Oracle® Financial Services Customer Screening

User Guide

Release 8.1.2.9.0
G29737-02
April 2025

Oracle Financial Services Customer Screening User Guide, Release 8.1.2.9.0

G29737-02

Contents

Preface

This guide explains Oracle Financial Services (OFS) 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.

Who Should Use This Guide

The Customer Screening User Guide is designed for the following users:

- **Reviewer**: This user works on the alerts within the application frequently. This user can only view within the application and cannot perform any action.
- **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.

How this Guide is Organized

The Customer Screening User Guide includes the following topics:

- 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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Resources

This topic identifies additional resources to the OFS Customer Screening. You can access additional documents from the Oracle Help Center.

Conventions

The following text conventions are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Document Control

Table 1 Revision History

Version Number	Revision Date	Change Log
8.1.2.9.0	February2025	No content updates for this release.
8.1.2.8.0	January 2025	Updated File Upload section. Added Promoting to Case for SAN - Supervisor section.
8.1.2.8.0	August2024	Added information for Multiple Identifier Screening.
8.1.2.7.0	February2024	• Added information about splitting of alert based on the event type in Real-Time Screening section. • Added note in Bulk Action section about bulk action of event and configuration. • Added information about the following functions in Events section: – Expand – Collapse – Save – Clear – Match Details
8.1.2.6.0	October 2023	No content updates for this release.
8.1.2.5.1	August2023	Updated the note in Alert List section about alert list default field property.
8.1.2.5.0	June2023	• Added Reviewer user role information. • Added Bulk Action section. • Updated the Alert List section and Field Descriptions table with new attribute field details.

Table 1 (Cont.) Revision History

Version Number	Revision Date	Change Log
8.1.2.4.1	April2023	• Added note about Multi select option and Search using code functionality for Country fields in Managing Customer Screening section. • Added supported file formats for uploading an attachment to the alert list in Attaching a File to an Alert(Only Analyst/ Supervisor/Senior Supervisor) section. • Added customer status, gender, tax id and tax country attributes to the Customer Details Corresponding Watchlist Details section
8.1.2.4.0	March2023	• Added File Upload section. • Added Alerts for Migrated OWS Watchlist data section. • Updated Events section with information about Select All option. • Added Alert Status for Alerts for Migrated OWS Watchlist data section.
8.1.2.3.0	December 2022	• Updated the Alert List section with new customization features. • Added information about enhanced UI experience in the Queue, Alert List, and Alert Details, which sup- port more than the high, medium, and low classifications per queue in the Grid View section.
8.1.2.2.0	October 2022	• Added information about Source Request ID attribute in Real-Time Screening section. • Added supported file formats for uploading an attachment to the alert list in Attaching a File to an Alert(Only Analyst/ Supervisor/Senior Supervisor) section.
8.1.2.0.0	July2022	The first version of 8.1.2.0.0 release.

1

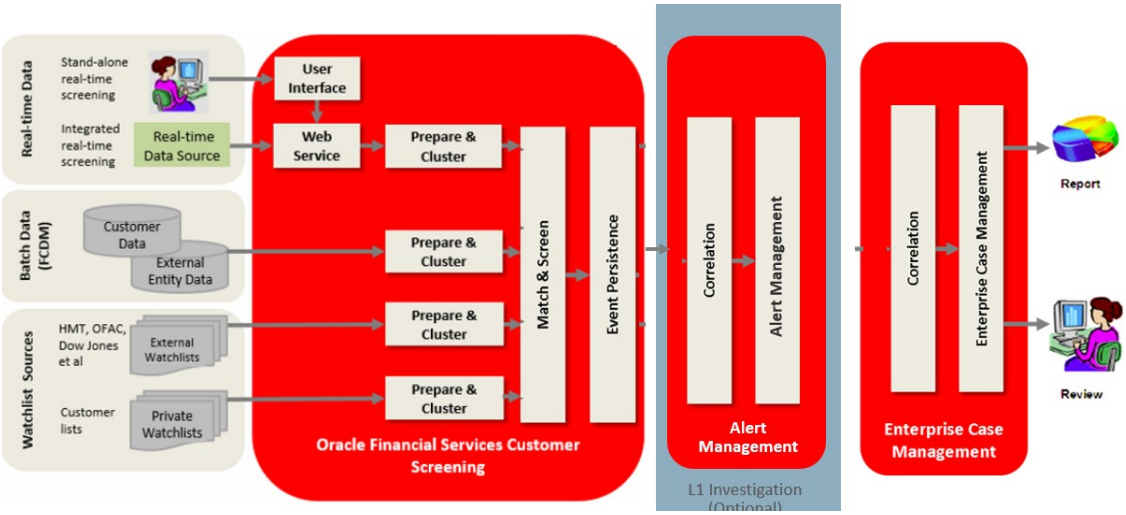
About Customer Screening

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.

1.1 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 1-1 Customer Screening Architecture

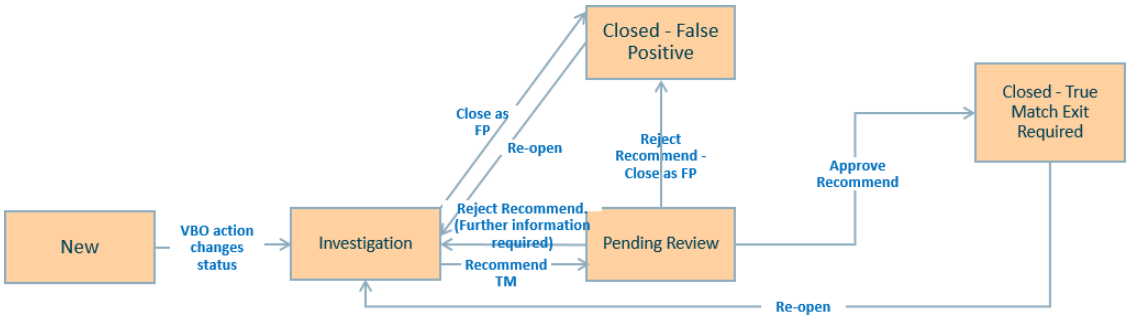


1.2 Default Workflow

The workflow is applicable only for L1 investigation.

