

# **Oracle Financial Services Transaction Filtering**

**User Guide**

**Release 8.0.7.0.0**

**April 2021**

**E91801-01**

**ORACLE**  
Financial Services

**ORACLE**

## OFS Transaction Filtering User Guide

Copyright © 2021 Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

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

# Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
8.0.7.1.9	August 2021	<ul style="list-style-type: none"> <li>Added a Note for alert suppression related to the good guy in the <i>Transaction Filtering Workflows</i> section. For more information, see <a href="#">Transaction Filtering Workflows</a>.</li> </ul>
8.0.7.1.8	April 2021	<ul style="list-style-type: none"> <li>Incorporated "My Assigned Alert for user level 1 and 2" criteria.</li> <li>The exact match is highlighted with Red color and partially matched data is highlighted in Yellow color.</li> </ul>
8.0.7.1.7	April 2021	<ul style="list-style-type: none"> <li>Updated the <i>Good Guy Matching</i> section to indicate that the good guy button is disabled after it is added to the allow list.</li> <li>Updated the <i>Locking the Alert</i> section to include the lock information for the supervisor user.</li> </ul>
8.0.7.1.12	November 2020	<ul style="list-style-type: none"> <li>Updated the <i>Raw Message Format for SWIFT</i> screen to display only the matched portion of the message which is highlighted in the <i>Message and Audit</i> Section.</li> <li>Updated the <i>Risk Details</i> screen to display the <b>Number of Hits</b> counter in the <i>Risk Summary</i> section.</li> <li>Updated the <i>Match Summary</i> screen to display the sequence of matches in the <i>Match Summary</i> section.</li> <li>Updated the <i>Audit</i> screen to display the actions performed on attachments in the <i>Message and Audit</i> section.</li> </ul>
8.0.7.0.36	October 2020	Added a new option, <i>Allow</i> , for transactions in the <i>Match Summary Section</i> .
8.0.7.0.30	July 2020	<ul style="list-style-type: none"> <li>Added two search criteria, business domain, and jurisdiction, to filter alerts in the Investigation User Interface in the <i>Alert Summary</i> section of the <i>Managing Transaction Filtering</i> chapter.</li> <li>Updated the RAW message screen in the <i>Message and Audit</i> Section of the <i>Managing Transaction Filtering</i> chapter.</li> </ul>
8.0.7.0.29	June 2020	Added content that tells the logged-in analyst how to view all alerts that are closed by all analysts in the <i>Alert Summary</i> Section of the <i>Managing Transaction Filtering</i> chapter.
8.0.7.0.23	March 2020	Updated the <i>List Details</i> section in the <i>Managing Transaction Filtering</i> chapter.
8.0.7.0.22	January 2020	<ul style="list-style-type: none"> <li>Updated images in all chapters to include the label changes, new images for ISO20022, and icon for overdue alerts in the <i>Managing Transaction Filtering</i> chapter.</li> <li>Updated the <i>Introduction</i> section in the <i>About Transaction Filtering</i> chapter.</li> </ul>

Version Number	Revision Date	Change Log
8.0.7.0.0	July 2019	Updated the <i>Types of Feedback Messages Sent</i> section in the <i>About Transaction Filtering</i> chapter.

# Table of Contents

<b>1</b>	<b>About This Guide .....</b>	<b>7</b>
1.1	Who Should Use This Guide .....	7
1.2	How this Guide is Organized .....	7
1.3	Where to Find More Information.....	7
1.4	Conventions Used in This Guide .....	8
<b>2</b>	<b>About Transaction Filtering.....</b>	<b>9</b>
2.1	Transaction Filtering Workflow .....	10
2.1.1	<i>Process for Messages Containing a Single Transaction</i> .....	11
2.1.2	<i>Process for Messages Containing Multiple Transactions or Multiple Batches</i> .....	11
2.2	Features of Transaction Filtering.....	12
2.3	Score Matching Logic.....	12
2.4	User Roles and Actions.....	13
<b>3</b>	<b>Getting Started.....</b>	<b>14</b>
3.1	Accessing the Oracle Financial Services Analytical Applications (OFSAA) Page.....	14
3.2	Managing the Oracle Financial Services Analytical Applications (OFSAA) Page .....	16
3.2.1	<i>Applications Tab</i> .....	16
3.2.2	<i>Changing the Application Password</i> .....	16
3.2.3	<i>Viewing the Application's Copyright Information</i> .....	17
3.3	Troubleshooting Your Display .....	17
3.3.1	<i>Enabling JavaScript</i> .....	18
3.3.2	<i>Enabling Cookies</i> .....	18
3.3.3	<i>Enabling Temporary Internet Files</i> .....	18
3.3.4	<i>Enabling File Downloads</i> .....	18
3.3.5	<i>Setting Print Options</i> .....	18
3.3.6	<i>Enabling the Pop-Up Blocker</i> .....	19
3.3.7	<i>Setting Home Page Preferences</i> .....	19
3.4	Logging into the Transaction Filtering Application.....	20
<b>4</b>	<b>Managing Transaction Filtering .....</b>	<b>21</b>
4.1	Transaction Filtering Workflows.....	21

4.2	Locking the Alert .....	25
4.3	Analyzing the Alert .....	25
4.3.1	Alert Summary Section.....	26
4.3.2	Message and Audit Section .....	29
4.3.3	Match Summary Section .....	34
4.3.4	List Details .....	35
4.3.5	Risk Summary Section .....	39
4.3.6	Notification and Reporting Section .....	40
4.3.7	Good Guy Matching .....	41
4.4	Taking an Action on an Alert.....	44
4.4.1	Recommending to Block an Alert.....	45
4.4.2	Recommending to Release an Alert .....	45
4.4.3	Escalating an Alert.....	46
4.4.4	Blocking an Alert.....	46
4.4.5	Releasing an Alert.....	46
4.4.6	Rejecting an Alert.....	46
4.4.7	Alert Statuses.....	47
4.5	Task Emails.....	48

# 1 About This Guide

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

## Topics:

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

## 1.1 Who Should Use This Guide

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

- **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.

## 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 Where to Find More Information

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

- Oracle Financial Services Sanctions Installation Guide
- Transaction Filtering Administration and Transaction Filtering Release Notes

These documents are available at the following link:

[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 Used in This Guide

The following table mentions the conventions used in this guide.

**Table 2: Conventions Used**

Conventions	Meaning
<i>Italics</i>	Names of books as references Emphasis Substitute input values
<b>Bold</b>	Menu names, field names, options, button names Commands typed at a prompt User input
Monospace	Directories and subdirectories File names and extensions Code sample, including keywords and variables within text and as separate paragraphs, and user-defined program elements within text
<a href="#">Hyperlink</a>	Hyperlink type indicates the links to external websites, internal document links to sections.
Asterisk (*)	Mandatory fields in User Interface
<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 either be suspicious, restricted, or sanctioned with 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 which are in SWIFT, ISO20022, Fedwire, NACHA, or any custom format.

The OFS Transaction Filtering application is built using components of the Oracle Financial Services Analytical Applications (OFSAA) product suite. 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 who were either sanctioned or who lived in sanctioned countries and identify any transactions which were associated with these customers. FIs are now expected to also 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 therefore minimizes the operational impact on FIs.

