

**Oracle Financial Services**

**Transaction Filtering**

**User Guide**

**Release 8.1.2.8.0**

**August 2024**

**F22529-05**

**ORACLE<sup>®</sup>**  
**Financial Services**

---

## OFS Sanctions Transaction Filtering User Guide

Copyright © 2024 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

This table records the number of revisions or changes done to this document as part of a release.

**Table 1: Document Control**

Version Number	Revision Date	Change Log
8.1.2.8.0	August 2024	No content updates for this release.
8.1.2.7.0	February 2024	Added Expand and Collapse button for <b>Events</b> .
8.1.2.6.0	October 2023	No content updates for this release.
8.1.2.5.0	June 2023	<ul style="list-style-type: none"><li>• Added Reviewer user role information.</li><li>• Added <b>Bulk Action section</b>.</li><li>• Updated the <b>Alert List</b> section and <b>Table 3</b> with new attribute field details.</li></ul>
8.1.2.4.0	March 2023	<ul style="list-style-type: none"><li>• Added information about Show Wire Stripping Alert Count toggle button in <b>Queue Management section</b>.</li><li>• Updated the <b>Alert List</b> and <b>Alert Details</b> section with information about Wire Stripping Alert.</li><li>• Updated <b>Events</b> section with information about Select All option.</li></ul>

---

## Contents

<b>1</b>	<b>Preface .....</b>	<b>3</b>
1.1	Who Should Use This Guide .....	3
1.2	How this Guide is Organized.....	3
1.3	Related Documents.....	3
1.4	Conventions .....	4
<b>2</b>	<b>About Transaction Filtering.....</b>	<b>5</b>
2.1	Transaction Filtering Workflow .....	5
2.2	Features of Transaction Filtering.....	6
2.3	Score Matching Logic.....	7
2.4	User Roles and Actions .....	7
<b>3</b>	<b>Getting Started.....</b>	<b>10</b>
3.1	Accessing OFSAA Page.....	10
3.2	Managing OFSAA Page.....	11
3.2.1	<i>Applications Tab</i> .....	11
3.2.2	<i>Changing the Application Password</i> .....	11
3.2.3	<i>Viewing the Application's Copyright Information</i> .....	12
3.3	Troubleshooting Your Display.....	13
3.3.1	<i>Enabling JavaScript</i> .....	13
3.3.2	<i>Enabling Cookies</i> .....	13
3.3.3	<i>Enabling Temporary Internet Files</i> .....	13
3.3.4	<i>Enabling File Downloads</i> .....	13
3.3.5	<i>Setting Print Options</i> .....	14
3.3.6	<i>Enabling the Pop-Up Blocker</i> .....	14
3.3.7	<i>Setting Home Page Preferences</i> .....	14
3.4	Logging in to the Transaction Filtering Application .....	15
<b>4</b>	<b>Managing Transaction Filtering .....</b>	<b>16</b>
4.1	Investigation User Interface Workflow .....	16
4.2	List Management .....	18
4.2.1	<i>Good Guy Summary Section</i> .....	19
4.2.2	<i>List History Section</i> .....	20

---

4.2.3	Match History .....	21
4.2.4	Approving or Rejecting Alerts .....	21
4.2.5	Watchlist Details .....	22
4.3	Queue Management.....	22
4.3.1	List View .....	23
4.3.2	Grid View .....	24
4.4	Alert List .....	26
4.4.1	Managing the Alerts .....	28
4.4.2	Field Descriptions .....	38
4.5	Alert Details .....	40
4.5.1	Analyzing the Alert .....	40
4.5.2	Analyzing the Wire Stripping Alert .....	41
4.5.3	Field Descriptions .....	65
<b>5</b>	<b>OFSAA Support Contact Details .....</b>	<b>68</b>
<b>6</b>	<b>Send Us Your Comments.....</b>	<b>69</b>

# 1 Preface

This guide explains Oracle Financial Services Transaction Filtering concepts and provides step-by-step instructions for navigating the Oracle Financial Services Transaction Filtering web pages, analyzing, acting on, and researching the business information.

## 1.1 Who Should Use This Guide

The Transaction Filtering User Guide is designed for the following users:

- **Reviewer:** This user works on the alerts within the application frequently. This user can only view within the application and cannot perform any actions.
- **Analyst:** This user works on the alerts within the application frequently. This user's specific role determines what they can view and perform within the application.
- **Supervisor:** This user works on the alerts within the application daily and is typically a higher-level Analyst or Compliance Officer.
- **Senior Supervisor:** This user works on the alerts within the application with additional functionalities as a Bulk update, set priorities, and change Due Date Time.

## 1.2 How this Guide is Organized

The Transaction Filtering User Guide includes the following chapters:

- [About Transaction Filtering](#), provides an overview of Oracle Financial Services Transaction Filtering, how it works, and what it does.
- [Getting Started](#), explains common elements of the interface, includes instructions on how to configure your system, access Transaction Filtering, and exit the application.
- [Managing Transaction Filtering](#), explains the Transaction Filtering application components.

## 1.3 Related Documents

For more information about Oracle Financial Services Transaction Filtering, refer to the following documents:

- Oracle Financial Services Sanctions Installation Guide
- Oracle Financial Services Sanctions Release Notes
- Oracle Financial Services Sanctions Queue Management User Guide
- Transaction Filtering Administration Guide
- Transaction Filtering User Guide
- Transaction Filtering Reporting Guide
- Transaction Filtering Matching Guide

These documents are available at the following links:

- [Sanctions Application Pack home page](#)
- [Transaction Filtering Guides home page](#)

To find more information about Oracle Financial Services Transaction Filtering and our complete product line, visit our Web site at [Oracle for Financial Services home page](#).

## 1.4 Conventions

The following table explains the text conventions used in this guide.

**Table 1: Conventions**

Convention	Description
<i>Italics</i>	<ul style="list-style-type: none"> <li>Names of books, chapters, and sections as references</li> <li>Emphasis</li> </ul>
<b>Bold</b>	<ul style="list-style-type: none"> <li>Object of an action (menu names, field names, options, button names) in step-by-step procedures</li> <li>Commands typed at a prompt</li> <li>User input</li> </ul>
Monospace	<ul style="list-style-type: none"> <li>Directories and subdirectories</li> <li>File names and extensions</li> <li>Process names</li> <li>Code sample, including keywords and variables within a text and as separate paragraphs, and user-defined program elements within a text</li> </ul>
<Variable>	Substitute input value

## 2 About Transaction Filtering

Oracle Financial Services Transaction Filtering is a Sanctions screening system that identifies Individuals, entities, cities, countries, goods, ports, BICs, and Stop keywords that may be suspicious, restricted, or sanctioned in relation to a financial transaction that is processed through the TF application. The application enables you to integrate with any clearing or payment system, accept messages from the source system, and scans them against different watch lists maintained within the application to identify any suspicious data present within the message. The TF application can scan messages that are in SWIFT, ISO20022, Fedwire, NACHA, or any custom format.

The OFS Transaction Filtering application is built using the Oracle Financial Services Analytical Applications (OFSAA) product suite components. These components are Oracle Enterprise Data Quality (OEDQ) and Inline Processing Engine (IPE).

Financial Institutions are required to comply with regulations from different authorities. Some of them are:

- USA PATRIOT Act
- U.S. Treasury's Office of Foreign Assets Control (OFAC), USA
- Office of the Superintendent of Financial Institutions (OSFI), Canada
- Financial Action Task Force (on Money Laundering) (FATF/GAFI)
- EU Commission
- Country-specific authorities

While the regulations can differ between countries, the spirit of regulatory intervention is uniform, and that is to hold financial institutions responsible and accountable if they have been a party, intentionally or unintentionally, to a criminal or terrorist-related transaction.

Sanctions include the withholding of diplomatic recognition, the boycotting of athletic and cultural , and the sequestering of the property of citizens of the sanctioned country. However, the forms of sanctions that attract the most attention and are likely to have the greatest impact are composed of various restrictions on international trade, financial flows, or the movement of people.

Transaction Filtering against government-regulated watch lists and internal watch lists is a key compliance requirement for financial institutions across the globe. At the turn of the century, Financial Institutions (FIs) were expected to identify customers either who were sanctioned or who lived in sanctioned countries and identify any transactions that were associated with these customers. FIs are now expected to identify any suspicious dealings and parties involved in the transaction, and more recently, identify information that is deliberately hidden or removed.

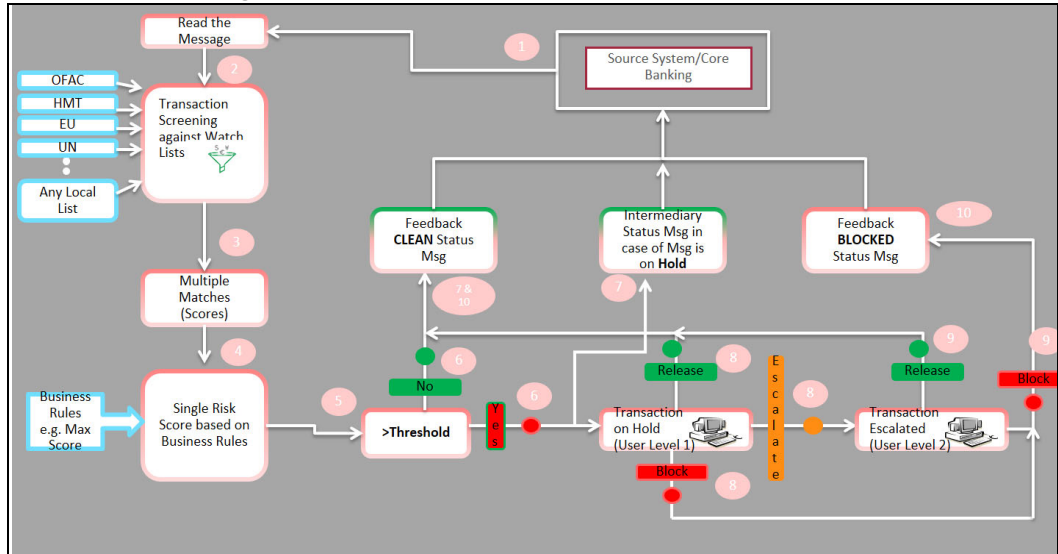
The TF application delivers a strong, effective filter that identifies all sanctioned individuals or entities with true positives and exploits all available information (internal and external) to reduce false positives and minimizes the operational impact on FIs.

### 2.1 Transaction Filtering Workflow

The following image describes the Transaction Filtering workflow:



**Figure 1: Transaction Filtering Workflow**



The application first receives a message from the payment system and scans it against the watch lists, and then provides a risk score for the message. If no suspicious data is found during screening, then the TF application sends a feedback message with the status CLEAN back to the payment system through the message queue. If suspicious data is found during screening, then the message is sent to an Analyst who investigates it using the TF User Interface. Feedback is sent to the payment system through a message queue, which indicates that the message is on hold. The Analyst reviews the message, which is the first level of review, and decides to release, block or escalate the message. Based on the decision, the system sends a feedback message, either CLEAN or BLOCKED, to the payment system for the reviewed message.

If the four-eyes workflow is enabled, then the Analyst can additionally Recommend to Release, Recommend to Block, or escalate the message to the Supervisor. If the Analyst escalates the message, then the message is sent to the Supervisor, which is the second level of review. The Supervisor can block or release the message and add comments. For four-eyes workflow, the Supervisor can Release, Block, or Reject the message. You can view the associated matched data of a message from the Match Summary section. You can also view the risk score details from the Risk Summary section. Both these sections are present in the Investigation User Interface.

The Senior Supervisor can perform Bulk Update (Assign alerts, set alert priority, and change the Due Date Time) and add attachments.

**NOTE** As a Senior Supervisor privilege, the Senior Supervisor can work on a queue only if there is a backlog.

Reviewer can view and review the messages and the alerts but cannot perform any other action.

## 2.2 Features of Transaction Filtering

Following are the features of Transaction Filtering:

- Screens financial transactions to detect blacklisted entities such as individuals, Organizations, Countries, and Cities with whom any business or transaction is prohibited.
- Generates a match score for any given message or alert through rules configured within the application using the IPE system. These match rules screen entities such as individuals,

- Organizations, Countries, and Cities with whom any business or transaction is prohibited using EDQ.
- Generates a risk score for any given message or alert through rules configured within the application. These risk rules contain parameters such as amount, currency, destination country, and so on in the IPE system.
  - Marks suspicious alerts based on configured parameters.
  - Configures scores for different matching rules.
  - Provides the ability to add general notes/comments to the alert, either as an Analyst or as Supervisor.
  - Provides the ability to add notes/comments while taking action on the alert. For a standard workflow, the actions are Release, Block, and Escalate for an Analyst, and Release and Block for a Supervisor. For a four-eyes workflow, the actions are recommended to Release, Recommend to Block, and Escalate for an Analyst, and Release, Block and Reject for a Supervisor. Manages and maintains multiple watch lists.
  - Supports a flexible and configurable workflow. It can have many levels of alert management and user profiles to enable the segregation of duties.

## 2.3 Score Matching Logic

There are two types of scores:

- **Match Score:** A number indicating the strength of the correlation between the input message data and the match list record. The match score is expressed as an integer between 1 and 100, with higher numbers indicating a stronger match.
- **Risk Score:** A number indicating the relative 'riskiness' of the message. The risk score is expressed as an integer between 1 and n, with higher numbers indicating a higher risk.

Transaction Filtering includes a mechanism for estimating the relative risk associated with a message. A risk score is calculated based on risk rules. Each risk rule contains attributes such as currency, amount, destination country, originator country, and so on. See the *Configuring Risk Scoring Rules* section in the *OFS Transaction Filtering Administration Guide* for a complete description of the risk scores.

The logic used in scoring the and its respective alerts is as follows:

A match score is generated out of the screening results generated from the Enterprise Data Quality (EDQ) matching engine. A risk score is then generated from the risk assessment in the Inline Processing Engine (IPE) risk rule engine. The risk rule is the sum of the match score and the risk scores that are generated for each message. Also, if the risk score is greater than the risk threshold configured in the risk rule engine, then an alert is generated.

## 2.4 User Roles and Actions

The following user roles are defined in OFS Transaction Filtering:

- Reviewer
- Analyst
- Supervisor
- Senior Supervisor

- Queue Administrator

---

**NOTE**

The Queue Administrator can add/edit/assign the queues to user groups. for more information on Queue Administrator, see the [OFS Queue Management User Guide](#).

The following table explains the tasks that can be performed by various users in the Transaction Filtering application:

**Table 2: User Roles and Actions**

Action	Reviewer	Analyst	Supervisor	Senior Supervisor	Queue Administrator
<b>Queue Level</b>					
Add					✓
Edit					✓
Assign					✓
Delete					✓
Open	✓	✓	✓	✓	
<b>Alert Level</b>					
Access to View UI	✓	✓	✓	✓	
Recommend to Release Transaction		✓			
Recommend to Block Transaction		✓			
Release Transaction		✓	✓		
Block Transaction		✓	✓		
Escalate Transaction		✓			
Reject Transaction			✓		
Bulk Update: <ul style="list-style-type: none"> <li>• Assign Alerts</li> <li>• Change the Priority</li> <li>• Change Due Date Time</li> </ul>				✓	
Add attachments		✓	✓	✓	
Download attachments	✓	✓	✓	✓	
Bulk Action		✓	✓		

**NOTE**

The user actions of each role can be configured as per the requirement except **Bulk Update** and **Add Attachments**. For more information, see [OFS Transaction Filtering Administration Guide](#).

## 3 Getting Started

### 3.1 Accessing OFSAA Page

Access to the Oracle Financial Services application depends on the Internet or Intranet environment. Oracle Financial Services can be accessed through Google Chrome. Your system administrator provides the intranet address uniform resource locator.

Your system administrator provides you with a User ID and Password. Log in to the application through the Login page. You will be prompted to change your password on your first login. You can change your password whenever required by logging in. For more information, see [Changing the Application Password](#).