Sanctions and Prohibition

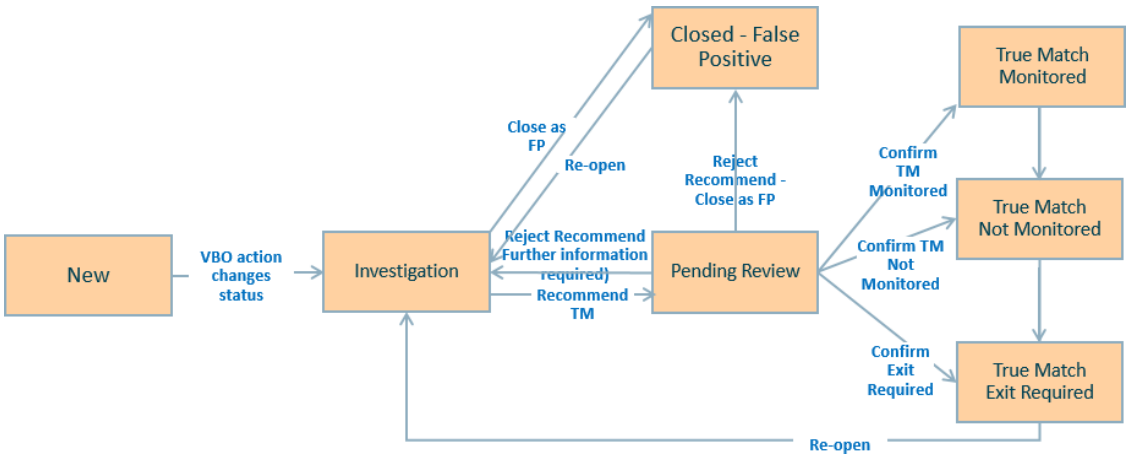
Figure 1-2 Sanctions and Prohibited Workflow



> **Note:**
>
> Escalated is enabled only when L2 Investigation enabled.

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

Figure 1-3 Politically Exposed Person (PEP) and Enhanced Due Diligence (EDD) Workflow



> **Note:**
>
> Escalated is enabled only when L2 Investigation enabled.

1.3 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.

1.4 User Roles and Actions

The following user roles are defined in OFS Customer Screening:

- Reviewer
- 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 1-1 User Roles and Actions

Level	Action	Reviewer	Analyst	Supervisor	Senior Supervisor	Queue Administrator
Queue Level	Add	-	-	-	-	✓
Queue Level	Edit	-	-	-	-	✓
Queue Level	Assign	-	-	-	-	✓
Queue Level	Delete	-	-	-	-	✓
Queue Level	Open	✓	✓	✓	✓	-
Alert Level	Access to View UI	✓	✓	✓	✓	✓

Table 1-1 (Cont.) User Roles and Actions

Level	Action	Reviewer	Analyst	Supervisor	Senior Supervisor	Queue Administrator
Alert Level	Recommend True Match	-	✓	-	-	-
Alert Level	Close as False Positive	-	✓	-	-	-
Alert Level	Re-Open	-	-	✓	-	-
Alert Level	Approve Recommended	-	-	✓	-	-
Alert Level	Reject as False Positive	-	-	✓	-	-
Alert Level	Confirm TM Monitored	-	-	✓	-	-
Alert Level	Confirm TM Not Monitored	-	-	✓	-	-
Alert Level	Confirm Exit Required	-	-	✓	-	-
Real-Time Screening UI	Scan	-	✓	✓	-	-
Real-Time Screening UI	Scan and Investigate	-	✓	✓	-	-
Real-Time Screening UI	File Upload	-	✓	✓	-	-
Customer Screening Alert List	Bulk Update: • Assign Alerts • Change the Priority • Change Due Date Time	-	✓	✓	-	-
Customer Screening Alert List	Add attachments	-	✓	✓	✓	-
Customer Screening Alert List	Download attachments	✓	✓	✓	✓	-
Customer Screening Alert List	Bulk Action	-	✓	✓	-	-
Event Level	True Positive	-	✓	✓	-	-
Event Level	False Positive	-	✓	✓	-	-

> **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.

2
Getting Started

This topic describes how to login and access the Customer Screening application.

