or unreviewed status. ● Reviewed: Displays trades that are in the Reviewed status. ● Reviewed w/Follow - Up: Displays trades that are in the Reviewed with Follow-up status.
Organization	Filters the Trade List by the names of organizations to which you have access.
Division	Filters the Trade List by the division names within an organization to which you have access.

Table 30. Simple Search Components

Criteria	Description
Branch	Filters the Trade List by the branch names within a division to which you have access.
Rep/Advisor Name	Filters the Trade List by the name of the registered Representative or the Advisor associated with the trade.
Rep/Advisor ID	Filters the Trade List by the identifier of the registered Representative or the Advisor associated with the trade.
Buy/Sell	Filters the Trade List by whether the trader is buying or selling the security. You can select either *Yes* or *No* from the drop-down list.
Client	Filters the Trade List by the names of the clients who placed the orders.
Client ID	Filters the Trade List by the identifiers of the clients who placed the orders.
Solicited	Filters the Trade List by whether the client of the Oracle Financial Services client solicited this order. You can select either *Yes* or *No* from the drop-down list.
Account	Filters the Trade List by the name associated with the account that is associated with the trade.
Account ID	Filters the Trade List by the identifier associated with the account that is associated with the trade.
Associated Alert ID	Filters the Trade List by the trade or trades associated with the entered alert identifier or identifiers.
Security Short Name	Filters the Trade List by the short names of the securities that were traded.
Security ID	Filters the Trade List by the identifiers of the securities that were traded.
Trade ID	Filters the Trade List by the trade IDs that you enter.
Trade Date From	Filters the Trade List by the beginning trade execution date against which the data is being filtered.
To	Filters the Trade List by the ending trade execution date against which the data is filtered.

3. Click **Go** on the **Search** toolbar**.** The updated Trade Blotter list page is displayed.

   The Trade List section enables you to view details about the trades and lets you to take various actions, depending on the user access.

Logic to include trades based on a user's selection in the filters, Organization, Division, and Branch:

The system includes trades under the following three conditions:

1. When only an Organization is selected, trades are included from:

● Selected Organization

- All Divisions mapped to the selected Organization
- All Branches mapped to the selected Divisions

2. When only an Organization and a Division is selected, trades are included from:

- Selected Organization
- Selected Division
- All Branches mapped to the selected Division

3. When an Organization and a Division and a Branch is selected, trades are included from:

- Selected Organization
- Selected Division
- Selected Branch

Example Hierarchy:

In the following diagram:

- A = Organization
- B,C,D = Divisions mapped to Organization A
- E,F = Branches mapped to Division B
- G,H = Branches mapped to Division C
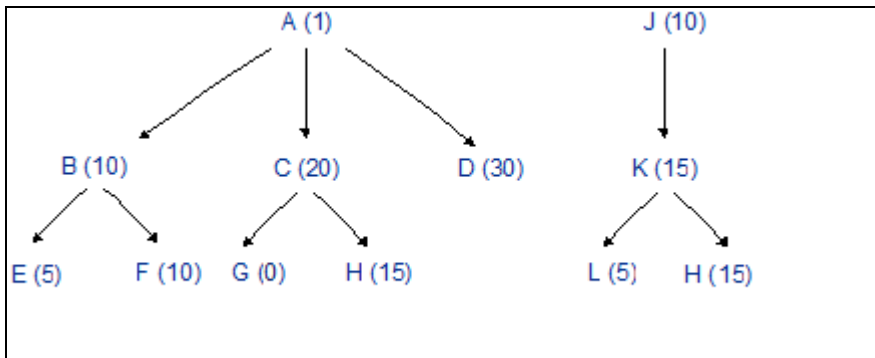
The following table explains how the system selects trades based on a user's selection in these three filters:

User Selection (Organization), (Division), (Branch)	Included in search	Number of trades displayed on UI
(A)	A,B,C,D,E,F,G,H	91
(A), (B,C,D)	A,B,C,D,E,F,G,H	91
(A), (B)	A,B,E,F	26
(A), (B), (E,F)	A,B,E,F	26
(A), (B), (E)	A,B,E	16
(A), (B), (F)	A,B,F	21

User Selection (Organization), (Division), (Branch)	Included in search	Number of trades displayed on UI
(A), (C)	A,C,G,H	36
(A), (C), (G,H)	A,C,G,H	36
(A), (C), (H)	A,C,H	36
(A), (C), (G)	A,C,G	21
(A), (B,C)	A,B,E,F,C,G,H	61
(A),(B,C), (E,F,G,H)	A,B,E,F,C,G,H	61
(A), (B,C), (F)	A,B,F,C,G,H	56
(A), (B,C),(F,H)	A,B,F,C,H	56
(A), (C,D)	A,C,G,H,D	66
(A), (C,D), (G)	A,C,D,G	51
(A), (D)	A,D	31

Searching Trades using Advanced Search

The Advanced Search offers the same search fields as provided for a simple search with an additional set of fields.

Figure 50. Trade Blotter Advanced Search

In addition to Simple Search, the Advanced Search section contains the following sections:

- Trade

- Review

- Product/Security

To search for trades using the Advanced search components, follow these steps:

1. Navigate to the Trade Blotter Search and List page.

2. Enter the search components in the following sections:

■ Simple

Table 31. Simple Search Components

Criteria	Description
Review Status	This is a default search. Filters the Trade List by the trade review status. Following are the options available: ● New - Unreviewed: Displays trades that are in New or unreviewed status. ● Reviewed: Displays trades that are in the Reviewed status. ● Reviewed w/Follow - Up: Displays trades that are in the Reviewed with Follow-up status.
Organization	Filters the Trade List by the names of organizations to which you have access.
Division	Filters the Trade List by the division names within an organization to which you have access.
Branch	Filters the Trade List by the branch names within a division to which you have access.
Rep/Advisor Name	Filters the Trade List by the name of the registered Representative or the Advisor associated with the trade.
Rep/Advisor ID	Filters the Trade List by the identifier of the registered Representative or the Advisor associated with the trade.
Buy/Sell	Filters the Trade List by whether the trader is buying or selling the security. You can select either *Yes* or *No* from the drop-down list.
Client	Filters the Trade List by the names of the clients who placed the orders.
Client ID	Filters the Trade List by the identifiers of the clients who placed the orders.
Solicited	Filters the Trade List by whether the client of the Oracle Financial Services client solicited this order. You can select either *Yes* or *No* from the drop-down list.
Account	Filters the Trade List by the name associated with the account that is associated with the trade.
Account ID	Filters the Trade List by the identifier associated with the account that is associated with the trade.
Associated Alert ID	Filters the Trade List by the trade or trades associated with the entered alert identifier or identifiers.
Security Short Name	Filters the Trade List by the short names of the securities that were traded.
Security ID	Filters the Trade List by the identifiers of the securities that were traded.
Trade ID	Filters the Trade List by the trade IDs that you enter.

Table 31. Simple Search Components

Criteria	Description
Trade Date From	Filters the Trade List by the beginning trade execution date against which the data is being filtered (start date).
To	Filters the Trade List by the ending trade execution date against which the data is filtered (end date).

■   Trade: This search section retreives details related to the trade.

Table 32. Trade Search Components

Criteria	Description
Settlement Date From	Filters the Trade List by the beginning trade settlement date against which to filter data.
To	Filters the Trade List by the beginning trade settlement date against which to filter data.
Trade Characteristics	Filters the Trade List based on the Trading Characteristics display criteria associated with the trade.
Trade Desk	Filters the Trade desk name associated with the trade.
Trade Event Type	Filters the Trade List by the entered trade or trades associated with the selected trade event type.
Gross Amount >=	Filters the Trade List by the principal amounts of the trades expressed in the issuing currency plus the commission associated with each trade expressed in the issuing currency the totals of which are greater than or equal to the entered amount.
Principal Amount >=	Filters the Trade List by the principal amounts of the trades expressed in the issuing currency that are greater than or equal to the entered amount.
Quantity >=	Filters the Trade List by the total number of units of the security that was traded that are greater than or equal to the entered amount.
Market Price >=	Filters the Trade List by trades associated with market prices greater than or equal to the entered market price.
Commission >=	Filters the Trade List by the monetary amount greater than or equal to that of the broker commission associated with this trade, expressed in the issuing currency.
Agent/Principle	Filters the Trade List by the agent or principal associated with the trade. You can select either *Yes* or *No* from a drop-down list.
Trader Name	Filters the Trade List by the name of the trader who executed the trade.
Trader ID	Filters the Trade List by the identifier of the trader who executed the trade.
Trade Entered From	Filters the Trade List by the date on which the trade was entered into the system (start date).
To	Filters the Trade List by the date on which the trade was entered into the system (end date).

■   Review: This search section searches for details using the values provided by the reviewer .

Table 33. Review Search Components

Criteria	Description
Reviewer Name	Filters the Trade List by the name of the person reviewing the trades.
Reviewer ID	Filters the Trade List by the identifier of the person reviewing the trades.
Score >=	Filters the Trade List by a score that is greater than or equal to that associated with the trade.
Standard Comments	Filters the Trade List by the standard comments (comments selected from a pre-defined list of comments) entered by the person associated with the trade. Following are the options available: ● Awaiting Response ● Price Adjust Recommended ● No Pattern/Practice Identified ● Events Appear Coincidental ● Info Barrier Policies Obeyed ● Customer Not Disadvantaged ● In Line w/ Permissions Granted ● Informed Broker/Retail Org ● Action(s) Order Driven ● No Info Sharing Indicated ● Caused by System Problems ● Fair Prices ● Incidental ● No Violative Intent ● Regulations Followed ● No Abnormality Indicated ● Order Instructions Followed
Comments	Filters the Trade List by the free text comments entered by the person associated with the trade.
Review Status From	Filters the Trade List by the status of trades reviewed within a duration starting with this date.
To	Filters the Trade List by the status of trades reviewed within a duration ending with this date.

■   Product/Security: This search section retreives details about the product categories, product types, interest rates, and so on that are associated with the trade.

Table 34. Product/Security Search Components

Criteria	Description
Product Category	Filters the Trade List by the product category associated with a trade. Following are the options available: ● Corporate Fixed Income ● Commodity ● Convertible ● Equity ● Exchange Traded Fund ● Fixed Income ● Future ● Foreign Exchange ● Insurance Fund ● Mutual Fund ● Money Market ● Option ● Other ● Preffered ● Swap
Product Type	Filters the Trade List by the product type designation of the security associated with the trade. You can choose from the drop-down list.
Product Subtype	Filters the Trade List by the product subtype associated with the trade. You can choose from the drop-down list.
ISIN	Filters the Trade List by the International Securities Identification Numbers (ISIN), which are unique international codes that identify securities issues.
CUSIP	Filters the Trade List by the Committee on Uniform Security Identification Procedures (CUSIP) unique identifier of the issuer of the trade
Yield	Filters the Trade List by the rate of return on the security
Coon Rate	Filters the Trade List by the interest rates paid for the securities that are greater than or equal to the entered amount.
Maturity Date	Filters the Trade List by the date on which the security matures.

3. Click **Go** on the **Search** toolbar.. The updated Trade Blotter List page is displayed.

The Trade List section enables you to view details about the trades and take various actions, depending on the user access.

Trade Characteristics

The Trade List page displays special text in the Trade Characteristics column of a trade row to represent the specific attributes associated with that trade that can make the trade of higher interest than the other trades (For example, the system displays RET in this column for a trade that is associated with a Retirement Account). If a trade matches more than one of the Trade Characteristics criteria, the page displays a comma-separated list of these characteristics in order according each characteristic's display ranking.

Table 35 lists the default trade characteristics and the text and ranking associated with each.

Table 35. Trade Characteristics Display Ranking

Trade Characteristics Display Criteria	Text Displayed on the User Interface	Display Ranking
Employee Account	EA	1
Age 64+	C64+	2
Cancelled Trade	CT	3
Cancelled and Replaced Trade	CRT	4
Retirement Account	RET	5
Trade associated with an Annuity	ANNU	6

Criteria for "Requires More Analysis"

If a trade is associated with one or more specific attributes (depending on your site's business needs and configured during deployment) that can require that you review the details of a trade, the system will force you to navigate to the Trade Details pop-up window for that trade before you can save an R or an RF action on the trade. As a system default, Alert Management flags trades for which the last action was **Cancelled** as *Requires more analysis.*

Jump to page

The Jump to page feature allows you to switch to any particular page by specifying the page number in the text box. For example, if a list is divided in 10 pages and the user directly wants to navigate to page # 5, then the user can write 5 in the text box provided and press Enter. The user is navigated directly to page # 5.

Number of Rows

The Number of Rows feature allows you to select the number of rows that you want to view under the Trade Blotter List grid.

For example, if a list is displaying 50 rows and the user wants to view only 10 rows, then the user can write 10 in the text box provided and press Enter. Then the system displays 10 number of rows.

Trade Details Pop-up window

The Trade Details pop-up window allows you to view additional details about a trade, such as, account details associated with the trade, customer details associated with the trade, alerts associated with the trade, and so on. Double-clicking on a trade row of any one of the Trade Blotter List section displays the Trade Details pop-up window specifically for that trade.

The Trade Details pop-up window displays all the sections configured for display for this particular trade in the expanded format. Refer to Appendix I, "Trade Blotter List Component Matrix", for information on the fields that will display on the Trade Details pop-up window by user interface section and product category.

Components of the Trade Details Pop-up window

Depending on the data associated with a particular trade, the Trade Details pop-up window displays one or more of the following areas of information:

Figure 51. Trade Details Pop-up window

- Trade Review Action History

- Associated Alert List

- Trade

- Customer

- Account

- Representative

- IA

- Trader

- Order

- Security Rating

Refer to Appendix I, "Trade Blotter List Component Matrix", for a detailed table with all possible fields that can display on the Trade Details pop-up window by user interface section and product category. These sections are summarized here.

Trade Review Action History

The Trade Review Action History section allows you to view the various actions and modifications that are saved on the selected trade during the trade review process.

Following are the columns displayed under the Trade Review Action History section:

Associated Alert List

Table 36. Trade Review Action History

Fields	Description
Action	This field displays the action performed on the trade.
Date and Time	This field displays the date and time of the action performed.
By	This field displays the user ID of the user who performed the action.
User Display Name	This field displays the user name of the user who performed the action
Resulting Status	This field displays the status resulting from the action.
Comments	This field displays the comments and attachments that were added.

An alert is considered to be associated with a trade if the alert was created within the same batch in which the trade was ingested and the trade is recorded as a matched record on the alert.

The following columns are displayed under the Associated Alert List section:

Table 37. Associated Alert List

Fields	Description
Score	This field displays the score associated with the trade.
Focus	This field displays the focus type associated with the trade.
Scenario	This field displays the scenario associated with the trade.

Table 37. Associated Alert List

Fields	Description
Created	This field displays the date when the alert was created.
Status	This field displays the status of the alert created.
ID	This field displays the alert ID associated with the trade.

For each alert in the Associated Alert List section, a hyperlinked alert ID displays, which when clicked, displays the Alert History Details page for that alert.

An alert will display in this section only if you have appropriate access permissions to view that alert.

Trade

The Trade section displays detailed information about the trade you selected on the Trade Blotter List section.

Following are the columns displayed under the Trade section:

Table 38. Trade

Fields	Description
Trade ID	This field displays the trade identifier for the trade.
Trade Date	This field displays date on which the trade was executed.
Desk ID	This field displays the identifier of the desk that performed the trade.
Subdesk ID	This field displays the identifier of the sub-desk that performed the trade.
Executing Organization IDs	This field displays the identifier of the organization within which this trade execution was performed.
Security Short Name	This field displays the short name of the security that was traded.
Security ID	This field displays the identifier of the security that was traded.
Security Description	This field displays the description of the security that was traded.
Product Category	This field displays the product category designation for the security associated with this trade.
Product Type	This field displays the product type designation for the security associated with this trade.
Product Subtype	This field displays the product sub type designation for the security associated with this trade.
Trade Purpose	This field displays the purpose for which this trade was executed.
Trader Buy/Sell	This field indicates whether the trader is buying or selling the security.
Quantity	This field displays the total number of units of the security.
Price (Base)	This field displays the price at which the security was traded (buy or sell) as expressed in base currency.
Price (Issuing)	This field displays the price at which the security was traded (buy or sell) as expressed in the issuing currency.
Price (Traded)	This field displays the last activity price for the trade.

Table 38. Trade

Fields	Description
Price (Settlement	This field displays the trade price expressed in the currency in which the trade is to be settled.
Commission (Issuing)	This field displays the monetary amount of the broker commission associated with this trade, expressed in the issuing currency.
Principal (Issuing)	This field displays the monetary amount of the broker commission associated with this trade, expressed in the issuing currency.
Gross Amount	This field displays the principal amount of the trade expressed in the issuing currency plus the commission associated with the trade expressed in the issuing currency.
Settlement Date	This field displays the date on which the trade is to settle.
Agent ID	This field displays the identifier of the trader who acted as the agent on the execution (for agency trades).
Solicited	This field displays the indicator of whether a person affiliated with the Oracle client solicited this order.
Event Type	This field displays the trade event type associated with the trade.
ISIN	This field displays the International Securities Identification Number (ISIN) associated with the security that was traded.
Load	This field displays the type of load for this mutual funds security.
Load/Fee	This field displays the mutual fund load fee amount in this issuing currency.
NAV	This field displays the closing price, in the issuing currency, for this security in its primary market on this market date.
CSDC (Issuing)	This field displays the Contingent Deferred Sales Charge amount in the issuing currency.
Customer Buy/Sell	This field displays whether the customer is buying or selling as part of the trade.
Last Reviewed By	This field displays the user who approved or rejected the trade (via Trade Blotter).
Organization Name/ID	This field displays the display name or identifier (configured at deployment) of the organization that originated the trade.

Customer

The Customer section displays details related to the customer associated with the selected trade.

Following are the columns displayed under the Customer section:

Table 39. Customer

Fields	Description
Customer Name	This field displays the name of the customer who placed the order.
Customer ID	This field displays the customer identifier associated with the account involved in the trade.
Tax ID	This field displays the customer's tax identification number.
Type	This field displays the indicator of whether this customer is an individual or organization.
Business Type	This field displays the functional area in which this customer does business.
Date of Birth	This field displays the date on which the customer was born.
Legal Structure	This field displays the Oracle client's legal entity that is the principal in this structured deal.
Broker/Dealer	This field displays the indicator of whether this customer has provided notification of employment by a financial institution.
Effective	This field displays the date on which an investment rating service established this investment rating for the security associated with the trade.
Effective Match	This field displays the level of risk associated with this customer as determined in large part by membership on one or more Watch Lists plus text of the identifier or name associated with the Watch List record that was used to populate Watch List Risk for this customer.
Business Risk	This field displays the level of risk associated with the general business characteristics of this customer as determined by the Oracle client.
List	This field displays the identifier of the level of risk associated with a customer determined by membership on one or more watch lists..
Annual Income	This field displays the customer's self-reported annual income, expressed in base currency.
Employee	This field displays the indicator of whether the customer is also an Oracle client.
Estimated Liquid Networth	This field displays the customer's self-reported liquid assets, expressed in base currency.
Source of Wealth	This field displays the customer's self-reported source of wealth.
Marital Status	This field displays the marital status of the customer.
Occupation	This field displays the occupation of the customer.
Employer	This field displays the name of the customer's employer.
Credit Rating	This field displays the rating for this customer, based on credit rating score.
Credit Score	This field displays the actual score for the customer's credit rating, based on the credit rating score.

Table 39. Customer

Fields	Description
Credit Rating Source	This field displays the source associated with the credit rating assigned to the customer.
Citizenship	This field displays the customer's primary country of citizenship.

Account

The Account section displays details related to the customer's account associated with the selected trade.

Following are the columns displayed under the Account section:

Table 40. Account

Fields	Description
Account Name	This field displays the account display name of the account associated with the trade.
Account ID	This field displays Identifier of the customer's account involved in the trade, as last reflected in the events for the execution.
Account type	This field displays the Oracle client-specified account type classification for the use of this account.
Source of Funds	This field displays the source from which the initial funds will come as stated by the customer for the account associated with the trade.
Registration	This field displays the Registration Type.
Open Date	This field displays the date on which the account associated with the trade was opened.
Last Activity	This field displays the date of the last trading or transaction activity in the account that is associated with the trade.
Business Unit	This field displays the the identifier for the organization that owns the account, for firm accounts.
Branch	This field displays the Branch Code organization where the account is domiciled.
Tax ID	This field displays the tax identification number associated with the account that is associated with the trade
Risk Tolerance	This field displays the degree of risk the customer is willing to take with investments in this account (that is, the customer's ability to handle declines in the net worth of this account).

Representative

The Representative section displays detailed information about the registered representative associated with the selected trade.

Following are the columns displayed under the Representative section:

Table 41. Representative

Fields	Description
Primary Representative ID	This field displays the primary representative identifier that is used by this employee.
Employee Name	This field displays the name to be displayed for this employee.
Primary Service Team ID	This field displays the identifier of the primary service team of which this employee is a member.
CRD#	This field displays the the unique identifier that the authoritative regulator assigned to this employee, for employees who must be registered with a regulator.
Employee ID	This field displays the identifier for an employee that is unique across the enterprise.
Title	This field displays the job title for this employee.
Role	This field identifies their employment role or title.
Employee Type	This field displays the code that identifies the type of employee.
Part Time/Full Time	This field is an indicator of whether this employee is part time or full time.
Supervisor Name	This field displays the name to be displayed for this employee's supervisor.
Supervisory Organization ID	This field displays the identifier of the organization that is responsible for monitoring the activities of this employee.
Supervisory Organization Name	This field displays the name of the organization that is responsible for monitoring the activities of this employee.
Line Organization ID	This field displays the identifier of the primary line organization to which this employee is assigned.
Line Organization Name	This field displays the name of the primary line organization to which this employee is assigned.
Company	This field displays the name of the company for which this employee or contractor works.
Cost Center	This field displays the cost center to which this employee is assigned.
Office	This field displays the identifier of the office to which this employee is assigned.
Office Location	This field displays the text that describes this employee's work location
Tax ID	This field displays the employee's tax identification number.
Tax ID Format	This field displays the indicator of whether the employee tax identifier is a Social Security Number (SSN) or another type of identifier.
Hire Date	This field displays the date this employee was hired.
Employee Status	This field displays the employment status of this employee. For example, active or inactive.
Employee Status Date	This field displays the date that this employee's status was last changed.

IA

The IA section displays detailed information about the investment advisor associated with the order that is associated with the selected trade.

Following are the columns displayed under the IA section:

Table 42. IA

Fields	Description
Employee Name	This field displays the name to be displayed for this employee.
Employee ID	This field displays the identifier for an employee.
Tax ID	This field displays the the employee's tax identification number.
Tax ID Format	This field displays the Indicator of whether the employee tax identifier is a Social Security Number (SSN) or another type of identifier.
IA Firm ID	This field displays the identifier for an employee that is unique across the enterprise.
IA Firm Name	This field displays the Investment Advisor firm name.
# of Sub-Accounts	This field displays the number of active sub-accounts that this investment advisor manages.
AUM	This field displays the total net worth of all active sub-accounts that this investment advisor manages, expressed in base currency.

Trader

The Trader section displays details related to the trader who executed the selected trade.

Following are the columns displayed under the Trader grid:

Table 43. Trader

Fields	Description
Employee	This field displays the name to be displayed for this employee.
CRD#	This field displays the the unique identifier that the authoritative regulator assigned to this employee, for employees who must be registered with a regulator.
Employee ID	This field displays the identifier for an employee that is unique across the enterprise.
Title	This field displays the job title for this employee.
Role	This field identifies their employment role or title.
Supervisor Name	This field displays the name to be displayed for this employee's supervisor.
Line Organization ID	This field displays the identifier of the primary line organization to which this employee is assigned.
Line Organization Name	This field displays the name of the primary line organization to which this employee is assigned.

Table 43. Trader

Fields	Description
Company	This field displays the name of the company for which this employee or contractor works.
Cost Center	This field displays the cost center to which this employee is assigned.
Office	This field displays the identifier of the office to which this employee is assigned.
Office Location	This field displays the text that describes this employee's work location
Employee Status	This field displays the Employment status of this employee. For example, active or inactive.
Employee Status Date	This field displays the date that this employee's status was last changed.

Order

The Order section displays details related to the order associated with the selected trade.

Following are the columns displayed under the Order grid:

Table 44. Trader

Fields	Description
Order ID	This field displays the identifier of the order associated with the trade.
Order Placed	This field displays the date and time on which the order was placed.
First Routed	This field displays the date and time on which the order was first routed.
Order Filled	This field displays the date and time on which the order was completely filled.
Order Buy/Sell	This field is an indicator of whether an order is an instruction to buy or sell a security.
Originating Order Quantity	This field displays the Original number of units of the security (For example, shares, contracts or face value) that were to be bought or sold through this order.
Last Order Type	This field displays the type of this order.
Limit Price	This field displays the price at which this limit order is to be executed, as expressed in issuing currency.
Security Short Name	This field displays the short name of the security that was traded.
Buyer/Seller	This field displays the indicator for the type of buyer/seller for which the order was placed and the buyer/seller associated with the order.
Parent Order ID	This field displays the Identifier that the Oracle client assigns which uniquely identifies this order throughout the enterprise during the day in which it was performed.

Security Rating

The Security Rating section displays detailed information about the investment rating service for the security associated with the selected trade.

Following are the columns displayed under the Security Rating grid:

Table 45. Security Rating

Fields	Description
Source	This field displays the investment rating service that is the source of the investment rating for the security associated with the trade.
Rating	This field displays the specific investment rating value determined by an investment rating service for the security that was traded.
Effective	This field displays the date on which an investment rating service established this investment rating for the security associated with the trade.
Expires	This field displays the date on which an investment rating service removed this investment rating for the security associated with the trade.

Viewing and Changing the Status of a Trade

You can view or modify the status of a trade only if you have access permissions to do so.

You must have access to view and modify the status of trades on the Trade Blotter page: New - Unreviewed, Reviewed, and Reviewed w/Follow-Up.

Note: User must select trades with the same review status while taking actions, on more than one trade. If the user tries to select different statuses, the following message is displayed: Y*ou have selected trades with different statuses. To take an action, only select trades with the same status.*

To view or modify the status of one or more trades currently in the New - Unreviewed status, follow these steps:

1. Ensure that the trade is in New - Unreviewed status and perform one of the following:

   To view trade details, follow these steps:

   a. Double-click the row of the trade you want to view.

      The Trade Details pop-up window for that trade displays.

   b. When you are finished viewing that trade, close the pop-up window and go on to the next trade you want to view.

   To change the status of one or more trades to Reviewed, follow these steps:

   a. Select the check box on the row of the trade or trades for which you want to change the status to **Reviewed**.

   b. Click **Actions**.

   c. The Review Actions pop-up window displays. If you are viewing only one Trade ID, the Trade ID field is pre-populated. If you are viewing multiple Trade IDs, the number of Trade IDs you are viewing displays in the field.

   d. Select Reviewed from the **Select an Action** drop-down list.

e. Select a standard comments from the **Standard Comments** drop-down list.

   Optional: Enter any custom comments, if applicable in the text fields.

f. Click **Save**.

   The Trade Blotter List grid refreshes the list, changing the trades to the Reviewed status..

To change the status of one or more trades to Reviewed with Follow-Up, follow these steps:

a. Select the check box on the row of the trade or trades for which you want to change the status to **Reviewed w/Follow-Up**.

b. Click **Actions**.

c. The Review Actions pop-up window displays. If you are saving only one Trade ID, the Trade ID field is pre-populated. If you are saving multiple Trade IDs, the number of Trade IDs you are viewing displays in the field.

d. Select Reviewed with Follow-Up from the **Select an Action** drop-down list.

e. Select a standard comments from the **Standard Comments** drop-down list.

   Optional: Enter any custom comments, if applicable in the text fields.

f. Click **Save**.

   The Trade Blotter List grid refreshes the list, changing the trades to the Reviewed w/Follow-Up status.

To view one or more trades currently in the Reviewed status or to modify the status of one or more trades from Reviewed to Reviewed w/Follow-Up, follow these steps:

1. Ensure that the trade is in Reviewed status and perform one of the following:

   To view trade details, follow these steps:

   a. Double-click on the row of the trade you want to view.

      The Trade Details pop-up window for that trade displays.

   b. When you are finished viewing that trade, close the pop-up window and go on to the next trade you want to view.

   To change the status of one or more trades, go to Step 2.

2. Select the check box on the row of the trade or trades for which you want to change the status to **Reviewed w/Follow-Up**.

3. Click **Actions**.
   The Review Actions pop-up window displays. If you are viewing only one Trade ID, the Trade ID field is pre-populated. If you are viewing multiple Trade IDs, the number of Trade IDs you are viewing displays in the field.

4. Select Reviewed w/Follow-Up from the **Select an Action** drop-down list.

5. Select a standard comments from the **Standard Comments** drop-down list.

   Optional: Enter any custom comments, if applicable in the text fields.

6. Click **Save**.

   The Trade Blotter List grid refreshes the list, changing the trades to the Reviewed w/Follow-Up status.

To view one or more trades currently in the Reviewed w/Follow-Up status or to modify the status of one or more trades from Reviewed w/Follow-Up to Reviewed status, follow these steps:

1. Ensure that the trade is in Reviewed w/Follow-Up status and perform one of the following:

   ● To view trade details:

   a. Double-click on the row of the trade you want to view.

      The Trade Details pop-up window for that trade displays.

   b. When you are finished viewing that trade, close the pop-up window and go on to the next trade you want to view.

   ● To change the status of one or more trades to Reviewed:

   a. Select the check box on the row of the trade or trades for which you want to change the status to **Reviewed**.

   b. Click **Actions**.

   c. The Review Actions pop-up window displays. If you are viewing only one Trade ID, the Trade ID field is pre-populated. If you are viewing multiple Trade IDs, the number of Trade IDs you are viewing displays in the field.

   d. Select Reviewed w/Follow-Up from the **Select an Action** drop-down list.

   e. Select a standard comments from the **Standard Comments** drop-down list.

      Optional: Enter any custom comments, if applicable in the text fields.

   f. Click **Save**.

      The Trade Blotter List grid refreshes the list, changing the trades that you have marked as Reviewed to the Reviewed status.

Locking and Unlocking a Trade

Alert Management controls access to trades via a locking mechanism in order to prevent inconsistent results caused by more than one user at a time trying to take an action on the same trade or trades. The system locks unlocked trades for you when you select one or more check boxes of one or more trades. In addition, the system locks a trade when you click on the **Comments**, **email,** or **Attachments** icon of an individual trade and then taking an action. The system maintains the lock on a particular trade if you take additional actions on that trade until you save or deselect all the actions on that trade.