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

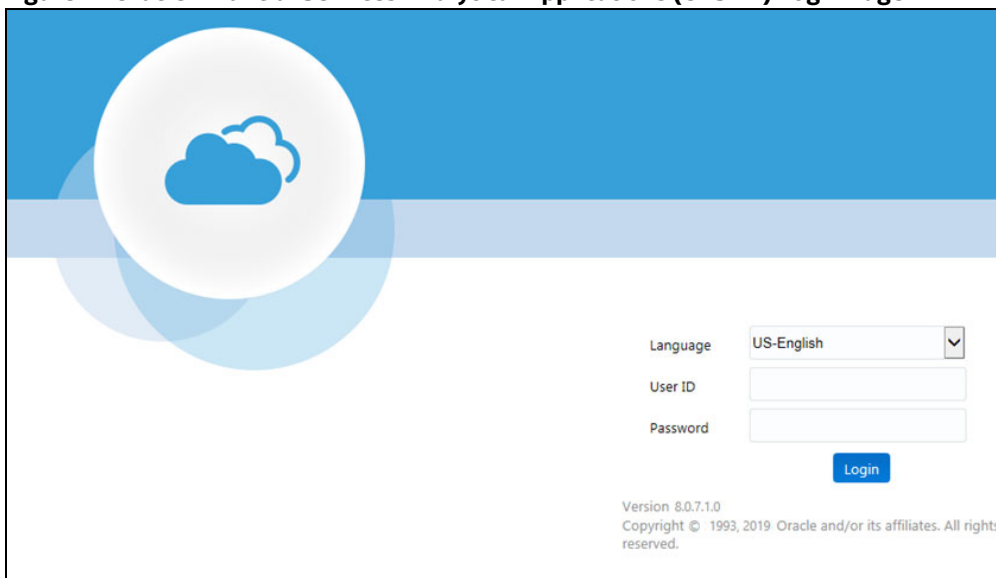
1. Enter the URL into your browser using the following format:

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

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

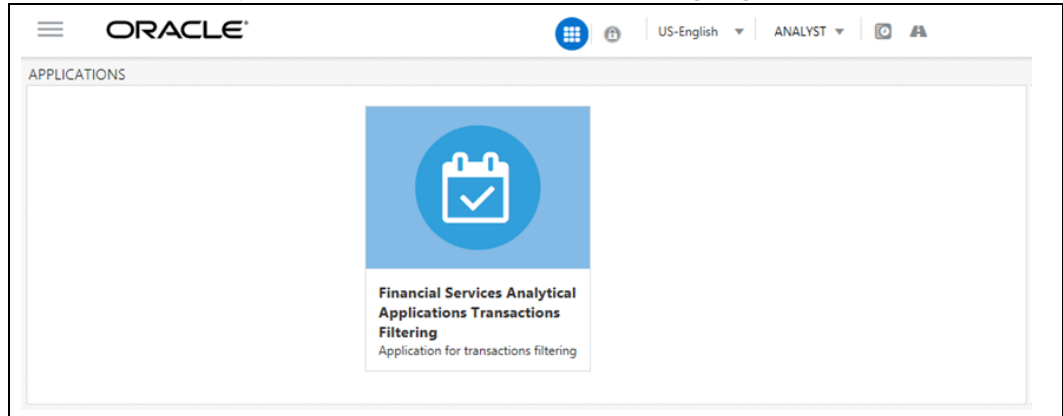
The **Oracle Financial Services Analytical Applications (OFSAA)** login page is displayed.

**Figure 2: Oracle Financial Services Analytical Applications (OFSAA) Login Page**



2. Select the language from the **Language** drop-down list. This allows you to use the application in the language of your selection.
3. Enter your User ID and Password in the respective fields.
4. Click **Login**. The **Financial Services Analytical Applications Transactions Filtering** home page is displayed.

Figure 3: Financial Services Analytical Applications Transactions Filtering Page



To view the **Financial Services Analytical Applications Transactions Filtering** home page, click **Calendar** .

## 3.2 Managing OFSAA Page

### 3.2.1 Applications Tab

The Applications tab lists the various OFSAA Applications that are installed in the OFSAA setup based on the logged-in user and mapped OFSAA Application User Groups.

For example, to access the OFSAA Applications, select the required Application from the **Select Application** drop-down list. Based on your selection, the page refreshes the menus and links across the panes.

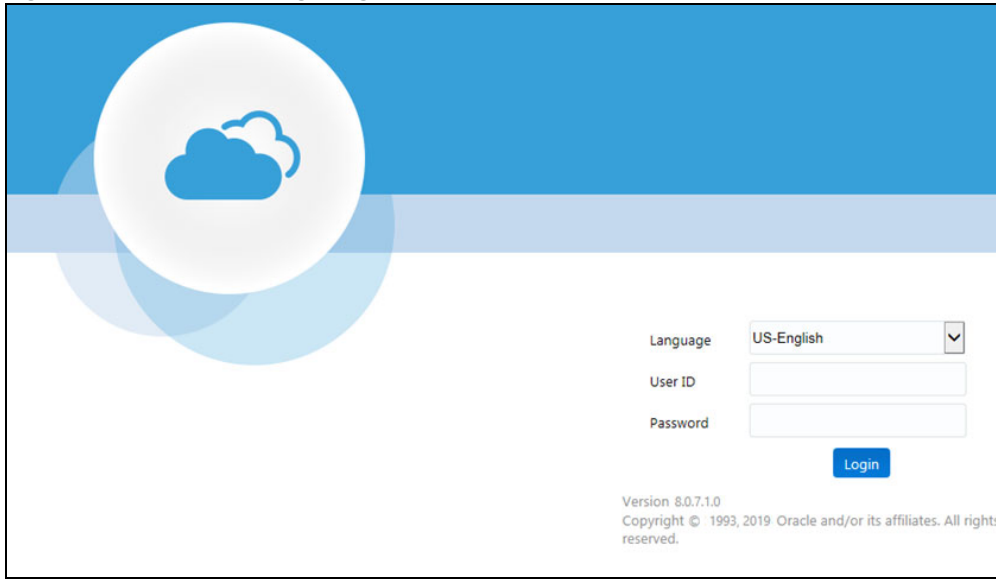
### 3.2.2 Changing the Application Password

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

To change the password, follow these steps:

1. Navigate to the **Oracle Financial Services Analytical Applications** page.
2. Click the **User** drop-down list and select **Change Password**. The **Password Change** page is displayed.

**Figure 4: Password Change Page**



3. Enter your old and new passwords in the respective fields.
4. Click **OK**. Your password is changed successfully. The application navigates back to the login page, where you can log in with the new password.

**NOTE**

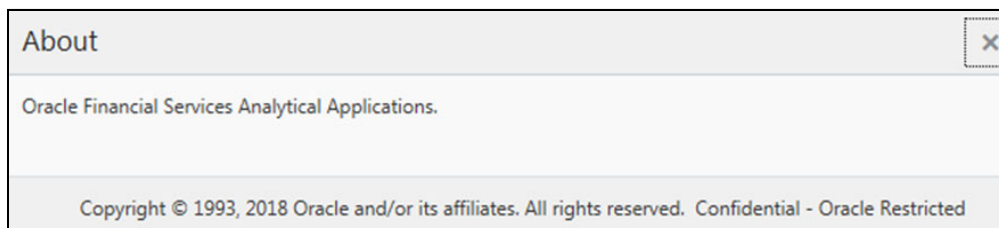
Your password is case-sensitive. If you have problems with the password, verify that the Caps Lock key is off. If the problem persists, contact your System Administrator.

### 3.2.3 Viewing the Application's Copyright Information

To access copyright information, follow these steps:

1. Navigate to the **Oracle Financial Services Analytical Applications (OFSAA)** page.
2. Click the **About** hyperlink on the **Oracle Financial Services Analytical Applications** login page. The copyright text displays in a new window.

**Figure 5: Financial Services Transaction Filtering Copyright Information**



To close the window, click **Close** **X**.

## 3.3 Troubleshooting Your Display

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

### 3.3.1 Enabling JavaScript

This section describes how to enable JavaScript. To enable JavaScript, follow these steps:

1. Navigate to the Tools menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**. The **Security Settings** dialog box displays.
5. In the **Settings** list and under the **Scripting** setting, enable all options.
6. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

### 3.3.2 Enabling Cookies

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

### 3.3.3 Enabling Temporary Internet Files

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

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

1. Navigate to the Tools menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. On the **General** tab, click **Settings**. The **Settings** dialog box displays.
4. Click the **Every visit to the page** option.
5. Click **OK**, then click **OK** again to exit the **Internet Options** dialog box.

### 3.3.4 Enabling File Downloads

This section describes how to enable file downloads.

To enable file downloads, follow these steps:

1. Navigate to the Tools menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Security** tab and then click the **Local Intranet** icon as your Web content zone.
4. Click **Custom Level**. The **Security Settings** dialog box displays.
5. Under the **Downloads** section, ensure that **Enable** is selected for all options.



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

### 3.3.5 Setting Print Options

This section explains how to enable printing background colors and images.

To enable this option, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Advanced** tab. In the **Settings** list, under the **Printing** setting, click **Print background colors and images**.
4. Click **OK** to exit the **Internet Options** dialog box.

---

**NOTE**

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

### 3.3.6 Enabling the Pop-Up Blocker

You may experience difficulty running the Oracle Financial Services application when the Pop-up Blocker is enabled. It is recommended to add the application URL to the Allowed Sites in the Pop-up Blocker Settings.

To enable Pop-up Blocker, follow these steps:

1. Navigate to the **Tools** menu.
2. Click **Internet Options**. The **Internet Options** dialog box is displayed.
3. Click the **Privacy** tab. In the Pop-up Blocker setting, select the **Turn on Pop-up Blocker** option. The **Settings** enable.
4. Click **Settings** to open the Pop-up Blocker Settings dialog box.
5. In the Pop-up Blocker Settings dialog box, enter the application URL in the text area.
6. Click **Add**. The URL appears in the Allowed site list.
7. Click **Close**, then click **Apply** to save the settings.
8. Click **OK** to exit the **Internet Options** dialog box.

### 3.3.7 Setting Home Page Preferences

The **Preferences** section enables you to set the preferences for your home page.

To access this section, follow these steps:

1. Navigate to the **Oracle Financial Services Analytical Applications (OFSAA)** page.
2. Click **Preferences** from the drop-down list in the top right corner, where the user name is displayed. The **Preferences** page is displayed.

**Figure 6: Financial Services Transaction Filtering Preferences Page**

Property Name	Property Value
Set My Home Page	Default Screen <input type="button" value="v"/>

3. In the **Property Value** drop-down list, select the application you want to set as the home page.

**NOTE** Whenever a new application is installed, the corresponding value is found in the drop-down list.

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

## 3.4 Logging in to the Transaction Filtering Application

You can access the Transaction Filtering (TF) application from the **Oracle Financial Services Analytical Applications** page. This page is divided into two panes:

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

To access the Transaction Filtering application, follow these steps:

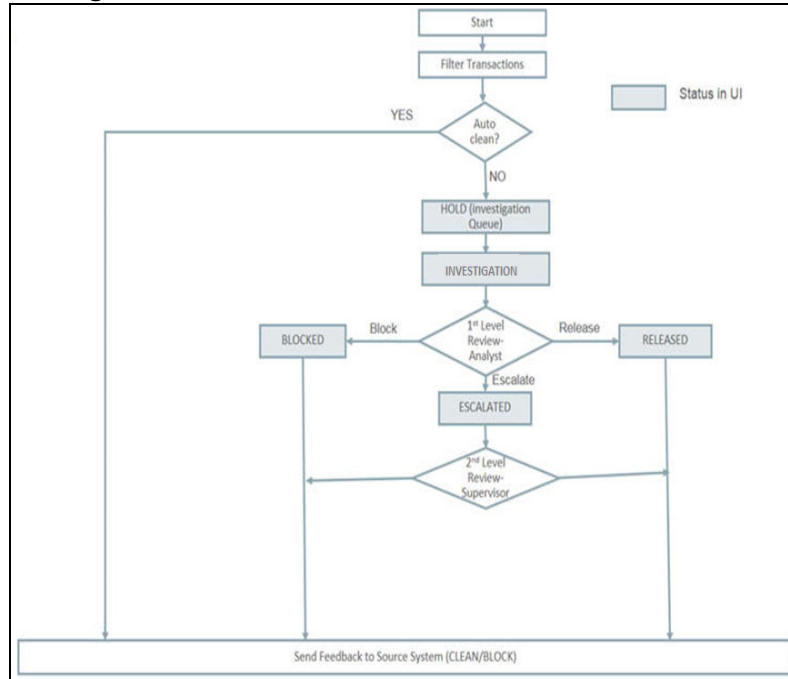
1. Navigate to the **Oracle Financial Services Analytical Applications** page.
2. Click **Financial Services Sanctions Pack**.
3. Click **Transaction Filtering**. The **Investigation User Interface** page is displayed.

## 4 Managing Transaction Filtering

### 4.1 Investigation User Interface Workflow

The Investigation User Interface for Transaction Filtering has the following workflow:

**Figure 7: Investigation User Interface Workflow**

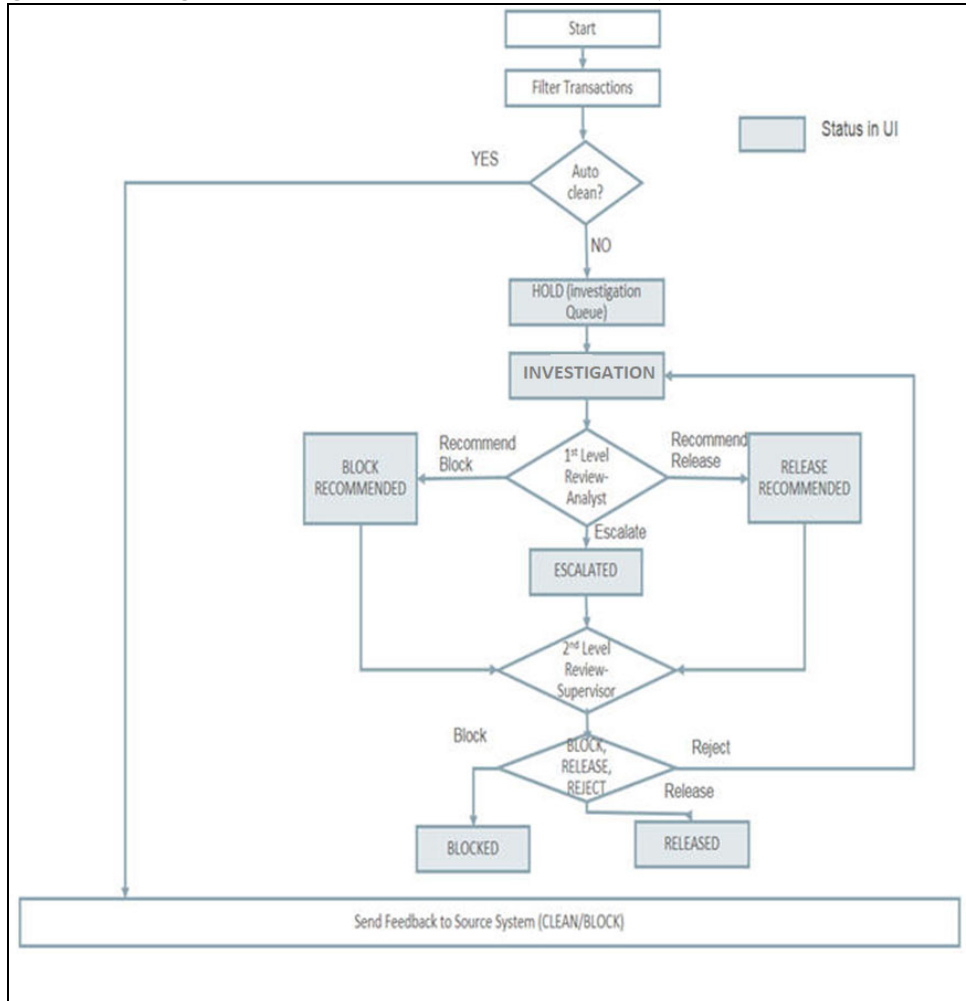


A suspicious message that is obtained after transactions are filtered is displayed in the Analyst’s queue. These messages are auto cleaned by the application. If the message is clean, then a feedback message is sent back to the Transaction Filtering application. If not, the message is put on Hold (**H**). The Analyst picks up the message from the queue by locking it. The message is then Investigation (**I**). Then the Analyst must analyze the message by observing the message details that are displayed in different sections of the UI. The Analyst can then decide if the message must be Blocked (**B**), Released (**R**), or Escalated (**E**). If the message is escalated, then the alert is assigned to the Supervisor. The Supervisor can then Release or Block the message.

The Supervisor can overwrite any action provided by the Analyst. So if the Analyst has selected Release, the Supervisor can block or release the message, and if the Analyst has selected Block, the Supervisor can block or release the message. The Supervisor can also view any messages irrespective of the message status and take final action on the message.