2.1 Accessing OFSAA Page

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

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

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

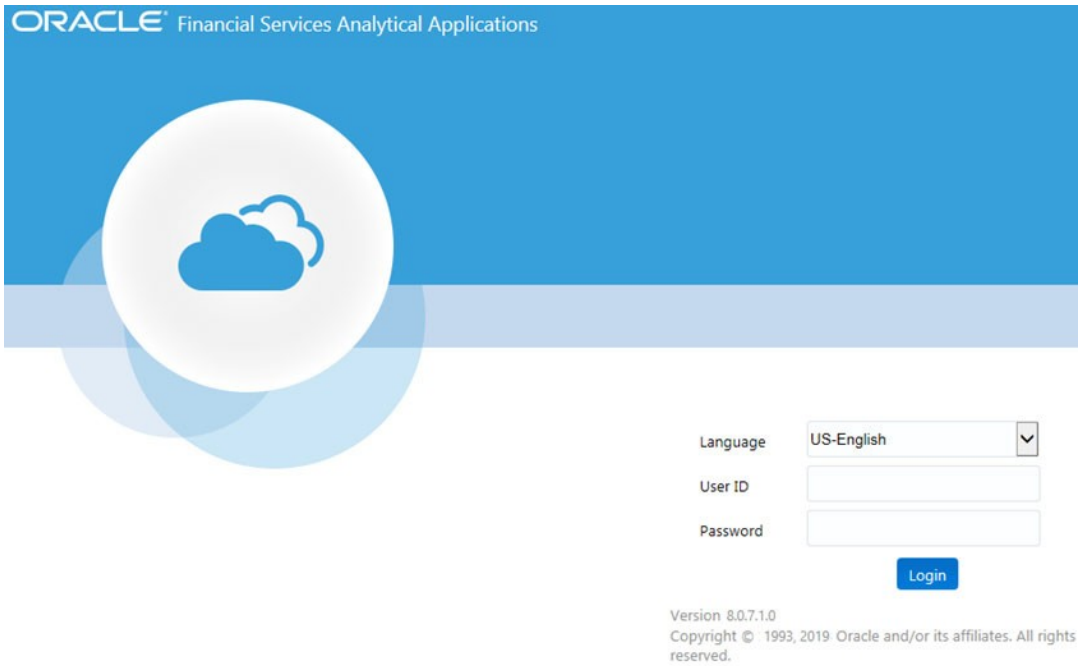
1. Enter the URL into your browser using the following format:

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

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

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

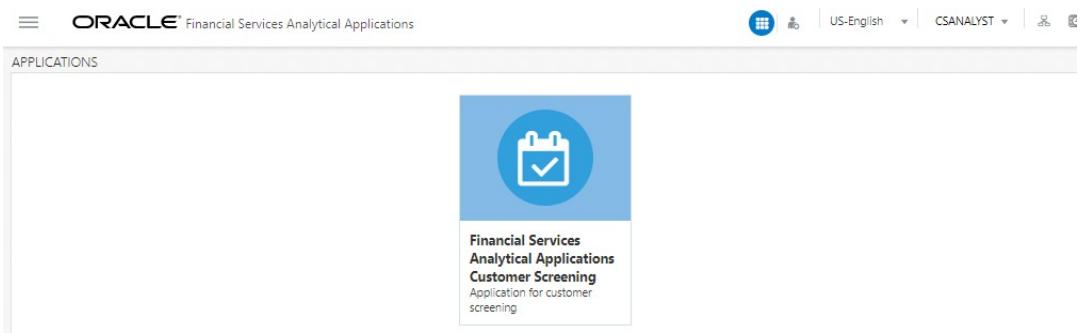
Figure 2-1 OFSAA Login Page



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 2-2 Customer Screening Home Page



To view the Financial Services Analytical Applications Customer Screening Home page, click **Calendar**  .

2.2 Managing OFSAA Page

This topic describes how to access information available in the OFSAA page.

2.2.1 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.

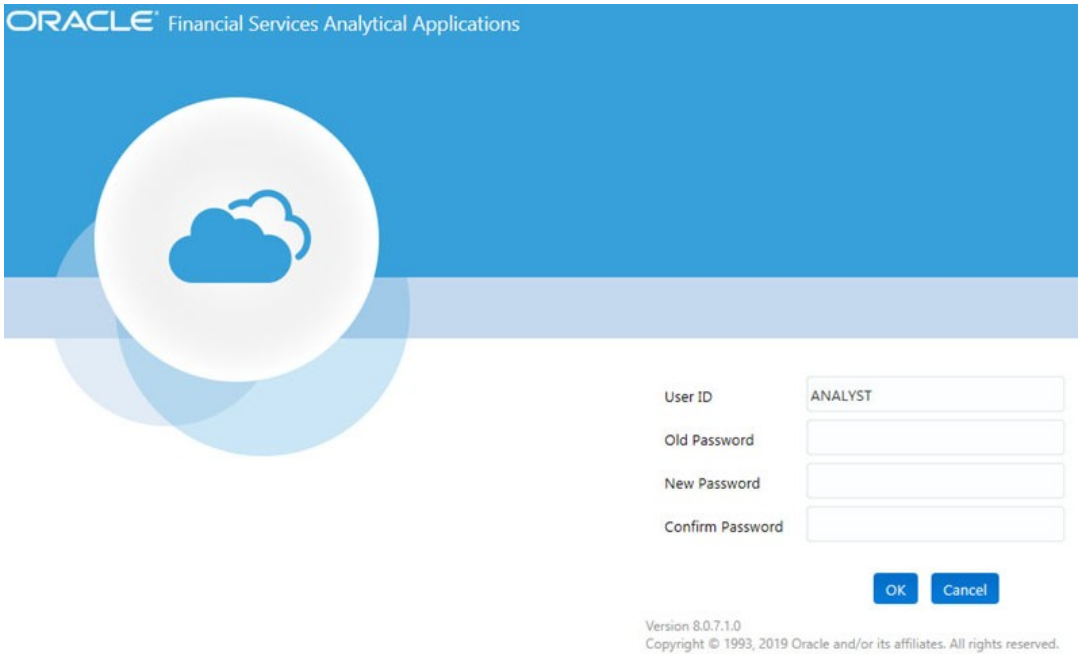
2.2.2 Changing the Application Password

You can change password for security purposes.

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 2-3 Password Change Page



3. Enter your **Old Password** and **New Password** in the respective fields.
4. Enter the new password again in the **Confirm Password** field.
5. Click **OK**. Your password is changed successfully. The application navigates back to the login page, where you can log in with the new password.

