

# **Oracle Financial Services Customer Screening**

**User Guide**

**Release 8.1.2.2.0**

**June 2023**

**F47824-01**

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

Oracle Financial Services Customer Screening User Guide.

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

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

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

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

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

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

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

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

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

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

# Document Control

Table 1: Document Control

Revision No.	Revision Date	Change Log
8.1.2.2	October 2022	<ul style="list-style-type: none"><li>• Added information about Source Request ID attribute in <a href="#">Real-Time Screening</a> section.</li><li>• Added supported file formats for uploading an attachment to the alert list in <a href="#">Attaching a File to an Alert</a> section.</li></ul>

---

# Table of Contents

<b>1</b>	<b>Preface .....</b>	<b>3</b>
1.1	Who Should Use This Guide .....	3
1.2	How this Guide is Organized.....	3
1.3	Related Documents.....	3
1.4	Conventions .....	4
<b>2</b>	<b>About Customer Screening .....</b>	<b>5</b>
2.1	Introduction.....	5
2.2	Architecture Overview.....	5
2.3	Default Workflow.....	5
2.3.1	<i>Sanctions and Prohibition</i> .....	5
2.3.2	<i>Politically Exposed Person (PEP) and Enhanced Due Diligence (EDD)</i> .....	6
2.4	Features of Customer Screening .....	6
2.5	User Roles and Actions .....	7
<b>3</b>	<b>Getting Started .....</b>	<b>9</b>
3.1	Accessing OFSAA Page.....	9
3.2	Managing OFSAA Page.....	10
3.2.1	<i>Applications Tab</i> .....	10
3.2.2	<i>Changing the Application Password</i> .....	10
3.2.3	<i>Viewing the Application's Copyright Information</i> .....	11
3.3	Troubleshooting Your Display.....	12
3.3.1	<i>Enabling JavaScript</i> .....	12
3.3.2	<i>Enabling Cookies</i> .....	12
3.3.3	<i>Enabling Temporary Internet Files</i> .....	12
3.3.4	<i>Enabling File Downloads</i> .....	12
3.3.5	<i>Setting Print Options</i> .....	13
3.3.6	<i>Enabling the Pop-Up Blocker</i> .....	13
3.3.7	<i>Setting Home Page Preferences</i> .....	13
3.4	Logging in to the Customer Screening Application.....	14
3.4.1	<i>Related Alerts</i> .....	16

---

3.4.2	<i>Field Descriptions</i> .....	17
<b>4</b>	<b>Managing Customer Screening</b> .....	<b>19</b>
4.1	Real-Time Screening .....	19
4.1.1	<i>Creating a Case or Alert</i> .....	19
4.1.2	<i>Field Descriptions</i> .....	22
4.2	Queue Management.....	24
4.2.1	<i>List View</i> .....	24
4.2.2	<i>Grid View</i> .....	24
4.3	Alert List .....	26
4.3.1	<i>Managing the Alerts</i> .....	27
4.4	Alert Details .....	31
4.4.1	<i>Analyzing the Alert</i> .....	31
4.4.2	<i>Navigating to the Previous and Next Alert</i> .....	33
4.4.3	<i>Printing the Alert Details</i> .....	34
4.4.4	<i>Reload the Grid</i> .....	34
4.4.5	<i>Alert Summary</i> .....	34
4.4.6	<i>Events</i> .....	35
4.4.7	<i>External Entity Details and Corresponding Watchlist details</i> .....	37
4.4.8	<i>Candidate Details Corresponding Watchlist details</i> .....	37
4.4.9	<i>Customer Details Corresponding Watchlist Details</i> .....	37
4.4.10	<i>Alert Decision</i> .....	38
4.4.11	<i>Alert Status</i> .....	39
4.4.12	<i>Audit History</i> .....	39
4.4.13	<i>Related Alerts</i> .....	41
4.4.14	<i>Field Descriptions</i> .....	43
<b>5</b>	<b>OFSAA Support Contact Details</b> .....	<b>46</b>
<b>6</b>	<b>Send Us Your Comments</b> .....	<b>47</b>

# 1 Preface

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

## 1.1 Who Should Use This Guide

The Customer Screening 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.
- **Senior Supervisor:** This user works on the alerts within the application with additional functionalities such as a Bulk update, set priorities, and change Due Date Time.

## 1.2 How this Guide is Organized

The Customer Screening User Guide includes the following chapters:

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

## 1.3 Related Documents

For more information about Oracle Financial Services Customer Screening, 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
- Customer Screening Administration Guide
- Customer Screening Data Interface Guide
- Customer Screening Matching Guide

These documents are available at the following links:

- [Sanctions Application Pack home page](#)
- [Customer Screening Guides home page](#)

To find more information about Oracle Financial Services Customer Screening and our complete product line, visit our Website at [Oracle for Financial Services home page](#).

## 1.4 Conventions

Table 1 lists the text conventions used in this guide

**Table 1: Conventions**

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

## 2 About Customer Screening

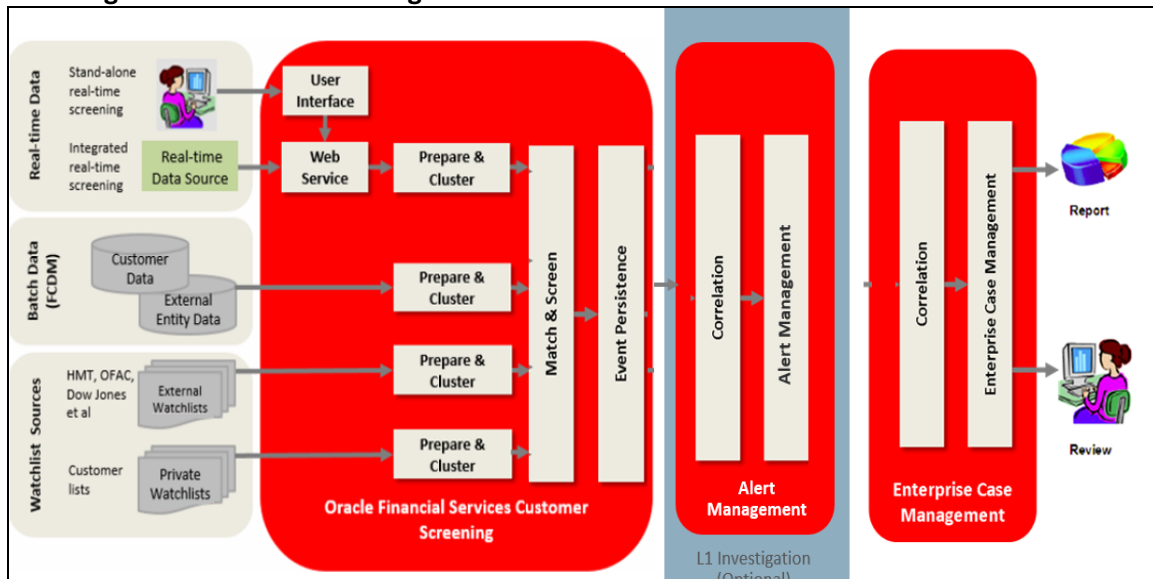
### 2.1 Introduction

Oracle Financial Services Customer Screening (OFS CS) enables organizations to effectively and efficiently screen their customers to meet anti-bribery, anti-corruption, export control, and other legal regulations and meet anti-money laundering counter-terrorism financing legislation. Screening customers enables organizations to keep track of and avoid the risk of being exposed to suspicious or sanctioned individuals and organizations. Customer Screening uses the Oracle Enterprise Data Quality (OEDQ) platform to manage watch list data and apply match rules, Process Modelling Framework (PMF) to generate alerts, and Enterprise Case Management (ECM) to investigate cases generated from the alerts based on the match rules.

