

Oracle Financial Services Transaction Filtering

User Guide

Release 8.0.8.2.0

September 2021

F22529-01

ORACLE
Financial Services

ORACLE

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

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

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

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

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

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

Revision No.	Revision Date	Change Log
8.0.8.2.15	April 2023	Added Reviewer user role information.
8.0.8.2.7	April 2022	Added the new section Auditing of a Good Guy and added a Note related to Good Guy Suppression at the end of the section Good Guy Summary Section .
8.0.8.2.2	November 2021	Updated the Grid View section with Queue Prioritization updates.
8.0.8.2.0	September 2021	Restructured the sections according to the re-designed Transaction Filtering Alert List User Interface and added the new Queue Management page details.
8.0.8.1.1	April 2021	New Search Filters: <ul style="list-style-type: none"> Added search criteria, overdue SLA, to filter alert SLAs based on their due date in the Investigation User Interface. For more information on the usage, see Alert Summary Section. New notification icon for overdue SLAs. For more information, see the Notification and Reporting Section.
8.0.8.1.5	December 2020	Automatically release clean messages: <ul style="list-style-type: none"> Clean messages which are false positives or confirmed matches must be automatically released. For more information, see Automatically Releasing Transactions.
8.0.8.1.0	August 2020	New Search Filters: <ul style="list-style-type: none"> Added two search criteria, business domain, and Jurisdiction, to filter alerts in the Investigation User Interface. For more information on the usage, see Alert Summary Section. View the RAW message format in the Investigation User Interface. For more information on the message format, see the Message and Audit Section. Any Analyst who logs in can now see all closed alerts. For more information on this feature, see Alert Summary Section. View the number of matches for a watch list record. For more information on this feature, see List Details.
8.0.8.0.0	May 2019	This is the first release of the document.

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

Table of Contents

1	Preface.....	6
1.1	Who Should Use This Guide.....	6
1.2	How this Guide is Organized.....	6
1.3	Related Documents.....	6
1.4	Conventions.....	7
2	About Transaction Filtering.....	8
2.1	Transaction Filtering Workflow.....	9
2.2	Features of Transaction Filtering.....	10
2.3	Score Matching Logic.....	10
2.4	User Roles and Actions.....	11
3	Getting Started.....	13
3.1	Accessing OFSAA Page.....	13
3.2	Managing OFSAA Page.....	14
3.2.1	Applications Tab.....	14
3.2.2	Changing the Application Password.....	14
3.2.3	Viewing the Application’s Copyright Information.....	15
3.3	Troubleshooting Your Display.....	16
3.3.1	Enabling JavaScript.....	16
3.3.2	Enabling Cookies.....	16
3.3.3	Enabling Temporary Internet Files.....	16
3.3.4	Enabling File Downloads.....	17
3.3.5	Setting Print Options.....	17
3.3.6	Enabling the Pop-Up Blocker.....	17
3.3.7	Setting Home Page Preferences.....	18
3.4	Logging in to the Transaction Filtering Application.....	18
4	Managing Transaction Filtering.....	20
4.1	Investigation User Interface Workflow.....	20
4.2	List Management.....	24
4.2.1	Good Guy Summary Section.....	24
4.2.2	List History Section.....	26
4.2.3	Match History.....	26
4.2.4	Approving or Rejecting Alerts.....	27
4.2.5	Watchlist Details.....	27

4.3	Queue Management.....	28
4.3.1	List View.....	28
4.3.2	Grid View.....	29
4.4	Alert List	32
4.4.1	Managing the Alerts.....	34
4.4.2	Field Descriptions	39
4.5	Alert Details	41
4.5.1	Analyzing the Alert.....	41
4.5.2	Field Descriptions	65

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

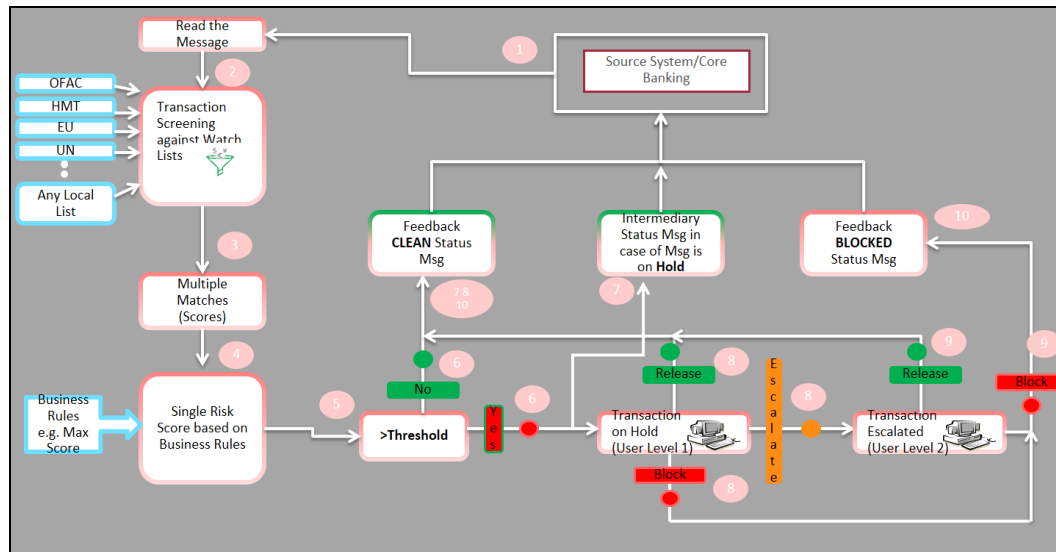
Transaction Filtering against government-regulated watch lists and internal watch lists is a key compliance requirement for financial institutions across the globe. At the turn of the century, Financial Institutions (FIs) were expected to identify customers either who were sanctioned or who lived in 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.

