

Oracle Financial Services Behavior Detection

User Guide

Release 8.1.2.4.0

March 2023

F17987-01



Oracle Financial Services Behavior Detection

Copyright © 2023 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

For information on third party licenses, click [here](#).

Document Control

Table 1: Revision History

| Date | Edition | Description |
|----------------|----------------------------|--|
| March 2023 | First edition of 8.1.2.4.0 | Updates were made to Chapter 3, <i>Managing Watch List Management</i> to provide details of the watch list and watch list member workflows. |
| December 2022 | First edition of 8.1.2.3.0 | There are no content changes in this release. |
| September 2022 | First edition of 8.1.2.2.0 | There are no content changes in this release. |
| June 2022 | First edition of 8.1.2.1.0 | There are no changes to this guide in this release. |
| March 2022 | First edition of 8.1.2.0.0 | There are no changes to this guide in this release. |
| July 2021 | First edition of 8.1.1.0.0 | Updates were made to reflect the Financial Crimes and Compliance Applications that are no longer being offered by Oracle Financial Services. These products are not supported on release 8.1.1: <ul style="list-style-type: none">• Oracle Financial Services Trading Compliance• Oracle Financial Services Trading Compliance Enterprise Edition• Oracle Financial Services Broker Compliance• Oracle Financial Services Broker Compliance Enterprise Edition• Oracle Financial Services Trade Blotter For more information, see the <i>Oracle Financial Services Behavior Detection Release Notes, Release 8.1.1</i> |
| April 2020 | First edition of 8.0.8.0.1 | There are no content changes to this guide in this release. |
| October 2019 | First edition of 8.0.8.0.0 | This is the first publication of this guide. Much of the information contained in this guide was previously found in the <i>Oracle Financial Services Alert Management User Guide</i> . |

Table of Contents

| | | |
|----------|--|-----------|
| 1 | About this Guide | 7 |
| 1.1 | Who Should Use this Guide..... | 7 |
| 1.2 | How this Guide is Organized..... | 7 |
| 1.3 | Where to Find More Information | 8 |
| 1.4 | Conventions Used in this Guide..... | 9 |
| 2 | About Behavior Detection | 11 |
| 2.1 | Overview of Behavior Detection | 11 |
| 2.2 | Data Loading and Processing..... | 11 |
| 2.3 | Behavior Detection (BD) | 11 |
| 2.3.1 | <i>Scenarios</i> | 12 |
| 2.4 | Post Processing | 12 |
| 2.5 | Ingesting Trusted Pairs | 12 |
| 2.6 | Watch List Management..... | 13 |
| 2.7 | User Privileges | 13 |
| 3 | Getting Started | 15 |
| 3.1 | Accessing OFSAA Applications | 15 |
| 3.2 | Changing the Password | 16 |
| 3.2.1 | <i>Selecting Applications</i> | 17 |
| 4 | Managing Watch List Management | 19 |
| 4.1 | About Watch List Management | 19 |
| 4.1.1 | <i>Introduction</i> | 19 |
| 4.2 | Key Features..... | 19 |
| 4.3 | Watch List Management Architecture | 20 |
| 4.3.1 | <i>Watch List Management Workflows</i> | 20 |
| 4.4 | Accessing Watch List Management | 22 |
| 4.5 | Managing Watch Lists..... | 22 |
| 4.5.1 | <i>Accessing the Managing Watch Lists Page</i> | 22 |
| 4.5.2 | <i>Adding Watch Lists</i> | 23 |
| 4.5.3 | <i>Editing Watch Lists</i> | 24 |
| 4.5.4 | <i>Deactivating Watch Lists</i> | 25 |

| | | |
|----------|--|-----------|
| 4.5.5 | <i>Reviewing Watch Lists</i> | 26 |
| 4.5.6 | <i>Viewing Watch Lists History</i> | 27 |
| 4.5.7 | <i>Searching Watch Lists</i> | 27 |
| 4.6 | Managing Watch List Members | 30 |
| 4.6.1 | <i>Accessing the Watch List Members Page</i> | 31 |
| 4.6.2 | <i>Adding Watch List Members</i> | 31 |
| 4.6.3 | <i>Deactivating a Watch List Member</i> | 34 |
| 4.6.4 | <i>Reviewing Watch List Members</i> | 35 |
| 4.6.5 | <i>Viewing Watch List Member Details</i> | 35 |
| 4.6.6 | <i>Searching Watch List Members</i> | 37 |
| 5 | Setting User Preferences | 40 |
| 5.1 | About Preferences page | 40 |
| 5.2 | Key Features..... | 40 |
| 5.3 | Accessing Preferences Page | 40 |
| 5.4 | Managing Preferences | 40 |
| 5.4.1 | <i>Setting Alert Search and List Options</i> | 41 |
| 5.4.2 | <i>Setting Options for Alert Search</i> | 41 |
| 5.4.3 | <i>Setting the Options for Replay Page</i> | 46 |
| 5.4.4 | <i>Setting Options for Audit Display</i> | 46 |
| 5.4.5 | <i>Saving Preferences</i> | 47 |
| 6 | Alert Components and Tables | 48 |
| 6.1 | Alert Context Information | 48 |
| 6.2 | Search Components | 49 |
| 6.2.1 | <i>Views Search</i> | 50 |
| 6.2.2 | <i>Alert Information</i> | 51 |
| 6.2.3 | <i>Alert List Matrix</i> | 54 |
| 6.2.4 | <i>Additional Information</i> | 56 |
| 6.3 | Alert List Display Configuration | 57 |
| 7 | Business Tabs | 59 |
| 7.1 | Alert Business Tabs..... | 59 |
| 8 | Using Behavior Detection UI | 60 |

| | | |
|-----------|---|-----------|
| 8.1 | Common Screen Elements..... | 60 |
| 8.1.1 | <i>Masthead</i> | 60 |
| 8.1.2 | <i>Buttons</i> | 60 |
| 8.1.3 | <i>Expand/Collapse</i> | 62 |
| 8.1.4 | <i>Field Types</i> | 63 |
| 8.1.5 | <i>ToolTips</i> | 64 |
| 8.2 | Using the Browser | 64 |
| 8.3 | Navigating in Oracle Financial Services Behavior Detection | 64 |
| 8.3.1 | <i>Navigation List</i> | 64 |
| 8.3.2 | <i>Links</i> | 65 |
| 8.3.3 | <i>Search Bars</i> | 65 |
| 8.3.4 | <i>Page Context Controls</i> | 65 |
| 8.3.5 | <i>Business Tabs</i> | 65 |
| 8.3.6 | <i>Paging</i> | 65 |
| 8.4 | Message Pages | 65 |
| 9 | Security within OFSAAI | 66 |
| 10 | Calculating Risk | 67 |
| 10.1 | Determining Entity Risk | 68 |
| 10.1.1 | <i>Deriving Customer Entity Risk</i> | 69 |
| 10.1.2 | <i>Deriving Account Entity Risk</i> | 69 |
| 10.1.3 | <i>Deriving Correspondent Bank Entity Risk</i> | 69 |
| 10.1.4 | <i>Determining Front Office Transaction Party Entity Risk</i> | 72 |
| 10.1.5 | <i>Determining Back Office Transaction Party Entity Risk</i> | 72 |
| 10.2 | Determining Activity Risk | 73 |
| 10.2.1 | <i>Determining Activity Risk on Front Office Transactions</i> | 73 |
| 10.2.2 | <i>Determining Activity Risk on Back Office Transactions</i> | 74 |
| 11 | OFSA Support Contact Details | 76 |
| 12 | Send Us Your Comments | 77 |

0 About this Guide

This guide explains the concepts of Oracle Financial Services Behavior Detection application and provides step-by-step instructions for navigating the Oracle Financial Services web pages, analyzing cases, and researching the business information.

This chapter focuses on the following topics:

- [Who Should Use this Guide](#)
- [How this Guide is Organized](#)
- [Where to Find More Information](#)
- [Conventions Used in this Guide](#)

0.1 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).

0.2 How this Guide is Organized

NOTE

Upgrading customers, please note that the dispositioning of alerts through Alert Management (AM) is no longer supported. AM is only used for verifying the output of the behavior detection scenarios and is no longer used for alert review. By using AM for dispositioning alerts customers will be out of compliance with their support contract.

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. Customers are required 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 the available batch processes to automatically move Alerts from BDF into ECM where correlation rules will promote them to a case. From the case 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.

The *Behavior Detection User Guide* includes the following chapters:

- [Chapter 1, About Behavior Detection](#), provides an overview of the Behavior Detection 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 Behavior Detection, and exit the application.

- [Chapter 3, Managing Watch List Management](#), describes the Oracle Financial Services Watch List Management feature.
- [Chapter 4, Setting User Preferences](#), explains how to setup Oracle Financial Services Behavior Detection preferences.
- [Appendix A, Alert Components and Tables](#), provides the additional information on various components and tables of Behavior Detection.
- [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 Behavior Detection UI](#), explains common elements of the interface.
- [Appendix D, Security within OFSAAI](#), explains how Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) security is used.
- [Appendix E, Calculating Risk](#), describes how Oracle Financial Services Behavior Detection application uses risk calculations as part of managing sensitivity when detecting behaviors of interest.

0.3 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
- Fraud Technical Scenario Descriptions
- Glossary
- Release Notes

These documents are available at the following link:

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

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

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

1 About Behavior Detection

This chapter gives an overview of the Behavior Detection application and discusses the following topics:

- [Overview of Behavior Detection](#)
- [Data Loading and Processing](#)
- [Behavior Detection \(BD\)](#)
- [Post Processing](#)
- [Ingesting Trusted Pairs](#)
- [Watch List Management](#)
- [User Privileges](#)

1.1 Overview of Behavior Detection

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

1.2 Data Loading and Processing

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

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

1.3 Behavior Detection (BD)

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

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

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

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

Depending on your deployment, one or more of the following solution sets are available: Anti-Money Laundering (AML) Fraud (FR), and Currency Transaction Reporting (CTR).

1.3.1 Scenarios

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

1.4 Post Processing

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

- **Augmentation:** Collects additional information related to the matched behavior and focus for pattern detection, which enables proper display or analysis of the generated matches.
- **Match Scoring:** Computes a ranking for scenario matches indicating a degree of risk associated with the detected event or behavior.
- **Alert Creation:** Packages the scenario matches as units of work (alerts), potentially grouping similar matches together, for disposition by end users. This is applicable when multiple matches with distinct scores are grouped into a single alert.
- **Alert Scoring:** Ranks the alerts (including each match within the alerts) to indicate the degree of risk associated with the detected event or behavior.
- **Highlight Generation:** Generates highlights for alerts that appear in the alert list of the Behavior Detection subsystem and stores them in the database.
- **Historical Data Copy:** Identifies the records against which the current batch's scenario runs generated alerts and copies them to archive tables. This displays a snapshot of information as of the time the alert behavior was detected.

1.5 Ingesting Trusted Pairs

Trusted Pairs can be designated by Oracle clients providing trusted pairs via the Data Interface Specification (DIS) file.

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

1.6 Watch List Management

The Watch List Management feature allows watch lists to be added, updated and deactivated. You can also add and deactivate watch list members. A watch list is a list of entries that have known risk characteristics. Watch lists can represent public sources or can be created and managed internally by the institution. Common public sources for watch lists include Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF). Watch lists are associated with a score. See [Chapter 3, Managing Watch List Management](#), for more information.

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

1.7 User Privileges

Oracle Financial Services Behavior Detection allows different types of roles to access the Behavior Detection UI. The various roles are: Alert Viewer, AM Admin, Data Miner, WLM Viewer, WLM Analyst, and WLM Supervisor.

NOTE The Alert Viewer user role is only available in 8.1.1.0 and higher.

Table 1: User Roles and Privileges

| Privileges | Alert Viewer | Data Miner | AM Administrator | WLM Analyst | WLM Viewer | WLM Supervisor |
|---------------------------------|--------------|------------|------------------|-------------|------------|----------------|
| Access to Search and List page. | X | | | | | |
| View Entity details. | X | | | | | |
| Access to Business Tabs. | X | | | | | |

Table 1: User Roles and Privileges

| Privileges | Alert Viewer | Data Miner | AM Administrator | WLM Analyst | WLM Viewer | WLM Supervisor |
|---|--------------|------------|------------------|-------------|------------|----------------|
| Access to BD Administration Tasks. For more information about BD Administration tasks, refer to the Administration Guide . | | | X | | | |
| Access to Scenario Wizard. For more information about Scenario Wizard, refer to the Scenario Wizard Configuration Guide . | | X | | | | |
| View all pages within the WLM application. | | | | X | X | X |
| Create new watch lists and Watch List Members. | | | | X | | X |
| Edit watch lists. | | | | X | | X |
| Deactivate watch lists and Watch List Members. | | | | X | | X |
| View watch lists and Watch List Members in Pending status. | | | | X | X | X |
| Approve recommended action on watch lists and Watch List Members. Actions taken by WLM Supervisor do not need any approvals. | | | | | | X |
| Reject recommended action on watch lists and Watch List Members. Actions taken by WLM Supervisor do not need any approvals. | | | | | | X |

2 Getting Started

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](#)
- [Changing the Password](#)

2.1 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). 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 [Changing the 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.