### 2.2 Architecture Overview

This image shows data movement from a real-time data source, batch data from the Financial Crime Data Model (FCDM), and data from watch list sources such as OFAC, HM Treasury, and Dow Jones. This data then moves to the Customer Screening user interface, where it is prepared and screened. Finally, alerts or cases are generated based on Alert Management or Enterprise Case Management matches, respectively.

**Figure 1: Customer Screening Architecture**



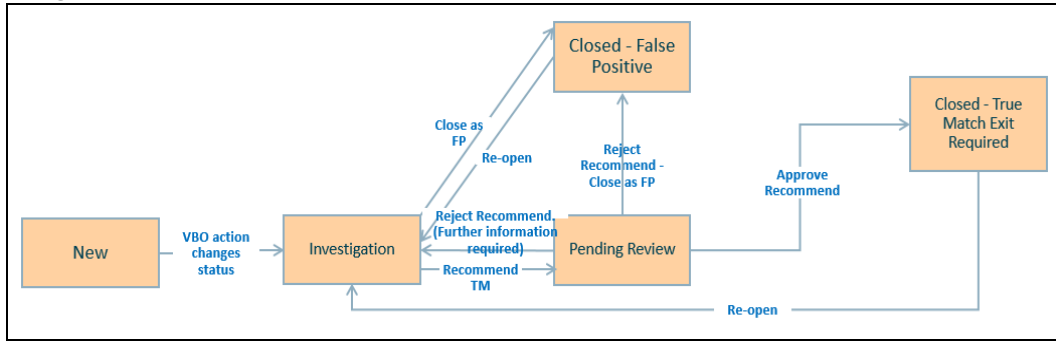
### 2.3 Default Workflow

The workflow is applicable only for L1 investigation.

#### 1.3.1 Sanctions and Prohibition



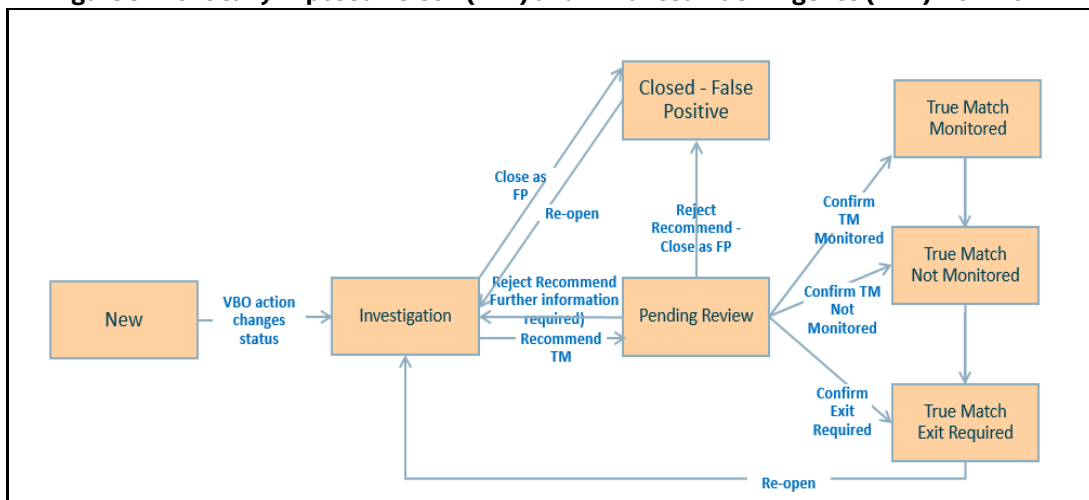
**Figure 2: Sanctions and Prohibited workflow**



**NOTE** Escalated is enabled only when L2 Investigation enabled.

### 2.3.2 Politically Exposed Person (PEP) and Enhanced Due Diligence (EDD)

**Figure 3: Politically Exposed Person (PEP) and Enhanced Due Diligence (EDD) workflow**



**NOTE** Escalated is enabled only when L2 Investigation enabled.

## 2.4 Features of Customer Screening

The following are the key features of Customer Screening:

- Batch and real-time screening.
- Batch screening generates alerts from the different screening sources. For details on screening sources, see the *OFS Customer Screening Administrator Guide*.
- Advanced data preparation techniques.
- Sophisticated matching algorithms, with over 450 standard match rules.
- Customized workflow tailored for compliance investigations.

- Rapid Disposition of Alerts in Alert Management.
- Risk and match scoring published to Alert or Case Management.
- Rapid Disposition of Alerts in L1 (Alert Management)
- Support for multiple list data sources, including HMT, OFAC, EU, UN, Accuity, Dow Jones (Factiva), private blacklists, and World-Check (Thomson Reuters).
- Plug-in language packs and transliteration support multiple writing systems.
- The optional country packs offering name and geographical reference data.

## 2.5 User Roles and Actions

The following user roles are defined in OFS Customer Screening:

- Analyst
- Supervisor
- Senior Supervisor
- Queue Administrator

---

**NOTE**

Analyst, Supervisor, and Senior Supervisor roles are for L1 investigation. 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 Customer Screening application:

**Table 2** lists the User Roles and Actions.

**Table 2: User Roles and Actions**

Action	Analyst	Supervisor	Senior Supervisor	Queue Administrator
<b>Queue Level</b>				
Add				X
Edit				X
Assign				X
Delete				X
Open	X	X	X	
<b>Alert Level</b>				
Access to View UI	X	X	X	
Recommend True Match	X			
Close as False Positive	X			
Re-Open		X		
Approve Recommended		X		
Reject as False Positive		X		
Confirm TM Monitored		X		
Confirm TM Not Monitored		X		
Confirm Exit Required		X		
<b>Real-Time Screening UI</b>				
Scan	X	X		
Scan and Investigate	X	X		
<b>Customer Screening Alert List</b>				
Bulk Update:			X	
1. Assign Alerts				
2. Change the Priority				
3. Change Due Date Time				
Add attachments	X	X	X	
<b>Event Level</b>				
True Positive	X	X		
False Positive	X	X		

**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 Customer Screening 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:

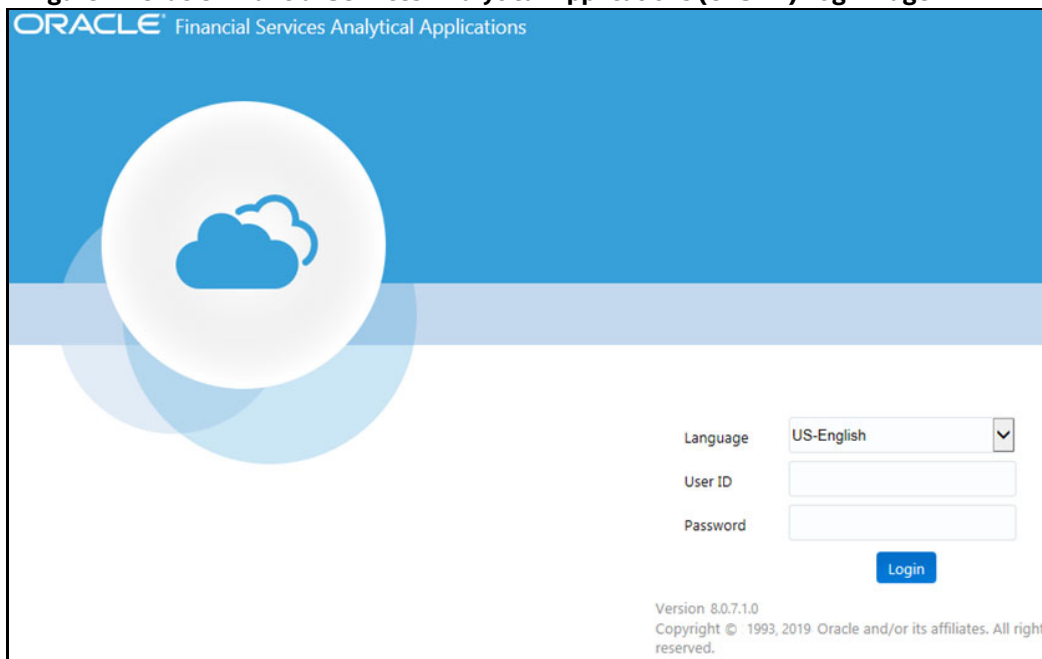
1. Enter the URL into your browser using the following format:

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

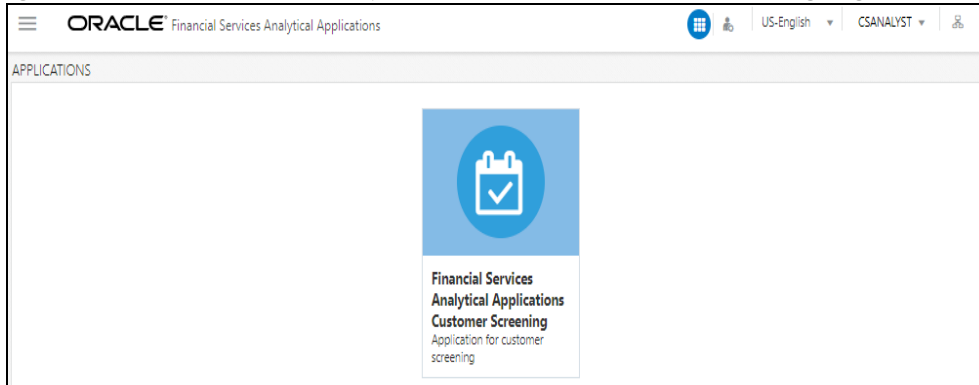
For example: `https://myserver:9080/ofsaaapp/login.jsp`

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

**Figure 4: 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 Customer Screening** home page is displayed.

**Figure 5: Financial Services Analytical Applications Customer Screening Page**

To view the **Financial Services Analytical Applications Customer Screening** 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.

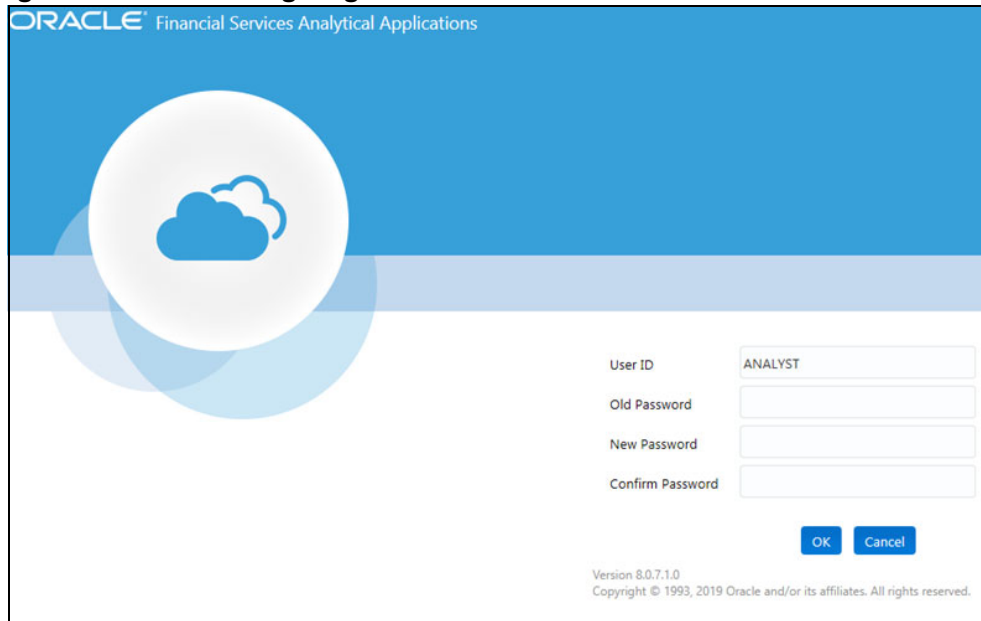
For example, to access the OFSAA Applications, select the required Application from the **Select Application** drop-down list. Based on your selection, the page refreshes the menus and links across the panes.

### 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 6: Password Change Page**


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

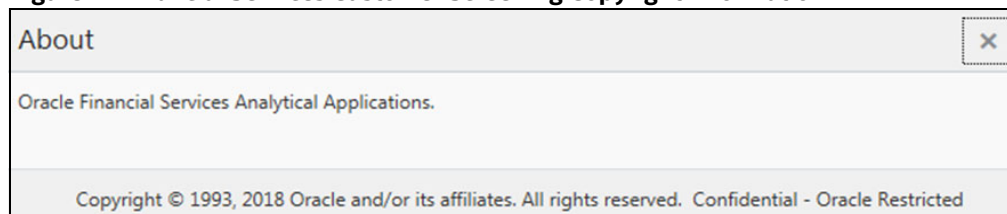
**NOTE**


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

### 3.2.3 Viewing the Application's Copyright Information

To access copyright information, follow these steps:

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

**Figure 7: Financial Services Customer Screening Copyright Information**

3. 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.

### 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 8: Financial Services Customer Screening Preferences Page**

Preferences

▼ Home Page

Property Name	Property Value
Set My Home Page	Default Screen ▼

Save Cancel

- In the **Property Value** drop-down list, select the application that 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.

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

## 3.4 Logging in to the Customer Screening Application

You can access the Customer Screening (CS) 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 Customer Screening application, follow these steps:

- Navigate to the **Oracle Financial Services Analytical Applications** page.
- Click Financial Services Sanctions Pack.
- Click **Customer Screening**. The L1 Investigation User Interface page is displayed.

Figure 9: Audit History

Updated By	Date and Time	Action	Event Id	Owner	Previous Owner	Resulting Status	Comments	
CSSUPERVISOR	03/24/2022 12:03:39	Reject Recommend		CSSUPERVISOR		Investigation	testing	0
CSSUPERVISOR	03/24/2022 12:03:30	False Positive	11004	CSSUPERVISOR		Pending Review	Country Mismatch	0
CSANALYST1	03/24/2022 11:07:12	Recommend True Match		CSANALYST1		Pending Review	testing	0
CSANALYST	03/24/2022 11:05:56			CSANALYST		Pending Test Review	testing	0
CSANALYST	03/24/2022 11:05:42	True Positive	11004	CSANALYST		Investigation	City Match	0
CSANALYST	03/24/2022 10:15:42	Alert Status Change		CSANALYST		Investigation	Alert status changed to Investigation	0
csanalyst	03/23/2022 08:17:52	New Alert Created				New		0

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

- Updated By
- Date and Time
- Action
- Event Id
- Owner
- Previous Owner
- Resulting Status
- Comments
- Attachments

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.

Table 3 lists the Field descriptions for Audit History.

**Table 3: Field descriptions for Audit History**

Fields	Description
Updated By	Displays the name of the person who updated the Alert.
Date and Time	Displays the date-time details when the actions are performed on the Alert.
Action	Displays the action taken on the Alert.
Event ID	Displays the unique id that was created for the event.
Owner	Displays the name of the owner who created the alert audit history.
Previous Owner	Displays the name of the previous owner of the Alert.
Resulting Status	Displays the resulting status value of the Alert.
Comments	Displays the details of the comments that are added to the audit history.
Attachments	Displays the details of the attachment, if any, are added to the audit history of the Alert.