The 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 events 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 3: User Roles and Actions

Action	Reviewer	Analyst	Supervisor	Senior Supervisor	Queue Administrator
Queue Level					
Add					✓

Action	Reviewer	Analyst	Supervisor	Senior Supervisor	Queue Administrator
Edit					✓
Assign					✓
Delete					✓
Open		✓	✓	✓	
Alert Level					
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"> • Assign Alerts • Change the Priority • Change Due Date Time 				✓	
Add attachments		✓	✓	✓	
Download attachments	✓	✓	✓	✓	

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:

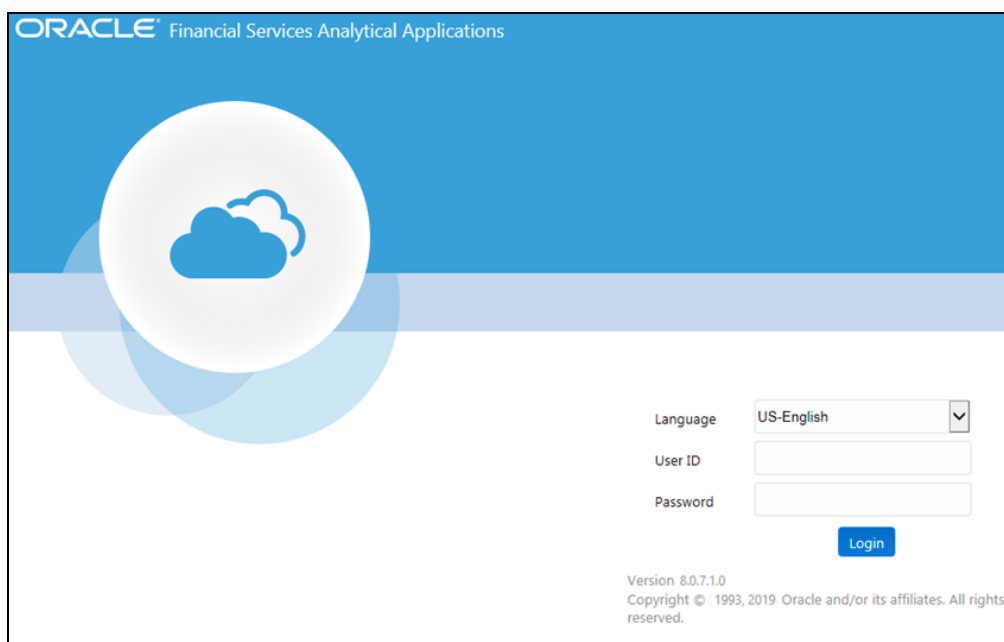
- 1 Enter the URL into your browser using the following format:

```
<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.

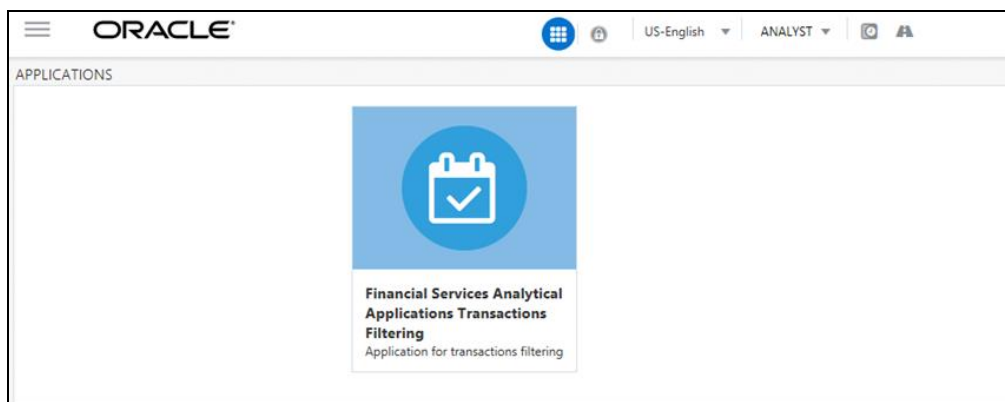
Figure 2: Oracle Financial Services Analytical Applications (OFSAA) Login Page



- 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.

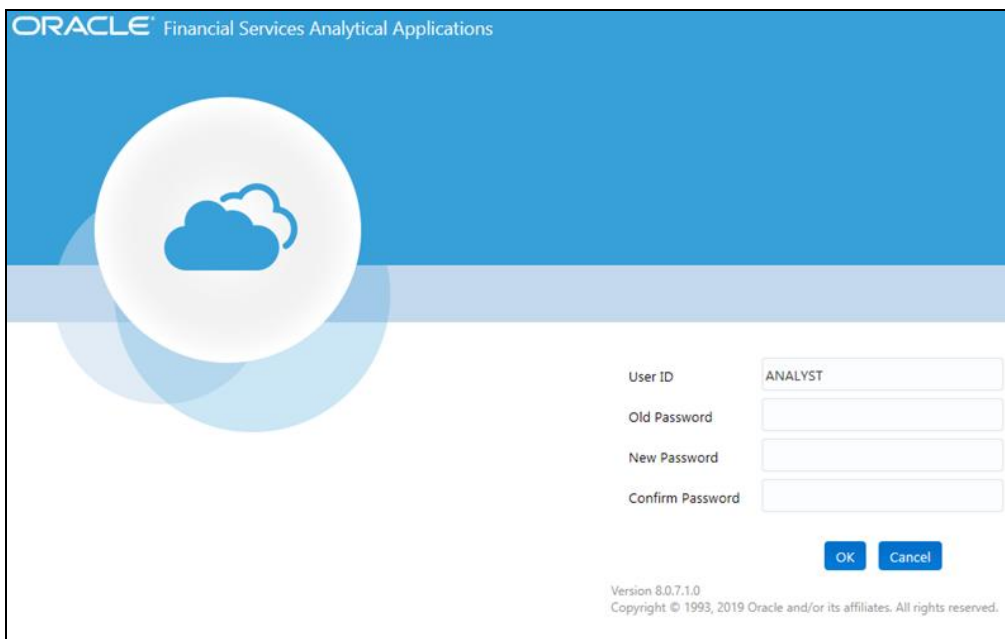
3.2.2 Changing the Application Password

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



The screenshot shows the Oracle Financial Services Analytical Applications Password Change Page. The page has a blue header with the Oracle logo and the text "ORACLE Financial Services Analytical Applications". Below the header is a large white circle containing a blue cloud icon. The main content area is white and contains a form with the following fields:

- User ID: ANALYST
- Old Password: [Empty text box]
- New Password: [Empty text box]
- Confirm Password: [Empty text box]

At the bottom right of the form are two buttons: "OK" and "Cancel". At the bottom left of the page, the version and copyright information are displayed: "Version 8.0.7.1.0 Copyright © 1993, 2019 Oracle and/or its affiliates. All rights reserved."

- 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** .

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

The screenshot shows a 'Preferences' dialog box with a 'Home Page' section. It contains a table with two columns: 'Property Name' and 'Property Value'. The first row has 'Set My Home Page' in the first column and 'Default Screen' in the second column, which has a dropdown arrow. Below the table are 'Save' and 'Cancel' buttons.

Property Name	Property Value
Set My Home Page	Default Screen

- 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:

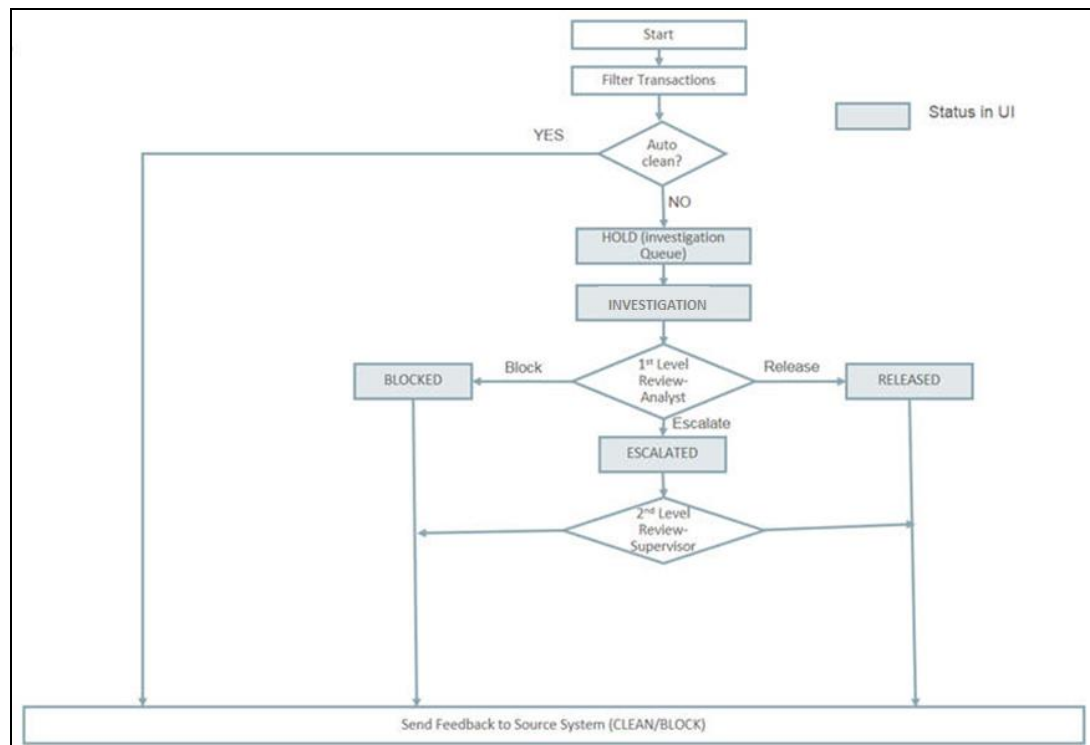
- 1 Navigate to the **Oracle Financial Services Analytical Applications** page.
- 2 Click **Financial Services Sanctions Pack**.
- 3 Click **Transaction Filtering**. The **Investigation User Interface** page is displayed.

4 Managing Transaction Filtering

4.1 Investigation User Interface Workflow

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

Figure 6: Investigation User Interface Workflow

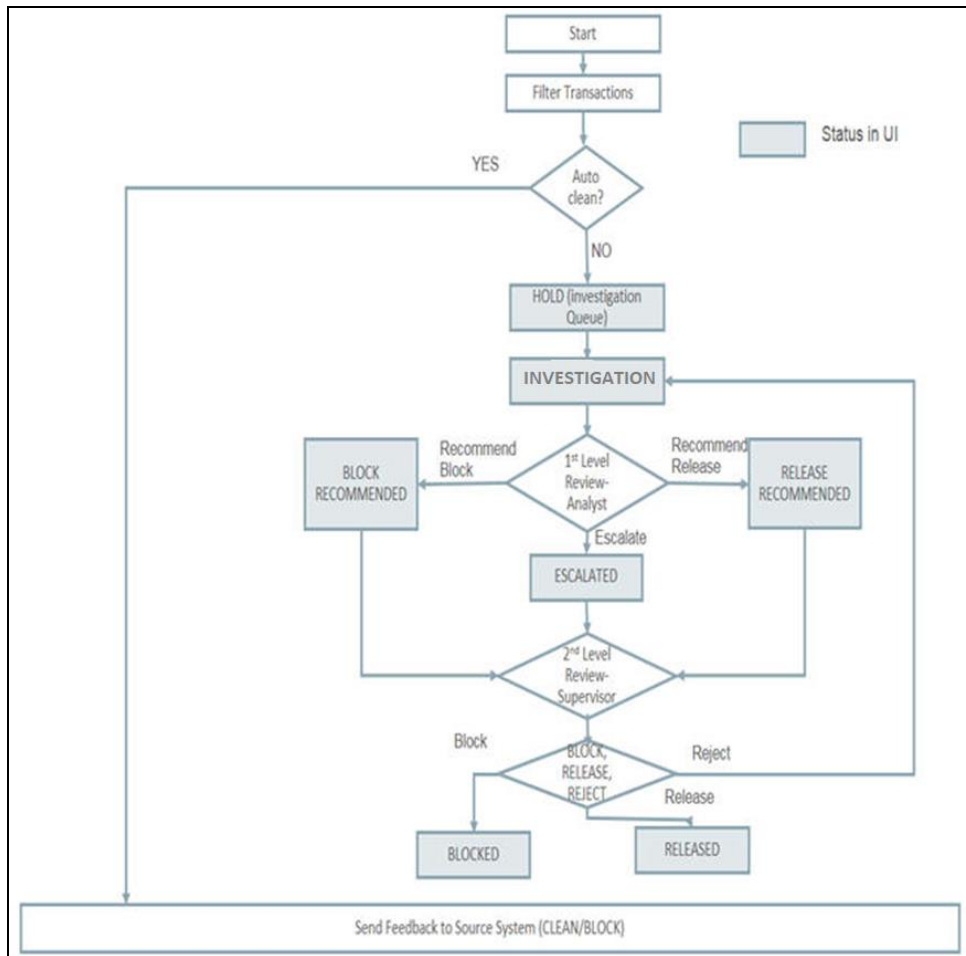