The Investigation User Interface for Transaction Filtering has the following workflow for four-eyes approval:

Figure 8: Investigation User Interface Workflow for Four-Eyes Approval

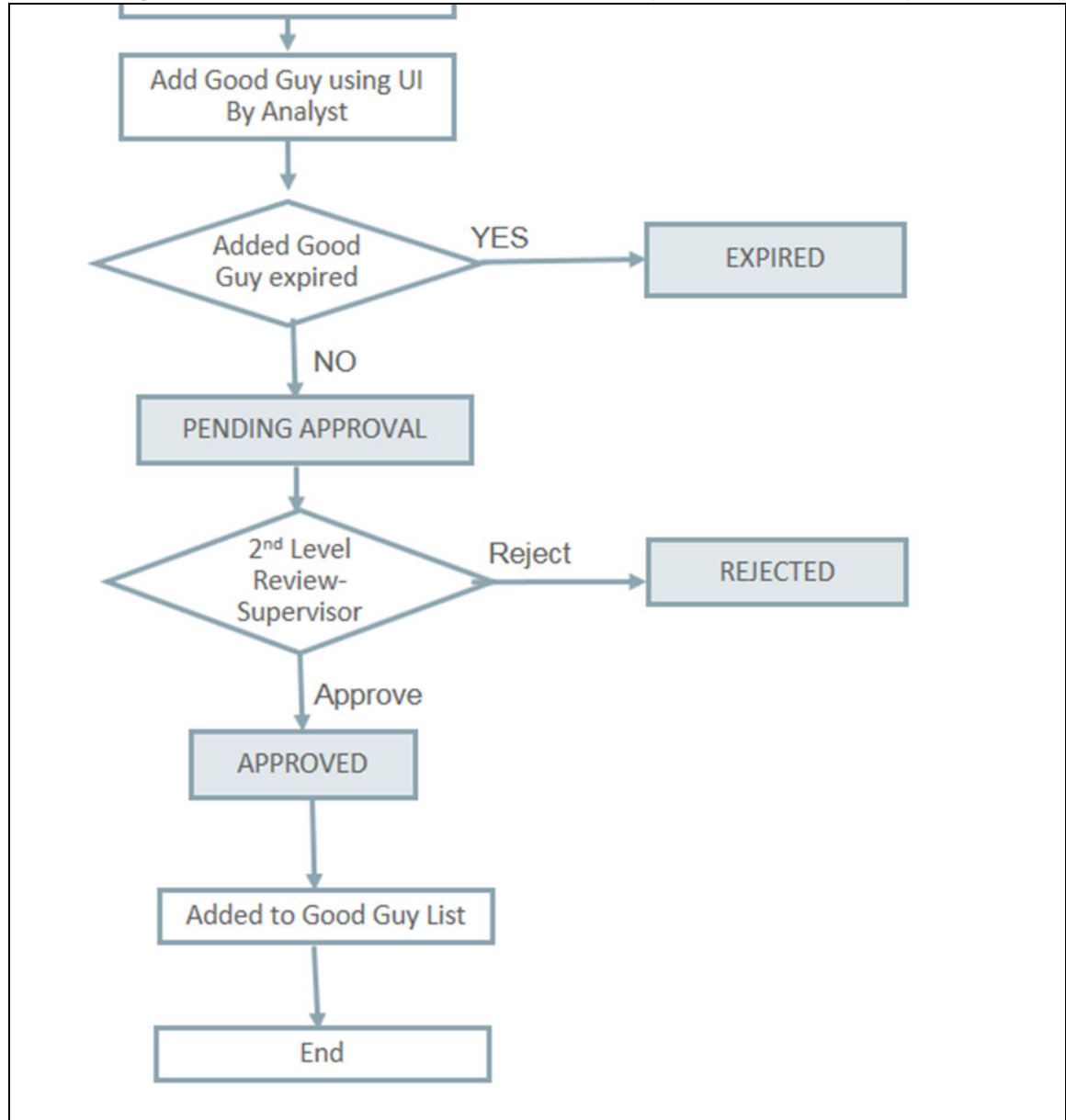


A suspicious message that is obtained after transactions are filtered is displayed in the Analyst’s queue. These messages are auto-cleaned by the application. If the message is clean, then a feedback message is sent back to the Transaction Filtering application. If not, the message is put on Hold (**H**). The Analyst picks up the message from the queue by locking it. The message is moved to Investigation (**I**). Then the Analyst must analyze the message by observing the alert details that are displayed in different sections of the UI. The Analyst can then decide if the message action must be Recommend to Block (**BR**), Recommend to Release (**RR**), or Escalated (**E**). If the message is escalated, then the message is assigned to the Supervisor. The Supervisor can then Release, Block or Reject the message.

The Supervisor can overwrite any action provided by the Analyst. So if the Analyst has selected Release, the Supervisor can block or release the message, and if the Analyst has selected Block, the Supervisor can block or release the message. The Supervisor can also view any message irrespective of the message status and take final action on the message.

The Investigation User Interface for Transaction Filtering has the following workflow to add a Good Guy record to the Good Guy list.

Figure 9: Investigation User Interface Workflow to add a Good Guy Record to the Good Guy List



The Analyst adds the Good Guy record in the Investigation User Interface. It then goes to the Supervisor for approval. If the Supervisor approves the Good Guy record, it is added to the Good Guy list. For information on the elements in the **Investigation User Interface** page, see [Good Guy Summary Section](#).

## 4.2 List Management

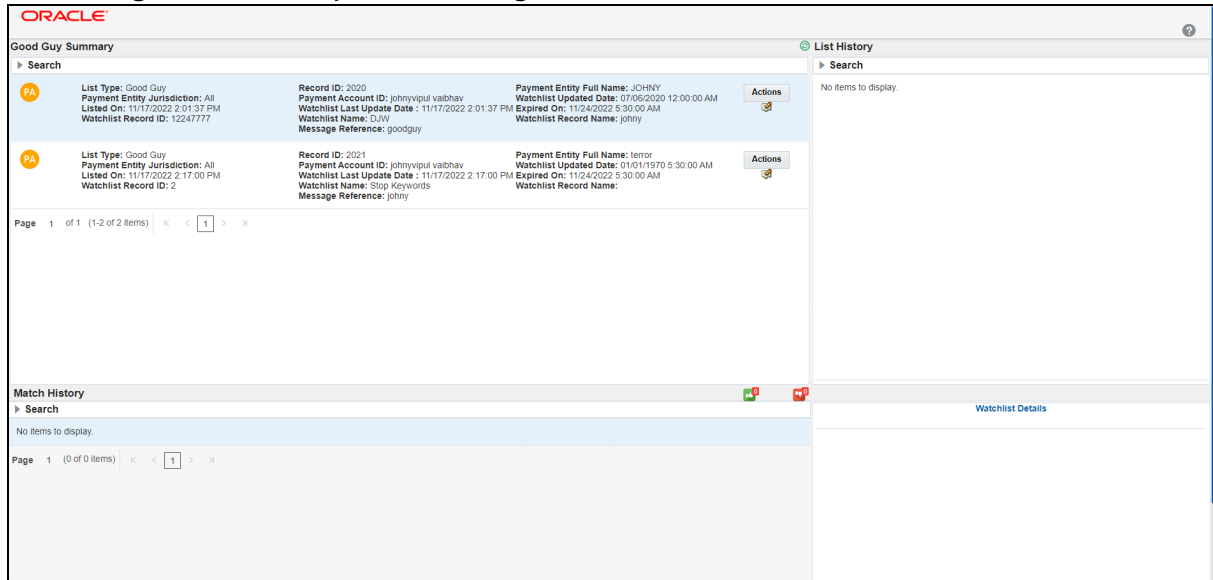
This section displays the Good Guy Summary, List History, Match History, and the Watchlist Details sections.

User with Reviewer, Supervisor and Administrator roles can access the data but only users with Supervisor and Administrator roles can manage the lists under the Good Guy Summary, List History, and Match History sections using the search criteria.

As a Supervisor, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**.
2. Click **Financial Services Sanctions Pack**.
3. Click **List Management**. The **Good Guy List Details** page appears.

**Figure 10: Good Guy List Details Page**



### 4.2.1 Good Guy Summary Section

This section displays the list of alerts that the Analyst has sent to the Supervisor. The Supervisor can approve or reject the alert by clicking **Actions**.

Supervisor user with the new role **TFLTGGUPDT** can also perform the **Add/Edit/Delete** actions.


If the Supervisor approves the alert, the orange tick changes to a green tick, and the color of the **Add to Good Guy** button changes to grey. The record is added to the FCC\_WHITELIST table.


If the Supervisor rejects the alert, the orange tick changes to a red cross, and the color of the **Add to Good Guy** button changes to grey. For more information, see [Approving or Rejecting Alerts](#).

You can also search for a message using the following criteria:

- **Record ID:** Enter or search for a record ID.
- **Payment Entity Full Name:** Enter or search for record name.
- **Payment Entity Jurisdiction:** You can either enter a jurisdiction name or select from the drop-down list.
- **Payment Account ID:** Enter the identifier.
- **Listed On**
  - **Basic Search:** Enter the listed date value.
  - **Advanced Search:** Select the From Date and To Date to identify the alerts listed between the date.

- **Watchlist Last Update Date**
  - **Basic Search:** Enter the last updated date value.
  - **Advanced Search:** Select the From Date and To Date to identify the alerts updated between the date.
- **Expired On**
  - **Basic Search:** Enter the expired date value.
  - **Advanced Search:** Select the From Date and To Date to identify the alerts that expired.
- **Watchlist Record ID:** Enter the origin record id.
- **Watchlist Name:** Enter the name of the origin.
- **Watchlist Record Name:** Enter the origin record name.
- **Status:** Enter the status of a message.

To reset the search criteria, click **Reset** 

To refresh the page, click **Refresh** .

**NOTE**

If the alert has only the good guy matches and there are no pending actions, then the alert will be automatically suppressed, and the feedback message will be displayed as the alert is clean and suppressed. You can find the released alert details in the Feedback Messages. For more information, see the Feedback Messages section in [Technical Integration Guide](#).

#### 4.2.1.1 Auditing of a Good Guy

This section displays the auditing of a good guy in the following cases:


- When the Alert is suppressed, then the status of the alert in the `FSI_RT_RAW_DATA` table will come as GGS (Good Guy Suppression).
- If there is a match in message for Good Guy, `N_WHITE_LIST_ID` from table `FCC_WHITE_LIST` of that Good Guy will be mapped to `N_RESPONSE_ID` from `FSI_RT_WLS_RESPONSE` table of that match in the `FCC_RESP_WHITE_LIST_MAP` table.


#### 4.2.2 List History Section

This section displays the list of history. You can use the following **Search Filter** fields to perform the search:

- **Payment Entity Jurisdiction:** You can either enter a jurisdiction name or select from the drop-down list.
- **Record ID:** Enter the record id value.
- **Watchlist Name:** Enter the name of the origin
- **Watchlist Record ID:** Enter the origin record id value.
- **Status:** Enter the status value.
- **Payment Entity Full Name:** Enter the record name.

- **Watchlist Record Name:** Enter the origin record name.


To reset the search criteria, click **Reset** 

To refresh the page, click **Refresh** .

### 4.2.3 Match History

This section provides the Match History list details. Users can use the following **Search Filter** fields to perform the search:


- **Match History:** Enter the match history.
- **Matched Type:** Enter the matched type value.
- **Matched List:** Enter the matched list value.
- **Match Score:** Enter the match score value.
- **Matched Sub List:** Enter the match sub-list value.
- **Matched Rule Name:** Enter the matched rule name.
- **Status:** Enter the status value.

To reset the search criteria, click **Reset** 

To refresh the page, click **Refresh** .


### 4.2.4 Approving or Rejecting Alerts

To approve or reject the alert as a Supervisor, follow these steps:

1. Log in to the **Financial Services Analytical Applications Transactions Filtering home page** as the Supervisor.
2. Click **Calendar** .
3. Click **Financial Services Sanctions Pack**.
4. Click **List Management**. The **Good Guy List Details** page appears.



**Figure 11: Good Guy List Details**

5. In the **Actions** button, click **Approve** to approve the alert or click **Reject** to reject the alert.
6. It is mandatory to add comments after the alert is approved or rejected. To add comments, follow these steps:
  - a. Click **Add Comments**  that is in line with the alert that you want to add comments to. The comments window is displayed.
  - b. Enter your comments and click **Save**. The comment is added to the audit history of that alert.

---

**NOTE** The Supervisor can change the Matching Configuration per record.

## 4.2.5 Watchlist Details

This section displays the watch list details that match with the alert data. This helps you analyze the alert and decide if it has to be passed or not. A unique Record ID is assigned to every watchlist/sanctioned record. See the Watch Lists appendix in the [OFS Transaction Filtering Administration Guide](#) for information on the different watch lists used.

## 4.3 Queue Management

Queue Management is a common dashboard where the following users can see queues related to CS and TF that are created by the Queue Administrator and the system (OOB):

- Reviewer
- Analyst
- Supervisor
- Senior Supervisor

Queue management page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups see the [OFS Transaction Filtering Administration Guide](#).

You can view the Queue details in the following formats:

- [List View](#)
- [Grid View](#)

By default, queue details are displayed in the List View.

For more information on Queue Administrator. See the [OFS Sanctions Queue Management User Guide](#).

### 4.3.1 List View

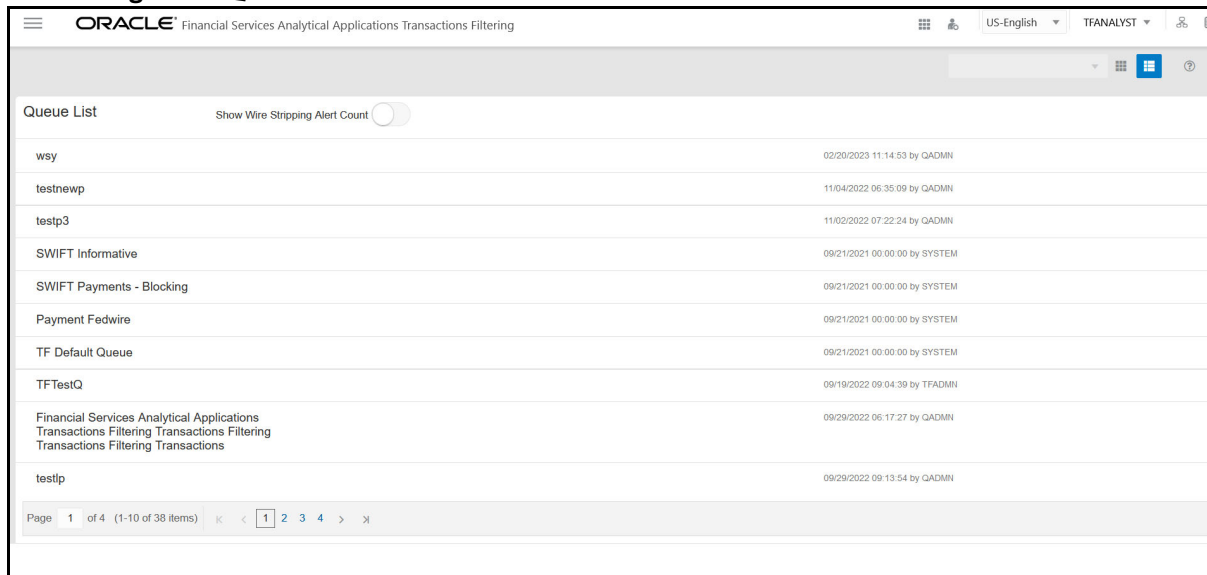
1. Log in to the application as Reviewer/Analyst/Supervisor/Senior Supervisor.
2. Select the **Financial Services Analytical Applications Transaction Filtering**.
3. From the **Application Navigation List**, select **Queue Management**.

You can select the **hamburger**  icon to view the **Queue List** for **All Teams** in List View.

By default, queue details are displayed in the List View.

Queue List displays the queues assigned to all user groups and the value. **All Team** is selected in the drop-down list and is disabled. It is displayed as the title for Queue List.

**Figure 12: Queue List in List View**



Queue Name	Date Time Created By
wsy	02/20/2023 11:14:53 by QADMIN
testnewp	11/04/2022 06:35:09 by QADMIN
testp3	11/02/2022 07:22:24 by QADMIN
SWIFT Informative	09/21/2021 00:00:00 by SYSTEM
SWIFT Payments - Blocking	09/21/2021 00:00:00 by SYSTEM
Payment Fedwire	09/21/2021 00:00:00 by SYSTEM
TF Default Queue	09/21/2021 00:00:00 by SYSTEM
TFTestQ	09/19/2022 09:04:39 by TFADMIN
Financial Services Analytical Applications Transactions Filtering Transactions Filtering Transactions Filtering Transactions	09/29/2022 06:17:27 by QADMIN
testtp	09/29/2022 09:13:54 by QADMIN

The following details are displayed in the List View for **All Team**:

- Queue Name
- Date Time Created By (For example, 09/09/2021 14:06:39 by QADMIN/SYSTEM)

You can view ten queues in the Queue List and use the navigation to view the next set of queues.