### 3.4.0.1 Exporting the details 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.

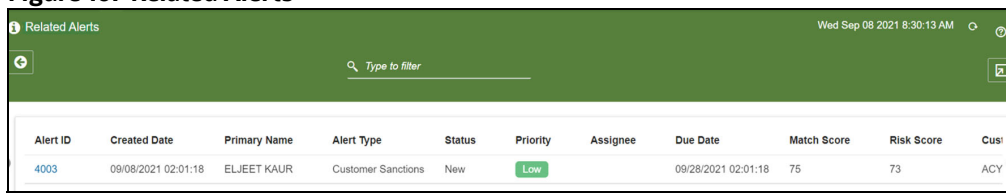
### 3.4.1 Related Alerts

This section displays the related alerts list based on party relationships, such as the alerts for the same customer/EE and alerts sharing a parent id based on security attributes.

The latest relationships are to be considered as related customers/EE. Relationships are to be looked at in both directions. i.e., if C1 is related to R1 when looking at C1, all C1 and R1 alerts are to be displayed (Except the current Alert), and if we are looking at R1, All alerts of R1 and C1 are the be displayed.

Also, it shows the relationship between the alerting customer/EE/Response ID and the parent id in the Related Alerts.

**Figure 10: Related Alerts**



Alert ID	Created Date	Primary Name	Alert Type	Status	Priority	Assignee	Due Date	Match Score	Risk Score	Cust
4003	09/08/2021 02:01:18	ELJEET KAUR	Customer Sanctions	New	Low		09/28/2021 02:01:18	75	73	ACV

This section contains the following components:

- Alert ID
- Created Date
- Primary Name
- Alert Type

- Status
- Priority
- Assignee
- Due Date
- Match Score
- Risk Score
- Customer ID

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.

**Table 4** lists the Field descriptions for Related Alerts.

**Table 4: Field descriptions for Related Alerts**

Field	Descriptions
Alert ID	Displays the alert identification number.
Created Date	Displays the Date the Alert was created.
Primary Name	Displays the Primary Name of the Customer.
Alert Type	Displays the type of Alert.
Status	Displays the status of the Alert.
Priority	Displays the priority value of the Alert.
Assignee	Displays the assignee name of the Alert.
Due Date	Displays the due Date the Alert has to review.
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.

### 3.4.1.1 Exporting the Related 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.

### 3.4.2 Field Descriptions

Table 5 lists the Field descriptions for Alert Details.

**Table 5: Field descriptions for Alert Details**

Field	Description
Case ID	Displays the unique Identification Number of the Case.
Created Date	Displays the Date the Alert was created.
Primary Name	Display 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.
Screening Type	Displays the type of screening, either Batch or Real-Time screening.
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 Business domain the Alert belongs to
Jurisdiction	Displays the Jurisdiction of the Alert belongs to.
Customer/EE/ Response ID	Displays the Customer/External Entity ID/Response ID.
From Date	Displays the Date the Alert is from.
To Date	Displays the Date the Alert was sent to.
Due Date Time	Displays the due date value of the Alert.
Watchlist ID	Displays the unique id assigned to batch.
List Type	Displays the type of watchlist.
Event Type	Displays the type of the event.
Matched Rule Name	Displays rules against which match is generated.
Watch List Primary Name	Displays the primary name of watch list data.

## 4 Managing Customer Screening

This chapter describes the concept and process of analyzing the alerts for L1 investigation. It provides instructions to carry out various actions according to the workflow and user roles using the Investigation User Interface page.

There are two ways to perform screening in the Customer Screening application:

- Real-time Screening

Real-time screening is the screening of individuals and entities that occur when you enter data in the Real-Time Screening page and click Scan & Investigate. When you screen data in real-time, you can see the screening results after running the real-time screening job. For more information, see **Running the Real-Time Screening Job** in the *OFS Customer Screening Administrator Guide*.

- Batch Screening

Batch screening is the screening of individuals and entities that occur when you run the batch screening job. Before running the job, you must first configure the Enterprise Data Quality (Director) details and then prepare and analyze the customer screening and external entity data in the Financial Crime Data Model (FCDM). For more information, see the *OFS Customer Screening Administrator Guide*.

### 4.1 Real-Time Screening

Real-time screening is the screening of individuals and entities that occur when you enter data in the Real-Time Screening page and click Scan & Investigate to see the screening results and details of Alert generation or Case creation. You can also view the Alert details or Case details from screening results.

**NOTE**

Creating an Alert or Case is configurable. The Alert or Case will be generated when you select CSAM or ECM, respectively, while configuring EDQ URL. To enable Scan & Investigate, map the role Scan & Investigate to CSRTGRP group. For more details, see Configuring the EDQ URL section in the *OFS Customer Screening Administrator Guide*.

#### 4.1.1 Creating a Case or Alert

To screen watch list records and to create an Alert or Case, follow these steps:

1. Log on to the Customer Screening application.

**NOTE**

The user who has permission to do the RT screening OOB.

2. Click Real-Time Screening. The Real-Time Screening page appears.

3. In the **Real-Time Screening** page, select the search type as **Individual** or **Entity**.

**NOTE**

- When L1 Investigation is CSAM, the `fcc_zcs_security_attr_grp_map` table must be populated to populate the business domain and jurisdiction.
- When L1 Investigation is ECM, the ECM security mapper batch must be executed to populate the business domain and jurisdiction.

4. Enter/Select values for the fields.

- Individual:

- Given Name
- Family Name
- Original Script Name:
- Date of Birth
- Jurisdiction (Mandatory)
- Business Domain (Mandatory)
- City
- Passport Number
- Address Country
- Residency Country
- Nationalities
- Passport Issuing Country
- Country of Birth
- External ID Type
- External ID
- Identification Numbers
- Source Request ID

**NOTE**

- The combination of Given Name and Family Name or Original Script Name or Passport Number along with Jurisdiction and Business Domain must be provided to Scan or Scan & Investigate.
- The External ID Type and External ID are the additional details to identify the RT request. External ID Type and External ID are not used in EDQ for screening. Using the external ID, cases can be searched in the case list in ECM.

- Entity

- Entity Name

- Original Script Name:
- Identification Numbers
- Jurisdiction
- Business Domain
- Registration Country
- External Type
- External ID
- City
- Operating Countries:
- Address Country
- Source Request ID

**NOTE** The combination of Entity Name or Original Script Name along with Jurisdiction and Business Domain must be provided to Scan or Scan & Investigate.

For details on fields, see the [Field Descriptions](#) section.