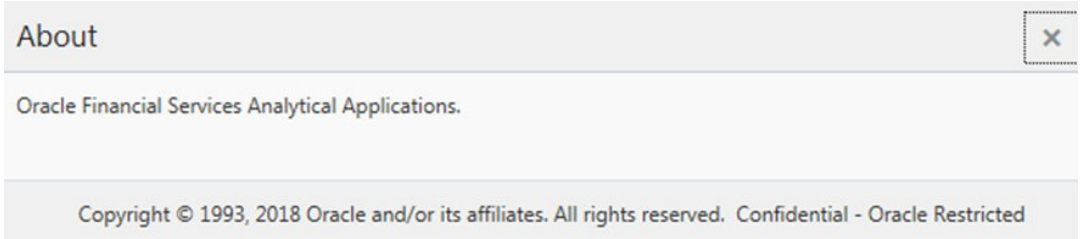
> **Note:**
>
> Your password is case-sensitive. If you have problems with the password, verify that the Caps Lock key is off. If the problem persists, contact your system administrator.

2.2.3 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** link on the **Oracle Financial Services Analytical Applications** login page. The copyright text displays in a new window.

Figure 2-4 Copyright Information



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

2.3 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 topics provide instructions for setting your Web display options for OFSAA applications.

2.3.1 Enabling JavaScript

This topic 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.

2.3.2 Enabling Cookies

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

2.3.3 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.

2.3.4 Enabling File Downloads

This topic 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.

2.3.5 Setting Print Options

This topic 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.

2.3.6 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.

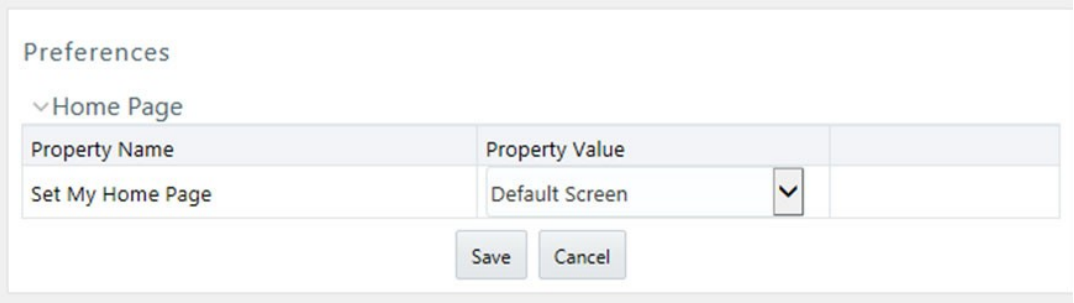
2.3.7 Setting Home Page Preferences

This topic 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 2-5 Preferences Page



3. 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.

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

2.4 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:

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

3
Managing Customer Screening

This topic 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-TimeScreening**: 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.

3.1 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.

You can configure the functionality assigned to user group in the Real-time Screening page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups, see the OFS Customer Screening Administrator Guide.

> **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.

3.1.1 Creating a Case or Alert for Individual and Entity

This topic describes how to create a case or alerts for Individual and Entity search type.

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

1. Login 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 is displayed.
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 following 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.
> - Address Country, Residency Country, Nationalities, Passport Issuing Country, and Country of Birth fields have the Multi-select option and Search using code functionality to select the country. You can choose the country from the drop-down or by typing the country code or name. For information on populating country codes, see the General Configuration section in the OFS Customer Screening Administrator Guide.
> - 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.
> - Registration Country, Operating Countries, and Address Country fields have the Multi-select option and Search using code functionality to select the country. You can choose the country from the drop-down or by typing the country code or name. For information on populating country codes, see the General Configuration section in the OFS Customer Screening Administrator Guide.

For field information, see the Field Descriptions for Individual and Entity Search Type.

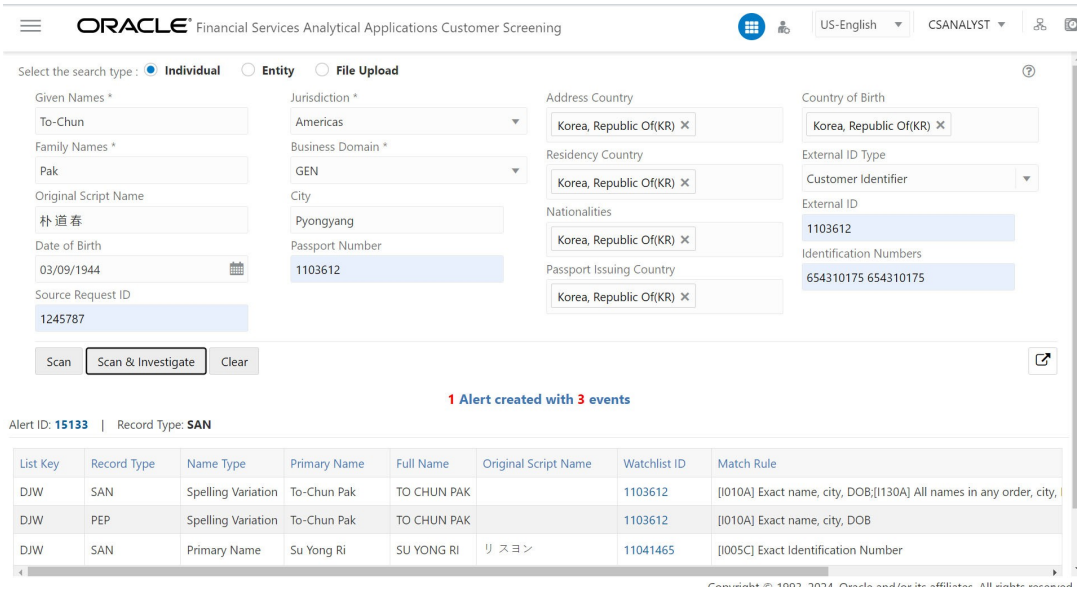
5. Perform the following for **Individual** or **Entity**:

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.