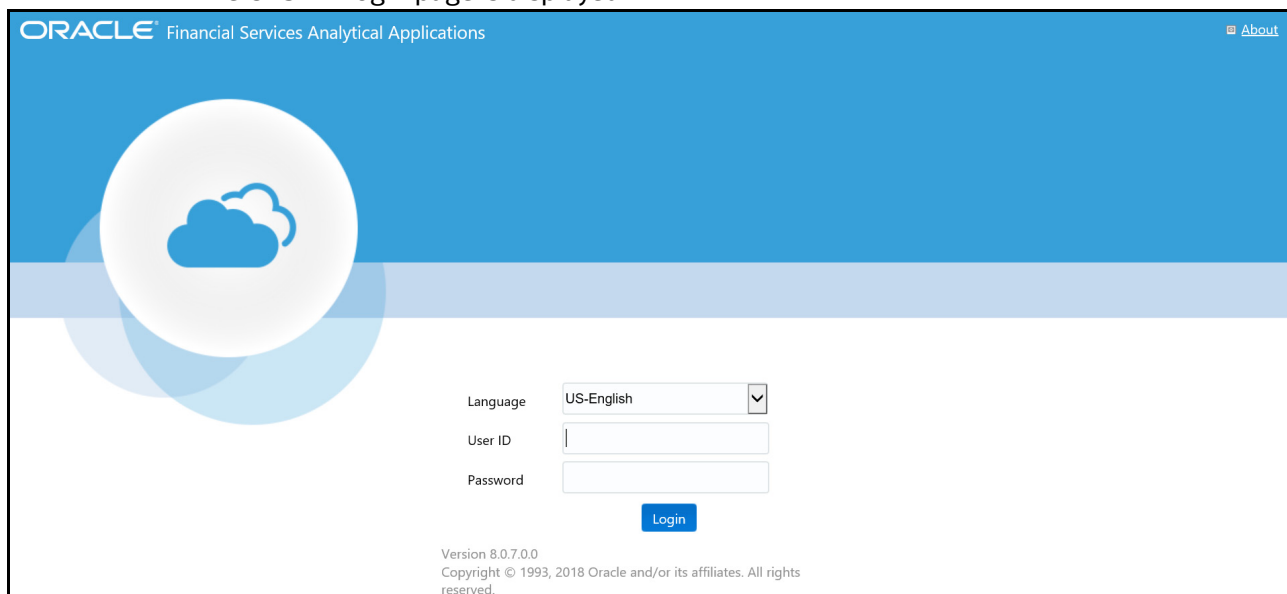


Figure 1: OFSAA Login page

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

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

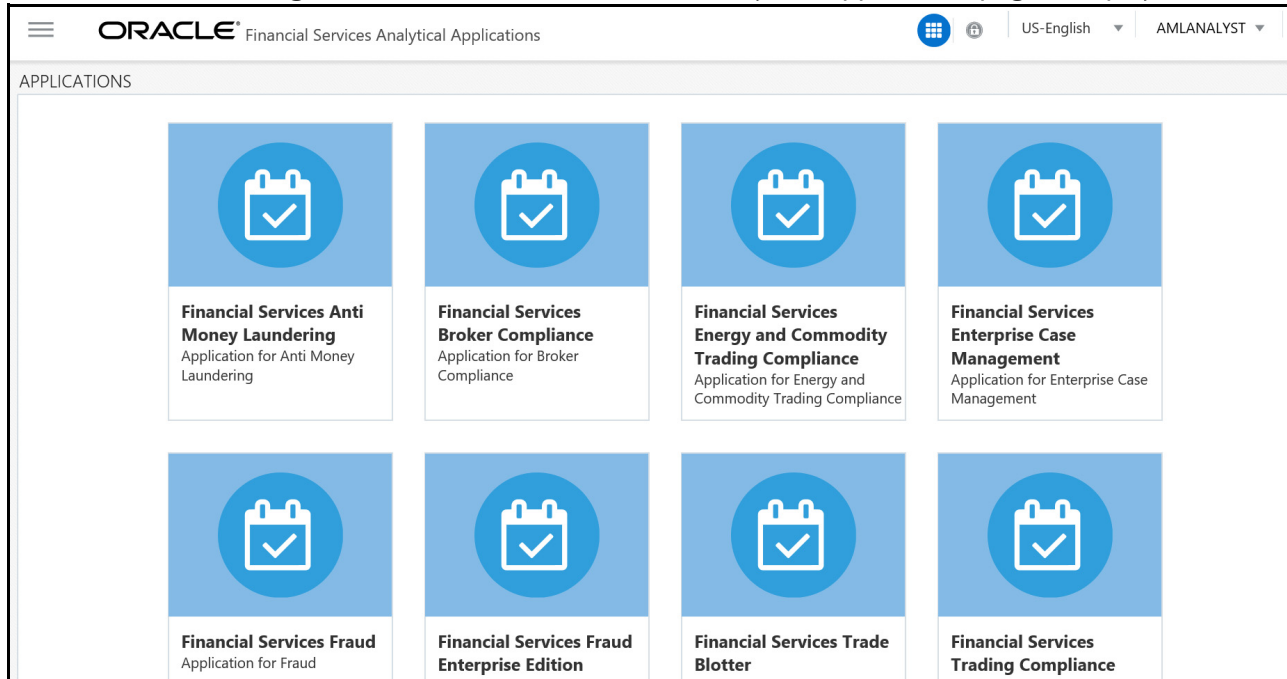


Figure 2: Oracle Financial Services Analytical Applications page

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, Managing Security Restrictions](#). You can use the OFSAA Application page to access the Oracle Financial Services applications in your environment.

2.2 Changing the Password

For security purposes, you can change the password. To change the password, follow these steps:

1. Navigate to the OFSAA Applications page.

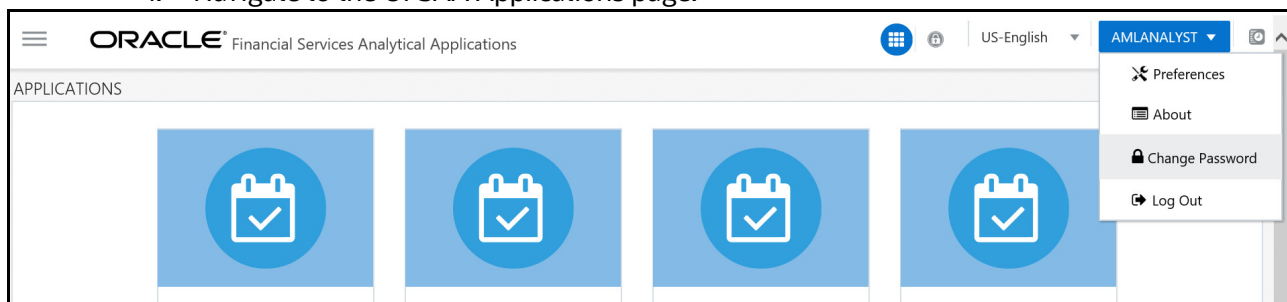
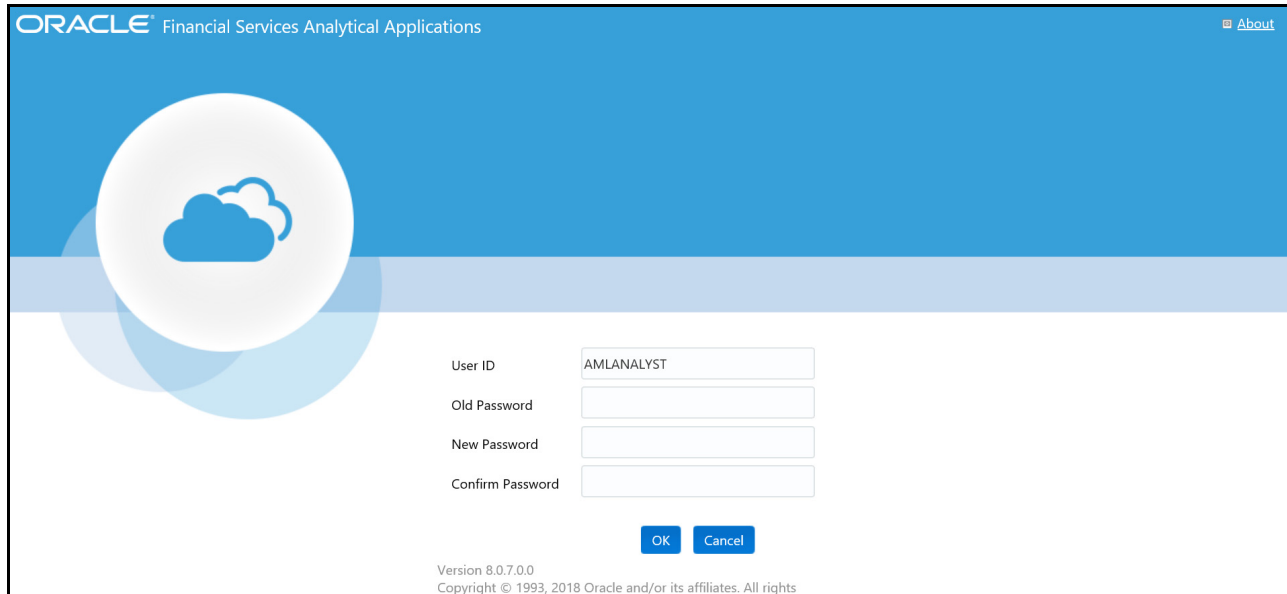


Figure 3: Change Password

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



The screenshot shows the Oracle Financial Services Analytical Applications interface. At the top left is the Oracle logo and the text "Financial Services Analytical Applications". At the top right is an "About" link. The main content area features a large circular icon with a cloud and a key. Below this is a form with four input fields: "User ID" (containing "AMLANALYST"), "Old Password", "New Password", and "Confirm Password". At the bottom of the form are "OK" and "Cancel" buttons. At the very bottom, it says "Version 8.0.7.0.0" and "Copyright © 1993, 2018 Oracle and/or its affiliates. All rights reserved."

Figure 4: 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.

2.2.1 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.

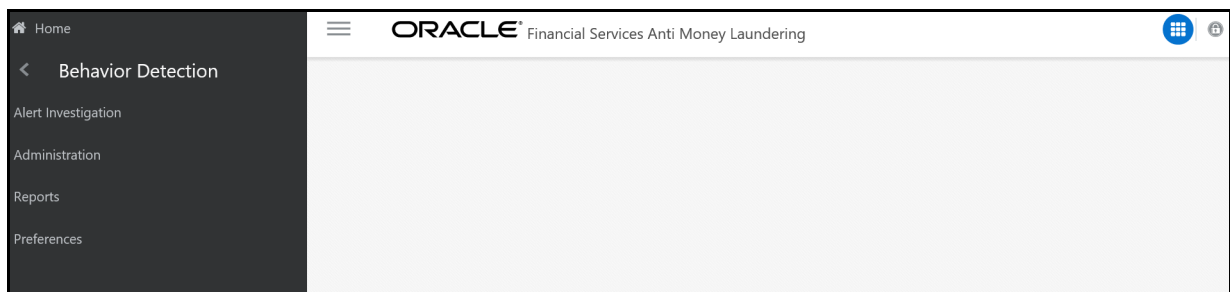


Figure 5: Behavior Detection Anti Money Laundering page

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

3 Managing Watch List Management

This chapter describes the Watch List Management functionality and gives step-by-step instructions for using it. The following topics are covered in this chapter:

- [About Watch List Management](#)
- [Accessing Watch List Management](#)
- [Managing Watch Lists](#)
- [Managing Watch List Members](#)

3.1 About Watch List Management

This section covers the following topics:

- [Introduction](#)
- [Key Features](#)
- [Watch List Management Architecture](#)

3.1.1 Introduction

A Watch List is a list of entries that are known to have the same level of risk characteristics. Watch Lists can represent public sources or can be created and managed internally by the institution. Watch List data can originate from public sources. For example, the Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF) or private sources like a client's list of entities on which suspicious activity reports are filed.

Oracle Financial Services Watch List Management gathers risk metrics based on the processing of risk or trust values from client records during data ingestion. You can then use these risk metrics to find high-risk behaviors. Watch lists and their entries conform to types and characters that the *Data Interface Specification (DIS)* specifies; OFSBD audits all changes.

Public lists used by clients are huge, and can contain typographical errors. Without the Watch List Management UI, clients must accept these errors, or manually correct them each time the list is updated and transformed for delivery to Ingestion. Some clients established staging databases in which they applied corrections, managed internal lists, and transformed lists into the Oracle Financial Services DIS format.

The staging database process created the following limitations:

- Inefficient processing
- Increased complexity
- Increased cost for installation
- Requirement that clients review

3.2 Key Features

The Watch List Management UI allows you to perform the following actions:

- Add new watch lists
- Add new watch list members to watch lists
- Modify watch lists

- Deactivate existing watch list members and watch lists
- Review recommended actions to approve or reject

3.3 Watch List Management Architecture

The following figure depicts the architecture of Watch List Management.

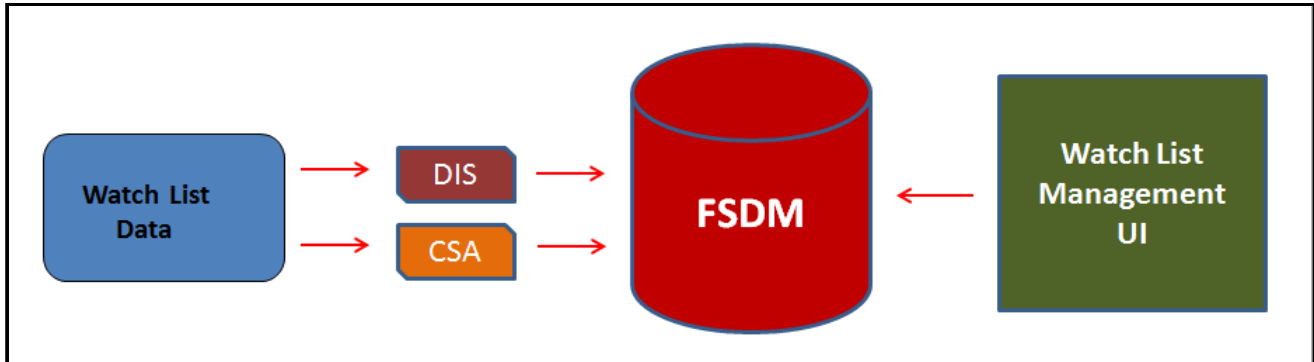


Figure 1: Watch List Management Architecture

3.3.1 Watch List Management Workflows

This section describes the workflow of Watch Lists and Watch List Members.

NOTE: Only an Analyst requires approval from a Supervisor to accomplish actions in the Watch Lists and Watch List Members workflow. The Supervisor role does not require any approval.

The following figure shows the Watch Lists and Watch List Members Management workflow.

Figure 2: Watch List and Watch List Members Management Workflow

3.3.1.1 Watch Lists Workflow

1. Using the UI, an Analyst adds, modifies, or deactivates a watch list. These actions are recommended to the Supervisor for review.
2. The Supervisor reviews the actions recommended by the Analyst. The status of the watch list is Pending in Review Pending tab.
3. If the Supervisor approves the action, the data is updated in the Watch List main table and displayed in the Watch List tab with Active status.

If the Supervisor rejects the action, the data is not updated and displayed in the Review Pending tab with Rejected status.

The following table describes the Manage Watch Lists workflow.

Table 1: Manage Watch List Workflow

| Action | Description | Roles |
|--------------------|-------------------------------|-------------------------|
| Adding Watch Lists | User can add new watch lists. | Analyst/ WLM Supervisor |

Table 1: Manage Watch List Workflow

| Action | Description | Roles |
|--------------------------|---|-------------------------|
| Editing Watch Lists | User can modify existing watch lists which are in Active status. | Analyst/ WLM Supervisor |
| Deactivating Watch Lists | User can deactivate existing watch lists which are in Active status. Note: User cannot activate the deactivated watch lists. | Analyst/ WLM Supervisor |
| Reviewing Watch Lists | User can review the actions recommended by the Analyst and take appropriate actions to approve or reject. | WLM Supervisor |

NOTE Analysts can only view the status of watch list in the Review Pending tab.
The watch list is locked when the Supervisor selects an existing watch list for reviewing a modification or deactivation.