5. Perform the following for **Individual** or **Entity**:
  - a. Click **Scan**. It displays the screened watch list records.
  - b. Click **Scan & Investigate**. It generates an alert or case based on the configurations. The alert ID or Case ID results are displayed:
    - **Individual:**

**Figure 11: Real-Time Screening for Individual**

The screenshot shows the Oracle Financial Services Analytical Applications Customer Screening interface. The search type is set to 'Individual'. The form includes fields for Given Names (DO CHUCK), Family Names (PAK), Original Script Name, Date of Birth, Jurisdiction (Asia Pacific), Business Domain (GEN), City, Passport Number, Address Country, Residency Country, Nationalities, Passport Issuing Country, Country of Birth, External ID Type, External ID, and Identification Numbers. Below the form, there are buttons for 'Scan', 'Scan & Investigate', and 'Clear'. A notification indicates '1 Alert created with 1 events'. Below this, a table displays the search results:

List Key	Record Type	Name Type	Primary Name	Full Name	Original Script Name	Watchlist ID	Match Rule	Match Score	Country	Nationality
D/W	SAN	Spelling Variation	To-Chun Pak	DO CHUN PAK		1103612	[0700] Given name similar and sounds like only	80	KP	KP

Page: 1 of 1 (1 of 1 items)

- **Entity**



**Figure 12: Real-Time Screening for Entity**

The screenshot shows the Oracle Financial Services Analytical Applications Customer Screening interface. At the top, there is a navigation bar with the Oracle logo and the text "Financial Services Analytical Applications Customer Screening". Below this, there are options for "Select the search type" with radio buttons for "Individual" and "Entity" (selected). The search form includes several fields: "Entity Name \*" (MAITLAND CAPITAL LTD), "Jurisdiction \*" (Americas), "External Type", "Operating Countries", "Original Script Name", "Business Domain \*" (GEN), "External ID", "Address Country", "Identification Numbers", "Registration Country", and "City". Below the form are buttons for "Scan", "Scan & Investigate", and "Clear". A notification message states "1 Alert created with 1 events". Below the notification, the "Alert ID: 352" and "Record Type: EDD" are displayed. A table shows the search results with columns: List Key, Record Type, Name Type, Primary Name, Entity Name, Original Script Name, Watchlist ID, Match Rule, and Match Score. The table contains one row with the following data: DJW, EDD, Primary Name, Maitland Capital Ltd., Maitland Capital Ltd., [E010D] Part-standardized name exact only, 1031121, [E010D] Part-standardized name exact only, 92. At the bottom right of the table, it says "Page 1 of 1 (1 of 1 items)".

You can view generated alert ID or Case ID in the results and click Alert ID or Case ID to view the Alert Details or Case Details page, respectively.

6. Click **Clear** to clear the field data and re-enter.

## 4.1.2 Field Descriptions

Table 6 lists the Field description for Real-Time Screening

**Table 6: Field description for Real-Time Screening**

Field	Description
Given Name	Enter the first name of the Individual.
Entity Name	Enter the entity name.
Family Name	Enter the family name of the Individual.
Jurisdiction	Select the Jurisdiction to which the Individual or Entity belongs.
Business Domain	Select the business domain to which the Individual or Entity belongs.
Original Script Name	Enter the Individual or Entity's name in the original script if the script is a non-Latin script.
Address Country	Enter the current address of the Individual or Entity.
Country of Birth	Enter the country code in which the Individual was born, or the Entity originated. This field is applicable only when you select the search type as Individual.
Residency Country	Enter the country code of residence of the Individual or Entity. This field is applicable only when you select the search type as Individual.
Operating Countries	Enter the country codes the Entity operates in. To add more than one country code, add a comma between the countries. For example, the US, IN. This field is applicable only when you select the search type as Entity.
Registration Country	Enter the country code the Entity is registered in. This field is applicable only when you select the search type as Entity.
External ID Type*	Select the external ID type of the Individual or Entity.
External Type	Enter the city of residence of the Individual or Entity.
City	Enter the city of residence of the Individual or Entity.
Nationalities	Enter the nationality country code of the Individual. This field is applicable only when you select the search type as Individual.
External ID*	Enter the external ID unique to the Individual or Entity.
Date of Birth	Enter the Date of birth of the Individual. This field is applicable only when you select the search type as Individual.
Passport Number	Enter the passport number of the Individual.
Passport Issuing Country	Enter the country code in which the passport is issued.
Identification Numbers	Enter the identification numbers of the Individual or Entity.
Operating Countries	Enter the identification numbers of the Individual or Entity.
Source Request ID	Enter the request identification number of the Individual or Entity.
<p><b>NOTE:</b> The External ID Type and External ID are the additional details to identify the RT request. External ID Type and External ID are not used in EDQ for screening. Using the external ID, cases can be searched in the case list in ECM.</p>	

## 4.2 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):

- Analyst
- Supervisor
- Senior Supervisor

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](#).

### 4.2.1 List View

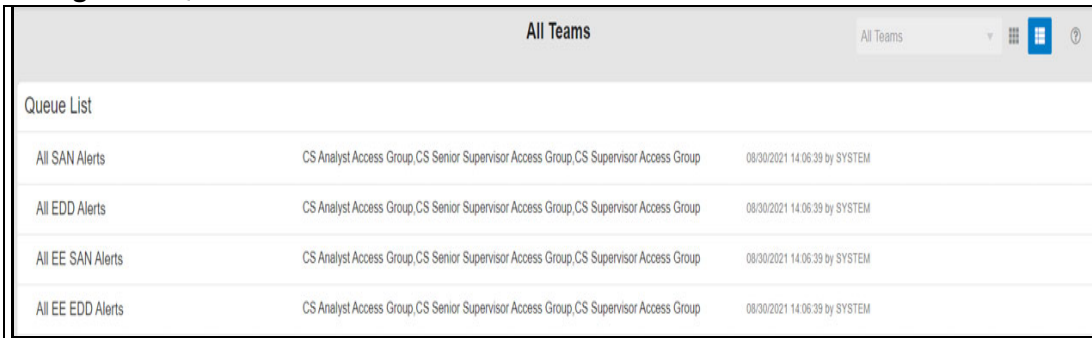
1. Log in to the application as Analyst/Supervisor/Senior Supervisor.
2. Select the **Financial Services Analytical Applications Customer Screening**.
3. From the **Application Navigation List**, select **Queue Management**.

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 13: Queue List in List View**



All Teams		
Queue List		
All SAN Alerts	CS Analyst Access Group, CS Senior Supervisor Access Group, CS Supervisor Access Group	08/30/2021 14:06:39 by SYSTEM
All EDD Alerts	CS Analyst Access Group, CS Senior Supervisor Access Group, CS Supervisor Access Group	08/30/2021 14:06:39 by SYSTEM
All EE SAN Alerts	CS Analyst Access Group, CS Senior Supervisor Access Group, CS Supervisor Access Group	08/30/2021 14:06:39 by SYSTEM
All EE EDD Alerts	CS Analyst Access Group, CS Senior Supervisor Access Group, CS Supervisor Access Group	08/30/2021 14:06:39 by SYSTEM

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)

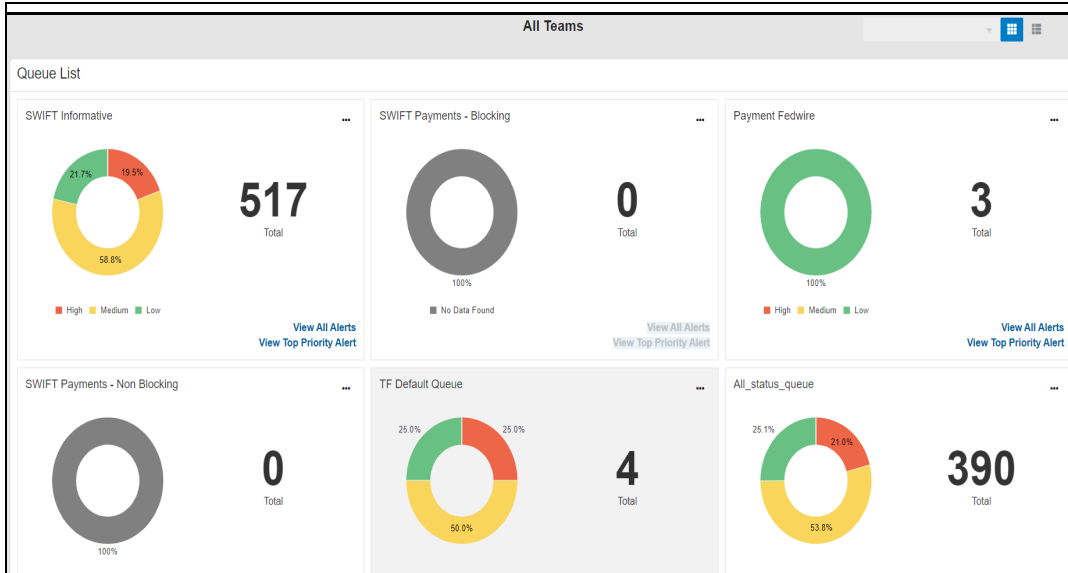
You can view ten queues in the Queue List and use the navigation to view the next set of queues.