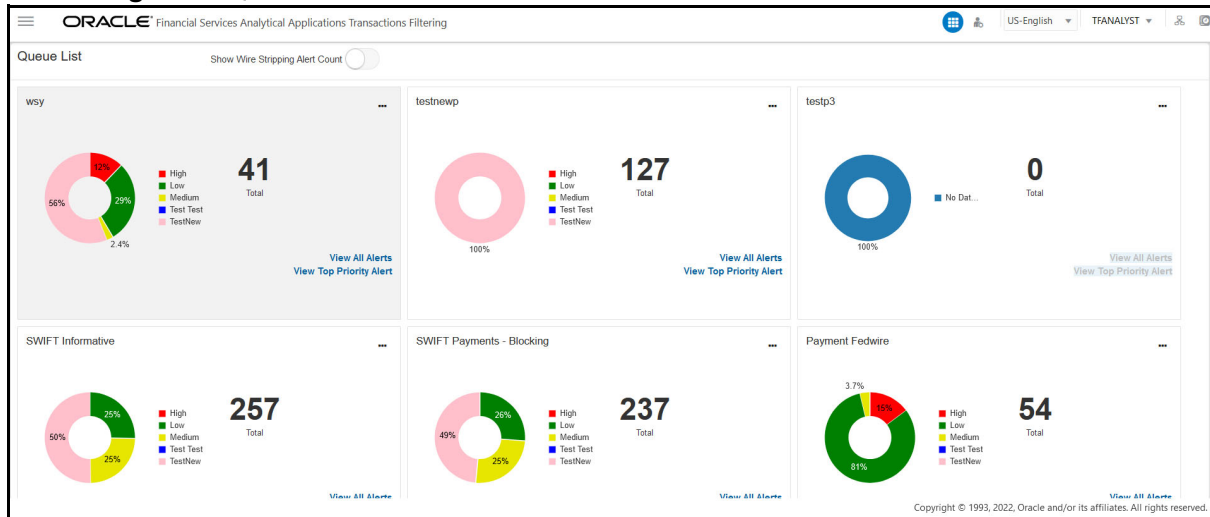
A Reviewer user can access and view all the alerts from any queue.

## 4.3.2 Grid View

You can select the **thumbview**  icon to view the **Queue List** for **All Teams** in Grid View.

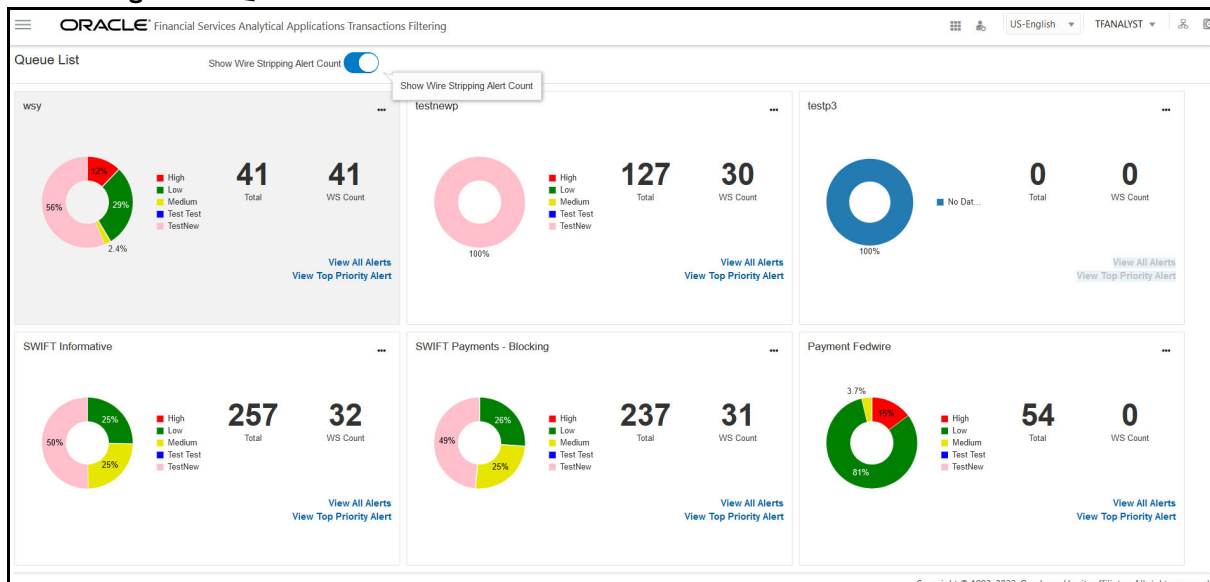
Queue List displays the queues assigned to all user groups and the value. **All Team** is selected in the drop-down list and is disabled. It is displayed as the title for Queue List.

**Figure 13: Queue List in Grid View**



You can click on the **Show Wire Stripping Alert Count** toggle button to display the WS alert count for each queue which makes the WS alert easily identifiable. For More Information Configuring WS Fingerprint, see [OFS Transaction Filtering Administration Guide](#).

**Figure 14: Queue List in Grid View with WS Alert Count**



The Queue List appears in doughnut charts displays each cell's data as a slice of a doughnut. A pie chart data visualization uses a single circle divided into slices, each slice representing a numerical proportion of the whole circle's value. Hover over the slices to see the details of the **Series** and the **Value** of the queue.

By default, the color-coding displayed for three priorities of the alerts and the **Total** numeric value indicates the number of alerts in that Queue.

The following are the default priorities in the application:

- High
- Medium
- Low

An admin can configure any number of priorities and color code that needs to be displayed on the Queue Management Dashboard against each of the priority based on their requirement in the backend based on the match score, screening type, event type, jurisdiction and business domain.

The Queue Management dashboard displays all the priorities defined by the admin and the number of alerts meeting the priority condition. If there are alerts which doesn't fall under any priority criteria are displayed as **No Priority Set**.

Priority configuration for all the alerts to be defined before transaction filtering.

You can view six queues in Queue List and use the navigation to view the next set of queues.

Queue Admin can assign one Queue to multiple User Groups and multiple Queues to one User Group.

For example, the 4 queues are in the following priority:

- 1 - Sanctions Queue
- 2 - Prohibition Queue
- 3 - PEP Queue
- 4 - EDD Queue

Once all the alerts in the Sanctions queue are investigated, when user navigates to the next alert, then the user will automatically pick up the alerts from the next most prioritized queue, which is Prohibition Queue.

While the user is working on Prohibition Queue and navigates to next alert, if in case any new alerts gets generated in the highest priority queue, which is Sanctions Queue, then the user will get the alerts from the Sanctions Queue.

If you try to access any Queue apart from the prioritized one, then an Alert Message **You cannot access the alerts in this queue as there are alerts already in high priority Queue** will be displayed. However, if there are no alerts in the high priority Queue, then the user can access the alerts in the next priority Queue.

**NOTE**

- The above scenario is applicable for Analyst and Supervisor roles only. Senior supervisor can access alerts from any queue.
- As an Analyst or Supervisor user, he/she should be able to access a specific alert across the Queues, (based on the security attributes) to make a decision and come back to the Alert List page, where all the alerts in the queue(s) are listed.
- A Reviewer user can access and view all the alerts from any queue.

You can perform the following actions on each queue:

- **Open:** Click the Ellipsis menu and then select **Open** to open the queue to see alerts inside the Queue. It is the same as View All. For more information on Managing Alerts, see the [Alert List](#) section.
- **View All Alerts:** Select View All Alerts to see the list of alerts in the Queue. For more information on Managing Alerts, see the [Alert List](#) section.
- **View Top Priority Alert:** Select View Priority Alert to see the alert details based on their priority. You can navigate to the next alert using the **Get Next** icon in the top right corner. For more information about Alert details, see the [Alert Details](#) section.

## 4.4 Alert List

The Alert List page displays a list of alerts assigned to the Analyst/Supervisor/Senior Supervisor in a default view. The users with the Senior Supervisor role can access all the alerts that are assigned/unassigned to the other users.

A Reviewer can see, access, customize the Alert List page and download attachments uploaded by other users in the Alert List page. A Reviewer cannot perform the following function:

- Bulk update on the alerts
- Save or update an attachment to an alert.
- Bulk Action

### NOTE

When a Reviewer opens an alert with any status, the status is unaffected, and the alert will not be assigned to the Reviewer user.

You can configure the functionality assigned to user group in the Alert list page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups see the [OFS Transaction Filtering Administration Guide](#).

Follow the subsequent steps to access the Alert List page:

1. Log on to the **Transactions Filtering** application.
2. Select the **Financial Services Transactions Filtering Application**.
3. From the **Navigation List**, select **Financial Services Sanctions Pack**.
4. Select the **Transactions Filtering Alert List**. The **Alert List** page appears.

Figure 15: Alert List Page

Alert ID	Message Reference	Transaction Reference	Status	Message Type	Cut-off Time	Message Category	Assignee	Message Direction	Amount	Currency	Priority	Last Updated Date Time	Due Date
69328		2015110500000001	Hold	MT101	N/A	SWIFT		INBOUND	11100	USD	Technical	03/03/2023 12:55:43	
69173	20200317CTRFULLC000156	N/A	Investigation	FDBTR1002	00:02 America/Chicago (-3h -10m -35m -5s)	FEDWIRE	TFANALYST	INBOUND		USD	High	03/02/2023 14:44:45	
69146	20200317CTRFULLC000156	N/A	Investigation	FDBTR1002	00:02 America/Chicago (-3h -10m -35m -5s)	FEDWIRE	TFANALYST	INBOUND		USD	High	03/02/2023 14:31:08	
69110	20200317CTRFULLC000156	N/A	Investigation	FDBTR1002	00:02 America/Chicago (-3h -10m -35m -5s)	FEDWIRE	TFANALYST	INBOUND		USD	High	03/02/2023 14:29:33	
69074	20200317CTRFULLC000156	N/A	Hold	FDBTR1002	00:02 America/Chicago (-3h -10m -35m -5s)	FEDWIRE		INBOUND		USD	High	03/02/2023 14:28:29	
69055	LKJOKJY000202210112010044900001	PE15E9THW2	Investigation	pac008.001.02	00:13 America/Argentina (-3h -23m -46s)	ISO20022	TFANALYST	OUTBOUND		EUR	Low	03/02/2023 14:25:34	
69051	LKJOKJY000202210112010044900001	PE15E9THW2	Investigation	pac008.001.02	00:13 America/Argentina (-3h -23m -46s)	ISO20022	TFANALYST	OUTBOUND		EUR	Low	03/02/2023 14:23:08	
69047	fb2a2619a1d86004	N/A	Investigation	MT103	N/A	SWIFT	TFANALYST	INBOUND	100	USD	Technical	03/02/2023 14:25:00	
69044	fb2a2619a1d86004	N/A	Hold	MT103	N/A	SWIFT		INBOUND	100	USD	Technical	03/02/2023 14:19:18	
69036	LKJOKJY000202210112010044900001	PE15E9THW2	Investigation	pac008.001.02	00:13 America/Argentina (-3h -23m -46s)	ISO20022	TFANALYST	INBOUND		EUR	Low	03/02/2023 14:13:50	

Alert List page contains the following default field details:

- Alert ID

**NOTE**

The Alerts with exclamation mark icon are Wire Stripping Alerts.

- Message Reference
- Transaction Reference
- Status
- Message Type
- Cut-off Time
- Message Category
- Assignee
- Message Direction
- Amount
- Currency
- Priority
- Last Updated Date Time
- Due Date Time
- Match Score
- Risk Score
- Alert Created Date

- Watchlist ID

**NOTE** Hover over the Watchlist ID value to display the complete list of watchlist IDs.

- Standard Comments
- Is wire Stripping Alert?
- Count of WL Record IDs
- Count of
- Is Bulk Actioned?
- Resolution Comment

**NOTE** Using the **Column** menu you can customize the optional fields. For more information, see [Customizing the Field Columns](#) section.

## 4.4.1 Managing the Alerts

You can carry out the following actions on the Alert List page:

- [Filtering the Alert List](#)
- [Sorting the Alerts](#)
- [Updating the Alerts \(Bulk Update\)](#)
- [Attaching a File to an Alert \(Analyst/Supervisor/Senior Supervisor\)](#)
- [Customizing the Field Columns](#)
- [Reordering the Columns](#)
- [Saving the View](#)
- [Managing Views](#)
- [Closed Alerts](#)
- [Exporting the Alerts from the List](#)
- [Reload the Grid](#)
- [Bulk Action](#)

### 4.4.1.1 Filtering the Alert List

You can filter the data to be displayed by selecting one of the criteria as mentioned in the **Alert list Filter**. In the top left corner, click **Filter**. You can also reset the search criteria by clicking the **Clear** button.

From the **Filter** menu select a criterion to filter the alerts. The following search filters are displayed:

- Resolution comment
- Assignee
- Cutoff Overdue
- Cut-off Time
  - From Date

- To Date
- Alert ID
- Created Date
  - From Date
  - To Date
- Received Date
  - From Date
  - To Date
- Message category
- Message Direction
- Transaction Ref
- Message Ref
- Batch Ref
- Related Ref
- BIC code
- Message Type
- Amount
- Currency
- Priority
- Status
- Match Score
- Risk Score
- Jurisdiction
- Overdue
  - From Date
  - To Date
- Ordering Party A/c No
- Ordering party name
- Beneficiary Party A/c No
- Beneficiary party name
- Creditor Account
- Creditor Name
- Debtor Name
- Debtor Account
- Requested Execution Date
  - From Date



- To Date
- Sender
- Receiver
- Domain
- Alert Type
- Standard Comment
- Case ID
- Count of WL Record IDs
- Count of
- Is Bulk Actioned?
- Watchlist ID
- Is Wire Stripping Alert?

#### 4.4.1.2 **Sorting the Alerts**

You can use the sort filters option available on the field names in the list to filter the alerts based on the sort order. To sort the alerts, use the following methods:

- Select the sort icon available on the field names.
- Right click on the field names and select **Sort Ascending** or **Sort Descending** options from the list.

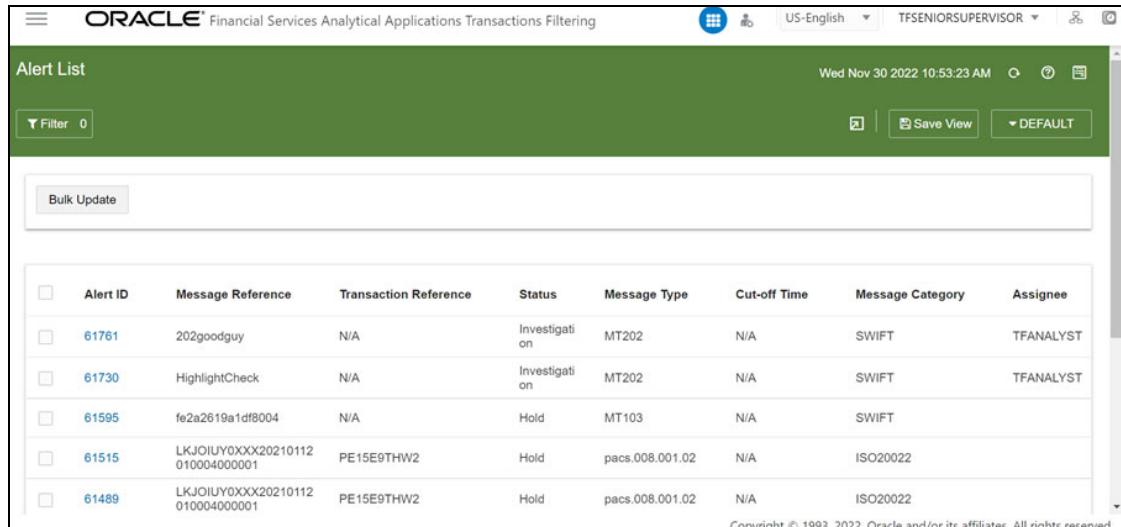
#### 4.4.1.3 **Updating the Alerts (Bulk Update)**

**NOTE** The Senior Supervisor only can **Bulk Update** the alerts on the Alerts List page.

You can bulk update the alerts from the list. To bulk update the alerts, follow these steps:

1. Select one or more alerts and click **Bulk Update**. The **Bulk Update** window is displayed.
2. Provide the details for the following fields, and the alerts get updated based on the below action performed:
  - Due Date Time
  - Priority
  - Assignee
3. Click **Save**. The details related to the bulk actions will be added to the Audit History of each alert.