3.3.1.2 Watch List Members Workflow

1. Using the UI, an Analyst adds or deactivates a watch list member. These actions are recommended to the Supervisor for review.
2. The Supervisor reviews the actions recommended by the Analyst. The status of the watch list member is Pending in Review Pending tab.
3. If the Supervisor approves the action, the data is updated in the Watch List Member main table and displayed in the Watch List Member tab with Active status.

If the Supervisor rejects the action, the data is not updated and displayed in the Review Pending tab with Rejected status.

NOTE Analysts can only view the status of a watch list in the Review Pending tab.
The watch list member is locked when the Supervisor selects an existing watch list member for reviewing a deactivation.

The following table describes the Manage Watch List Members workflow.

Table 2: Manage Watch List Members Workflow

| Action | Description | Roles |
|----------------------------------|---|-------------------------|
| Adding Watch List Members | User can add new watch list members to a watch list. | Analyst/ WLM Supervisor |
| Deactivating a Watch List Member | User can deactivate existing watch list members which are in Active status. Note: User cannot activate the deactivated watch list members. | Analyst/ WLM Supervisor |

Table 2: Manage Watch List Members Workflow

| Action | Description | Roles |
|------------------------------|---|----------------|
| Reviewing Watch List Members | User can review the actions recommended by the Analyst and take appropriate actions to approve or reject. | WLM Supervisor |

3.4 Accessing Watch List Management

To access the Watch List Management page, follow these steps:

1. Navigate to the OFSAA Application page. For more information on how to navigate to the OFSAA Application, see [Chapter 2, Getting Started](#).
2. Select the **Financial Services Anti-Money Laundering**. The Behavior Detection- Anti-Money Laundering page is displayed.
3. Select **Behavior Detection** from the Navigation List.
4. Select **Watch List Management**.
5. Select either **Manage Watch Lists** or **Manage Watch List Members**, depending on your needs.

3.5 Managing Watch Lists

This section explains how to add, modify, and deactivate watch lists.

The following sections describe how to manage watch lists:

- [Accessing the Managing Watch Lists Page](#)
- [Adding Watch Lists](#)
- [Editing Watch Lists](#)
- [Deactivating Watch Lists](#)
- [Viewing Watch Lists History](#)
- [Searching Watch Lists](#)

3.5.1 Accessing the Managing Watch Lists Page

To access the Manage Watch Lists page, follow these steps:

1. Select **Behavior Detection** from the Navigation List. Then select **Watch List Management**.
2. Select **Manage Watch Lists**. The Watch List Management page is displayed.

ORACLE Financial Services Anti Money Laundering en_US ALERTVIEWER

Home > Watch List Search

Search Search Reset

| | | |
|-----------------|------------------|------------|
| Watch List Name | Status date from | MM/dd/yyyy |
| Watch List Code | Status Date To | MM/dd/yyyy |
| List Type | Created By | |
| Risk Level | Created From | 01/14/2023 |
| Public/Private | Created To | 03/15/2023 |
| Reason added | Business Domain | |
| Status | Jurisdiction | |

Watch List Review Pending Changes

Manage Watch Lists [Share] [Refresh] [Refresh]

Add Deactivate

| Status | Watch List Code | Watch List Name | List Type | Risk Level |
|--------------------------------------|---------------------|-----------------|-----------|------------|
| <input type="checkbox"/> Deactivated | S03 | Sample_03_1 | Exemption | -2 |

Figure 3: Watch List Management

3. Select **Behavior Detection** from the Navigation List. Then select **Watch List Management**.
4. Select **Manage Watch Lists**. The Manage Watch Lists Search and List page is displayed.

3.5.2 Adding Watch Lists

To add new watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.
2. Click **Add**. The Add Watch List window is displayed.

Add Watch List [Close]

| | |
|--------------------------------------|--------------------------------------|
| * Watch List Name | Reason added |
| * Watch List Code | * Business Domain |
| * List Type <i>Select a value</i> | * Jurisdiction <i>Select a value</i> |
| * Risk Level | * Comments |
| Public/Private <i>Select a value</i> | * Processing Batch Name |

[Cancel] [Save]

Figure 4: Add Watch List window

3. Enter the following information in the appropriate fields.

Table 3: Add Watch List fields

| Field | Description |
|-----------------------|---|
| Watch List Name | Enter the name of the watch list you wish to add. |
| Watch List Code | Enter the unique, three character identifier for the watch list you wish to add. |
| List Type | Select the type of watch list you wish to add from the drop-down list. The Watch List Type you select helps displayed your options in the Risk Level drop-down list. |
| Risk Level | Select the degree of risk associated with the watch list you wish to add from the drop-down list. The drop-down list is displayed with specific values based on your selection in the Watch List Type drop-down list. If you have selected the Watch List Type Trust or Exemption, the system automatically assigns a risk level -1 and -2 (respectively) to the watch list and you need not select a value. |
| Public/Private | Select whether the watch list you are adding is public or private from the drop-down list. |
| Reason Added | Enter the reason to add new watch list. |
| Business Domain | Select the business domain you wish to associate with the watch list from the drop-down list. You must be mapped to the business domain associated with the watch list to be able to view it on the UI. |
| Jurisdiction | Select the jurisdiction you wish to associate with the watch list from the drop-down list. You must be mapped to the jurisdiction associated with the watch list to be able to view it on the UI. |
| Comments | Enter appropriate comments for this watch list. |
| Processing Batch Name | Select the Processing Batch you wish to associate with the watch list from the drop-down list. |

4. Click **Save**. A confirmation message displays.
5. Click **OK**.

3.5.3 Editing Watch Lists

To modify existing watch lists which are in *Active* status, follow these steps.

1. Navigate to the Manage Watch Lists Search and List page.
2. Select a watch list you wish to modify. Click **Edit**. The Edit Watch List window is displayed.

Figure 5: Edit Watch List window

3. Modify the necessary information in the appropriate field.

NOTE You cannot remove a business domain or jurisdiction that is currently linked with at least one watch list member associated with this watch list.

4. Click **Save**. The following message is displayed:
You have selected to edit this record. Click OK to continue and save changes.
5. Click **OK**.

3.5.4 Deactivating Watch Lists

This section describes how to deactivate one or more watch lists in *Active* status.

- NOTE**
- To deactivate a watch list all watch list members must be unlocked.
 - If you add watch list members to the deactivated watch list, the watch list members are also deactivated.
 - The Watch List Management Utility does not allow you to reactivate the deactivated watch lists. Therefore, you must perform the deactivation action carefully.
 - If you deactivate a watch list, any watch list members associated with that watch list will be deactivated.

To deactivate watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.

2. Select one or more watch lists. The status of the selected watch lists must be *Active*.

NOTE

If you select a watch list which is already recommended for deactivation, the following message is displayed:

Pending watch lists (members) cannot be deactivated.
Please select only active watch lists (members).

3. Click **Deactivate**. The Watch List Action window displays.

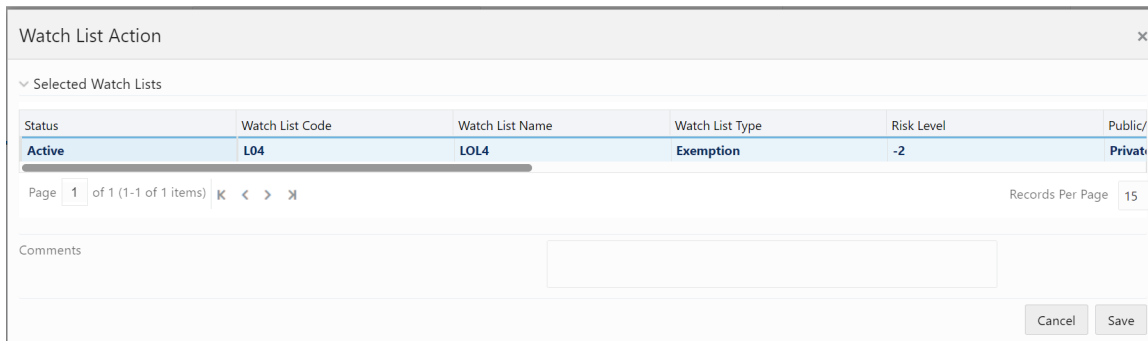


Figure 6: Watch List Action window

The Watch List Action window lists the watch lists you have selected to deactivate.

4. Enter the justification for deactivating watch lists in the Comments field.
5. Click **Save**. A confirmation message is displayed.
6. Click **OK**.

3.5.5 Reviewing Watch Lists

When an Analyst recommends to add a new watch list, modify an existing watch list, or deactivate a watch list, the Supervisor reviews the recommended action to approve or reject.

NOTE

Only a Supervisor can perform this action.

The newly added watch list is not locked when it is under review. The watch list is locked when the Supervisor selects an existing watch list for reviewing a modification or deactivation.

Analysts can view the status of watch lists in the Review Pending Changes tab.

To review a watch list, follow these steps:

1. Navigate to the Manage Watch List page. Click the **Review Pending Changes** tab.
2. Select one or more watch lists in Pending status.
3. Click either **Approve** or **Reject**. The Review Watch List window is displayed.

The Review Watch Lists window lists the watch lists you have selected to review.

4. Enter comments in the **Comments** field to support your action.

5. Click **Save**. The watch list or lists are approved or rejected. A confirmation message is displayed.
6. Click **OK** on the confirmation window to navigate to the Manage Watch Lists page. The updated watch lists are displayed with relevant status.

3.5.6 Viewing Watch Lists History

To view watch list history, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.
2. Select a required watch list. Click **History**. The Watch List History window is displayed.

| Action Name | Date and Time | By | Status | Watch List Name | List Type | Risk Level | Public/Private | Reason Added | Comments | Business Domain | Jurisdiction |
|-------------|---------------------|-----------|--------|-----------------|-----------|------------|----------------|--------------|----------|-----------------|--------------|
| Created | 09/22/2013 02:26:04 | SUPERV... | Active | Test | Risk List | 1 | Private | Y | tes | C/WS.EMP... | SA |

Figure 7: Watch List History window

The history of the watch list displays in ascending order, based on date and time the action is recorded. The following table describes the columns in the Watch List History window.

Table 4: Watch List History Columns

| Column Name | Description |
|-----------------|--|
| Action Name | Displays the name of the action which was taken on the watch list. |
| Date and Time | Displays the date and time at which the action was taken. |
| By | Displays the name of the user who has taken the action on the. |
| Status | Displays the status of the watch list after the action was recorded. |
| Watch List Name | Displays the name of the watch list after the action was recorded. |
| List Type | Displays the list type associated with the watch list after the action was recorded. |
| Risk Level | Displays the risk level assigned to the watch list after the action was recorded. |
| Public/Private | Displays the whether the watch list was public or private after the action was recorded. |
| Reason Added | Displays the description of the watch list after the action was recorded. |
| Comments | Displays any user comments recorded with the action. |
| Business Domain | Displays the business domain associated with the watch list after the action was recorded. |
| Jurisdiction | Displays the jurisdiction associated with the watch list after the action was recorded. |

3. Click **Close** to close the Watch List History window.

3.5.7 Searching Watch Lists

The Manage Watch Lists Search section enables you to search for watch lists based on criteria that you provide within this search section. Drop-down lists and text boxes enable you to filter available watch

lists more precisely for analysis. A blank value in a filter means that no specific value is selected. If the blank value is selected, it will have no impact on filter criteria.

The following fields are displayed:

- **Created From:** Displays today's date - 60 days
- **Created To:** Displays today's date.

If a search is performed with blank values in fields, then the results are displayed without applying filters on those fields. In particular, if a status is not specified, the system applies a set of underlying rules to the records returned in the results. Blank search is not supported. You need to enter one or more search criteria in order to execute a search.

To search watch lists, follow these steps:

1. Navigate to the Manage Watch Lists Search and List page.

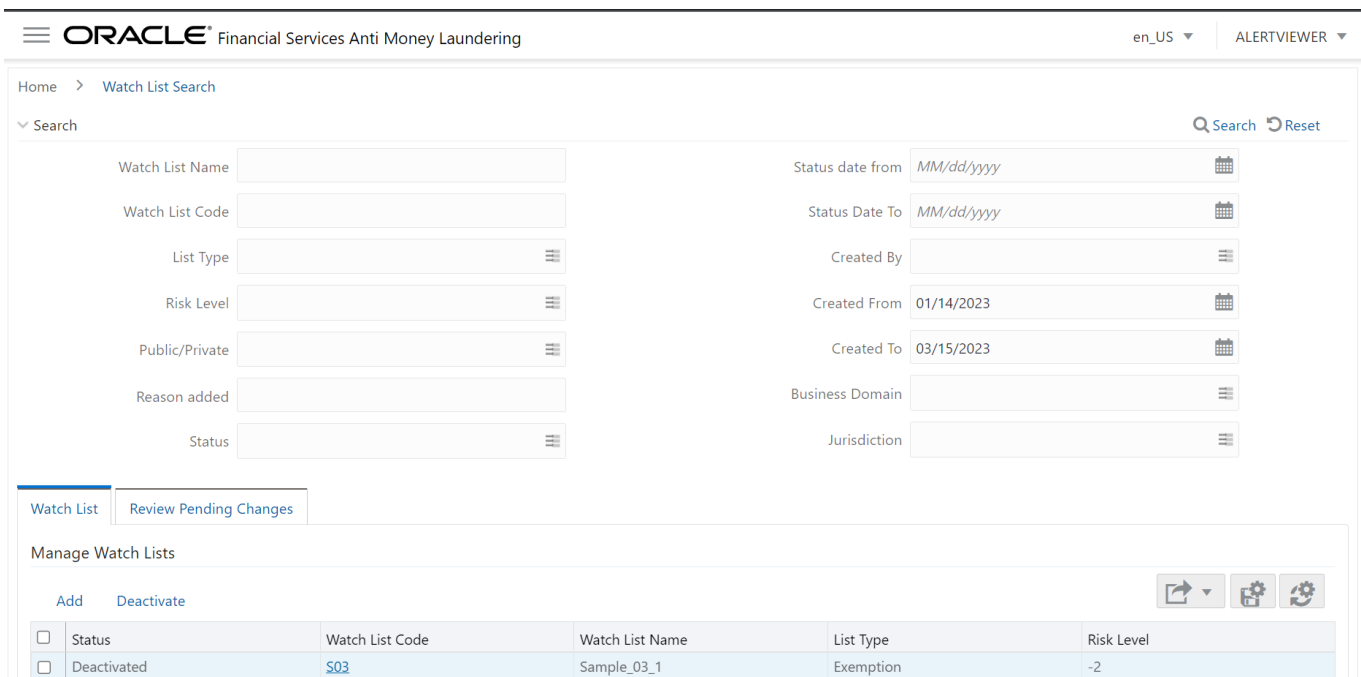


Figure 8: Manage Watch Lists page

2. Enter the following information in the respective fields.

Table 5: Watch List Search Section Filters

| Field | Description |
|-----------------|--|
| Watch List Name | Enter the name of the watch list that you wish to search for. |
| Watch List Code | Enter the unique three-character identifier of the watch list that you wish to search for. |
| List Type | Select the type of watch list you wish to search for from the drop-down list. |
| Risk Level | Select the degree of risk associated with the watch list from the drop-down list. |