A suspicious message that is obtained after transactions are filtered is displayed in the Analyst's queue. These messages are auto cleaned by the application. If the message is clean, then a feedback message is sent back to the Transaction Filtering application. If not, the message is put on Hold (**H**). 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 7: Investigation User Interface Workflow for Four-Eyes Approval



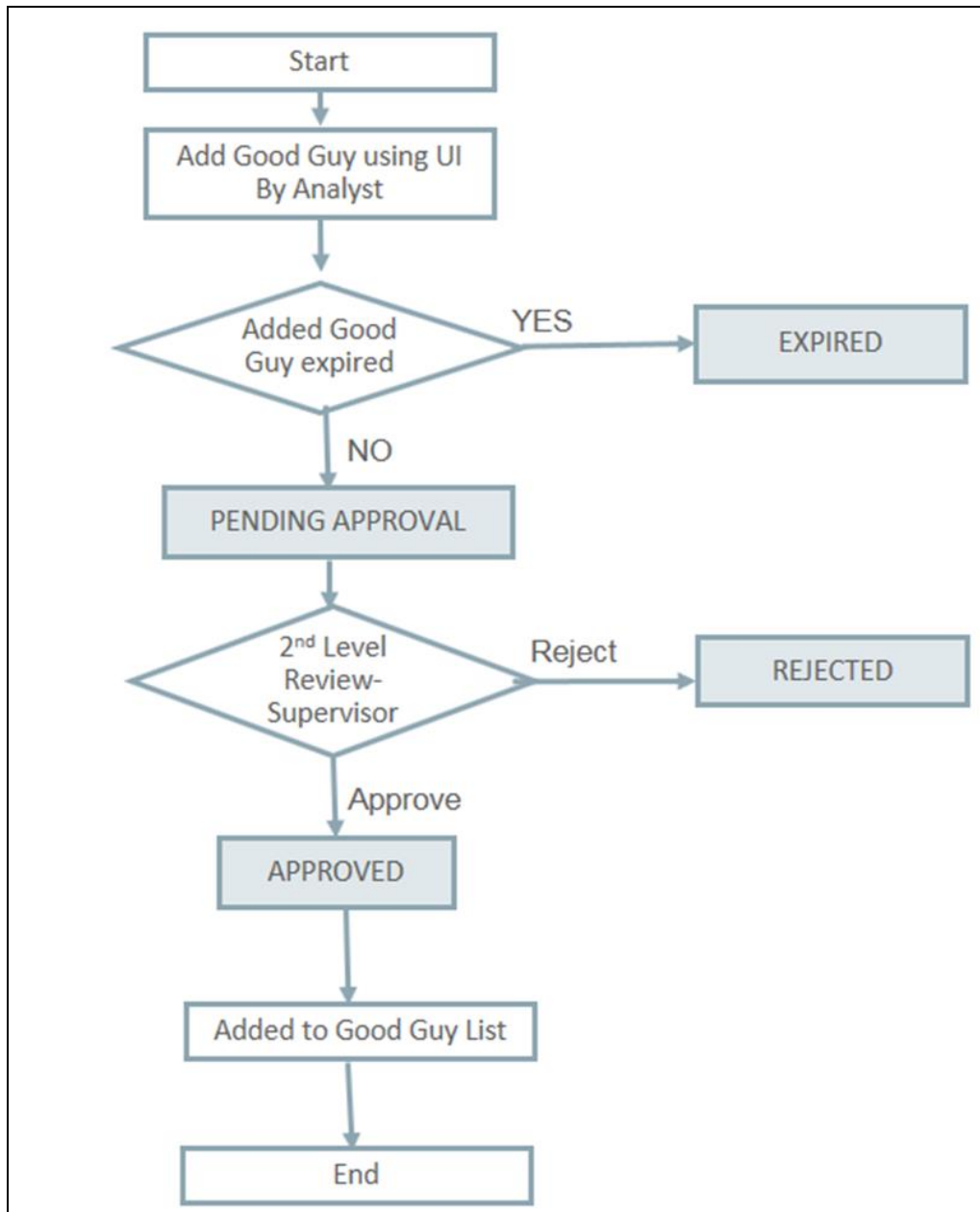
A suspicious message that is obtained after transactions are filtered is displayed in the Analyst’s queue. These messages are auto-cleaned by the application. If the message is clean, then a feedback message is sent back to the Transaction Filtering application. If not, the message is put on Hold (**H**). 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 8: 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 Matching](#).

4.2 List Management

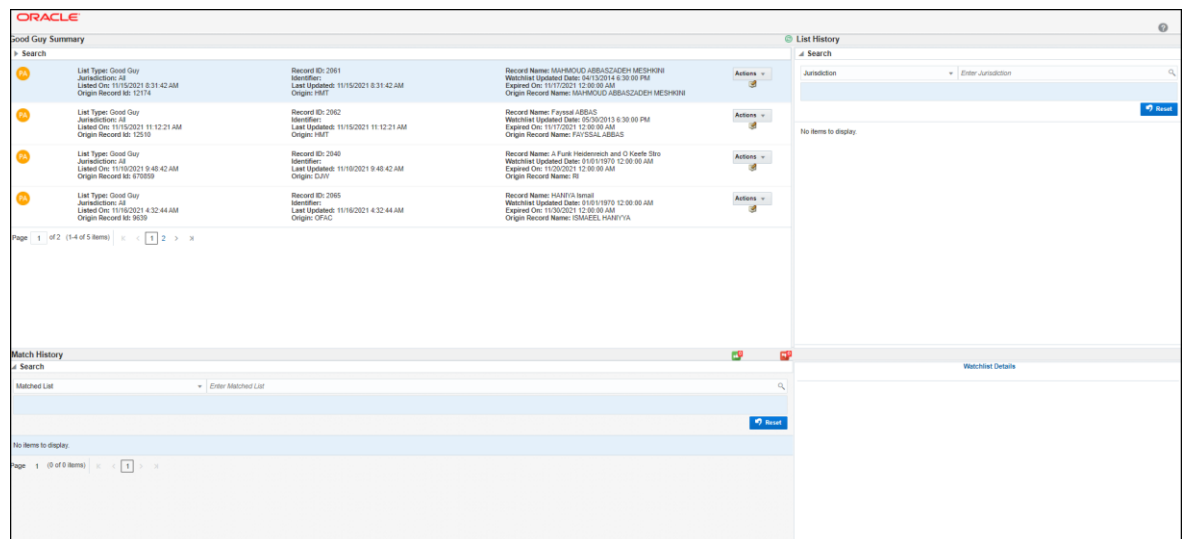
This section displays the Good Guy Summary, List History, Match History, and the Watchlist Details sections.

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 9: 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.
- **Record Name:** Enter or search for record name.
- **Jurisdiction:** You can either enter a jurisdiction name or select from the drop-down list.
- **Identifier:** 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.
- **Last Updated**
 - **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.
- **Origin Record ID:** Enter the origin record id.
- **Origin:** Enter the name of the origin.
- **Origin 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:

- **Jurisdiction:** You can either enter a jurisdiction name or select from the drop-down list.
- **Record ID:** Enter the record id value.
- **Origin:** Enter the name of the origin
- **Origin Record ID:** Enter the origin record id value.
- **Status:** Enter the status value.
- **Record Name:** Enter the record name.
- **Origin 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.
- 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:
 - 1 Click **Add Comments**  that is in line with the alert that you want to add comments to. The comments window is displayed.
 - 2 Enter your comments and click **Save**. The comment is added to the audit history of that alert.

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

You can configure the functionality assigned to user group in the 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 10: Queue List in List View

All Teams		
Queue List		
MT101_Hold	Transaction Filtering Analyst Group,Transaction Filtering Supervisor Group,TF Supervisor Access Group	08/31/2021 12:59:46 by QADMIN
MT202Testing	Transaction Filtering Supervisor Group	08/31/2021 13:07:46 by QADMIN
MT701_Hold	Transaction Filtering Analyst Group,Transaction Filtering Supervisor Group	08/31/2021 13:23:56 by QADMIN
Non-Blocked_Default_Jur_Queue	Transaction Filtering Analyst Group,Transaction Filtering Supervisor Group,TF Supervisor Access Group	09/02/2021 06:36:43 by QADMIN