Figure 16: Alert List Page- Bulk Update

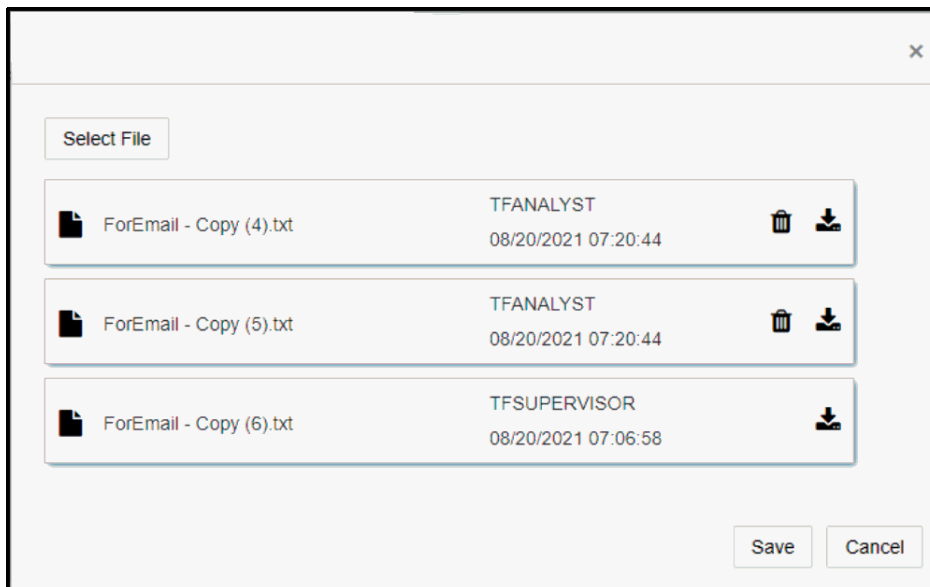


#### 4.4.1.4 Attaching a File to an Alert (Analyst/Supervisor/Senior Supervisor)

You can also attach a file to any alert. Only user with Analyst, Supervisor or Senior Supervisor role can perform this action.

Reviewer can download and view the attachment uploaded by other users in the alert but cannot attach a file to an alert.

Figure 17: Add Attachments



To attach a file to an alert, follow these steps:

1. Select the alert from the list. The **Attachment** option is displayed.
2. Click **Attachment**. The **Attachment** window is displayed.
3. Click **Select Files** to select the files.
4. Click **save**. The attachments are added to the list.
5. Click **Delete** icon next to the Attachment name to delete any of the attachments.

6. Click **Ok** to confirm. The file will be marked to delete. Click **Save** to delete the file.
7. Click **Download** icon next to the **Delete** icon to download the attachment.

**NOTE**

The maximum allowed size for the attachment is 9 MB and The attachments uploaded by other users cannot be deleted.

#### 4.4.1.5 Customizing the Field Columns

You can customizing your field columns in the Alert list as per your requirement. To Customize the field columns follow these steps:

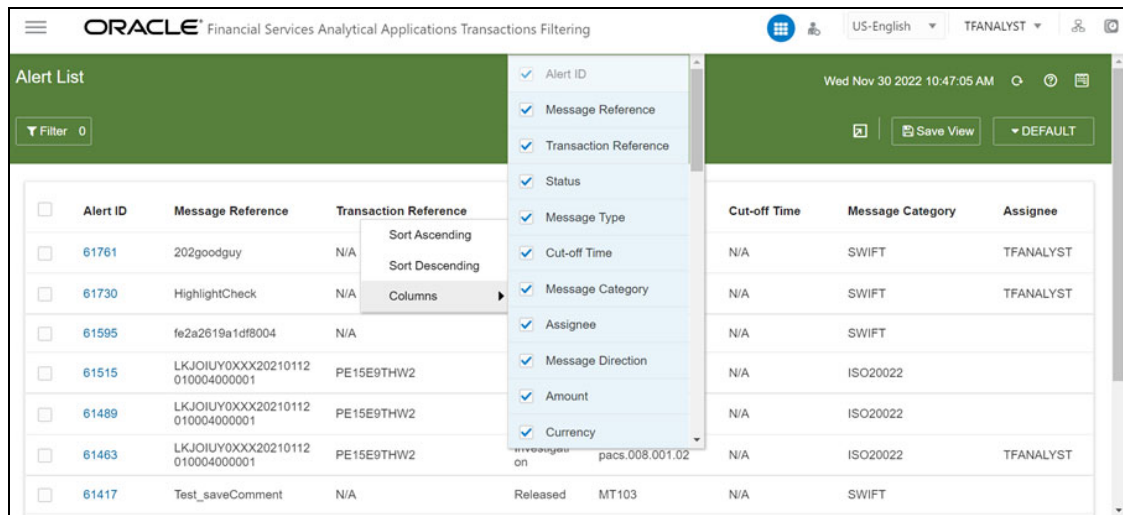
1. Select and right click the alert list fields names. The **Column** field option is displayed.
2. Click and Expand the **Column** field. All the Column names are listed.
3. Select and deselect the column name from the list to customize the field column of the Alert list page.

Using the **Columns** menu you can customize the following optional fields:

- Message Reference
- Transaction Reference
- Status
- Message Type
- Cut-off Time
- Message Category
- Assignee
- Message Direction
- Amount
- Currency
- Priority
- Last Updated Date Time
- Due Date Time
- Match Score
- Risk Score
- Alert Created Date
- Received Date Time
- Batch Reference
- Watchlist ID
- Decision
- Comments
- Standard Comments
- Domain
- Jurisdiction

- Ordering Party A/c No
- Ordering Party name
- Beneficiary Party A/c No
- Beneficiary party Name
- Creditor Account
- Creditor Name
- Debtor Name
- Debtor Account
- Requested Execution Date
- Sender
- Receiver
- Alert Type
- Related Reference
- BIC Code
- Is wire Stripping Alert?
- Count of WL Record IDs
- Count of
- Is Bulk Actioned?
- Resolution Comment

**Figure 18: Column field**



#### 4.4.1.6 Reordering the Columns

You can reorder the column as per the priority and requirement. To reorder the column, click and select the column, drag, and drop in the required order.

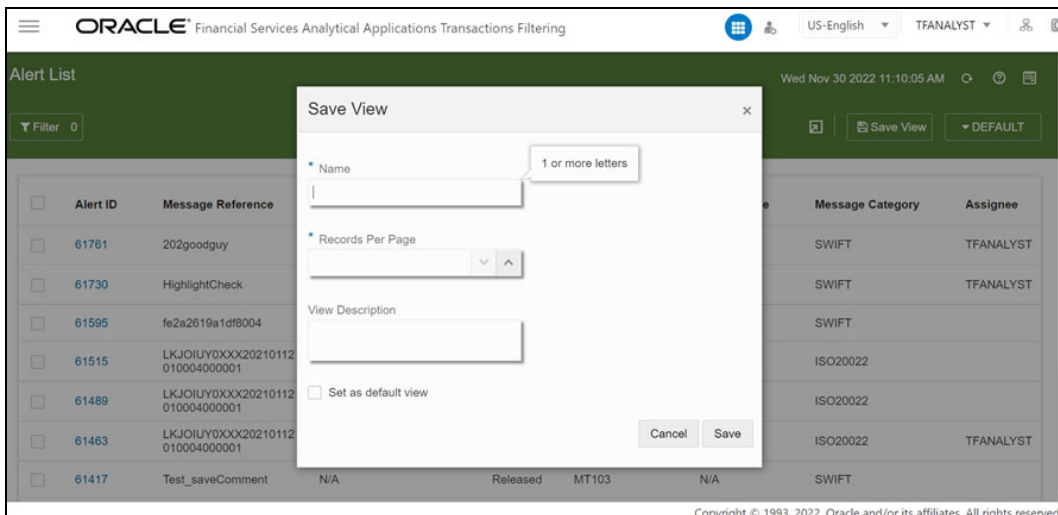
#### 4.4.1.7 Saving the View

You can add the Customized View to the Views List by saving it. To save and add the customized view, follow these steps:

1. Click **Save View** field after customizing the **Alert List** page with the required columns and properties. The **Save View** window is displayed.
2. Enter the name of the view in mandatory **Name** Field.
3. Select the mandatory **Records Per Page** value.
4. Enter the description in the **View Description** field.
5. To set the current view as the default view click **Set as default view** check box.
6. Click **Save**.


You can find the saved views list from the **Views** menu by selecting the **DEFAULT** option next to the **Save View** button. You can also use the Search bar in the **View** window to search for the views.

**Figure 19: Save View Window**







### 4.4.1.8 Managing Views

You can edit, delete or set as default the saved Views. To manage the views, follow these steps:

1. Select the **DEFAULT** button. The **Views** window is displayed.
2. Use the Search bar to search for the views and select to apply or click the **View All** button in the right corner to view the complete list of available views. The **Manage Views** window appears. You can view all the list of user created views with default and closed Alerts views which are system default views in the **Manage Views** window.
3. To edit, delete or set as default, select the view from the list and click the bullet option  icon and select the required action from the drop down.

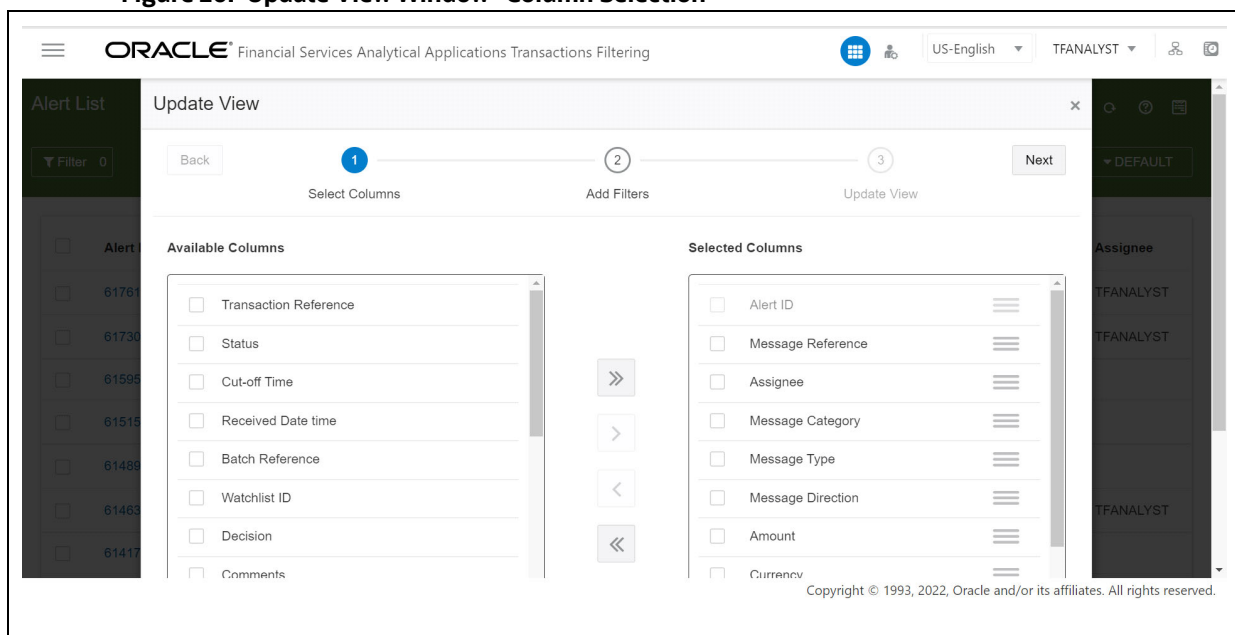
To edit the View follow these steps:

- a. Click **Edit**. The **Update View** window displays.
- b. To add new column to the View or delete the column from the View, select the required column from the **Available Column** list or **Selected Column** list and use the following icon to move columns:

- Use  icon to move all Columns from the **Available Columns** list to the **Selected Columns** list to add new columns
- Use  icon to move the selected Columns from the **Available Columns** list to the **Selected Columns** list to add new columns
- Use  icon to move the selected Columns from the **Selected Columns** list to the **Available Columns** list to delete the columns
- Use  icon to move All Columns except Alert ID from **Selected Columns** list to the **Available Columns** list to delete the columns

c. Click **Next** for **Add Filters** page.

**Figure 20: Update View Window- Column Selection**



d. You can add or edit the required fields in the **Add Filter** page. Click **Next** for **Update View** page.

**NOTE**

Use the **Reset** option to reset all the filter values.

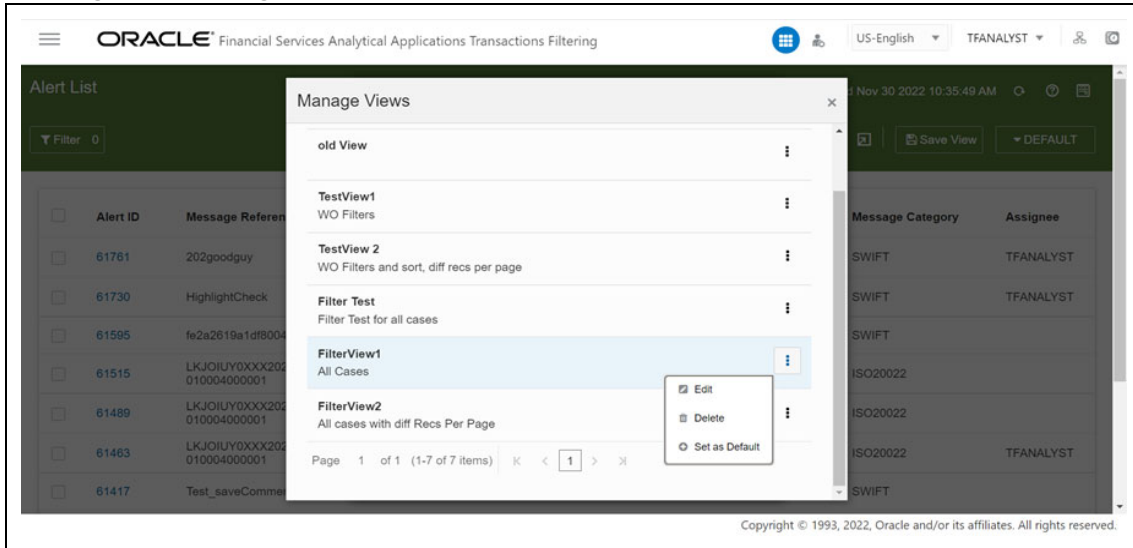
**Figure 21: Update View Window- Add Filters**

- e. You can edit **Name**, **View Description** and **Records Per Page** field in the **Update View** page. To set the current view as the default view click **Set as default view** check box.

**NOTE** **Name** and **Records Per Page** are mandatory fields.

- f. Click **Update**. A warning message is displayed.
- g. To overwrite the existing view click **Yes**. To cancel click **No**.
- To delete the View follow these steps:
- Click **Delete**. A warning message is displayed.
  - To delete the selected View click **Yes**. To cancel click **No**.
- To set the view as default view click **Set as Default**.
- To remove the applied default view click **Remove Default**.

Figure 22: Manage View Window




#### 4.4.1.9 Closed Alerts


To see the list of closed alerts that the user has access to, follow the below steps:

1. Click the **DEFAULT** button from the **Alert List** window. The **Views** window is displayed.
2. Click **Closed Alerts**. Closed alerts are displayed.

If you want to go back to the previous screen, click on **Closed Alerts button** select **DEFAULT** from the list.

#### 4.4.1.10 Exporting the Alerts from the List

To export one or more alerts from the list, select the alerts from the list and then click the **Export**  icon.

To export the entire alert list, click the **Export**  icon.

An **Excel** file will be downloaded with the alert list details based on the selected View.

#### 4.4.1.11 Reload the Grid

In the top right corner, click the **Reload**  icon to reload the alert list details.

#### 4.4.1.12 Bulk Action

You can take bulk action against alerts by selecting multiple alerts from the list. To take bulk action on the alerts, follow these steps:

1. Select an alert or multiple alerts from the list. The **Bulk Action** button is displayed.



2. Click the **Bulk Action** button. The Bulk Action window is displayed.

**NOTE** A Warning message popup is displayed with the list of selected alert IDs in the following scenarios:

- If the selected alert IDs have any pending .
- If any alert is locked by other users.

Click **Yes** to continue or **No** to cancel. If you click **Yes**, Alert ID locked by other users will be filtered, and the Bulk Action window will be displayed.

**NOTE** The **Bulk Action** window will not be displayed if no common actions are available for selected alerts.

3. From the **Bulk Action** window, select the decision. The decisions common to all the selected alerts are only displayed in the list. Selecting the decision is a mandatory field. You can configure the alert decision to be displayed for the bulk action for the alerts. For more information on configuring alert decisions, see [OFS Transaction Filtering Administration Guide](#).
4. Select one or more Standard Comments from the drop-down list in the Standard Comments section. It is mandatory to provide a standard comment or a free text comment.
5. In the Comments section, enter your comments and click **Save**. A warning message is displayed.

**NOTE** A Warning message popup is displayed in the following scenarios:

- Close the event as **Block** if all the are marked as **Clean**.
- Close the event as **Release** if any one of the event is marked as **suspicious**.

You can review the alerts and change the event status for bulk action against these alert IDs or click Yes to complete bulk action for the remainder of the alert.