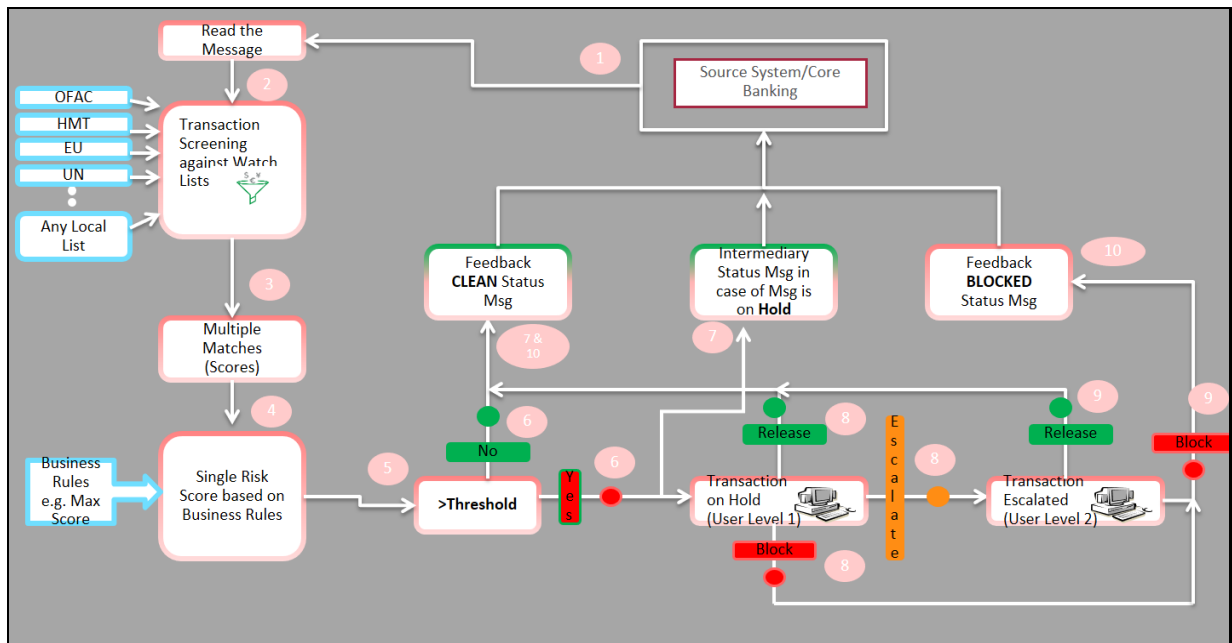
### Topics:

- [Transaction Filtering Workflow](#)
- [Features of Transaction Filtering](#)
- [Score Matching Logic](#)
- [User Roles and Actions](#)

## 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, 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 a 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.

### Topics:

- [Process for Messages Containing a Single Transaction](#)
- [Process for Messages Containing Multiple Transactions or Multiple Batches](#)

### 2.1.1 Process for Messages Containing a Single Transaction

For messages that contain a single transaction, follow these steps:

1. The TF application receives a message from the payment system, scans it against the watch lists, and provides a risk score for the message.
2. If no suspicious data is found during screening, the TF application sends a feedback message with the status **CLEAN** back to the payment system through the message queue.
3. If suspicious data is found during screening, 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.
4. The Analyst reviews the message, which is the first level of review and makes a decision 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.
5. For a four-eyes workflow, the Analyst can *Recommend to Release*, *Recommend to Block*, or escalate the message to the Supervisor.
6. If the Analyst escalates the message, 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 a four-eyes workflow, the Supervisor can *Release*, *Block*, or *Reject* the message.
7. 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. For more information, see [Match Summary Section](#) and [Risk Summary Section](#).

### 2.1.2 Process for Messages Containing Multiple Transactions or Multiple Batches

For messages that contain multiple transactions, follow these steps:

1. OFS Transaction Filtering (OFS TF) receives messages from the payment system and scans the transactions or batches in the message against the watch lists and does risk scoring on that message.
2. For the NACHA and some ISO20022 message types, transactions are generated at the batch level. But where transactions are not generated at the batch level, that is, for SWIFT, Fedwire, and other ISO20022 message types, transactions are generated at the message level.
3. If all transactions within a message or a batch (for NACHA and ISO20022) are found **CLEAN**, OFS TF sends a feedback message with **CLEAN** status back to the payment system.
4. If any of the transactions in the message are found suspicious, all transactions in the message will be held and an Analyst investigates further. Intermediary feedback is sent to the payment system, indicating that the message is on hold.
5. For the NACHA and ISO20022 message types, if any of the transactions within a batch are found to be suspicious, then all transactions belonging to that batch are kept in HOLD status for an Analyst to investigate further.
6. The Analyst reviews all transactions and decides to Release or Block the message or batch. In this configuration, the decision status is associated with the message or batch and not an individual transaction. Either all transactions get released or all transactions get blocked. You

can view the associated matched data of a transaction and take a decision. OFS TF sends a feedback (**CLEAN/BLOCKED**) message to the payment system for the message reviewed.

7. For a four-eyes workflow, the Analyst can *Recommend to Release*, *Recommend to Block* or escalate the transaction to the Supervisor.
8. If the Analyst escalates the transaction, the transaction is sent to the Supervisor (Second level review). The Supervisor can block or release the message and add comments.
9. For a four-eyes workflow, the Supervisor can *Release*, *Block*, or *Reject* the transaction.

You can view the associated matched data of a message or transaction from the **Match Summary** section. You can also view the risk score details from the **Risk Summary** section. For more information, see [Match Summary Section](#) and [Risk Summary Section](#).

## 2.2 Features of Transaction Filtering

Following are the features of Transaction Filtering:

- Screens financial transactions to detect blocklisted 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. 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.
- 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 Supervisor.
- Provides the ability to add notes/comments while taking an 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 *Recommend 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 has multiple 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. For a full description of the risk scores, see the **Configuring Risk Scoring Rules** section in the [Transaction Filtering Administration Guide](#).

The logic used in scoring the 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:

- Analyst
- Supervisor

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	Analyst	Supervisor
Access to View UI	X	X
Recommend to Release Transaction	X	
Recommend to Block Transaction	X	
Release Transaction	X	X
Block Transaction	X	X
Escalate Transaction	X	
Reject Transaction		X

## 3 Getting Started

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

### Topics:

- [Accessing the Oracle Financial Services Analytical Applications \(OFSAA\) Page](#)
- [Managing the Oracle Financial Services Analytical Applications \(OFSAA\) Page](#)
- [Troubleshooting Your Display](#)
- [Logging in to the Transaction Filtering Application](#)

### 3.1 Accessing the Oracle Financial Services Analytical Applications (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](#).

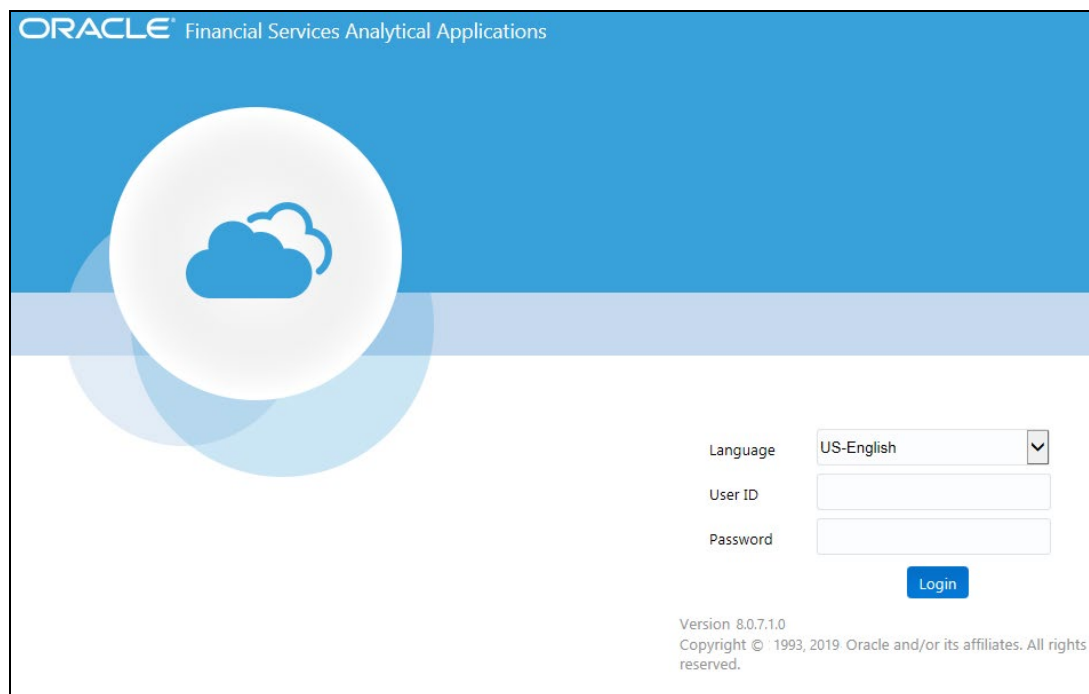
To access the Oracle Financial Services Analytical Applications, follow these steps:

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

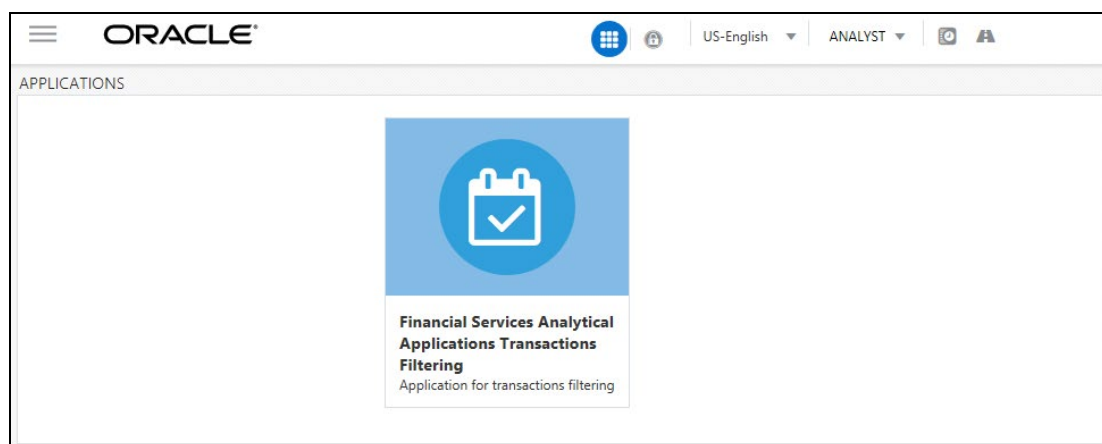
```
<scheme/ protocol>://<ip address/ hostname>:<port>/<context-name>/login.jsp
```

For example: `https://myserver:9080/ofsaapp/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 the Oracle Financial Services Analytical Applications (OFSAA) Page

### Topics:

- [Applications Tab](#)
- [Changing the Application Password](#)
- [Viewing the Application's Copyright Information](#)

### 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.

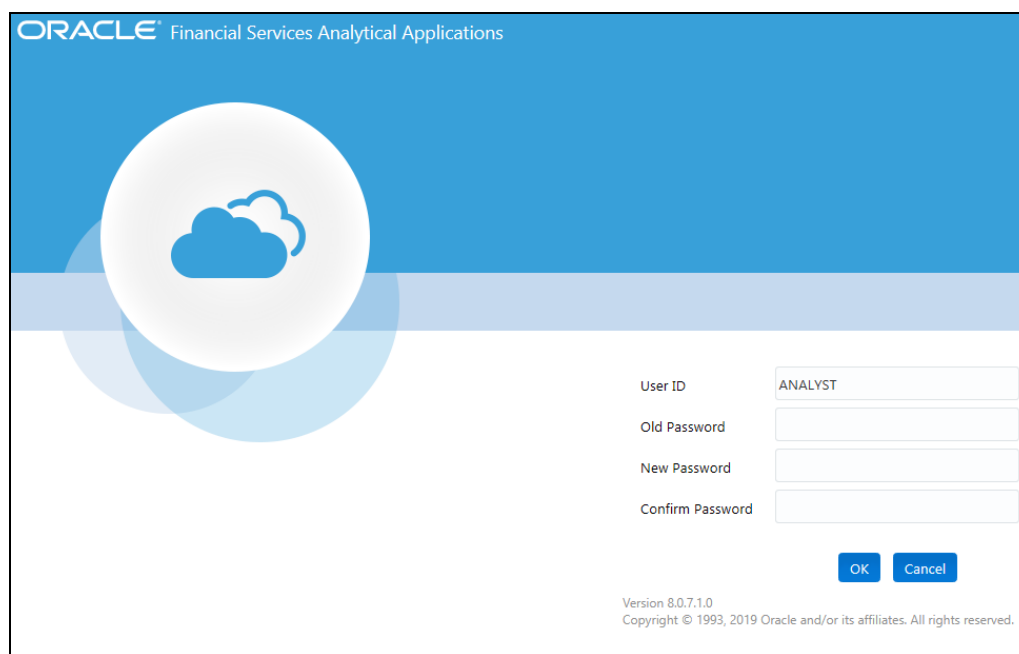
### 3.2.2 Changing the Application Password

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 "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". Below the buttons, 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 password 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.

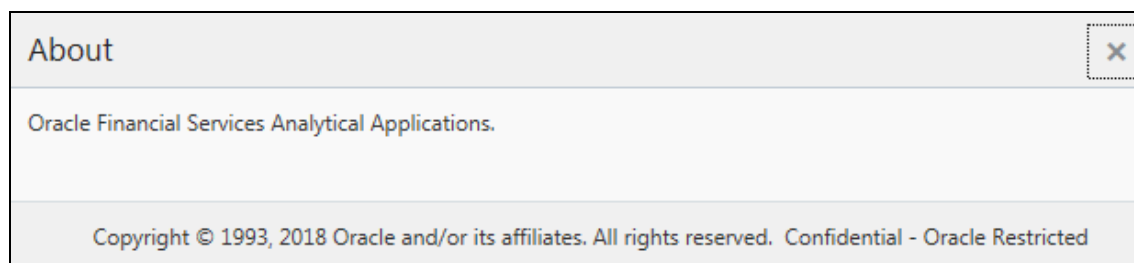
**NOTE** Your password is case sensitive. If you have problems with the password, verify that the Caps Lock key is off. If the problem persists, contact your system administrator.

### 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 (OFSA)** 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 with 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.

### Topics:

- [Enabling JavaScript](#)
- [Enabling Cookies](#)
- [Enabling Temporary Internet Files](#)
- [Enabling File Downloads](#)
- [Setting Print Options](#)
- [Enabling the Pop-Up Blocker](#)
- [Setting Home Page Preferences](#)

### 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:

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

**TIP**

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 URL of the application 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 URL of the application 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**

Preferences

▼ Home Page

Property Name	Property Value
Set My Home Page	Default Screen ▼

Save Cancel

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

**NOTE**

Whenever a new application is installed, the related value for that application 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

This chapter describes the concept and process of filtering messages. It provides instructions to carry out various actions according to the workflow and user roles using the **Investigation User Interface** page. This also helps you to understand the various components to accomplish each task.

