

# Alert Management User Guide

*Release 8.0.7.0.0*  
*August 2019*





# **Alert Management User Guide**

*Release 8.0.7.0.0*  
*August 2019*

Part Number: **E90434-01**

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

Part Number: E86109-01  
First Edition (August 2019)

**Copyright © 2019, Oracle and/or its affiliates. All rights reserved.**

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

**Trademarks**

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.  
Other names can be trademarks of their respective owners.

Oracle Financial Services Software, Inc.  
1900 Oracle Way  
Reston, VA 20190  
*Phone:* (703) 478-9000  
*Fax:* (703) 318-6340  
*Internet:* [www.oracle.com/financialservices](http://www.oracle.com/financialservices)

---

# Contents

---

<b>About this Guide .....</b>	<b><i>i</i></b>
Who Should Use this Guide .....	i
How this Guide is Organized .....	i
Conventions Used in this Guide .....	ii
Where to Find More Information .....	iii
<b>CHAPTER 1            <i>About Alert Management</i> .....</b>	<b>5</b>
Overview of Alert Management .....	5
Oracle Financial Services Behavior Detection UI .....	5
Alert Statuses .....	6
Related Alerts .....	7
Related Cases .....	7
Correlation .....	7
Suppression Rules .....	8
Four - Eyes Approval .....	8
Trusted Pairs .....	9
User Privileges .....	9
<b>CHAPTER 2            <i>Getting Started</i> .....</b>	<b>11</b>
Accessing OFSAA Applications .....	11
Change Password .....	13
Selecting Applications .....	14
<b>CHAPTER 3            <i>Investigating Alerts</i> .....</b>	<b>15</b>
About Alerts .....	15
User Roles and Actions .....	16
Alert/Case Locked Messages .....	17
Alert Workflow .....	18
Analyzing Alerts .....	19
Using Alert Details Tabs .....	19
<i>Accessing Alert Details page</i> .....	19
<i>Using Operational Tabs</i> .....	22
<i>Managing Business Tabs</i> .....	36
Searching for Alerts .....	50
Searching for Alerts using Views .....	50
Searching for Alerts using Alert IDs .....	51
Searching for Alerts using Search Criteria .....	51
Acting on Alerts .....	54

About Alert Actions .....	54
<i>Types of Actions</i> .....	54
<i>Action Categories</i> .....	54
<i>Taking Action on Alerts</i> .....	55
Taking Follow-up Actions on Alerts.....	56
Reassigning Alerts .....	58
Taking Additional Actions on Alerts .....	58
<i>Emailing Alerts</i> .....	59
<i>Generating Regulatory Reports</i> .....	60
<i>Reviewing Alerts</i> .....	61
Closing Alerts .....	61
Auto-closing System Alerts .....	62
<i>Defining Auto-Close Alert Algorithm</i> .....	62
<i>Reopening Automatically Closed Alerts</i> .....	62
Auto-suppressing System Alerts .....	62
<i>Defining Auto-suppress Alert Algorithm</i> .....	62
<i>Reopening Automatically Suppressed Alerts</i> .....	62
<i>Suppressing a Scenario for a Specific Focus</i> .....	63
Reopening Alerts Closed by Suppression .....	63
Creating a Tailored Suppression Rule.....	63
Manually Closing Alerts with Four-Eyes Approval.....	64
<i>Recommending To Close Alerts</i> .....	64
<i>Approving Alerts Recommended for Closure</i> .....	64
Reopening Alerts .....	65
<b>CHAPTER 4</b> <b>Managing Suppression Rules</b> .....	<b>67</b>
About Suppression Rules .....	67
Key Features.....	68
User Roles and Actions .....	68
Suppression Rules Workflow.....	69
Suppression Rules Workflow .....	69
Four- Eyes Approval Process Workflow .....	70
Accessing Suppression Rules page.....	70
Creating Suppression Rules.....	70
Updating Suppression Rules .....	70
Ending Suppression Rules.....	72
Managing Four-Eyes Approval Process.....	73
Recommending Alert Suppression Rules .....	73
Approving Suppression Rules.....	73
Updating and Approving Suppression Rules.....	74
Rejecting Suppression Rules.....	74
Recommending to End Suppression Rule .....	75
Ending Suppression Rules .....	75
Searching Suppression Rules .....	75
<i>Visual Indicators</i> .....	77

<b>CHAPTER 5</b>	<b><i>Setting User Preferences</i></b> .....	<b>79</b>
About Preferences page.....		79
Key Features.....		79
User Roles and Actions .....		80
Accessing Preferences page.....		80
Managing Preferences .....		80
Setting Alert Search and List Options .....		80
Setting Options for Alert Search .....		81
Setting AML Specific Search Options .....		84
Setting Broker Compliance Specific Search Options .....		84
Setting Fraud Specific Search Options .....		85
Setting Trading Compliance Specific Search Options.....		86
Setting Options for Replay page.....		86
Setting Options for Audit Display.....		87
Saving Preferences .....		87
<b>APPENDIX A</b>	<b><i>Alert Components and Tables</i></b> .....	<b>89</b>
Alert Context Information.....		89
Actions with Post Status as Follow-up.....		91
Network Analysis Details .....		92
Start Entities List.....		92
Include Link Types List .....		92
<i>Known Relationships</i> .....		94
<i>Shared Activity</i> .....		94
<i>Filters</i> .....		95
Search Components .....		96
Views Search.....		96
Alert List Matrix .....		100
<i>Alert List Components</i> .....		100
Additional Information .....		102
Alert List Display Configuration.....		104
<b>APPENDIX B</b>	<b><i>Business Tabs</i></b> .....	<b>107</b>
Alert Business Tabs.....		107
<b>APPENDIX C</b>	<b><i>Using Alert Management UI</i></b> .....	<b>109</b>
Common Screen Elements .....		109
Masthead.....		110
Buttons.....		110
<i>Task Buttons</i> .....		110
<i>Action Buttons</i> .....		111
<i>Help Button</i> .....		111
<i>Calendar Button</i> .....		111

<i>Expand/Collapse</i> .....	112
Field Types .....	113
<i>Text Area</i> .....	113
<i>Text Box</i> .....	113
<i>Wildcard Text Box</i> .....	113
<i>Context-Sensitive Text Box</i> .....	113
<i>Drop-down List</i> .....	113
<i>Selection Box</i> .....	113
<i>Check Box</i> .....	114
ToolTips .....	114
Using the Browser .....	115
Navigating in Oracle Financial Services Alert Management.....	115
Navigation Menus .....	115
Links.....	115
Search Bars.....	116
Page Context Controls .....	116
Business Tabs .....	116
Paging.....	116
Message pages .....	116

**APPENDIX D            *Security within Oracle Financial Services Alert Management 117***



---

# 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](#)
- [Conventions Used in this Guide](#)
- [Where to Find More Information](#)

## 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 may 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 information 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, About Alert Management](#), provides an overview of the Alert Management application, how it works, and what it does.
- [Chapter 2, Getting Started](#), explains common elements of the interface. includes instructions on how to configure your system, access Alert Management, and exit the application.
- [Chapter 3, Investigating Alerts](#), explains the Alerts workflow, how to search for business data and create alerts, and the actions you can take on alerts.
- [Chapter 4, Managing Suppression Rules](#), provides instructions for managing suppression rules.
- [Chapter 5, Setting User Preferences](#), explains how to setup Oracle Financial Services Alert Management preferences.

- [Appendix A, Alert Components and Tables](#), provides the additional information on various components and tables of Alert Management.
- [Appendix B, Business Tabs](#), identifies the possible business tab pages that the Oracle Financial Services application displays for a specific scenario class and focus type.
- [Appendix C, Using Alert Management UI](#), explains common elements of the interface.
- [Appendix D, Security within Oracle Financial Services Alert Management](#), explains how Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) security is used.

**Important Note:** With the release of Behavior Detection Framework (BDF) 8.0.5, dispositioning alerts through Alert Management (AM) is only applicable to Trading Compliance and Broker Compliance. For AML and Fraud alerts, the Event Correlation module in Enterprise Case Management (ECM) should be used to correlate events from the FCCM Behavior Detection engine or those ingested from external applications. AM can be used as read-only for viewing historical alerts but it is not to be used for investigating alerts, taking action on alerts, editing alerts and/or promoting alerts to a case. The manual Promote to Case functionality is no longer supported. Customers are to use ECM for reviewing and investigating alerts. A restricted use license of ECM is provided with the BDF license which replicates the functionality available in AM to the best that is currently available within ECM. Implementations should use event correlation to move Alerts from BDF into ECM and then use alert correlation/promote to a case where all levels of investigation can occur. If this updated process is not clear to your implementation team it is advised that you contact Oracle Partner Network or Oracle Consulting to be trained.