6. Click **Save** to save the decision or click **Cancel** to cancel the decision.

## 4.4.2 Field Descriptions

[Table 3](#) provides the Field descriptions for Alert List

**Table 3: Field descriptions for Alert List**

Field	Description
Alert ID	Displays the unique Identification Number of the Alert.
Alert Created Date	Displays the Date the alert was created.
Primary Name	Displays the Primary Name of the customer or external entity.
Status	Displays the status of the alert.
Priority	Displays the priority of the alert.
Alert Type	Displays the alert type details.
Assignee	Displays the alert assignee name.
Due Date	Displays the due date of the alert.
Match Score	Displays the Match Score value of the alert.
Risk Score	Displays the Risk Score value of the alert.
Customer ID	Displays the customer identification number of the alert.
Decision	Displays the decision details on the alert.
Comments	Displays the comments provided for the alert.
Standard Comments	Displays the predefined comments provided for the alert.
Domain	Displays the domain value of the alert.
Jurisdiction	Displays the Jurisdiction of the alert belongs to.
From Date	Displays the name of the user who sent the alert.
To Date	Displays the name of the user the alert was sent.
Created Date Range	Displays the date range value of the alert.
Message Reference	Displays the message reference details.
Transaction Reference	Displays the transaction reference details.
Message Type	Displays the message type details.
Message Category	Displays the message category details.
Message Direction	Displays the message direction details.
Amount	Displays the transaction amount value details.
Currency	Displays the currency value.
Last Updated Date Time	Displays the date and time when the alert was last updated.
Due Date Time	Displays the due date value of the alert.
Received Date time	Displays the date the alert was received.
Batch Reference	Displays the reference number of the batch.
Watchlist ID	Displays the unique id assigned to batch with country code.
Decision	Displays the decision details of the alert.
Comments	Displays the comments provided for the alert.
Domain	Displays the Business domain of the alert.
Ordering Party A/c No	Displays the Ordering Party A/c No details.
Ordering Party Name	Displays the Ordering Party Name.
Beneficiary Party A/c No.	Displays the Beneficiary Party A/c No details.
Beneficiary Party Name	Displays the Beneficiary Party Name.
Creditor Name	Displays the Creditor Name of the alert.
Debtor Name	Displays the Debtor Name.
Debtor Account	Displays the Debtor Account details.
Requested Execution Date	Displays the Requested Execution Date.
Sender	Displays the sender name of the alert.
Receiver	Displays the Receiver name of the alert.
Creditor Account	Displays the creditor account details.
Related Reference	Displays the related reference details.

Field	Description
BIC Code	Displays the Bank Identifier Code.
Is wire Stripping Alert?	Displays, is the alert wire stripping alert or not (Yes/No).
Count of WL Record IDs	Displays the count of watchlist IDs
Count of	Displays the count of .
Is Bulk Actioned?	Displays whether the alert bulk actioned or not (Yes/No).
Resolution Comment	Displays the free text comment by user based on analysis

## 4.5 Alert Details

### 4.5.1 Analyzing the Alert

At a time, only one user can perform the actions on an event. Suppose the Analyst performs any action on an event in the alert. In that case, the alert will be locked to that specific user and cannot be edited by the Supervisor or vice-versa. The alert will be unlocked automatically when the user completes his actions and moves to any other alert.

The Reviewer can view the Alert Details page and can perform the following functions in an Alert Details page:

- Download attachments uploaded by other users
- See the actions taken by other users
- Perform the actions such as print pdf, view audit history and view watchlist details.

You can configure the functionality assigned to user group in the Alert Details page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups see the [OFS Transaction Filtering Administration Guide](#).

The Analyst/Supervisor works on the alert by observing its details. Click on the **Alert ID** to see the alert details in the following sections on the alert details page:

- Alert Summary Section
- - Match Summary
  - Risk Assessment
- Message Details
  - Raw Message
  - Structured Message
  - Additional Details
- WatchList Summary
- Alert Decision
- Audit History
- Related Alerts

**Figure 23: Alert Details**

**Alert Summary**

Message Type	MT101	Message Reference		Amount	11100	Assignee	TFANALYST	
Message Direction	INBOUND	Transaction Reference	201511050000001	Currency	USD	Decision	Investigation	
Message Category	SWIFT	Batch Reference	N/A	Jurisdiction	All	Comments		98 Match Score
Created Date	03/03/2023 12:55:42	Related Reference	N/A	Business Domain	All	Attachments		98 Risk Score
Cutoff Time	N/A	Due Date Time	N/A	Case ID		Alert Type	Blocking	Investigation
Is Wire Stripping Alert	No							TestNew

**Events**

Event Id	Matched Type	Country and City	Matched List	Matched Sub-list	Status	Blacklisted Country Reference Data	Match Score
69317	[C0011]Exact country Code	UA			Pending	N/A	98
69315							98

**Message Details**

Raw Message: [1:F01MORKUAJAUXXX0000000000]

Structured Message: [2:O1011200010103DDDDGRABAXXX2221234560101031201N]

## 4.5.2 Analyzing the Wire Stripping Alert

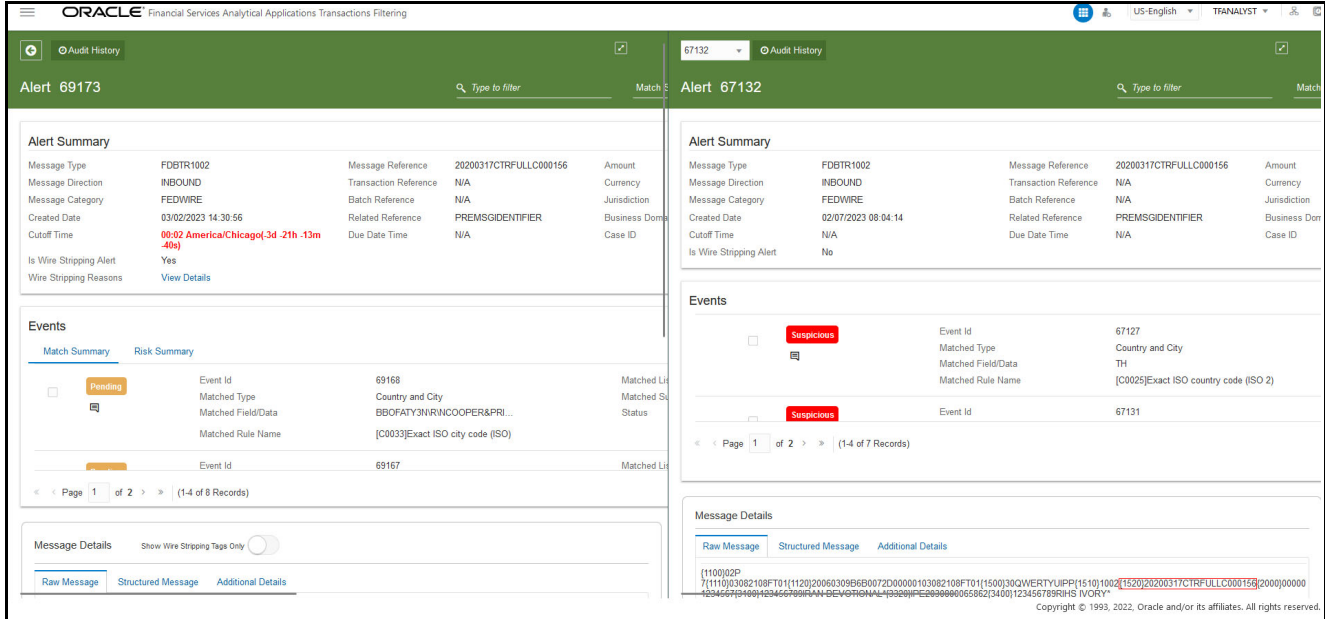
To detect potential wire-stripping activity, the message is compared with previous blocked alert (alert status can be configured) which is stored in the database with unique identifier code or Fingerprint status configured. Using this Fingerprint, identical wire transfers are identified with variable attributes and a look back period.

A WS Alert Details page is same as normal Alert details page except that WS Alert details page UI provides a side-by-side comparison between the potential wire-stripped alert and other matched alerts. For More Information Configuring WS Fingerprint, see [OFS Transaction Filtering Administration Guide](#).


**NOTE**

- WS Alerts are not created for messages which are before release 8.1.2.4.
- Wire Stripped alerts can be set to any alert status (The default OOB setting is to match with older blocked alerts).

Figure 24: Wire Stripping Alert Details




#### 4.5.2.1 Navigating to Previous and Next Alert

Use the **Previous**  icon in the top-left corner to navigate to the previous screen.

#### NOTE

Navigating to the **Next Alert** icon will be available only when you select **View Details** in Grid View from the **Queue Management** page to view the Alert Details.

Use the **Next**  icon in the top right corner to navigate to the next alert. The next will be loaded based on the sorting criteria given.

#### NOTE

Whenever you navigate to Alert Details page via Queue View All or View Top Priority Alerts, you can see both **Save and Next** and **Save and Close** buttons.

#### 4.5.2.2 Expanding and Minimizing WS Alert Details Screen

To Expand the alert details page click on the  icon. You can view the alert details page without the side-by-side comparison.

To Minimize the alert details page click on the  icon. You can view the alert details page with the side-by-side comparison


#### 4.5.2.3 Printing the Alert Details

To print the alert details, click the  icon. The PDF file will be downloaded with the alert details.

#### 4.5.2.4 Reload the Grid

In the top right corner, click the **Reload**  icon to reload the alert list details.

#### 4.5.2.5 Matched Alerts List Drop Down for WS Alert

The matched alert details page provides the list of all alerts that are matched against the new message. To view the list of matched alerts, click on the drop-down available at the top left corner of the matched alert details page. You can select the matched alerts from the drop-down and compare them to the WS alert. Matched alerts that are compared with WS alerts are identified using a  icon.

#### 4.5.2.6 Alert Summary Section

This section displays the alert details in the following components that are in the Analyst's/Supervisor's/Senior Supervisor's queue:

- Message Type
- Message Direction
- Message Category
- Created Date Time
- Cutoff Time
- Is Wire Stripping Alert
- Wire Stripping Reasons

**NOTE** Wire Stripping Reasons is only applicable to WS alert. Click **View Details** to view the Wire Stripping Reasons page.

- Message Reference
- Transaction Reference
- Batch Reference
- Related Reference
- Jurisdiction
- Business Domain
- Due Date Time
- Amount
- Currency
- Assignee
- Decision
- Comments
- Alert Type
- Attachments
- Match Score
- Risk Score

- Status
- Priority

**NOTE**

The **Case ID** field will be displayed only when the alert is escalated to ECM. Users with specific role permissions to ECM Case Type can click on the **Case ID** to view the case in ECM.

**Figure 25: Alert Summary Section**

Alert Summary											
Message Type	MT103	Message Reference	fe2a2619a1df8004	Amount	100	Assignee	TFANALYST				
Message Direction	INBOUND	Transaction Reference	N/A	Currency	USD	Decision	Investigation				
Message Category	SWIFT	Batch Reference	N/A	Jurisdiction	All	Comments					
Created Date	03/15/2023 05:32:47	Related Reference	N/A	Business Domain	All	Attachments		98	198	I	
Cutoff Time	N/A	Due Date Time	N/A	Case ID		Alert Type	Blocking	Match Score	Risk Score	Investigation	TestNew
Is Wire Stripping Alert	Yes										
Wire Stripping Reasons	<a href="#">View Details</a>										

**4.5.2.6.1 Wire Stripping Reasons**

Alert Summary will provide the Wire Stripping Reasons component view the reasons for the alert being detected as a Wire Stripping alert. To view the Wire Stripping Reasons follow the below steps:

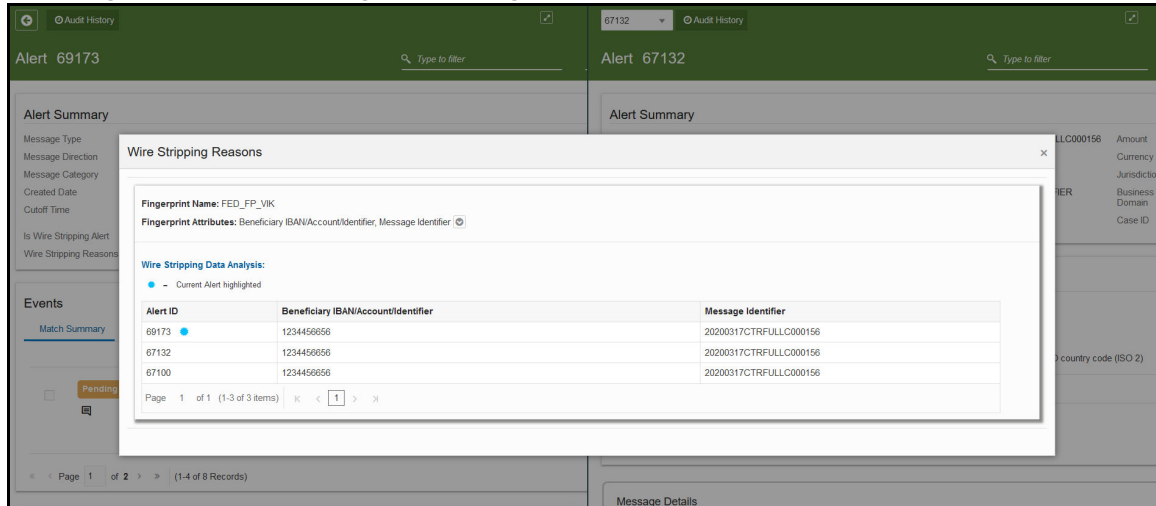
1. Click **View Details**. Wire Stripping Reasons page is displayed.

The Wire Stripping Reasons page provide the following information on the WS alert:

- Fingerprint name: Unique name of the finger print.
- Fingerprint Attributes: Attributes against which the alert is generated. Click on the icon for the complete attribute details.
- Wire Stripping Data Analysis: Provide the details of all the matched alerts and their attributes against which the WS alert is generated. In the WS Data Analysis table, icon identifies the current WS alert that is being investigated.

2. Click the **close** button.

Figure 26: Wire Stripping Reasons page





### 4.5.2.7 Events

This section displays the list of in the Event Summary and Risk Assessment tabs.

By default, the number of event records displayed per page in the event table is 5.

You can click the **Expand** button to expand the event page and view the event records (Records Per Page) simultaneously. Click on the **Collapse** button to collapse the event record. You can save the

preference by clicking the **Save Preference** (  ) icon and click the **Clear Preference** (  ) icon for the default view.

### 4.5.2.7.1 Match Summary

This section lists all the matches, if any, for a message. You can review all matches in this section before blocking/releasing a message.

The Event Summary tab contains the following components:

- Event ID
- Matched Type
- Matched Field /Data
- Matched Rule Name
- Matched List
- Matched Sub-list
- Status
- Match Score
- Edit Comments Icon

You can use the search filter in the top middle of the page to filter the in the alert with the Match Score criteria. Follow these steps to filter the :


- Enter the Match Score value in the Search Filter.



- From the Filter menu, select the **Match Score**.

Click on the **Select All** check box to select all the event records for the bulk update. Select All option is configurable. To enable and disable Select All option, see [Configuring the Application Level Parameters and Configuring Select All Option for the Table section in OFS Transaction Filtering Administration Guide](#).

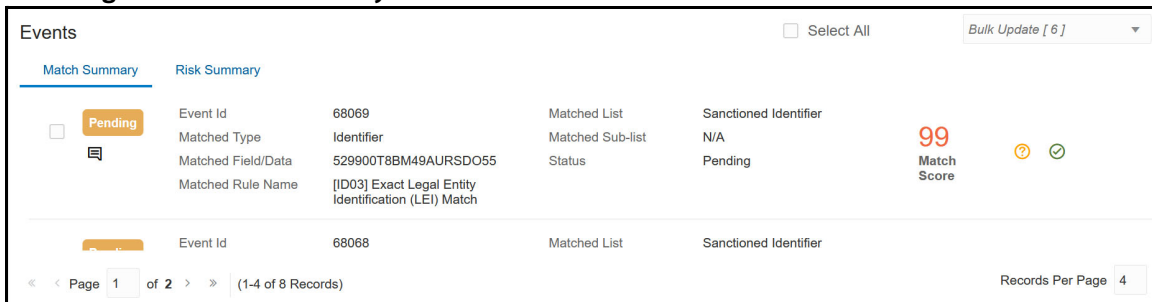
To Customize the number records displayed per page in the event table, enter the number in the **Records Per Page** entry box. The value must be between 4 and 100.

Click the Sort  icon to sort the search criteria in ascending and descending order.

**NOTE**

- The Senior Supervisor can change Assignee of the Alert.
- You cannot change the status of an Alert.



**Figure 27: Event Summary**



You can perform the following actions on the :


**4.5.2.7.1.1 Adding Comments to an Event**

You must enter comments for an alert. Follow these steps to add a comment:

1. In the section, click the **Comments**  icon. The *Add Comments* window is displayed.
2. In the *Standard Comments* section, select one or more Standard Comments from the drop-down list.
3. In the Comments section, enter your comments and click **Save**. The Comment details are added to the **Audit History** of that alert. For more information, see **Audit History**.
4. Click the **Comments**  icon in an Event to edit a comment and click **Save**.