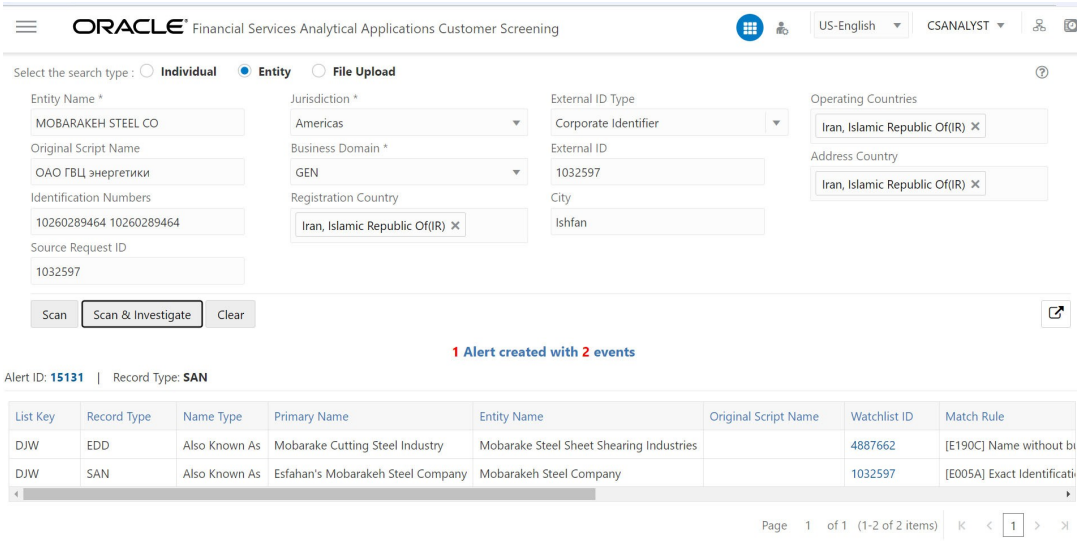
For Individual

Figure 3-1 Real-Time Screening for Individual



For Entity

Figure 3-2 Real-Time Screening for Entity



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. You can split the alerts by event type rather than group them in one alert. Based on the matches generated, separate alerts

are created for SAN, PEP, EDD, and PRB. For more information on splitting the alerts based on event type, see the General Configuration section in the OFS Customer Screening Administrator Guide.

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

3.1.1.1 Field Descriptions for Individual and Entity Search Type

This topic provides field descriptions for selected search type (Individual or Entity).

Table 3-1 Individual and Entity Search Type - Field Description

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. Multiple Identification Numbers can be scanned. The delimiters between multiple Identification Numbers can either be space or comma or semi colon.
Operating Countries	Enter the identification numbers of the Individual or Entity.
Source Request ID	Enter the request identification number of the Individual or Entity.

> **Note:**
>
> 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.

3.1.2 File Upload

File upload facilitates bulk screening and process Real-time screening data without compromising quality or time.

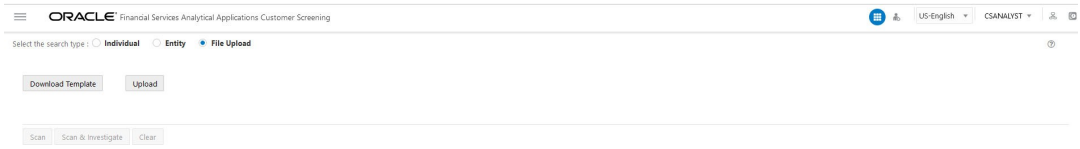
File upload is suitable for institutions that need to review a large number of customers. This allows instant results for multiple searches at once without having to conduct the search one by one. This data search saves time and allows the user to focus on entities that pose the highest risk to the institution.

The results of the screening can be downloaded from the system for internal use. The bulk screening result is very detailed and allows the user to see the results for each customer, including those who do not pose any risk.

To screen the bulk records and to create an Alert or Case, follow these steps:

1. Login to the **Customer Screening Application**.
2. Click **Real-Time Screening**. The Real-Time Screening page appears.
3. In the Real-Time Screening page, select the search type as **File Upload**.

Figure 3-3 File Upload



4. Click **Download Template**. The Download Template button allows you to download the Excel file for the input data. Save the `RealTimeScreening Input File Template.xlsx` file to a local folder.

> **Note:**
>
> You can alter the file name.

5. Enter the bulk screening request data for the candidates in the excel file. See the following information for entering the data:

> **Note:**
>
> You can request a maximum of 100 records.

- **Fields Mapped for Individual Screening:**

  - Given Names
  - Family Names
  - Original Script Name
  - Date of Birth
  - Jurisdiction
  - Business Domain
  - 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 mandatory fields are Given Names, Family Names, Jurisdiction and Business Domain.

- **Fields mapped for Entity Screening**:
  - Entity Name
  - Original Script Name
  - Jurisdiction
  - Business Domain
  - City
  - Address Country
  - Registration Country
  - Operating Countries
  - External ID Type
  - External ID
  - Identification Numbers
  - Source Request ID

> **Note:**
>
> The mandatory fields are Entity Name, Jurisdiction, and Business Domain. For the country field inputs, refer to the country sheet in the Excel file for information on Country Names and corresponding Country Codes. You can enter multiple country code values for country fields. For information on populating country codes, see **General Configuration** section in the OFS Customer Screening Administrator Guide.

The following instructions must be followed while entering the candidate data in the file:

- Enter valid field data.
- There are no restrictions on the number of data, and size of the file.
- The processing time for the file upload depends upon the system resource and capability.
- The Excel file has four sheet where the first sheet has the fields for input and remaining sheets provide information and instructions on the fields.
- Do not delete or alter the file columns and headings in the first sheet.
- Value for all the mandatory fields must be entered.
- To pass multiple values for countries, entered values must be space separated.