Table 5: Watch List Search Section Filters

| Field | Description |
|------------------|--|
| Public/Private | Select whether the watch list you are searching for is a public or private watch list. |
| Reason Added | Enter the description of the watch list you wish to search for. |
| Status | Displays current status of the watch list. There are four possible statuses: <ul style="list-style-type: none"> • Active • Deactivated • Pending • Rejected If you have access to view only Deactivated lists, this field will be blank. |
| Status Date From | Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database. |
| Status Date To | Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database. |
| Created From | Select a date range from which the watch list was created. By default, this field selects a date 60 days ago. |
| Created To | Select a date range during which the watch list was created. By default, this field selects today's date. |
| Created By | Select the name of the watch list creator from the drop-down list of all users that have a role with permission to Add Lists and Watch List Members. |
| Business Domain | Select the business domain associated with the watch list. You must be mapped to the business domain that is associated with the watch list to be able to view it on the UI. |
| Jurisdiction | Select the jurisdiction associated with the watch list. You must be mapped to the jurisdiction that is associated with the watch list to be able to view it on the UI. |

3. Click **Go**. The relevant list of watch lists is displayed.

3.5.7.1 Viewing Watch Lists and Review Pending Tabs

This section explains the search result of watch lists. Most of the column headings in the Watch Lists section are sortable. You will be able to sort each column by right-clicking on the column header and choosing ascending or descending options.

The column heading that is selected for the sorting option displays with an arrow beside it. The direction of the arrow indicates the sort order (ascending or descending). When you click a different column heading, the arrow displays beside that column with the direction indicating the sort direction. Oracle Financial Services Behavior Detection refreshes the list and re-sorts the watch lists display by that field, retaining the current list entries based upon the criteria you selected in the Watch List Search. If you click the same column heading again, Oracle Financial Services Behavior Detection sorts the column in the opposite direction.

3.5.7.1.1 Watch Lists Tab Columns

The following table describes the columns in the Watch Lists section.

Table 6: Watch List Columns

| Column Name | Description |
|-----------------|---|
| Status | Displays the current status of the watch list and an icon that represents the status. The following statuses may display: <ul style="list-style-type: none"> • Pending • Rejected • Active • Deactivated |
| Watch List Code | Lists the unique three-character identifier of the watch list as a hyperlink. Click the Watch List Code to view the Manage Watch List Members page, which displays all members associated with the selected watch list. Use the bread crumbs to navigate back to the Manage Watch Lists page. |
| Watch List Name | Displays the name of the watch list. |
| List Type | Displays the type associated with the watch list. |
| Risk Level | Displays the degree of risk associated with members of the watch list. |
| Public/Private | Indicates the origin of the watch list: <ul style="list-style-type: none"> • Public: Indicator of a public source as the origin of the watch list. • Private: Indicator of a private source as the origin or watch list; that is, a list maintained by the Oracle client. • All: Indicator of both Public and Private sources of watch lists. |
| Reason Added | Displays the watch list description. |
| Business Domain | Displays the business domains associated with the watch list. You must be mapped to the business domain that is associated with the watch list to be able to view it on the UI. |
| Jurisdiction | Displays the jurisdictions associated with the watch list. You must be mapped to the jurisdiction that is associated with the watch list to be able to view it on the UI. |
| Created By | Name of the user who created the watch list. |
| Create Date | Date the watch list was created. |
| Status Date | The date when the status of this watch list was last updated. |
| Edit | Click the Edit button to open the Edit Watch Lists pop-up window and edit the watch list details. The Edit button is enabled only when you have access to edit and the list is not in Deactivated status. Deactivated lists cannot be edited. For more information, refer to Editing Watch Lists, on page 24,. |
| History | Click the History button to open the Watch Lists History pop-up window and view the watch list history. For more information, refer to Deactivating Watch Lists , on page 25,. |

3.6 Managing Watch List Members

This section explains how to add, deactivate, and search watch list members.

This section covers the following topics:

- [Accessing the Watch List Members Page](#)
- [Adding Watch List Members](#)
- [Deactivating a Watch List Member](#)
- [Viewing Watch List Member Details](#)
- [Searching Watch List Members](#)

3.6.1 Accessing the Watch List Members Page

To access the Watch List Members page, follow these steps:

1. Select **Behavior Detection** from the Navigation List. Then select **Watch List Management**.
2. Select **Manage Watch List Members**. The Watch List Members Search and List page is displayed.

Figure 9: Watch List Members Search and List page.

3.6.2 Adding Watch List Members

This section allows you to add new watch list members to the watch list.

NOTE If you add watch list members to a deactivated watch list, the watch list members are also deactivated.

To add a watch list member, follow these steps:

1. Navigate to the Watch List Members Search and List page.

2. Click **Add**. The Add Watch List Member window is displayed.

Figure 10: Add Watch List Member window

3. Enter the following information in the appropriate fields.

Table 7: Add Watch List Member fields

| Field | Description |
|-------------------|---|
| Watch List Code | Select the unique identifier Watch List Code from the drop- down list. This is the watch list you wish to associate with this member. |
| Watch List Name | Displays the name of the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| Watch List Type | Displays the watch list type for the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| Watch List Status | Displays the status of the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| Risk Level | Displays the risk level of the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| Public/Private | Displays the whether the watch list associated with this member is public or private. This field is pre-populated based on the Watch List Code. |
| Business Domain | Displays the business domains associated with the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| Jurisdiction | Displays the jurisdiction associated with the watch list associated with this member. This field is pre-populated based on the Watch List Code. |
| ID Type | Select the type of entity represented by the member from the drop-down list. |
| ID | Enter the identifier or name of the member you wish to add. |
| Source | Select the source of the member from the drop-down list. |
| Business Cluster | Select the business cluster associated with the member you wish to add from the drop-down list. |
| Reason Added | Select the reason this member is being added from the drop-down list. |
| Description | Enter a description for this member. |
| Comments | Enter appropriate comments to add this member. |

Table 7: Add Watch List Member fields

| Field | Description |
|-----------------|---|
| Business Domain | <p>By default, this drop-down list is disabled and the Inherit Watch List Business Domains Check box is checked. This means that the watch list member inherits all domains assigned to the parent watch list (selected via the Watch List Code).</p> <p>Uncheck the Inherit Watch List Business Domains check box to enable the Domains drop-down list, which is populated with all domains assigned to the watch list. If a watch list has not been selected via the Watch List Code, then the Domains drop-down list is blank.</p> <p>Check the check box again to clear and disable the Domains drop-down list.</p> |
| Jurisdiction | Displays jurisdiction associated with the watch list member. |

NOTE A watch list member must be associated with a watch list.

The values in the Business Cluster and Reason Added fields in the Add Watch List Member window displays based on the attribute values available in the Reference Table Detail table.

The following table describes the attribute values for these fields:

Table 8: Values in the Business Cluster and Reason Added fields

| Business Table | Business Field | Code Set Identifier | Instruction |
|------------------|------------------|-----------------------------------|--|
| Watch List Entry | Reason Added | Watch List Entry Reason Added | <ul style="list-style-type: none"> Code 1: Code for the Reason Added Code 2: not used Code Description: Description of reason for creating the watch list entry. Code Additional Information: not used |
| Watch List Entry | Source | Watch List Entry Source | <ul style="list-style-type: none"> Code 1: Code for the Source Code 2: not used Code Description: Description of source of the watch list entry. Code Additional Information: not used |
| Watch List Entry | Business Cluster | Watch List Entry Business Cluster | <ul style="list-style-type: none"> Code 1: Code for the business cluster Code 2: not used Code Description: Description of business cluster of the watch list entry. Code Additional Information: not used |

- Click **Save**. A confirmation message is displayed.
- Click **OK**.

3.6.3 Deactivating a Watch List Member

This section guides how to deactivate watch list members. The Watch List Management option does not allow you to reactivate the deactivated watch list members.

To deactivate a watch list member, follow these steps:

1. Navigate to the Watch List Members Search and List page.
2. Select one or more watch list members. The status of the selected watch list members must be *Active*.

NOTE

If you select a watch list member which is already recommended for deactivation by another user, the following message is displayed:

Pending watch lists (members) cannot be deactivated.
Please select only active watch lists (members).

3. Click **Deactivate**. The Watch List Member Action window is displayed.

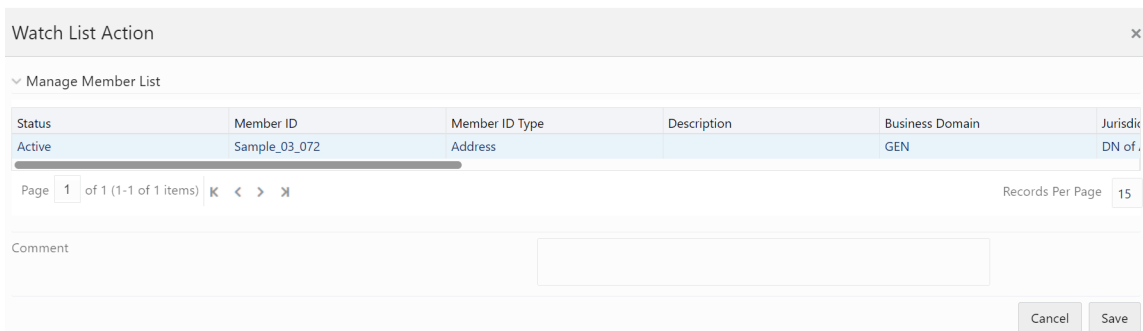


Figure 11: Watch List Member Action window

The Deactivate Watch List Member window lists the watch list members you have selected to deactivate.

4. Enter justification to deactivate watch list member in the Comments field.
5. Click **Save**. The following message is displayed. *The following watch list members are being deactivated. Click OK to Save. Click Cancel to go back to the Watch List Member Action popup.*
6. Click **OK**.

3.6.4 Reviewing Watch List Members

When an Analyst recommends to add new watch list members or deactivate watch list members, a Supervisor reviews the recommended action to approve or reject.

NOTE Only a Supervisor can perform this action.
The newly added watch list member is not locked when it is under review. The watch list member is locked when the Supervisor selects an existing watch list member for reviewing a deactivation
An Analyst can view the status of watch list members in the Review Pending Changes tab.

To review a watch list member, follow these steps:

1. Navigate to the Watch List Members Search and List page.
2. Click the **Review Pending Changes** tab.
3. Select one or more watch list members in the Pending status.
4. Click either **Approve** or **Reject**. The Review Watch List Members window is displayed.

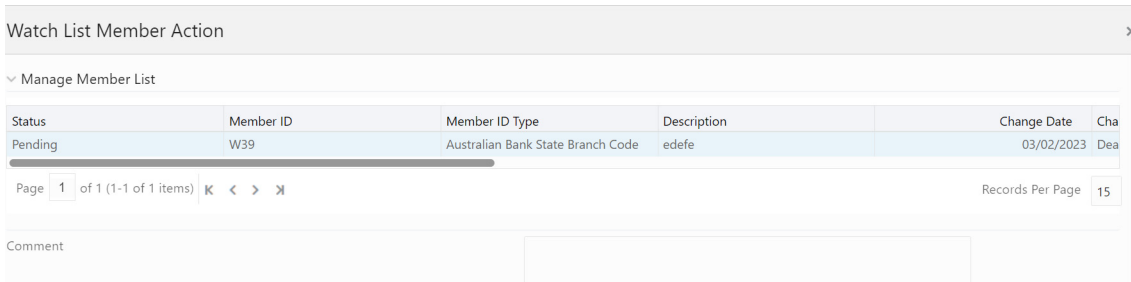


Figure 12: Review Watch List Members Window

The Review Watch List Members window lists the watch list members you have selected to review.

5. Enter comments in the **Comments** field to support your action.
6. Click **Save**. The watch list member or members are approved or rejected. A confirmation message displays.
7. Click **OK**. The updated watch lists are displayed with relevant status.

3.6.5 Viewing Watch List Member Details

This section allows you to a view complete history of the Watch List Members details. To view member details, follow these steps:

1. Navigate to the Watch List Members Search and List page.

- Click the **Member ID** of the member you wish to view details for. The Watch List Member Details and History window is displayed.

| Member Details | | | | |
|---|---------------------|--------------------|--------------|------------------------|
| Watch List Details | | | | |
| Watch List Name: | A9 | Watch List Code: | A9 | |
| Watch List Type: | Risk List | Watch List Status: | Active | |
| Public/Private: | Private | Risk Level: | 0 | |
| Member Details | | | | |
| Member ID: | 1st member of A9 | Member ID Type: | Central Bank | |
| Status: | Active | Status Date: | 09/27/2013 | |
| Source: | -- | Business Cluster: | -- | |
| Business Domain: | INST | Jurisdiction: | DN of AMEA | |
| Created By: | FCCM SUPERVISOR | Create Date: | 09/27/2013 | |
| Reason Added: | Internet | | | |
| Description: | -- | | | |
| Member History (1) Expand All | | | | |
| Action Name | Date and Time | Status | By | Comments |
| Created | 09/27/2013 02:31:06 | Active | SUPERVISOR | Illegal Money Trasfer. |

Figure 13: Watch List Member Details and History window

The following table describes the columns in the Watch List Member Details and History window.