To unlock a trade, deselect the selected check boxes. If no check boxes are selected, the Comments, email or Attachments actions remove the lock automatically when saved or cancelled.

Note: If you try to select a trade that is locked by another user, the system displays a Selected Trade Locked dialog box with an error message.

When you click **OK**, the system closes the dialog box and returns you to the original tab on the List page.

Adding Comments on a Trade

If you have the appropriate access permissions, you can add comments to selected trades on the Trade Blotter page. When you save comments to a trade, the status of that trade does not change as a result of those comments. However, the comment action is added to the Comment Audit History matrix.

You can add a free-text comment to more than one trade, add one or more standard comments to those trades, and view the comment audit history for those trades.

Note: User must select trades with the same review status while taking actions, on more than one trade. If the user tries to select different statuses, the following message is displayed: You have selected trades with different statuses. To take an action, only select trades with the same status.

Figure 52. Global Comments pop-up window

To add global comments to more than one trade, follow these steps:

1. On the Trade Blotter page, perform one of the following depending on whether you want to add comments on more than one trade but not the whole page of trades, or add global comments to the whole page of trades:

   - For comments on more than one trade, select the check boxes adjacent to the trades and click **Comments**.

   - For comments on the entire page of trades, click on the check box on list header and click **Comments**.

2. In the Global Comments pop-up window, follow these steps:

   a. Select one or more applicable standard comments from the **Select a standard comment** drop-down list.

   b. Type free-text comments in the **Comments** text area.

3. Click **Save**.

   A confirmation message displays.

Adding an Attachment to a Trade

You can add one or more attachments to an individual trade, remove one or more attachments from an individual trade, and view the attachment action history for that trade.

Figure 53. Add Attachment pop-up window

To add one or more attachments to a trade, follow these steps:

1. On the Trade Blotter List section, select the check box adjacent to the trade to which you want to add an attachment.

   The Add Attachments pop-up window displays.

2. In the Add Attachments pop-up window, enter file name in the **Logical File Name** text field.

3. Browse for the file you want to add via the **Choose a file** field.

4. When the Choose File to Upload dialog appears, select the file you want to attach to the trade and click **Open**.

5. Click **Attach File**.

   The display name of the file appears in the Attachments Action History list.

6. If you want to add another attachment to this trade, repeat Steps 1 through 4.When you are sure of the file or files you want to attach to this trade, click **Save**.

   The pop-up window returns you to the Trade Blotter page and adds the attachments to the Attachments Action History section.

   If you do not want to save the trade with the attachments you added, click **Cancel**. The system returns you to the Trade Blotter page and your attachments are not added to the Attachments Action History.

Exporting Trades to Excel

You can export trades from the Trade Blotter List section to a Microsoft Excel format where you can then review and edit the data as necessary.
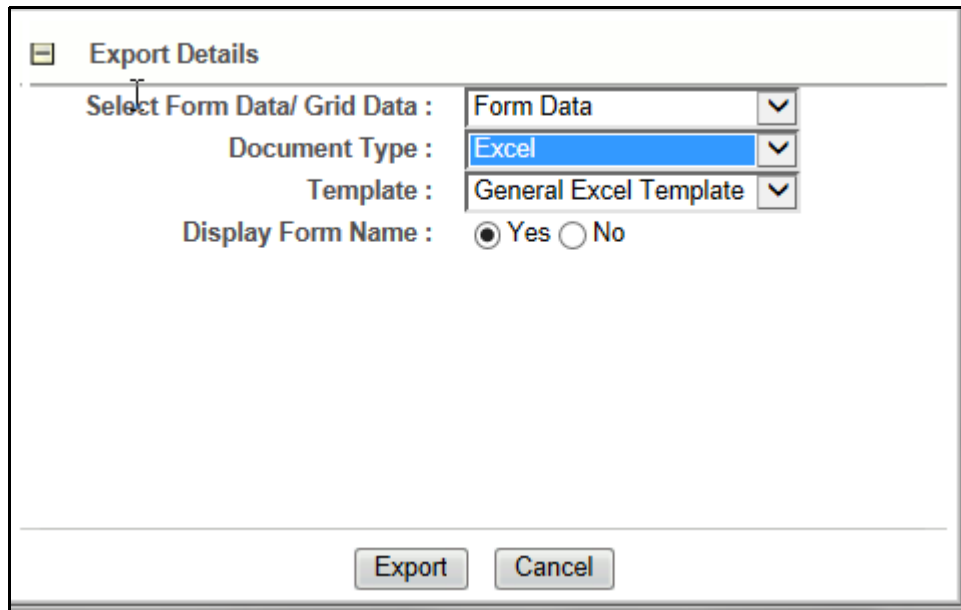
Figure 54. Export pop-up window

Note: Oracle does not currently support exporting grid data to formats other than Excel. The Excel functionality works successfully on MS Excel 2003 and MS Excel 2007.

Sending an email on a Trade

If you have the appropriate access permissions, you can send an email and request a response regarding a particular trade.

The system does not automatically include any information on the trade. You can enter any trade details in the body of the email message.

Figure 55. Trade Blotter Send email pop-up window

To send an email regarding a particular trade, follow these steps:

1. From the Trade List, click the check box associated with the particular trade or trades you want to discuss. The Send email pop-up window displays.
   If you are sending an email regarding only one trade, the Trade ID displays in the Selected Trades field. If you are sending an email regarding multiple trades, the number of trades you are viewing displays in the field.

2. Enter the email recipient's email address in the **To**: field.

3. Provide an appropriate subject in the **Subject** field.

4. Select the **Request Response** check box if you want a response. If not, go to Step 5.

   If you select Request Response, the system attaches a response form in which the recipient can enter comments. When the recipient has finished entering comments and clicks **Send Comments,** the response is automatically returned to you.

5. Type your message in the **Body** field.

6. Click **Save** to send the message.

   The system sends your message and records information about it in the email Action History list.

CHAPTER 8   *Managing Controlling Customers*

The Manage Controlling Customer feature provides a way to search customer relationships based on user-specified search parameters. It also enables you to view existing or historical data, update certain components of the controlling customer, and delete existing controlling customers. This feature enables you to establish new controlling customers.

This chapter focuses on the following topics:

- About Controlling Customers

- Key Features

- User Roles and Actions

- Controlling Customer Workflow

- Accessing Controlling Customer page

- Adding Controlling Customer

- Updating Controlling Customer

- Commenting Controlling Customer

- Removing Controlling Customer

About Controlling Customers

A Controlling Customer is in a controlling position in a company represented by a specific security. A customer can have a controlling position in more than one security. Controlling customer relationships are considered by some Oracle Financial Services behavior detection scenarios during alert generation. The controlling customer information flows into Oracle Financial Services Enterprise Alert Management and be used for behavior detection through one of two ways. A client can choose to provide information regarding controlling customer relationships during the batch process of loading data from files (for more information on Controlling Customer Data Files, see *Data Interface Specification*, for more information on Controlling Customer data files). Or, a client can choose to add and maintain controlling customer relationships via the Manage Controlling Customer interface provided in the Monitoring workflow as described in this chapter.

Key Features

The Alert Management UI allows you to perform the following actions:

- Search the existing conditions on controlling customers trading.

- Provide relevant information on the conditions related to controlling customers trading.

- Add new controlling customers.

- Update and comment existing controlling customers.

- Remove controlling customers from the list.

User Roles and Actions

This section describes various user roles and actions they can perform in the Controlling Customer workflow.

The following table details the user roles and actions in the Controlling Customer workflow:

User Actions	User Roles									
Privileges	**Analyst I**	**Analyst II**	**Analyst III**	**Supervisor**	**Executive**	**Internal Auditor**	**External Auditor**	**Data Miner**	**AM Administrator**	**WLM Supervisor**
View Search and List page of Controlling Customer	X	X	X	X	X	X				
Update Controlling Customer (Add, Edit, and Add Comment)			X	X						
Remove Controlling Customer			X	X						

Controlling Customer Workflow

The following figure shows the Controlling Customer workflow.
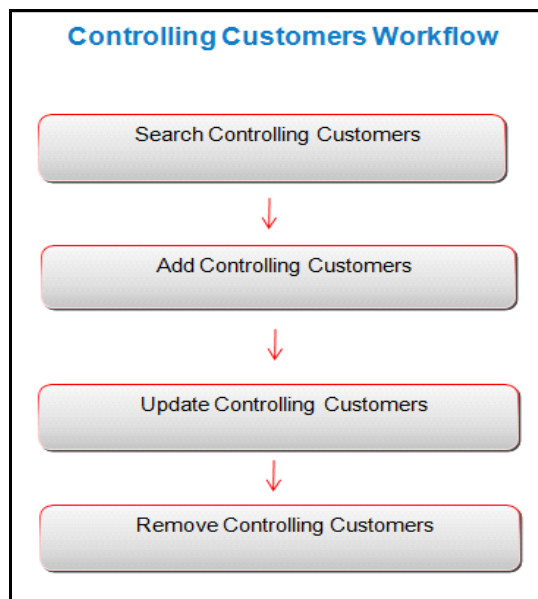
Figure 56. Controlling Customer Workflow

The following table describes the Controlling Customer workflow.

Table 46. Controlling Customer Workflow Table

Action	Description	Roles
Searching Controlling Customers	Users can search existing controlling customers using search criteria such as Customer ID, Security ID, and so on.	Analysts I, II, III, and Supervisors
Adding Controlling Customer	Users can add new controlling customers and enables them to set conditions related to the controlling customers trading.	Analysts III and Supervisors
Updating Controlling Customer	Users can modify existing controlling customers by providing appropriate comments.	Analysts III and Supervisors
Removing Controlling Customer	Users can remove existing controlling customers by providing appropriate comments.	Analysts III and Supervisors

Accessing Controlling Customer page

This section explains how to access the Controlling Customer page. The page is available only to those users who require entering the data related to adding controlling customers through the Oracle Financial Services Alert Management UI.

To access the Controlling Customer page, follow these steps:

1. Navigate to the OFSAA Applications home page. For more information, see *Chapter 3, Getting Started*.

2. Click **Administration** in the RHS menu.

3. Hover over the **List Management** menu and click **Manage Controlling Customer**. The Manage Controlling Customer Search page is displayed.

Searching Controlling Customers

The Controlling Customer Search bar enables you to search for a selected list of controlling customers based on the criteria that you have selected within this search bar.

To search controlling customers, follow these steps:

1. Navigate to the Manage Controlling Customer Search page.

2. Enter the following information.

Table 47. Controlling Customer Search Components

Criteria	Description
Customer ID	Enter the Customer ID of the business entity. If you search by Customer ID then Customer Name field is disabled.
Customer Name	Enter the Customer Name of the business entity. If you search by Customer Name then Customer ID field is disabled. You can also search using the wildcard entries in the text field. **Note:** This search is mutually exclusive.

Table 47. Controlling Customer Search Components (Continued)

Criteria	Description
Security ID	Enter the Security ID of the business entity. If you search by Security ID then Security Name field is disabled.
Security Name	Enter the Security Name of the business entity. If you search by Security Name then Security ID field is disabled. You can also search using the wildcard entries in the text field.
Controlling Relationship Type	Enter the Controlling Relationship type. You can also search using the wildcard entries in the text field.
Controlling Record ID	Enter the control ID. **Note**: Search by Controlling ID ignores all other search criteria.

3. Click **Go**. The updated Controlling Customer list page is displayed.

The List page enables you to view the details of the controlling customers' relationships existing in the system and also to update and delete particular relationships, depending on the user access.
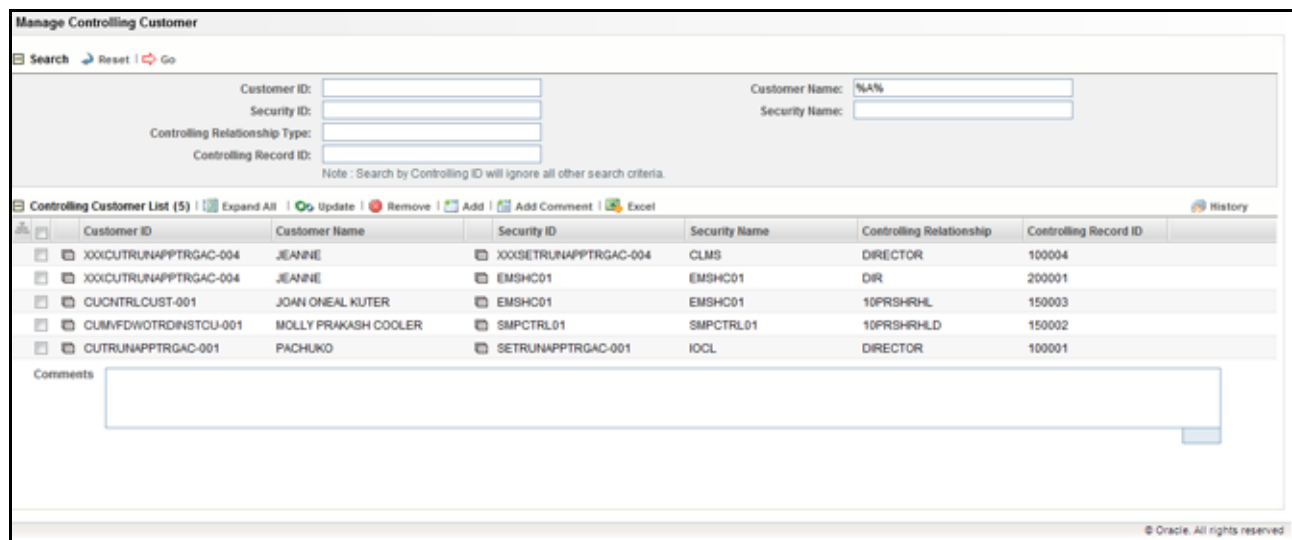
Figure 57. Controlling Customer List page

Adding Controlling Customer

The Add Controlling Customer page enables you to set conditions related to controlling customers trading.
To add controlling customer, follow these steps:

1. Navigate to the Manage Controlling Customer Search and List page.

2. Click **Add**. The Add Manage Controlling Customer dialog box is displayed.

3. **Add Controlling Customer page**Enter the following information in the respective fields.

Table 48. Add Controlling Customer

Field	Description
Customer ID	Enter the unique customer identification. Multiple comma separated values are not allowed. If the Customer ID is not available in the system, the following message is displayed: *Entered Customer ID value does not exist. Please check and enter again.*
Security ID	Enter unique security identification. Multiple comma separated values are not allowed. If the Security ID is not available in the system, the following message is displayed: *Entered Security ID value does not exist. Please check and enter again.*
Controlling Relationship Type	Enter the controlling relationship type.
Comments	Enter the appropriate comments for adding a new controlling customer. The Comments text box has no character restrictions and has scroll which bars can be used for text that exceeds the visible space provided.

4. Click **Save**. The following message is displayed: *You have successfully added the following customer Record ID to controlling customer.*

5. Click **OK**. The new Controlling Customer record is added.

Updating Controlling Customer

This section enables you to modify the customers records imposed on the securities.

To update controlling customer, follow these steps:

1. Navigate to the Manage Controlling Customer Search and List page.
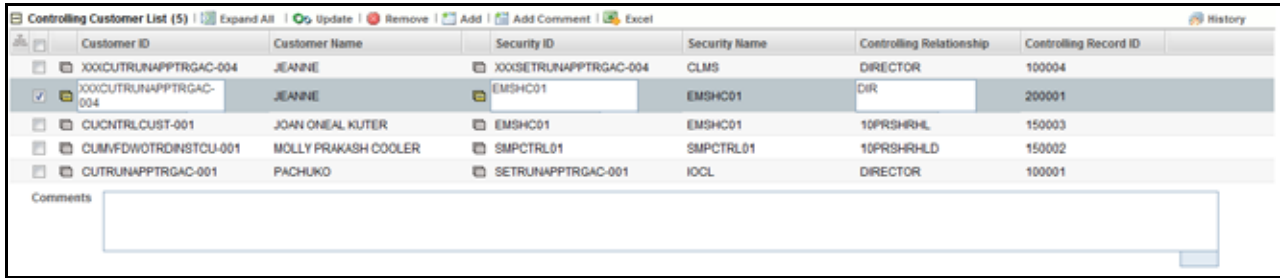
Figure 58. Controlling Customer Update page

2. Select one or more check boxes against the Customer IDs in the list. The selected Customer IDs are enabled for modification.

3. Modify the necessary changes. For more information on the fields, see *Table 36*.

4. Click **Update**. The following message is displayed: *You have successfully updated Controlling Record ID*.

   Note: In the Update Controlling Customer section, if you modify one or more Customers IDs, and either the security does not exist within the available Customers Master table or you do not have access to the updated Customers IDs, the page displays an error message. For more information on the error messages, see Controlling Customer Error Messages.

5. Click **OK**. The selected controlling customer records are updated.

Commenting Controlling Customer

This section explains how to add comments to the selected controlling customers.

To add comments to controlling customer, follow these steps:

1. Navigate to the Manage Controlling Customer Search and List page.
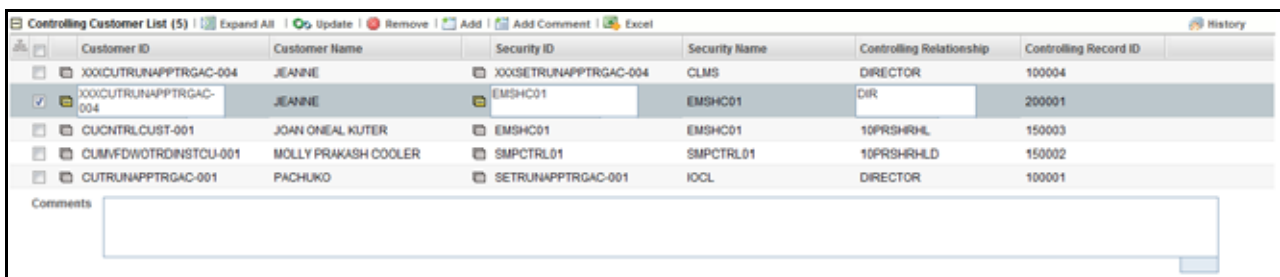
Figure 59. Controlling Customer Update page

2. Select one or more check boxes against the Customer IDs in the list.

3. Enter appropriate comments for the selected Customer IDs.

4. Click **Add Comments**. The following message is displayed: *Records updated with comments.*

5. Click **OK**. The selected controlling customer records are updated with recently added comments.

Removing Controlling Customer

This section describes how to delete the selected customers from the Controlling Customer List section.

To delete customers from the Controlling Customer list, follow these steps:

1. Navigate to the Manage Controlling Customer Search and List page.

Figure 60. Controlling Customer Update page

2. Select one or more check boxes against the Customer IDs in the list.

3. Enter appropriate comments to delete the selected Customer IDs from the list.

   Note: If you do not enter comments before deleting a customer in the list, the following message displays: *You are attempting to delete, but you have not added comment. Please add comments.*

4. Click **Remove**. The following message is displayed: *1 record(s) are going to be deleted from the list. To confirm deletion select OK. Select Cancel to cancel deletion and return to the list page.*

5. Click **OK**. The selected controlling customer records are removed from the list.

Managing Security Restrictions

This chapter describes the concept and process of managing the Security Restriction workflow of the Alert Management system. It provides systematic instructions to carry out various actions according to the workflow and user roles. This helps you to understand how to use various components to accomplish each task.

This chapter focuses on the following topics:

- About Security Restrictions
- Key Features
- User Roles and Actions
- Security Restrictions Workflow
- Accessing Security Restrictions page
- Searching Security Restrictions
- Adding Security Restrictions
- Updating Security Restrictions
- Adding comments to Security Restrictions
- Removing Security Restrictions

About Security Restrictions

A security restriction sets the conditions related to restrictions on trading specific securities. Oracle Financial Services Alert Management uses this information to generate alerts on suspicious trading behavior involving these restricted securities. The Security Restriction information flows into Oracle Financial Services Alert Management and can be used for behavior detection through one of two ways. A client can choose to provide information regarding security restrictions during the batch process of loading data from files (for more information on Security Restrictions data files, see *Data Interface Specification*). Or, a client can choose to add and maintain security restrictions via the Manage Security Restrictions interface.

The Manage Security Restrictions feature provides a way to search for existing trading restrictions on different securities based on user-specified search parameters. It also enables you to view existing or historical data, update certain components of the restriction, and delete existing restrictions. In addition, it enables you to establish new security trading restriction conditions. Access to the Manage Securities Restriction workflow is dependent on your role.

Key Features

The Alert Management UI allows you to perform the following actions:

- Search the existing conditions on security restrictions trading.

- Provide relevant information on the conditions related to security restrictions trading.

- Add new security restrictions.

- Update and comment existing security restrictions.

- Remove security restrictions from the list.

User Roles and Actions

This section describes various user roles and actions they can perform in the Security Restrictions workflow.

The following table details the user roles and actions in the Security Restrictions workflow:

User Actions	User Roles									
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
View Search and List page of Security Restrictions	X	X	X	X	X	X				
Update Security Restrictions (Add, Edit, and Add Comment)			X	X						
Remove Security Restrictions			X	X						

Security Restrictions Workflow

The following figure shows the Security Restrictions workflow.
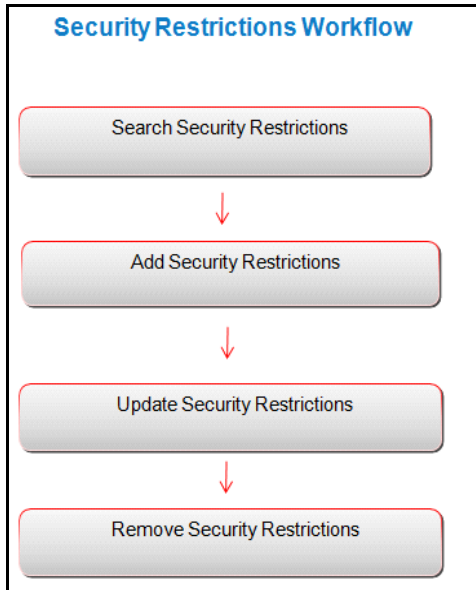
Figure 61. Security Restrictions Workflow

The following table describes the Security Restrictions workflow.

Table 49. Security Restrictions Workflow Table

Action	Description	Roles
Searching Security Restrictions	Users can search existing security restrictions using search criteria such as Security ID, Restriction Type, and so on.	Analysts I, II, III, and Supervisors
Adding Security Restrictions	Users can add new security restrictions and enables them to set conditions related to the security restrictions trading.	Analysts III and Supervisors
Updating Security Restrictions	Users can modify existing security restrictions by providing appropriate comments.	Analysts III and Supervisors
Removing Security Restrictions	Users can remove existing security restrictions by providing appropriate comments.	Analysts III and Supervisors

Accessing Security Restrictions page

This section explains how to access the Security Restrictions page. This page is available only to users who require entering the data related to adding security restrictions through the Oracle Financial Services Alert Management UI.

Note: The Security Restriction data can flow either through DIS files or be entered manually on the Oracle Financial Services Alert Management UI, but not both.

To access the Security Restrictions page, follow these steps:

1. Navigate to the OFSAA Applications home page. For more information, see *Chapter 3, Getting Started.*

2. Click **Administration** in the RHS menu.

3. Hover over the **List Management** menu and click **Manage Security Restrictions**. The Manage Security Restrictions Search page is displayed.

Searching Security Restrictions

The Security Restriction Search page enables you to search trading restrictions on different securities based on the search criteria. If a search is performed with blank values in a search field, an error message displays.

To search security restrictions, follow these steps:

1. Navigate to the Manage Security Restriction Search page.

2. Enter the following information.

Table 50. Security Restriction Search Components

Criteria	Description
Security ID	Enter the security ID of the business entity. If you search by Security ID then the Security Name field is disabled.
Security Name	Enter the security name of the business entity. If you search by Security Name then the Security ID field is disabled. You can also search using the wild card entries in the text field.
Restriction Type	Select the restriction types from the Restriction Type drop-down list. For example, Threshold, Short term, and so on.
Restriction List	Select the restriction list types from the Restriction List drop-down list.
Restriction List ID	Select the restriction list IDs from the Restriction List ID drop-down list.
Effective Date 'From' and 'To'	Select the effective start and end date from the Calender Control. 24. **Note:** The *From* date must be less than the *To* date.
Expiry Date 'From' and 'To'	Select the expiration start and end date from the Calender Control. **Note:** The *From* date must be less than the *To* date.
Trading Activity	Select trading activities from the Trading Activity drop-down list (for example, Buy, Sell, and combined).
Restriction Quantity >=	Enter the restriction quantity value greater than or equal to. The restriction quantity value should be a positive numeric value.
Search By Restriction Record ID	Enter the restriction record ID. To search for multiple IDs, you must enter the IDs individually and separated by commas. **Note:** Search by Restriction Record ID ignores all other search criteria.

3. Click **Go**. The updated Security Restriction list page is displayed.

The Security Restriction List page displays information regarding the applicable restrictions on trading of securities. The List page enables you to view the details of the security restrictions existing in the system and also to update, add, and delete a security restriction, depending on the user access.

Figure 62. Security Restriction List page

Adding Security Restrictions

The Add Securities Restriction page enables you to set the conditions related to restriction on trading of securities manually.

To add security restriction, follow these steps:

1. Navigate to the Manage Security Restriction Search and List page.

2. Click **Add**. The Add Manage Security Restriction dialog box is displayed.

Figure 63. Add Security Restriction page

3. Enter the following information in the respective fields.

Table 51. Add Securities Restriction Fields

Field	Description
Security ID	Enter security ID. Multiple comma separated values are not allowed.
Restriction Type	Select a restriction type from the Restriction Type drop-down list. For example, Short term, Threshold, and so on.
Restriction List	Select a restriction list from the Restriction List drop-down list.
Trading Activity	Select a trading activity from the Trading Activity drop-down list. For example, Buy, Sell, and Combined.
Effective Date	Enter the effective date or select date from the calender control.
Expiry Date	Enter the expiration date or select date from the calender control.
Restriction Quantity >=	Enter a positive number. ?
Comment	Enter comments while creating new security restriction. The Comments text box has no character restrictions and scroll bars can be used for text that exceeds the visible space provided.

Note: Trading activity and the Effective date are mandatory.

4. Click **Save**. The following message is displayed: *You have successfully added the following Restriction Record ID to Security Restrictions.*

5. Click **OK**. The new Security Restriction is added to the list.

Updating Security Restrictions

This section enables you to modify the conditions related to restriction on trading of securities.

To update security restriction, follow these steps:

1. Navigate to the Manage Security Restriction Search and List page.

Figure 64. Security Restriction Update page

2. Select one or more check boxes against the Security IDs in the list. The selected Security IDs are enabled for modification.

3. Modify the necessary changes. For more information on the fields, see *Table 51*.

4. Click **Update**. The following message is displayed: *You have successfully updated Security Record ID.*

   Note: In the Update Securities Restriction area, if you modify one or more Security IDs, and either the security does not exist within the available Security master table or you do not have access to the updated Security IDs, the page displays an error message. For more information on error messages, see *Security Restriction Error Messages*.

5. Click **OK**. The selected security restriction records are updated.

Adding comments to Security Restrictions

This section explains how to add comments to the selected security restriction.

To add comments to security restriction, follow these steps:

1. Navigate to the Manage Security Restriction Search and List page.

Figure 65. Security Restriction Comment page

2. Select one or more check boxes against the Security IDs in the list.

3. Enter the appropriate comments for the selected Security IDs.

4. Click **Add Comments**. The following message is displayed: *Records updated with comments.*
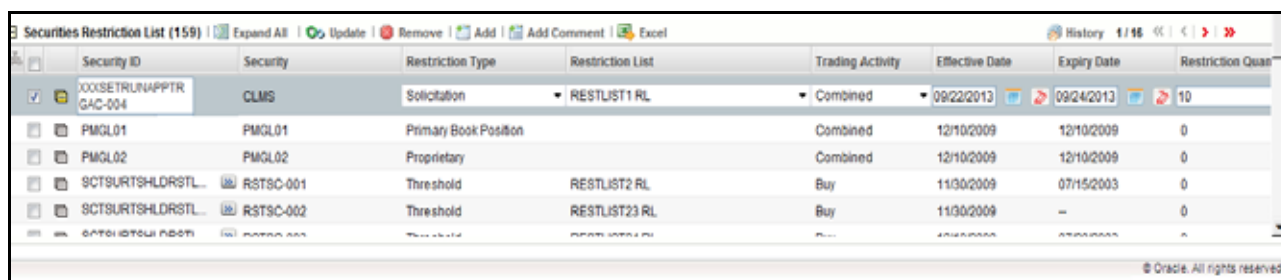
5. Click **OK**. The selected security restrictions records are updated with recently added comments.

Removing Security Restrictions

This section describes how to delete the selected restrictions records imposed on the securities from the Security Restriction List section.

To delete securities from the Security Restriction list, follow these steps:

1. Navigate to the Manage Security Restriction Search and List page.

Figure 66. Security Restriction Comments page

2. Select one or more check boxes against the Security IDs in the list.

3. Enter appropriate comments to delete the selected Security IDs from the list.

   Note: If you do not enter comments before deleting a security in the list, the following message displays: *You are attempting to delete, but you have not added comment. Please add comments.*

4. Click **Remove**. The following message is displayed: *1 record(s) are going to be deleted from the list. To confirm deletion select OK. Select Cancel to cancel deletion and return to the list page.*

5. Click **OK**. The selected security restriction records are removed from the list.

CHAPTER 10 *Researching Business Data*

This chapter describes how to use the Research workflow to search and inquire about a specific focus type and its related information. It also provides step-by-step instructions to create an alert on an entity.

This chapter covers the following topics:

- About Research Business Data
- Key Features
- User Roles and Actions
- Research Workflow
- Searching for an Entity
- Viewing and Researching Entity Details
- Creating an Alert

About Research Business Data

The Research workflow allows you to search for entities of interest. You can use this functionality to research business data or to aid in the research of alerts. The Search page captures your selection criteria related to a type of entity and then performs a search to find the specified entity. You can use the Research Search page to retrieve background and business information about a focus, as well as the related alerts and cases that are generated for that focus.

Key Features

The Alert Management UI allows you to perform the following actions:

- Search for a specific entity
- Analyze and research entity using detailed information
- Create an alert for an entity
- View the Relationships tab, which includes Related Alerts and Related Cases

User Roles and Actions

This section describes various user roles and actions they can perform in the Researching Business Data workflow.

The following table details about user roles and actions in the Researching Business Data workflow.