## 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 . . .
<i>Italics</i>	<ul style="list-style-type: none"><li>● Names of guides as references</li><li>● Emphasis</li><li>● Substitute input values</li></ul>
<b>Bold</b>	<ul style="list-style-type: none"><li>● Menu names, field names, options, button names</li><li>● Commands typed at a prompt</li><li>● User input</li></ul>
Monospace	<ul style="list-style-type: none"><li>● Directories and subdirectories</li><li>● File names and extensions</li><li>● Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text</li></ul>
<Variable>	<ul style="list-style-type: none"><li>● Substitute input value</li></ul>

## **Where to Find More Information**

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

- *Administration Guide*
- *Administration Tools User Guide*
- *Configuration Guide*
- *Data Interface Specification (DIS)*
- *Financial Services Data Model 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*
- *Glossary*
- *Release Notes*
- *Readme*

These documents are available at the following link:

[http://docs.oracle.com/cd/E60570\\_01/homepage.htm](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](http://www.oracle.com/financialservices).



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

- [Overview of Alert Management](#)
- [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 Behavior Detection platforms detect potentially problematic behaviors by identifying patterns in data and generating alerts. The output of these engines is an alert that 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 are then investigated by individuals within a Compliance department.

## ***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 3, 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 2. 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.

**Table 2. Alert Status Descriptions (Continued)**

Status	Description
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.

## 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 Behavior Detection 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.

Alert Correlation is only applicable to Trading Compliance and Broker Compliance. For AML and Fraud alerts, the Event Correlation module in Enterprise Case Management should be used to correlate events from the FCCM Behavior Detection engine or those ingested from external applications. For more information about how event correlation within ECM, see the Event Correlation section in the *Oracle Financial Services Enterprise Case Management User Guide*.

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.

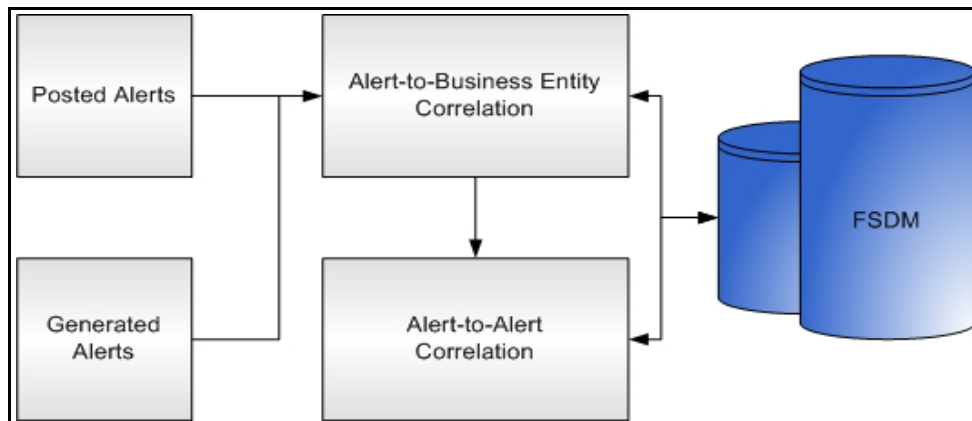


Figure 1. Alert Correlation -Process Flow

## 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 4, 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 acknowledgment 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. For AML and Fraud, since all alert disposition is completed through ECM, Trusted Pairs can only be managed by the client providing trusted pairs via the DIS.

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, 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 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.

## ***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.



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

This chapter discusses the following topics:

- [Accessing OFSAA Applications](#)
- [Troubleshooting Your Display](#)

## Accessing OFSAA Applications

Access to the Oracle Financial Services Behavior Detection application depends on the Internet or Intranet environment. Oracle Financial Services Behavior Detection is accessed through Microsoft Internet Explorer (IE), Microsoft Edge, Google Chrome and Mozilla Firefox. 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/ofsaapp/login.jsp`

The OFSAA Login page is displayed.

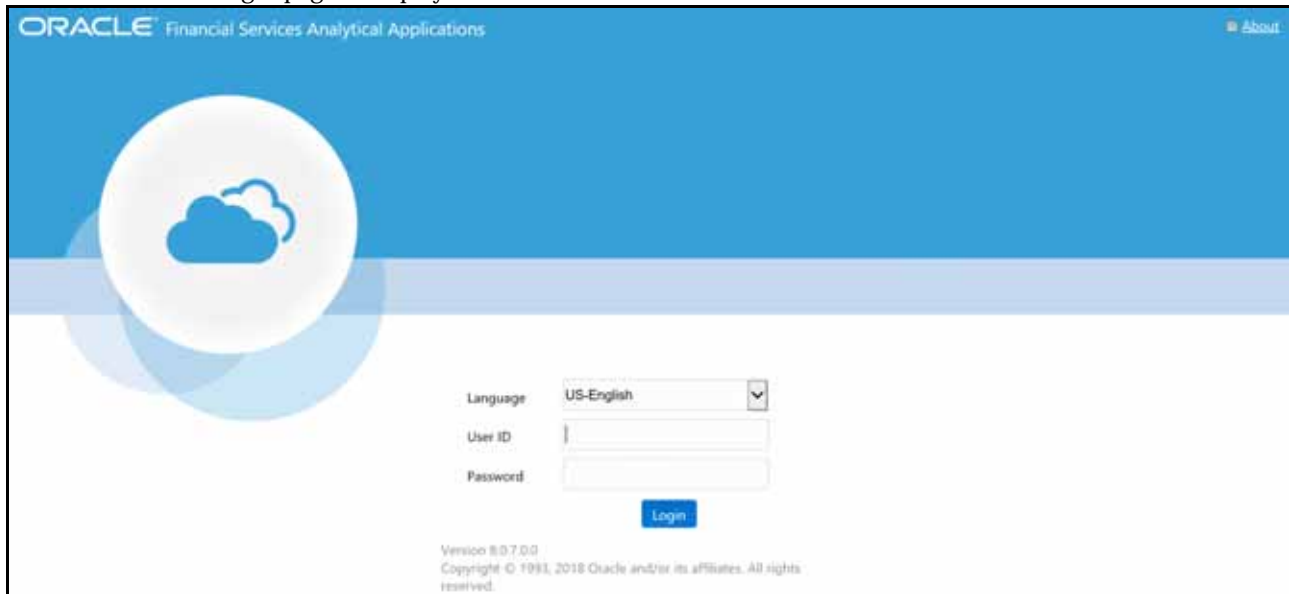


Figure 2. OFSAA Login page

2. Enter your User ID and Password in the respective fields.
3. Click **Login**. The Oracle Financial Services Analytical Applications page is displayed.

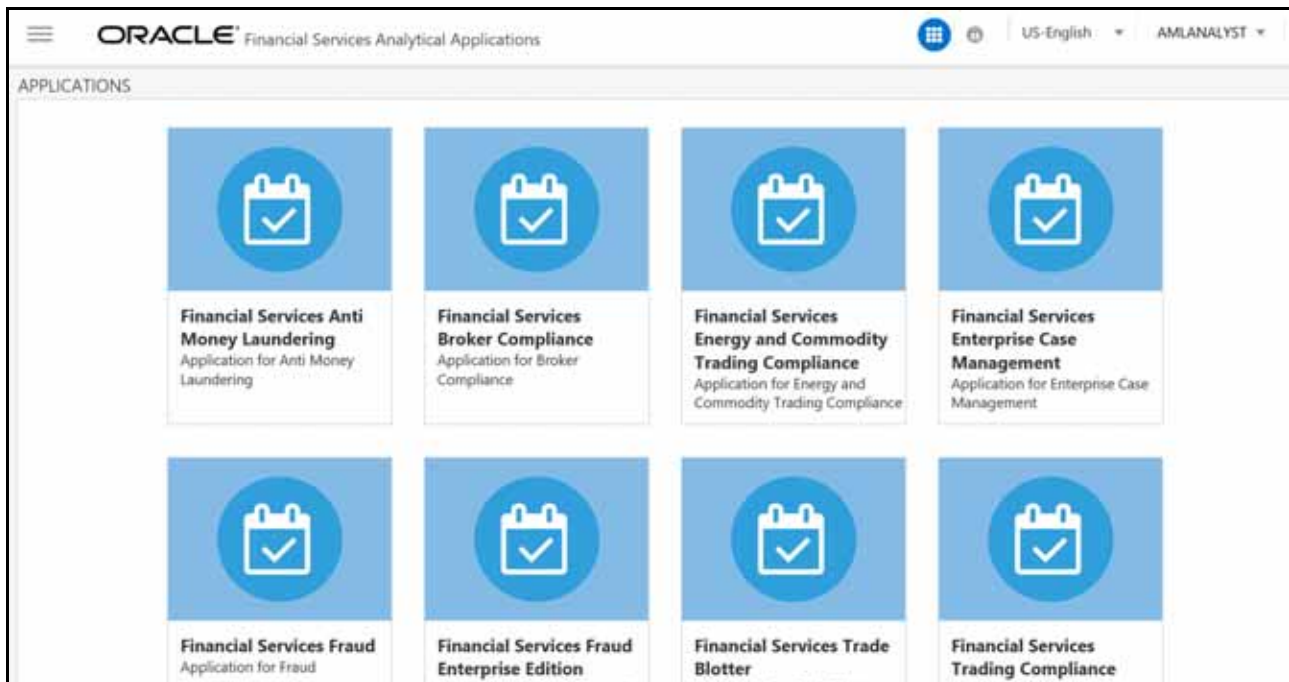


Figure 3. Oracle Financial Services Analytical Applications page

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 5, Setting](#)