Multiple criteria Hold_Queue	Transaction Filtering Analyst Group,Transaction Filtering Supervisor Group,TF Supervisor Access Group	09/02/2021 07:22:03 by QADMIN

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

- Queue Name
- User Group names (that are assigned by the Queue Administrator)
- 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.

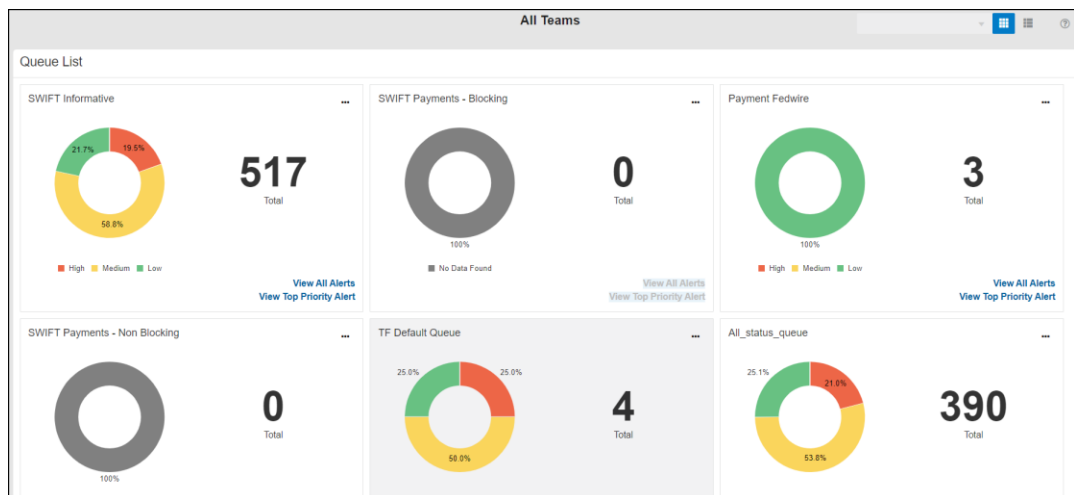
4.3.2 Grid View



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 11: Queue List in Grid View



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 only available priorities in the application:

- High
- Medium
- Low

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.

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 details page appears.

Figure 12: Alert List

The screenshot shows the Oracle Alert List interface. At the top, there is a navigation bar with the Oracle logo and the text 'Financial Services Analytical Applications Transactions Filtering'. The user is logged in as 'TFSUPERVISOR' in 'US-English'. The page title is 'Alert List' and the date is 'Thu Aug 26 2021 12:55:52 PM'. There is a 'Filter 0' button and a 'Save View' button. Below the header is a table with the following data:

Alert ID	Message Reference	Transaction Reference	Message Type	Message Category	Message Direction	Amount	Currency
51571	BlockedRecom	N/A	MT103	SWIFT	INBOUND	143585.91	USD
51343	Evaluatn2	N/A	MT101	SWIFT	INBOUND	11100	USD
51070	MTsaiteja	N/A	MT101	SWIFT	INBOUND	11100	USD
50865	MT2021	N/A	MT202	SWIFT	OUTBOUND	222	USD

At the bottom of the table, there is a pagination control showing 'Page 1 of 4' and '(1-10 of 32 Records)'. The 'Records Per Page' is set to 10.

This section contains the following default field details:

- 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 Date

The following are the optional fields that you can customize using the **Columns** menu:

- Received Date Time
- Batch Reference
- Watch List ID
- Decision
- 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

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

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 - Only Senior Supervisor)
- Attaching a File to an Alert (Only Analyst/Supervisor/Senior Supervisor)
- Customizing the Field Columns
- Saving the View
- Managing Views
- Closed Alerts
- Exporting the Alerts from the List
- Reload the Grid

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.

The following search filters are displayed. Select a criterion to filter the alerts based on the selection:

- Related Ref
- Created Date Time
- To Date
- From Date
- Received Date
- Alert Type
- Alert Id
- Priority

- Status
- Match Score
- Risk Score
- Alert Creation Date
- Message Category
- Message Direction
- Transaction Ref
- Message Ref
- Batch Ref
- BIC Code
- Message Type
- Amount
- Currency
- Overdue
- Ordering Party A/c No
- Ordering party Name
- Beneficiary Party A/C No
- Beneficiary Party Name