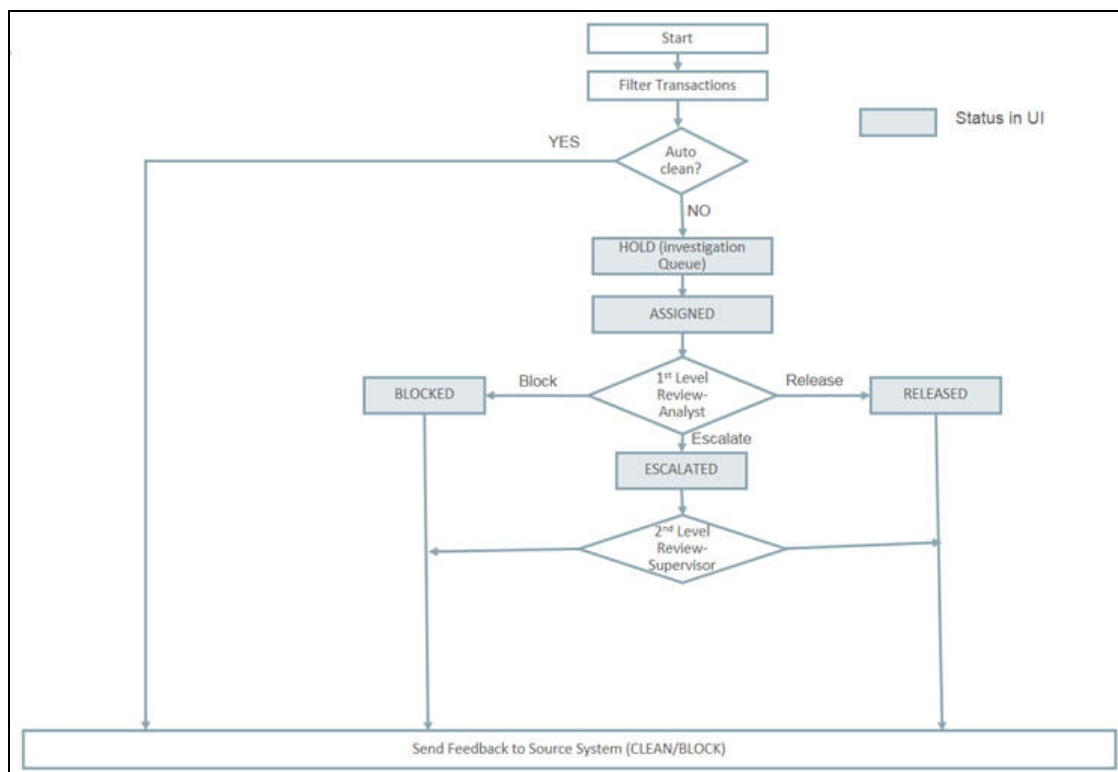
### Topics:

- [Transaction Filtering Workflows](#)
- [Locking the Alert](#)
- [Analyzing the Alert](#)
- [Taking an Action on an Alert](#)
- [Task Emails](#)

### 4.1 Transaction Filtering Workflows

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

**Figure 7: Investigation User Interface Workflow**



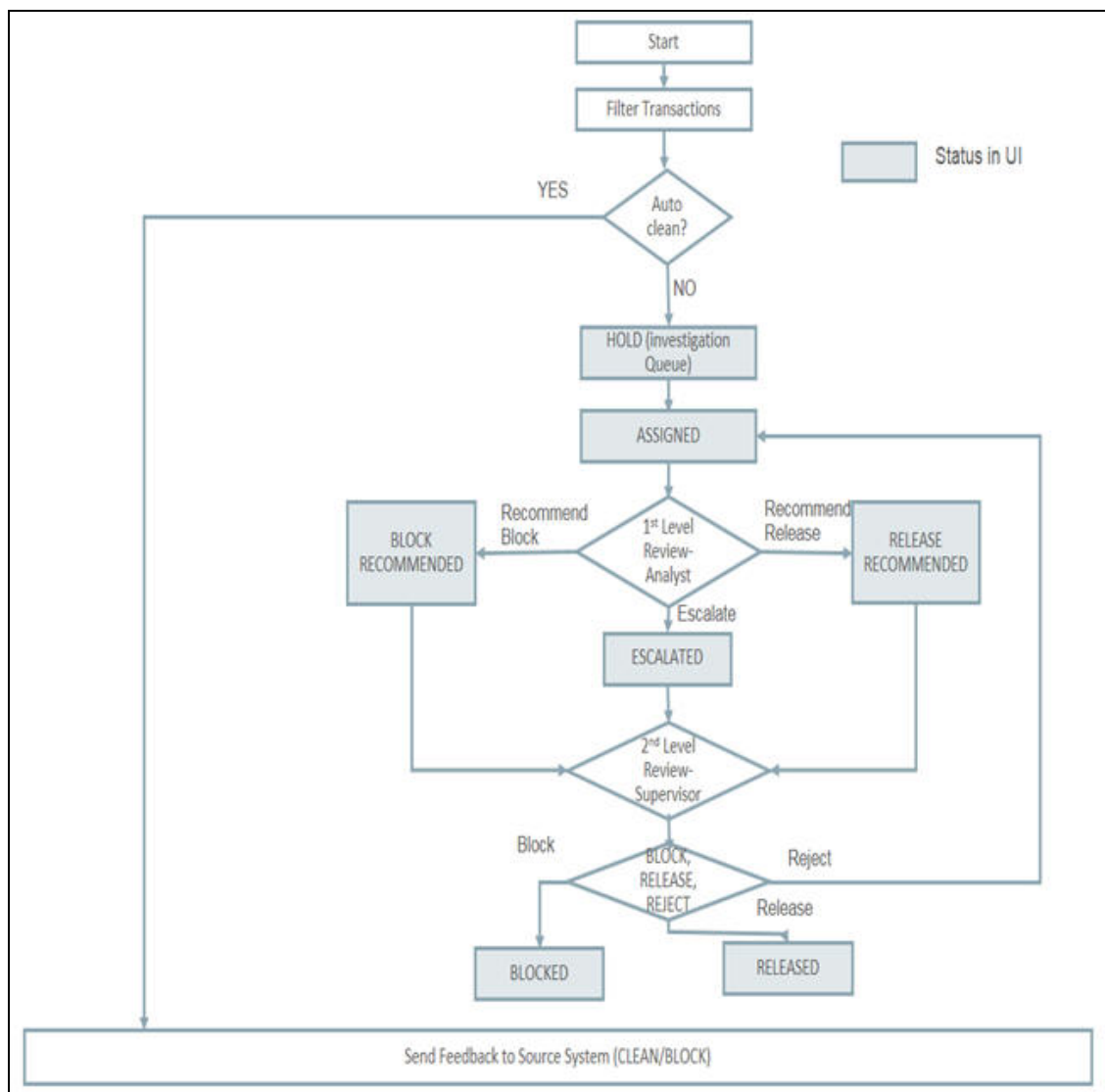
A suspicious message that is obtained after transactions are filtered is displayed in the Analyst's queue. These messages are auto-cleaned by the application. If the message is clean, then a feedback message is sent back to the Transaction Filtering application. If not, the message is put on Hold (**H**). The Analyst picks up the message from the queue by locking it. The message is then Assigned (**A**).

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 a 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**