*User Preferences.* You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

## 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.

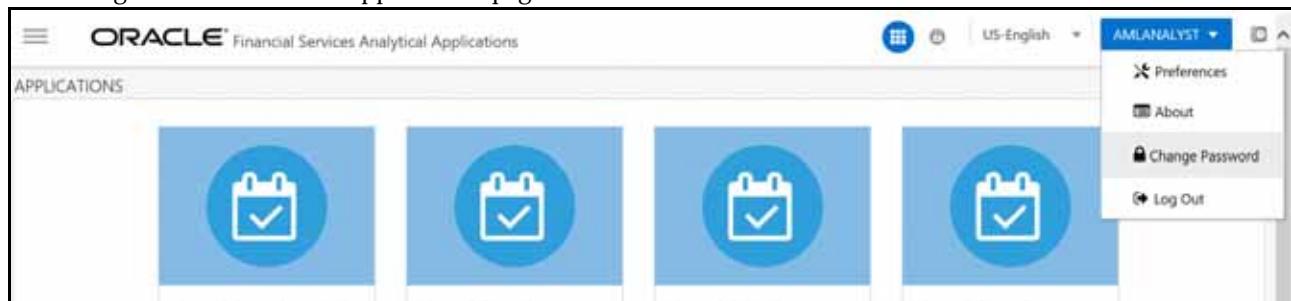


Figure 4. Change Password

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

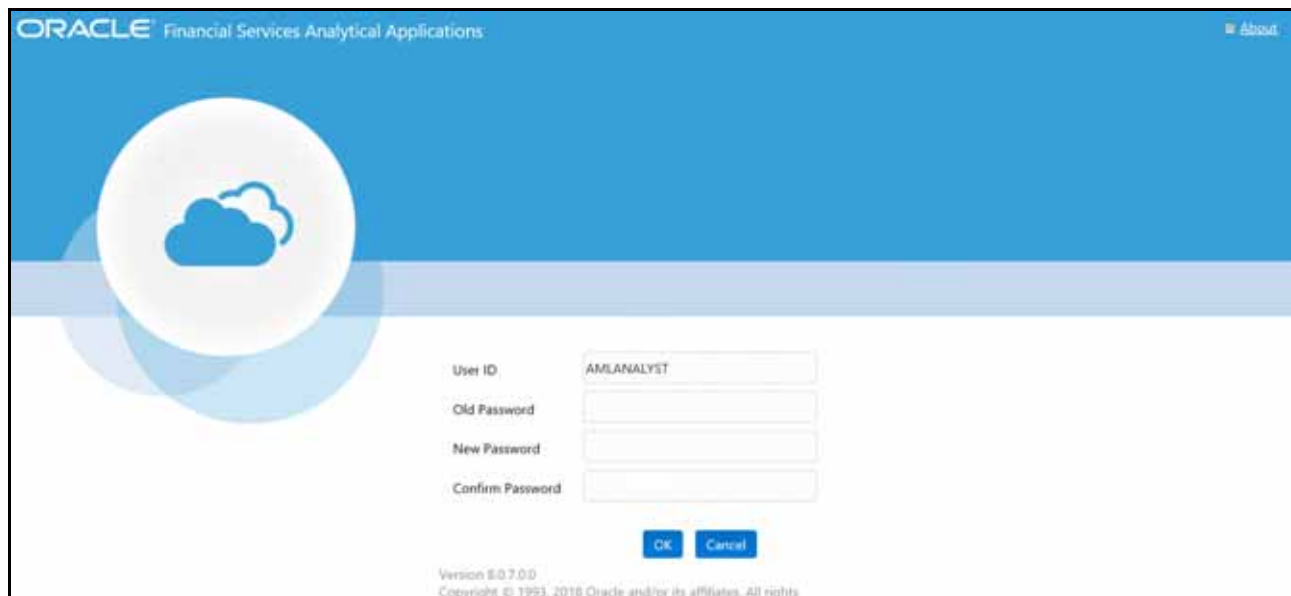


Figure 5. Change Password

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.

## Selecting Applications

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

To access Behavior Detection applications, such as the Anti Money Laundering application, follow these steps:

1. Navigate to the OFSAA Applications home page.
2. Select **Financial Services Anti Money Laundering**. The Behavior Detection Anti Money Laundering page opens.



**Figure 6. Behavior Detection Anti Money Laundering page**

3. Click **Behavior Detection** to expand the menu, then select **Alert Investigation**. The *Alert Search and List Page* is displayed.

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
- 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 3. Alert Management User Roles and Actions**

User Actions	User Roles						
	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor
<b>Privileges</b>							
<b>Access to Tabs</b>							
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
<b>Access to Alert Actions</b>							
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	
<b>Access to Financials Functionality</b>							
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	
Access to edit existing data on Financials tab		X	X	X			
Access to delete existing data on Financials tab		X	X	X			



## Alert/Case Locked Messages

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:

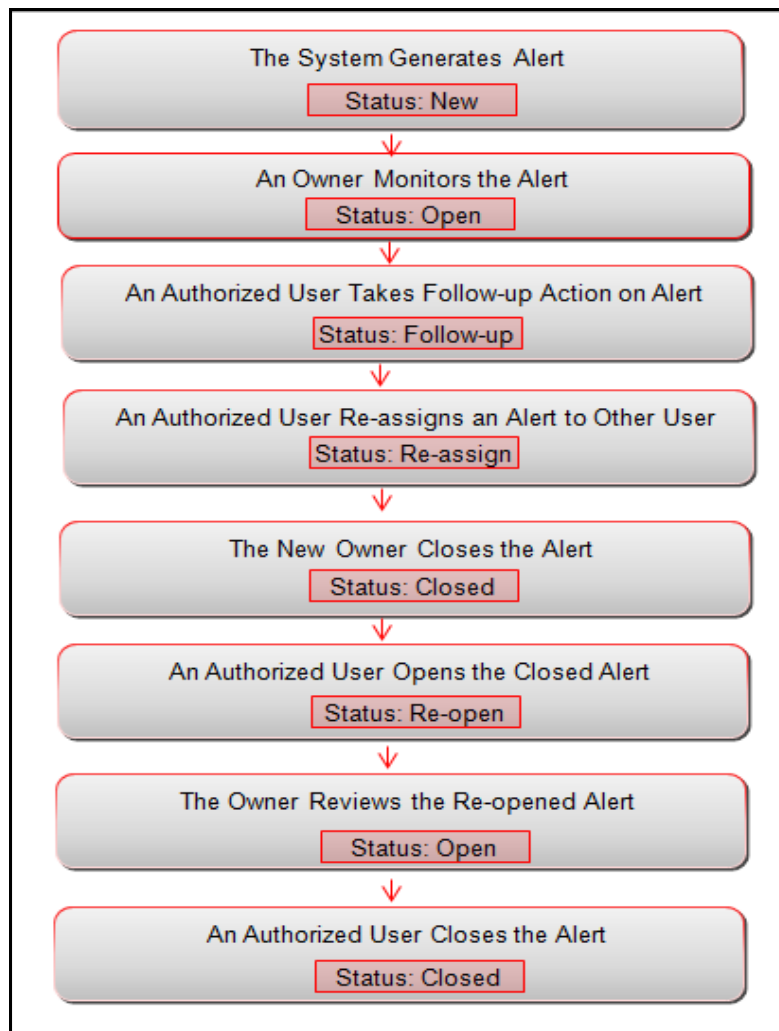
- **When some alerts are locked:** *One or more Alerts are locked by another user. Select OK to continue, Cancel to return to the Alert List.*
- **When some cases are locked:** *One or more cases are locked by another user. Click OK to continue performing actions for cases which are not locked.*

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.*

## Alert Workflow

The following figure shows the potential workflow for managing alerts.



**Figure 7. Potential alerts workflow**

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

**Table 4. 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 4. Managing Alerts Workflow Table**

Action	Description	Roles
<a href="#">Closing Alerts</a>	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
<a href="#">Reopening Alerts</a>	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 2, 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.