Table 9: Fields in Watch List Member Details and History

| Field Name | Description |
|-------------------|--|
| Watch List Name | Displays the watch list name. |
| Watch List Code | Displays the watch list unique identifier. |
| Watch List Type | Displays the type of watch list. |
| Watch List Status | Displays the status of watch list. |
| Risk Level | Displays the degree of Risk associated with the watch list. |
| Public/Private | Displays the public or private watch list. |
| Status | Displays the current status of this member. |
| Status Date | Last status change date for this member. |
| Created By | Displays the creator of the member. |
| Create Date | Displays the date the member was created. |
| ID Type | Displays the type of entity represented by the member. |
| ID | Displays the identifier or name of a member. The value for this field is automatically populated as the Entity Identifier 1 Text field in the Watch List Entry FSDM table. |
| Source | Displays the source of the member. |
| Business Cluster | Displays the business cluster associated with the member. |
| Business Domain | Displays the business domain(s) associated with the member. If the member is associated with more than one domain, the UI displays available business domains in alphabetical order. |

Table 9: Fields in Watch List Member Details and History

| Field Name | Description |
|--------------|---|
| Jurisdiction | Displays the jurisdiction associated with the member. |
| Reason Added | Displays the reason member was added. |
| Description | Displays the description of the watch list member. |

3.6.6 Searching Watch List Members

The Manage Watch List Members Search section enables you to search for watch list members based on criteria that you provide within this search section. Drop-down lists and text boxes enable you to filter available watch list members more precisely for analysis.

The following fields are displayed:

- **Created From:** Displays today's date - 60 days
- **Created To:** Displays today's date

To search watch list members, follow these steps:

1. Navigate to the Manage Watch List Members Search and List page.

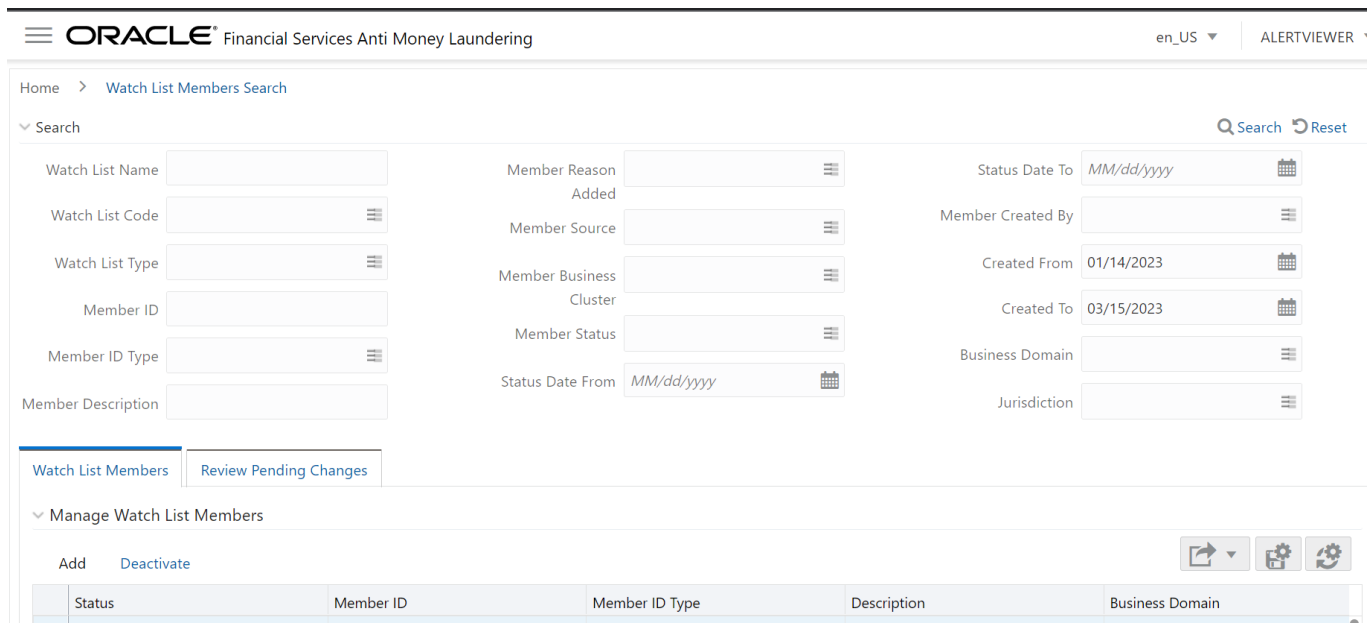


Figure 14: Manage Watch List Members page

2. Enter the following information in the respective fields.

Table 10: Watch List Members Search Section Filters

| Fields | Description |
|-----------------|---|
| Watch List Name | Enter the name of the watch list associated with the watch list member you wish to search for. |
| Watch List Code | Enter the unique, three character identifier of the watch list associated with the watch list member that you wish to search for. |

Table 10: Watch List Members Search Section Filters

| Fields | Description |
|-------------------------|--|
| Watch List Type | Select the type of watch list associated with the watch list member you wish to search for from the drop-down list. |
| Member ID | Enter the identifier or name of the member on the watch list. |
| Member ID Type | Select the type of entity represented by the member you wish to search for from the drop-down list. |
| Member Description | Enter a description for the watch list member. |
| Member Reason Added | Select the reason the member was added from the drop-down list. |
| Member Source | Select the source of the member you wish to search for from the drop-down list. |
| Member Business Cluster | Select the business cluster associated with the member you wish to search for from the drop-down list. |
| Member Status | Select the status of the watch list member you wish to search for from the drop-down list. There are four possible statuses: <ul style="list-style-type: none"> • Active • Deactivated • Pending • Rejected If you have access to view only Deactivated lists, this field will be blank. |
| Status Date From | Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database. |
| Status Date To | Select the date range when the last status change took place. This drop-down list is populated with values based on your mapping to statuses in the database. |
| Member Created By | Select the name of the user who created the watch list member you wish to search for in the drop-down list. |
| Created From | Select a date range from which the watch list member was created. By default, this field selects a date 60 days ago. |
| Created To | Select a date range during which the watch list member was created. By default, this field selects today's date. |
| Business Domain | Select the business domain associated with the watch list member you wish to search for. You must be mapped to the business domain associated with the member to be able to view it on the UI. |
| Jurisdiction | Select the jurisdiction associated with the watch list member you wish to search for. You must be mapped to the jurisdiction associated with the member to be able to view it on the UI. |

3. Click **Search**. The relevant watch list members list is displayed.

3.6.6.1 Viewing Watch List Members and Review Pending Tabs

This section describes the search result of watch list members. Most of the column headings in the Watch List Members section are sortable. You will be able to sort each column by right-clicking on the column header and choosing ascending or descending options.

The column heading that is selected for the sorting option displays with an arrow beside it. The direction of the arrow indicates the sort order (ascending or descending). When you click a different column heading, the arrow displays beside that column with the direction indicating the sort direction. Oracle Financial Services Behavior Detection refreshes the list and re-sorts the watch lists display by that field, retaining the current list entries based upon the criteria you selected in the Watch List Search. If you click the same column heading again, Oracle Financial Services Behavior Detection sorts the column in the opposite direction. The following table describes the columns in the Watch List Members section.

3.6.6.1.1 Watch List Members Tab Columns

The following table describes the columns in the Watch List Members section.

Table 11: Watch List Members Columns

| Column Name | Description |
|-----------------|---|
| Status | Displays the current status of the watch list member and an icon that represents the status. The following statuses may display: <ul style="list-style-type: none"> Active Deactivated |
| Member ID | Displays the identifier or name of the watch list member. This identifier is a hyperlink that opens the Member Details popup. You will be able to see only the first 50 characters of the Member ID. You can increase the width of the field via the Field Chooser. |
| Member ID Type | Displays the type of entity represented by the watch list member. |
| Description | Provides a description of the watch list member. |
| Business Domain | Displays the business domains associated with the watch list member. |
| Jurisdiction | Displays the jurisdiction associated with the watch list member. |
| Created By | Displays the name of the watch list creator who created this member. |
| Create Date | Displays the date this watch list member was created. |
| List Code | Lists the unique identifier of the watch list this member is associated with. |
| List Name | Displays the name of the watch list this member is associated with. |
| List Type | Displays the type of watch list this member is associated with. |
| List Status | Displays the current status of the watch list this member is associated with. |

Review Pending Changes

4 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](#)
- [Accessing Preferences Page](#)
- [Managing Preferences](#)

NOTE

Some components of the Preference page are specific to either Enterprise Case Management or Behavior Detection. 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.

4.1 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 **Expand** > - to expand the section and **Collapse** < to collapse the section.

4.2 Key Features

- Set preferences for the Alert Search and List page
- Set preferences for the Simple and Advanced Search sections.
- Set preferences for AML, and Fraud search options
- Set preference for the Replay Tab
- Set preferences for the Audit Display Tab

4.3 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.

4.4 Managing Preferences

This section explains you how to manage preferences in Behavior Detection 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 Fraud Specific Search Options](#)
- [Setting the Options for Replay Page](#)
- [Setting Options for Audit Display](#)
- [Saving Preferences](#)

4.4.1 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:

1. Navigate to the Preferences page and go to the Set Alert Search and List Options section.
2. Select the preferred options from the respective drop-down lists.

Table 1: 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"> • Anti-Money Laundering • Fraud • Standard <p>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"> • Views • Simple Search • Advanced Search |
| 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> |

4.4.2 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:

1. Navigate to the Preferences page and go to the Set Option for Alert Search.
2. Select common filters for the solution set. For more information, see [Table 1](#) Setting the Alert Display Configuration section.

Table 2: Alert Search Components

| Fields | Description | Standard | AML | 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 |
| 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. If you filter by Organization, you cannot filter by Owner. | 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. If you filter by Owner, you cannot filter by Organization. | 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. If you filter by Class, you cannot filter by Scenario. | 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 |
| 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 |

Table 2: Alert Search Components (Continued)

| Fields | Description | Standard | AML | Fraud |
|----------------|---|----------|-----|-------|
| Focus | <p>Select the focus from the drop-down list.</p> <p>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.</p> <p>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.</p> <p>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>.</p> | X | X | X |
| Score | <p>Select alerts with scores greater than equal to, equal to, or less than equal to, to the score you enter in the box.</p> <p>This filters the alert list by the score the alert received when based against the criteria selected by your firm.</p> | X | X | X |
| Age | <p>Select alerts with age greater than equal to, equal to, or less than equal to, to the age you enter in the box.</p> <p>This filters the alert list by the number of calendar or business days since the creation of an Active alert.</p> | X | X | X |
| Jurisdiction | <p>Select the jurisdiction from the drop-down list.</p> <p>This filters the alert list by jurisdiction to which you are assigned.</p> | X | X | X |
| Domain | <p>Select the business domain from the drop-down list.</p> <p>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.</p> | X | X | X |
| Alerts Due | <p>Select the alert due from the drop-down list.</p> <p>This filters the alert list by the date by which an action should be taken on the alert.</p> | X | X | X |
| Closing Action | <p>Select the closing action from the drop-down list.</p> <p>This filters the alert list by one or more selected closing actions that are taken on an alert.</p> | X | X | X |
| Last Action | <p>Select the last action from the drop-down list.</p> <p>This filters the alert list by the selected action or actions representing the last action recorded for a alert.</p> | X | X | X |
| Action | <p>Select the action from the drop-down list.</p> <p>This filters the alert list by one or more actions that are taken on an alert.</p> | X | X | X |

Table 2: Alert Search Components (Continued)

| Fields | Description | Standard | AML | Fraud |
|--------------------------|---|----------|-----|-------|
| 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 |
| 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 |
| 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 |
| Linked Cases | Select alerts with prior value greater than equal to, equal to, or less than equal to, to the value you enter in the box. This filters the alert list by the cases that are linked to the alert. | X | X | X |
| 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 |
| 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 |
| 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 |
| Entity Name | Enter the entity name associated with alerts you want to view. | X | X | X |

4.4.2.1 Setting AML Specific Search Options

The Behavior Detection 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.
- 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 3: 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. |

4.4.2.2 Setting Fraud Specific Search Options

The Behavior Detection 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.
- 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 4: 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. |

4.4.3 Setting the 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 Behavior Detection system enables Analyst II, Analyst III, and Supervisor roles to configure the Security Group filters in the Replay page.

To set options for Replay page, follow these steps:

1. Navigate to the Preferences page. Go to the Set Options for Replay page section.
2. Select either **Disable** or **Enable** in the Set Option for Security Group.

NOTE

By default, the Behavior Detection UI selects the Security Group option as Enable if you do not save your settings.

4.4.4 Setting Options for Audit Display

This section explains how to set preferences on the audit display.

To set options for audit display, follow these steps:

1. Navigate to the Preferences page. Go to the Set Options for Audit Display section.
2. To view a history of when the current alert is viewed by the owner or other users regardless of any action being taken, select the **Display View Only Action** checkbox.
3. To view a history of when the status of the current alert is changed, select the **Display Status Changing Actions** checkbox.
4. To view all the alerts which have attachments, select the **Attachments Included** checkbox.

4.4.5 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 you access the system, the preferences are displayed.

A Alert Components and Tables

This appendix provides additional information on various tables of alert management and covers following sections:

- [Alert Context Information](#)
- [Search Components](#)
- [Alert List Display Configuration](#)

A.1 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 1: Alert Context Information by Scenario Class

| Column | Description | AML | Fraud |
|-----------------------------|--|-----|-------|
| Alert ID | Unique ID of the alert. | 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 |
| Score | Score the alert received. | X | X |
| Scenario | Scenario short name of the scenario that generated the alert. | X | X |
| Owner | Name of an individual or group of users to whom the alert is assigned. | X | X |
| Organization | Name of the organization for which an alert is assigned. | X | X |
| Business Domain | Business domain(s) associated with the alert focus. | X | X |
| Same Scenario Prior | Number of previous matches associated with the focus of the current alert and of the same scenario. | 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 |
| Linked Cases | The count of cases linked to the alert. | X | X |
| Status | Current state of the alert relative to its analysis and closure. | X | X |
| Alerts Due [Date and Time] | Date and time by which an action should be taken on the alert. | X | X |
| Highlights | Pertinent information related to the alert. | 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 |
| 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 |

Table 1: Alert Context Information by Scenario Class (Continued)

| Column | Description | AML | Fraud |
|------------------------------|--|-----|-------|
| 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 |
| Security ID | Identification number of the security involved in the alert. | | |
| Security | Name of the security involved in the alert. | | |
| Trader ID | Identification number of the trader involved in the alert. | | |
| Trader | Name of the trader involved in the alert. | | |
| Investment Advisor Firm ID | Identification of the firm associated with the Investment Advisor. | | |
| Service Team ID | Identifier of the primary service team of which this employee is a member. | | |
| Registered Representative ID | Identification number of the employee or contractor who is the Registered Representative. | | |
| Representative | Employee or contractor who is the Registered Representative. | | |
| Branch ID | Identification number of the organization where this account is domiciled. | | |
| Branch | Name of the organization where this account is domiciled. | | |
| Supervisory Organization ID | Identification number of the organization where the Registered Representative is employed. | | |
| Supervisory Organization | Name of the organization where the Registered Representative is employed. | | |
| 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. | | |

A.2 Search Components

This section covers the following topics:

- [Views Search](#)

- [Alert List Matrix](#)
- [Additional Information](#)

A.2.1 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.