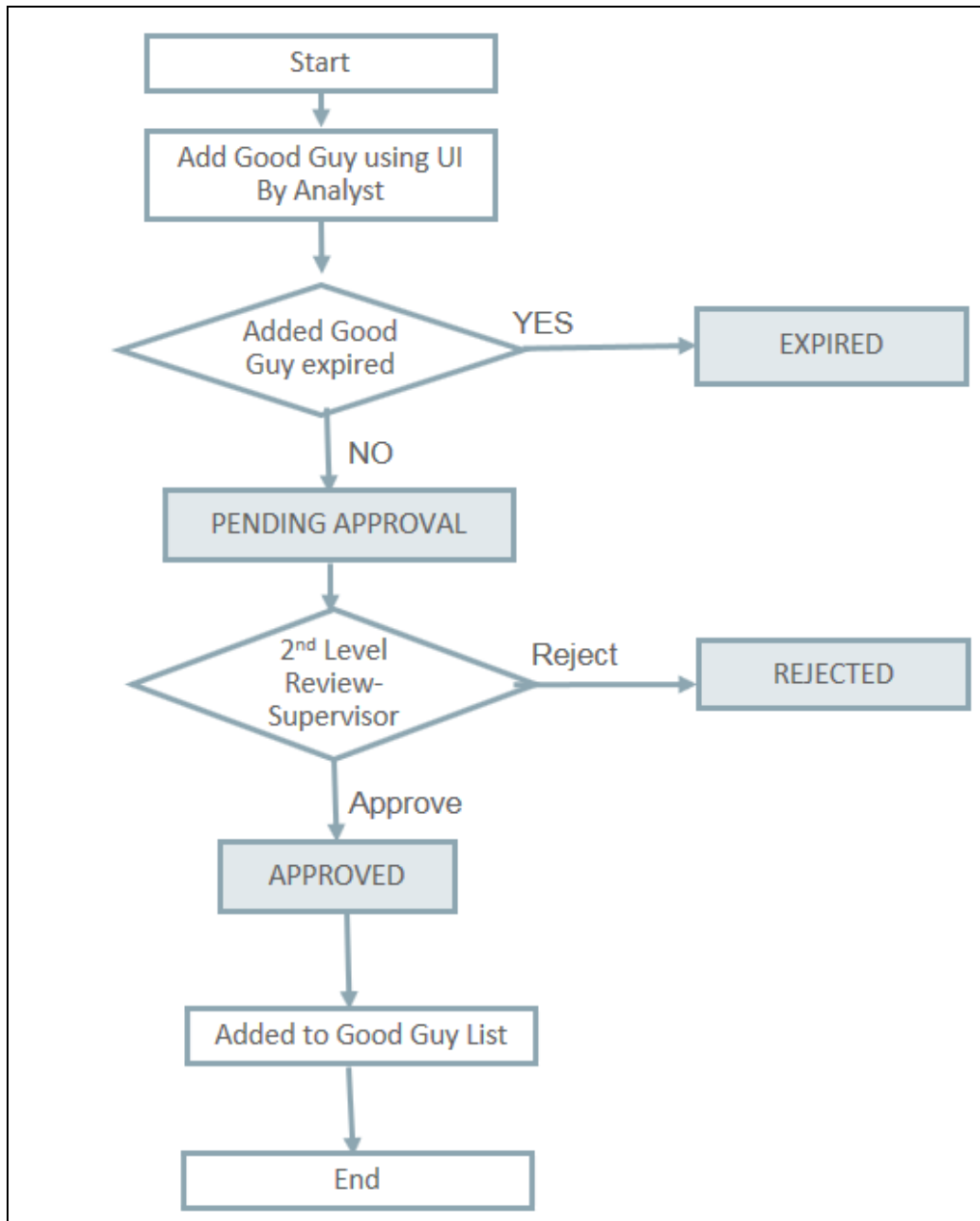
A suspicious message that is obtained after transactions are filtered is displayed in the Analyst's queue. These messages are auto-cleaned by the application. If the message is clean, then a feedback

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 then Assigned (**A**). 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 a 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



**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](#).





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 Locking the Alert

To work on an alert as a Supervisor, lock and self-assign the alert. After the alert is self-assigned, no other Supervisor can work on the alert.

To lock an alert, follow these steps:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**.
2. In the **Alert Summary** section, click **Toggle (Hold to Assigned)** . It changes to **Toggle (Hold to Assigned)** , and the status of the alert changes from **H** (Hold) to **A** (Assigned).

## 4.3 Analyzing the Alert

Once the alert is locked, the Analyst works on the alert by observing its details. These alert details are displayed in the following sections of the **Financial Services Analytical Applications Transactions Filtering home page**:

- Alert Summary Section
- Message and Audit Section
- Match Summary Section
- List Details
- Risk Summary Section
- Notification and Reporting Section

The following image shows the different components of the **Investigation User Interface** page:

**Figure 10: Components of the Investigation User Interface**

The screenshot displays the Oracle Financial Services Transaction Filtering Alert Summary interface. It features a list of alerts with columns for Message Identifier, Transaction Ref ID, Amount, Currency, and Business Domain. Below the list is a Match Summary section with a table of references and pending actions. On the right, there is a List Details section showing record ID, BIC, and data source.

Message Identifier	Transaction Ref ID	Amount	Currency	Business Domain
psm.001.001.01	Transaction Ref ID: Received Date: 03/16/2020 4:46:10 PM	Amount: 09	Currency: JPY	Business Domain: J
psm.001.001.01	Transaction Ref ID: Received Date: 03/16/2020 4:46:10 PM	Amount: 09	Currency: JPY	Business Domain: J
psm.001.001.01	Transaction Ref ID: Received Date: 03/13/2020 6:20:23 PM	Amount: 25000	Currency: JPY	Business Domain: J
psm.001.001.01	Transaction Ref ID: Received Date: 03/13/2020 5:23:26 PM	Amount: 25000	Currency: JPY	Business Domain: J

Matched Type	Matched Field	Matched Rule Name	Matched Sub-Item	Matched Status	Matched Score
ETIC <td>FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td></td></td>	FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td></td>	0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td>	Sanctioned BIC <td>Pending <td>95</td> </td>	Pending <td>95</td>	95
ETIC <td>FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td></td></td>	FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td></td>	0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td>	Yokohai BIC <td>Pending <td>95</td> </td>	Pending <td>95</td>	95
ETIC <td>FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td></td></td>	FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td></td>	0001Exact bank identification code (BIC) match <td>Yokohai BIC <td>Pending <td>95</td> </td></td>	Yokohai BIC <td>Pending <td>95</td> </td>	Pending <td>95</td>	95
ETIC <td>FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td></td></td>	FTCKPPY <td>0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td></td>	0001Exact bank identification code (BIC) match <td>Sanctioned BIC <td>Pending <td>95</td> </td></td>	Sanctioned BIC <td>Pending <td>95</td> </td>	Pending <td>95</td>	95

Record ID	BIC	Data Source
2	FTCKPPY	FOREIGN TRADE BANK OF THE O.P.R. OF KOREA
		OFAC

## Topics:

- [Alert Summary Section](#)
- [Message and Audit Section](#)
- [Match Summary Section](#)
- [List Details](#)
- [Risk Summary Section](#)
- [Notification and Reporting Section](#)
- [Good Guy Matching](#)

### 4.3.1 Alert Summary Section

This section displays the list of alerts that are in the Analyst's/Supervisor's queue.

You can perform the following actions in this section:

- Taking an action on an alert. You can block the alert, release the alert, or escalate the alert.
- Adding comments to an alert. This also contains the user details who has locked an alert. For more information, see [Adding Comments to an Alert](#).
- Adding an attachment to an alert. You can add an attachment to an alert. For more information, see [Attaching a File to an Alert](#).
- To perform these actions, unlock the alert.

This section contains the following components:

- Message Identifier
- Message Type
- Message Category

- Batch Reference
- Transaction Reference
- Related Reference
- Message Direction
- Currency
- Status

By default, the logged-in analyst can only see the alerts they have closed. To see the alerts closed by all analysts, run the `select t.v_attribute_value1 from setup_rt_params t where t.v_param_name = 'ALL_CASES_FOR_ANALYSTS'` query in the ATOMIC schema and set the `ALL_CASES_FOR_ANALYSTS` value to **Y**.

- Jurisdiction
- Business Domain
- Overdue Transactions
- Basic search and advanced search for:
  - Amounts
  - Match score
  - Risk score
  - Receipt date
  - Last updated date
  - User Assigned

For the amounts, match score, and risk score criteria, you can search for alerts based on a specific range. The **Receipt Date** shows the date when an alert was received within the system. The **Last Updated Date** shows when an alert was last updated. For example, when you escalate an alert, then it shows the date that it was escalated.

- Advanced search for:
  - Originator Account Number
  - Beneficiary Account Number
  - Originator Country
  - Destination Country
  - Matched Rule
  - Risk Rule

**NOTE**

The Supervisor can change an alert which is in Assigned status back to Hold status.

You can filter the data to be displayed by selecting one of the criteria in the **Search** toolbar. You can also reset the search criteria by clicking the **Reset** button.

The **Sort by** section has the following criteria. Select a criterion to filter the alerts based on the selection.