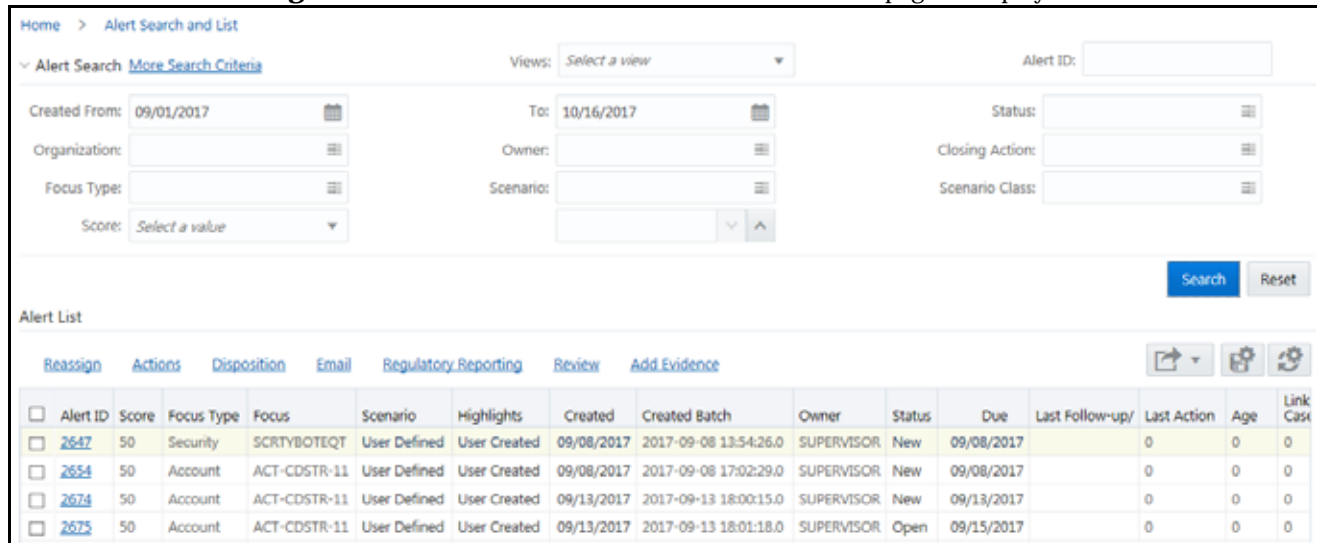


Figure 8. Alert Search and List Page

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

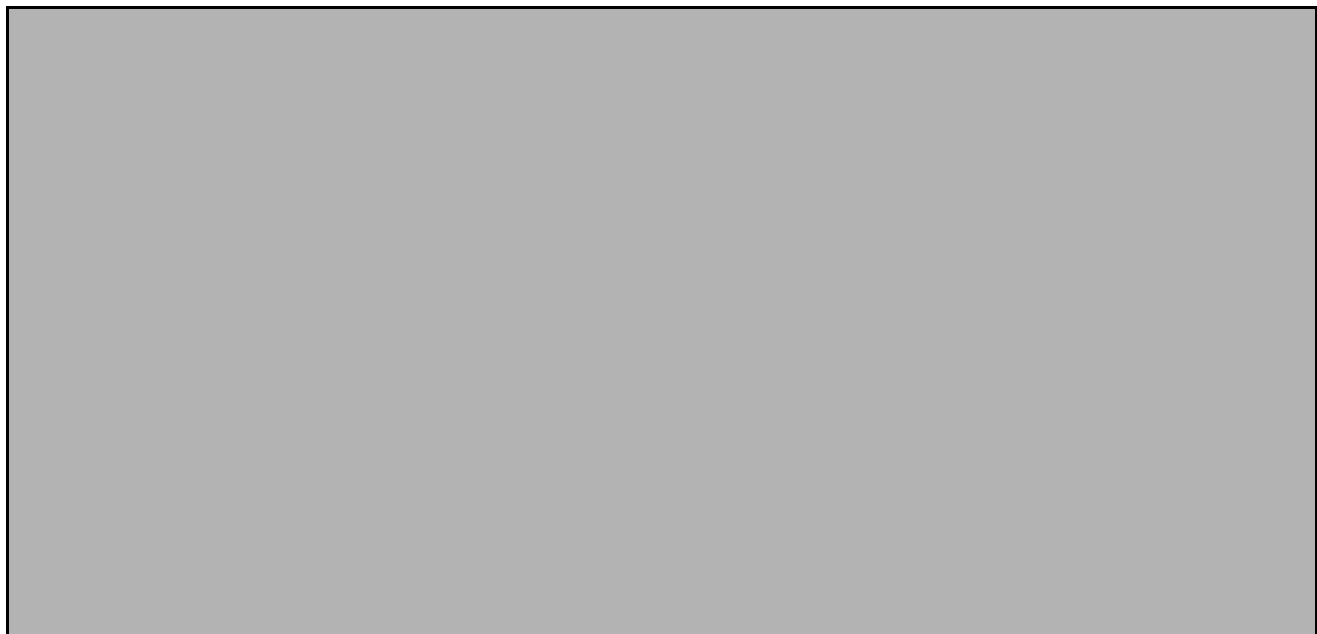
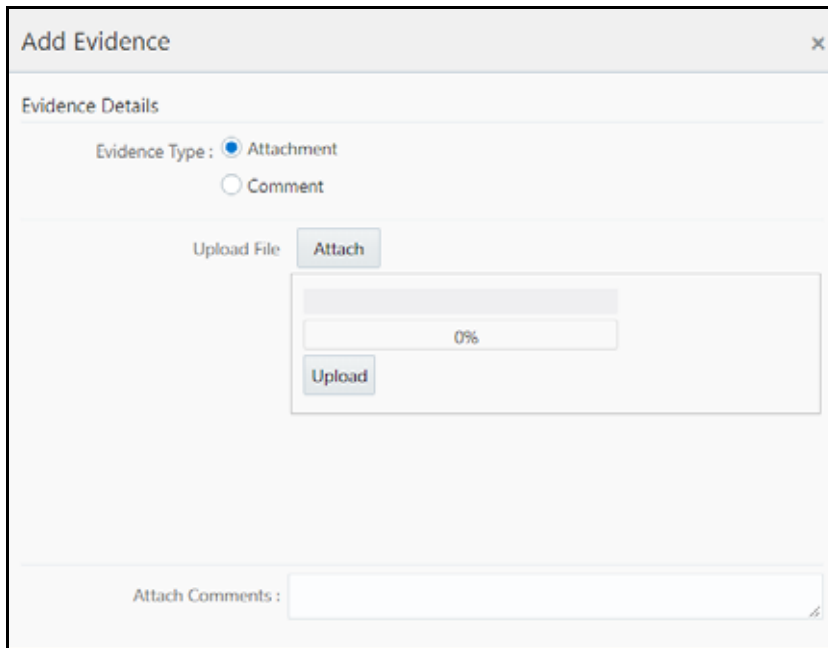


Figure 9. Add Evidence link - Add a comment

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



The screenshot shows a dialog box titled "Add Evidence" with a close button (X) in the top right corner. Below the title bar is a section labeled "Evidence Details". Under "Evidence Type", there are two radio buttons: "Attachment" (which is selected) and "Comment". Below this, there is an "Upload File" label and an "Attach" button. A file selection area is visible, showing a progress bar at 0% and an "Upload" button. At the bottom of the dialog, there is a text input field labeled "Attach Comments:".

Figure 10. Add Evidence link - Add an attachment

- 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.

Home > Alert Search and List > Alert Details

Actions   Email   Regulatory Reporting   Review   Add Evidence   Print

> Alert ID: 1      Focus: Address 17 S BRIDGE      Status: Follow - Up      Score: 1

Details   Disposition   Correlation   Relationship   Narrative   Evidence   Audit History

▼ Matched Information

Designate Trusted Pair      Export ▼     

Score	Scenario	Highlights		
0	Terrorist Fin...	Tot Trans Amt = USD 212,010.00; Tot Trans Ct = 48...	<a href="#">Thresholds</a>	<a href="#">Score</a>
0	Terrorist Fin...	Tot Trans Amt = USD 212,010.00; Tot Trans Ct = 48...	<a href="#">Thresholds</a>	<a href="#">Score</a>

▼ Derived Address

Export ▼     

Address	Last Activity	Risk	Match
17 S BRIDGE STREET	12/10/2015	7(PRIORITY 7 COUNTRIES)	CNT

Figure 11. 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 then 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.

### 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](#)

- [Using Disposition Tab](#)

### **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.



## *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.

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 12. 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.

Field	Description
Suppression End Date	Select the date until when the alert is suppressed. This action is editable only if you select <b>Close and Suppress-Enter Date</b> 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 Operator	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.