Table 52. Researching Business Data User Roles and Actions

User Actions	User Roles						
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor
Access to Search and List page		X	X	X	X	X	
View Entity details		X	X	X	X	X	
Create an Alert		X	X	X			

Research Workflow

The following figure shows the Research workflow.
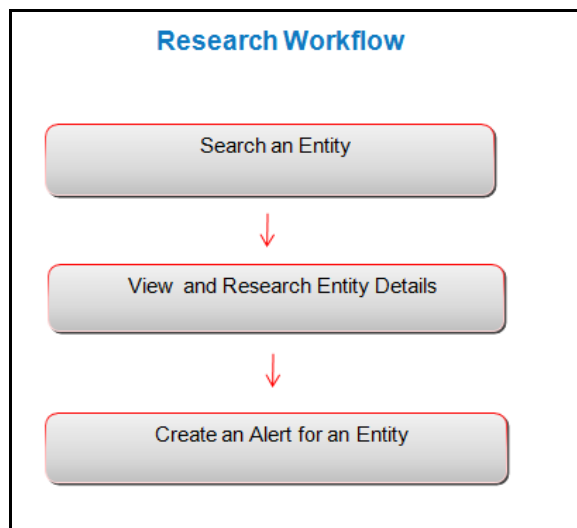
Figure 67. Research Workflow

The following table details about the Research workflow.

Table 53. Research Workflow

Action	Description	Roles
Searching for an Entity	A user can research business data or to aid in the research of a specific alert.	Analysts II, III, and Supervisors
Viewing and Researching Entity Details	A User can view additional information about the entity for in depth research.	Analysts II, III, and Supervisors
Creating an Alert	Based on the research and analysis, a user can create an alert for the selected entity.	Analysts II, III, and Supervisors

Accessing Research Business Data page

This section explains how to access the Research page.

To access the Research page, follow these steps:

1. Navigate to the OFSAA Applications Home page. For more information, see *Chapter 3, Getting Started.*

2. Click **Research** in the RHS menu. The Entity Search page is displayed.

Searching for an Entity

The Entity Search and List page allows you to research business data or to help in the research of a specific alert. This page captures your selection criteria related to a type of entity and then performs a search to find the specified entity.

To search for an entity, follow these steps:

1. Navigate to the Entity Search and List page.

2. Select the **Entity Type** from the drop-down list.

3. Select a scenario class from the **Context** drop-down list to give context for the type of business problem you are researching. The list has the abbreviated scenario class to which you have access.

   Note: The context you select does not restrict the entities displayed in the search results. However, the context does define the Business tabs and data format displayed.

4. Depending on the Entity Type and Context you have selected, additional search criteria are enabled. Enter the pertinent search criteria.

   The following table describes the additional search criteria which are enabled. The filter criteria for your deployment can vary.

   Note:

   - All Name Type fields have wildcard search.

■ All search fields are mutually exclusive unless otherwise noted. You can search for an entity by only one criteria at a time.

Table 54. Additional Search Criteria

Field	Description
ID Type	Select the unique identification number based on the entity type and scenario class selected. **Note:** This field displays only if you select the entity type as Security or External Entity.
Entity ID	Enter the unique identification number of the entity selected in the Entity Type field. **Note:** This field displays only if you select the entity type as Account, Customer, Security, Order, Execution, Employee, Trader, Registered Representative, External Entity, Household, Organization, or Portfolio Manager.
Value	Enter the security name or symbol as per the ID Type selected. This field accepts wildcards. To search using wildcard, use the % symbol. Minimum of two characters are required for wildcard search. **Note:** This field displays only if you select the entity type as Security.
Alternate ID	Enter an alternative unique identification number for this account if you do not have a value for the ID type. **Note:** This field displays only if you select the entity type as Account or Customer.
Entity Name	Enter the name of the entity to be searched if you do not have a value for the ID type or an alternate ID for the account. This field accepts wildcards. To search using wildcard, use the % symbol. Minimum of two characters are required for wildcard search. **Note:** This field displays only if you select the entity type as Account, Customer, Correspondent Bank, Employee, Trader, Registered Representative, External Entity, Organization, or Portfolio Manager.
Tax ID	Enter the tax identification number associated with the account if you do not have a value for the ID type, an alternate ID for the account, or the name of the entity to be searched. **Note:** This field displays only if you select the entity type as Account or Household.
Account ID	Enter the unique identification number of the correspondent bank. **Note:** This field displays only if you select the entity type as Correspondent Bank or Household.
Placement Date	Select the date on which the order was submitted. **Note:** This field displays only if you select the entity type as Order.
Execution Date	Select the date on which the order was submitted. **Note:** This field displays only if you select the entity type as Execution.
Firm ID	Enter the unique identification number of the investment advisor firm. **Note:** This field displays only if you select the entity type as Investment Advisor.
Firm Name	Enter the name of the external investment advisor's firm if you do not know the name of the Firm ID.This field accepts wildcards. To search using wildcard, use the % symbol. Minimum of two characters are required for wildcard search. **Note:** This field displays only if you select the entity type as Investment Advisor.
Employee ID	Enter the employee unique identification number of the investment advisor. **Note:** This field displays only if you select the entity type as Investment Advisor.
Employee Name	Enter the name of the internal investment advisor if you do not know the employee ID. This field accepts wildcards. To search using wildcard, use the % symbol. Minimum of two characters are required for wildcard search. **Note:** This field displays only if you select the entity type as Investment Advisor.

5. Click **Search**. If the search criteria are entered correctly, the Entity Search and List page is displayed.

Note: If no matches are found for the focus based on the entered search criteria, a *No Data Found* message displays in the Entity Search and List page.

Figure 68. Entity Search and List page

Note: The Entity Search and List allows you to view additional information about the selected entities. The columns which display in the Entity List vary depending on the entity type selected. All entity types display the Details column and the Alert Count and Case Count, which displays the total number of alerts or cases associated with this entity.

Viewing and Researching Entity Details

This section allows you to view additional information about the entity you are researching.

To view additional information, follow these steps:

1. Navigate to the Entity Search and List page.

2. Enter the search criteria for the entity you are researching.

3. Click **Search**. The page displays the search results based on your search criteria.

4. Click **Details** in the Entity Search and List page for the entity that you want to investigate. The Entity Details page is displayed.

Figure 69. Entity Details page

On the Entity Details page, you can view additional details based on the focus of your initial search. The other tabs are business tabs that show current information about the searched for an entity.

The display of the tab pages in the Research workflow is identical to those in the Monitoring workflow, with the exception of the following:

- The location information displayed in the page context control area specifies that you are in the Research workflow (as with the Entity Details page).

- Entity context information displays above the entity details information rather than alert context information.

- The Entity Details page provides an Alert Details link in the Relationships tab that takes you out of the Research workflow and places you in the Monitoring workflow to take actions on the alert pertaining to that entity.

- The Create New Alert button is displayed, which allows you to manually create an alert for this entity. The section *Creating an Alert* explains the alert creation.

  For more information on the tab pages, see *Using Details Tab*.

Creating an Alert

You get complete details of entities when you do a reserach on entities. Based on the research result, you analyze and determine to create an alert. This section explains how to create an alert for an entity.

To create an alert, follow these steps:

1. Navigate to the Entity Search and List page.

2. Enter the search criteria for the entity for which you want to create an alert. For more information, see *Searching for an Entity*.

3. Click **Search**. The page displays the search results based on your search criteria.

4. Click **Details** in the Entity List for the entity that you want to create the alert. The Entity Details page is displayed.

5. Click **Create an Alert**. The New Alert window is displayed.

   The New Alert window enables you to create user-defined alerts within the Research workflow.

Figure 70. Create New Alert

6. Enter the following information in the respective fields.

Table 55. Create New Alert

Field	Description
Entity Type	Displays the Entity Type and ID concatenated, as per your selection from the Entity List page.
Entity Name	Displays the Entity Name as per your selection from the Entity List page.
Score	Enter a score for the alert. The default value is displayed.The score value must be in the range of minimum and maximum score. **Note:** If you attempt to enter less than a minimum score or more than the maximum score, a message displays asking you to enter a value within the range of minimum and maximum score. The default, minimum, and maximum score value is configurable. Contact your system administrator for the default, minimum, and maximum scores.
Creation Date	Displays the creation date with the current date.
Scenario Class	The possible values are displayed based on the selection of the focus type.
Due Date	Select the date by which an action must be taken on the alert.
Auto Assignment check box	Select the Auto Assignment check box to automate the assignment of ownership of the alert. Selecting this check box disables the *Reassign Ownership To* field and the system automatically assigns the owner as per rules defined in the Alert Assigner Editor under Alert Management Configuration settings set by an Oracle Administrator.
Owner	Select an owner for the newly created alert. The list displays owners who have access to the focal entity selected and scenario class.
Status	Displays the status as *New*.
Comments	Enter comments to support the creation of a new alert.

7. Click **Save**. The following confirmation message is displayed: *A new alert will be created. Click OK to continue to the Alert Details for your newly created alert. Click Cancel to remain within the Create Alert workflow.* The application creates an alert.

8. Click **OK**. The Alert Details page for the newly created alert displays. Once you create an alert successfully, if you select **OK** in the message box, it will take you to the Alert Details page with all applicable business tabs for this alert.

   The values in the Same Scenario Prior and Same Class Prior fields in the alert context are set to zero and display as hyphens "-" in those fields.This is because the process which calculates the earlier alerts for the entity is done as part of scheduled batches and will not update real-time.

   For more details on the tabs that display based on the Scenario Class and Focus, see *Appendix D, Business Tabs*. Because user created alerts are based on business entities and not actual transactional activity, you do not see transactional information or other matched data on the Details tab. If your role permits, you can take actions on the alert from the Details page.

Managing Compliance Regulatory Reporting

This chapter provides high-level information about Compliance Regulatory Reporting (CRR). Compliance Regulatory Reporting is integrated with the Oracle Financial Services Behavior Detection Framework to allow users to generate reports automatically populated with information relevant to the investigation which triggered the need for report to be filed.

The chapter covers the following topics:

- About Compliance Regulatory Reporting
- Where to Find More Information

About Compliance Regulatory Reporting

As part of Regulations and Compliances, organizations are required to perform appropriate analysis and report any suspicious activities that can lead to fraud or money laundering within the institution to the regulatory authorities. These regulatory bodies are responsible for safeguarding financial institutions and consumers from abuse, providing transparency in the country's financial system, enhancing that country's security, and deterring and detecting criminal activity in the financial system.

As part of this goal, these regulatory bodies require the Financial Crimes Unit (FCU), also referred to as Financial Intelligence Units (FIUs), in financial institutions to provide data regarding suspicious activities. These reports, depending on the regulatory geographic region, can be delivered in either printed or electronic format.

Oracle Financial Services Compliance Regulatory Reporting supports the management, delivery, and resolution of these regulatory reports across multiple geographic regions and across multiple financial lines of business. Since there are several differences in requirements for paper-based formats versus electronic formats, and between different geographic regions and the data elements that are required on these reports, the approach to satisfying the end goal is to provide a Regulatory Reporting framework that is configured to support paper-based and electronic formats for different geographic regions and to generate and file different types of reports.

Compliance Regulatory Reporting is integrated with the Oracle Financial Services Behavior Detection Framework to allow users to generate reports automatically populated with information relevant to the investigation which triggered the need for report to be filed. Compliance Regulatory Reporting is an optional product. Access to Compliance Regulatory Reporting actions and functions depends on whether your firm have implemented the Compliance Regulatory Reporting application pack.

Where to Find More Information

In order to have more information about the Oracle Financial Services Compliance Regulatory Reporting application, refer to the following Compliance Regulatory Reporting documents on OTN:

- *Install Guide*
- *Web Services Guide*
- *Data Model Ref Guide*
- *Release Notes*

In addition, Compliance Regulatory Reporting has the following form-specific documents:

- *User Guide and Admin Guide for United States SAR*
- *User Guide and Admin Guide for Singapore STR*
- *User Guide and Admin Guide for Malaysia STR*
- *User Guide and Admin Guide for Nigeria STR*
- *User Guide and Admin Guide for Bahamas STR*
- *User Guide and Admin Guide for New Zealand STR*
- *User Guide and Admin Guide for Egypt STR*
- *User Guide and Admin Guide for Pakistan STR*
- *User Guide and Admin Guide for Burundi STR*
- *User Guide and Admin Guide for Rwanda STR*
- *User Guide and Admin Guide for Uganda STR*
- *User Guide and Admin Guide for Philippines STR*
- *User Guide and Admin Guide for Kenya STR*
- *User Guide and Admin Guide for Indonesia STR*
- *User Guide and Admin Guide for Canadian STR*

Managing Watch List Management

This chapter describes the Watch List Management functionality and gives step-by-step instructions for using it. The following topics are covered in this chapter:

- About Watch List Management
- Accessing Watch List Management
- Managing Watch Lists
- Managing Watch List Members

About Watch List Management

This section covers the following topics:

- Introduction
- Key Features
- Watch List Management Architecture

Introduction

A Watch List is a list of entries that are known to have the same level of risk characteristics. Watch Lists can represent public sources or can be created and managed internally by the institution. Watch List data can originate from public sources. For example, the Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF) or private sources like a client's list of entities on which suspicious activity reports are filed.

Oracle Financial Services Watch List Management gathers risk metrics based on the processing of risk or trust values from client records during data ingestion. You can then use these risk metrics to find high-risk behaviors. Watch lists and their entries conform to types and characters that the *Data Interface Specification (DIS)* specifies; OFSBD audits all changes.

Public lists used by clients are huge, and can contain typographical errors. Without the Watch List Management UI, clients must accept these errors, or manually correct them each time the list is updated and transformed for delivery to Ingestion. Some clients established staging databases in which they applied corrections, managed internal lists, and transformed lists into the Oracle Financial Services DIS format.

The staging database process created the following limitations:

- Inefficient processing
- Increased complexity
- Increased cost for installation
- Requirement that clients review

Key Features

The Watch List Management UI allows you to perform the following actions:

- Add new watch lists
- Add new watch list members to watch lists
- Modify watch lists
- Deactivate existing watch list members and watch lists
- Review recommended actions to approve or reject

Watch List Management Architecture

The following figure depicts the architecture of Watch List Management.
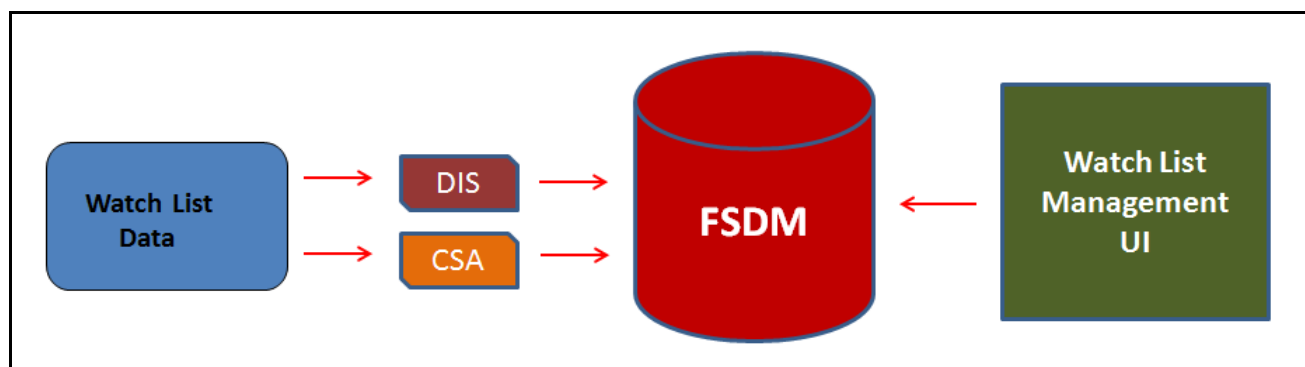
Figure 71. Watch List Management Architecture

User Roles and Actions

This section describes various user roles and actions they can perform in the Watch List Management (WLM) workflow.

Table 56. User Roles and Actions

User Actions		User Roles		
Features	**Description**	**WLM Viewer**	**WLM Analyst II**	**WLM Supervisor**
Watch List Management	View all pages within the WLM application.	X	X	X
Watch List Management - Add Lists and Watch List Members	Create new watch lists and Watch List Members.		X	X
Watch List Management - Edit Lists	Edit watch lists.		X	X
Watch List Management - Deactivate Lists and Watch List Members	Deactivate watch lists and Watch List Members.		X	X

User Actions		User Roles		
Features	**Description**	**WLM Viewer**	**WLM Analyst II**	**WLM Supervisor**
Watch List Management - View Pending Changes	View watch lists and Watch List Members in *Pending* status	X	X	X
Watch List Management - Approve Pending Changes	Approve recommended action on watch lists and Watch List Members. **Note:** Actions taken by WLM Supervisor do not need any approvals.			X
Watch List Management - Reject Pending Changes	Reject recommended action on watch lists and Watch List Members. **Note:** Actions taken by WLM Supervisor do not need any approvals.			X

Watch List Management Workflows

This section describes the complete workflow of Watch Lists and Watch List Members.

Note: Only Analyst requires an approval from Supervisor to accomplish actions in Watch Lists and Watch List Members workflow. The Supervisor role does not require any approval.

- **Watch Lists Workflow:**

  - Using UI, Analyst adds, modifies, or deactivates a watch list. These actions are recommended to the Supervisor for review.

  - The Supervisor reviews the actions recommended by the Analyst. The status of the watch list is *Pending* in Review Pending tab.

  - If the Supervisor approves the action, the data is updated in the Watch List main table and displayed in the Watch List tab with *Active* status.

  - If the Supervisor rejects the action, the data is not updated and displayed in the Review Pending tab with *Rejected* status.

Note: Analyst can only view the status of watch list in Review Pending tab.

Note: The watch list is locked, when the Supervisor selects an existing watch list for reviewing a modification or deactivation.

- **Watch List Members Workflow:**

  - Using UI, Analyst adds or deactivates a watch list member. These actions are recommended to the Supervisor for review.

  - The Supervisor reviews the actions recommended by the Analyst. The status of the watch list member is *Pending* in Review Pending tab.

  - If the Supervisor approves the action, the data is updated in the Watch List Member main table and displayed in the Watch List Member tab with *Active* status.

■ If the Supervisor rejects the action, the data is not updated and displayed in the Review Pending tab with *Rejected* status.

Note: Analyst can only view the status of watch list in Review Pending tab.

Note: The watch list member is locked, when the Supervisor selects an existing watch list member for reviewing a deactivation.

The following figure shows the Watch Lists and Watch List Members Management workflow.
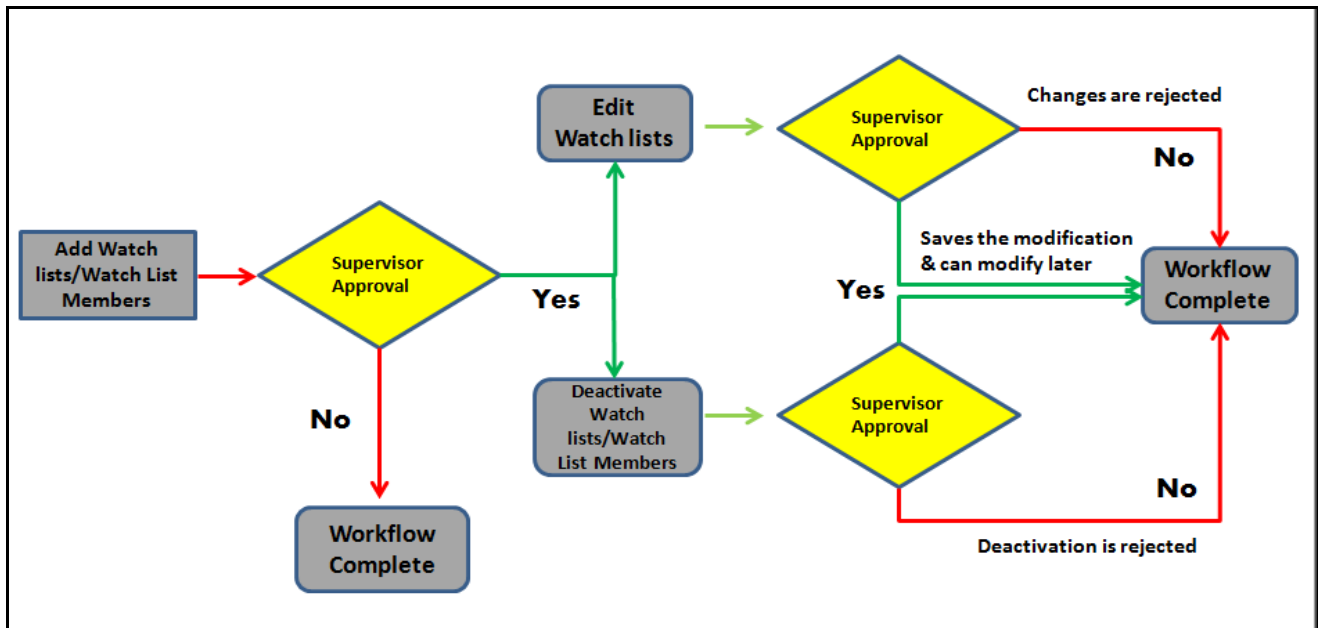
Figure 72. Watch List and Watch List Members Management Workflow

The following table details about the Manage Watch Lists workflow.

Table 57. Manage Watch Lists Workflow

Action	Description	Roles
Adding Watch Lists	User can add new watch lists.	Analyst/ WLM Supervisor
Editing Watch Lists	User can modify existing watch lists which are in *Active* status.	Analyst/ WLM Supervisor
Deactivating Watch Lists	User can deactivate existing watch lists which are in *Active* status. **Note:** User cannot activate the deactivated watch lists.	Analyst/ WLM Supervisor
Reviewing Watch Lists	User can review the actions recommended by the Analyst and take appropriate actions to approve or reject.	WLM Supervisor

The following table details about the Manage Watch List Members workflow.

Table 58. Manage Watch List Members Workflow

Action	Description	Roles
Adding Watch List Members	User can add new watch list members to a watch list.	Analyst/ WLM Supervisor
Deactivating a Watch List Member	User can deactivate existing watch list members which are in *Active* status. **Note:** User cannot activate the deactivated watch list members.	Analyst/ WLM Supervisor
Reviewing Watch List Members	User can review the actions recommended by the Analyst and take appropriate actions to approve or reject.	WLM Supervisor

Accessing Watch List Management

This section explains how to access the Watch List Management page.

To access the Watch List Management page, follow these steps:

1. Navigate to the OFSAA Application page. For more information on how to navigate to the OFSAA Application, see *Chapter 3, Getting Started.*

2. Select the **Financial Services Anti-Money Laundering**. The Behavior Detection- Anti-Money Laundering page is displayed.

3. Click **Watch List Management** in RHS. The Watch List Management page is displayed.
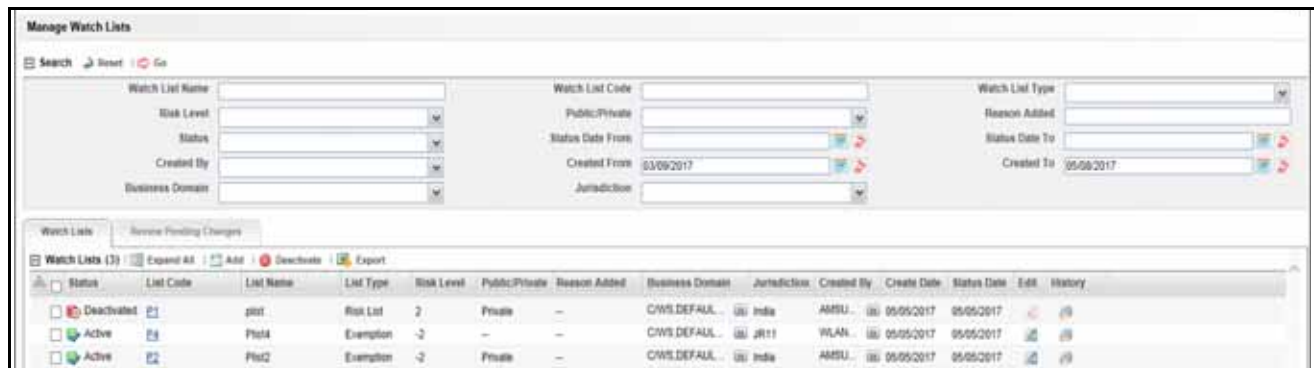
Figure 73. Watch List Management

Managing Watch Lists

This section explains how to add, modify, and deactivate watch lists.

The following sections describe how to manage watch lists:

- Accessing Managing Watch Lists page
- Adding Watch Lists
- Editing Watch Lists

- Deactivating Watch Lists

- Reviewing Watch Lists

- Viewing Watch Lists History

- Searching Watch Lists

Accessing Managing Watch Lists page

This section explains how to access the Manage Watch Lists page.

To access the Manage Watch Lists page, follow these steps:

1. Navigate to the Watch Lists Management page. By default, The Manage Watch Lists Search and List page is displayed.

   Or, hover over the **Watch Lit Management** main menu. Select the **Manage Watch Lists** submenu. The Manage Watch Lists Search and List page is displayed.

Adding Watch Lists

This section describes how to add new watch list.

To add a watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page. click the **Add**. The Add Watch List window is displayed.
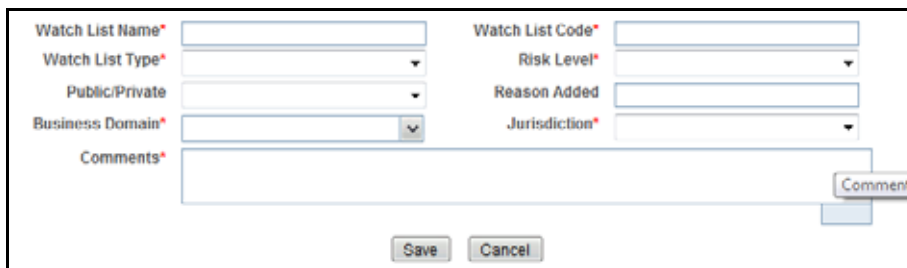
Figure 74. Add Watch List window

2. Enter the following information in the appropriate fields.

Table 59. Add Watch List fields.

Field	Description
Watch List Name	Enter the name of the watch list you wish to add.
Watch List Code	Enter the unique, three character identifier for the watch list you wish to add.
Watch List Type	Select the type of watch list you wish to add from the drop-down list. The Watch List Type you select helps displayed your options in the Risk Level drop-down list.

Table 59. Add Watch List fields.

Field	Description
Risk Level	Select the degree of risk associated with the watch list you wish to add from the drop-down list. The drop-down list is displayed with specific values based on your selection in the Watch List Type drop-down list. **Note:** If you have selected the Watch List Type *Trust* or *Exemption*, the system automatically assigns a risk level -1 and -2 (respectively) to the watch list and you need not select a value.
Public/Private	Select whether the watch list you are adding is public or private from the drop-down list.
Reason Added	Enter the reason to add new watch list.
Business Domain	Select the business domain you wish to associate with the watch list from the drop-down list. **Note:** You must be mapped to the business domain associated with the watch list to be able to view it on the UI.
Jurisdiction	Select the jurisdiction you wish to associate with the watch list from the drop-down list. **Note:** You must be mapped to the jurisdiction associated with the watch list to be able to view it on the UI.
Comments	Enter appropriate comments for this watch list.

3. Click **Save.** The following message is displayed: *Watch List will be created. Click OK to Save. Click Cancel to go back to the Add Watch List popup.*

4. Click **OK**.

Note:

- If the Supervisor adds a watch list, the newly added watch list is displayed in the Watch List tab in the *Active* status.

- If the Analyst adds a watch list, the newly added watch list is displayed in the Review Pending tab in the *Pending* status. Once the Supervisor approves the action, the newly added watch list is displayed in the Watch List tab in *Active* status. If the Supervisor rejects the action, the Review Pending tab displays the watch list in *Rejected* status.

Editing Watch Lists

This section guides you how to modify existing watch lists which are in *Active* status.

To edit a watch list, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.

2. Select a watch list you wish to modify. Click **Edit**. The Edit Watch List window is displayed.

Figure 75. Edit Watch List window

3. Modify the necessary information in the appropriate field. For more information on the fields, see *Table 59*.

   Note: You cannot remove a business domain or jurisdiction that is currently linked with at least one watch list member associated with this watch list.

4. Click **Save**. The following message is displayed: *You have selected to edit this record. Click OK to continue and save changes.*

5. Click **OK**.

Note:

- If the Supervisor edits a watch list, the modified watch list data is displayed in the Watch List tab in the *Active* status.

- If the Analyst edits a watch list, the modified watch list data is displayed in the Review Pending tab in the *Pending* status. Once the Supervisor approves the action, the modified watch list data is displayed in the Watch List tab in *Active* status. If the Supervisor rejects the action, the Review Pending tab displays the watch list in *Rejected* status.

- When the Analyst modifies the watch list, the status of watch list remains *Active* in Watch list tab. The data of the watch list is updated once the Supervisor approves the modification and the status remain *Active.*

Deactivating Watch Lists

This section describes how to deactivate one or more watch lists in *Active* status.

Note:

- To deactivate a watch list all watch list members must be unlocked.

- If you add watch list members to the deactivated watch list, the watch list members are also deactivated.

- The Watch List Management Utility does not allow you to reactivate the deactivated watch lists. Therefore, you must perform the deactivation action carefully.

- If you deactivate a watch list, any watch list members associated with that watch list will be deactivated.

To deactivate watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.

2. Select one or more watch lists. The status of the selected watch lists must be *Active*.

   Note: If you select a watch list which is already recommended for the deactivation, the following message is displayed: *Pending watch lists (members) cannot be deactivated. Please select only active watch lists (members).*

3. Click **Deactivate** icon. The Deactivate Watch List window displays.

Watch List (1)											
Status	Watch List Code	Watch List Name	List Type	Risk Level	Public/Private	Reason Added	Business Domain	Jurisdiction	Created By	Create Date	Status Date
Active	TC	Test	Risk List	1	Private	Y	C/WS,EMP,GE...	DN of ...	supervisor	09/22/2013	09/22/2013

Comments

Save   Cancel
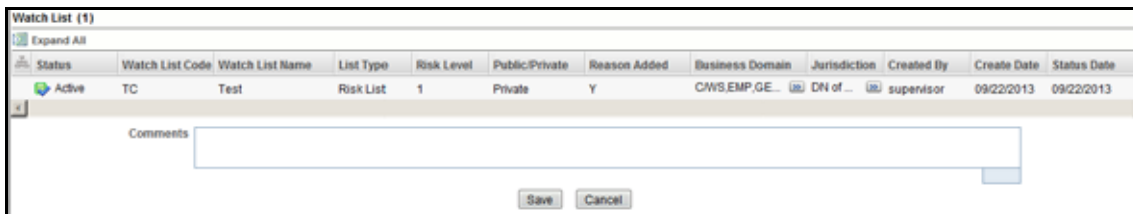
Figure 76. Deactivate Watch List pop-up window

The Deactivate Watch List window lists the watch lists you have selected to deactivate.