- Receipt Date/Time
- Amount
- Match Score
- Risk Score
- Last Updated Score

**Figure 11: Alert Summary Section**

#### Topics:


- [Adding Comments to an Alert](#)
- [Attaching a File to an Alert](#)

### 4.3.1.1 Adding Comments to an Alert

You must enter comments for an alert. There are two ways:


- Comments logged during taking Release/Block/Escalate action
- Ad hoc comments when an alert is in locked status or escalated status.

Follow these steps to add an ad hoc comment:

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**.
2. Assign the alert to yourself by locking it. The status changes from **H** to **A**.
3. Click **Add Comments**  that is in line with the alert that you want to add comments to. The comments window is displayed.
4. Enter your comments and click **Save**. The comment is added to the audit history of that alert.

### 4.3.1.2 Attaching a File to an Alert

You can also attach a file to the alert. Follow these steps:

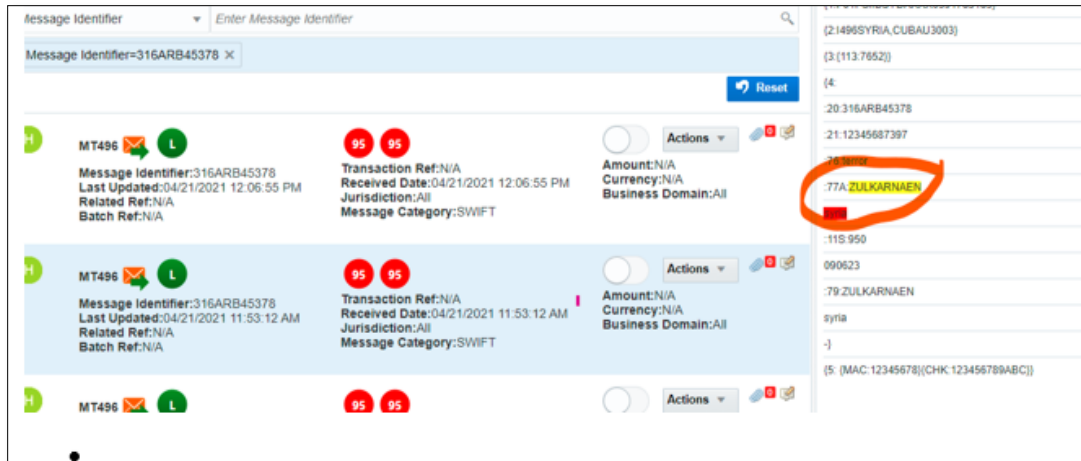
1. Click **Attach** . The *Attach a File* window is displayed.
2. Click the **Browse** button.
3. Select the file you want to attach.
4. Click **Save**.

### 4.3.2 Message and Audit Section

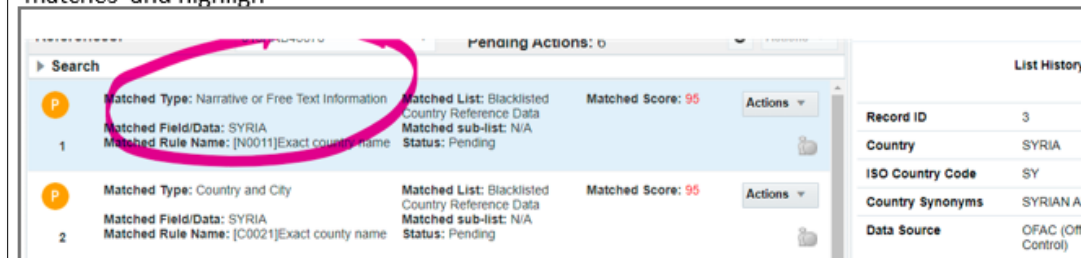
This section contains three tabs.

- **Raw Message:** The following image shows the different fields available for the SWIFT message in a raw format. The exact suspicious/ matched data is highlighted in Red and partially matched data is highlighted in Yellow.

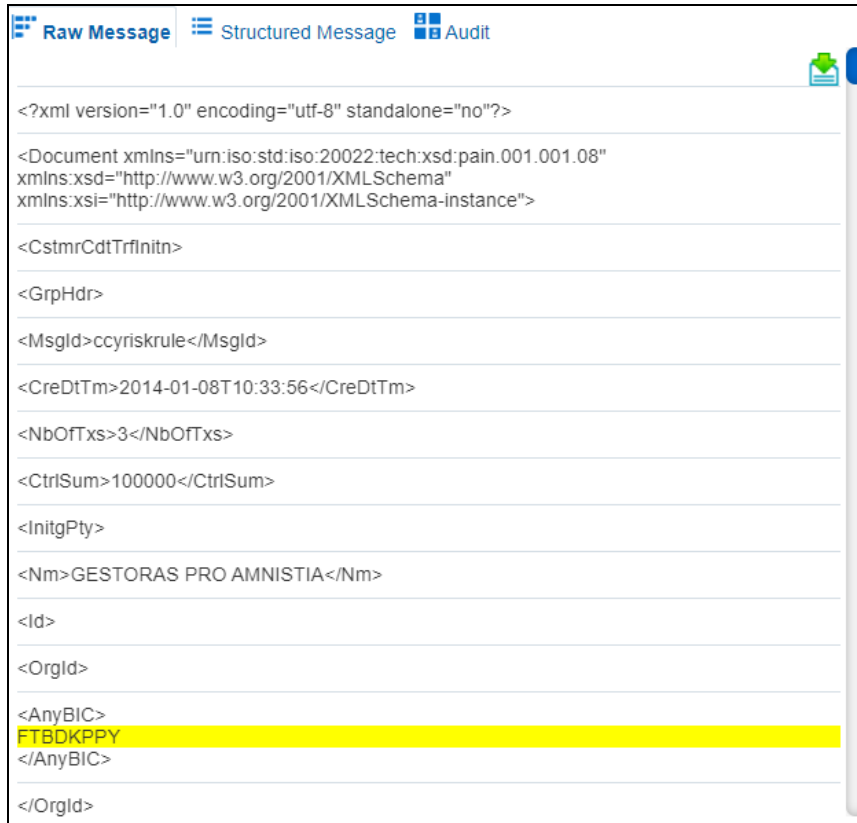
Figure 12: Raw Message Format for SWIFT



Matches getting only country and Highlight not for name only 77A tag . and for 79 tag not getting matches and highlight



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 13: Raw Message Format for ISO20022**

```
<?xml version="1.0" encoding="utf-8" standalone="no"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.08"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<CstmrCdtTrfInItn>
<GrpHdr>
<MsgId>ccyriskrule</MsgId>
<CreDtTm>2014-01-08T10:33:56</CreDtTm>
<NbOfTxs>3</NbOfTxs>
<CtrlSum>100000</CtrlSum>
<InitgPty>
<Nm>GESTORAS PRO AMNISTIA</Nm>
<Id>
<OrgId>
<AnyBIC>
FTBDKPPY
</AnyBIC>
</OrgId>
```

- To download the XML file, click **Download** .
- **Structured Message:** The following image shows the structured form of the message. This displays the important fields in a key-value format.

Figure 14: Structured Message Format for SWIFT

<span>Raw SWIFT</span> <span>Structured SWIFT</span> <span>Audit</span>	
	<b>Additional Details</b>
Sender:	CHASUS33XXX
Receiver:	ESSESESSXXX
Amount:	11100
Currency:	USD
Requested Execution Date:	2015-11-05 00:00:00.0
Originator Identifier:	/LV21HABA0551003219457
Originator Address:	GUSTAVO LIATANO MICKIEWICZ ULICA LOTWA MIASTO LV/LOTWA
Beneficiary Address:	ROBERT GABRIEL MUGABE ULICA SK/MIASTO
Destination Country:	SY
	<b>Additional Details</b>

Click **Additional Details** to view the message parameters. For more information on the message parameters, see [Oracle Financial Services Transaction Filtering Administration Guide](#).

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

- **Header Information:** Click this tab to view the transaction information such as the number of transactions, total transaction amount, user who initiated the transaction, date on which the batch was executed, and the country from where the amount originated.