### ***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.

Home > Alert Search and List > Alert Details

Actions Email Regulatory Reporting Review Add Evidence Print

> **Alert ID:** 26      **Focus:** Correspondent Bank      **Status:** Open      **Score:** 1

Details Correspondent Bank Disposition **Correlation** Relationship Narrative Evidence Audit History

Correlation Summary

Correlation ID	Correlation Name	Score
<a href="#">COR4</a>	Correlated Alerts By Business Entity	1
<a href="#">COR3</a>	Potential Identity Theft	1

Page 1 of 1 (1-9 of 9 items)    Records Per Page 9

Correlation Business Entities

Correlated Business Entities Network

Entity	Relationship	Total # of Correlated Alerts	Focus	Focus
<a href="#">SC ABSF01</a>	Derived Address for the Matched Account	1	Security	SC
<a href="#">AC 100IOSNL05</a>	Derived Address for the Matched Account	1	Account	AC
<a href="#">CU CUTSRMFALLCU-100</a>	Derived Address for the Matched Account	1	Customer	CU
<a href="#">CB IA-FBML42NJ</a>	Self - Focus	1	Correspondent Bank	CB
<a href="#">EE EEMLNOAAC-101</a>	Derived Address for the Matched Account	1	Employee	EE
<a href="#">TR XXEMPTRAHMTREVTR-001</a>	Derived Address for the Matched Account	1	Trader	TR
<a href="#">EN ACXA102</a>	Derived Address for the Matched Account	1	External Entity	EN
<a href="#">AD 12/129ABLOCK D</a>	Derived Address for the Matched Account	1	Address	AD
<a href="#">HH HHCSTLPESH-003</a>	Derived Address for the Matched Account	1	Household	HH

**Figure 13. 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 5* describes the fields for the Correlated Business Entities section.

**Table 5. 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.

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.

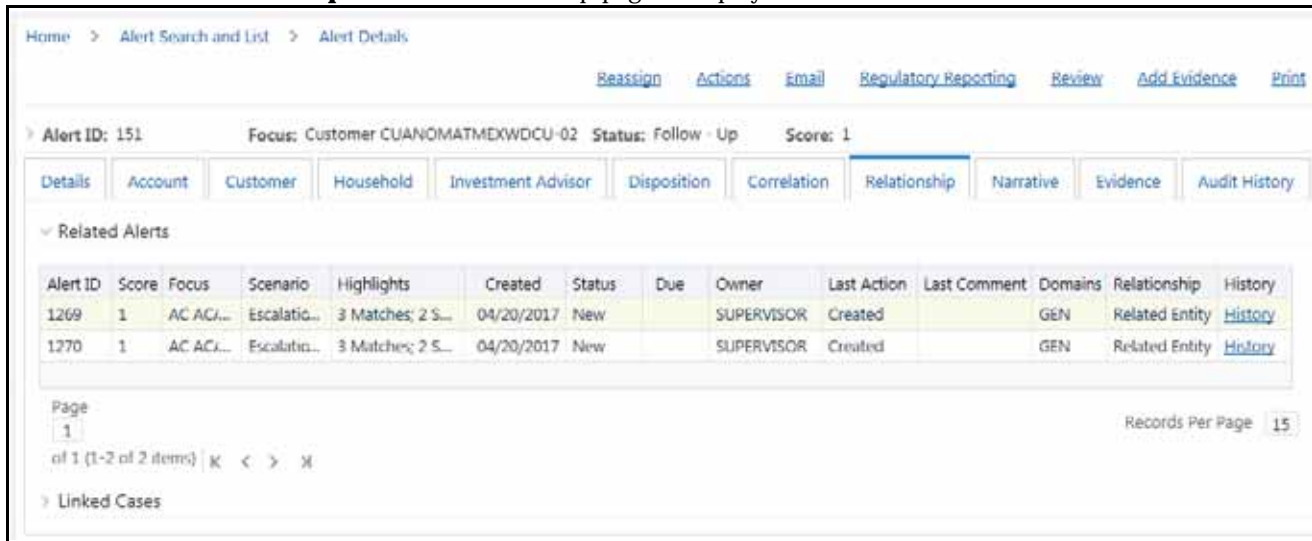


Figure 14. Relationship Page

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

Table 6. 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 7. 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 7. 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 <b>History</b> to view the history of the related alert in a window.

### 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:

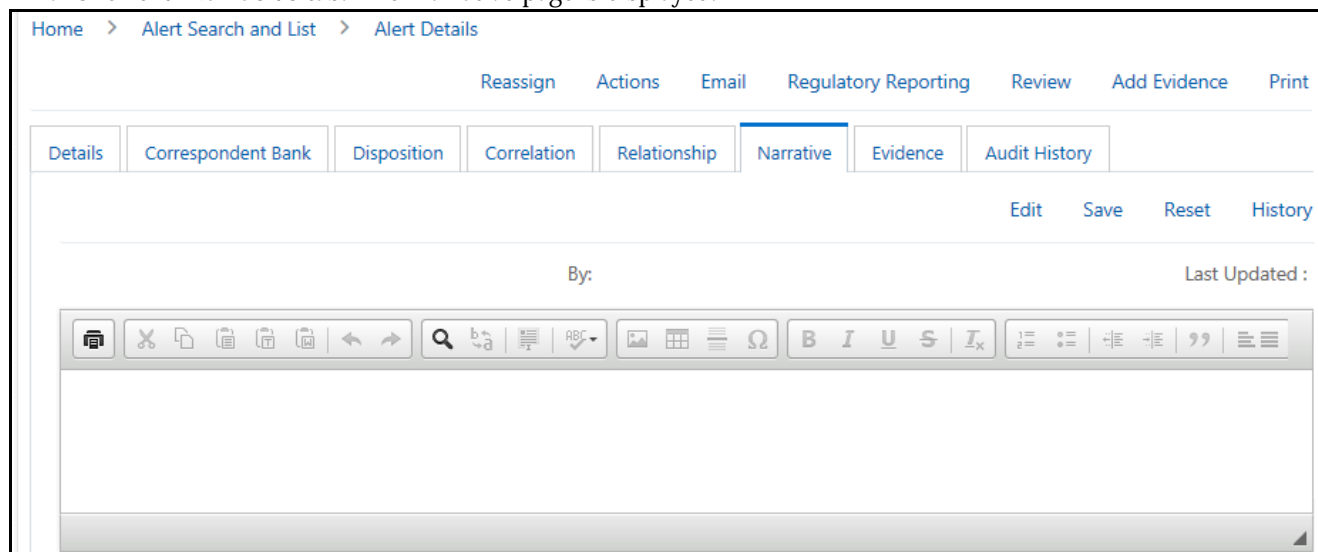
- [Creating Narrative](#)
- [Editing Narrative](#)
- [Deleting Narrative](#)

### 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 15. 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.



Home > Alert Search and List > Alert Details

Reassign Actions Email Regulatory Reorting Review Add Evidence Print

Details Correspondent Bank Disposition Correlation Relationship Narrative Evidence Audit History

▼ Comments

Date and Time	By	Status	Comments
07/06/2017 11:34 EST	SUPERVISOR	Open	
07/06/2017 11:35 EST	SUPERVISOR	Open	test
07/06/2017 12:45 EST	SUPERVISOR	Open	test
07/07/2017 12:32 EST	SUPERVISOR	Open	test
07/07/2017 12:33 EST	SUPERVISOR	Open	test

Page 1 of 1 (1-2 of 2 items) Records Per Page 2

▼ Attachments

Date and Time	By	Status	Comments	Attachment Name
07/05/2017 18:54 EST	SUPERVISOR	Open		802changed.txt
07/20/2017 19:55 EST	SUPERVISOR	Open		again

Page 1 of 1 (1-2 of 2 items) Records Per Page 2

Figure 16. 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.

**Table 9. Attachment section**

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,

Date and Time	Action	By	Resulting Status	Comments	Attachment Name	Attachment
08/18/2017 17:54:50 EST	Created	SUPERVISOR	New	AAAA		<a href="#">0</a>
08/18/2017 17:54:51 EST	Viewed By Owner	SUPERVISOR	Open			<a href="#">0</a>

**Figure 17. 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 attachments. 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 B, *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*.

Date	Amount	GL Account	Cost Center	Loss Payee	Entered By	Entered Date	Description
09/12/2017	USD 343	ddf	FID06A		SUPERVISOR	09/27/2017	ddf

Figure 18. 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.

∨ Current Loss and Recovery Summary

Total Potential Loss Amount :	USD 35,423,215.00	Primary GL Account :	financial
Total Averted Loss Amount :	USD 22.00	Primary Cost Center :	FI006A
Total Recovered Amount :	USD 3.00	Offset Account :	financial
Total/Net Loss Amount :	USD (35,423,190.00)	Offset Cost Center :	FI006A

**Figure 19. 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.

ID	Status	Primary GL Account	Primary Cost Center
2	Active	123	FI006A
2	Inactive		
1	Inactive	123	FI006A
1	Inactive	123	FI006A

Figure 20. 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 and click **Add**. The Loss and Recovery Data Entry dialog box is displayed.