Table 2 list the View Filter and Sort Criteria for the default View Names.

Table 2: 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

A.2.2 Alert Information

Table 3 provides a list of the alert search components that display in the alert Simple and Advanced Search bar.

Table 3: Alert Search Components

| Column | Description | Simple Search | Advanced Search | |
|----------------|---|---------------|-----------------|-------|
| | | | AML | Fraud |
| Created From | Filters the alert list by the date the alert was created. | X | X | X |
| Created To | Filters the alert list by the date the alert was created. | X | X | X |
| Business Date | Filters the alert list with a processing date between start date and end date. | 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 |
| 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 |
| 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 |
| 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 |
| Scenario | Filters the alert list by the scenario, which is name of the behavior or activity that generated the alert. | 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 |
| Score | Filters the alert list by the score the alert received when based against your firm selected. Oracle Financial Services Behavior Detection retrieves alerts and cases greater than or equal to the score you enter in this text box. | X | X | X |

Table 3: Alert Search Components (Continued)

| Column | Description | Simple Search | Advanced Search | |
|-----------------|--|---------------|-----------------|-------|
| | | | AML | Fraud |
| Closing Action | Filters the alert list by one or more selected closing actions that are taken on an alert. | 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| Action | Filters the alert list by one or more actions that are taken on an alert. | | X | X |
| Last Action | Filters the alert list by one or more selected last actions that are taken on an alert. | | 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 |
| 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 |

Table 3: Alert Search Components (Continued)

| Column | Description | Simple Search | Advanced Search | |
|------------------------------|---|---------------|-----------------|-------|
| | | | AML | Fraud |
| 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 |
| 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 |
| Limit to Focus | Filters the alert list to where the specified entity is the focus. | | X | X |
| Entity Type | Filters the alert list by the type of business entity you select in the drop-down list box. Select the focus from the Entity Type drop-down list and type either Entity Name or Entity ID to search for alerts. | | X | X |
| 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 |
| Entity Name | The entity name associated with alerts you want to view. | | 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. | | | |
| Security | Filters the alert list by the name of security involved in the alert. | | | |
| Trader ID | Filters the alert list by the identification number of the trader involved in the alert. | | | |
| Trader | Filters the alert list by the name of the trader involved in the alert. | | | |
| Investment Advisor Firm ID | Filters the alert list by the identification of the firm associated with the Investment Advisor. | | | |
| Investment Advisor Firm | Filters the alert list by the name of the firm associated with the Investment Advisor. | | | |
| Service Team ID | Filters the alert list by the identifier of the primary service team of which this employee is a member. | | | |
| Registered Representative ID | Filters the alert list by identification number of the employee or contractor who is the Registered Representative. | | | |

Table 3: Alert Search Components (Continued)

| Column | Description | Simple Search | Advanced Search | |
|-----------------------------|--|---------------|-----------------|-------|
| | | | AML | Fraud |
| Representative | Filters the alert list by name of the employee or contractor who is the Registered Representative. | | | |
| Branch ID | Filters the alert list by the identification number of the organization where this account is domiciled. | | | |
| Branch | Filters the alert list by the name of the organization where this account is domiciled. | | | |
| Supervisory Organization ID | Filters the alert list by unique ID of the organization where the Registered Representative is employed. | | | |
| Supervisory Organization | Filters the alert list by the name of the organization where the Registered Representative is employed. | | | |
| 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 |

A.2.3 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.

A.2.3.1 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).

Before you take action on the selected alerts, Oracle Financial Services Behavior Detection 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 4 provides a list of the columns that display in the Alert List matrix.

Table 4: Alert List Components by Display Configuration by Solution Sets

| Column and Field | Anti-Money Laundering | Fraud | Standard |
|---|-----------------------|-------|----------|
| Alert ID | X* | X | X |
| SC [ore] | X | X | X |
| Focus Type | X | X | X |
| Focus Name | X | X | X |
| Scenario | X | X | X |
| Highlights | | | X |
| Created [Date] | X | X | X |
| Status | X | X | X |
| Alerts Due [Date and Time] | X | X | X |
| Regulatory Reporting Status | | | X |
| Regulatory Reporting Type | | | X |
| Owner | X | X | X |
| Class] Prior | | | X |
| SCN [Scenario] Prior | | | X |
| Closing Action | | | X |
| [Business] Domain | | | X |
| [Involved] Security | | | |
| [Involved] Trader | | | |
| [Involved] Service Team ID | | | |
| [Involved] Registered Representative ID | | | |
| Total/Net Loss Amount | | X | |
| Primary Cost Center | | X | |
| Linked Cases | X | X | X |
| Commodity Instrument ID | | | |
| Threshold Set Name | X | X | X |

A.2.4 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 5: 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)). This feature is available only if Oracle Financial Services Regulatory Reporting (OFSRR) application is | X | |
| Regulatory Report Status | The current reporting status of a case that is recommended for Regulatory Reporting. This feature is available only if Oracle Financial Services Regulatory Reporting (OFSRR) application is installed. | X | |

A.3 Alert List Display Configuration

Table 4 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 6: Alert List, General Overview, and Metrics Display Configuration by Solution Sets

| Column and Field | Anti-Money Laundering | Fraud | Standard |
|------------------|-----------------------|-------|----------|
| Alert ID | L* | L | X |
| SC [ore] | L | L | X |

Table 6: Alert List, General Overview, and Metrics Display Configuration by Solution Sets

| Column and Field | Anti-Money Laundering | Fraud | Standard |
|---|-----------------------|-------|----------|
| Focus [Type and Name] | L | L | X |
| Scenario | L | L | X |
| Highlights | O** | O | X |
| Created [Date] | L | L | X |
| Status | L | L | X |
| Alerts Due [Date and Time] | L | L | X |
| Organization | O | O | |
| Regulatory Reporting Status | O | O | X |
| Regulatory Reporting Type | O | O | X |
| Owner | L | L | X |
| CL [Class] Prior | O | O | X |
| SCN [Scenario] Prior | O | O | X |
| Closing Action | O | O | X |
| [Business] Domain | O | O | X |
| [Involved] Security | | | |
| [Involved] Trader | | | |
| [Involved] Service Team ID | | | |
| [Involved] Registered Representative ID | | | |
| [Involved] Branch | | | |
| [Involved] Supervisory Organization | | | |
| Total/Net Loss Amount | | L | |
| Primary Cost Center | | L | |
| Linked Cases | L | L | X |
| Alerts for Prior Class Count | M# | M | X |
| Alerts for Prior Scenario Count | M | M | X |
| Correlation Membership Count | M | M | X |
| Commodity Instrument ID | | | X |

where, L* are fields in the Alert List section; O** are fields in the General Overview section; M# are fields in the Metrics section.

B Business Tabs

Oracle Financial Services Alert Management consists of Business tabs that display in the Monitoring workflow. Within the Monitoring workflow, these tabs are displayed according to the focus type and scenario class of the alert you select.

B.1 Alert Business Tabs

Table 1 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 1: Business Tab pages by Scenario Class

| Focus Type | Possible Business Tabs |
|---|--|
| Scenario Class: Institutional Money Laundering | |
| Customer (CU) | Account, Customer, and Investment Advisor |
| External Entity (EN) | External Entity |
| Scenario Class: Money Laundering | |
| Account (AC) | Account, Customer, Employee, Household, and Investment Advisor |
| Correspondent Bank (CB) | Correspondent Bank |
| Customer (CU) | Account, Customer, Household, and Investment Advisor |
| External Entity (EN) | External Entity |
| Household (HH) | Account, Customer, Household, and Investment Advisor |
| Scenario Class: Fraud | |
| Account (AC) | Account, Customer, Household, Investment Advisor, Employee, and Financials |
| Customer (CU) | Account, Customer, Household, Investment Advisor, and Financials |
| Employee (EE) | Account, Employee, Financials, and Household |
| External Entity (EN) | External Entity |
| Household (HH) | Account, Customer, Household, and Investment Advisor |
| Scenario Class: Mutual Funds | |
| Account (AC) | Account, Customer, Household, Investment Advisor, Registered Representative, and Trade |
| Household (HH) | Account, Customer, Household, Investment Advisor, Registered Representative, and Trade |
| Investment Advisor (IA) | Account, Investment Advisor, and Trade |
| Registered Representative (RR) | Account, Registered Representative and Trade |

C Using Behavior Detection UI

The information provided in the following sections helps you achieve optimal use of the Oracle Financial Services Behavior Detection UI:

- [Common Screen Elements](#)
- [Using the Browser](#)
- [Navigating in Oracle Financial Services Behavior Detection](#)
- [Message Pages](#)

C.1 Common Screen Elements

The following section describes the common screen elements in the Oracle Financial Services Behavior Detection.

Common screen elements are those elements that consistently perform the same type of function in the same way when they display in the UI. Some serve as labels and never change (Matrix header); some enable you to get help or complete a task (buttons); some offer an explanation for a specific item (tool tips); and some operate as variables that allow you to type entries (text boxes) and make selections (drop-down lists).

C.1.1 Masthead

The masthead displays at the top of the page and contains the following components:

- Navigation Bar as Menus
- Session Information with session user name, day, and date.
- Help Button

C.1.2 Buttons

Buttons on the Behavior Detection UI enable you to perform tasks such as executing and canceling actions or commands. Click a button to complete the desired task.

C.1.2.1 Task Buttons

Task buttons display throughout Behavior Detection and include the following:

- The **Search** and **Advanced Search** buttons display on the Search & List page of the Monitoring workflow to filter data based on the criteria you set with basic filters and advanced additional filters respectively.
- The **Save** button records actions and navigates you to the appropriate page and displays the updated alert information accordingly.
- The **Save & Attach** button records actions and navigates you to a page providing the option to attach a document with the action. Once you complete the attachment you are navigated to the appropriate page and the alert information is updated accordingly.
- The **Clear** button displays on those actionable sections of the UI which do not display any pre-populated data. It clears the data entered by you when clicked.
- The **Reset** button displays on those actionable sections of the UI which display some pre-populated data. It discards the data entered by you and resets the contents to their original state.

- The **Cancel** button displays on all the actionable sections of the UI and cancels the action you intend to take and closes the action pop-up window.
- The **Send** button displays in the email pop-up window and sends the email to the addressed parties.
- The **Create** button in the Create Alert workflow displays fields for you to enter data for the new alert being created.
- The **Related to Focus** button displays in some specific business tabs where this information is available. It refreshes the tab details to replace the Related to Alert information with what is often a broader set of information that is applicable to the focus of the alert and not limited to just the activity of the alert.
- The **Related to Alert** button in specific business tabs does not display by default. The **Related to Alert** button replaces the **Related to Focus** button once the **Related to Focus** button is clicked. Selecting **Related to Alert** refreshes the tab information to display information that is applicable to the alert activity only.
- The **Add** button displays in the some Business tabs, Financials tab and in the Evidence tab. It provides you with a pop-up window to add a new piece of information.
- The **Edit** button displays in the some Business tabs, Financials tab, Narrative, and Evidence tabs. It provides you with a pop-up window to edit the existing piece of information you have chosen for edit.
- The **Remove** button displays in the some Business tabs, Financials tab, and in the Attachment List matrix present in the attachment section of the Evidence tab. It also display in the Financials tab. It helps you delete information that you think is not relevant.
- The **Update** button displays in the Suppression Rule List. It provides you with a UI to modify a suppression rule with appropriate comments.
- The **End** button displays in the Suppression Rule List and provides you with a UI to end a suppression rule.
- The **History** button displays in the Financials tab, Manage Suppression Rules workflow. It provides you with a detailed account of previous activities on the selected record.
- The **Go** button displays in all the Case Search bars Alert/Manage Suppression Rule and performs the search function. It also displays in the various action pop-up window. In the action pop-up window, the **Go** button helps display the appropriate fields as per the actions you have selected.

C.1.2.2 Action Buttons

The Action buttons display in the Search & List page and in the Details page. Each of these buttons provides you with an action pop-up window for taking actions in the category these buttons are representative of. These include buttons for each action category:

- Reassign
- Actions
- Disposition
- Review
- Regulatory Reporting
- Assignment
- Escalate
- Resolution

- Research & Review
- Monitor
- email
- Export
- Evidence
- Excel
- Reopen
- Due Date
- Print Details
- Print Comments

C.1.2.3 Help Button

A **Help** button, in the form of a question mark, displays to the extreme right of the bread crumbs. Click **Help** to get the following:

- More detailed information about the page
- Explanations of the screen elements
- How to perform instructions on a task that you want to perform

C.1.2.4 Calendar Button

A **Calendar** button displays when you have the option of selecting a date. For example, you can specify a date range to search for closed alerts. If you click **Calendar** icon, a calendar of the current month displays and highlights the current date.

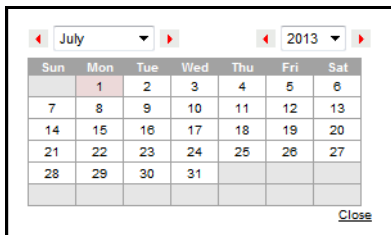


Figure 1: Calendar Button

To use the Calendar window to select dates, follow these steps:

1. Select a date. The application will automatically enter the selected date in the date field.
2. Click the arrows at the top of the Calendar window to view other months or years.
3. Click the **Close** link to close the calendar without selecting a date.

C.1.3 Expand/Collapse

You can view the complete information in a section, matrix, and field by using various expand or collapse options.

C.1.3.1 Column Expand All

When values are displayed in a matrix and there are columns which have lengthier values, then you can use the drag option to expand each column. This displays the entire value.

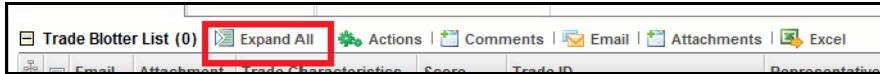


Figure 2: Column Expand All Button

C.1.3.2 Column Collapse All

When values are displayed in a matrix and there are columns, which have lengthier values, then you can use the **Column Collapse All** button to collapse all the values that are already expanded for display, together at once.