4. Enter the justification for deactivating watch lists in the Comments field.

5. Click **Save**. The following message is displayed. *The following watch lists are being deactivated-konda.Click OK to Save. Click Cancel to go back to the Watch List Action popup.*

6. Click **OK**.

   Note:

   ■   If the Supervisor deactivates, the watch list is displayed in the Watch List tab in the *Active* status.

   ■   If the Analyst deactivates, the watch list is displayed in the Review Pending tab in the *Pending* status. Once the Supervisor approves, the watch list is displayed in the Watch List tab in the *Active* status. If the Supervisor rejects the action, the Review Pending tab displays the watch list in the *Rejected* status.

Reviewing Watch Lists

When an Analyst recommends to add a new watch list, modify an existing watch list, or deactivate a watch list, the Supervisor reviews the recommended action to approve or reject.

Note:

   ■   Only a Supervisor can perform this action.

   ■   The newly added watch list is not locked when it is under review.

   ■   The watch list is locked when the Supervisor selects an existing watch list for reviewing a modification or deactivation

   ■   Analyst can view the status of watch lists in the *Review Pending Changes* tab.

To review a watch list, follow these steps:

1. Navigate to the Manage Watch List page. Click **Review Pending Changes** tab.

2. Select one or more watch lists in *Pending* status.

3. Click the **Approve or Reject** icon. The Review Watch List window is displayed.
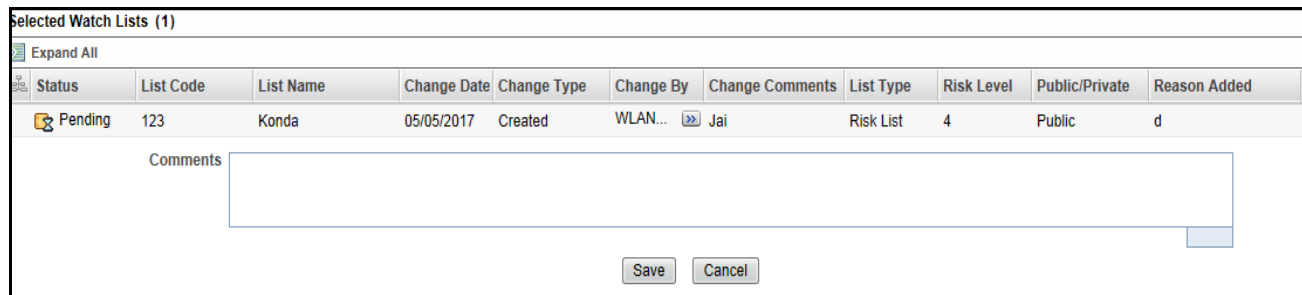
Figure 77. Review Watch List window

The Review Watch Lists window lists the watch lists you have selected to review.

4. Enter comments in the Comments field to support your action.

5. Click **Save**. The watch list or lists are approved or rejected. The following message is displayed: *The following watch lists are being approved. Click OK to Save. Click Cancel to go back to the Watch List Action popup.*

6. Click **OK** on the confirmation window to navigate to the Manage Watch Lists page. The updated watch lists are displayed with relevant status.

Viewing Watch Lists History

To view watch list history, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.

2. Select a required watch list. Click **History** icon. The Watch List History window is displayed.
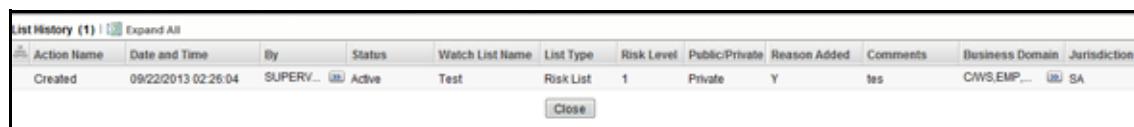
Figure 78. Watch List History window

The history of the watch list displays in ascending order, based on date and time the action is recorded. The following table describes the columns in the Watch List History window.

Table 60. Watch List History Columns

Column Name	Description
Action Name	Displays the name of the action which was taken on the watch list.
Date and Time	Displays the date and time at which the action was taken.
By	Displays the name of the user who has taken the action on the.
Status	Displays the status of the watch list after the action was recorded.
Watch List Name	Displays the name of the watch list after the action was recorded.
List Type	Displays the list type associated with the watch list after the action was recorded.
Risk Level	Displays the risk level assigned to the watch list after the action was recorded.
Public/Private	Displays the whether the watch list was public or private after the action was recorded.

Table 60. Watch List History Columns

Column Name	Description
Reason Added	Displays the description of the watch list after the action was recorded.
Comments	Displays any user comments recorded with the action.
Business Domain	Displays the business domain associated with the watch list after the action was recorded.
Jurisdiction	Displays the jurisdiction associated with the watch list after the action was recorded.

3. Click **Close** to close the Watch List History window.

Searching Watch Lists

The Manage Watch Lists Search section enables you to search for watch lists based on criteria that you provide within this search section. Drop-down lists and text boxes enable you to filter available watch lists more precisely for analysis. A blank value in a filter means that no specific value is selected. If the blank value is selected, it will have no impact on filter criteria.

The following fields are displayed:

- **Created From:** Displays today's date - 60 days

- **Created To:** Displays today's date.

If a search is performed with blank values in fields, then the results are displayed without applying filters on those fields. In particular, if a status is not specified, the system applies a set of underlying rules to the records returned in the results. Blank search is not supported. You need to enter one or more search criteria in order to execute a search.

To search watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.
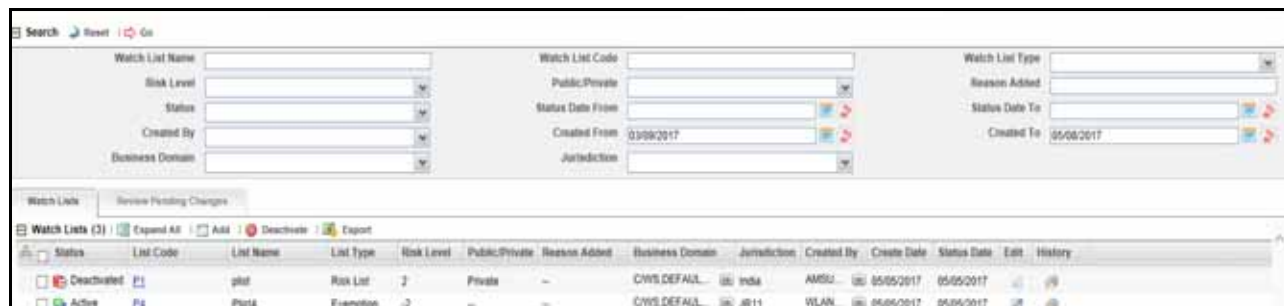
Figure 79. Manage Watch Lists page

2. Enter the following information in the respective fields.

Table 61. Watch List Search Section Filters

Field	Description
Watch List Name	Enter the name of the watch list that you wish to search for.
Watch List Code	Enter the unique three-character identifier of the watch list that you wish to search for.
Watch List Type	Select the type of watch list you wish to search for from the drop-down list.

Table 61. Watch List Search Section Filters

Field	Description
Risk Level	Select the degree of risk associated with the watch list from the drop-down list.
Public/Private	Select whether the watch list you are searching for is a public or private watch list.
Reason Added	Enter the description of the watch list you wish to search for.
Status	Displays current status of the watch list. There are four possible statuses: ● Active ● Deactivated ● Pending ● Rejected If you have access to view only Deactivated lists, this field will be blank.
Status Date From	Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database.
Status Date To	Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database.
Created From	Select a date range from which the watch list was created. By default, this field selects a date 60 days ago.
Created To	Select a date range during which the watch list was created. By default, this field selects today's date.
Created By	Select the name of the watch list creator from the drop-down list of all users that have a role with permission to Add Lists and Watch List Members.
Business Domain	Select the business domain associated with the watch list. You must be mapped to the business domain that is associated with the watch list to be able to view it on the UI.
Jurisdiction	Select the jurisdiction associated with the watch list. You must be mapped to the jurisdiction that is associated with the watch list to be able to view it on the UI.

3. Click **Go**. The relevant list of watch lists is displayed.

Viewing Watch Lists and Review Pending Tabs

This section explains you search result of watch lists. You can view the complete infromation of watch lists in two tabs.

- Watch Lists Tab Columns
- Review Pending Changes Tab Columns

Based on your tab selection, column headings provide labels that tell you what kind of information displays in the columns. These columns are displayed based on the tab you select- Watch Lists or Review Pending Changes.

Most of the column headings in the Watch Lists section are sortable. You will be able to sort each column by right-clicking on the column header and choosing ascending or descending options.

The column heading that is selected for the sorting option displays with an arrow beside it. The direction of the arrow indicates the sort order (ascending or descending). When you click a different column heading, the arrow displays beside that column with the direction indicating the sort direction. Oracle Financial Services Alert Management refreshes the list and re-sorts the watch lists display by that field, retaining the current list entries based upon the criteria you selected in the Watch List Search. If you click the same column heading again, Oracle Financial Services Alert Management sorts the column in the opposite direction.

Watch Lists Tab Columns

The following table describes the columns in the Watch Lists section.

Table 62. Watch List Columns

Column Name	Description
Status	Displays the current status of the watch list and an icon that represents the status. The following statuses may display: ● Pending ● Rejected ● Active ● Deactivated
List Code	Lists the unique three-character identifier of the watch list as a hyperlink. Click the Watch List Code to view the Manage Watch List Members page, which displays all members associated with the selected watch list. Use the bread crumbs to navigate back to the Manage Watch Lists page.
List Name	Displays the name of the watch list.
List Type	Displays the type associated with the watch list.
Risk Level	Displays the degree of risk associated with members of the watch list.
Public/Private	Indicates the origin of the watch list: ● **Public**: Indicator of a public source as the origin of the watch list. ● **Private**: Indicator of a private source as the origin or watch list; that is, a list maintained by the Oracle client. ● **All:** Indicator of both Public and Private sources of watch lists.
Reason Added	Displays the watch list description.
Business Domain	Displays the business domains associated with the watch list.You must be mapped to the business domain that is associated with the watch list to be able to view it on the UI.
Jurisdiction	Displays the jurisdictions associated with the watch list. You must be mapped to the jurisdiction that is associated with the watch list to be able to view it on the UI.
Created By	Name of the user who created the watch list.
Create Date	Date the watch list was created.
Status Date	The date when the status of this watch list was last updated.
Edit	Click the Edit button to open the Edit Watch Lists pop-up window and edit the watch list details. The Edit button is enabled only when you have access to edit and the list is not in Deactivated status. Deactivated lists cannot be edited. For more information, refer to *Editing Watch Lists*.
History	Click the History button to open the Watch Lists History pop-up window and view the watch list history. For more information, refer to *Deactivating Watch Lists*.

Review Pending Changes Tab Columns

The Review Pending Changes tab displays the columns described in the *Table 63* and *Table 62*.

Table 63. Review Pending Changes Columns

Column Name	Description
Change Date	Displays the action taken date.
Change Type	Displays the changed action. For example, Created, Deactivated, and so on.

Table 63. Review Pending Changes Columns

Column Name	Description
Change By	Displays the authorized user who took the action.
Change Comments	Displays the comments provided by the user who took the action.
Review Date	Displays the date on when the review was done.
Reviewed By	Displays the user's role who reviewed the watch list.
Review Comments	Displays the comments provided by the user who reviewed the watch lists.

Managing Watch List Members

This section explains how to add, deactivate, and search watch list members.

This section covers following topics:

- Accessing Watch List Members page
- Adding Watch List Members
- Deactivating a Watch List Member
- Reviewing Watch List Members
- Viewing Watch List Member Details
- Searching Watch List Members

Accessing Watch List Members page

This section explains how to access the Watch List Members page.

To access the Watch List Members page, follow these steps:

1. Navigate to the Watch List Management page.

2. Hover over **Watch List Management** main menu. Select the **Watch List Members** submenu. The Watch List Members Search and List page is displayed.

Adding Watch List Members

This section allows you to add new watch list members to the watch list.

Note: If you add watch list members to the deactivated watch list, the watch list members are also deactivated.

To add a watch list member, follow these steps:

1. Navigate to the Watch List Members Search and List page.

2. Click **Add**. The Add Watch List Member window is displayed.

Figure 80. Add Watch List Member window

3. Enter the following information in the appropriate fields.

Table 64. Add Watch List Member fields

Field	Description
Watch List Code	Select the unique identifier Watch List Code from the drop- down list. This is the watch list you wish to associate with this member.
Watch List Name	Displays the name of the watch list associated with this member. This field is pre-populated based on the Watch List Code.
Watch List Type	Displays the watch list type for the watch list associated with this member. This field is pre-populated based on the Watch List Code.
Watch List Status	Displays the status of the watch list associated with this member. This field is pre-populated based on the Watch List Code.
Risk Level	Displays the risk level of the watch list associated with this member. This field is pre-populated based on the Watch List Code.
Public/Private	Displays the whether the watch list associated with this member is public or private. This field is pre-populated based on the Watch List Code.
Business Domain	Displays the business domains associated with the watch list associated with this member. This field is pre-populated based on the Watch List Code.
Jurisdiction	Displays the jurisdiction associated with the watch list associated with this member. This field is pre-populated based on the Watch List Code.
ID Type	Select the type of entity represented by the member from the drop-down list.
ID	Enter the identifier or name of the member you wish to add.
Source	Select the source of the member from the drop-down list.
Business Cluster	Select the business cluster associated with the member you wish to add from the drop-down list.
Reason Added	Select the reason this member is being added from the drop-down list.
Description	Enter a description for this member.
Comments	Enter appropriate comments to add this member.
Business Domain	By default, this drop-down list is disabled and the Inherit Watch List Business Domains Check box is checked. This means that the watch list member inherits all domains assigned to the parent watch list (selected via the Watch List Code). Uncheck the Inherit Watch List Business Domains check box to enable the Domains drop-down list, which is populated with all domains assigned to the watch list. If a watch list has not been selected via the Watch List Code, then the Domains drop-down list is blank. Check the check box again to clear and disable the Domains drop-down list.
Jurisdiction	Displays jurisdiction associated with the watch list member.

Note: A watch list member must be associated with a watch list.

The values in the Business Cluster and Reason Added fields in the Add Watch List Member window displays based on the attribute values available in the Reference Table Detail table.

The following table describes the attribute values for these fields:

Table 65. Values in the Business Cluster and Reason Added fields

Business Table	Business Field	Code Set Identifier	Instruction
Watch List Entry	Reason Added	Watch List Entry Reason Added	Code 1: Code for the Reason Added Code 2: not used Code Description: Description of reason for creating the watch list entry. Code Additional Information: not used
Watch List Entry	Source	Watch List Entry Source	Code 1: Code for the Source Code 2: not used Code Description: Description of source of the watch list entry. Code Additional Information: not used
Watch List Entry	Business Cluster	Watch List Entry Business Cluster	Code 1: Code for the business cluster Code 2: not used Code Description: Description of business cluster of the watch list entry. Code Additional Information: not used

4. Click **Save.** The following message is displayed: *Watch List Member will be created. Click OK to Save. Click Cancel to go back to the Add Watch List popup*.

5. Click **OK**.

Note:

- If the Supervisor adds a watch list member, the newly added watch list is displayed in the Watch List Member tab in the *Active* status.

- If the Analyst adds a watch list member, the newly added watch list member is displayed in the Review Pending tab in the *Pending* status. Once the Supervisor approves the action, the newly added watch list member is displayed in the Watch List Member tab in *Active* status. If the Supervisor rejects the action, the Review Pending tab displays the watch list member in *Rejected* status.

Deactivating a Watch List Member

This section guides how to deactivate watch list members. The Watch List Management option does not allow you to reactivate the deactivated watch list members.

To deactivate a watch list member, follow these steps:

1. Navigate to the Watch List Members Search and List page.

2. Select one or more watch list members. The status of the selected watch list members must be *Active*.

   Note: If you select a watch list member which is already recommended for the deactivation by another user, the following message is displayed: *Pending watch lists (members) cannot be deactivated. Please select only active watch lists (members).*

3. Click **Deactivate** icon. The Deactivate Watch List Member window is displayed.
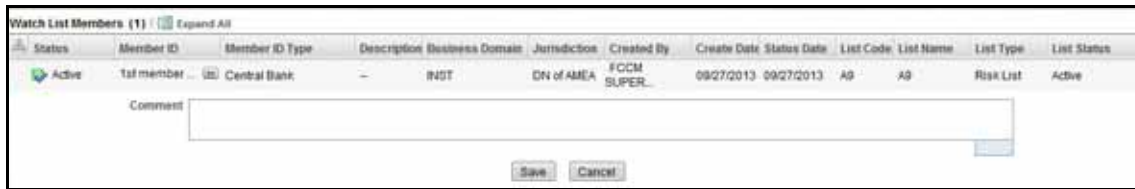
Figure 81. Deactivate Watch List Member window

The Deactivate Watch List Member window lists the watch list members you have selected to deactivate.

4. Enter justification to deactivate watch list member in the Comments field.

5. Click **Save**. The following message is displayed. *The following watch list members are being deactivated.Click OK to Save. Click Cancel to go back to the Watch List Member Action popup.*

6. Click **OK.**

Note:

- If the Supervisor deactivates a watch list member, the deactivated watch list member is displayed in the Watch List Members tab in the *Deactivated* status.

- If the Analyst deactivates a watch list member, the deactivated watch list member is displayed in the Review Pending tab in the *Pending* status. Once the Supervisor approves the action, the watch list member is displayed in the Watch List Members tab in the *Deactivated* status. If the Supervisor rejects the action, the Review Pending tab displays the watch list in the *Rejected* status.

Reviewing Watch List Members

When an Analyst recommends to add new watch list members or deactivate watch list members, a Supervisor reviews the recommended action to approve or reject.

Note:

- Only a Supervisor can perform this action.

- The newly added watch list member is not locked when it is under review

- The watch list member is locked when the Supervisor selects an existing watch list member for reviewing a deactivation

- An Analyst can view the status of watch list members in the *Review Pending Changes* tab.

To review a watch list member, follow these steps:

1. Navigate to the Manage Watch List Members page. Click the **Review Pending Changes** tab.

2. Select one or more watch list members in the *Pending* status.

3. Click the **Approve or Reject** icon. The Review Watch List Members window is displayed.
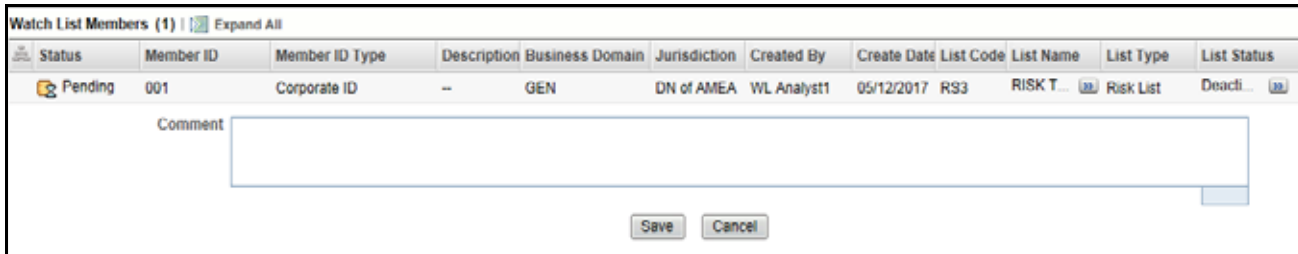
Figure 82. Review Watch List Members Window

The Review Watch List Members window lists the watch list members you have selected to review.

4. Enter comments in the Comments field to support your action.

5. Click **Save**. The watch list member or members are approved or rejected. The following message is displayed: *The following watch lists are being approved. Click OK to Save. Click Cancel to go back to the Watch List Action popup.*

6. Click **OK** on the confirmation window to navigate to the Manage Watch List Member page. The updated watch lists are displayed with relevant status.

Viewing Watch List Member Details

This section allows you to a view complete history of the Watch List Members details.

To view member details, follow these steps:

1. Navigate to the Watch List Members Search and List page.

2. Click the **Member ID** of the member you wish to view details for. The Watch List Member Details and History window is displayed.
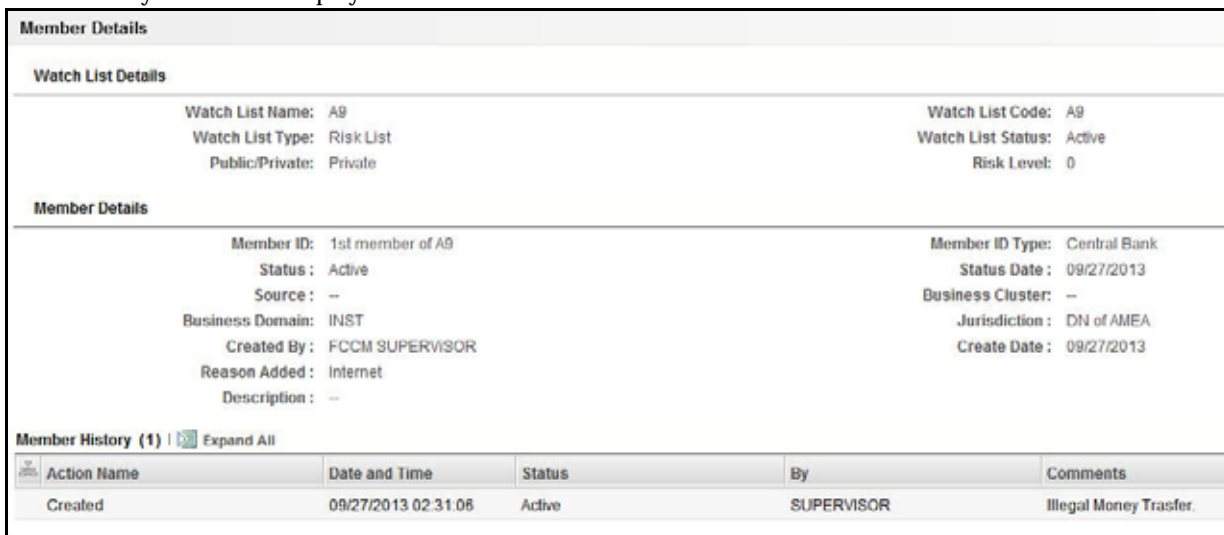
Figure 83. Watch List Member Details and History window

The following table describes the columns in the Watch List Member Details and History window.

Table 66. Fields in Watch List Member Details and History

Field Name	Description
Watch List Name	Displays the watch list name.
Watch List Code	Displays the watch list unique identifier.
Watch List Type	Displays the type of watch list.
Watch List Status	Displays the status of watch list.
Risk Level	Displays the degree of Risk associated with the watch list.
Public/Private	Displays the public or private watch list.
Status	Displays the current status of this member.
Status Date	Last status change date for this member.
Created By	Displays the creator of the member.
Create Date	Displays the date the member was created.
ID Type	Displays the type of entity represented by the member.
ID	Displays the identifier or name of a member. The value for this field is automatically populated as the Entity Identifier 1 Text field in the Watch List Entry FSDM table.
Source	Displays the source of the member.
Business Cluster	Displays the business cluster associated with the member.
Business Domain	Displays the business domain(s) associated with the member. If the member is associated with more than one domain, the UI displays available business domains in alphabetical order.
Jurisdiction	Displays the jurisdiction associated with the member.
Reason Added	Displays the reason member was added.
Description	Displays the description of the watch list member.

Searching Watch List Members

The Manage Watch List Members Search section enables you to search for watch list members based on criteria that you provide within this search section. Drop-down lists and text boxes enable you to filter available watch list members more precisely for analysis.

The following fields are displayed:

- **Created From:** Displays today's date - 60 days

- **Created To:** Displays today's date

To search watch list members, follow these steps:

1. Navigate to the Manage Watch List Members Search and List page.

Figure 84. Manage Watch Lists page

2. Enter the following information in the respective fields.

Table 67. Watch List Members Search Section Filters

Fields	Description
Watch List Name	Enter the name of the watch list associated with the watch list member you wish to search for.
Watch List Code	Enter the unique, three character identifier of the watch list associated with the watch list member that you wish to search for.
Watch List Type	Select the type of watch list associated with the watch list member you wish to search for from the drop-down list.
Member ID	Enter the identifier or name of the member on the watch list.
Member ID Type	Select the type of entity represented by the member you wish to search for from the drop-down list.
Member Description	Enter a description for the watch list member.
Member Reason Added	Select the reason the member was added from the drop-down list.
Member Source	Select the source of the member you wish to search for from the drop-down list.
Member Business Cluster	Select the business cluster associated with the member you wish to search for from the drop-down list.
Member Status	Select the status of the watch list member you wish to search for from the drop-down list. There are four possible statuses: ● Active ● Deactivated ● Pending ● Rejected If you have access to view only Deactivated lists, this field will be blank.
Status Date From	Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database.
Status Date To	Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database.
Member Created By	Select the name of the user who created the watch list member you wish to search for in the drop-down list.
Created From	Select a date range from which the watch list member was created. By default, this field selects a date 60 days ago.
Created To	Select a date range during which the watch list member was created. By default, this field selects today's date.

Table 67. Watch List Members Search Section Filters

Fields	Description
Business Domain	Select the business domain associated with the watch list member you wish to search for. You must be mapped to the business domain associated with the member to be able to view it on the UI.
Jurisdiction	Select the jurisdiction associated with the watch list member you wish to search for. You must be mapped to the jurisdiction associated with the member to be able to view it on the UI.

3. Click **Go**. The relevant watch list members list is displayed.

Viewing Watch List Members and Review Pending Tabs

This section explains you search result of watch list members. You can view the complete infromation of watch list members in two tabs.

- Watch list Members Tab Columns

- Review Pending Changes Tab Columns

Based on the tab you select, the column headings provide labels that tell you what kind of information displays in the columns. These columns are displayed based on the tab you select- Watch List Members or Review Pending Changes.

Most of the column headings in the Watch List Members section are sortable. You will be able to sort each column by right-clicking on the column header and choosing ascending or descending options.

The column heading that is selected for the sorting option displays with an arrow beside it. The direction of the arrow indicates the sort order (ascending or descending). When you click a different column heading, the arrow displays beside that column with the direction indicating the sort direction. Oracle Financial Services Alert Management refreshes the list and re-sorts the watch lists display by that field, retaining the current list entries based upon the criteria you selected in the Watch List Search. If you click the same column heading again, Oracle Financial Services Alert Management sorts the column in the opposite direction. The following table describes the columns in the Watch List Members section.

Watch list Members Tab Columns

The following table describes the columns in the Watch List Members section.

Table 68. Watch List Members columns

Column Name	Description
Status	Displays the current status of the watch list member and an icon that represents the status. The following statuses may display: ● Active ● Deactivated
Member ID	Displays the identifier or name of the watch list member. This identifier is a hyperlink that opens the Member Details popup. You will be able to see only the first 50 characters of the Member ID. You can increase the width of the field via the Field Chooser.
Member ID Type	Displays the type of entity represented by the watch list member.
Description	Provides a description of the watch list member.
Business Domain	Displays the business domains associated with the watch list member.

Table 68. Watch List Members columns

Column Name	Description
Jurisdiction	Displays the jurisdiction associated with the watch list member.
Created By	Displays the name of the watch list creator who created this member.
Create Date	Displays the date this watch list member was created.
List Code	Lists the unique identifier of the watch list this member is associated with.
List Name	Displays the name of the watch list this member is associated with.
List Type	Displays the type of watch list this member is associated with.
List Status	Displays the current status of the watch list this member is associated with.

Review Pending Changes Tab Columns

The Review Pending Changes tab displays the columns described in the *Table 68* and *Table 69*.

Table 69. Review Pending Changes Columns

Column Name	Description
Change Date	Displays the action taken date.
Change Type	Displays the changed action. For example, Created or Deactivated.
Change By	Displays the authorized user who took the action.
Change Comments	Displays the comments provided by the user who took the action.
Review Date	Displays the date on when the review was done.
Reviewed By	Displays the user's role who reviewed the watch list members.
Review Comments	Displays the comments provided by the user who reviewed the watch list members

Setting User Preferences

This chapter describes the concept and process of managing Alert Management UI preferences. It provides systematic instructions to carry out various actions according to user roles. This helps you to understand how to use various components to accomplish each task.

This chapter covers following topics:

- About Preferences page
- Key Features
- User Roles and Actions
- Accessing Preferences page
- Managing Preferences

Note: Some components of the Preference page are specific to either Enterprise Case Management or Alert Management. Firms that have implemented both and users who have access to both will see a supers et of items for which preferences can be set. Where only one is installed or users can access one or the other, they will see preferences related to the component for which they have access.

About Preferences page

You can change your default preferences for Alert Management using the Preferences page. You can manage preferences in Workflow, Search, Graph, Audit, and other sections according your convenience. Use ˃ - to expand the section and ˅ to collapse the section..

Key Features

- Set preferences for the Alert Search and List page
- Set preferences for the Simple and Advanced Search sections.
- Set preferences for AML, Broker Compliance, ECTC, Fraud, and Trading Compliance search options
- Set preference for the Replay Tab
- Set preferences for the Audit Display Tab

User Roles and Actions

This section describes various user roles and actions they can perform in the Alert Management UI preferences.

The following table details the user roles and actions in the Alert Management UI preferences:

User Actions	User Roles									
Privileges	**Analyst I**	**Analyst II**	**Analyst III**	**Supervisor**	**Executive**	**Internal Auditor**	**External Auditor**	**Data Miner**	**AM Administrator**	**WLM Supervisor**
Access to Preferences	X	X	X	X	X	X	X	X		

Accessing Preferences page

This section explains how to access the Preferences page.

To access the Preferences page, follow these steps:

1. Navigate to the OFSAA Applications Home page. For more information, see *Chapter 3, Getting Started*.

2. Click **Preferences**. The Preferences page is displayed.

Managing Preferences

This section explains you how to manage preferences in Alert Management UI.

This section helps you in managing following default settings:

- Setting Alert Search and List Options
- Setting Options for Alert Search
- Setting AML Specific Search Options
- Setting Broker Compliance Specific Search Options
- Setting Energy and Commodity Trading Compliance Specific Search Options
- Setting Fraud Specific Search Options
- Setting Trading Compliance Specific Search Options
- Setting Trade Blotter Default Search
- Setting Options for Replay page
- Setting Options for Audit Display
- Saving Preferences

Setting Alert Search and List Options

The Set Alert Search and List Options section enables you to set the display preferences in the Search and Alert List page.