- Creditor Name
- Debtor Name
- Creditor Account
- Debtor Account
- Requested Execution Date
- Sender
- Receiver
- Standard Comments
- Created Date Range
- Primary Name
- Assignee
- Decision
- Customer/EE/Response ID
- Domain

- Jurisdiction

4.4.1.2 **Sorting the Alerts**

You can use the sort filters based on the field names in the list to filter the alerts based on the sort order.

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. Select one or more alerts and then click **Bulk Update**. The *Bulk Update* window is displayed.

Provide the details for the following fields, and the alerts get updated based on the below action performed:

- Due Date Time
- Priority
- Assignee

Click **Save**. The details related to the bulk actions will be added to the Audit History of each alert.

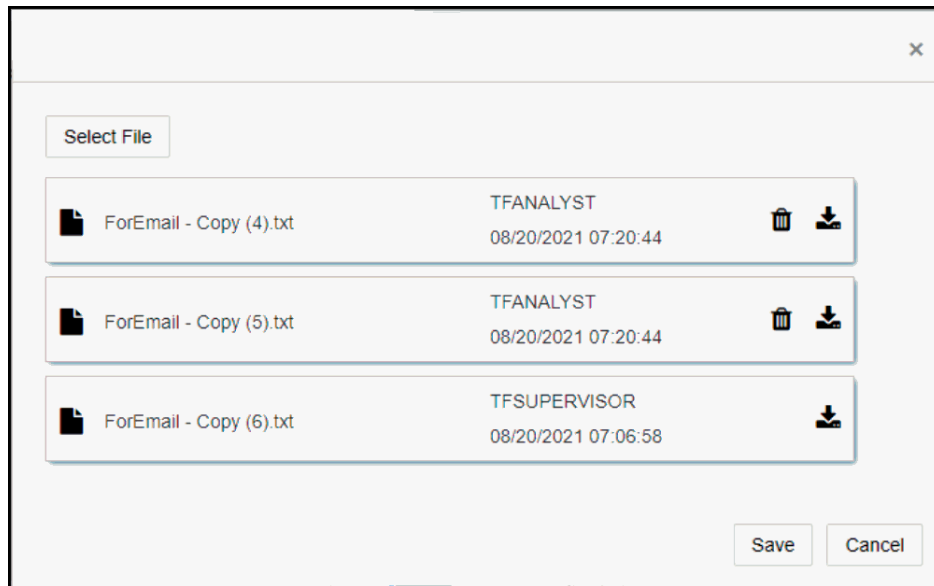
4.4.1.4 **Attaching a File to an Alert (Analyst/Supervisor/Senior Supervisor)**

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.

Select an alert from the list and follow these steps:

Figure 13: Add Attachments



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. Click **Delete** icon next to the Attachment name to delete any of the attachments,
5. Click **Ok** to confirm. The file will be marked to delete. Click **Save** to delete the file.
6. Click **Download** icon next to the **Delete** icon to download the attachment.

NOTE

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

4.4.1.5 Defining the View

You can define the view by customizing your field columns in the list as per your requirement. Follow these steps:

1. In the top right corner, select the **Columns** menu. The **Filter Columns** window appears.
2. Click **My Default** to set the default columns in the list.
3. You can filter the field data with the **Search** toolbar and select or select the fields from the list.
4. Click **Restore Defaults** to restore the selected fields by default.
5. Click **Save** to save your preference.

4.4.1.6 Saving the View


You can add the Customized View to the views list by saving it. Follow these steps:

1. Click **Save View**. The *Save View* window is displayed.
2. Enter the name of the View.
3. Optionally, click the **Set as default view** checkbox to set the current View as the default.
4. Click **Save**.

You can find the saved views list from the **Views** menu next to the **Save View** button.


4.4.1.7 Managing Views

To manage the views, follow these steps:


1. Select the **DEFAULT / <View Name>**. The *Views* window is displayed.
2. Use the Search bar to search for the views and select to apply or click the **View All** in the bottom right corner to view the complete list of available views.
3. The **Manage Views** window appears. You can find the View Name and the list of field columns details.
4. Click on any of the **View Name** or **Columns** to sort the views list.
5. You can delete any of the views from the list by clicking on the **Delete**  icon in the list.