6. Click **Upload** to upload the excel file. In the File Upload pop-up menu you can either drag and drop the file or you click add icon to select the file from local folder. When the upload is complete the following buttons are enabled:
   - **Scan**: Click to displays the screened watch list records.
   - **Scan & Investigate**. Click to generate an alert or case based on the configurations.
   - **Clear**: Click to delete the uploaded file.

   > **Note:**
   >
   > You can delete the uploaded Excel file by the following methods:
   >
   > – Click on the delete icon available adjacent to the uploaded file field in screen.
   >
   > – The Uploaded file be auto deleted if you switch between the search type.
   >
   > – Click Clear.

7. Click **Scan or Scan & Investigate** to initiate the Real-time Screening.

   > **Note:**
   >
   > - The processing time for Scan depends on the system resource and capability.
   > - If the instruction are not followed, you will receive an error message and screening will not happen. In that case delete the uploaded excel file and repeat the file upload after rectifying the errors.

If the candidate request count is less than 20, the **File Upload summary Table** section and the alert ID or Case ID request results sections are displayed after a successful scan, see Figure 3-4. If candidate request count is more than 20 only **File Upload summary Table** section is displayed, see Figure 3-5.

> **Note:**
>
> The candidate request count limit to display the request result section in the UI is configurable. For more information, see OFS Customer Screening Administrator Guide.

8. The **File Upload summary Table** section contains the following information:
   - Total Number of Submitted Request
   - Total Number of Submitted Name with a Match
   - Total Number of Duplicate Requests

> **Note:**
>
> The File Upload summary Table is displayed in all scenarios.

Click the **Export** icon to download the screened excel file to the local folder. The exported file will have only Real-time Screening Input sheet with newly populated columns.

- For **Scan** the following columns are auto populated:
  - Duplicate Flag
  - Match or No match
  - Number of Matches
- For **Scan & Investigate** the following columns are auto populated:
  - Duplicate Flag
  - Match or No match
  - Number of Matches
  - Alert ID/Case ID

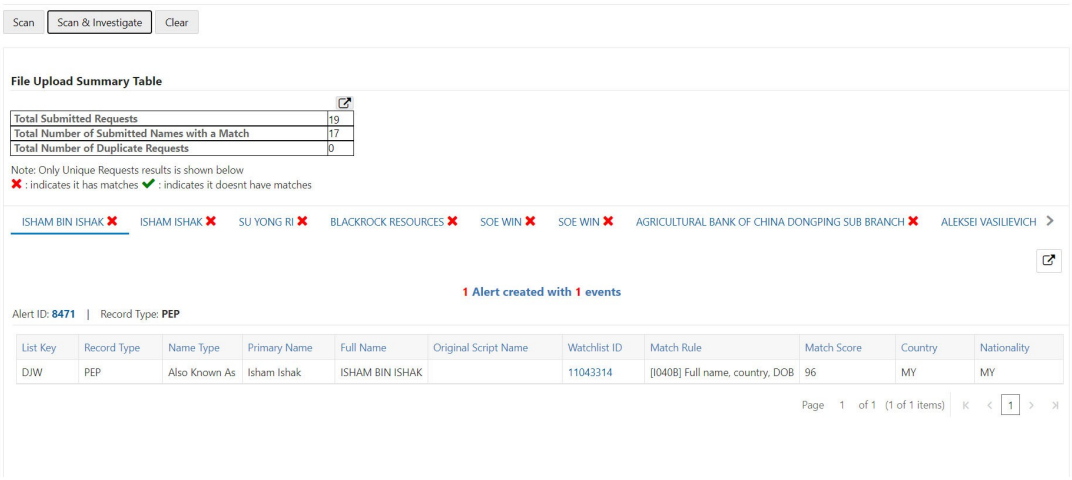
> **Note:**
>
> Creating an Alert or Case is configurable. The Alert or Case will be generated when you select CSAM or ECM, respectively while configuring EDQ URL.

9. The request results sections displays the response of each request inside the different tabs. You can click on the request name tabs to switch between multiple request data to check on each responses. The response tab name for entity will be the entity name and for individual will be the combination of given name and family name.

   Responses for duplicate requests are not displayed in the UI, only unique request results are displayed. The green tick  icon indicate the results with no matches and the red cross  icon indicate result with matches.

If Requests are less than 20, you can see the following image.

Figure 3-4 Scan Result for Less than 20 Request

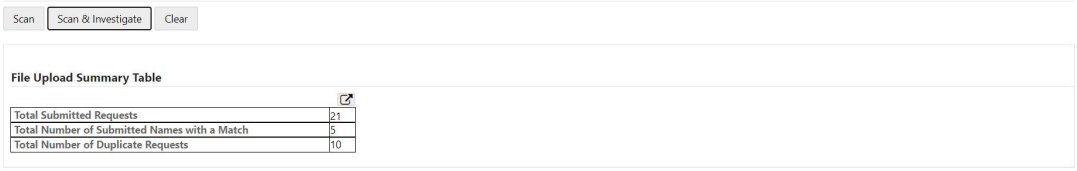


In the request results sections, you can view generated Alert ID/Case ID and Watchlist ID. Click **Alert ID/Case ID** or **Watchlist ID** to view the Alert Details or Watchlist Details page, respectively.

You can download the results to a local folder using the **Export** icon.

If Requests are more than 20, you can see the following image.

Figure 3-5 Scan Result for More than 20 Requests



> **Note:**
>
> The request result section is displayed only when the request number is less than 20. If the request number is more than 20, you must use the **Export** icon to download the requested results.