To set alert search and list options, follow these steps:

Figure 85. Navigate to the Preferences page and go to the Set Alert Search and List Options section.

3. Select the preferred options from the respective drop-down lists.

Table 70. Set Alert Search and List Options

Field	Description
Set Alert Display Configuration	To set your alert display configuration based on deployed solution sets or other configurable criteria, select one of the following solutions sets to display a custom set of controls and fields in the Alert Search and List section. The following are the available options: - Anti-Money Laundering - Broker Compliance and Control Room - ECTC - Fraud - Standard - Trading Compliance For more information on setting the alert display configuration, see *Alert List Display Configuration*. **Note:** These solution sets are provided with standard deployment. Additional custom solution sets can be configured in the Alert Display Configuration selection.
Set Default Search	To set default search fields based on the deployed solution sets or other configurable criteria, select the mutually exclusive default search type from the drop-down list. The following are the available options: - Views - Simple Search - Advanced Search
Set View for Alert List	To set the view for the alert list in the Search and Alert List page, select the view for alert list type from the drop-down list. For example, My Open Alerts, My New Alerts, and so on. By default, the *My Open Alerts* option is selected if you have not previously saved your View option.

Setting Options for Alert Search

This section explains how to set field options in the Simple and Advanced Search sections. The fields that are set in the Preferences page display in the Alert Search page.

Note: This section appears only if you select **Simple Search** or **Advanced Search** in the **Set Default Search** field.

To set options for Alert Search page, follow these steps:

Figure 86. Navigate to the Preferences page and go to the Set Option for Alert Search.

4. Select common filters for the solution set. For more information, see *Table 70* Setting the Alert Display Configuration section.

Table 71. Alert Search Components

Fields	Description	Standard	AML	TC	BC	Fraud	ECTC
Alerts Created in the Last	Select alerts created in the last 1, 5, 10, or 30 days from the drop-down list.	X	X	X	X	X	X
Organization	Select the organization from the drop-down list. This filters alert list by the ID of the organization associated with the owner of an alert. This drop-down list only contains the organizations (and the organizations subordinate to it) to which you have a business association and are authorized to view. **Note:** If you filter by Organization, you cannot filter by Owner.	X	X	X	X	X	X
Owner	Select the owner from the drop-down list. This filters the alert list by a user or user group to whom an alert is assigned. This drop-down list contains user or user group within the organization. **Note:** If you filter by Owner, you cannot filter by Organization.	X	X	X	X	X	X
Scenario Class	Select the scenario class from the drop-down list. This filters the alert list by the scenario class associated with an alert, it is listed by its abbreviation. This drop-down list contains only the scenario classes that you are authorized to view. **Note:** If you filter by Class, you cannot filter by Scenario.	X	X	X	X	X	X
Scenario	Select the scenario from the drop-down list. This filters the alert list by the scenarios name of the behavior or activity that generated the alert.	X	X	X	X	X	X
Status	Select the status from the drop-down list. This filters the alert list by the current status of an alert, relative to its analysis and closure in the drop-down list.	X	X	X	X	X	X
Focus	Select the focus from the drop-down list. This filters the alert list by the type of business object that exhibits the behavior of interest, focus is a two-part representation including focus type and an associated focal entity. Your access control privileges determine which focus types display in the drop-down list. If you filter by Focus, you cannot filter by Focus Type. For example, a focus of *TR SmithJ* consists of a focus type of *TR* and a focal entity of *SmithJ.*	X	X	X	X	X	X

Table 71. Alert Search Components (Continued)

Fields	Description	Standard	AML	TC	BC	Fraud	ECTC
Score	Select alerts with scores greater than equal to, equal to, or less than equal to, to the score you enter in the box. This filters the alert list by the score the alert received when based against the criteria selected by your firm.	X	X	X	X	X	X
Age	Select alerts with age greater than equal to, equal to, or less than equal to, to the age you enter in the box. This filters the alert list by the number of calendar or business days since the creation of an Active alert.	X	X	X	X	X	X
Jurisdiction	Select the jurisdiction from the drop-down list. This filters the alert list by jurisdiction to which you are assigned.	X	X	X	X	X	X
Domain	Select the business domain from the drop-down list. This filters the alert list by the business domain associated with an alert. The drop-down list only contains the business domains with which you are authorized to view.	X	X	X	X	X	X
Alerts Due	Select the alert due from the drop-down list. This filters the alert list by the date by which an action should be taken on the alert.	X	X	X	X	X	X
Closing Action	Select the closing action from the drop-down list. This filters the alert list by one or more selected closing actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.	X	X	X	X	X	X
Last Action	Select the last action from the drop-down list. This filters the alert list by the selected action or actions representing the last action recorded for a alert. **Note:** You must specify an Action To or Action From date for this search.	X	X	X	X	X	X
Action	Select the action from the drop-down list. This filters the alert list by one or more actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.	X	X	X	X	X	X
Regulatory Report Type	Select the Regulatory Reporting type from the drop-down list. This filters the alert list by the regulatory reporting types that are available to you (for example, (SARDI). The Regulatory Reporting is an optional Oracle application.	X	X	X	X	X	X

Table 71. Alert Search Components (Continued)

Fields	Description	Standard	AML	TC	BC	Fraud	ECTC
Regulatory Report Status	Select the Regulatory Reporting status from the drop-down list. This filters the alert list by the current status of an alert that is recommended for Regulatory Reporting, an optional Oracle application.	X	X	X	X	X	X
Prior All	Select alerts with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the number of previously generated matches for the same focal entity across all scenarios and solution sets.	X	X	X	X	X	X
Linked Cases	Select alerts with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the cases that are linked to the alert.	X	X	X	X	X	X
Limit to Focus checkbox	Select the limit to focus or not. This filters the alert list to where the specified entity is the focus.	X	X	X	X	X	X
Entity Type	Select the focus from the drop-down list and type either Entity Name or Entity ID to search for alerts. This filters the alert list by the type of business entity you select in the drop-down list box.	X	X	X	X	X	X
Entity ID	Enter the unique identifier for entity that is associated with alerts you want to view.The field accepts up to fifty characters of text in the Entity ID box.	X	X	X	X	X	X
Entity Name	Enter the entity name associated with alerts you want to view.	X	X	X	X	X	X

Setting AML Specific Search Options

The Alert Management system enables you to set AML specific search fields.

To set AML specific search options, follow these steps:

1. Navigate to the Preferences page. Go to the Set AML Specific Search Options section.

   Note: This section displays only if you select **Anti - Money Laundering** in the S**et Alert Display Configuration** drop-down list and **Simple Search** or **Advanced Search** in the **Set Default Search** drop-down list.

Note: Some AML filters are applicable to another display configuration. Setting defaults for these filters applies across display configuration.

2. Select the preferred options from the respective drop-down lists.

Table 72. AML Specific Search Options

Fields	Description
Prior Scenario	Select scenario with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the number of matches previously generated for the same focal entity by the same scenario as the current alert.
Prior Class	Select class with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the number of matches previously generated for the same scenario class associated with an alert.

Setting Broker Compliance Specific Search Options

The Alert Management system enables you to set Broker Compliance specific search fields.

To set Broker Compliance specific search options, follow these steps:

1. Navigate to the Preferences page. Go to the Set Broker Compliance Specific Search Options section.

   Note: This section displays only if you select **Broker Compliance and Control Room** in the S**et Alert Display Configuration** drop-down list and **Simple Search** or **Advanced Search** in the **Set Default Search** drop-down list.

   Note: Some AML filters are applicable to another display configuration. Setting defaults for these filters will apply across display configuration.

2. Select the preferred options from the respective drop-down lists.

Table 73. Broker Compliance Specific Search Options

Fields	Description
IA Firm ID	Enter the investment advisor firm ID. This filters the alert list by the identification of the firm associated with the investment advisor.
IA Firm	Enter the investment advisor firm name. This filters the alert list by the name of the firm associated with the investment advisor.
Service Team ID	Enter the service team ID. This filters the alert list by the identification of the primary service team of which this employee is a member.
Representative ID	Enter the registered representative ID. This filters the alert list by identification number of the employee or contractor who is the registered representative.
Representative	Enter the representative name. This filters the alert list by name of the employee or contractor who is the registered representative.
Branch ID	Enter the branch ID. This filters the alert list by the identification number of the organization where this account is domiciled.
Branch	Enter the branch name. This filters the alert list by the name of the organization where this account is domiciled.
Supervisory Organization ID	Enter the supervisory organization ID. This filters the alert list by unique identification number of the organization where the registered representative is employed.
Supervisory Organization	Enter the supervisory organization name. This filters the alert list by the name of the organization where the registered representative is employed.

Setting Energy and Commodity Trading Compliance Specific Search Options

The Alert Management system enables you to set Energy and Commodity Trading Compliance specific search fields.

To set the Energy and Commodity Trading Compliance specific search options, follow these steps:

1. Navigate to the Preferences page. Go to the Set Energy and Commodity Trading Compliance Specific Search Options section.

   Note: This section displays only if you select **ECTC** in the S**et Alert Display Configuration** drop-down list and **Simple Search** or **Advanced Search** in the **Set Default Search** drop-down list.

Note: Some AML filters are applicable to another display configuration. Setting defaults for these filters will apply across display configuration.

Table 74. Energy and Commodity Trading Compliance Specific Search Options

Fields	Description
Commodity Instrument ID	Enter the identification number of the commodity instrument.This filters the alert list by the identification number of the commodity instrument involved in the alert.
Commodity Instrument Name	Enter the name of the commodity instrument. This filters the alert list by the name of the commodity instrument involved in the alert.
Trader	Enter the name of the trader. This filters the alert list by the name of the trader involved in the alert.
Trader ID	Enter the identification number of the trader. This filters the alert list by the identification number of the trader involved in the alert.

Setting Fraud Specific Search Options

The Alert Management system enables you to set Fraud specific search fields.

To set Fraud specific search options, follow these steps:

1. Navigate to the Preferences page. Go to the Set Fraud Specific Search Options section.

   Note: This section displays only if you select **Fraud** in the S**et Alert Display Configuration** drop-down list and **Simple Search** or **Advanced Search** in the **Set Default Search** drop-down list.

Note: Some AML filters are applicable to another display configuration. Setting defaults for these filters will apply across display configuration.

2. Select the preferred options from the respective drop-down lists.

Table 75. Fraud Specific Search Options

Fields	Description
Total/Net Loss Amount	Enter the total/net loss amount value. This filters the alert list by the total net loss amount associated with the alert. This is the total loss remaining after Averted and Recovery Amounts are subtracted from the Potential Loss.
Primary Cost Center	Enter the primary cost center value. This filters the alert list by the primary cost center to which the total net loss amount for an alert is associated.

Table 75. Fraud Specific Search Options

Fields	Description
Prior Scenario	Select scenario with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the number of matches previously generated for the same focal entity by the same scenario as the current alert.
Prior Class	Select class with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the number of matches previously generated for the same scenario class associated with an alert.

Setting Trading Compliance Specific Search Options

The Alert Management system enables you to set Trading Compliance specific search fields.

To set Trading Compliance specific search options, follow these steps:

1. Navigate to the Preferences page. Go to the Set Trading Compliance Specific Search Options section.

   Note: This section displays only if you select **Trading Compliance** in the S**et Alert Display Configuration** drop-down list and **Simple Search** or **Advanced Search** in the **Set Default Search** drop-down list.

Note: Some AML filters are applicable to another display configuration. Setting defaults for these filters will apply across display configuration.

2. Select the preferred options from the respective drop-down lists.

Table 76. Trading Compliance Specific Search Options

Fields	Description
Security ID	Enter the security ID. This filters the alert list by the identification number of the security involved in the alert.
Security	Enter the security name. This filters the alert list by the name of security involved in the alert.
Trader	Enter the trader name. This filters the alert list by the name of the trader involved in the alert.
Trader ID	Enter the trader ID. This filters the alert list by the identification number of the trader involved in the alert.

Setting Trade Blotter Default Search

If Trade Blotter is enabled at the deployment and if you have the appropriate access permissions for the Trade Blotter functionality, the Set Trade Blotter Default Search section on the Preferences page enables you to set the display preferences for the simple and advanced searches.

1. Navigate to the Preferences page. Go to the Set Trade Blotter Default Search section.

2. Select the following mutually exclusive options displays in the Trade Blotter section:

   ■ Simple Search

   ■ Advanced Search

Refer to Chapter 7,*Managing Trade Blotter*, for a description of all the possible fields on the Trade Blotter Search section.

Setting Simple Search Options for Trade Blotter

Oracle Financial Services Alert Management enables you to set preference for the search options that are configured for the Simple Trade Search section of Trade Blotter Search page.

The values you set here are automatically pre-populated in the corresponding fields of the Search page. The time you select from the **Trades executed in the Last:** drop-down list on the Preferences page is calculated to populate the correct dates in the **Trade Date From** and **To** fields on the Search page.

Setting Advanced Search Options for Trade Blotter

In addition to specifying preference for the Simple Trade Search section, you can set options for all the search filters and the view and sort fields that are configured for the Advanced Trade Search section.

The values you set here are automatically pre-populated in the corresponding fields of the Search page. The following discrepancies exist between the fields displayed on the Advanced section of the Trade Blotter Search page, and the Advanced section of the Trade Blotter section of the Preferences page:

- For Organization, Division, and Branch filters, if the one or two filters are configured for display on the Search page, the system does not display the third filter as a preference option. Also, the Division filter is enabled only if you select a value in the Organization preference option. Further, the Division preference option is populated based on the selection made in the Organization preference option, and so forth.

- For dates (in other words, the Trade Date, Trade Entered Date, Settlement Date, and Review Status To and From fields), instead of displaying preference options for the date To and From fields, a Trades Reviewed in the Last drop-down list displays with the following values:

    - Blank

    - 1 Day

    - 5 Days

    - 10 Days

    - 30 Days

    - 60 Days

    Based on the value you select here, the system resets the values in the To and From date fields on the Search page accordingly. For example, if you select 30 days as the preference setting, the To date field is populated with the current system date and the From date field is populated with the date 30 calendar dates prior to the current system date. If you select the Blank option as the default preference, the system resets the To and From date fields on the Search page to a blank value.

Setting Options for Replay page

The Set Options for Replay page section displays if your role is associated with one or more scenarios belonging to a scenario class and focus that display on the Replay tab, and have access to the Replay tab in the application. The Alert Management system enables Analyst II, Analyst III, and Supervisor roles to configure the Security Group filters in the Replay page.

To set options for Replay page, follow these steps:

1. Navigate to the Preferences page. Go to the Set Options for Replay page section.

2. Select either **Disable** or **Enable** in the Set Option for Security Group.

Note: By default, the Alert Management UI selects the Security Group option as Enable if you do not save your settings.

Setting Options for Audit Display

This section explains how to set preferences on the audit display.

To set options for audit display, follow these steps:

1. Navigate to the Preferences page. Go to the Set Options for Audit Display section.

2. To view a history of when the current alert is viewed by the owner or other users regardless of any action being taken, select the **Display View Only Action** checkbox.

3. To view a history of when the status of the current alert is changed, select the **Display Status Changing Actions** checkbox.

4. To view all the alerts which have attachments, select the **Attachments Included** checkbox.

Saving Preferences

Once you complete setting your preferences, click **Save**.

Note: You do not have to logout for new preferences to take effect. The system remembers your preferences. Each time when you accesses the system, the preferences are displayed.

APPENDIX A *User Privileges*

This appendix provides the detailed information on various user roles and privileges in alert management workflow.

Oracle Financial Services Alert Management allows different types of roles to access the Alert Management UI. The various roles are: Analyst I, Analyst II, Analyst III, Supervisor, Executive, Internal Auditor, External Auditor, Data Miner, Oracle Administrator, and WLM Supervisor.

Table 4 describes the privileges for each role level.

Table 77. User Privileges

User Actions	User Roles									
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
Access to Components										
Access to Monitoring workflows	X	X	X	X	X	X	X			
Access to Reports workflow			X	X	X	X				
Access to Administration workflow									X	
Access to Manage Security Restrictions	X	X	X	X	X	X				
Access to Manage Controlling Customer	X	X	X	X	X	X				
Access to Manage Suppression Rules	X	X	X	X	X	X				
Access to Manage Trusted Pairs	X	X	X	X	X	X				
Access to Trade Blotter			X	X	X	X				
Access to Preferences	X	X	X	X	X	X	X		X	
Access to Research		X	X	X	X	X		X	X	X
Access to Manage Watch Lists						X	X			X
Access to Manage Watch List Members						X	X			X
Access to Tabs										
Access to Relationships Tab	X	X	X	X	X	X	X			
Access to Narrative Tab	X	X	X	X	X	X	X			
Access to Disposition Tab	X	X	X	X						
Access to Audit Tab	X	X	X	X	X	X	X			
Access to Evidence Tab	X	X	X	X	X	X	X			
Access to Correlations Tab	X	X	X	X		X	X			
Access to Financials Tab	X	X	X	X	X	X	X			
Access to Manage Suppression Rules Functionality										
Access to View Search and List of for Suppression Rules	X	X	X	X	X	X				

Table 77. User Privileges (continued)

User Actions	User Roles									
Privileges	**Analyst I**	**Analyst II**	**Analyst III**	**Supervisor**	**Executive**	**Internal Auditor**	**External Auditor**	**Data Miner**	**AM Administrator**	**WLM Supervisor**
Add Suppression Rules			X	X						
Reject Suppression Rules			X	X						
Update Suppression Rules			X	X						
End Suppression Rules			X	X						
View Suppression Rule Action History			X	X	X	X				
Access to Alert Actions										
Access to Add/Modify narrative		X	X	X						
Access to Print Alert Investigative reports (detailed and summary level)		X	X	X	X	X				
Access to Create Alerts		X	X	X						
Access to add comments	X	X	X	X		X				
Access to remove attachments	X	X	X	X		X				
Access to Follow-up or Closing actions (additional restrictions can apply)		X	X	X						
Access to the Reassign action	X	X	X	X						
Ability to Reassign to owners in all organizations (additional access control restrictions can apply)	X	X	X	X						
Access to export actions		X	X	X						
Access to email actions		X	X	X						
Access to suppression actions			X	X						
Ability to modify the highlight value while creating a suppression rule.			X	X						
Access to reopen actions		X	X	X						
Access to add attachments	X	X	X	X		X				
Access to Manage Trusted Pairs Functionality										
Access to Designate Trusted Pairs button on Matched Information section		X	X	X						
Access to View Search and List for Trusted Pairs	X	X	X	X	X	X				
Ability to Reject Trusted Pairs recommendations				X						
Ability to Self-Reject Trusted Pairs recommendations		X	X							
Ability to approve Trusted Pairs recommendations				X						
Ability to cancel Trusted Pairs				X						
Ability to recommend to cancel Trusted Pairs		X	X							
Ability to modify Trusted Pairs				X						
Ability to recommend to modify Trusted Pairs		X	X							
Ability to view Trusted Pairs History	X	X	X	X	X	X				
Access to Financials Functionality										
Access to enter data in Financials data entry sections		X	X	X						

Table 77. User Privileges (continued)

User Actions	User Roles									
Privileges	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
Access to view history in the Financials tab		X	X	X	X	X				
Access to edit existing data on Financials tab		X	X	X						
Access to delete existing data on Financials tab		X	X	X						
Access to Adm in Tools										
Access to Threshold Editor								X		
Access to Alert Scoring Editor									X	
Access to Alert Creator Editor									X	
Access to Alert Assigner Editor									X	
Access to Scenario Wizard								X		
Access to Threshold Analyzer								X	X	
Access to Common Productivity Reports for Alerts										
Alerts by Final Disposition - Monthly			X	X	X			X	X	
Alerts by Final Disposition - Weekly			X	X	X			X	X	
Alerts by Final Disposition - Yearly			X	X	X			X	X	
Alerts by Jurisdiction			X	X	X			X	X	
Alerts by Scenario			X	X	X			X	X	
Alerts by Status			X	X	X			X	X	
Alerts Late or near Late distributed by Jurisdiction			X	X	X			X	X	
Alerts Late or near Late distributed by Owner			X	X	X			X	X	
Alerts Late or near Late distributed by Scenario			X	X	X			X	X	
Access to AML Reports for Alerts										
SARs Submitted in a Period Distributed by Owner			X	X	X	X				
SARs Submitted in a Period Distributed by Scenario			X	X	X	X				
SARs Submitted in a Period Distributed by Jurisdiction			X	X	X	X				
False Positive Alerts Over a Period Distributed by Owner			X	X	X	X				
False Positive Alerts Over a Period Distributed by Scenario			X	X	X	X				
False Positive Alerts Over a Period Distributed by Jurisdiction			X	X	X	X				
AML Reports - Others										
SARs Due in a Period Distributed by Owner			X	X	X	X				
SARs Due in a Period Distributed by Jurisdiction			X	X	X	X				
Top 10 Branches with High Risk Customers			X	X	X	X				
Alert Entity Search Reports			X	X	X	X				
Access to Trade Blotter Reports										
Trade Review Activity Report			X	X	X					

Table 77. User Privileges (continued)

User Actions	User Roles									
Privileges	**Analyst I**	**Analyst II**	**Analyst III**	**Supervisor**	**Executive**	**Internal Auditor**	**External Auditor**	**Data Miner**	**AM Administrator**	**WLM Supervisor**
Compliance Staff Productivity Report			X	X	X					
Access to Trade Blotter Functionality										
Access to View Trades in "Reviewed" status (This controls user's access to trades that are in the Reviewed status, and thus, also to the display of the "Reviewed" tab)			X	X	X	X				
Access to View Trades in "New- Un reviewed" status (This controls user's access to trades that are in the Pending status, and thus, also to the display of the "Pending" tab)			X	X	X	X				
Access to View Trades in "Reviewed with Follow-Up" status (This controls user's access to trades that are in the Reviewed with Follow-Up status, and thus, also to the display of the "Reviewed with Follow-Up" tab)			X	X	X	X				
Access to mark a trade as a "Reviewed" Trade (when the existing trade review status is "New- Un reviewed")				X	X					
Access to mark a trade as a "Reviewed with Follow-Up" Trade (when the existing trade review status is "New- Un reviewed")				X	X					
Access to Add Attachments to Trades				X	X					
Access to Add Comments to Trades				X	X					
Access to View Trade Attachments Audit History, Comment Audit History and Trade Action History				X	X		X			
Access to mark a trade as a Reviewed Trade (when the existing trade review status is Reviewed with Follow-Up)					X					
Access to mark a trade as a Reviewed with Follow-Up Trade (when the existing trade review status is Reviewed)					X					
Access to Send email via Trade Blotter				X	X					
Access to Send email and Request a Response via Trade Blotter				X	X					
Access to Watch List Management Functionality										
Access to Add Lists & Entries										X
Access to Edit Lists										X
Access to Deactivate Lists & Entries										X
Managing Controlling Customer										
Access to Manage Controlling Customer	X	X	X	X	X	X				
Update Controlling Customer (Add, Edit, Add Comment)			X	X						
Remove Controlling Customer			X	X						
Managing Security Restrictions										
Access to Manage Security Restrictions	X	X	X	X	X	X				
Update Security Restrictions (Add, Edit, Add Comment)			X	X						
Remove Security Restrictions			X	X						

APPENDIX B

Alert Components and Tables

This appendix provides the additional information on various tables of alert management.

This appendix covers following sections:

- Alert Context Information
- Actions with Post Status as Follow-up
- Network Analysis Details
- Search Components
- Alert List Display Configuration

Alert Context Information

The following table provides a list of the fields that display in the Alert Context information based on your scenario class of the alert.

Table 78. Alert Context Information by Scenario Class

Column	Description	AML	Fraud	TC	BC	ECTC
Alert ID	Unique ID of the alert.	X	X	X	X	X
Focus [Type and Name]	Focus on which the alert is based. Both the focus type abbreviation and the focus name display.	X	X	X	X	X
Score	Score the alert received.	X	X	X	X	X
Scenario	Scenario short name of the scenario that generated the alert.	X	X	X	X	X
Owner	Name of an individual or group of users to whom the alert is assigned.	X	X	X	X	X
Organization	Name of the organization for which an alert is assigned.	X	X	X	X	X
Business Domain	Business domain(s) associated with the alert focus.	X	X	X	X	X
Same Scenario Prior	Number of previous matches associated with the focus of the current alert and of the same scenario.	X	X	X	X	X
Same Class Prior	Number of previous matches associated with the focus of the current alert and of the same scenario class.	X	X	X	X	X
Linked Cases	The count of cases linked to the alert.	X	X	X	X	X
Status	Current state of the alert relative to its analysis and closure.	X	X	X	X	X
Alerts Due [Date and Time]	Date and time by which an action should be taken on the alert.	X	X	X	X	X
Highlights	Pertinent information related to the alert.	X	X	X	X	X
Total/Net Loss Amount	The total loss remaining after Averted Loss and Recovery Amounts are subtracted from the Potential Loss. Applicable to Fraud class alerts.		X			

Table 78. Alert Context Information by Scenario Class (continued)

Column	Description	AML	Fraud	TC	BC	ECTC
Total Potential Loss Amount	The total potential financial loss that the institution can experience as a result of the fraudulent activity identified by the alert. Applicable to Fraud class alerts.		X			
Total Averted Loss Amount	The total financial loss amounts that the institution can be able to prevent based on actions taken during the course of the investigation into the fraudulent activity identified by the alert. Applicable to Fraud class alerts.		X			
Total Recovery Amount	The total financial losses that are recovered during the course of the investigation into the fraudulent activity identified by the alert. Applicable to Fraud class alerts.		X			
Primary Cost Center	The primary cost center to which the total net loss amount for this investigation should be associated. Applicable to Fraud class alerts.		X			
Create Date	Date the alert was created.	X	X	X	X	X
Security ID	Identification number of the security involved in the alert.			X		
Security	Name of the security involved in the alert.			X		
Trader ID	Identification number of the trader involved in the alert.			X		
Trader	Name of the trader involved in the alert.			X		X
Investment Advisor Firm ID	Identification of the firm associated with the Investment Advisor.				X	
Service Team ID	Identifier of the primary service team of which this employee is a member.				X	
Registered Representative ID	Identification number of the employee or contractor who is the Registered Representative.				X	
Representative	Employee or contractor who is the Registered Representative.				X	
Branch ID	Identication number of the organization where this account is domiciled.				X	
Branch	Name of the organization where this account is domiciled.				X	
Supervisory Organization ID	Identification number of the organization where the Registered Representative is employed.				X	
Supervisory Organization	Name of the organization where the Registered Representative is employed.				X	
Commodity ID	Filters the alert list by the identification number of the commodity instrument involved in the alert.					X
Commodity	Filters the alert list by the name of the commodity instrument involved in the alert.					X

Actions with Post Status as Follow-up

This section provides information on Actions with Post Status as Follow-up

Table 79. Actions with Post Status as Follow-up

Action Category	Action	Post Status
Actions	Awaiting Response	Follow-Up
Actions	Extend Due Date	Follow-Up
Actions	Further Analysis Required	Follow-Up
Actions	Requested Updated Customer Information	Follow-Up
Actions	Requested Updated Investment Profile	Follow-Up
Actions	Requested Updated Option Trading Approval	Follow-Up
Actions	Downgraded Option Trading Level	Follow-Up/Closed *
Actions	Removed Margin Feature	Follow-Up/Closed *
Actions	Restricted Account to Cash Up Front	Follow-Up/Closed *
Actions	Restricted Account to Liquidating Transactions Only	Follow-Up/Closed *
Actions	Canceled Trade(s)	Follow-Up/Closed *
Actions	Corrected Trade(s)	Follow-Up/Closed *
Actions	Adjusted Price	Follow-Up/Closed *
Actions	Closed Account	Follow-Up/Closed *
Actions	Corrected Reporting Error	Follow-Up/Closed *
Actions	Noted Price Error	Follow-Up/Closed *
Actions	Noted Timestamp Error	Follow-Up/Closed *
Actions	Removed Investment Advisor	Follow-Up/Closed *
Actions	Updated Investment Profile	Follow-Up/Closed *
Actions	Updated Option Trading Approval	Follow-Up/Closed *
Disposition	Close and Suppress - Enter Date	Follow-Up/Closed *
Disposition	Close and Suppress 1 month	Follow-Up/Closed *
Disposition	Close and Suppress 1 year	Follow-Up/Closed *
Disposition	Close and Suppress 3 months	Follow-Up/Closed *
Disposition	Close and Suppress 6 months	Follow-Up/Closed *
Disposition	Opened Investigation	Follow-Up/Closed *
Disposition	Withheld Action	Follow-Up/Closed *
Export	Export to Case Tool	Follow-Up/Closed *
Regulatory Reporting	Close and File CTR	Follow-Up/Closed *
Regulatory Reporting	Close and File UK SAR	Follow-Up/Closed *
Regulatory Reporting	Close and File US SAR	Follow-Up/Closed *
Review	Internally	Follow-Up/Closed *
Review	Registration Status	Follow-Up/Closed *
Review	Reviewed with Account Representative	Follow-Up/Closed *

Table 79. Actions with Post Status as Follow-up (continued)

Action Category	Action	Post Status
Review	Reviewed with Customer	Follow-Up/Closed *
Review	Reviewed with Investment Advisor	Follow-Up/Closed *
Review	Reviewed with Manager	Follow-Up/Closed *
Review	Reviewed with Portfolio Manager	Follow-Up/Closed *
Review	Reviewed with Trader	Follow-Up/Closed *
Review	Reviewed with Other	Follow-Up/Closed *
Review	Reviewed with POA	Follow-Up/Closed *

Network Analysis Details

This section covers following sections:

- Start Entities List
- Include Link Types List

Start Entities List

Use the Start Entities List to build the network around entities associated with the Alert. These entities are considered the starting point of the network.

The following entity types display, based on which entities are associated with the Alert:

- Accounts
- Customers
- Households
- External Entity
- Employee
- Correspondent Banks

When multiple entities are selected, then each entity becomes a primary node and the network is built considering each as a starting point. The entities are highlighted in the Netwok Graph.

Include Link Types List

The Link Types List contains all the valid links, or relationship types, that are identified between two nodes (entities) in the Network Graph. The links are created based on Shared Activity and Known Relationship between two nodes.

The following link types display:

Table 80. Link Types

Link Type	Type of Relationship	Description
Account to Customer	Known Relationship	This relationship is used to create a link between account (node) and a customer (node) identified from the starting node.
Account to Household	Known Relationship	This relationship is used to create a link between account (node) and a customer (node) identified from the starting node.
Account to Correspondent Banks	Known Relationship	This relationship is used to create a link between account (node) and a customer (node) identified from the starting node.
Account to Employee	Known Relationship	This relationship is used to create a link between account (node) and a customer (node) identified from the starting node.
Customer to Customer	Known Relationship	This relationship is used to create a link between customer(node) and a customer(node) identified from the starting node.