**4.5.2.7.1.2 Adding Suspicious Status to an Event**

If the Analyst/Supervisor identifies the event as suspicious, he can add the suspicious status to the event on the fly.

1. Click the **Suspicious**  button next to the Match Score. The *Add Comments* window is displayed.
2. Enter the comments and click **Save**. For more information, see [Adding comments to an Event](#).
3. If the event is marked as **Suspicious**, then the **Clean** button and **Add to Good Guy** will be disabled.

#### 4.5.2.7.1.3 Adding Clean Status to an Event

If the Analyst/Supervisor identifies the event as clean, he can add the clean status to the event on the fly.

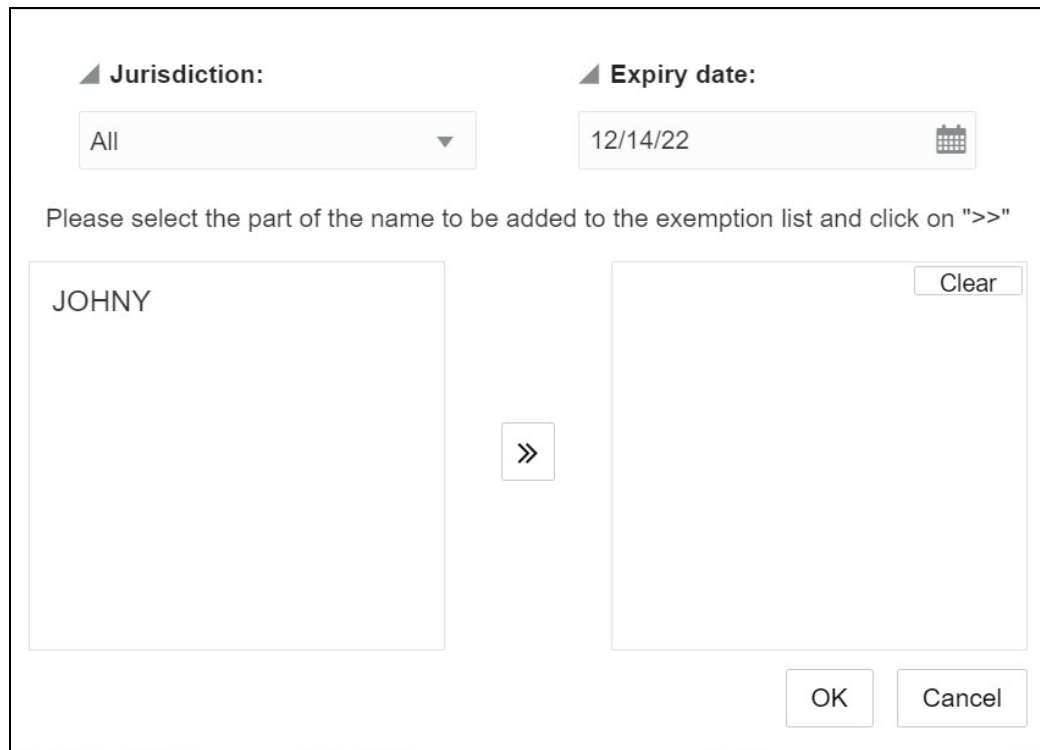
1. Click the **Clean**  button next to the Suspicious button. The *Add Comments* window is displayed.
2. Enter the comments and click **Save**. For more information, see [Adding comments to an Event](#).
3. If the event is marked as **Clean**, then the Clean button will be disabled, but **Suspicious** and **Add to Good Guy** buttons will be enabled.

#### 4.5.2.7.1.4 Good Guy Matching

The Event Summary section can add a record to the FCC\_WHITELIST table using the Add to Good Guy button. This button is initially green, and the color changes to gray after the record is added to the watch list table.

After you receive the record, click **Add to Good Guy**  to open a pop-up window.

**Figure 28: Good Guy Pop-up Window**



For Narrative matched type, only for individual and entity matches, the good guy button will be enabled. From the good guy window we can select jurisdiction and expiry date. Select the full/partial text from the left panel and click on the ">>" button to request the selection to be added to the exemption list.

Select the Jurisdiction and Expiry date for the record. Select the part of name to be added to exemption list and click on button and click **OK**. The record status or alert changes from Assigned (**A**) to Pending approval (**P**).

**NOTE** You can click on clear button to clear the selected name.

After you click **OK**, the message is sent to the Supervisor for review. An orange tick appears next to the **Clean** status, and the Add to Good Guy button remains green, as shown in the above image.

#### 4.5.2.7.1.5 Bulk Update the

You can bulk update the status of the in the alert. Follow these steps to Bulk update the status:

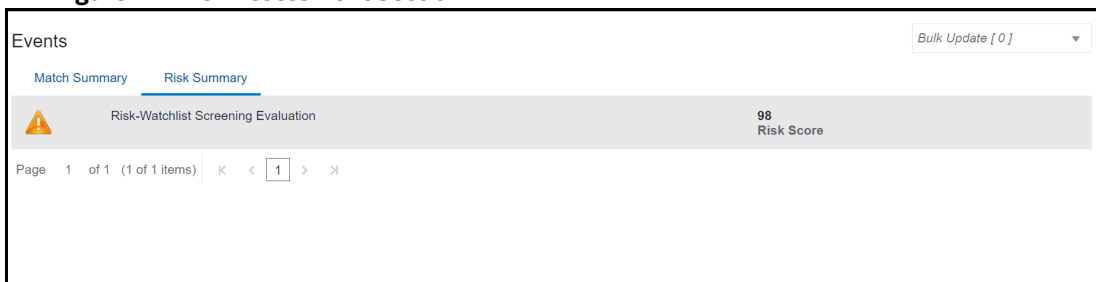
1. In the section, select one or more or click **Select All** check box.
2. In the top right corner of the section, select the **Bulk Update** drop-down list and then select **Clean/Suspicious** status. The Add Comments window is displayed.
3. Enter the comments and click **Save**. For more information, see [Adding Comments to an Event](#).
4. The status of the event will be updated. The Decision and Comment are added to the **Audit History** of that alert.

#### 4.5.2.7.2 Risk Summary

To view the Risk Assessment section, select the **Risk Summary** tab. This section lists all the risk rules and associated risk scores for a message. Click on a risk rule to view the corresponding risk details. See the Configuring Rules in the IPE chapter in the [OFS Transaction Filtering Administration Guide](#) for information on the risk rules.

The following image displays an example:

**Figure 29: Risk Assessment Section**



You can use the search filter in the top middle of the page to filter the Event Summary and Risk Assessment lists. Enter the search term in the search box to filter the list. Select the criterion as **Match**

**Score/Risk Score**. Click the **Sort By**  to filter the data in ascending and descending order.

#### 4.5.2.8 Message Details

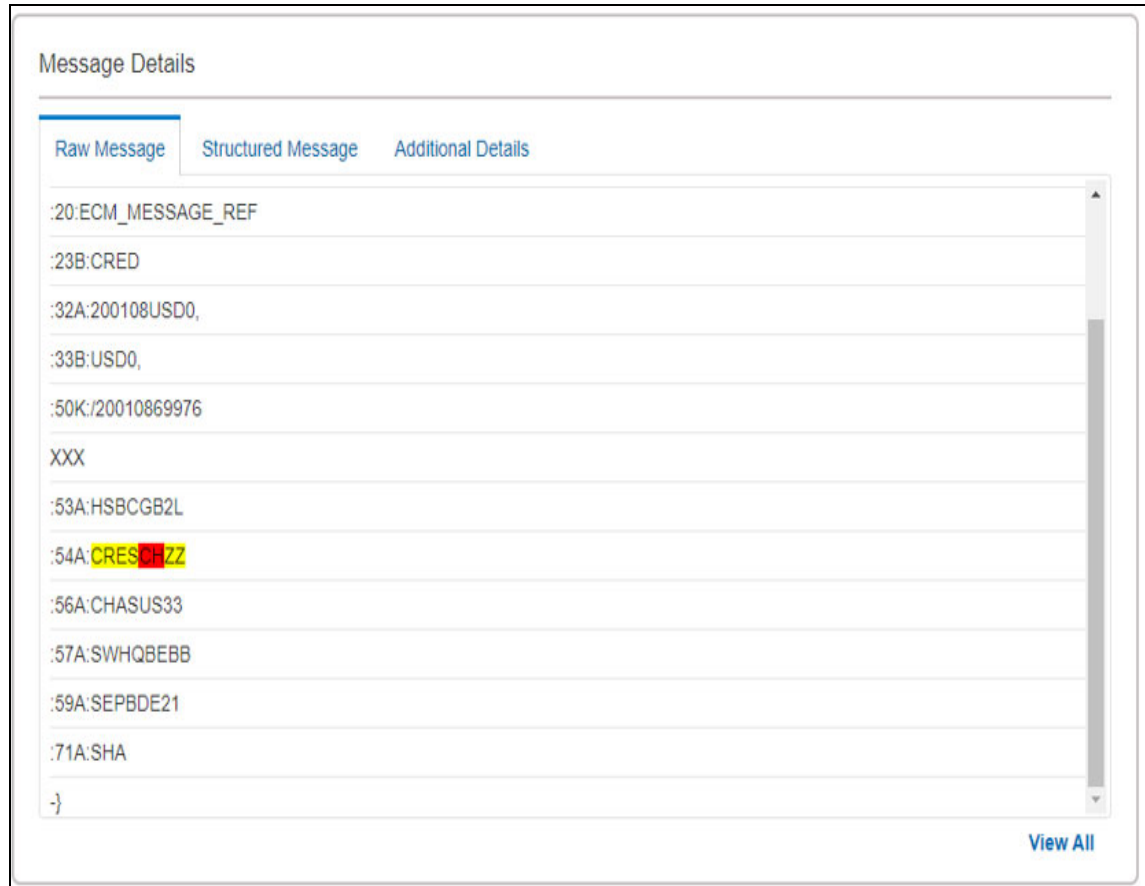
This section contains three tabs.

- **Raw Message:**

The following image shows the different fields available for the SWIFT message in a raw format. The suspicious matched data is highlighted in yellow.

To configure the parameters to highlight the matched data, See [Configuring the Parameters for highlighting the matched data in the OFS Transaction Filtering Administration Guide](#).

**Figure 30: Raw Message Format for SWIFT**



The following image shows the different fields available for the ISO20022 message in a raw format. The suspicious/ matched data is highlighted in yellow.

**Figure 31: Raw Message Format for ISO20022**

Message Details

---

Raw Message
Structured Message
Additional Details

```

<PstlAdr>
<Ctry>NL</Ctry>
<AdrLine>EOVMOVMSLA 6E</AdrLine>
<AdrLine>8765 GR EOWEMCK</AdrLine>
</PstlAdr>
<Id>
<OrgId>
<Othr>
<Id>980227001</Id>
<SchmeNm>
          
```

[View All](#)

To download the XML file, click **Download**. Click **View All** to see the complete list of Message Details.

- **Structured Message:**

The following image shows the structured form of the message. This displays the important fields in a key-value format.

**Figure 32: Structured Message Format for SWIFT**

Message Details		
Raw Message	Structured Message	Additional Details
Sender:	IRVTUS3NXXX	
Receiver:	ICBCVNVXXXX	
Requested Execution Date:	2019-02-28 00:00:00.0	
Originator Identifier:	/950800362384	
Originator Address:	1/MANSOUR, Yasser Daoud 2/CUBA 2/NORTH KOREA 3/IRAN	
Beneficiary Identifier:	/950800362384	
Originator Country:	SY	
Destination Country:	VN	

[View All](#)

The Structured Message format for ISO20022 has **Header Information** and **Transaction Information**.

- **Header Information:** This section displays the transaction information, such as the number of transactions, total transaction amount, the user who initiated the transaction, the date on which the batch was executed, and the country from where the amount originated.
- **Transaction Information:** This section displays the transaction ID, the destination country of the transaction, and the details of the user who received the transaction amount. Click **View All** to see the complete list of Message Details.
- **Additional Details:**  
To view the transaction XPath of the XML file, click **Additional Details**. For more information, see the *Configuring the ISO20022 Parameters* chapter in the *OFS Transaction Filtering Administration Guide*.

**Figure 33: Additional Details**

Message Details

Raw Message   Structured Message   **Additional Details**

	Field Name
▲ Basic Header Block	
Block Identifier	1
Application Identifier	F
Service Identifier	01
LT Identifier	ICBCVNVXAXXX
Session Number	0037
Sequence Number (ISN or OSN)	827144
▶ Application Header Block	
▶ User Header Block	
▶ Text Block	
▶ Trailer Block	

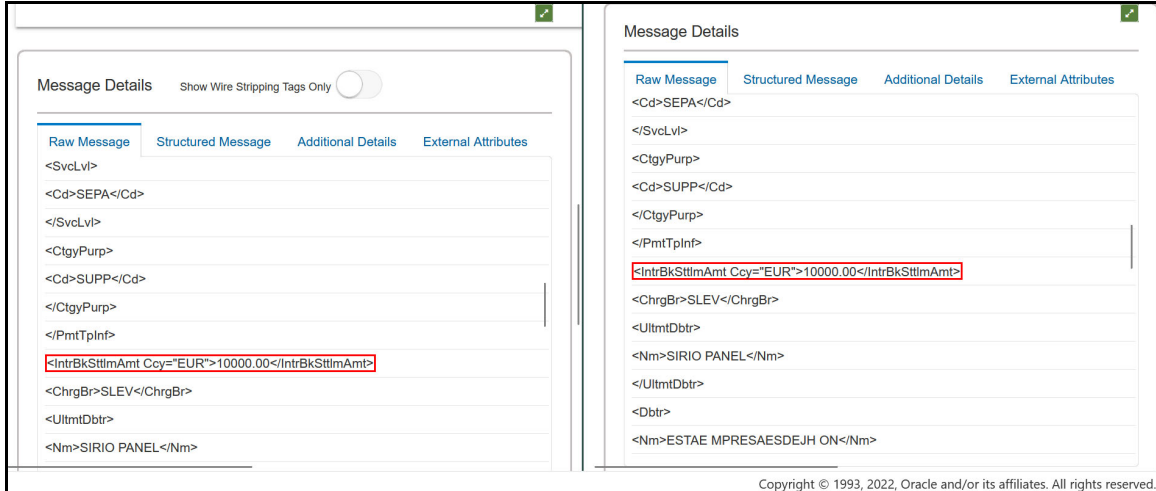
[View All](#)

Expand each category to view its additional details. Click **View All** to see the complete list of Message Details.

#### 4.5.2.9 Message Details for WS Alert

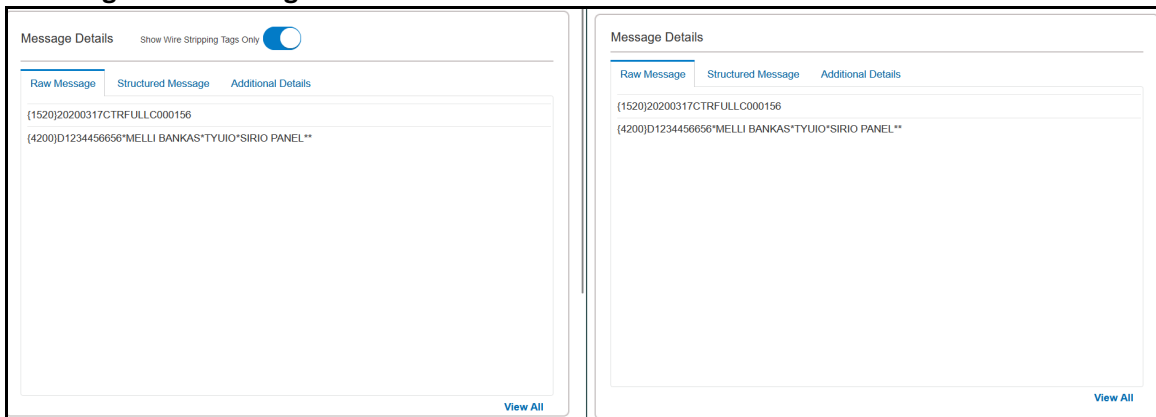
The message Details section in WS Alert provides an additional option to filter and display Wire Stripping tags only. For the WS alert, in the raw the message, the wire-stripped tags will be highlighted in a red box.

**Figure 34: Message Details Section for WS Alert**



In the Message details screen the Raw Message will highlight the potential wire-stripped tags. To filter the raw message to show the fingerprint matched data, click on the **Show Wire Stripping Tags Only** toggle button.

**Figure 35: Message Details- WS filtered**



#### 4.5.2.10 WatchList Summary

This section displays the watch list details that match with the alert data. This helps you analyze the alert and decide if it has to be passed or not. A unique Record ID is assigned to every watch list/sanctioned record. See the Watch Lists appendix in the *OFS Transaction Filtering Administration Guide* for information on the different watch lists used. The suspicious/ matched data is highlighted in yellow.