### 4.2.2 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 14: 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

The priorities configuration for all the alerts is to be defined before running the batch or real-time screening.

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.

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 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.

### 4.3 Alert List

The Alert List page displays a list of alerts assigned to the Analyst/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.

1. Log on to the application.
2. Select the **Financial Services Customer Screening** Application.
3. From the **Navigation List**, select **Financial Services Sanctions Pack**.
4. Select the **Customer Screening Alert List**. The Alert List details appear.

**Figure 15: Alert List**

Alert ID	Created Date	Primary Name	Status	Priority	Alert Type	Assignee	Due Date	Match Score	Risk Score
2013	09/14/2021 11:50:27	Ismail Abdul Saah HANIYA	Pending Review	Medium	Real time Sanctions		01/12/2022 11:50:27	85	90
2009	09/14/2021 10:26:36	BANK OF INDUSTRY AND MINE (OF IRAN)	Pending Review	High	Real time Sanctions	CSSUPERVISOR	01/12/2022 10:26:36	96	95
2007	09/14/2021 10:22:49	Fathi Mohammed QARAWI	New	High	Real time Sanctions		01/12/2022 10:22:49	93	80
2006	09/14/2021 10:19:55	Ahmad Yousef ABU HALABIYYE	New	High	Real time Sanctions		01/12/2022 10:19:55	96	80
2001	09/14/2021 09:16:22	RAFAEL ENRIQUE BASTARDO MENDOZA	New	Medium	Real time Sanctions	CSANALYST	01/12/2022 09:16:22	85	92
1002	09/14/2021 06:31:14	MUHAMMAD MUHAMMAD	New	Low	Real time Sanctions		01/12/2022 06:31:14	77	100
1001	09/14/2021 06:30:19	MUHAMMAD MUHAMMAD	New	Low	Real time Sanctions		01/12/2022 06:30:19	77	100
1	09/14/2021 02:41:54	HAR MOHAN SING	Closed - True Match Exit Required	Low	Customer Sanctions	CSSUPERVISOR	01/12/2022 02:41:54	75	73

The alerts types are categorized as follows:

- Alerts from Customer:
  - Customer Sanctions
  - Customer Politically Exposed Person
  - Customer Enhanced Due Diligence
  - Customer Prohibition
- Alerts from External Entity:
  - External Entity Sanctions
  - External Entity Politically Exposed Person
  - External Entity Enhanced Due Diligence
  - External Entity Prohibition
- Alerts from Real-Time screening:
- Real time Sanctions
- Real time Politically Exposed Person
- Real time Enhanced Due Diligence
- Real time Prohibition

This section contains the following default field details:

- Alert ID
- Created Date
- Primary Name
- Status
- Priority
- Alert Type
- Assignee
- Due Date
- Match Score
- Risk Score

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

- Customer ID
- Screening Type
- Decision
- Comments
- Standard Comments
- Domain
- Jurisdiction

### **4.3.1 Managing the Alerts**

You can perform 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
- Customizing the Field Columns
- Saving the View
- Managing Views
- Closed Alerts
- Exporting the Alerts from the List
- Reload the Grid

#### **4.3.1.1 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.

- Customer/EE/Response ID
- Alert Type
- Alert ID
- Primary Name
- Priority
- Assignee
- Status
- Match Score
- Risk Score
- Decision
- Standard Comments
- Domain
- jurisdiction
- Created Date Range
  - From Date
  - To Date

#### **4.3.1.2 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 (Ascending/Descending).

### 4.3.1.3 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:

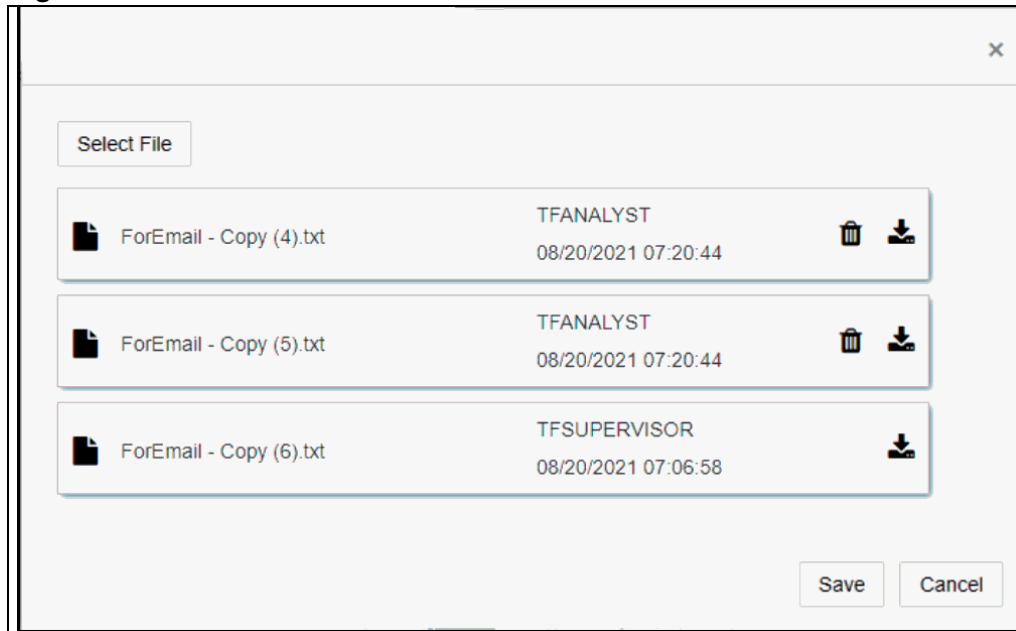
- Due Date Time
- Priority
- Assignee

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

### 4.3.1.4 Attaching a File to an Alert

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

**Figure 16: 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.



- Click **Download** icon next to the **Delete** icon to download the attachment.

**NOTE**

- The maximum allowed size for the attachment is 9MB.
- The Attachments uploaded by other users cannot be deleted.
- The supported file formats for uploading an attachment to the alert list are txt, pdf, doc, Doc, html, htm, xls, zip, jar, xml, jpg, bmp, and jpeg. You can allow more formats by modifying the configuration table in Conig Schema.

#### 4.3.1.5 Defining the View

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

- Click **Columns** button. The Filter Columns window appears.
- Click **My Default** to set the default columns in the list.
- You can filter the field data with the Search toolbar and select or select the fields from the list.
- Click **Restore Defaults** to restore the selected fields by default.
- Click **Save** to save your preference.

#### 4.3.1.6 Saving the View


You can add the customized view to the views list by saving it. Follow these steps:

- Click **Save View** button. The Save View window is displayed.
- Enter the name of the view.
- Optionally, click the **Set as default** view check-box to set the current view as default.
- Click **Save**.

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

#### 4.3.1.7 Managing Views

To manage the views, follow these steps:

- Click **DEFAULT/<View Name>** button. The Views window is displayed.
- 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.
- The **Manage Views** window appears. You can find the View Name and the list of field columns details.
- Click on any of the View Name or Columns to sort the views list.
- You can delete any of the views from the list by clicking on the **Delete**  icon in the list.


#### 4.3.1.8 Closed Alerts


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

To come back to the previous screen, click on Reload  icon.