Click the **Export** icon to download the request result to a local folder. The exported file will have the following information sheets:

- Request Details
- Event Details
- Watchlist Details

3.1.2.1 File Upload Input Guidelines

This topic provides information about input guidelines for uploading file.

Table 3-2 Input Guidelines for File Upload

Field	Maximum Field Length	Input Description
Candidate Type	-	For Individual Screening enter Individual Screen and for Entity Screening enter Entity Screen.
Given Names	255	Enter Given Name of the Individual for Screening.
Family Names	255	Enter Family Name of the Individual for Screening.
Entity Name	255	Enter Entity Name of the Entity for Screening.
Original Script Name	No Restriction	Enter Original Script Name of the Individual/Entity for Screening.
Date of Birth	No Restriction	Enter Date of Birth of the Individual for strong matches. Date Format must be **YYYY-MM-DD**.
Jurisdiction	4	Use **D** for Default and **AMEA** for Americas as Jurisdiction Code.
Business Domain	1	Use **D** for Default and **A** for GEN as Business Domain Code.
City	No Restriction	City data is used to strengthen potential match information.
Passport Number	No Restriction	Enter Passport Number of the Individual.
Address Country	No Restriction	Enter Country code of the Individual being screened.
Residency Country	No Restriction	Enter Residency Country code of the Individual being screened.
Registration Country	No Restriction	Enter Registration Country Code of the Entity being screened.
Operating Countries	No Restriction	Enter Operating Country Code of the Entity being screened.
Nationalities	No Restriction	Enter Nationality Code of the Individual being screened.
Passport Issuing Country	No Restriction	Enter Country Code of the Individual where Passport is issued.
Country of Birth	No Restriction	Enter Birth Country Code of the Individual being screened.
External ID Type	No Restriction	Enter the external ID type.
External ID	255	Enter External ID. This field is mandatory if you select External ID Type.

Table 3-2 (Cont.) Input Guidelines for File Upload

Field	Maximum Field Length	Input Description
Identification Numbers	No Restriction	Enter Identification Number of the Individual being screened. Multiple Identification Numbers can be scanned. The delimiters between multiple Identification Numbers can either be space or comma or semi colon.
Source Request ID	3000	The Source Request ID can be used to provide the customer ID while screening.

3.2 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).

- Reviewer
- 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.

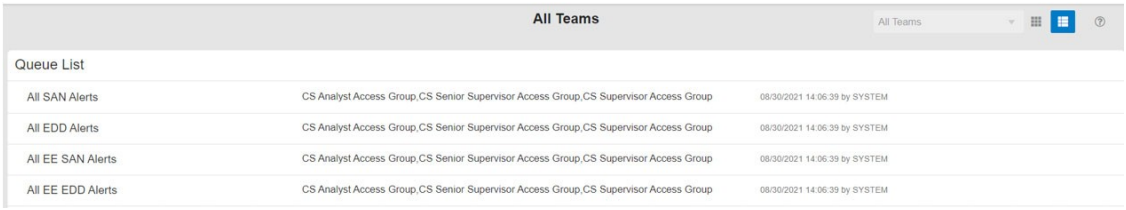
3.2.1 List View

To view queue list in list view, follow these steps:

1. Log in to the application as Reviewer/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 3-6 Queue List in List View



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

- Queue Name
- User Group names (that are assigned by the Queue Administrator)
- Date Time Created By (For example, 09/09/2021 14:06:39 by QADMIN/SYSTEM)

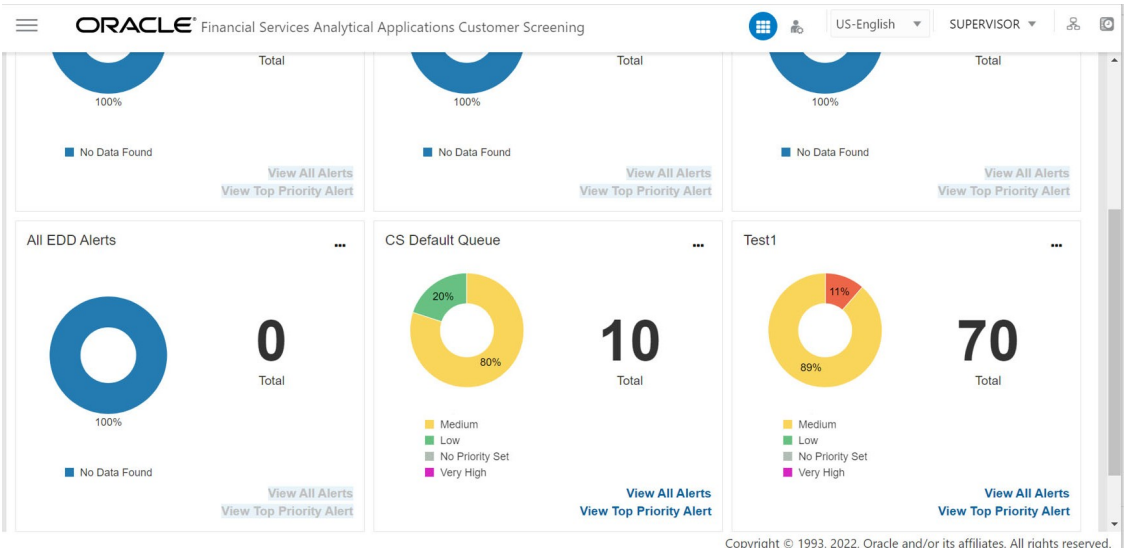
You can view ten queues in the Queue List and use the navigation to view the next set of queues.

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

3.2.2 Grid View

You can select the thumb-view  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 3-7 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 default priorities in the application:

- High
- Medium
- Low

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

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

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

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

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

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

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

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

You can perform the following actions on each queue:

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

3.3 Alert List

The Alert List page displays a list of alerts assigned to the Analyst/Supervisor/Senior Supervisor in a default view.