4.4.1.8 Closed Alerts

Click the **Closed Alerts** button to see the list of closed alerts that the user has access to.

If you want to go back to the previous screen, click on **Reload**  icon.

4.4.1.9 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.

4.4.1.10 Reload the Grid

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

4.4.2 Field Descriptions

Table 4: 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.

Field	Description
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.
Comments	Displays the comments provided for the alert.
Domain	Displays the Business domain of the alert.
Jurisdiction	Displays the Jurisdiction 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.

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:

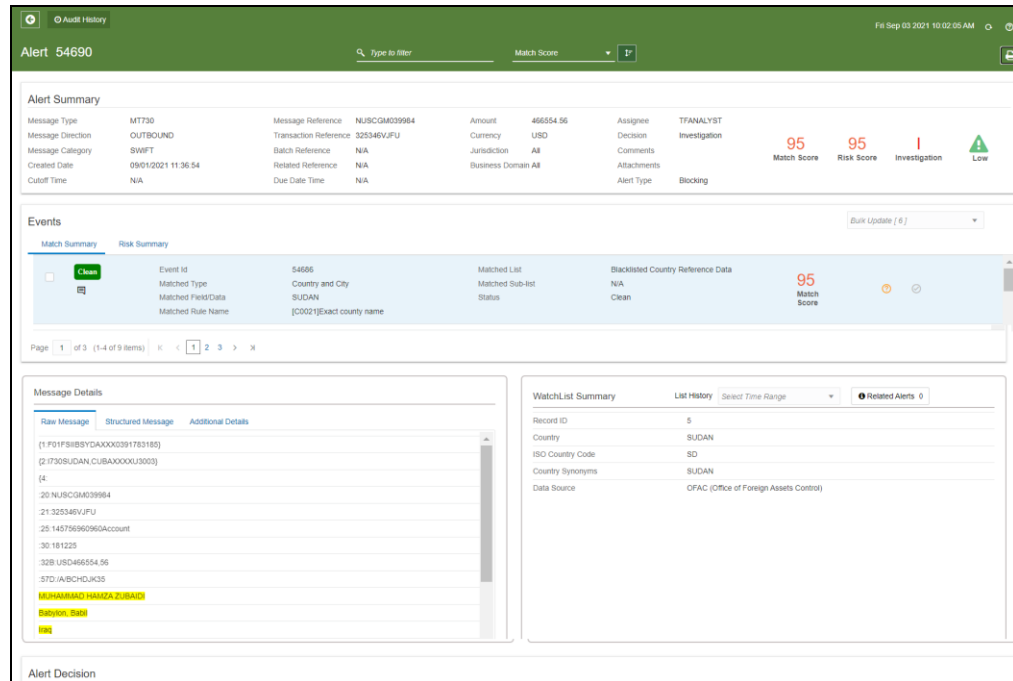
- Download attachments uploaded by other users
- See the actions taken by other users
- Perform the actions such as print pdf, view audit history and view watchlist details.

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

Figure 13: Alert Details




4.5.1.1 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.

4.5.1.2 Printing the Alert Details


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

4.5.1.3 Reload the Grid

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

4.5.1.4 Alert Summary Section

Figure14: Alert Summary Section

Alert Summary										
Message Type	MT103	Message Reference	BlockedRecom	Amount	143585.91	Assignee	TFANALYST			
Message Direction	INBOUND	Transaction Reference	N/A	Currency	USD	Decision	Block Recommended			
Message Category	SWIFT	Batch Reference	N/A	Jurisdiction	All	Comments	View Details	98	98	B
Created Date	08/25/2021 13:50:26	Related Reference	N/A	Business Domain	All	Attachments		Match Score	Risk Score	Block Recommended
Cutoff Time	N/A	Due Date Time	N/A			Alert Type	Blocking			Medium 

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
- 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.

4.5.1.5 Events

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

- Event Summary
- Risk Assessment

4.5.1.5.1 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:

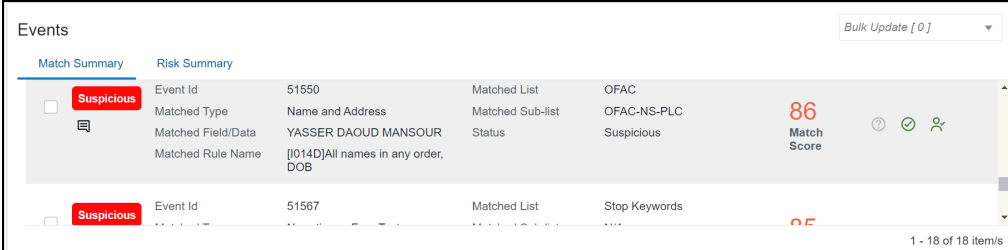
- Event ID
- Matched Type
- Matched Field /Data
- Matched Rule Name
- Matched List
- Matched Sub-list
- Status
- Match Score
- Edit Comments Icon

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

- Enter the Match Score value in the Search Filter.
- From the Filter menu, select the **Match Score**.

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

Figure 15: Event Summary





Event Id	Matched List	Matched Type	Matched Field/Data	Matched Rule Name	Matched Sub-list	Status	Match Score
51550	OFAC	Name and Address	YASSER DAOUD MANSOUR	[I014D]All names in any order, DOB	OFAC-NS-PLC	Suspicious	86
51567	Stop Keywords						85

An Analyst/Supervisor/Senior Supervisor can perform the following actions on the Events:


Adding Comments to an Event