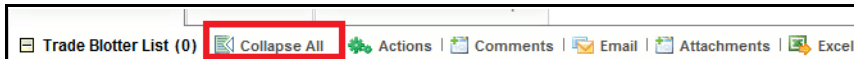


Figure 3: Column Collapse All Button

C.1.3.3 Section Expand Button

If you want to expand a section on a page, you can click the **(+)** button displayed at the top left corner of the section. This expands the section and all the fields in the section are visible.

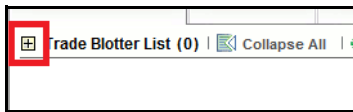


Figure 4: Section Expand Button

C.1.3.4 Section Collapse Button

If you want to collapse a section, which is already expanded, you can click the **(-)** button displayed at the top left corner of the section. This collapses the section and all the fields in the section are hidden.

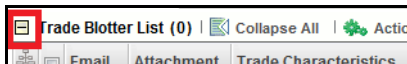


Figure 5: Section Collapse Button

C.1.4 Field Types

The following sections describe field types.

C.1.4.1 Text Area

A multi-line rectangular box in which you can type text, such as alertcase comments. If the box already contains text, you can select the default text or delete it and type new text. You can type as many characters in this box as desired.

C.1.4.2 Text Box

A single-line rectangular box in which you can type text. If the box already contains text, you can select the default text or delete it and type new text. Text boxes can limit the number of characters that you can enter. If so, the text box will show the maximum number of characters you can enter.

C.1.4.3 Wildcard Text Box

Oracle Financial Services Behavior Detection permits the use of wildcards in specific text boxes. If you do not know all of the information to type into the text box field, you can type a wildcard character for the missing part of the information. The application recognizes the percent sign (%) and underscore (_)

as wildcard characters. You can use the wildcard character at the beginning, end, and anywhere within a string.

The more specific you are when using the wildcard character, the fewer extraneous matches are returned. For example, if you specify a last name of `Smit%`, the application can return 100 matches, but if you specify a last name of `Smit%`, it can return only 17 matches.

C.1.4.4 Context-Sensitive Text Box

Behavior Detection permits the use of context-sensitive input in specific text boxes. If you want to perform a search on multiple values, you can enter a string of comma-separated values in the Alert/Suppression Rule ID search field.

C.1.4.5 Drop-down List

A list of items from which you can select one item. Selecting the blank (empty) option applies no filter to your selection.

C.1.4.6 Selection Box

A list from which you can choose multiple items by selecting the check box against each item. Checking the value *Select All* represents the selection of all the values available in the selection box. Un-checking the value *Select All* represents the de-selection of all the values in the selection box.

C.1.4.7 Check Box

A square box that displays beside an item or option. Select the check box once to place a check mark in the box. Select the check box again to clear it.

C.1.5 ToolTips

A Tooltip displays when you position the mouse cursor over an abbreviated field, usually indicated by an ellipsis, or a column label in the UI. A Tooltip displays for approximately three seconds and provides the definition or other pertinent information for the abbreviated field or column label.

C.2 Using the Browser

The browser cache does not completely refresh the data. Therefore, using keys from keyboards, like Ctrl+Left arrow or Backspace keys for backward navigation, and Ctrl+ Right arrow keys for forward navigations displays data that can be outdated. Using navigation, pages are refreshed so the information is always up-to-date.

C.3 Navigating in Oracle Financial Services Behavior Detection

The following sections describe the navigation features that you can use to navigate within Behavior Detection

Navigation features enable you to move easily between pages in the UI to view, analyze, or research alerts and focuses while working in Behavior Detection.

C.3.1 Navigation List

The Navigation list displays in the upper left corner of the page. The Navigation list displays the applications and features which are associated with your user role.

C.3.2 Links

Links display as hypertext (underlined text) on the page that, when clicked, takes you to other pages within the Oracle Financial Services Behavior Detection UI.

C.3.3 Search Bars

Some Behavior Detection pages have a *Search bar* that allows you to specify values with which to filter and sort your data. Search bars for a specific page are described in the chapter where that page's use is explained.

C.3.4 Page Context Controls

Page context controls (also called bread crumbs) show your location in the UI. They allow you to navigate back to the previous page to a particular workflow. The current workflow displays the current entry in the page context controls.

C.3.5 Business Tabs

In Behavior Detection, business data tabs display in the Alerts workflow after you have accessed an alert.

The business data tabs that display are dependent on the focus and the scenario class of the alert you are viewing and your role in Behavior Detection.

Business data tab pages display detailed information about a business entity. Depending on the type of business entity being displayed (for example, Account, Customer), the content of the tab is different and specific to that type of entity.

C.3.6 Paging

Paging refers to the mechanism on the page that enables you to move through multiple pages of information (alerts, transactions, and so forth).

You can move forward and backward through the pages one at a time by clicking the back arrow to the left of the page text box (unless you are on page #1) or the forward arrow to the right of the total number of pages (unless you are on the last page).

You can directly navigate to a page by entering the page number you wish to navigate to in the Jump to page box and clicking the **Enter** key.

Some pages within the UI display only an initial, limited set of information on first navigating to that page. This information is often displayed in a tabular matrix at the top of the page. Additional information relevant to the page along with an LHS menu can be displayed by clicking one of the initially displayed records.

C.4 Message Pages

Behavior Detection describes the various types of error and status message pages that you can see in the application.

D Security within OFSAAI

Oracle Financial Services Analytical Applications Infrastructure (OFSAAI) uses six layers of security to control data access as defined in Table 1. 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 1: 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. |

E Calculating Risk

Oracle Financial Services Behavior Detection uses risk calculations as part of managing sensitivity when detecting behaviors of interest in Money Laundering and Fraud scenarios. Risk Information can be provided through watch list or an attribute of the record provided to the ingestion manager for given customers and accounts.

Based on several risk inputs, Oracle Financial Services Behavior Detection calculates effective risks for business entities and calculates both Party Risk and Activity Risk on Transactions and Settlement Instructions.

Figure 1 displays the basic flow of the calculation.

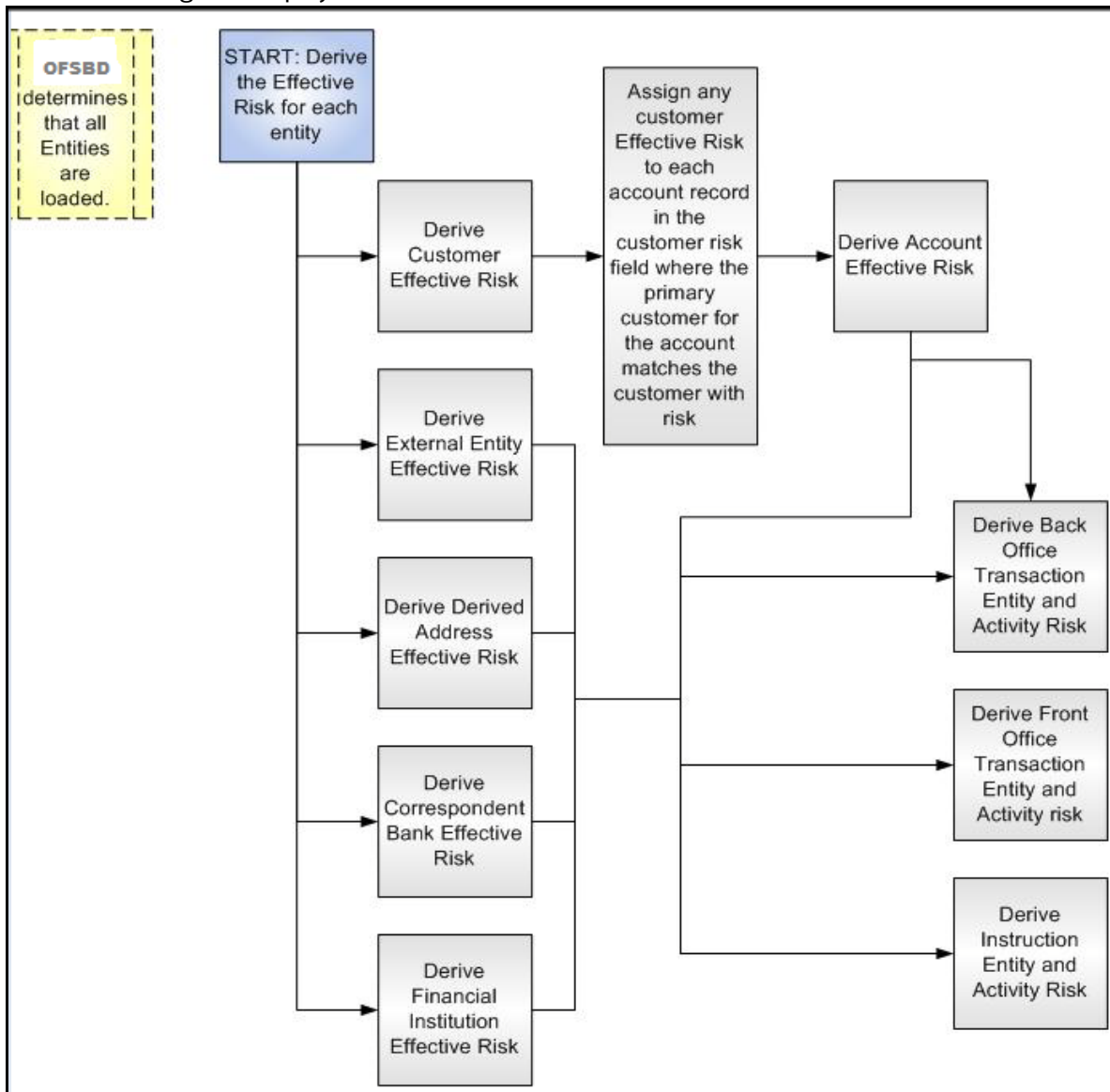


Figure 1: Risk Derivation-Overview

In addition to risk, Oracle Financial Services Behavior Detection supports the concepts of Exempt Entities and Trusted Entities. These concepts are discussed in more detail in section *Watch Lists*. In brief, Exempt Entities are those that should not be alerted in Anti-Money Laundering scenarios. Trusted

entities are those that meet specific criteria which demonstrates that they are more trustworthy than the general population.

Risk levels use a ten-point scale, with one representing moderate risk and ten representing highest risk. Entities that have no known risk receive a risk score of zero.

E.1 Determining Entity Risk

Oracle Financial Services Behavior Detection clients can provide risk factors for business entities through the Oracle Financial Services Data Interface Specification (DIS). The risk can be assigned to the same business entity in the several ways. The Ingestion Manager resolves across these various risks to create an Entity Effective Risk.

Figure 2 reflects the basic flow for deriving Entity Effective Risk.

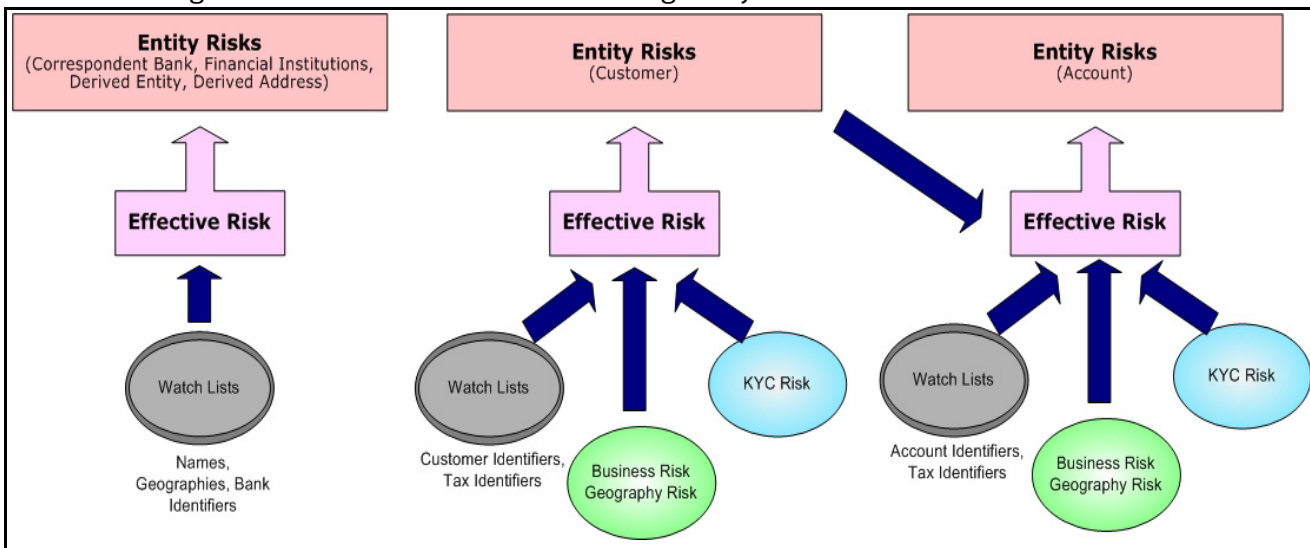


Figure 2. Entity's Effective Risk

Oracle Financial Services Behavior Detection derives risk on the following business entities:

- Customers
- Accounts
- Financial Institutions
- Correspondent Banks
- Derived Addresses
- Derived Entities (Names)
- Derived Entities (Identifiers)

The client can provide risk information directly through the Account and Customer input files as specified in the DIS. Accounts and Customers can also receive Know Your Customer (KYC) risk information through the Account Supplemental Attributes and Customer Supplemental Attributes DIS files. All of the business entity types can receive risk information through watch lists.

When determining an entity's effective risk, the approach to resolving across multiple sources of risk varies based on the entity type. The general rules to follow are:

- Watch List risk has higher priority than other risk factors.
- Exemption and Trust take priority over risk.

- More specific risk factors are preferred over less specific risk factors (for example, risk associated with an Identifier is more specific than risk associated with a Name).

Derivations of Customer, Account, and Correspondent Bank Effective Risk are the most complex. The following sections outline the rules for these derivations.

E.1.1 Deriving Customer Entity Risk

Customer records can provide risk through the following distinct mechanisms:

- Business Risk or Geography Risk provided in the Customer DIS file
- KYC Risk provided in the Customer Supplemental Attributes DIS file
- Watch List entries matching the Customer ID or Customer's Tax ID

If the Customer has any Watch List risk information, then the Customer's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Customer, then the Effective Risk is derived as the highest of Business Risk, Geography Risk, and KYC Risk. KYC Risk can be provided as either Trust or Exclusion. If that is the case, the KYC trust is selected over positive risk factors in Business Risk or Geography Risk.