Figure 15: Structured Message Format for ISO20022 – Header Information

Raw Message	Structured Message	Audit
<a href="#">Additional Details</a>		
<b>Header Information</b>   Transaction Information		
<b>Group Header</b>		
Message Control Sum Amount : 100000		
Message Number Of Transactions : 3		
<b>Initiating Party Details</b>		
Name : GESTORAS PRO AMNISTIA		
<b>Batch Header</b>		
Batch Control Sum Amount : 49		
Batch Number Of Transactions : 3		
Requested Execution Date : 2014-01-08		
Sender : SIIBSYDA		
Originator Country : SY		
<b>Debtor Details</b>		

- Transaction Information:** Click this tab to view the transaction ID, the destination country of the transaction, and the details of the user who received the transaction amount. 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 [Transaction Filtering Administration Guide](#).

**Figure 16: Structured Message Format for ISO20022 – Transaction Information**

Raw Message | **Structured Message** | Audit

Header Information | **Transaction Information** | Additional Details

**Transaction**

End to End Identifier : TXN11

Requested Execution Date : 2014-01-08

Receiver : SIIBSYDA

Destination Country : SY

**Creditor Details**

Name : ROBERT GABRIEL MUGABE

Address Town : Bangalore

Account : NL69INGB0123456789

Page 1 of 3 (1 of 3 items) | < > 1 2 3 > >

Additional Details

- **Audit:** You can see the last action of the user, the name of the user who performed the action, and the date and time the message was initiated. For example, if you attach a document, the following comment appears in the image:

**Figure 17: Audit Section**

Raw SWIFT	Structured SWIFT	Audit
TFANALYST	11/24/2020 6:07:31 PM	Attachment
Comments : Document Name- test Added		
TFANALYST	11/24/2020 6:05:48 PM	Assigned
Comments : Transaction is assigned		

### 4.3.3 Match Summary Section

This section lists all the matches, if any, for a message. In the case of multiple transactions within a message, matches get grouped under the respective alert reference for transaction-level match and message-level matches separately. You can review all matches in this section before blocking/releasing a message.

Select the transaction-level matches or message-level matches (common for all messages) by selecting **Transaction Reference** or **Message Reference** from the drop-down list:

- Matched Type
- Matched List
- Matched Sub List
- Match Score
- Matched Rule Name

For each of these messages, based on the information displayed, an Analyst can select one of the following actions from the **Actions** button in the Match Summary section, after unlocking the alert message in the **Alert Summary** section. For more information on locking and unlocking the alert, see [Locking the Alert](#).

- **Suspicious:** Select this action if the alert is suspicious.
- **Clean:** Select this action if the alert is clean.
- **Allow:** Select this action if the alert has some suspicious data but the transaction is allowed to go through.

To select an alert, unlock the alert in the **Alert Summary** section and select an action for the alert in the **Match Summary** section. The matches are displayed in a sequence. Use the numbers to keep a track of the matches you have worked on.


The following image displays an example.

**Figure 18: Match Summary Section**

Match ID	Matched Type	Matched Field/Data	Matched Rule Name	Matched List	Matched sub-list	Matched Score	Actions
1	EIC	FTEDKPPY	[B0011]Exact bank identification code (BIC) match	Sanctioned BIC	N/A	95	Actions
2	EIC	FTEDKPPY	[B0011]Exact bank identification code (BIC) match	Watchlist BIC	N/A	95	Actions
3	EIC	FTEDKPPY	[B0011]Exact bank identification code (BIC) match	Watchlist BIC	N/A	95	Actions
4	EIC	FTEDKPPY	[B0011]Exact bank identification code (BIC) match	Sanctioned BIC	N/A	95	Actions

### 4.3.4 List Details Section

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

You can also view the history of matches for a watch list record ID in the **Number of Hits**  counter. This counter displays the number of hits for a watch list record ID over a specified lookback period. You can select the lookback period from the dropdown list in the **List History** field.

In the following figure, the number of hits over the last 10 days is 12.

Figure 19: List Details Section

List Details	
List History:	Last 10 days <span>12</span>
Record ID	3
Country	SYRIA
ISO Country Code	SY
Country Synonyms	SYRIAN ARAB REPUBLIC
Data Source	OFAC (Office of Foreign Assets Control)

To see a detailed view of all hits, click **Number of Hits** 12. A **Detailed View** window appears.

Figure 20: Detailed View Window

The screenshot shows a 'Detailed View' window for Record ID: 3. It displays a list of four transaction hits. Each hit includes a message identifier (MT101), transaction reference number, received date, jurisdiction, and amount. Callouts highlight the 'Alert Status' (red 'B' icon), 'Hit Match Status' (red 'S' icon), and 'Hit Match Score' (yellow '98' icon). The right side of the window shows a 'Raw Message' tab with the full SWIFT message content.

Mouse over the icons to view the icon name. Close the **Detailed View** window to go back to the **List Details** section.

The details that are displayed in the **List Details** section depend on the type of sanctioned data that is found. This sanctioned data is based on the following search criteria:

- 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

### 4.3.5 Risk Summary Section

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


The following image displays an example:

**Figure 21: Risk Summary Section**

RiskSummary		MATCHSUMMARY
	Risk Rule: Risk-Watchlist Screening Evaluation	Risk Score: 85
	Risk Rule: Risk-Currency VS Amount Threshold Evaluation	Risk Score: 25
	Risk Rule: Risk-Currency VS Destination Country Evaluation	Risk Score: 90

Page 1 of 1 (1-3 of 3 items) | < 1 >

**Figure 22: Risk Details**

Risk Details	
List History : Last 10 days ▼	
	
Amount	11100
Currency	EUR
Destination Country	PK
Direction	OUTBOUND
Message Type	MT101
Transaction Reference	TRSCNREF0011

### 4.3.6 Notification and Reporting Section

This section displays the number of notifications when you log in to the system. This is displayed on the top right-hand corner of the application. The notifications that appear depend on the logged-in user role. You can see notifications for the following:

- Hold Transactions
- Escalated Transactions
- False Positive Transactions
- Overdue Transactions



Figure 23: Notification and Reporting Section




### 4.3.7 Good Guy Matching

A record can be added to the FCC\_WHITELIST table using the **Add to Good Guy** button in the **Match Summary** section. This button is initially green, and the color changes to grey after the record is added to the watch list table. This means that the record is now added to the allow list.

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

Figure 24: Good Guy Pop-up Window

Select the Jurisdiction and Expiry date for the record and click **OK**. The status of the record 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 below the message status and the **Add to Good Guy** button is disabled.

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 25: Good Guy List Details Page

The screenshot displays the 'Good Guy List Details Page' with two main sections: 'Good Guy Summary' and 'List History'.

**Good Guy Summary:** This section contains a table of three alerts. Each row includes a 'PA' button, a list of details (List Type, Jurisdiction, Listed On, Origin Record Id), and a set of detailed fields (Record ID, Identifier, Record Name, Last Updated, Origin, Expired On, and Origin Record Name). An 'Actions' dropdown menu is visible for each row.