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

1. In the *Events* 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**.


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.

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.

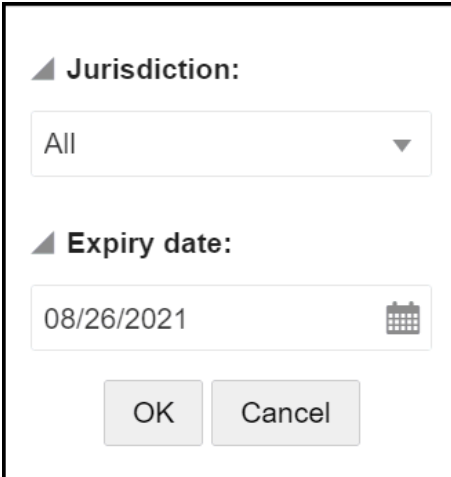
1. Click the **Clean**  button next to the Suspicious button. The *Add Comments* window is displayed.
2. Enter the comments and click **Save**. For more information, see [Adding comments to an Event](#).
3. If the event is marked as **Clean**, then the Clean button will be disabled, but **Suspicious**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

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 grey 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 16: Good Guy Pop-up Window



Select the Jurisdiction and Expiry date for the record and click **OK**. The record status or alert changes from Assigned (**A**) to Pending approval (**P**).

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.

Bulk Update the Events

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

1. In the **Events** section, select one or more events.
2. In the top right corner of the *Events* section, select the **Bulk Update** drop-down list and then select **Clean/Suspicious** status. The Add Comments window is displayed.

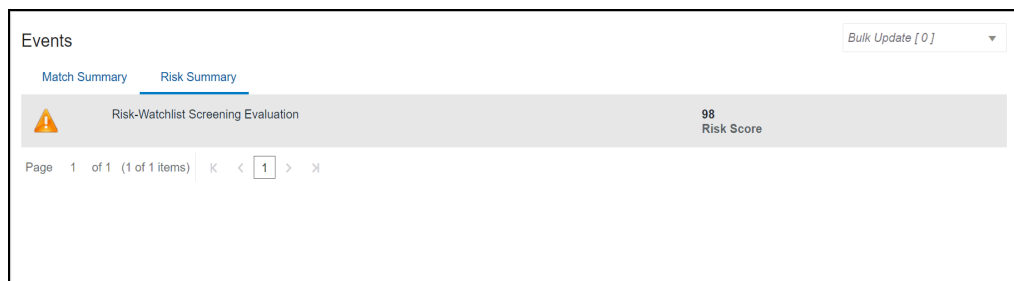
3. Enter the comments and click **Save**. For more information, see [Adding comments to an Event](#).
4. The status of the event will be updated. The Decision and Comment are added to the **Audit History** of that alert.

4.5.1.5.2 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 17: 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.

4.5.1.6 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.

Figure 18: Raw Message Format for SWIFT

Message Details

Raw Message Structured Message Additional Details

3/IRAN

:52A:REBSSYDA

:53B:SUDAN

:54D:EUZKADI TA ASKATASUNA

:59F:/950800362384

1/Mohammed Sani ABACHA NIGERIA

2/CUBA

2/NORTH KOREA

3/IRAN

:70:TEST

:71A:SHA

:71F:USD22,

:72:Zebra finches

[View All](#)

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 19: 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 20: 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*s 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 21: 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.

4.5.1.7 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 22: Watchlist Details Section

WatchList Summary	
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
- PassportType
- 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

4.5.1.8 Risk Indicator Details

NOTE

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

Figure 23: Risk Indicator Details

Risk Indicator Details	List History	Select Time Ra...	Related Alerts 0
Screening Rule	[C0025]Exact ISO country code (ISO 2)		
Screening Score	94		
Screening Rule	[I001U]Exact name only (Conflict)		
Screening Score	70		