Table 80. Link Types

Link Type	Type of Relationship	Description
Wire Transaction	Shared Activity	This is used to create a link between two accounts (nodes) or link between account and external entity or link between two external entities which share a common wire transaction between them.
Monetary Instruments Transaction	Shared Activity	This is used to create a link between accounts (nodes) which share a common MI transaction between them.
Journal Transaction	Shared Activity	This is used to create a link between accounts (nodes) which share a common Journal Transactions.
Insurance Transaction	Shared Activity	This is used to create a link between two accounts (nodes) or between account and an external entity which share a common Insurance Transactions.

Selecting a Link Type means only links of the selected type display in the graph. For example, the Account to Household link type will only ever discover accounts or household nodes.

Some of the Link Type and Starting Entity combinations can result in no results being returned. For example selecting only a Household entity in the Start Entities list and selecting Wire Transaction in the Include Link Types list will return no nodes other than the starting Household entity. This is because transactions do not focus on household entities. The following table provides the Valid Link Types for each node.

Table 81. Valid Entity-Link Types

Starting Entity	Valid Link Types
Household (HH)	Account to Household
Account (AC)	Account to Correspondent Bank Account to Customer Account to Household Account to Employee Journal Transaction MI Transaction Wire Transaction Insurance Transaction
Employee (EE)	Employee to Account
Customer (CU)	Account to Customer Customer to Customer
Correspondent Bank (CB)	Account to Correspondent Bank
External Entity (EN)	MI Transaction Wire Transaction Insurance Transaction

If you select an invalid link type for the entity, an error message is displayed.

The system uses this information to find the most recent available information and determines known relationships and shared attributes.

Known Relationships

Known relationships are determined based on the criteria described in the following table:

Table 82. Known Relationship Identification

Start Entity	Link Type	Relationship Identified
Account (AC)	Account to Customer	Account to Customer
	Account to Household	Account to Account Group
	Account to Employee	Account Owned by Employee
	Account to Correspondent Bank	Account to Client Bank
Customer (CU)	Account to Customer	Account to Customer
	Customer to Customer	Related Customer to Customer
		Customer to Related Customer
Correspondent Bank (CB)	Account to Correspondent Bank	Account to Client Bank
Employee (EE)	Account to Employee	Account Owned by Employee
Household (HH)	Account to Household	Account to Household

Shared Activity

The following attributes are considered for establishing a link between the nodes:

- **Wire Transactions:** The activity link is established:

   - Between Beneficiary and Originator

   - Between Secondary Beneficiary and Originator

   - Between Secondary Originator and Beneficiary

   - Between Secondary Originator and Secondary Beneficiary

   - Between Sending Institution and Receiving Institution

   For **Account** starting nodes the link is established using Account to Account wire transactions, and Account to External Entity wire transactions.

   For **External Entity** primary nodes the link is established using External Entity to Account wire transaction, and External Entity to External Entity wire transactions.

   For **Correspondent Bank** primary nodes the link is established between Sending and Receiving Institution.

- **Journal Transactions:** The nature of relationship is established:

   - Between Account and Offset Account

   For **Account** primary nodes the link is established between Account and Offset Account (where focal account is the offset account and vice versa).

- **Monetary Instrument Transactions:** The nature of relationship is established:

   - Between Beneficiary and Remitter

   - Between Secondary Beneficiary and Remitter

   - Between Issuing Institution and Depositing Institution

For **Account** primary nodes the link is established using Account to Account MI transactions, and Account to External Entity Monetary Instrument transactions.

For **External Entity** primary nodes the link is established using External Entity to Account Monetary Instrument transactions, and External Entity to External Entity Monetary Instrument transactions.

For **Correspondent Bank** primary nodes the link is established between Issuing and Depositing Institution.

- **Insurance Transactions:** The nature of relationship is established:

  - Between Insurance Policy Identifier and the Counter Party Derived Entity Identifier

  - Between Insurance Policy Identifier and the Counter Party Identifier

Filters

This section contains filters which allow you to further define the network which displays in the Network Graph. The following filters display:

- **Transaction Date >=** builds the network based on shared activity. Whenever this date is selected, the system checks for transactions between the Transaction Date >= and Transaction Date <= to establish links for Wire Transactions, Journal Transactions, Monetary Instrument Transactions and Insurance Transactions**.**

- **Transaction Date <=** builds the network based on shared activity. Whenever this date is selected, the system checks for transactions between the Transaction Date >= and Transaction Date <= to establish links for Wire Transactions, Journal Transactions, Monetary Instrument Transactions and Insurance Transactions**.**

- **Maximum Degrees of Separation** field. The value you provide determines how many cycles out from starting entity a repetition of queries will go. This number must be within your institution's limits (the default is 1-10). You cannot enter 0, decimals, or negative numbers. If you do not enter a number, the value displays the default of 3.

Search Components

This section covers following topics:

- Views Search
- Alert List Matrix
- Additional Information

Views Search

Views represent pre-populated search queries. Selecting a View for searching allows a single-click option for returning a filtered alert list based on the view's preset search criteria. By default, the Views search is available with **My Open Alerts** as the default queue. To search using views select the desired view from the list.

Following table should be part of Appendix

Table 83 list the View Filter and Sort Criteria for the default View Names.

Table 83. List of Views

View Name	View Filter and Sort criteria
My New Alerts	From: Current Date -1 To: Current Date
	Owner: current user or pool to which the current user belongs
	Status: New
My Open Alerts	Owner: current user or pool to which the current user belongs
	Status: Open or Follow-up
My Reassigned Alerts	Owner: current user or pool to which the current user belongs
	Status: Reassigned
My Overdue Alerts	Due Date is not null and is <= Current Date
	Owner: current user or pool to which the current user belongs
My Near Due Alerts	Due Date is not null and is > Current Day and <= (Current Day +4)
	Owner: current user or pool to which the current user belongs
	Sort: By Due Date Ascending; Alert ID Ascending
Management - Overdue Alerts	Due Date is not null and is <= Current Date
	Owner: Organizational pool(s) for which the current user is supervisor or user within that pool
Management - Near Due Alerts	Due Date is not null and is > Current Day and <= (Current Day +4)
	Owner: Organizational pool(s) for which the current user is supervisor or user within that pool
Management - Aged Alerts	Alert Age >= 30 days
	Owner: Organizational pool(s) for which the current user is supervisor or user within that pool
	Status: Any status but a closed status

The Alert Search bar supports the ability to search across the following types of information:

- Alert Search Dates

- Alert by Entity

- Linked Cases

Alert Information

Table 84 provides a list of the alert search components that display in the alert Simple and Advanced Search bar.

Table 84. Alert Search Components

Column	Description	Simple Search	Advanced Search				
			AML	Fraud	BC	TC	ECTC
Created From	Filters the alert list by the date the alert was created.	X	X	X	X	X	X
Created To	Filters the alert list by the date the alert was created.	X	X	X	X	X	X
Business Date	Filters the alert list with a processing date between start date and end date.	X	X	X	X	X	X
Organization	Filters the alert list by the name of the organization associated with the owner of an alert. The drop-down list contains only the organizations (and the organizations subordinate to it) to which you have a business association and are authorized to view. If you filter by Organization, you cannot filter by Owner.	X	X	X	X	X	X
Owner	Filters the alert list by a user or group of users to whom an alert is assigned. This drop-down list contains users or groups of users within the Organization. If you filter by Owner, you cannot filter by Organization.	X	X	X	X	X	X
Focus	Filters the alert list by the type of business object that exhibits the behavior of interest. Focus is a two-part representation that can display a focus type or the associated focal entity. Your access control privileges determine which focus types display in the drop-down list. For example, a focus of *TR SmithJ* can consist of a focus type of TR and a focal entity of SmithJ.	X	X	X	X	X	X
Scenario Class	Filters the alert list by the scenario class associated with an alert, listed by its abbreviation. This drop-down list contains only the scenario classes that you are authorized to view. If you filter by Class, you cannot filter by Scenario.	X	X	X	X	X	X
Scenario	Filters the alert list by the scenario, which is name of the behavior or activity that generated the alert.	X	X	X	X	X	X
Status	Filters the alert list by the current status of an alert, relative to its analysis and closure in the drop-down list.	X	X	X	X	X	X
Score	Filters the alert list by the score the alert received when based against your firm selected. Oracle Financial Services Alert Management retrieves alerts and cases greater than or equal to the score you enter in this text box.	X	X	X	X	X	X
Closing Action	Filters the alert list by one or more selected closing actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.	X	X	X	X	X	X

Table 84. Alert Search Components (continued)

Column	Description	Simple Search	Advanced Search				
			AML	Fraud	BC	TC	ECTC
Jurisdiction	Filters the alert list by the business jurisdiction associated with an alert. The drop-down list contains only the jurisdictions with which you are authorized to view.		X	X	X	X	X
Business Domain	Filters the alert list by the business domain associated with an alert. The drop-down list contains only the business domains with which you are authorized to view.		X	X	X	X	X
Due Date <=	Filters the alert list by past and up to the date you enter by which an action should be taken on the alert.		X	X	X	X	X
Prior All	Filters the alert list by the number you enter, and any number greater than of previously generated matches for the same focal entity across all scenarios and solution sets.		X	X	X	X	X
Prior Scenario	Filters the alert list by the number of matches previously generated for the same focal entity by the same scenario as the current alert.		X	X			
Prior Class	Filters the alert list by the number of matches previously generated for the same scenario class associated with an alert.		X	X			
Age	Filters the alert list by the number of calendar or business days, and any number greater, since the creation of an Active alert.		X	X	X	X	X
Action	Filters the alert list by one or more actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.		X	X	X	X	X
Last Action	Filters the alert list by one or more selected last actions that are taken on an alert. **Note:** You must specify an Action To or Action From date for this search.		X	X	X	X	X
Linked Cases	Filters the alert list by the number of cases that are linked to the alert. Oracle Financial Services Alert Management retrieves alerts, which are either greater than or equal to, equal to, or less than or equal to the count you enter in the text box. This search option is only be available if your firm has implemented Oracle Financial Services Enterprise Case Management.		X	X	X	X	X
Alert ID	Filters the alert list by the one or more Alert IDs entered in this text field. To search for multiple IDs, separate IDs with commas. If the alerts are found, the Alert List Matrix displays information about the alerts with the IDs that exactly matches the values you entered. The Alert ID search is mutually exclusive with all other filter criteria.	X	X	X	X	X	X
Regulatory Reporting Type	Filters the alert list by the Regulatory Reporting types that are available to you (for example, (SARDI). Regulatory Reporting is an optional Oracle application.		X	X	X	X	X

Table 84. Alert Search Components (continued)

Column	Description	Simple Search	Advanced Search				
			AML	Fraud	BC	TC	ECTC
Regulatory Reporting Status	Filters the alert list by the current status of an alert that is recommended for Regulatory Reporting, an optional Oracle application.		X	X	X	X	X
Limit to Focus	Filters the alert list to where the specified entity is the focus.		X	X	X	X	X
Entity Type	Filters the alert list by the type of business entity you select in the drop-down list box. Select the focus from the Entity Type drop-down list and type either Entity Name or Entity ID to search for alerts.		X	X	X	X	X
Entity ID	The unique identifier for entity that is associated with alerts you want to view.The field accept up to 50 characters of text in the Entity ID text box.		X	X	X	X	X
Entity Name	The entity name associated with alerts you want to view.		X	X	X	X	X
Commodity Instrument ID	Filters the alert list by the identification number of the commodity instrument involved in the alert.						X
Commodity Instrument Name	Filters the alert list by the name of the commodity instrument involved in the alert.						X
Security ID	Filters the alert list by the identification number of the security involved in the alert.					X	
Security	Filters the alert list by the name of security involved in the alert.					X	
Trader ID	Filters the alert list by the identification number of the trader involved in the alert.					X	X
Trader	Filters the alert list by the name of the trader involved in the alert.					X	X
Investment Advisor Firm ID	Filters the alert list by the identification of the firm associated with the Investment Advisor.				X		
Investment Advisor Firm	Filters the alert list by the name of the firm associated with the Investment Advisor.				X		
Service Team ID	Filters the alert list by the identifer of the primary service team of which this employee is a member.				X		
Registered Representative ID	Filters the alert list by identification number of the employee or contractor who is the Registered Representative.				X		
Representative	Filters the alert list by name of the employee or contractor who is the Registered Representative.				X		
Branch ID	Filters the alert list by the identification number of the organization where this account is domiciled.				X		
Branch	Filters the alert list by the name of the organization where this account is domiciled.				X		

Table 84. Alert Search Components (continued)

Column	Description	Simple Search	Advanced Search				
			AML	Fraud	BC	TC	ECTC
Supervisory Organization ID	Filters the alert list by unique ID of the organization where the Registered Representative is employed.				X		
Supervisory Organization	Filters the alert list by the name of the organization where the Registered Representative is employed.				X		
Total/Net Loss Amount	Filters the alert list by the total net loss amount associated with the alert. This is the total loss remaining after Averted and Recovery Amounts are subtracted from the Potential Loss.			X			
Primary Cost Center	Filters the alert list by the primary cost center to which the total net loss amount for an alert is associated.			X			

Alert List Matrix

The Alert List matrix displays summarized information of alerts that you can further investigate or take actions.

When you search from Simple or Advanced search, the default sort order is based on Due Date Ascending followed by Create Date Description and Alert ID Ascending.

By default, the list matrix displays 20 alerts. To view additional alerts returned by search, use the pagination controls to move to additional pages of alerts. Click the **Pagination Options** button. Select or enter the number of rows that you want to display. Click the **Go** arrow. The alerts are displayed based on the data you entered.

Alert List Components need add in the end

The Alert List matrix of the Alert Search & List page consists of the Alert List header and a matrix containing one or more alerts and associated data. Each alert has a check box and an **ID** link associated with it.

The components within the Alert List matrix are as follows:

- **Alert List** header: Contains the number of alerts displayed in the list, the total number of alerts returned by the search. Pagination controls within the header allow you to navigate to the additional pages of alerts.

- **List of Alerts**: Displays a list of alerts based on your search criteria on the Alert Search bar. Click the **Alert ID** link for any alert in the list to access the Alert Details page. If the selected alert is locked (meaning, another user has currently accessed the same alert), a message displays:

   The selected alert is locked by another user. Click **OK** to view the alert details page in view mode only and **Cancel** to return to list page.

   If you click **OK** in the dialog box, you navigate to the alert details page in view mode. In the view mode, you cannot take any action on the alert.

   The Alert List header contains a check box, which enables you to select all the check boxes for each row on the page. Selecting the check box again enables you to clear all the check boxes.

The **Expand image (>>)** displays inside the **Scenario** and **Focus** fields if the text in the field is more than the column width. Clicking the **Expand image (>>)** refreshes the data to display the complete Scenario and Focus name.

After you click the **Expand image (>>)** link, it displays the **Contract image (<<)**, which, when clicked, refreshes the data to display only the abbreviated Scenario and Focus name.

For all other fields when the text in the field is more than the column width, a Tool tip displays for approximately three seconds when you position the mouse cursor over the field to display the complete text.

- **Check Boxes:** Appears at the beginning of each row. Select one or more of these boxes to take action on one or more alerts. Select the check box again to clear it. When you select using the check box, the alert row displays a blue color highlight.

- **Action Buttons:** Enables you to select and take action on one or more alerts. When an action button is clicked, the application navigates you to the applicable Actions pop up. You can take an action on a single alert or on several alerts (batch action). Refer to Acting on Alerts for more information on taking actions on alerts.

    Before you take action on the selected alerts, Oracle Financial Services Alert Management checks each alert to determine if it is locked. If all the selected alerts are locked by another user, a message displays:

    All selected alert records are locked by another user. Please try again later.

    If some, but not all, of the selected alerts are locked, a message displays:

    One or more Alerts are locked by another user. Select **OK** to continue; **Cancel** to return to the Alert List.

    If you click the **OK** button, you can take actions on the alerts that are not locked.

    If you fail to select at least one check box and click on any action button, a message displays:

    You have not selected any alerts). Please select one or more alerts.

- **Column Headings:** Labels that tell you what kind of information displays in the columns. All column headings in the Alert List matrix are sortable. You can sort each column in the alert list by right-clicking on the column header and choosing the ascending or descending options.

- **Jump To:** User can use this feature switch to any particular page by specifying the page number in the text box.

    For example: If a list is divided in 10 pages and user directly wants to navigate to page # 5, then user can write 5 in the text box provided with *Jump To page* and press enter. The user will be taken directly to page # 5.

Table 85 provides a list of the columns that display in the Alert List matrix.

Table 85. Alert List Components by Display Configuration by Solution Sets

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	ECTC	Standard
Alert ID	X[*]	X	X	X	X	X
SC [ore]	X	X	X	X	X	X
Focus Type	X	X	X	X	X	X
Focus Name	X	X	X	X	X	X
Scenario	X	X	X	X	X	X
Highlights						X
Created [Date]	X	X	X	X	X	X
Status	X	X	X	X	X	X
Alerts Due [Date and Time]	X	X	X	X	X	X
Regulatory Reporting Status						X
Regulatory Reporting Type						X
Owner	X	X	X	X	X	X
Class] Prior						X
SCN [Scenario] Prior						X
Closing Action						X
[Business] Domain						X
[Involved] Security				X		
[Involved] Trader				X	X	
[Involved] Service Team ID			X			
[Involved] Registered Representative ID			X			
Total/Net Loss Amount		X				
Primary Cost Center		X				
Linked Cases	X	X	X	X	X	X
Commodity Instrument ID					X	
Threshold Set Name	X	X	X	X	X	X

Additional Information

The Additional Information section consists of the General Overview and Metrics bar and displays below the Alert List. The section refreshes to display additional information about the alert when you click the alert row in the Alert List section.

By default, the section is in the contracted mode. You can click the Expand ▼ image or Collapse ▲ in the section header to expand or contract the section.

Note: The Additional Information section display values only if you have clicked on the alert row. The section does not display if you only click the check box. The check box should be used only to perform actions from the action categories.

The following table provides a list of fields that display in the General Overview and Metrics section.

Table 86. General Overview and Metrics section

Column	Description	General Overview	Metrics
Highlights	Pertinent information related to the alert.	X	
Organization	Organization associated with the owner of the alert.	X	
Business Domain	Business Domains associated with the alert.	X	
Closing Action:	Closing action that is taken on an alert.	X	
Alerts for Prior Class Count	Number of matches previously generated for the same scenario class associated with the alert.		X
Alerts for Prior Scenario Count	Number of matches previously generated for the same focal entity by the same scenario as the alert.		X
Correlation Membership Count	Number of correlations the alert is a member of.		X
Regulatory Report Type	Regulatory Reporting types that are available to the user (for example, (SARDI). **Note:** This feature is available only if Oracle Financial Services Regulatory Reporting (OFSRR) application is installed.	X	
Regulatory Report Status	The current reporting status of a case that is recommended for Regulatory Reporting. **Note:** This feature is available only if Oracle Financial Services Regulatory Reporting (OFSRR) application is installed.	X	

Alert List Display Configuration

Table 85 provides a list of all columns and fields that display in the Alert List, General Overview, and Metrics section based on solution set selection as well as the components that display in the standard display of the Search and List page.

Table 87. Alert List, General Overview, and Metrics Display Configuration by Solution Sets

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	ECTC	Standard
Alert ID	L*	L	L	L	L	X
SC [ore]	L	L	L	L	L	X
Focus [Type and Name]	L	L	L	L	L	X
Scenario	L	L	L	L	L	X
Highlights	O**	O	O	O	O	X
Created [Date]	L	L	L	L	L	X
Status	L	L	L	L	L	X
Alerts Due [Date and Time]	L	L	L	L	L	X
Organization	O	O	O	O	O	
Regulatory Reporting Status	O	O	O	O	O	X
Regulatory Reporting Type	O	O	O	O	O	X
Owner	L	L	L	L	L	X
CL [Class] Prior	O	O	O	O	O	X
SCN [Scenario] Prior	O	O	O	O	O	X
Closing Action	O	O	O	O	O	X
[Business] Domain	O	O	O	O	O	X
[Involved] Security				L		
[Involved] Trader				L	L	
[Involved] Service Team ID			L			
[Involved] Registered Representative ID			L			
[Involved] Branch				O	O	
[Involved] Supervisory Organization				O	O	
Total/Net Loss Amount		L				
Primary Cost Center		L				

Table 87. Alert List, General Overview, and Metrics Display Configuration by Solution Sets (continued)

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	ECTC	Standard
Linked Cases	L	L	L	L	L	X
Alerts for Prior Class Count	M$^{\#}$	M	M	M	M	X
Alerts for Prior Scenario Count	M	M	M	M	M	X
Correlation Membership Count	M	M	M	M	M	X
Commodity Instrument ID					L	X

where, L* are fields in the Alert List section; O** are fields in the General Overview section; M$^{\#}$ are fields in the Metrics section

APPENDIX C

Results from Updating Trusted Pairs Relationships

The system updates the trusted pairs with the relevant dates or direction or both once you save the changes. Once you have saved your changes, the system updates the status of the trusted pairs accordingly (setting it to either Pending or Active based on your role) and you are navigated back to a refreshed Trusted Pairs List page.

The following table illustrates how the Expiration date reflects changes based on updates made.

Table 88. Results from Updating the Expiration Date

Trusted Pairs ID	Expiration date (before updating)	Results (after updating Trust Period 6 months)	Results (after updating Expiration Date to 05/25/2009)
TP1	03/16/2009	09/16/2009	05/25/2009
TP2	04/17/2009	10/16/2009	05/25/2009

The following table illustrates the update actions and status for users requiring Four-Eyes Approval for updating trusted pairs relationships.

Table 89. Results for User Requiring Four-Eyes Approval for Updating

Current Status	Action	Resulting Status	Action By
None	Created	Pending	User
Active	Cancelled	User Rec Cancel	User
Pending	Rejected**	Inactive	User
User Rec Cancel	Rejected**	Inactive	User
Pending/User Rec Cancel/Risk Esc Rec Cancel/Active	Comments	No change	User
Expired	Modified	Pending	User
Inactive	Modified	Pending	User

** Four-Eyes Approval users can modify or reject their own Pending recommendations if they have not be acted on.

The following table illustrates the update actions and status for users requiring Four-Eyes Approval for updating trusted pairs relationships.

Table 90. Results for User Not Requiring Four-Eyes Approval for Updating

Current Status	Action	Resulting Status	Action By
None	Created	Active	User
Pending	Approved	Active	User
Pending	Rejected	Inactive	User
Active	Cancelled	Inactive	User
User Rec Cancel	Approved	Inactive	User
User Rec Cancel	Rejected	Active	User
Risk Esc Rec Cancel	Approved	Inactive	User
Risk Esc Rec Cancel	Rejected	Active	User

Table 90. Results for User Not Requiring Four-Eyes Approval for Updating

Current Status	Action	Resulting Status	Action By
Pending/User Rec Cancel/Risk Esc Rec Cancel/Active	Comments	No change	User
Expired	Modified	Active	User
Inactive	Modified	Active	User

APPENDIX D

Business Tabs

Oracle Financial Services Alert Management consists of Business tabs that display in the Monitoring workflow. Within the Monitoring workflow, these tabs are displayed according to the focus type and scenario class of the alert you select.

Alert Business Tabs

Table 91 identifies the possible Business tab pages that Oracle Financial Services Alert Management displays for a specific scenario class and focus type in the Monitoring workflow

Table 91: Business Tab pages by Scenario Class

Focus Type	Possible Business Tabs
Scenario Class: Institutional Money Laundering	
Customer (CU)	Account, Customer, and Investment Advisor
External Entity (EN)	External Entity
Scenario Class: Control Room	
Account (AC)	Account, Trade, Order, Execution, Security, Replay, and Trader
Employee (EE)	Account, Customer, Trade, Order, Execution, Security, Replay, and Trader
Trader (TR)	Account, Trade, Order, Execution, Security, Replay, and Trade
Organization (OG)	Account, Trade, Execution, Household, Security, Customer, Replay, Trader, and Registered Representative
Scenario Class: Investment Advisor	
Investment Advisor (IA)	Account, Investment Advisor, and Trade
Scenario Class: Money Laundering	
Account (AC)	Account, Customer, Employee, Household, and Investment Advisor
Correspondent Bank (CB)	Correspondent Bank
Customer (CU)	Account, Customer, Household, and Investment Advisor
External Entity (EN)	External Entity
Household (HH)	Account, Customer, Household, and Investment Advisor
Scenario Class: Fraud	
Account (AC)	Account, Customer, Household, Investment Advisor, Employee, and Financials
Customer (CU)	Account, Customer, Household, Investment Advisor, and Financials
Employee (EE)	Account, Employee, Financials, and Household
External Entity (EN)	External Entity
Household (HH)	Account, Customer, Household, and Investment Advisor
Scenario Class: Best Execution	
Order (OR)	Account, Execution, Market Participant, Order, Replay, Security, and Trader
Scenario Class: Trading Compliance	
Account (AC)	Account, Execution, Order, Replay, Security, Trade, and Customer
Customer (CU)	Account, Customer, Execution, Order, Replay, Security and Trade

Table 91: Business Tab pages by Scenario Class (Continued)

Focus Type	Possible Business Tabs
Employee (EE)	Account, Trade, Order, Execution, Security, Employee, Customer, Replay
Execution (EX)	Account, Execution, Market Participant, Order, Replay, Security, Trade, and Trader
Investment Advisor (IA)	Account, Trade, Order, Execution, Security, Investment Advisor, Customer, Replay
Order (OR)	Account, Trader, Order, Execution, Security, Replay, and Market Participant
Security (SC)	Order, Trade, Execution, Replay, and Security
Trader (TR)	Account, Trader, Trade, Execution, Order, Replay, and Security
Organization (OG)	Replay, Security, Trade, Trader, and Execution
Scenario Class: Mutual Funds	
Account (AC)	Account, Customer, Household, Investment Advisor, Registered Representative, and Trade
Household (HH)	Account, Customer, Household, Investment Advisor, Registered Representative, and Trade
Investment Advisor (IA)	Account, Investment Advisor, and Trade
Registered Representative (RR)	Account, Registered Representative and Trade
Scenario Class: Employee Trading	
Employee (EE)	Account, Employee, Security, and Trade
Scenario Class: Customer Risk and Suitability	
Account (AC)	Account, Customer, Household, Investment Advisor, Loan Origination, Registered Representative, Security, Trade and Order
Household (HH)	Account, Customer, Household, Investment Advisor, Trade, IOS Review, Registered Representative, and Security
Organization (OG)	Loan Origination
Registered Representative (RR)	Account, Registered Representative, Trade, Execution, Order, and Security
Scenario Class: Asset Management	
Portfolio Manager (PM)	Account, Employee, Order, and Security
Scenario Class: Energy and Commodity Trading Compliance	
Commodity Instrument (CI)	Energy and Commodity Trade, Energy and Commodity Instrument, ECTC Replay, Trader, and Natural Gas Flow
Trader (TR)	Energy and Commodity Trade, Energy and Commodity Instrument, ECTC Replay, and Trader

Using Alert Management Web pages

The information provided in the following sections helps you achieve optimal use of the Oracle Financial Services Alert Management UI:

- Common Screen Elements

- Using the Browser

- Navigating in Oracle Financial Services Alert Management

- Message pages

Common Screen Elements

The following section describes the common screen elements in the Oracle Financial Services Alert Management UI.

Figure 87. Common Screen Elements

Common screen elements are those elements that consistently perform the same type of function in the same way when they display in the UI. Some serve as labels and never change (Matrix header); some enable you to get help or complete a task (buttons); some offer an explanation for a specific item (tool tips); and some operate as variables that allow you to type entries (text boxes) and make selections (drop-down lists).

Masthead

The masthead displays at the top of the page and contains the following components:

- Navigation Bar as Menus
- Session Information with session user name, day, and date.
- Help Button

Buttons

Buttons on the Oracle Financial Services Alert Management UI enable you to perform tasks such as executing and canceling actions or commands. Click a button to complete the desired task.

Task Buttons

Task buttons display throughout Oracle Financial Services Alert Management and include the following:

- The **Search** and **Advanced Search** buttons display on the Search & List page of the Monitoring workflow to filter data based on the criteria you set with basic filters and advanced additional filters respectively.

- The **Save** button records actions and navigates you to the appropriate page and displays the updated alert information accordingly.

- The **Save & Attach** button records actions and navigates you to a page providing the option to attach a document with the action. Once you complete the attachment you are navigated to the appropriate page and the alert information is updated accordingly.

- The **Set Values/Next** button displays only when taking the Promote to Case - Multiple Alert to Multiple Cases (MAMC) action. It saves any values entered on the global case information screen for all cases and navigates you to the first case of the multiple cases being created with all the global values entered pre-populated. This action is only available if your firm has implemented Oracle Financial Services Enterprise Case Management.

- The **Next** button displays only for Promote to Case - (MAMC) option. It allows you to by-pass setting any global case information and allows you to enter specific case information for each alert being promoted to a case. As with the **Set Values/Next** button, this action is only available if your firm has implemented Oracle Financial Services Enterprise Case Management.

- The **Clear** button displays on those actionable sections of the UI which do not display any pre-populated data. It clears the data entered by you when clicked.

- The **Reset** button displays on those actionable sections of the UI which display some pre-populated data. It discards the data entered by you and resets the contents to their original state.

- The **Cancel** button displays on all the actionable sections of the UI and cancels the action you intend to take and closes the action pop-up window.

- The **Send** button displays in the email pop-up window and sends the email to the addressed parties.

- The **Create** button in the Create Alert workflow displays fields for you to enter data for the new alert being created.

- The **Designate Trusted Pairs** button displays on specific transaction building blocks in the Details page and provides you with a pop-up window to create trusted pairs.

- The **Related to Focus** button displays in some specific business tabs where this information is available. It refreshes the tab details to replace the Related to Alert information with what is often a broader set of information that is applicable to the focus of the alert and not limited to just the activity of the alert.

- The **Related to Alert** button in specific business tabs does not display by default. The **Related to Alert** button replaces the **Related to Focus** button once the **Related to Focus** button is clicked. Selecting **Related to Alert** refreshes the tab information to display information that is applicable to the alert activity only.

- The **Add** button displays in the Financials tab and in the Evidence tab. It provides you with a pop-up window to add a new piece of information.

- The **Edit** button displays in the Financials tab, Narrative tabs. It provides you with a pop-up window to edit the existing piece of information you have chosen for edit.