PA	List Type: Good Guy Jurisdiction: US Listed On: 2018-07-03T18:18:14 Origin Record Id: 1	Record ID: 2235 Identifier: SK241111000002660919015 Last Updated: 2018-07-03T18:18:14 Origin: EU	Record Name: ROBERT GABRIEL MUGABE Origin Record Name: ROBERT GABRIEL MUGABE Expired On: 2018-07-19T00:00:00	Actions
PA	List Type: Good Guy Jurisdiction: INDA Listed On: 2018-07-03T16:15:45 Origin Record Id: SanT	Record ID: 2232 Identifier: SK22456 Last Updated: 1970-01-01T05:30:00 Origin: HMT	Record Name: KYC Origin Record Name: Santanu Expired On: 2018-07-28T00:00:00	Actions
PA	List Type: Good Guy Jurisdiction: INDA Listed On: 2018-07-04T15:54:57 Origin Record Id: E1164654	Record ID: 2237 Identifier: SK241111000006600619015 Last Updated: 2018-07-04T15:54:57 Origin: ACY	Record Name: ROBERT GABRIEL MUGABE Origin Record Name: ROBERT PETER JR MUGABE Expired On: 2018-07-31T00:00:00	Actions

Page 1 of 1 (1-3 of 3 items) | Search

**List History:** This section displays a list of historical alerts with similar details to the summary section.


**Match History:** This section shows 'No items to display'.

**Watchlist Details:** This section is currently empty.

**Topics:**

- [Good Guy Summary Section](#)
- [List History Section](#)
- [Approving or Rejecting Alerts](#)

**4.3.7.1 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** .

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:

- **Message Reference:** Enter or search for a message reference.
- **Message Type:** Enter or search for a message type.
- **Transaction Reference:** Enter or search for a transaction reference.
- **Match Score:** You can either select a score or a range of scores to display the respective messages by selecting Basic Search or Advanced Search respectively.
- **Risk Score:** You can either select a Risk score or a range of Risk scores to display the respective messages by selecting Basic Search or Advanced Search respectively.
- **Status:** Enter the status of a message.
- **Receipt Date:** You can either select a Receipt Date or a period range for the Receipt Date to display the respective messages.

To reset the search criteria, click **Refresh** .

### 4.3.7.2 List History Section

This section contains the following fields:

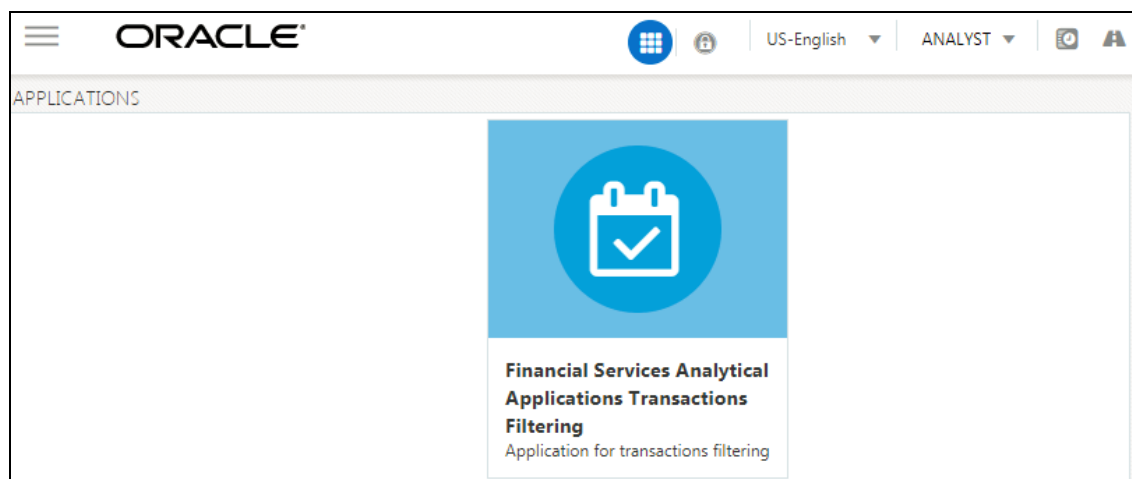
- List type
- Jurisdiction
- Record ID
- Expired on
- Origin
- Origin record ID
- Status
- Record name
- Origin record name

### 4.3.7.3 Approving or Rejecting Alerts

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

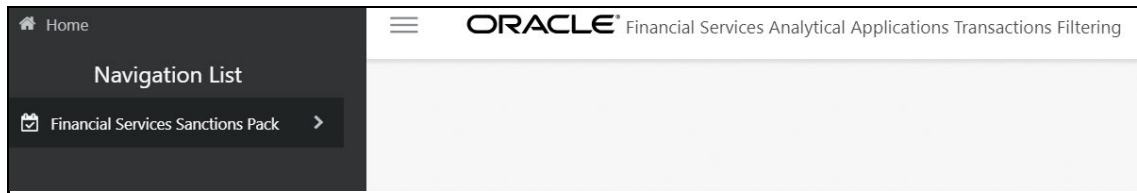
1. Log in to the **Financial Services Analytical Applications Transactions Filtering home page** as the Supervisor.
2. Click **Calendar** .

**Figure 26: Financial Services Analytical Applications Transactions Filtering Page**



3. Click **Financial Services Sanctions Pack**.


Figure 27: Financial Services Sanctions Pack Home Page



4. Click **List Management**. The **Good Guy List Details** page appears.

Figure 28: Financial Services Sanctions Pack Home Page – List Management



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.

## 4.4 Taking an Action on an Alert

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

- Blocked
- Released
- Escalated

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

- Recommend to Block
- Recommend to Release
- Escalated

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. For more information, see [Attaching a File to an Alert](#).

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

**Topics:**

- [Recommending to Block an Alert](#)
- [Recommending to Release an Alert](#)
- [Escalating an Alert](#)
- [Blocking an Alert](#)
- [Releasing an Alert](#)
- [Rejecting an Alert](#)
- [Alert Statuses](#)

#### 4.4.1 **Recommending to Block an Alert**

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Recommend to Block** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**. The status of the alert changes to **BR** (Block Recommended).

#### 4.4.2 **Recommending to Release an Alert**

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Recommend to Release** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**. The status of the alert changes to **RR** (Release Recommended). This alert is called a False Positive.
4. In the Match Summary section, if any of the matches in the alert is marked as suspicious, then a pop-up window is displayed when you release the alert. Click **OK** and change the status to Block Recommended or Escalated.

### 4.4.3 Escalating an Alert

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Escalate** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**. The status of the alert changes to **E** (Escalated).

### 4.4.4 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. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Block** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**. The status of the alert changes to **B** (Blocked).

### 4.4.5 Releasing an Alert

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Release** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**. The status of the alert changes to **R** (Released). This alert is called a False Positive.
4. In the **Match Summary** section, if any of the matches in the alert is marked as suspicious, then a pop-up window is displayed when you release the alert. Click **OK** and change the status to Block or Escalate.

### 4.4.6 Rejecting an Alert

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

1. Navigate to the **Financial Services Analytical Applications Transactions Filtering home page**. For more information, see [Accessing the OFSAA Applications](#).
2. Select **Reject** from the Actions drop-down list.
3. Provide comments to explain your analysis and click **Save**.
4. When you reject an alert, it is assigned back to the Analyst.

## 4.4.7 Alert Statuses

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

**Topics:**

- [Standard Flow For Analyst](#)
- [Standard Flow For Supervisor](#)
- [Four-Eyes Flow For Analyst](#)
- [Four-Eyes Flow For Supervisor](#)

### 4.4.7.1 Standard Flow For Analyst

- Hold
- Assigned
- Escalated
- Blocked
- Released

### 4.4.7.2 Standard Flow For Supervisor

- Escalated
- Blocked
- Released

### 4.4.7.3 Four-Eyes Flow For Analyst

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

### 4.4.7.4 Four-Eyes Flow For Supervisor

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

- Pending

## 4.5 Task Emails

The following emails are generated based on the actions selected:

**Table 4: Task Emails**

For a Task...	The task is assigned to the...
Which is Unassigned	Analyst
Where Analyst selects Recommend to Block action	Analyst and Supervisor
Where Analyst selects Recommend to Release action	Analyst and Supervisor
Where Analyst selects Escalated action	Analyst and Supervisor
Where Supervisor selects Reject action	Analyst
Where Analyst selects Block action	Analyst
Where Analyst selects Release action	Analyst
Where Supervisor selects Block action	Analyst and Supervisor
Where Supervisor selects Release action	Analyst and Supervisor



## 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 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 the My Oracle Support site that has all the revised/recently released documents.