Screening Rule	[I001U]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**.

4.5.1.9 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:

- Block
- Release
- Escalate

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

- 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 Alert](#).

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

4.5.1.9.1 **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).

4.5.1.9.2 **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**.

4.5.1.9.3 **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).

4.5.1.9.4 **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).

4.5.1.9.5 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**.

4.5.1.9.6 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.

4.5.1.9.7 Alert Statuses

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

Standard Flow For Analyst

- Hold
- Investigated
- Escalated
- Blocked
- Released

Standard Flow For Supervisor

- Escalated
- Blocked
- Released

Four-Eyes Flow For Analyst

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

Four-Eyes Flow For Supervisor

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

4.5.1.10 Audit History

The Audit History provides the match-level audit details on the alert. The details like a 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.

Figure 23: 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

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.

4.5.1.10.1 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.

4.5.1.10.2 Field Descriptions

Table 5: 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.

Fields	Description
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.

4.5.1.11 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.

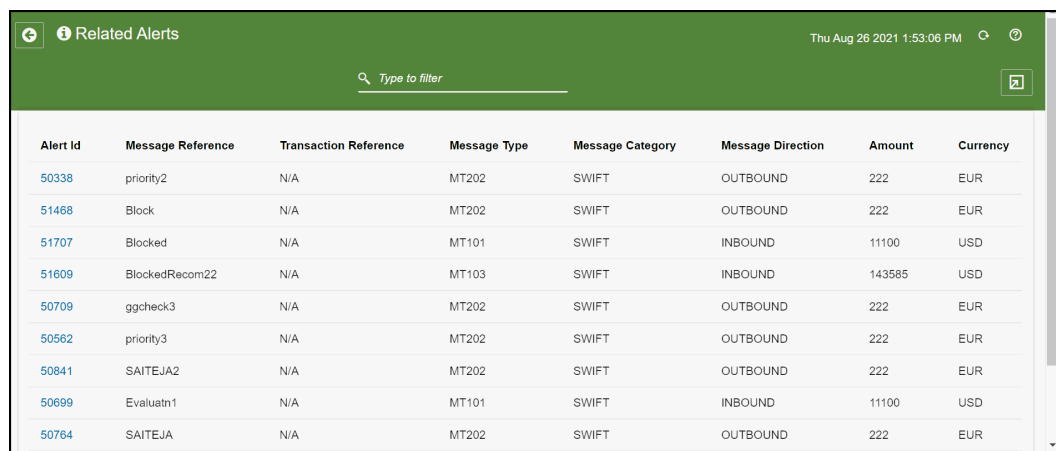
When the current case is 202COV message, its Transaction Reference no (Swift Field 21) is matched with Sender Reference (Swift Field 20) of 103 type case. These matched 103 message type cases are linked to the 202COV case.

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 24: Related Alerts



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
51609	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	SAITEJA2	N/A	MT202	SWIFT	OUTBOUND	222	EUR
50699	Evaluatn1	N/A	MT101	SWIFT	INBOUND	11100	USD
50764	SAITEJA	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.

4.5.1.11.1 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.

4.5.1.11.2 Field descriptions

Table 6: 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.

Fields	Description
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.

4.5.2 Field Descriptions

Table 7: 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.

Field	Description
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.
Receiver	Displays the Receiver name of the alert.

OFSAA Support

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 that has all the revised/recently released documents.