**Figure 21. 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. <b>Note:</b> 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. <b>Note:</b> 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: *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.*
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.

The screenshot shows the 'Replay' tab selected in a web application. At the top, there are navigation links: Actions, Email, Regulatory Reporting, Review, Add Evidence, and Print. Below these, the alert details are shown: Alert ID: 86, Focus: Security ISIN-MUPM, Status: Open, and Score: 1. A horizontal menu contains tabs for Details, Trade, Order, Execution, Security, Replay (selected), Disposition, Correlation, Relationship, Narrative, Evidence, and Audit History. The main content area is a search filter section with the following fields and options:

- Market Center: DOW JONES
- Security: SC-MUPMDOWN-SC-201U, ISIN-MUPMDOWN-201U (with a dropdown arrow)
- Or Security Group: (empty field)
- Start Date: 08/01/2017 (with a calendar icon)
- End Date: 09/30/2017 (with a calendar icon)
- Time From: 14:15:00:00
- Time To: 14:30:00:00
- Time Zone: EST (-05:00) (with a dropdown arrow)
- Radio buttons: Selected (unselected), Local (selected)
- View options:
  - Automated Quotes
  - Market Center Quotes  Inside Quotes
  - Executions  Order Events  Orders
  - Trades  Reported Sales
- Expand options:
  - Automated Quotes
  - Market Center Quotes  Inside Quotes
  - Executions  Order Events  Orders
  - Trades  Reported Sales
- Buttons: Reset, Search
- > List (link)

Figure 22. 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. <b>Note:</b> 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.
Security Group	Select the security group from the drop-down list of which the security is matched or bound to the alert. <b>Note:</b> 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: <i>Add securities to the Security selection box that share the same ISIN.</i>
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: <ul style="list-style-type: none"> <li>● ISIN of the securities matched to the Alert</li> <li>● 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: <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ If you clear the Expand by ISIN check box and click Search, the page restores the initial population of the Security list box.</li> </ul> </li> </ul>
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.  <b>Note:</b> 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	<p>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.</p> <p>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.</p> <p>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.</p> <p>Select the time zone as <b>Local</b>, the replay page displays the date and time value for each record in the time zone local to the record's event.</p> <p>Select the time zone as <b>Selected</b>, the replay page displays the date and time value for each record in the time zone selected in the Time Zone filter.</p> <p>For example, consider the following information shown on the Replay page:</p> <ul style="list-style-type: none"> <li>● <b>Case #1 (Default Case):</b> 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.</li> <li>● <b>Case #2:</b> 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.</li> <li>● <b>Case #3:</b> 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.</li> </ul>

Table 13. Replay Tab Search page

Fields	Description
View	<p>Select the check box to view columns of data in the match replay. You can select one or more of the following option:</p> <ul style="list-style-type: none"> <li>● <b>Inside Quotes:</b> Matched events of inside quote or framing records in the match, in case, order and execution are involved in the match.</li> <li>● <b>Market Center Quotes:</b> Matched events of Market Center quote records that were involved in the match.</li> <li>● <b>Automated Quotes:</b> Automated quote records that were either involved in the match or provided context for the events involved in the match.</li> <li>● <b>Trades:</b> Trade information during the time frame for the involved security.</li> <li>● <b>Orders:</b> Order records that were either involved in the match or the executions involved in the match.</li> <li>● <b>Order Events:</b> 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.</li> </ul> <p><b>Note :</b> 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.</p> <ul style="list-style-type: none"> <li>● <b>Executions:</b> Execution records that were involved in the match.</li> <li>● <b>Reported Sales:</b> Matched Reported Sales and Framing Records in case trade is matched.</li> </ul>
Expand	<p>Select a check box to expand the display of the corresponding column you selected in the View option.</p> <p>You can select one of the following: Inside Quotes, Market Center Quotes, Automated Quotes, Trades, Orders, Order Events, Executions, or Reported Sales.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p><b>Note:</b> If the default event is selected as Automated Quotes, then events Inside Quotes and Market Center Quotes must be deselected.</p>

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 <i>New</i> .
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 <i>Closed</i> .
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.

Table 17. More Search Criteria

Fields	Description
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. <b>Note:</b> 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.
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. <b>Note:</b> 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. <b>Note:</b> You must specify an Action To or Action From date for this search.

**Table 17. More Search Criteria**

Fields	Description
Limit to Focus	Select the Limit to Focus check box. This filters the alert focused on specified entities with a business relationship. <b>Note:</b> 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.
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. <b>Note:</b> If you are taking action on multiple alerts, system displays only actions and comments that are common to all selected alerts.
<b>Note:</b> 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	<p>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 <a href="#">Reassigning Alerts</a>.</p> <p><b>Note:</b> You can automate the assignment of ownership of the alert by selecting the Auto Assignment check box.</p>
Auto Assignment check box	<p>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 <i>Reassign Ownership To</i> 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.</p> <p><b>Note:</b> Deselect the Auto Assignment check box to enable the <i>Reassign Ownership To</i> 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.</p>
Set Due Date	<p>Select the due date from calendar icon. This provides an ability to select a date by which the selected action should complete.</p> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>● 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.</li> <li>● If multiple actions with default due-dates are taken on the alert then the nearest default due-date is applied to the alert.</li> <li>● 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.</li> </ul>
Suppression End Date	<p>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.</p> <p><b>Note:</b> 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.</p>
Suppression Condition	<p>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:</p> <ul style="list-style-type: none"> <li>● <b>Binding Name:</b> Select the binding name from the Binding Name drop-down list.</li> <li>● <b>Binding Operator:</b> 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 (&gt;=), less than or equal to (&lt;=), greater than (&gt;), less than (&lt;), and not equal to (!=).</li> </ul> <p><b>Binding Value:</b> 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 editable text. For more information on User privileges, see <a href="#">Appendix A, User Privileges</a>. 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.</p>

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: <ul style="list-style-type: none"> <li>● Email Alert Details</li> <li>● Email with Response Request</li> <li>● Email Alert Details with Response Request</li> <li>● Send Email</li> </ul>
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 <a href="#">Reassigning Alerts</a> . <b>Note:</b> 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 <i>Reassign Ownership To</i> 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. <b>Note:</b> Deselect the Auto Assignment check box to enable the <i>Reassign Ownership To</i> 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. <b>Note:</b> <ul style="list-style-type: none"> <li>● 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.</li> <li>● If multiple actions with default due-dates are taken on the alert then the nearest default due-date is applied to the alert.</li> <li>● 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.</li> </ul>
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. <b>Note:</b> 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.

## 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](#)
- [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 4, 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 acknowledgment 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 Alert and 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.

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									
	Analyst I	Analyst II	Analyst III	Supervisor	Executive	Internal Auditor	External Auditor	Data Miner	AM Administrator	WLM Supervisor
<b>Privileges</b>										
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.

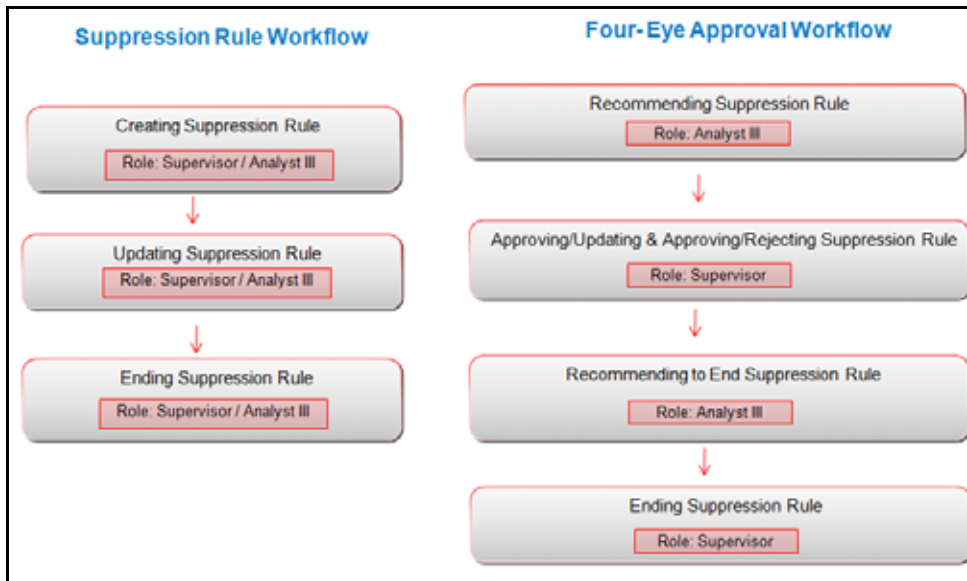


Figure 23. Suppression Rules Workflow

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
<a href="#">Creating Suppression Rules</a>	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
<a href="#">Updating Suppression Rules</a>	User can modify Extend the Suppression By or Suppression End Date by providing appropriate comments.	Analysts II, III, and Supervisors
<a href="#">Ending Suppression Rules</a>	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
<a href="#">Recommending Alert Suppression Rules</a>	Analyst II or III can recommend alert suppression rule. For users requiring supervisory approval, actions are labeled with <i>Recommend</i> to easily identify those actions that require additional oversight.	Analysts II and III
<a href="#">Approving Suppression Rules</a> Or <a href="#">Rejecting Suppression Rules</a>	User can approve or reject suppression rules which are Recommended for approval after providing justification in the comment box.	Supervisors
<a href="#">Recommending to End Suppression Rule</a>	User can recommend to end suppression rule.	Analysts II and III
<a href="#">Ending Suppression Rules</a>	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 2, 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 24. 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 <a href="#">Table 23</a> .  <b>Note:</b> 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: <ul style="list-style-type: none"> <li>• When you have selected only one rule from the List section</li> <li>• When multiple suppression rules are selected and all of them have the same end date</li> <li>• 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.</li> </ul>
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.  <b>Note:</b> 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.