E.1.2 Deriving Account Entity Risk

Account records can provide risk through the following distinct mechanisms:

- Business Risk or Geography Risk provided in the Account DIS file
- KYC Risk provided in the Account Supplemental Attributes DIS file
- Watch List entries matching the Account ID or Account's Tax ID

Accounts can also inherit risk from the Primary Customer identified on the Account. This risk is referred to as Account Customer Risk. Accounts inherit the Effective Risk from the Primary Customer as it is calculated using the rules described in Deriving Customer Entity Risk with the following exceptions:

- If the Customer's Effective Risk was driven by KYC risk, then the Account processing re-calculates the Customer's effective risk, ignoring KYC risk on the Customer. The reason for this is that the Account's risk factors are part of the Oracle Financial Services KYC product's risk derivations, so propagating that risk back to the Account is not productive. If the Customer's Effective Risk was driven by KYC, then the Account uses the highest of the Customer's Geography and Business risks as the Account Customer Risk.
- There is a configurable parameter in the Ingestion Manager to determine whether or not Trust and Exclusion should be inherited from the Customer record. If this is configured to NOT inherit this effective risk and the Customer's Effective Risk indicates Trust or Exclusion, then the Customer's risk is not considered when determining the Account Effective Risk.

If the Account has any Watch List risk information, then the Account's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Account, then the Effective Risk is derived as the highest of Business Risk, Geography Risk, KYC Risk, and Account Customer Risk.

E.1.3 Deriving Correspondent Bank Entity Risk

Correspondent Bank records can derive risk information through the following distinct mechanisms:

- Watch List entries matching the Correspondent Bank ID
- Watch List entries matching the Correspondent Bank Name

- Watch List entries matching the Correspondent Bank Address

If the Correspondent Bank has any Watch List risk information, then the Correspondent Bank's Effective Risk is derived directly from the Watch List risk factors. If there is no Watch List risk information on the Correspondent Bank identifier, then the Effective Risk is derived based on matching Watch List risk information pertaining to the Correspondent Bank name. If there is no Watch List risk information on the Correspondent Bank name, then the Effective Risk is derived based on the matching of the Correspondent Bank's address information to Watch List entries.

E.1.3.1 Watch Lists

A Watch List is a list of entities that have known risk characteristics. Watch Lists can represent public sources or can be created and managed internally by the institution. Common public sources for watch lists include Office of Foreign Asset Control (OFAC) and Financial Action Task Force (FATF). The types of entities provided on Watch Lists include:

- Identifiers (for example, SSN, Tax ID, and Passport ID)
- Organizations (for example, business name, SWIFT code, and ABA number)
- Accounts (for example, internal or external accounts)
- Persons (for example, personal name)
- Geography (for example, countries, state, city, postal code, and address)
- Combined Names and Geography

Refer to the *Data Interface Specification* for more information on Watch Lists and Watch List Entries.

Oracle Financial Services Behavior Detection categorizes Watch Lists into the following types:

- **Exempted Watch List:** Entities on Exempted Watch Lists are highly trusted clients on whom no Money Laundering alerts will be generated.
- **Trusted Watch Lists:** Entities on Trusted Watch Lists are known to be highly trustworthy. Certain scenarios can be configured to exclude trusted entities from monitoring.
- **Risk Watch List:** These are the entities that carry a risk value indicating that they should be monitored more closely than the general population. Money Laundering scenarios allow for separate threshold values to be set when monitoring entities with a certain risk level. Risk lists are risk weighted using values ranging from one (lowest risk) to ten (highest risk).

NOTE

There is no risk list with a risk level of zero. Risk level zero is reserved to indicate that there are no known risk factors to consider. It is also the default risk level for all entities in Oracle Financial Services Behavior Detection.

The matching criteria of Watch List Entry are as follows:

- All ID entries on a Watch List require an exact match to an entity .
- All Name entries on a Watch List require an exact or a fuzzy match to an entity .
- Addresses can be matched to watch list entries at multiple levels (for example, the same address can match one watch list entry for a Street Address and can match a separate entry for a Country)

For each Watch List match to an entity, a List Membership Record is created, which includes the following:

- ID of Watch List matched

- Date when the entity was added to the Watch List
- Date when the entity was removed from the Watch List
- Watch List entry that was matched
- Type of Watch List Entry that was matched

Fuzzy name matching is a technique to account for normal variations in names and still successfully match the names against watch lists. For more information on configuring Fuzzy Name Matching within Oracle Financial Services Behavior Detection, refer to the *Administration Guide*.

E.1.3.2 Determining Watch List Risk

Oracle Financial Services Behavior Detection defines each reference entity with an adjudicated Watch List Risk. An entity's Watch List Risk is determined through a hierarchy of rules as follows:

- If an entity is a member of a Watch List of type Exempt, then the Watch List Risk value is -2. This value is not displayed; it is used for internal processing.
- If an entity is a member of a Watch List of type Trusted, then the Watch List Risk value is -1. This value is not displayed; it is used for internal processing.
- If an entity is matched to multiple entries on one or more Watch Lists, the match that is the *most specific* is used to drive risk. The order of preference is:
 - a. ID match
 - b. Exact Name match
 - c. Fuzzy Name match
 - d. Street Address match
 - e. Postal Code match
 - f. City match
 - g. State/Province match
 - h. Country match

Not all entity types can match multiple types of watch list entries. For example:

- Accounts and Customers only match identifiers.
- Correspondent Banks can match either IDs, Names, or Addresses.
- Addresses can match at different granularities, ranging from Country to the specific street address.
- If multiple risk lists are matched with the same specificity, then the final Watch List Risk is the highest of the risks of the entities matched at the same level.

NOTE

All matches are retained and stored in List Membership Records associated with the entity.

E.1.3.3 Determining Risk on Transactional Data

After Effective Risk is derived for Entities, this risk is reflected on instructions and transactions. The risk is generally calculated for each party on the transaction and stored as a Party Entity Risk. The Entity Risks of each party is then used to calculate an Activity Risk for each party. Activity Risk is an assessment of the risk level of the activity in which that party has engaged. As such, that party's own Entity Risk is not considered when calculating the Activity Risk for the party.

The derivations for Party Entity Risk vary by the transaction type.

E.1.4 Determining Front Office Transaction Party Entity Risk

Front Office transactions contain the following distinct sources of risk for any one party:

- Party ID
- Party Name
- Party Location

As a general rule, Oracle Financial Services Behavior Detection uses the most specific risk factor possible when setting the Party Entity Risk. As such, risk information about the Party ID is considered more reliable than risk information about the Party Name or the Party Location. The Ingestion Manager can be configured to automatically accept the Party ID Risk only when it is above a certain threshold (this defaults to zero, meaning that non-zero Party ID Risk is always accepted as the Party Entity Risk).

For each Party, a Geography Risk is calculated using Watch List information as described in the section *Watch Lists*.

Party Entity Risk is determined by a hierarchy of rules as follows:

- If the Party ID Effective Risk is Trusted or Exempt, then set Party Entity Risk to the Party ID Effective Risk.
- If the Party ID Effective Risk is $>$ *Party ID Win Threshold*, then set Party Entity Risk to Party ID Effective Risk.
- If the Party Name combined with the Party Location matches a combined Name-Location Watch List record that represents Trust or Exclusion, then set the Party Entity Risk to the combined Name-Location and Trust-Exemption level.
- If the Party Name combined with Party Location matches a combined Name-Location Watch List record that represents Risk, then set the Party Entity Risk to the HIGHER of the Party ID Effective Risk and the combined Name-Location Risk level.
- If the Party Name Effective Risk alone is Trusted or Exempt, then set the Party Entity Risk to the Trust-Exemption level of the Name.
- If the Party Name Effective Risk indicates risk, set the Party Entity Risk to the HIGHER of the Party ID Effective Risk and the Party Name Effective Risk.
- If the Party Geography Risk is Trusted or Exempt, then set the Party Entity Risk to the Trust-Exemption level of the Geography.
- Set the Party Effective Risk to the HIGHER of the Party ID Entity Risk and the Party Geography Risk.

The Party Entity Risk is calculated for every party on each Front Office Transaction. This value displays when showing Front Office Transactions in the UI. This value is then used to calculate Party Activity Risk for each party on the transaction. Refer to section *Determining Activity Risk on Front Office Transactions* for details on the calculation of Party Activity Risk for Front Office Transactions.

E.1.5 Determining Back Office Transaction Party Entity Risk

Back Office Transactions contain only two parties, the Account that is the focus of the activity and the Offset Account involved in the transaction. As these are both Identifiers, setting the Party Entity Risk for Back Office Transactions is propagating the Account Effective Risk values for the related accounts to the transaction.

E.1.5.0.1 Determining Settlement Instruction Party Entity Risk

Based on how Settlement Instructions are used in scenarios, the processing of parties is handled somewhat differently than Front Office Transactions. Although there are multiple parties on a Settlement Instruction, there is only a Party Entity Risk calculated for the Account holding the Instruction. The processing is, therefore, simply to propagate the Account's Effective Risk to the Settlement Instruction Entity Effective Risk.

E.2 Determining Activity Risk

Activity Risk identifies the risk of the Activity as seen from the viewpoint of each Party on a transaction. In general, the Activity Risk is the highest risk of the other parties on the transaction or of the transaction Channel or Product itself. As with calculating Party Entity Risk, the derivation of Party Activity Risk varies by transaction type.

E.2.1 Determining Activity Risk on Front Office Transactions

Front Office Transaction Party Activity Risk calculates risk separately from the point of view of each party on the transaction. The risk is intended to identify how risky the activity is independent of risk factors already associated to the Party through the Party Entity Risk. As such, on Front Office Transactions, the risk is calculated using the Party Entity Risk of the parties on the other side of the transaction. The general approach is to use the highest of the Channel Risk, Product Risk, and Party Entity Risk of the other parties. Channel and Product Risk are provided in the DIS file for Front Office Transactions.

Several party roles effect activity risk. The following sections describe the relationship between varying party roles and activity risk for transactions.

Table 1 displays the party role-activity risk relationship for an electronic funds transaction.

Table 1: Electronic Funds Transfer Transaction

| Party Role | Roles impacting Activity Risk |
|--|--|
| Originator, Secondary Originator, Sending Bank | Intermediary Banks, Receiving Bank, Beneficiary, Secondary Beneficiary |
| Intermediary Banks | All roles except for the party for which the Activity Risk is being calculated |
| Receiving Bank, Beneficiary, Secondary Beneficiary | Intermediary Banks, Sending Bank, Originator, Secondary Originator |

E.2.1.1 Cash Transaction

Table 2 displays the party role-activity risk relationship for the cash transaction.

Table 2: Cash Transaction

| Party Role | Roles impacting Activity Risk |
|-------------|---------------------------------------|
| Originator | Location, Conductor |
| Location | Conductor, Originator, or Beneficiary |
| Conductor | Location, Originator, or Beneficiary |
| Beneficiary | Location, Conductor |

NOTE A Cash Transaction record can have an Originator or a Beneficiary, but not both.

E.2.1.2 Monetary Instrument and Check Transactions

Table 3 displays the party role-activity risk relationship for the monetary instrument and check transactions.

Table 3: Monetary Instrument and Check Transactions

| Party Role | Roles impacting Activity Risk |
|--|---|
| Remitter, Issuing Institution | Depositing Institution, Clearing Institution, Beneficiary, Secondary Beneficiary, Conductor |
| Clearing Institution | Remitter, Issuing Institution, Depositing Institution, Beneficiary, Secondary Beneficiary, Conductor |
| Depositing Institution, Beneficiary, Secondary Beneficiary | Remitter, Issuing Institution Clearing Institution, Conductor |
| Conductor | Remitter, Issuing Institution, Clearing Institution, Depositing Institution, Beneficiary, Secondary Beneficiary |

E.2.2 Determining Activity Risk on Back Office Transactions

Activity Risk on Back Office Transactions is only calculated for the Account that is the focus of the activity. Since the only other risk factors available are the Offset Account's Effective Risk and the Channel and Product Risks provided on the transaction, the Activity Risk is calculated as the highest of these factors.

E.2.2.1 Determining Activity Risk on Settlement Instructions

The Activity Risk calculated for Settlement Instructions is from the point of view of the Account holding the instructions. Calculating Activity Risk on Settlement Instructions follows a similar approach as Front Office Transactions whereby the Entity risk is calculated for each party and then used to calculate Activity Risk; however, on Settlement Instructions, the Entity Risks for each party are not stored. The Entity Risks are calculated as follows:

E.2.2.1.1 Destination Customer Entity Risk

The Destination Customer Entity Risk is calculated using the following hierarchical rules:

1. If the Destination Customer Account Effective Risk is non-zero, then set the Destination Customer Entity Risk to Destination Customer Account Effective Risk.
2. If the Destination Financial Institution Effective Risk is non-zero, then set the Destination Customer Entity Risk to Destination Financial Institution Effective Risk.
3. If the Destination Customer Name Risk \geq Destination Financial Institution Name Risk, then set the Destination Customer Entity Risk to Destination Customer Name Risk.
4. If the Destination Financial Institution Name Risk $>$ Destination Customer Name Risk, then set the Destination Customer Entity Risk to Destination Financial Institution Risk.
5. Set the Destination Customer Entity Risk to zero (0).

E.2.2.1.2 Physical Delivery Party Entity Risk

The Physical Delivery Party Entity Risk is calculated using the following hierarchical rules:

1. If the Physical Delivery Account Effective Risk is non-zero, then set the Physical Delivery Party Entity Risk to Physical Delivery Account Effective Risk.
2. If the Physical Delivery Financial Institution Effective Risk is non-zero, then set the Physical Delivery Party Entity Risk to Physical Delivery Financial Institution Effective Risk.
3. If the Physical Delivery Geography Risk is non-zero, then set the Physical Delivery Party Entity Risk to the Physical Delivery Geography Risk.
4. Set the Physical Delivery Party Entity Risk to zero (0).

The final Activity Risk setting on the Settlement Instruction is the highest level of the following risks:

- Destination Customer Entity Risk
- Physical Delivery Party Entity Risk
- Settlement Country Geography Risk
- Product Risk
- Channel Risk

This final Activity Risk is used in scenarios to determine the risk level of the Settlement Instruction without regard to the risk factors inherent in the Account holding the Instruction.

OFSAA Support Contact Details

Raise a Service Request (SR) in [My Oracle Support \(MOS\)](#) for queries related to OFSAA applications.

Send Us Your Comments

Oracle welcomes your comments and suggestions on the quality and usefulness of this publication. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most about this manual?

If you find any errors or have any other suggestions for improvement, indicate the title and part number of the documentation along with the chapter/section/page number (if available) and contact the Oracle Support.

Before sending us your comments, you might like to ensure that you have the latest version of the document wherein any of your concerns have already been addressed. You can access My Oracle Support site which has all the revised/recently released documents.