By default, the logged-in Analyst can only see the alerts they have closed. To see the alerts closed by all analysts, click **Closed Alerts** on the Alert List page.

### 4.3.1.9 Exporting the Alerts from the List

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

### 4.3.1.10 Reload the Grid

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

### 4.3.1.11 Field Descriptions

Table 7 lists the Field Description for Alert List.

**Table 7: Field Description for Alert List**

Field	Description
Alert ID	Displays the unique Identification Number of the 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.
Screening Type	Displays the type of screening, either Batch or Real-Time screening.
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.

## 4.4 Alert Details

### 4.4.1 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 and the Senior Supervisor or vice-versa. The Alert will be unlocked automatically when the user completes his actions and moves to any other alert.

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
- Events
- External Entity Details (External Entity Alerts)
- Customer Details (Customer Screening Alerts)
- Candidate Details (Real-Time Alerts)
- Alert Decision
- Alert Status
- Audit History
- Related Alerts

---


**NOTE**

The Alert Decision will be enabled only when you close all events in the Alert.


Figure 17: Alert Details

The screenshot displays the 'Alert 2011' details page. At the top, there are navigation links for 'Audit History' and 'Related Alerts', and a timestamp 'Thu Sep 16 2021 12:58:07 PM'. The main header includes a search bar 'Type to filter' and a 'Match Score' dropdown. The 'Alert Summary' section contains a table with fields: Primary Name (BANK REFAH KARGARAN), Alert Type, Real time Sanctions, Assignee (CSANALYST), Screening Type (Online), Jurisdiction (Americas), Decision, Match Score (95), Risk Score (88), Investigation (1), and Created Date (09/14/2021 10:30:41). Below this is the 'Events' section with a 'Bulk Update [ 0 ]' button and a table showing a 'False Positive' event with a match score of 95 and risk score of 88. The 'Candidate Details' and 'Watchlist Details' sections provide further information about the entity and watchlist. The 'Alert Decision' section at the bottom offers options to 'Recommend True Match' or 'Close as False Positive', along with text boxes for 'Standard Comments' and 'Comments', and an 'Attachments' section with an 'Attach File' button.

### 4.4.2 Navigating to the 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.

### 4.4.3 Printing the Alert Details

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

### 4.4.4 Reload the Grid

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

### 4.4.5 Alert Summary

**Figure 18: Alert Summary Section**

Alert Summary					
Primary Name	BANK REFAH KARGARAN	Alert Type	Real time Sanctions	Assignee	CSANALYST
Screening Type	Online	Jurisdiction	Americas	Decision	
Created Date	09/14/2021 10:30:41	Business Domain	General	Comments	
		Due Date Time	118d 8h 29m 34s	Attachments	
				Match Score	95
				Risk Score	88
				Investigation	1
					<b>High</b>

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



- Primary Name
- Screening Type
- Created Date
- Alert Type
- Jurisdiction
- Business Name
- Due Date Time
- Assignee
- Decision
- Comments
- Attachments
- Created Date
- Comments
- 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.

## 4.4.6 Events

Figure 19: Events

List Type	Event Type	Matched Rule Name	Watchlist Primary Name	Watchlist ID	Event ID	Match Score	Risk Score	
OFAC	OFAC-NS-PLC	(E010E) Part-standardized name exact, city (E080E) Name without suffixes starts with and multiple names in common, city		2025	2025	95	88	 


Page 1 of 1 (1 of 1 items)   

This section displays the list of events along with their details in the Alert in the following components:

- List Type
- Event Type
- Matched Rule Name
- Watch List Primary Name
- Watch List ID
- Event ID
- Match Score
- Risk Score
- Edit Comments Icon

### 4.4.6.1 Search Filters



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

- Enter the value in the Search Filter.
- From the Filter menu, select the Match Score/Risk Score.
- Click the Sort  icon to sort the search criteria in ascending and descending order.

You can perform the following actions on the Events:


### 4.4.6.2 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**.
4. Click the **Comments**  icon in an Event to edit a comment and click **Save**.

### 4.4.6.3 Adding False Positive to an Event


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

1. Click the **False Positive**  icon next to the Risk Score. 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 event will be marked with

**False Positive**

#### 4.4.6.4 Adding True Positive to an Event

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

1. Click the **True Positive**  icon next to the Risk Score. 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 event will be marked with

**True Positive**

#### NOTE

In the CS\_APPLN\_PARAMS table, the PARAMETER\_NAME is MANDATORY\_EVENT\_COMM. By default, this PARAMETER\_VALUE is "N".

If no comments are given in the comments section for this configuration at the event level for any alert, it will not display any message and the empty message will be saved.

If you change the PARAMETER\_VALUE for MANDATORY\_EVENT\_COMM to "Y" and no comments are given in the comments section for this configuration at the event level for any alert, the message "Please enter event level comments!" will be displayed and will not allow to save until the comments are provided.

In the CS\_APPLN\_PARAMS table, the PARAMETER\_NAME is MANDATORY\_ALERT\_COMM. By default, this PARAMETER\_VALUE is "Y".

If no comments are given in the comments section for this configuration at the alert level for any alert, it will display "Please enter Alert level comments!" message and will not allow to save until the comments are provided.

If you change the PARAMETER\_VALUE for MANDATORY\_ALERT\_COMM to "N" and no comments are given in the comments section for this configuration at the alert level for any alert, it will not display any message and the empty message will be saved.

#### 4.4.6.5 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 **True Positive/False Positive** 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.

### 4.4.7 External Entity Details and Corresponding Watchlist details

Provides the details of the external entities associated with the selected event in the following components:

The details that are displayed in this section depend on the type of Entity data that is found. You can compare the External Entity Details with the Watchlist Details. Click **View Full Comparison** at the bottom right corner of the section. The *View Full Comparison* window appears, and the matches are highlighted in yellow color.

**Figure 20: Customer Details**

External Entity Details		Watchlist Details	
External Entity Details	Address	List Sub-Key	DJW-SAN
Updated Date	1517529600000	List Record Type	SAN
Full Name	FOOLAD MOBARAKEH ESFAHAN	List Record Origin	3803, CA-DFAIT, GB-BERR, HK-HKMA, JP-METI, US-OFAC
		List Record Id	1032597
		Registration Number	10260289464, 10260289464

### 4.4.8 Candidate Details Corresponding Watchlist details

Provides the details of the candidate details associated with the selected event in the following components:

The details that are displayed in this section depend on the type of Candidate data that is found. You can compare the Candidate Details with the Watchlist Details. Click **View Full Comparison** at the bottom right corner of the section. The *View Full Comparison* window appears, and the matches are highlighted in yellow color.

**Figure 21: Customer Details**

Candidate Details		Watchlist Details	
Given Names	soe	List Key	DJW
Family Names	win	List Sub-Key	DJW-PEP
Jurisdiction	Americas	List Record Type	PEP
Business Domain	GEN	List Record Origin	3712; 4194; AU-DFAT; AU-RBA; CH-SECO; EU; G...
		List Record Id	1028014
		MatchRule	[10100] Exact name only
		MatchScore	85
		Identification Number	GHR0047 GLOMAG 27226 MMR 5453 10845 138...
		Title	Vice Senior General
		Original Full Name	Soe Win
		Original Given Names	Soe
		Original Family Name	Win
		Full Name	SOE WIN
		ListPrimaryName	Soe Win
		Given Names	SOE

### 4.4.9 Customer Details Corresponding Watchlist Details

Provides details of the Customer details associated with the selected event in the following components:



**Figure 22: Customer Details**

Candidate Details		Watchlist Details	
Given Names	soe	List Key	DJW
Family Names	win	List Sub-Key	DJW-PEP
Jurisdiction	Americas	List Record Type	PEP
Business Domain	GEN	List Record Origin	3712; 4194; AU-DFAT; AU-RBA; CH-SECO; EU; G...
		List Record Id	1028014
		MatchRule	[[0100] Exact name only
		MatchScore	85
		Identification Number	GHR0047 GLOMAG 27226 MMR 5453 10845 138...
		Title	Vice Senior General
		Original Full Name	Soe Win
		Original Given Names	Soe
		Original Family Name	Win
		Full Name	SOE WIN
		ListPrimaryName	Soe Win
		Given Names	SOE

[View Full Comparison](#)

The details that are displayed in this section depend on the type of Customer data that is found. You can compare the Customer Details with the Watchlist Details. Click **View Full Comparison** at the bottom right corner of the section. The **View Full Comparison** window appears, and the matches are highlighted in yellow color.