- The **Remove** button displays in the Financials tab, and in the Attachment List matrix present in the attachment section of the Evidence tab. It also display in the Financials tab. It helps you delete information that you think is not relevant.

- The **Update** button displays in the Suppression Rule List and Trusted Pairs List. It provides you with a UI to modify a suppression rule or trusted pairs with appropriate comments.

- The **End** button displays in the Suppression Rule List and provides you with a UI to end a suppression rule.

- The **History** button displays in the Financials tab, Manage Suppression Rules and Manage Trusted Pairs workflow. It provides you with a detailed account of previous activities on the selected record.

- The **Go** button displays in all the Search bars Alert/Manage Suppression Rule /Manage Trusted Pairs and performs the search function. It also displays in the various action pop-up window. In the action pop-up window, the **Go** button helps display the appropriate fields as per the actions you have selected.

Action Buttons

The Action buttons display in the Search & List page and in the Details page. Each of these buttons provides you with an action pop-up window for taking actions in the category these buttons are representative of. These include buttons for each action category:

- Reassign
- Actions
- Disposition
- Review
- Regulatory Reporting
- email
- Export
- Evidence
- Excel

Help Button

A **Help** button, in the form of a question mark, displays to the extreme right of the bread crumbs. Click **Help** to get the following:

- More detailed information about the page

- Explanations of the screen elements

- How to perform instructions on a task that you want to perform

Calendar Button

A **Calendar** button displays when you have the option of selecting a date. For example, you can specify a date range to search for closed alerts. If you click **Calendar** icon, a calendar of the current month displays and highlights the current date.
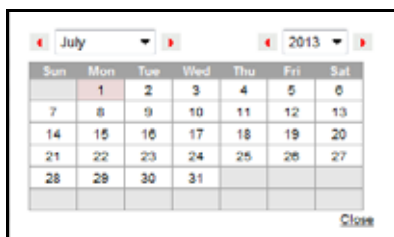
Figure 88. Calendar Button

To use the Calendar window to select dates, follow these steps:

1. Select a date. The application will automatically enter the selected date in the date field.

2. Click the arrows at the top of the Calendar window to view other months or years.

3. Click the **Close** link to close the calendar without selecting a date.

Expand/Collapse

You can view the complete information in a section, matrix, and field by using various expand or collapse options.

Column Expand All

When values are displayed in a matrix and there are columns which have lengthier values, then you can use the drag option to expand each column. This displays the entire value.
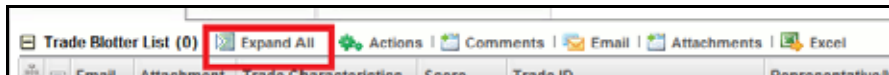
Figure 89. Column Expand All Button

Column Collapse All

When values are displayed in a matrix and there are columns, which have lengthier values, then you can use the **Column Collapse All** button to collapse all the values that are already expanded for display, together at once.
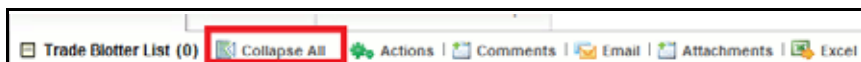
Figure 90. Column Collapse All Button

Section Expand Button

If you want to expand a section on a page, you can click the **(+)** button displayed at the top left corner of the section. This expands the section and all the fields in the section are visible.
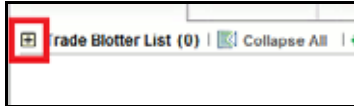
Figure 91. Section Expand Button

Section Collapse Button

If you want to collapse a section, which is already expanded, you can click the **(-)** button displayed at the top left corner of the section. This collapses the section and all the fields in the section are hidden.
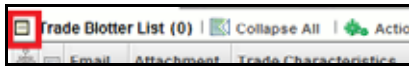
Figure 92. Section Collapse Button

Field Types

The following sections describe field types.

Text Area

A multi-line rectangular box in which you can type text, such as alert comments. If the box already contains text, you can select the default text or delete it and type new text. You can type as many characters in this box as desired.

Text Box

A single-line rectangular box in which you can type text. If the box already contains text, you can select the default text or delete it and type new text. Text boxes can limit the number of characters that you can enter. If so, the text box will show the maximum number of characters you can enter.

Wildcard Text Box

Oracle Financial Services Alert Management permits the use of wildcards in specific text boxes. If you do not know all of the information to type into the text box field, you can type a wildcard character for the missing part of the information. Oracle Financial Services Alert Management recognizes the percent sign (%) and underscore (_) as wildcard characters. You can use the wildcard character at the beginning, end, and anywhere within a string.

The more specific you are when using the wildcard character, the fewer extraneous matches Oracle Financial Services Alert Management returns. For example, if you specify a last name of `Sm%`, Oracle Financial Services Alert Management can return 100 matches, but if you specify a last name of `Smit%`, Oracle Financial Services Alert Management can return only 17 matches.

Context-Sensitive Text Box

Oracle Financial Services Alert Management permits the use of context-sensitive input in specific text boxes. If you want to perform a search on multiple values, you can enter a string of comma-separated values in the Alert/Suppression Rule/Trusted pairs ID search fields.

Drop-down List

A list of items from which you can select one item. Selecting the blank (empty) option applies no filter to your selection.

Selection Box

A list from which you can choose multiple items by selecting the check box against each item. Checking the value *Select All* represents the selection of all the values available in the selection box. Un-checking the value *Select All* represents the de-selection of all the values in the selection box.

Check Box

A square box that displays beside an item or option. Select the check box once to place a check mark in the box. Select the check box again to clear it.

ToolTips

A ToolTip displays when you position the mouse cursor over an abbreviated field, usually indicated by an ellipsis, or a column label in the Oracle Financial Services Alert Management UI. A Tooltip displays for approximately three seconds and provides the definition or other pertinent information for the abbreviated field or column label.

Using the Browser

The browser cache does not completely refresh the data. Therefore, using keys from keyboards, like Ctrl+Left arrow or Backspace keys for backward navigation, and Ctrl+ Right arrow keys for forward navigations displays data that can be outdated. Using Oracle Financial Services Alert Management navigation, pages are refreshed so the information is always up-to-date.

Navigating in Oracle Financial Services Alert Management

The following sections describe the navigation features that you can use to navigate within Oracle Financial Services Alert Management.
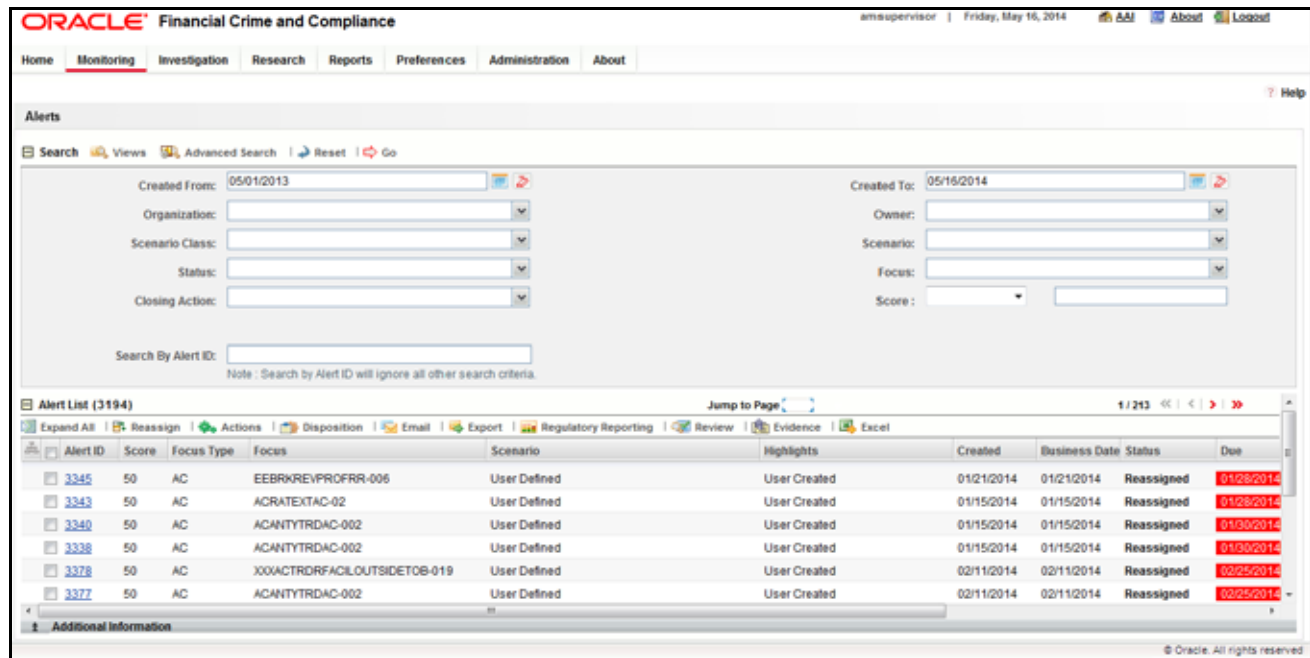
Figure 93. Navigation Features

Navigation features enable you to move easily between pages in the UI to view, analyze, or research alerts and focuses while working in Oracle Financial Services Alert Management.

Navigation Menus

The Navigation menu displays in the upper left corner of the page. The Navigation menu option includes: Home, Monitoring, Reports, and Administration. Menu options display as per your user role. Refer to *User Privileges* for more information on access to Oracle Financial Services Alert Management features based on role.

Links

Links display as hypertext (underlined text) on the page that, when clicked, takes you to other pages within the Oracle Financial Services Alert Management UI.

Search Bars

Some Oracle Financial Services Alert Management pages have a *Search bar* that allows you to specify values with which to filter and sort your data. Search bars for a specific page are described in the chapter where that page's use is explained. Refer to section *Accessing Alert Details page* for more information.

Page Context Controls

Page context controls (also called bread crumbs) show your location in Oracle Financial Services Alert Management. They allow you to navigate back to the previous page to a particular workflow. The current workflow displays the current entry in the page context controls.

Business Tabs

In Oracle Financial Services Alert Management, business data tabs display in the Alerts workflow after you have accessed an alert.

The business data tabs that display are dependent on the focus and the scenario class of the alert you are viewing and your role in Oracle Financial Services Alert Management.

Business data tab pages display detailed information about a business entity. Depending on the type of business entity being displayed (for example, Account, Customer), the content of the tab is different and specific to that type of entity.

Paging

Paging refers to the mechanism on the page that enables you to move through multiple pages of information (alerts, transactions and so forth).

You can move forward and backward through the pages one at a time by clicking the back arrow to the left of the page text box (unless you are on page #1) or the forward arrow to the right of the total number of pages (unless you are on the last page).

You can directly navigate to a page by entering the page number you wish to navigate to in the Jump to page box and clicking the **Enter** key.

Some pages within Oracle Financial Services Alert Management display only an initial, limited set of information on first navigating to that page. This information is often displayed in a tabular matrix at the top of the page. Additional information relevant to the page along with an LHS menu can be displayed by clicking one of the initially displayed records.

Message pages

Oracle Financial Services Alert Management describes the various types of error and status message pages that you can see in the application. Refer to Appendix F, *Message Pages* for an explanation of what causes the message pages to display and the appropriate way to handle them.

Message Pages

Oracle Financial Services Alert Management applications are Web-based and, therefore, you can occasionally see one or more of the following types of message pop-up windows apart from those directly related to the business function of the application. This section defines the following message types that are relevant to your activity within the application:

- **Error Messages:** Display to alert you that you have performed an activity that is not compatible with the application

- **Status Messages:** Display to alert you of the status of either your current activity or your access rights

- **Informational Messages:** Display to confirm actions you are taking or to warn you of additional requirements to be met to complete an action

Error Messages

The following error messages display to alert you that you have performed an activity that is not compatible with the application:

- Authentication Errors
- Multiple Session Errors

Authentication Errors

Authentication Error pages display if you enter an invalid user ID or password on the Login page.

Additionally, this type of message displays if you inadvertently type the correct login information with improper capitalization or with the Caps Lock key set, as passwords are case-sensitive. .

Figure 94. Authentication Error page

To reattempt your log in, click **OK** on the Authentication Error page.

Multiple Session Errors

If you try to login the application in a parallel browser when you have already logged into the application in another browser, the Multi Session Error displays. A parallel session is one which is improperly started by selecting **New/window** from the File menu in IE or by pressing the CTRL+N key and continuing to work in both sessions.

Figure 95. Multiple Session Error page

Clicking the **OK** button in the message will close the second browser.

In order to login to a second session in parallel with existing session, open a new browser, and select **File' New Session**. A second session opens that enables you to login. When working with two sessions, logout from one of the session does not affect the other session.

Status Messages

Status messages display to warn you that another user has locked an alert, case, suppression rule, or trade that you are trying to access.

The following items support the Lock feature:

- Alerts that are locked by another users.
- Suppression Rules creation
- Trade Blotter Rules Selection
- Watch List Management
- Cases that are locked by another users.
- Involved Party Creation

Alert/Case Locked

The Alert/Case Locked dialog box displays to let you know that the selected alert or case records are locked as a result of another user who is currently acting on an alert or a case you have selected.

If you have selected one or more alerts or cases to perform an action, and if another user is currently taking an action on all those selected alerts and cases, then the Alert/Case Locked dialog box displays with the following message:

- **When alerts are locked:** *All selected alert records are locked by another user. Please try again later.*
- **When cases are locked:** *All selected case records are locked by another user. Please try again later.*

If you have selected one or more alerts or cases to perform an action and if another user is currently taking an action on one or some of those selected alerts or cases, then the Alert/Case Locked dialog box displays with the following message:

- **When some alerts are locked:** *One or more Alerts are locked by another user. Select OK to continue, Cancel to return to the Alert List.*
- **When some cases are locked:** *One or more cases are locked by another user. Click OK to continue performing actions for cases which are not locked.*

If you have selected an alert or case which is already locked by another user, then clicking the **Alert ID** hyperlink to navigate to the Alert Details page displays the Alert/Case Locked dialog box with the following message:

- **When an alert is locked:** *The selected alert is locked by another user. Click OK to view the alert details page in view mode only and Cancel to return to list page.*
- **When a case is locked:** *The selected case is locked by another user. Click OK to view the case details page in view mode only and Cancel to return to list page.*

Informational Messages

The Informational messages display as a pop-up window either with the **OK** button, or with the **OK** and **Cancel** buttons. The following are a few instances where these messages display.

- If you do not enter information into a field which is required for an action to be performed

- A pre-save confirmation message asking you if you would like to save the actions you have chosen to perform

- A post-save confirmation message informing you whether the actions performed are successful or not

- A confirmation message if you choose to edit or remove a record

- If you have not selected an alert or business entity for an action to be performed

- If you choose to cancel an action which has not been saved

Informational messages help you successfully perform an action and warn you if you have missed certain steps required to complete an action.

Controlling Customer Error Messages

In the Controlling Customer chapter, if you add, modify, or add comments one or more Customers IDs, and either the security does not exist within the available Customers master table or you do not have access to the updated Customers IDs, the page displays one of the following error message:

Table 92 lists the error messages.

Table 92. Controlling Customer Error Messages

Workflow	Occurrence	Error Message
Update	If the user wants to update one or more Customer IDs or Security IDs for all the updated controlling records, but the new values entered are not available in the Customer table or Security table, or the user does not have access to that Customer ID.	Controlling Customer Record(s) are modified to reference Customer ID(s)/Security ID(s) that do not exist and will not be updated. Please check and enter again.
Update	If the user wants to update Customer list for some of the records Customer ID is invalid or the user doesn't have access to the modified Customer IDs.	Rec#, Rec# Controlling Customer Record(s) are modified to reference Customer ID(s) that do not exist and will not be updated. Click OK to proceed with changes. Click Cancel to modify your entries.
Update	If the user wants to update records, and modified records are duplicate of each other.	Some of the updated records are identical. Please check and enter again.
Update	If the user wants to update controlling records, and all entered records are duplicate of records already existing in database.	Controlling Record (s) that are modified are identical to existing records and will not be updated. Please check and enter again.
Update	If the user wants to update multiple controlling records, and some entered records are duplicate of records already existing in database.	Rec#, Rec# Controlling Customer Record(s) are identical to existing records and will not be updated. Click OK to proceed with changes. Click Cancel to modify your entries.
Add Comment	If user updates any selected record from the search list, enters comment text, and clicks on *Add Comment* instead of Update.	You are attempting to add comments only but some of the selected records are modified. Please use *Update* to save record modifications.
Add	If the user want to add a Customer ID which is not available with the system, or user does not have access to it.	Entered Customer ID value does not exist. Please check and enter again.
Add	If the user wants to add a Security ID which is not available with the system, user does not have access to it.	Entered Security ID value does not exist. Please check and enter again.

Security Restriction Error Messages

In the Update Securities Restriction area, if you modify one or more Security IDs, and either the security does not exist within the available Security master table or you do not have access to the updated Security IDs, the page displays an error message, as described in the following table.

Table 93. Securities Restriction Error Messages

Workflow	Occurrence	Error Message
Update	If the user enters Expiry date lesser than System date.	Please enter an Expiry date equal to or greater than the System date.
Update	If the user modifies one or more Security IDs such that all new values entered are not available in the Security table, or the user does not have access to the updated Security IDs.	Restriction Record(s) is modified to reference Security ID(s) that does not exist and will not be updated. Please check and enter again.
Update	If the user selects multiple security restrictions to update and enters values such that some of them pass validation as existing and accessible securities. However, for others either they do not have access to the security ID, or the security ID does not exist in the Security table.	Rec#, Rec# Restriction Record(s) are modified to reference Security ID(s) that do not exist and will not be updated. Click OK to proceed with changes. Click Cancel to modify your entries.
Update	If any two or more records updated by the user are identical to each other.	Some of the updated records are identical. Please check and enter again.
Update	If some of the updated records are duplicates and rest are fine (Rec # = rest rec id).	Rec#, Rec# Restriction Record ID(s) are identical to existing records and will not be updated. Click OK to proceed with changes. Click Cancel to modify your entries.
Update	If all the updated records are duplicates of already existing records in the database.	Restriction Record ID(s) that are modified are identical to existing records and will not be updated. Please check and enter again.
Add Comment	If the user updates any selected record from the search list, enters comment text, and clicks on 'Add Comment' instead of Update.	You are attempting to add comments only but some of the selected records are modified. Please use 'Update' to save record modifications.
Add	If the user enters a Security ID which is not available with the system, or if the user does not have access to it.	Entered Security ID value does not exist. Please check and enter again.
Add	If the User enters data in identical to the existing record in DB.	The entered Security Restriction already exists. Please check and enter again.

Security within Oracle Financial Services Alert Management

Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) uses six layers of security to control data access as defined in Table 94. You can view an alert if your combination of access controls authorizes you to viewthe alert and business information. Contact your system administrator for details about your access control permissions.

Table 94. Access Controls

Security Layer		
Type	**Controls**	**Description**
Roles	Features and Functions	This security layer identifies the features and functions you can perform within the Oracle Financial Services Solution Sets.
Organizations	Alert Information	This security layer enables your firm to restrict access using your firm's organizational hierarchy. To ensure accurate reporting, all users must be assigned one *primary organization*; however, a user can be assigned multiple viewable associations. To see an alert owned by an organization or by the users within an organization, you must have viewable rights to that organization.
Scenarios	Alert Information	This security layer enables your firm to restrict access by specific business problems (that is, scenarios). To see a linked alert generated by a scenario, you must have rights to view the scenario that generated the alert. To see a multi-match alert that is generated by several scenarios, you need rights to view at least one of the scenarios that generated the alert.
Domains	Alert and Business Information	This security layer enables your firm to restrict access along operational business lines and practices. You can only see entities and alerts that are assigned to at least one of the same business domains. Entities and alerts can have multiple domains.
Jurisdictions	Alert and Business Information	This security layer enables your firm to restrict access using geographic locations. You can only see entities and alerts that are assigned to the same jurisdictions.

APPENDIX H   *Calculating Risk*

Oracle Financial Services Alert Management uses risk calculations as part of managing sensitivity when detecting behaviors of interest in Money Laundering and Fraud scenarios. Risk Information can be provided through watch list or an attribute of the record provided to the ingestion manager for given customers and accounts.

Based on several risk inputs, Oracle Financial Services Alert Management calculates effective risks for business entities and calculates both Party Risk and Activity Risk on Transactions and Settlement Instructions.

Figure 96 displays the basic flow of the calculation.
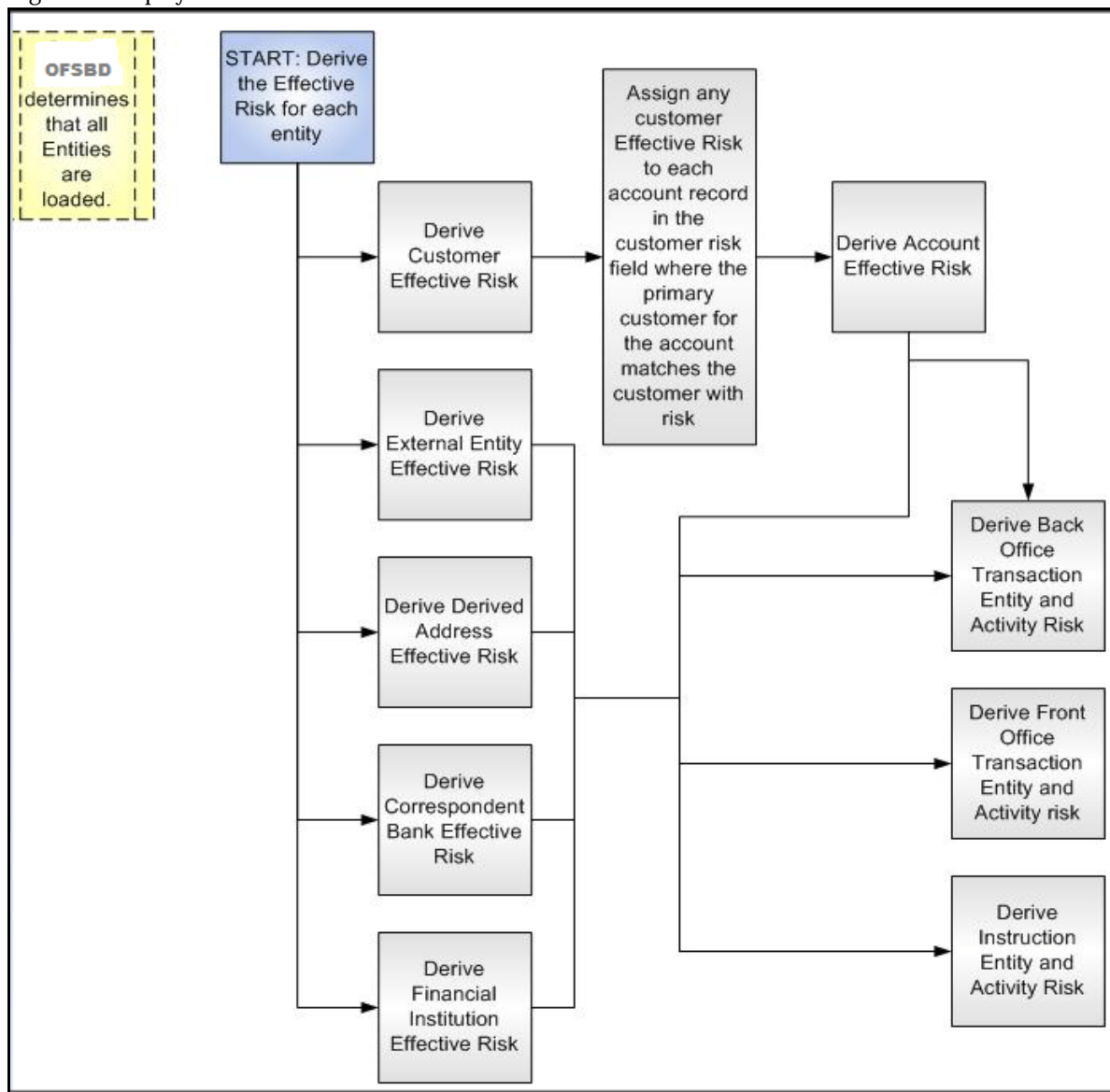
Figure 96. Risk Derivation-Overview

In addition to risk, Oracle Financial Services Alert Management supports the concepts of Exempt Entities and Trusted Entities. These concepts are discussed in more detail in section *Watch Lists*. In brief, Exempt Entities are those that should not be alerted in Anti-Money Laundering scenarios. Trusted entities are those that meet specific criteria which demonstrates that they are more trustworthy than the general population.

Risk levels use a ten-point scale, with one representing moderate risk and ten representing highest risk. Entities that have no known risk receive a risk score of zero.

Determining Entity Risk

Oracle Financial Services Alert Management clients can provide risk factors for business entities through the Oracle Financial Services Data Interface Specification (DIS). The risk can be assigned to the same business entity in the several ways. The Ingestion Manager resolves across these various risks to create an Entity Effective Risk.

Figure 97 reflects the basic flow for deriving Entity Effective Risk.
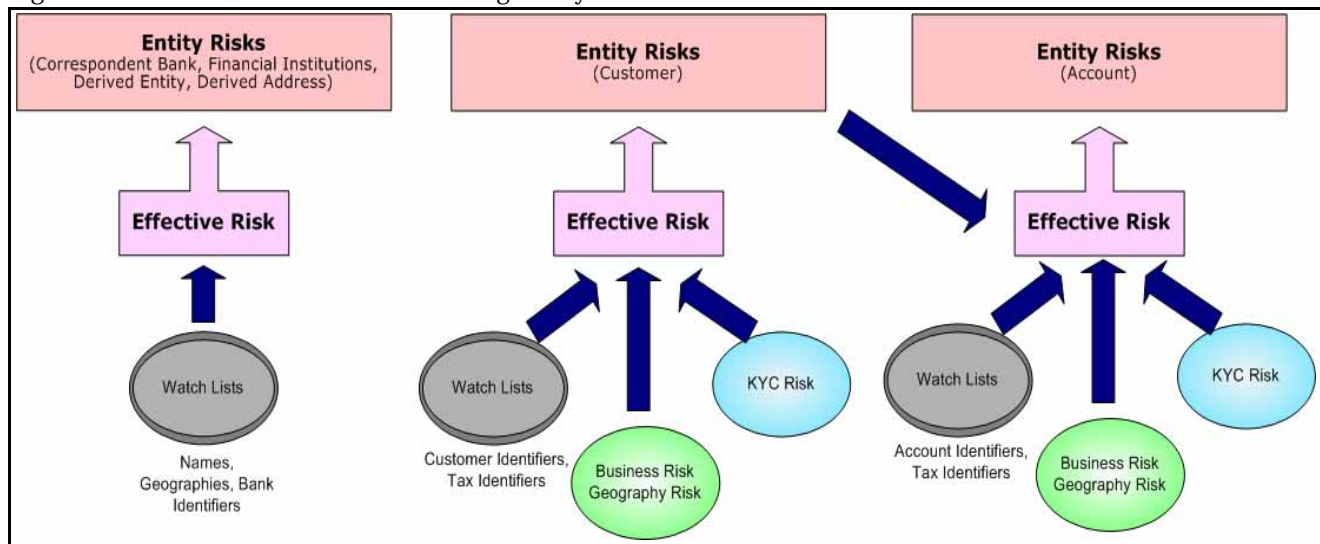
Figure 97. Entity's Effective Risk

Oracle Financial Services Alert Management derives risk on the following business entities:

- Customers
- Accounts
- Financial Institutions
- Correspondent Banks
- Derived Addresses
- Derived Entities (Names)
- Derived Entities (Identifiers)

The client can provide risk information directly through the Account and Customer input files as specified in the DIS. Accounts and Customers can also receive Know Your Customer (KYC) risk information through the Account Supplemental Attributes and Customer Supplemental Attributes DIS files. All of the business entity types can receive risk information through watch lists.

When determining an entity's effective risk, the approach to resolving across multiple sources of risk varies based on the entity type. The general rules to follow are:

- Watch List risk has higher priority than other risk factors.

- Exemption and Trust take priority over risk.

- More specific risk factors are preferred over less specific risk factors (for example, risk associated with an Identifier is more specific than risk associated with a Name).

Derivations of Customer, Account, and Correspondent Bank Effective Risk are the most complex. The following sections outline the rules for these derivations.

Deriving Customer Entity Risk

Customer records can provide risk through the following distinct mechanisms:

- Business Risk or Geography Risk provided in the Customer DIS file

- KYC Risk provided in the Customer Supplemental Attributes DIS file

- Watch List entries matching the Customer ID or Customer's Tax ID

If the Customer has any Watch List risk information, then the Customer's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Customer, then the Effective Risk is derived as the highest of Business Risk, Geography Risk, and KYC Risk. KYC Risk can be provided as either Trust or Exclusion. If that is the case, the KYC trust is selected over positive risk factors in Business Risk or Geography Risk.

Deriving Account Entity Risk

Account records can provide risk through the following distinct mechanisms:

- Business Risk or Geography Risk provided in the Account DIS file

- KYC Risk provided in the Account Supplemental Attributes DIS file

- Watch List entries matching the Account ID or Account's Tax ID

Accounts can also inherit risk from the Primary Customer identified on the Account. This risk is referred to as Account Customer Risk. Accounts inherit the Effective Risk from the Primary Customer as it is calculated using the rules described in Deriving Customer Entity Risk with the following exceptions:

- If the Customer's Effective Risk was driven by KYC risk, then the Account processing re-calculates the Customer's effective risk, ignoring KYC risk on the Customer. The reason for this is that the Account's risk factors are part of the Oracle Financial Services KYC product's risk derivations, so propagating that risk back to the Account is not productive. If the Customer's Effective Risk was driven by KYC, then the Account uses the highest of the Customer's Geography and Business risks as the Account Customer Risk.

- There is a configurable parameter in the Ingestion Manager to determine whether or not Trust and Exclusion should be inherited from the Customer record. If this is configured to NOT inherit this effective risk and the Customer's Effective Risk indicates Trust or Exclusion, then the Customer's risk is not considered when determining the Account Effective Risk.

If the Account has any Watch List risk information, then the Account's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Account, then the Effective Risk is derived as the highest of Business Risk, Geography Risk, KYC Risk, and Account Customer Risk.

Deriving Correspondent Bank Entity Risk

Correspondent Bank records can derive risk information through the following distinct mechanisms:

- Watch List entries matching the Correspondent Bank ID

- Watch List entries matching the Correspondent Bank Name

- Watch List entries matching the Correspondent Bank Address

If the Correspondent Bank has any Watch List risk information, then the Correspondent Bank's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Correspondent Bank identifier, then the Effective Risk is derived based on matching Watch List risk information pertaining to the Correspondent Bank name. If there is no Watch List risk information on the Correspondent Bank name, then the Effective Risk is derived based on the matching of the Correspondent Bank's address information to Watch List entries.