You can also view the history of matches for a watch list record ID in the **Related Alerts**. The List History displays the number of hits for a watch list record ID over a specified lookback period. You can select the lookback period from the **List History** drop-down list.



**Figure 36: Watchlist Details Section**

WatchList Summary		List History	Last 1 year ▼	📌 Related Alerts 4
Record ID	3			
Country	SYRIA			
ISO Country Code	SY			
Country Synonyms	SYRIAN ARAB REPUBLIC			
Data Source	OFAC (Office of Foreign Assets Control)			

[View All](#)

To see a detailed view of all hits, click **Related Alerts**. A **Related Alerts window appears**. For more information, see [Related Alerts](#).

The details displayed in the Watchlist Details section depend on the type of sanctioned data found. Click the **View All** button to see the complete Watchlist record with the following components:

If a match is found for a sanctioned Name or sanctioned Name and Address, then the following details are displayed:

- For an Individual:
  - Record ID
  - Name
  - Original Script Name
  - Alias Type
  - Alias Names
  - Primary Name
  - Address
  - Alias Address

- Type
- Gender
- Date Of Birth
- Town Of Birth
- City Of Birth
- State Of Birth
- Place Of Birth Country
- Country Of Birth
- Nationality
- Title
- Designation
- Language
- Passport Details
- Passport Type
- Passport Number
- Passport Issuing City
- Passport Issuing Country
- Passport Date Of Issue
- Passport Note
- NI Details
- National ID
- NI Type
- NI Issuing City
- NI Issuing Country
- NI Date Of Issue
- NI Note
- Other Information
- Residency Country
- Other Information
- Listed On

- Last Updated
- Record Type
- Program
- Reference Number
- Legal Basis
- Search Hyperlink
- For an Entity:
  - Record ID
  - Name
  - Original Script Name
  - Alias Type
  - Alias Names
  - Primary Name
  - Address
  - Alias Address
  - Other Information
  - Type
  - Date Of Birth
  - Place Of Birth
  - Passport Details
  - Nationality
  - Programme
  - Language
  - Legal Basis
  - Listed On
  - Last Updated
  - Program
  - Title
  - Call Sign
  - Vessel Type
  - Tonnage

- GRT
- Vessel Flag
- Vessel Owner
- Vessel Details
- Country of Registration
- Country of Operation
- Registration Number
- Search Hyperlink

If a match is found for a sanctioned Bank Identifier Code (BIC), then the following details are displayed:

- Record ID
- BIC
- BIC Details
- Data Source

If a match is found for a sanctioned Country, then the following details are displayed:

- Record ID
- Country
- ISO Country Code
- Country Synonyms
- Data Source

If a match is found for a sanctioned City, then the following details are displayed:

- Record ID
- Country
- City
- ISO City Code
- City Synonyms
- Data Source
- Country ISO Code

If a match is found for a sanctioned Stop Keywords, then the following details are displayed:

- Record ID
- StopKeyWords

#### 4.5.2.11 Risk Indicator Details

---

**NOTE** This section is only available when you select the Risk Summary tab.

**Figure 37: Risk Indicator Details**

Risk Indicator Details	
Screening Rule	[C0025]Exact ISO country code (ISO 2)
Screening Score	94
Screening Rule	[[001U]Exact name only (Conflict)
Screening Score	70
Screening Rule	[[001U]Exact name only (Conflict)
Screening Score	70

This section displays the risk indicator details data related to the Risk Assessment section.

You can also view the history of the Risk List for a selected risk in the **Related Alerts**. The List History displays the number of hits for risk details over a specified lookback period. You can select the lookback period from the **List History** drop-down list.

To see a detailed view of all hits, click **Related Alerts**. A Related Alerts window appears. For more information, see **Related Alerts**.

#### 4.5.2.12 Wire Stripping Validation

The wire Stripping Validation section provides information on the matched alert that is not viewed for comparison. You cannot take any action on the WS alert unless you validate all the matched alerts against the WS alert that is being investigated.

You can enable or disable Wire Stripping Validation. To Configure the WS Validation, see Configuring Wire Stripping Validation for WS Alert Details Screen section in [OFS Transaction Filtering Administration Guide](#).

**NOTE** By default, Wire Stripping Validation is enabled.

#### 4.5.2.13 Alerts Decision

The actions for each role can be configurable as per the requirement. For more information, see the [OFS Transaction Filtering Administration Guide](#).

---

**NOTE** A Reviewer user cannot access the alert decision.

The Analyst has the following actions available for a standard flow:

- Promote to Case

---

**NOTE** The Promote to Case action is available to the analyst when ECM L2 is enabled.

- Block
- Release
- Escalate

The Analyst has the following actions available for a four-eyes flow:

- Promote to Case

---

**NOTE** The Promote to Case action is available to the analyst when ECM L2 is enabled.

- Recommend to Block
- Recommend to Release
- Escalate

If a transaction is in the Auto Release (AR) status, the following actions are available:

- Escalate
- False Positive
- Confirmed Match

You must also add a comment for any alert. For more information, see [Adding Comments to an Event](#)

You can also attach a file to any alert. Select an alert from the list and follow these steps:

1. Click **Add Attachment**. The *Attachment* window is displayed.
2. Click **Select Files** to select the files.
3. Click **Save**. The attachments are added to the list.
4. If you want to delete any attachments, click the **Delete** icon next to the Attachment name.
5. Click **Ok** to confirm. The file will be marked to delete. Click **Save** to delete the file.

---

**NOTE** The maximum allowed size for the attachment is 9MB, and the Attachments uploaded by other users cannot be deleted.

If the Analyst escalates the alert to the Supervisor, the Supervisor has the following actions available for a standard flow:

- Block
- Release

If the Analyst escalates the alert to the Supervisor, the Supervisor has the following actions available for a four-eyes flow:

- Block
- Release
- Reject

#### 4.5.2.13.1 **Recommending to Block an Alert**

This action is only available to the Analyst and Senior Supervisor. You can block the alert if you find suspicious data. Follow these steps:

1. From the **Alert Decision** section, select the **Recommend to Block** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any, and click **Save and Close** or **Clear** to clear the attachment and details. The status of the alert changes to **BR** (Block Recommended).

#### 4.5.2.13.2 **Recommending to Release an Alert**

This action is only available to the Analyst and Senior Supervisor. You can release an alert if it is clean. Follow these steps:

1. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
2. Add the attachments, if any and, click **Save and Close** or **Clear** to clear the attachment and details. The status of the alert changes to **RR** (Release Recommended). This alert is called a **False Positive**.
3. In the Event Summary section, if any of the alerts' matches are marked as suspicious, then a pop-up window is displayed when you release the alert. Change the status to **Recommend to Block** or **Escalate**.

#### 4.5.2.13.3 **Escalating an Alert**

This action is only available to the Analyst and Senior Supervisor. You can escalate the alert to the Supervisor if you need further analysis and approval. Follow these steps:

1. From the **Alert Decision** section, select the **Escalate** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any and, click **Save and Close** or **Clear** to clear the attachment and details. The status of the alert changes to **E** (Escalated).

#### 4.5.2.13.4 **Blocking an Alert**

This action is only available to the Supervisor. You can block the alert if you find suspicious data. Follow these steps:

1. From the **Alert Decision** section, select the **Block** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.

3. Add the attachments, if any and click **Save and Close** or **Clear** to clear the attachment and details. The status of the alert changes to **B** (Blocked).

#### 4.5.2.13.5 Releasing an Alert

This action is only available to the Supervisor. You can release an alert if it is clean. Follow these steps:

1. From the **Alert Decision** section, select the **Release** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any, and click **Save and Close** or **Clear** to clear the attachment and details. The status of the alert changes to **R** (Released). This alert is called a **False Positive**.
4. In the **Event Summary** section, if any of the alerts' matches are marked as suspicious, then a pop-up window is displayed when you release the alert. Change the status to **Block** or **Escalate**.

#### 4.5.2.13.6 Rejecting an Alert

This action is available to the Supervisor. You can reject an alert if you think that the alert must be reanalyzed by the Analyst. Follow these steps:

1. From the **Alert Decision** section, select the **Reject** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any, and click **Save and Close** or **Clear** to clear the attachment and details.
4. When you reject an alert, it is assigned back to the Analyst.

#### 4.5.2.13.7 Promoting to case

This action is available to the Analyst when ECM L2 is enabled. Follow these steps:

1. From the **Alert Decision** section, select the **Promote to Case** button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any and, click **Save and Close** or **Clear** to clear the attachment and details.
4. When you select Promote to Case, a new case will be created in ECM for the same Alert for the next level analysis.

#### 4.5.2.13.8 Alert Statuses

The alerts that are displayed are in the following order for the Analyst and Supervisor users:

##### 4.5.2.13.8.1 Standard Flow For Analyst

- Hold
- Investigated
- Escalated
- Blocked



- Released

#### ***4.5.2.13.8.2 Standard Flow For Supervisor***

- Escalated
- Blocked
- Released
- Four-Eyes Flow For Analyst
- Hold
- Escalated
- Block Recommended
- Release Recommended
- Blocked
- Released
- Pending

#### ***4.5.2.13.8.3 Four-Eyes Flow For Supervisor***

- Escalated
- Block Recommended
- Release Recommended
- Blocked
- Released
- Pending

#### **4.5.2.14 Audit History**

The Audit History provides the match-level audit details on the alert. The details like decision taken, good guy details with comments, comments, bulk action details if taken, Alert level decision is taken, added attachments details, comments, and standard comments.

For Wire Stripping, when you compare the current alert against each matched alert, it will be added to the audit history of the content.

**Figure 38: Audit History**

Event ID	Comment	Comment Type	Action Details	Assignee User ID	Assignee User Name	Last Assignee Name
N/A	One of the events is a True Match	Alert Type	Blocked	N/A	N/A	TFANALYST
50333	N/A	Event Type	Suspicious	N/A	N/A	N/A
50334	N/A	Event Type	Suspicious	N/A	N/A	N/A
50335	N/A	Event Type	Suspicious	N/A	N/A	N/A
50336	N/A	Event Type	Suspicious	N/A	N/A	N/A
50337	N/A	Event Type	Suspicious	N/A	N/A	N/A
N/A	N/A	Alert Type	Investigation	TFANALYST	tfanalyst	N/A

The details are added to the **Audit History** in the following fields:

- Event ID
- Comment
- Comment Type
- Action Details
- Assignee User ID
- Assignee User Name
- Last Assignee Name
- Created Date
- Is Bulk Actioned?

You can use the search filter in the top middle of the page to filter the Audit History list. Enter the search term in the search box to filter the list.

Click the **Reload** icon next to the Last Modified Date Time to reload the Audit History list.

#### 4.5.2.14.1 Exporting the Alerts from the List

To export the Audit History list, click the **Export** icon in the top right corner. An **Excel** file will be downloaded with the Audit History list details.

#### 4.5.2.14.2 Field Descriptions

Table 4 provides the Field descriptions for Audit History.

**Table 4: Field descriptions for Audit History**

Fields	Description
Event ID	Displays the unique ID that was created for the event.
Comment	Displays the comments provided for the alert.
Comment Type	Displays the type of the comment details.
Action Details	Displays the type of action performed on the alert.
Assignee User ID	Displays the unique ID of the assignee.
Assignee User Name	Displays the name of the assignee user.
Last Assignee Name	Displays the last assignee user name.
Created Date	Displays the date the alert was created.

### 4.5.2.15 Related Alerts

This section displays the related alerts list. If two alerts are linked with two reference numbers, another message alert will be shown as related.

When the current case is 202COV message, its Transaction Reference no (Swift Field 21) is matched with Sender Reference (Swift Field 20) of 103 type case. These matched 103 message type cases are linked to the 202COV case.

By matching the BICs in Field 52A and 57A in 101 & 103, and the Field 32B with 33B in 101 & 103.

You can access the related alerts list from the *Watchlist Summary* and *Risk Indicator Details* window.

In the Watchlist Summary/Risk Indicator Details window, Select **Related Alerts** next to the **List History** menu.

**Figure 39: Related Alerts**

The screenshot shows a window titled 'Related Alerts' with a search bar and a table of data. The table has the following columns: Alert Id, Message Reference, Transaction Reference, Message Type, Message Category, Message Direction, Amount, and Currency. The data rows are as follows:

Alert Id	Message Reference	Transaction Reference	Message Type	Message Category	Message Direction	Amount	Currency
50338	priority2	N/A	MT202	SWIFT	OUTBOUND	222	EUR
51468	Block	N/A	MT202	SWIFT	OUTBOUND	222	EUR
51707	Blocked	N/A	MT101	SWIFT	INBOUND	11100	USD
51809	BlockedRecom22	N/A	MT103	SWIFT	INBOUND	143585	USD
50709	ggcheck3	N/A	MT202	SWIFT	OUTBOUND	222	EUR
50562	priority3	N/A	MT202	SWIFT	OUTBOUND	222	EUR
50841	SAITE.JA2	N/A	MT202	SWIFT	OUTBOUND	222	EUR
50899	Evaluatn1	N/A	MT101	SWIFT	INBOUND	11100	USD
50764	SAITE.JA	N/A	MT202	SWIFT	OUTBOUND	222	EUR

This section contains the following components:

- Alert ID
- Message Reference
- Transaction Reference
- Message Type
- Message Category
- Message Direction

- Amount
- Currency
- Priority
- Last Updated Date Time
- Due Date Time
- Match Score
- Risk Score
- Alert Created Dare

You can use the search filter in the top middle of the page to filter the Related Alerts list. Enter the search term in the search box to filter the list.

Click on the **Alert ID** to see the alert in a new window. Click the **Reload** icon next to the Last Modified Date Time to reload the Related Alerts list.

#### 4.5.2.15.1 Exporting the Alerts from the List

To export the Related Alerts list, click the **Export** icon in the top right corner. An **Excel** file will be downloaded with the Related Alerts list details.

#### 4.5.2.15.2 Field descriptions

Table 5 provides the Field descriptions for Related Alerts.

**Table 5: Field descriptions for Related Alerts**

Fields	Description
Alert ID	Displays the alert identification number.
Message Reference	Displays the message reference details.
Transaction Reference	Displays the transaction reference details.
Message Type	Displays the type of message.
Message Category	Displays the message category details.
Message Direction	Displays the message direction details.
Amount	Displays the transaction amount details.
Currency	Displays the type of currency value.
Priority	Displays the priority value of the alert.
Last Updated Date Time	Displays the last updated date-time value.
Due Date Time	Displays the due date the alert has to review.
Match Score	Displays the match score details.
Risk Score	Displays the risk score details.
Alert Created Date	Displays the date the alert was created.

### 4.5.3 Field Descriptions

Table 6 provides the Field descriptions for Alert Details.

**Table 6: Field descriptions for Alert Details**

Field	Description
Alert ID	Displays the unique Identification Number of the Alert.
Alert Created Date	Displays the Date the alert was created.
Primary Name	Displays the Primary Name of the Customer.
Status	Displays the status of the alert.
Priority	Displays the priority of the alert.
Alert Type	Displays the alert type details.
Assignee	Displays the alert assignee name.
Due Date	Displays the due date of the alert.
Match Score	Displays the Match Score value of the alert.
Risk Score	Displays the Risk Score value of the alert.
Customer ID	Displays the customer identification number of the alert.
Decision	Displays the decision details on the alert.
Comments	Displays the comments provided for the alert.
Standard Comments	Displays the predefined comments provided for the alert.
Domain	Displays the domain value of the alert.
Jurisdiction	Displays the Jurisdiction of the alert belongs to.
Customer/EE/Response ID	Displays the Customer/EE/Response ID details.
From Date	Displays the date the alert is from.
To Date	Displays the date the alert was sent to.
Created Date Range	Displays the date range value of the alert.
Message Reference	Displays the message reference details.
Transaction Reference	Displays the transaction reference details.
Message Type	Displays the message type details.
Message Category	Displays the message category details.
Message Direction	Displays the message direction details.
Amount	Displays the transaction amount value details.
Currency	Displays the currency value.
Last Updated Date Time	Displays the date and time when the alert was last updated.
Due Date Time	Displays the due date value of the alert.
Received Date time	Displays the date the alert was received.
Batch Reference	Displays the reference number of the batch.
Watchlist ID	Displays the unique id assigned to batch.
Decision	Displays the decision details of the alert.
Ordering Party A/c No	Displays the Ordering Party A/c No details.
Ordering Party Name	Displays the Ordering Party Name.
Beneficiary Party A/c No.	Displays the Beneficiary Party A/c No details.
Beneficiary Party Name	Displays the Beneficiary Party Name.
Creditor Name	Displays the Creditor Name of the alert.
Debtor Name	Displays the Debtor Name.
Debtor Account	Displays the Debtor Account details.
Requested Execution Date	Displays the Requested Execution Date.
Sender	Displays the sender name of the alert.

Field	Description
Receiver	Displays the Receiver name of the alert.

## **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.