Suppression Rule ID	Focus Name	Focus ID	Scenario	Highlight	Created By	Rule Status	Expires on	Triggering Alert ID	Action History
15	CU	CUEATMACC01	Exit in ATM Act. WD		ANALYST	Recommend	12/08/2015	464	History

Figure 25. 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.

Recommended User: ANALYST  
Comments :\*

Save Cancel

Figure 26. 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 27. Suppression Rules Search page**

**Note:** Blank search is not supported. You must 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)	<ul style="list-style-type: none"> <li>● In order to search for suppression rules after the specified date, you must enter only a From search date.</li> <li>● 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.</li> </ul>
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. <b>Note:</b> 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)	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. <ul style="list-style-type: none"> <li>● Enter Expiring From (Start Date). This filters the suppression rules list based on the expiration start date.</li> <li>● Enter Expiring From (End Date). This filters the suppression rules list based on the expiration end date.</li> </ul>
Expiring To (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 creator 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. <b>Note:</b> 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: <ul style="list-style-type: none"> <li>● Active</li> <li>● Inactive</li> <li>● Recommend</li> </ul>

3. Click **Go**. The relevant suppression rules are displayed.

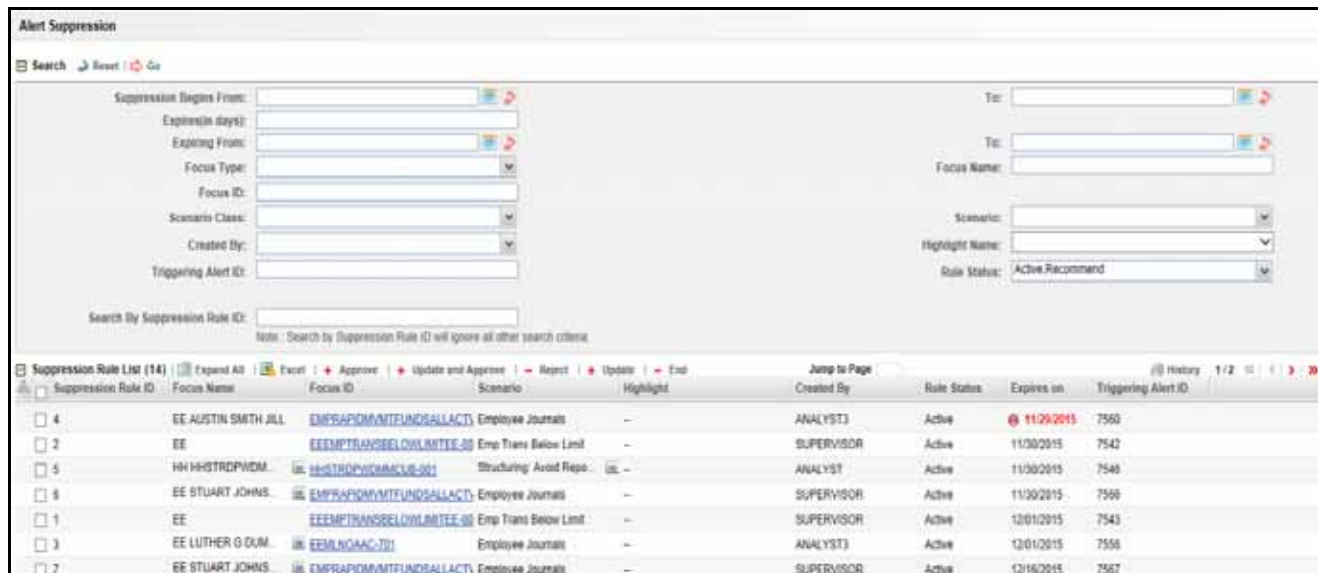


Figure 28. Suppression Rule List

### 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.

# Searching Suppression Rules

## Chapter 4—Managing Suppression Rules

Suppression Rule List (14)	Expand All	Excel	Approve	Update and Approve	Reject	Update	End	Jump to Page	History
Suppression Rule ID	Focus Name	Focus ID	Scenario	Highlight	Created By	Rule Status	Expires on	Triggering Alert ID	
<input type="checkbox"/> 4	EE AUSTIN SMITH JILL	<a href="#">EMPRAPDMNTEUNDALACT</a>	Employee Journals	--	ANALYST3	Active	11/06/2015	7540	
<input type="checkbox"/> 2	EE	<a href="#">EEEMTRANSGBELOWARTEE-00</a>	Emp Trans Below Limit	--	SUPERVISOR	Active	11/06/2015	7542	
<input type="checkbox"/> 5	HH HHTROPYDAL	<a href="#">HHTROPYDMACU-001</a>	Structuring Avoid Repe...	--	ANALYST	Active	11/06/2015	7548	
<input type="checkbox"/> 6	EE STUART JOHNS	<a href="#">EMPRAPDMNTEUNDALACT</a>	Employee Journals	--	SUPERVISOR	Active	11/06/2015	7568	
<input type="checkbox"/> 1	EE	<a href="#">EEEMTRANSGBELOWARTEE-00</a>	Emp Trans Below Limit	--	SUPERVISOR	Active	12/01/2015	7543	
<input type="checkbox"/> 3	EE LUTHER G DUM...	<a href="#">EEMLNQVAC-701</a>	Employee Journals	--	ANALYST3	Active	12/01/2015	7555	
<input type="checkbox"/> 7	EE STUART JOHNS	<a href="#">EMPRAPDMNTEUNDALACT</a>	Employee Journals	--	SUPERVISOR	Active	12/16/2015	7567	

Figure 29. Visual Indicators for Suppression Rules Expiration Dates

# Setting User Preferences



This chapter describes the concept and process of managing Behavior Detection 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, 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 2, 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 Fraud Specific Search Options](#)
- [Setting Trading Compliance Specific Search Options](#)
- [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 30.** 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 25. Set Alert Search and List Options**

Field	Description
Set Alert Display Configuration	<p>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:</p> <ul style="list-style-type: none"> <li>● Anti-Money Laundering</li> <li>● Broker Compliance and Control Room</li> <li>● Fraud</li> <li>● Standard</li> <li>● Trading Compliance</li> </ul> <p>For more information on setting the alert display configuration, see <a href="#">Alert List Display Configuration</a>.</p> <p><b>Note:</b> These solution sets are provided with standard deployment. Additional custom solution sets can be configured in the Alert Display Configuration selection.</p>
Set Default Search	<p>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:</p> <ul style="list-style-type: none"> <li>● Views</li> <li>● Simple Search</li> <li>● Advanced Search</li> </ul>
Set View for Alert List	<p>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 <i>My Open Alerts</i> option is selected if you have not previously saved your View option.</p>

## 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 31.** Navigate to the Preferences page and go to the Set Option for Alert Search.

- Select common filters for the solution set. For more information, see [Table 25](#) Setting the Alert Display Configuration section.

**Table 26. Alert Search Components**

Fields	Description	Standard	AML	TC	BC	Fraud
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
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. <b>Note:</b> If you filter by Organization, you cannot filter by Owner.	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. <b>Note:</b> If you filter by Owner, you cannot filter by Organization.	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. <b>Note:</b> If you filter by Class, you cannot filter by Scenario.	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
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
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 <i>TR SmithJ</i> consists of a focus type of <i>TR</i> and a focal entity of <i>SmithJ</i> .	X	X	X	X	X
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

Table 26. Alert Search Components (Continued)

Fields	Description	Standard	AML	TC	BC	Fraud
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
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
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
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. <b>Note:</b> You must specify an Action To or Action From date for this search.	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
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. <b>Note:</b> You must specify an Action To or Action From date for this search.	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. <b>Note:</b> You must specify an Action To or Action From date for this search.	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
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
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

Table 26. Alert Search Components (Continued)

Fields	Description	Standard	AML	TC	BC	Fraud
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
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
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
Entity Name	Enter the entity name associated with alerts you want to view.	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 **Set 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 27. 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 **Set 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 28. 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 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 **Set 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 29. 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.
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 **Set 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 30. 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 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:

**Figure 32.** Navigate to the Preferences page. Go to the Set Options for Replay page section.

3. 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.