Watch Lists

A Watch List is a list of entities that have known risk characteristics. Watch Lists can represent public sources or can be created and managed internally by the institution. Common public sources for watch lists include Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF). The types of entities provided on Watch Lists include:

- Identifiers (for example, SSN, Tax ID, and Passport ID)

- Organizations (for example, business name, SWIFT code, and ABA number)

- Accounts (for example, internal or external accounts)

- Persons (for example, personal name)

- Geography (for example, countries, state, city, postal code, and address)

- Combined Names and Geography

Refer to the *Data Interface Specification* for more information on Watch Lists and Watch List Entries.

Oracle Financial Services Alert Management categorizes Watch Lists into the following types:

- **Exempted Watch List:** Entities on Exempted Watch Lists are highly trusted clients on whom no Money Laundering alerts will be generated.

- **Trusted Watch Lists:** Entities on Trusted Watch Lists are known to be highly trustworthy. Certain scenarios can be configured to exclude trusted entities from monitoring.

- **Risk Watch List:** These are the entities that carry a risk value indicating that they should be monitored more closely than the general population. Money Laundering scenarios allow for separate threshold values to be set when monitoring entities with a certain risk level. Risk lists are risk weighted using values ranging from one (lowest risk) to ten (highest risk).

NOTE: There is no risk list with a risk level of zero. Risk level zero is reserved to indicate that there are no known risk factors to consider. It is also the default risk level for all entities in Oracle Financial Services Alert Management.

The matching criteria of Watch List Entry are as follows:

- All ID entries on a Watch List require an exact match to an entity .

- All Name entries on a Watch List require an exact or a fuzzy match to an entity .

- Addresses can be matched to watch list entries at multiple levels (for example, the same address can match one watch list entry for a Street Address and can match a separate entry for a Country)

For each Watch List match to an entity, a List Membership Record is created, which includes the following:

- ID of Watch List matched

- Date when the entity was added to the Watch List

- Date when the entity was removed from the Watch List

- Watch List entry that was matched

- Type of Watch List Entry that was matched

Fuzzy name matching is a technique to account for normal variations in names and still successfully match the names against watch lists. For more information on configuring Fuzzy Name Matching within Oracle Financial Services Alert Management, refer to the *Administration Guide.*

Determining Watch List Risk

Oracle Financial Services Alert Management defines each reference entity with an adjudicated Watch List Risk. An entity's Watch List Risk is determined through a hierarchy of rules as follows:

- If an entity is a member of a Watch List of type Exempt, then the Watch List Risk value is -2. This value is not displayed; it is used for internal processing.

- If an entity is a member of a Watch List of type Trusted, then the Watch List Risk value is -1. This value is not displayed; it is used for internal processing.

- If an entity is matched to multiple entries on one or more Watch Lists, the match that is the *most specific* is used to drive risk. The order of preference is:

  1 ID match

  2 Exact Name match

  3 Fuzzy Name match

  4 Street Address match

  5 Postal Code match

  6 City match

  7 State/Province match

  8 Country match

  Not all entity types can match multiple types of watch list entries. For example:

  - Accounts and Customers only match identifiers.

  - Correspondent Banks can match either IDs, Names, or Addresses.

- Addresses can match at different granularities, ranging from Country to the specific street address.

- If multiple risk lists are matched with the same specificity, then the final Watch List Risk is the highest of the risks of the entities matched at the same level.

NOTE: All matches are retained and stored in List Membership Records associated with the entity.

Determining Risk on Transactional Data

After Effective Risk is derived for Entities, this risk is reflected on instructions and transactions. The risk is generally calculated for each party on the transaction and stored as a Party Entity Risk. The Entity Risks of each party is then used to calculate an Activity Risk for each party. Activity Risk is an assessment of the risk level of the activity in which that party has engaged. As such, that party's own Entity Risk is not considered when calculating the Activity Risk for the party.

The derivations for Party Entity Risk vary by the transaction type.

Determining Front Office Transaction Party Entity Risk

Front Office transactions contain the following distinct sources of risk for any one party:

- Party ID
- Party Name
- Party Location

As a general rule, Oracle Financial Services Alert Management uses the most specific risk factor possible when setting the Party Entity Risk. As such, risk information about the Party ID is considered more reliable than risk information about the Party Name or the Party Location. The Ingestion Manager can be configured to automatically accept the Party ID Risk only when it is above a certain threshold (this defaults to zero, meaning that non-zero Party ID Risk is always accepted as the Party Entity Risk).

For each Party, a Geography Risk is calculated using Watch List information as described in the section *Watch Lists.*

Party Entity Risk is determined by a hierarchy of rules as follows:

- If the Party ID Effective Risk is Trusted or Exempt, then set Party Entity Risk to the Party ID Effective Risk.

- If the Party ID Effective Risk is > *Party ID Win Threshold*, then set Party Entity Risk to Party ID Effective Risk.

- If the Party Name combined with the Party Location matches a combined Name-Location Watch List record that represents Trust or Exclusion, then set the Party Entity Risk to the combined Name-Location and Trust-Exemption level.

- If the Party Name combined with Party Location matches a combined Name-Location Watch List record that represents Risk, then set the Party Entity Risk to the HIGHER of the Party ID Effective Risk and the combined Name-Location Risk level.

- If the Party Name Effective Risk alone is Trusted or Exempt, then set the Party Entity Risk to the Trust-Exemption level of the Name.

● If the Party Name Effective Risk indicates risk, set the Party Entity Risk to the HIGHER of the Party ID Effective Risk and the Party Name Effective Risk.

● If the Party Geography Risk is Trusted or Exempt, then set the Party Entity Risk to the Trust-Exemption level of the Geography.

● Set the Party Effective Risk to the HIGHER of the Party ID Entity Risk and the Party Geography Risk.

The Party Entity Risk is calculated for every party on each Front Office Transaction. This value displays when showing Front Office Transactions in the UI. This value is then used to calculate Party Activity Risk for each party on the transaction. Refer to section *Determining Activity Risk on Front Office Transactions* for details on the calculation of Party Activity Risk for Front Office Transactions.

Determining Back Office Transaction Party Entity Risk

Back Office Transactions contain only two parties, the Account that is the focus of the activity and the Offset Account involved in the transaction. As these are both Identifiers, setting the Party Entity Risk for Back Office Transactions is propagating the Account Effective Risk values for the related accounts to the transaction.

Determining Settlement Instruction Party Entity Risk

Based on how Settlement Instructions are used in scenarios, the processing of parties is handled somewhat differently than Front Office Transactions. Although there are multiple parties on a Settlement Instruction, there is only a Party Entity Risk calculated for the Account holding the Instruction. The processing is, therefore, simply to propagate the Account's Effective Risk to the Settlement Instruction Entity Effective Risk.

Determining Activity Risk

Activity Risk identifies the risk of the Activity as seen from the viewpoint of each Party on a transaction. In general, the Activity Risk is the highest risk of the other parties on the transaction or of the transaction Channel or Product itself. As with calculating Party Entity Risk, the derivation of Party Activity Risk varies by transaction type.

Determining Activity Risk on Front Office Transactions

Front Office Transaction Party Activity Risk calculates risk separately from the point of view of each party on the transaction. The risk is intended to identify how risky the activity is independent of risk factors already associated to the Party through the Party Entity Risk. As such, on Front Office Transactions, the risk is calculated using the Party Entity Risk of the parties on the other side of the transaction. The general approach is to use the highest of the Channel Risk, Product Risk, and Party Entity Risk of the other parties. Channel and Product Risk are provided in the DIS file for Front Office Transactions.

Several party roles effect activity risk. The following sections describe the relationship between varying party roles and activity risk for transactions.

Table 95 displays the party role-activity risk relationship for an electronic funds transaction.

Table 95.Electronic Funds Transfer Transaction

Party Role	Roles impacting Activity Risk
Originator, Secondary Originator, Sending Bank	Intermediary Banks, Receiving Bank, Beneficiary, Secondary Beneficiary
Intermediary Banks	All roles except for the party for which the Activity Risk is being calculated
Receiving Bank, Beneficiary, Secondary Beneficiary	Intermediary Banks, Sending Bank, Originator, Secondary Originator

Cash Transaction

Table 96 displays the party role-activity risk relationship for the cash transaction.

Table 96.Cash Transaction

Party Role	Roles impacting Activity Risk
Originator	Location, Conductor
Location	Conductor, Originator, or Beneficiary
Conductor	Location, Originator, or Beneficiary
Beneficiary	Location, Conductor

NOTE: A Cash Transaction record can have an Originator or a Beneficiary, but not both.

Monetary Instrument and Check Transactions

Table 97 displays the party role-activity risk relationship for the monetary instrument and check transactions.

Table 97.Monetary Instrument and Check Transactions

Party Role	Roles impacting Activity Risk
Remitter, Issuing Institution	Depositing Institution, Clearing Institution, Beneficiary, Secondary Beneficiary, Conductor
Clearing Institution	Remitter, Issuing Institution, Depositing Institution, Beneficiary, Secondary Beneficiary, Conductor
Depositing Institution, Beneficiary, Secondary Beneficiary	Remitter, Issuing Institution Clearing Institution, Conductor
Conductor	Remitter, Issuing Institution, Clearing Institution, Depositing Institution, Beneficiary, Secondary Beneficiary

Determining Activity Risk on Back Office Transactions

Activity Risk on Back Office Transactions is only calculated for the Account that is the focus of the activity. Since the only other risk factors available are the Offset Account's Effective Risk and the Channel and Product Risks provided on the transaction, the Activity Risk is calculated as the highest of these factors.

Determining Activity Risk on Settlement Instructions

The Activity Risk calculated for Settlement Instructions is from the point of view of the Account holding the instructions. Calculating Activity Risk on Settlement Instructions follows a similar approach as Front Office Transactions whereby the Entity risk is calculated for each party and then used to calculate Activity Risk; however, on Settlement Instructions, the Entity Risks for each party are not stored. The Entity Risks are calculated as follows:

Destination Customer Entity Risk

The Destination Customer Entity Risk is calculated using the following hierarchical rules:

1. If the Destination Customer Account Effective Risk is non-zero, then set the Destination Customer Entity Risk to Destination Customer Account Effective Risk.

2. If the Destination Financial Institution Effective Risk is non-zero, then set the Destination Customer Entity Risk to Destination Financial Institution Effective Risk.

3. If the Destination Customer Name Risk ≥ Destination Financial Institution Name Risk, then set the Destination Customer Entity Risk to Destination Customer Name Risk.

4. If the Destination Financial Institution Name Risk > Destination Customer Name Risk, then set the Destination Customer Entity Risk to Destination Financial Institution Risk.

5. Set the Destination Customer Entity Risk to zero (0).

Physical Delivery Party Entity Risk

The Physical Delivery Party Entity Risk is calculated using the following hierarchical rules:

1. If the Physical Delivery Account Effective Risk is non-zero, then set the Physical Delivery Party Entity Risk to Physical Delivery Account Effective Risk.

2. If the Physical Delivery Financial Institution Effective Risk is non-zero, then set the Physical Delivery Party Entity Risk to Physical Delivery Financial Institution Effective Risk.

3. If the Physical Delivery Geography Risk is non-zero, then set the Physical Delivery Party Entity Risk to the Physical Delivery Geography Risk.

4. Set the Physical Delivery Party Entity Risk to zero (0).

The final Activity Risk setting on the Settlement Instruction is the highest level of the following risks:

- Destination Customer Entity Risk
- Physical Delivery Party Entity Risk
- Settlement Country Geography Risk
- Product Risk
- Channel Risk

This final Activity Risk is used in scenarios to determine the risk level of the Settlement Instruction without regard to the risk factors inherent in the Account holding the Instruction.

APPENDIX I   *Trade Blotter List Component Matrix*

This appendix provides a detailed table that lists all possible fields that can display on the Trade Blotter List Details page by the user interface section and the product category specified on the Trade Blotter Search page.

Table 98: Trade Blotter List Components by UI Section and Trade Product Category

Column	Description	User Interface Section									Trade Product Category									Standard Configuration
		Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	
Trade Characteristics	Abbreviated text that describes any special criteria with which that trade is associated; for example, EA represents Employee Account. A hover over displays the full text.	X									X	X	X	X	X	X	X	X	X	X
Score	Score associated with the trade.	X									X	X	X	X	X	X	X	X	X	X
Trade ID	Trade identifier for the trade.	X	X								X	X	X	X	X	X	X	X	X	X
Trade Date	Date, time and time zone in which the trade was executed.		X								X	X	X	X	X	X	X	X		X
Currency Pair	Security short name.		X				X								X					X
Deal Trade Date	Original date that the structured deal was negotiated.		X																X	X
Desk ID	Identifier of the desk that performed the trade.		X								X	X	X	X	X	X	X	X	X	X
Subdesk ID	Identifier of the sub-desk that performed the trade.		X								X	X	X	X	X	X	X	X	X	X
Executing Organization ID	Identifier of the organization within which this trade execution was performed.		X								X	X	X	X	X	X	X	X	X	X
Post Position	Tracer Post Position. Number of units of this security held in the trading account associated with this trade execution immediately after the execution was performed.		X								X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
		User Interface Section									Trade Product Category									
Security Short Name	Short name of the security that was traded.	X	X				X				X	X	X	X		X	X	X	X	X
Security ID	Identifier of the security that was traded.		X								X	X	X	X		X	X	X	X	X
Security Description	Description of the security that was traded.		X								X	X	X	X		X	X	X	X	X
Foreign Exchange Type	Deal Type 1 and 2. Oracle Alert Management client-specified general type of the structured deal.		X												X					X
Foreign Exchange Description	Description of the structured deal (or swap) that the Oracle Alert Management client can use to identify specific information about the structured deal (or swap).		X												X					X
Security Alternate Name	Alternate name of the security.		X											X						X
Product Category	Product category designation for the security associated with this trade.	X	X								X	X	X	X	X	X	X	X	X	X
Product Type	Product type designation for the security associated with this trade.		X								X	X	X	X	X	X	X	X	X	X
Product Subtype	Product subtype designation for the security associated with this trade.		X								X	X	X	X	X	X	X	X	X	X
Trade Purpose	Purpose for which this trade was executed.		X								X	X	X	X	X	X	X	X	X	X
Trader Buy/Sell	Trader Buy/Sell. Indicates whether the trader is buying or selling the security.		X																	
Buyer	Buyer identifier and type		X								X		X	X	X	X	X	X	X	X
Seller	Seller identifier and type		X								X		X	X	X	X	X	X	X	X
Market Center	Market center on which the trade was executed.		X								X			X						X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
Quantity	Total number of units of the security (for example, shares, contracts, or face value) that were traded.	X	X								X	X	X	X		X	X	X		X
Price (Base)	Price at which the security was traded (buy or sell) as expressed in base currency.		X								X	X	X	X	X	X	X	X	X	X
Price (Issuing)	Price at which the security was traded (buy or sell) as expressed in the issuing currency.	X	X								X	X	X	X	X	X	X	X	X	X
Price (Traded)	Last activity price for the trade.		X								X	X	X	X	X	X	X	X	X	X
Price (Settle-ment)	Trade price expressed in the currency in which the trade is to be settled.		X								X	X	X	X	X	X	X	X	X	X
Commission (Base)	Monetary amount of the broker commission associated with this trade, expressed in base currency.		X									X	X	X	X	X	X	X	X	X
Commission (Issuing)	Monetary amount of the broker commission associated with this trade, expressed in the issuing currency.		X								X	X	X	X	X	X	X	X	X	X
Principal (Base)	Principal amount of the trade as expressed in base currency.		X									X	X	X	X	X	X	X	X	X
Principal (Issu-ing)	Principal amount of the trade as expressed in the issuing currency.	X	X								X	X	X	X	X	X	X	X	X	X
Principal (Traded)	Principal amount of the trade as expressed in the currency in which the trade was executed.		X									X	X	X	X	X	X	X	X	X
Principal (Settle-ment)	Principal amount of the trade as expressed in the currency in which the trade is to be settled.		X									X	X	X	X	X	X	X	X	X
Coon	The interest rate paid for the security.		X														X	X		X
Yield	For fixed income products, the rate of return on this security.		X										X					X		X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
											Trade Product Category									
Gross Amount	Principal amount of the trade expressed in the issuing currency plus the commission associated with the trade expressed in the issuing currency.	X									X	X	X	X	X	X	X	X	X	X
Settlement Date	Date on which the trade is to settle.	X									X		X	X	X	X	X	X		X
Settlement Value	For Foreign Exchange trades, the value of the trade on Value Date.	X													X					X
Settlement Country	Last known value for the country in which this trade was settled.	X											X						X	X	X
Conversion Ratio	Number of units (for example, shares) of the instrument that can be obtained by converting each single unit of the convertible security.	X																X	X		X
Conversion Price	Price per share for which investors can exchange the convertible security.	X																X	X		X
Swap Type	Deal Type 1 and 2. Type of this structured deal.	X																		X	
Swap Description	Description of this structured deal (or swap) that the Oracle Alert Management client can use to identify specific information about the structured deal (or swap).	X																		X	X
Legal Entity	Oracle Alert Management client's legal entity that is the principal in this structured deal.	X																		X	X
Customer ID	Identifier of the customer or counterparty involved in this structured deal.	X																		X	X
Source System	Source system from which this data content is extracted.	X																		X	X
Party 1 ID	Space-separated type and identifier of the first party involved in this swap.	X																		X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
Party 1 Account ID	Identifier of the account for the first party involved in this swap.		X																X	
Party 1 Payment Frequency	Expected frequency at which payments are to be made against this structured deal or swap (for example, daily or weekly).		X																X	X
Party 2 ID	Space-separated type and identifier of the second party involved in this swap.		X																X	X
Party 2 Account ID	Identifier of the account for the second party involved in this swap.		X																X	
Party 2 Payment Frequency	Expected frequency at which payments are to be made against this structured deal or swap (for example, daily or weekly).		X																X	X
Effective Date	Effective date on which the deal started.		X																X	X
Term Date	Date on which the deal ended.		X																X	X
Interbank Exchange Rate	Interbank exchange rate.		X												X					X
Spot Exchange Rate	Spot exchange rate.		X												X					X
Trade Exchange Rate	Exchange rate at which the trade executions were executed.		X												X					X
Principal Amount (Counter)	For foreign exchange trades, the principal amount of the trade expressed in the counter currency of the currency pair. This value does not include commissions or fees associated with the trade.		X												X					X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	User Interface Section									Trade Product Category									Standard Configuration
		Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	
Principal Amount (Treasury)	Principal amount of the trade expressed in the currency in which the trade is to be settled. For foreign exchange trades, the principal amount of the trade expressed in the treasury currency. This value does not include commissions or fees associated with the trade.		X												X					X
Load	Type of load for this mutual funds security.		X									X								X
Load/Fee	Mutual fund load fee amount in this issuing currency.		X									X								X
NAV	Closing price, in the issuing currency, for this security in its primary market on this market date.		X									X								X
CDSC (Issuing)	Contingent Deferred Sales Charge amount in the issuing currency.		X									X								X
Contract Size	For option products, the quantity of shares of the underlying security for which this options contract is written.		X											X						X
Option Type	For option products, indicator of whether the option can be exercised at any time prior to maturity or can only be exercised at maturity.		X											X						X
Customer Buy/Sell	Customer buy or sell.	X	X								X	X	X	X	X	X	X	X	X	X
Agent ID	Identifier of the trader who acted as the agent on the execution (for agency trades).		X								X									X
Solicited	Indicator of whether a person affiliated with the Oracle client solicited this order.		X								X									X
Event Type	Trade event type associated with the trade.		X								X									X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
		User Interface Section									Trade Product Category									
Customer Name	Name of the customer who placed the order.						X				X									X
Account [Display] Name	Account display name of the account associated with the trade.	X				X					X	X	X	X	X	X	X	X	X	X
Investment Objective	Specific investment objective of the account associated with the trade.	X									X	X	X	X	X	X	X	X	X	X
Source of Funds	Source from which the initial funds will come as stated by the customer for the account associated with the trade.					X					X	X	X	X	X	X	X	X	X	X
Source	Investment rating service that is the source of the investment rating for the security associated with the trade.			X							X	X	X	X	X	X	X	X	X	X
Rating	Specific investment rating value determined by an investment rating service for the security that was traded (for example, A+, BBB, or CC-).			X							X	X	X	X	X	X	X	X	X	X
Effective	Date on which an investment rating service established this investment rating for the security associated with the trade.			X							X	X	X	X	X	X	X	X	X	X
Expires	Date on which an investment rating service removed this investment rating for the security associated with the trade.			X							X	X	X	X	X	X	X	X	X	X
Maturity	For fixed income products, the date on which the security matures.		X										X							X
CUSIP	Committee on Uniform Securities Identification Procedures (CUSIP) identifier associated with the security that was traded.		X								X	X		X		X				X
ISIN	International Securities Identification Number (ISIN) associated with the security that was traded.		X								X	X	X	X		X	X	X		X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
		User Interface Section									**Trade Product Category**									
Deal ID	Oracle Alert Management identifier for a particular structured deal associated with the trade.		X								X		X	X		X	X		X	X
Last Reviewed By	User who approved or rejected the trade (via Trade Blotter).		X								X	X	X	X	X	X	X	X	X	X
Organization Name/ID	Display name or identifier (configured at deployment) of the organization that originated the trade.		X								X	X	X	X	X	X	X	X	X	X
Account ID	Identifier of the customer's account involved in the trade, as last reflected in the events for the execution.	X				X					X	X	X	X	X	X	X	X	X	X
Account Type	Oracle Alert Management client-specified account type classification for the use of this account.					X					X	X	X	X	X	X	X	X	X	X
Registration	Registration Type. Oracle Alert Management client-specified form of legal ownership for the account that is associated with the trade.					X					X	X	X	X	X	X	X	X	X	X
Open Date	(Account) Date on which the account associated with the trade was opened.					X					X	X	X	X	X	X	X	X	X	X
Last Activity	(Account) Date of the last trading or transaction activity in the account that is associated with the trade.					X					X	X	X	X	X	X	X	X	X	X
Business Unit	(Account) For firm accounts, the identifier for the organization that owns the account.					X					X	X	X	X	X	X	X	X	X	X
Branch	(Account) Branch Code. Organization where the account is domiciled.					X					X	X	X	X	X	X	X	X	X	X
Tax ID	(Account) Tax identification number associated with the account that is associated with the trade.					X					X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
Risk Tolerance	(Account) Degree of risk the customer is willing to take with investments in this account (that is, the customer's ability to handle declines in the net worth of this account).					X					X	X	X	X	X	X	X	X	X	X
Customer ID	Customer associated with the account involved in the trade.						X				X	X	X	X	X	X	X	X	X	X
Tax ID	(Customer) Customer's tax identification number.						X				X	X	X	X	X	X	X	X	X	X
Type	(Customer) Indicator of whether this customer is an individual or organization.						X				X	X	X	X	X	X	X	X	X	X
Business Type	(CustomLinker) Functional area in which this customer does business						X				X	X	X	X	X	X	X	X	X	X
Date of Birth	Date on which the customer was born.						X				X	X	X	X	X	X	X	X	X	X
Broker/Dealer	Indicator of whether this customer has provided notification of employment by a financial institution.						X				X	X	X	X	X	X	X	X	X	X
Customer Effective Risk	Level of risk associated with this customer as determined in large part by membership on one or more watch lists.						X				X	X	X	X	X	X	X	X	X	X
Effective Match	Level of risk associated with this customer as determined in large part by membership on one or more Watch Lists plus text of the identifier or name associated with the Watch List record that was used to populate Watch List Risk for this customer.						X				X	X	X	X	X	X	X	X	X	X
Business Risk	Level of risk associated with the general business characteristics of this customer as determined by the Oracle Alert Management client.						X				X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	User Interface Section									Trade Product Category									Standard Configuration
		Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	
List	Identifier of the level of risk associated with a customer determined by membership on one or more watch lists.						X				X	X	X	X	X	X	X	X	X	X
Annual Income	Customers self-reported annual income, expressed in base currency.						X				X	X	X	X	X	X	X	X	X	X
Employee	Indicator of whether the customer is also an Oracle Alert Management client.						X				X	X	X	X	X	X	X	X	X	X
Estimated Liquid Networth	Customer's self-reported liquid assets, expressed in base currency.						X				X	X	X	X	X	X	X	X	X	X
Source of Wealth	Customer's self-reported source of wealth.						X				X	X	X	X	X	X	X	X	X	X
Marital Status	Marital status of the customer.						X				X	X	X	X	X	X	X	X	X	X
Occupation	Occupation of the customer.						X				X	X	X	X	X	X	X	X	X	X
Employer	Name of the customer's employer.						X				X	X	X	X	X	X	X	X	X	X
Credit Rating	Rating for this customer, based on credit rating score.						X				X	X	X	X	X	X	X	X	X	X
Credit Score	Actual score for the customer's credit rating, based on the credit rating score.						X				X	X	X	X	X	X	X	X	X	X
Credit Rating Source	Source associated with the credit rating assigned to the customer.						X				X	X	X	X	X	X	X	X	X	X
Citizenship	Customer's primary country of citizenship.						X				X	X	X	X	X	X	X	X	X	X
Order ID	Identifier of the order associated with the trade.							X			X	X	X	X	X	X	X	X	X	X
Order Placed	Date and time on which the order was placed.							X			X	X	X	X	X	X	X	X	X	X
First Routed	Date and time on which the order was first routed.							X			X	X	X	X	X	X	X	X	X	X
Order Filled	Date and time on which the order was completely filled.							X			X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
Order Buy/Sell	Indicator of whether an order is an instruction to buy or sell a security.							X			X	X	X	X	X	X	X	X	X	X
Originating Order Quantity	Original number of units of the security (for example, shares, contracts or face value) that were to be bought or sold through this order.							X			X	X	X	X	X	X	X	X	X	X
Last Order Type	Type of this order; for example, market or limit.							X			X	X	X	X	X	X	X	X	X	X
Limit Price	Price at which this limit order is to be executed, as expressed in issuing currency.							X			X	X	X	X	X	X	X	X	X	X
Buyer/Seller	Indicator for the type of buyer/seller for which the order was placed and the buyer/seller associated with the order.							X			X	X	X	X	X	X	X	X	X	X
Parent Order ID	Identifier that the Oracle Alert Management client assigns which uniquely identifies this order throughout the enterprise during the day in which it was performed.							X			X	X	X	X	X	X	X	X	X	X
Primary Representative ID	Primary representative identifier that is used by this employee.								X		X	X	X	X	X	X	X	X	X	X
Employee Name	Name to be displayed for this employee.				X				X	X	X	X	X	X	X	X	X	X	X	X
Representative/ Investment Advisor	Registered Representative/Investment Advisor name associated with the trade.	X									X	X	X	X	X	X	X	X	X	X
Primary Service Team ID	Identifier of the primary service team of which this employee is a member.								X		X	X	X	X	X	X	X	X	X	X
Central Registration Depository ID	For employees who must be registered with a regulator, the unique identifier that the authoritative regulator assigned to this employee.				X				X		X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
Employee ID	Identifier for an employee that is unique across the enterprise. Note: This field is labeled Representative/Investment Advisor.				X				X	X	X	X	X	X	X	X	X	X	X	X
Title	Job title for this employee.				X				X		X	X	X	X	X	X	X	X	X	X
Role	For employees who are traders or registered representatives, identifies their employment role or title; for example, floor trader or branch manager.				X				X		X	X	X	X	X	X	X	X	X	X
Employee Type	Code that identifies the type of employee; for example, employee or contractor.								X		X	X	X	X	X	X	X	X	X	X
Part/Full Time	Indicator of whether this employee is part time or full time.								X		X	X	X	X	X	X	X	X	X	X
Supervisor Name	Name to be displayed for this employee's supervisor.				X				X		X	X	X	X	X	X	X	X	X	X
Supervisory Organization ID	Identifier of the organization that is responsible for monitoring the activities of this employee.								X		X	X	X	X	X	X	X	X	X	X
Supervisor Organization Name	Name of the organization that is responsible for monitoring the activities of this employee.								X		X	X	X	X	X	X	X	X	X	X
Line Organization ID	Identifier of the primary line organization to which this employee is assigned.				X				X		X	X	X	X	X	X	X	X	X	X
Line Organization Name	Name of the primary line organization to which this employee is assigned.				X				X		X	X	X	X	X	X	X	X	X	X
Company	Name of the company for which this employee or contractor works.				X				X		X	X	X	X	X	X	X	X	X	X
Cost Center	Cost center to which this employee is assigned.				X				X		X	X	X	X	X	X	X	X	X	X
Office	Identifier of the office to which this employee is assigned.				X				X		X	X	X	X	X	X	X	X	X	X

Table 98: Trade Blotter List Components by UI Section and Trade Product Category (Continued)

Column	Description	Trade List	Trade	Security Rating	Trader	Account	Customer	Order	Registered Rep.	Investment Advisor	Other/ Equity/ Exchange Traded Fund/ Commodities	Mutual Fund	Fixed Income	Options & Futures	Foreign Exchange	Money Market	Preferred	Convertible	Swap	Standard Configuration
				User Interface Section							**Trade Product Category**									
Office Location	Text that describes this employee's work location (for example, 123 Wall Street or Commonwealth Building, Third Floor).				X				X		X	X	X	X	X	X	X	X	X	X
Tax ID	Employee's tax identification number; for example, SSN.								X	X	X	X	X	X	X	X	X	X	X	X
Tax ID Format	Indicator of whether the employee tax identifier is a Social Security Number (SSN) or another type of identifier.								X	X	X	X	X	X	X	X	X	X	X	X
Hire Date	Date this employee was hired.								X		X	X	X	X	X	X	X	X	X	X
Employee Status	Employment status of this employee; for example, active or inactive.				X				X		X	X	X	X	X	X	X	X	X	X
Employee Status Date	Date that this employee's status was last changed.				X				X		X	X	X	X	X	X	X	X	X	X
Investment Advisor Firm ID	Investment advisor firm identifier. Identifier for a specific investment advisor that is unique across the enterprise.									X	X	X	X	X	X	X	X	X	X	X
Investment Advisor Firm Name	Investment advisor's firm name. For external advisors, the name of the investment advisor's firm.									X	X	X	X	X	X	X	X	X	X	X
# of Subaccounts	Number of active sub-accounts that this investment advisor manages.									X	X	X	X	X	X	X	X	X	X	X
Assets Under Management	Total net worth of all active sub-accounts that this investment advisor manages, expressed in base currency.									X	X	X	X	X	X	X	X	X	X	X

Index