**NOTE** Relationship category values will be separated by <> sign only for newly scanned records.

### 4.4.10 Alert Decision

You can add new alert-level actions and standard comments to Alert Decision. For more information, see Appendix N in *OFS Customer Screening Administrator Guide*.

#### 4.4.10.1 Alert Decision (For all Alert types) - Analyst

- Close as False Positive
- Recommend True Match

**NOTE** When the event is selected as **False Positive, Recommend True Match** decision cannot be taken or vice versa.

#### 4.4.10.2 Alert Decision for (SAN and Prohibition) - Supervisor

- Approve Recommend
- Reject Recommend – Further Information Required
- Reject Recommend – Close as False Positive
- Re-Open

#### 4.4.10.3 Alert Decision (PEP and EDD) - Supervisor

- Confirm Exit Required
- Confirm True Match Monitored
- Confirm True Match Not Monitored
- Reject Recommend – Further Information Required
- Reject Recommend – Close as False Positive
- Re-open

#### **4.4.11 Alert Status**

##### **4.4.11.1 Alert Status (For all Alert types) - Analyst**

- New
- Investigation

##### **4.4.11.2 Alert Status for (SAN and Prohibition) - Supervisor**

- Pending Review
- Closed False Positive
- Closed - True Match Exit Required

##### **4.4.11.3 Alert Status (PEP and EDD) - Supervisor**

- Pending Review
- Closed False Positive
- True Match Exit Required
- True Match Monitored
- True Match Not Monitored

#### **4.4.12 Audit History**

The Audit History provides the details of actions, who performed the actions, and results with other details.

**Figure 23: Audit History**

Updated By	Date and Time	Action	Event Id	Owner	Previous Owner	Resulting Status	Comments	A
CSSUPERVISOR	03/24/2022 12:03:39	Reject Recommend		CSSUPERVISOR		Investigation	testing	0
CSSUPERVISOR	03/24/2022 12:03:30	False Positive	11004	CSSUPERVISOR		Pending Review	Country Mismatch	0
CSANALYST1	03/24/2022 11:07:12	Recommend True Match		CSANALYST1		Pending Review	testing	0
CSANALYST	03/24/2022 11:05:56			CSANALYST		Pending Test Review	testing	0
CSANALYST	03/24/2022 11:05:42	True Positive	11004	CSANALYST		Investigation	City Match	0
CSANALYST	03/24/2022 10:15:42	Alert Status Change		CSANALYST		Investigation	Alert status changed to Investigation	0
csanalyst	03/23/2022 08:17:52	New Alert Created				New		0

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

- Updated By
- Date and Time
- Action
- Event Id
- Owner
- Previous Owner
- Resulting Status
- Comments
- Attachments

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.

Table 8 lists the Field descriptions for Audit History.

**Table 8: Field descriptions for Audit History.**

Fields	Description
Updated By	Displays the name of the person who updated the Alert.
Date and Time	Displays the date-time details when the actions are performed on the Alert.
Action	Displays the action taken on the Alert.
Event ID	Displays the unique id that was created for the event.
Owner	Displays the name of the owner who created the alert audit history.
Previous Owner	Displays the name of the previous owner of the Alert.
Resulting Status	Displays the resulting status value of the Alert.
Comments	Displays the details of the comments that are added to the audit history.
Attachments	Displays the details of the attachment, if any, are added to the audit history of the Alert.

#### 4.4.12.1 Exporting the details 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.

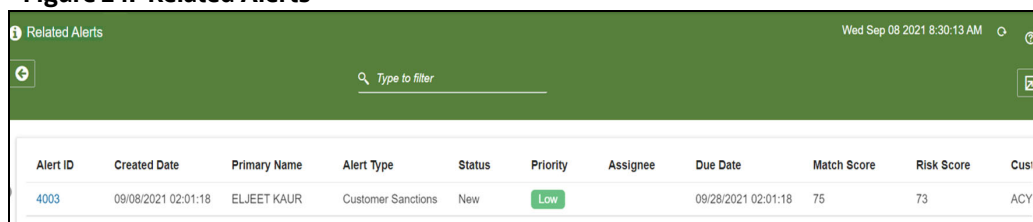
#### 4.4.13 Related Alerts

This section displays the related alerts list based on party relationships, such as the alerts for the same customer/EE and alerts sharing a parent id based on security attributes.

The latest relationships are to be considered as related customers/EE. Relationships are to be looked at in both directions. i.e., if C1 is related to R1 when looking at C1, all C1 and R1 alerts are to be displayed (Except the current Alert), and if we are looking at R1, All alerts of R1 and C1 are to be displayed.

Also, it shows the relationship between the alerting customer/EE/Response ID and the parent id in the Related Alerts.

**Figure 24: Related Alerts**



Alert ID	Created Date	Primary Name	Alert Type	Status	Priority	Assignee	Due Date	Match Score	Risk Score	Cusi
4003	09/08/2021 02:01:18	ELJEET KAUR	Customer Sanctions	New	Low		09/28/2021 02:01:18	75	73	ACY

This section contains the following components:

- Alert ID

- Created Date
- Primary Name
- Alert Type
- Status
- Priority
- Assignee
- Due Date
- Match Score
- Risk Score
- Customer ID

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.

Table 9 lists the Field descriptions for Related Alerts.

**Table 9: Field descriptions for Related Alerts**

Field	Descriptions
Alert ID	Displays the alert identification number.
Created Date	Displays the Date the Alert was created.
Primary Name	Displays the Primary Name of the Customer.
Alert Type	Displays the type of Alert.
Status	Displays the status of the Alert.
Priority	Displays the priority value of the Alert.
Assignee	Displays the assignee name of the Alert.
Due Date	Displays the due Date the Alert has to review.
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.

#### 4.4.13.1 Exporting the Related 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.

## 4.4.14 Field Descriptions

Table 10 lists the Field descriptions for Alert Details.

**Table 10: Field descriptions for Alert Details**

Field	Description
Case ID	Displays the unique Identification Number of the Case.
Created Date	Displays the Date the Alert was created.
Primary Name	Display 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.
Screening Type	Displays the type of screening, either Batch or Real-Time screening.
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 Business domain the Alert belongs to
Jurisdiction	Displays the Jurisdiction of the Alert belongs to.
Customer/EE/ Response ID	Displays the Customer/External Entity ID/Response ID.
From Date	Displays the Date the Alert is from.
To Date	Displays the Date the Alert was sent to.
Due Date Time	Displays the due date value of the Alert.
Watchlist ID	Displays the unique id assigned to batch.
List Type	Displays the type of watchlist.
Event Type	Displays the type of the event.
Matched Rule Name	Displays rules against which match is generated.
Watch List Primary Name	Displays the primary name of watch list data.

## **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.



## OFSAA Support Contact Details

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

## Send Us Your Comments

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

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

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

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