**Figure 33.**

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.





# 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 31. Alert Context Information by Scenario Class**

Column	Description	AML	Fraud	TC	BC
Alert ID	Unique ID of the alert.	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
Score	Score the alert received.	X	X	X	X
Scenario	Scenario short name of the scenario that generated the alert.	X	X	X	X
Owner	Name of an individual or group of users to whom the alert is assigned.	X	X	X	X
Organization	Name of the organization for which an alert is assigned.	X	X	X	X
Business Domain	Business domain(s) associated with the alert focus.	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
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
Linked Cases	The count of cases linked to the alert.	X	X	X	X
Status	Current state of the alert relative to its analysis and closure.	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
Highlights	Pertinent information related to the alert.	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 31. Alert Context Information by Scenario Class (continued)**

<b>Column</b>	<b>Description</b>	<b>AML</b>	<b>Fraud</b>	<b>TC</b>	<b>BC</b>
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
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	
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	Identification 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.				
Commodity	Filters the alert list by the name of the commodity instrument involved in the alert.				

## Actions with Post Status as Follow-up

This section provides information on Actions with Post Status as Follow-up

**Table 32. 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 32. 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 Network 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 33. 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.
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 34. 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

**Table 34. Valid Entity-Link Types**

Starting Entity	Valid Link Types
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 35. 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**  $\geq$  builds the network based on shared activity. Whenever this date is selected, the system checks for transactions between the Transaction Date  $\geq$  and Transaction Date  $\leq$  to establish links for Wire Transactions, Journal Transactions, Monetary Instrument Transactions and Insurance Transactions.
- **Transaction Date**  $\leq$  builds the network based on shared activity. Whenever this date is selected, the system checks for transactions between the Transaction Date  $\geq$  and Transaction Date  $\leq$  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 36 list the View Filter and Sort Criteria for the default View Names.

**Table 36. 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 37 provides a list of the alert search components that display in the alert Simple and Advanced Search bar.

**Table 37. Alert Search Components**

Column	Description	Simple Search	Advanced Search			
			AML	Fraud	BC	TC
Created From	Filters the alert list by the date the alert was created.	X	X	X	X	X
Created To	Filters the alert list by the date the alert was created.	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
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
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
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 <i>TR SmithJ</i> can consist of a focus type of TR and a focal entity of SmithJ.	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
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
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
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
Closing Action	Filters the alert list by one or more selected closing actions that are taken on an alert. <b>Note:</b> You must specify an Action To or Action From date for this search	X	X	X	X	X
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

Table 37. Alert Search Components (continued)

Column	Description	Simple Search	Advanced Search			
			AML	Fraud	BC	TC
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
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
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
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
Action	Filters the alert list by one or more actions that are taken on an alert. <b>Note:</b> You must specify an Action To or Action From date for this search		X	X	X	X
Last Action	Filters the alert list by one or more selected last actions that are taken on an alert. <b>Note:</b> You must specify an Action To or Action From date for this search		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
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
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
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
Limit to Focus	Filters the alert list to where the specified entity is the focus.		X	X	X	X

**Table 37. Alert Search Components (continued)**

Column	Description	Simple Search	Advanced Search			
			AML	Fraud	BC	TC
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
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
Entity Name	The entity name associated with alerts you want to view.		X	X	X	X
Commodity Instrument ID	Filters the alert list by the identification number of the commodity instrument involved in the alert.					
Commodity Instrument Name	Filters the alert list by the name of the commodity instrument involved in the alert.					
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
Trader	Filters the alert list by the name of the trader involved in the alert.					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 identifier 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	
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	

Table 37. Alert Search Components (continued)

Column	Description	Simple Search	Advanced Search			
			AML	Fraud	BC	TC
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

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 38 provides a list of the columns that display in the Alert List matrix.

**Table 38. Alert List Components by Display Configuration by Solution Sets**

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	Standard
Alert ID	X*	X	X	X	X
SC [ore]	X	X	X	X	X
Focus Type	X	X	X	X	X
Focus Name	X	X	X	X	X
Scenario	X	X	X	X	X
Highlights					X
Created [Date]	X	X	X	X	X

**Table 38. Alert List Components by Display Configuration by Solution Sets (continued)**

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	Standard
Status	X	X	X	X	X
Alerts Due [Date and Time]	X	X	X	X	X
Regulatory Reporting Status					X
Regulatory Reporting Type					X
Owner	X	X	X	X	X
Class] Prior					X
SCN [Scenario] Prior					X
Closing Action					X
[Business] Domain					X
[Involved] Security				X	
[Involved] Trader				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
Commodity Instrument ID					
Threshold Set Name	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 39. 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). <b>Note:</b> 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. <b>Note:</b> This feature is available only if Oracle Financial Services Regulatory Reporting (OFSRR) application is installed.	X	

## Alert List Display Configuration

Table 38 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 40. Alert List, General Overview, and Metrics Display Configuration by Solution Sets**

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	Standard
Alert ID	L*	L	L	L	X
SC [ore]	L	L	L	L	X
Focus [Type and Name]	L	L	L	L	X
Scenario	L	L	L	L	X
Highlights	O**	O	O	O	X
Created [Date]	L	L	L	L	X
Status	L	L	L	L	X
Alerts Due [Date and Time]	L	L	L	L	X
Organization	O	O	O	O	
Regulatory Reporting Status	O	O	O	O	X
Regulatory Reporting Type	O	O	O	O	X
Owner	L	L	L	L	X
CL [Class] Prior	O	O	O	O	X
SCN [Scenario] Prior	O	O	O	O	X
Closing Action	O	O	O	O	X
[Business] Domain	O	O	O	O	X
[Involved] Security				L	
[Involved] Trader				L	
[Involved] Service Team ID			L		
[Involved] Registered Representative ID			L		
[Involved] Branch				O	
[Involved] Supervisory Organization				O	
Total/Net Loss Amount		L			
Primary Cost Center		L			



**Table 40. Alert List, General Overview, and Metrics Display Configuration by Solution Sets (continued)**

Column and Field	Anti-Money Laundering	Fraud	Broker Compliance	Trading Compliance	Standard
Linked Cases	L	L	L	L	X
Alerts for Prior Class Count	M <sup>#</sup>	M	M	M	X
Alerts for Prior Scenario Count	M	M	M	M	X
Correlation Membership Count	M	M	M	M	X
Commodity Instrument ID					X

where, L<sup>\*</sup> are fields in the Alert List section; O<sup>\*\*</sup> are fields in the General Overview section; M<sup>#</sup> are fields in the Metrics section



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 41 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 41: Business Tab pages by Scenario Class**

<b>Focus Type</b>	<b>Possible Business Tabs</b>
<b>Scenario Class: Institutional Money Laundering</b>	
Customer (CU)	Account, Customer, and Investment Advisor
External Entity (EN)	External Entity
<b>Scenario Class: Control Room</b>	
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
<b>Scenario Class: Investment Advisor</b>	
Investment Advisor (IA)	Account, Investment Advisor, and Trade
<b>Scenario Class: Money Laundering</b>	
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
<b>Scenario Class: Fraud</b>	
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
<b>Scenario Class: Best Execution</b>	
Order (OR)	Account, Execution, Market Participant, Order, Replay, Security, and Trader
<b>Scenario Class: Trading Compliance</b>	
Account (AC)	Account, Execution, Order, Replay, Security, Trade, and Customer
Customer (CU)	Account, Customer, Execution, Order, Replay, Security and Trade

**Table 41: Business Tab pages by Scenario Class (Continued)**

<b>Focus Type</b>	<b>Possible Business Tabs</b>
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
<b>Scenario Class: Mutual Funds</b>	
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
<b>Scenario Class: Employee Trading</b>	
Employee (EE)	Account, Employee, Security, and Trade
<b>Scenario Class: Customer Risk and Suitability</b>	
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
<b>Scenario Class: Asset Management</b>	
Portfolio Manager (PM)	Account, Employee, Order, and Security
<b>Scenario Class: Energy and Commodity Trading Compliance</b>	
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

# 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 42. You can view an alert if your combination of access controls authorizes you to view the alert and business information. Contact your system administrator for details about your access control permissions.

**Table 42. Access Controls**

Security Layer		Description
Type	Controls	
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 <i>primary organization</i> ; 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.