The users with the Senior Supervisor role can access all the alerts that are assigned/ unassigned to the other users. A Reviewer can see, access, customize the Alert List page and download attachments uploaded by other users in the Alert List page. A Reviewer cannot perform the following function:

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

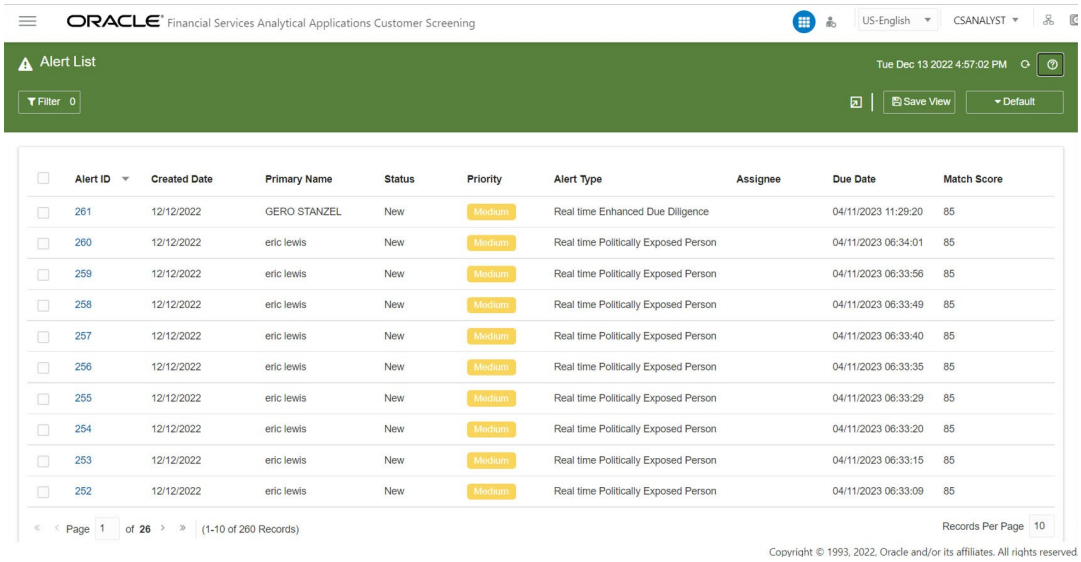
> **Note:**
>
> When a Reviewer opens an alert with any status, the status is unaffected, and the alert will not be assigned to the Reviewer user.

You can configure the functionality assigned to user group in the Alert list page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups, see the OFS Customer Screening Administrator Guide.

To access the Alert List page, follow these steps:

1. Log in to the **Customer Screening** 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 is displayed.

Figure 3-8 Alert List



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

  Alert List page contains the following default field details:
  - Alert ID
  - Created Date
  - Primary Name
  - Status
  - Priority
  - Alert Type
  - Assignee

- Due date
- Match Score
- Risk Score
- WL Record ID
- Count of WL Record IDs
- Count of Events
- Count of Event Types
- Is Bulk Actioned?
- Count of ML Closed Events
- Count of ML Escalated Events

> **Note:**
>
> You can customize the optional fields using the Column menu. For more information, see the section.

- Comments

> **Note:**
>
> If the field attribute characters exceed the threshold number, the field is limited and displays three bullets. Hover over the attributes field to display the complete list.

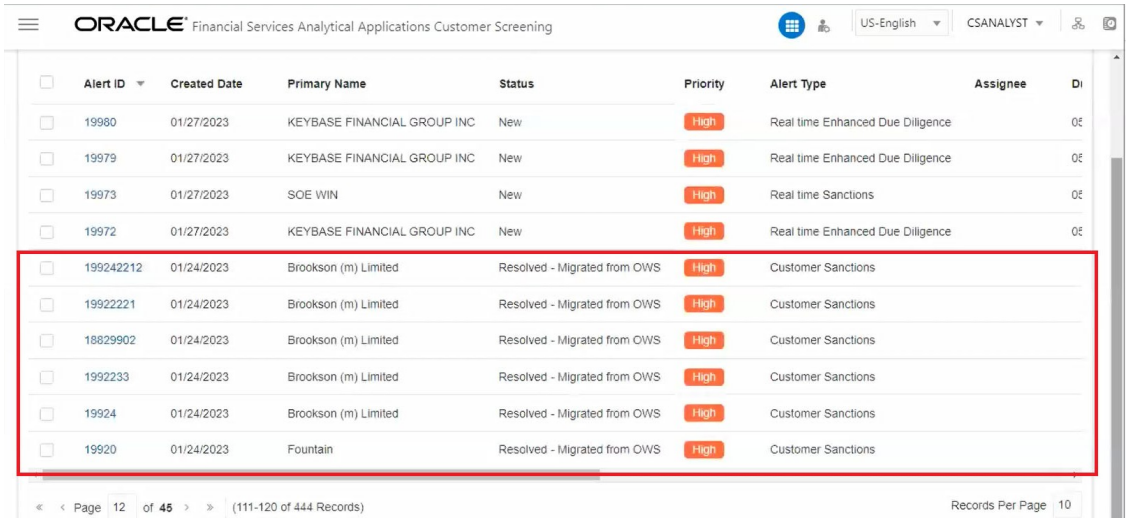
3.3.1 Alerts for Migrated OWS Watchlist Data

If the Oracle Watchlist Screening (OWS) data are migrated to CS screening, the Alert the list page displays both the CS-generated alert and the alert generated for migrated OWS data in the default view. If you are an analyst, you can access all the alerts assigned or unassigned to the other users.

You can filter the OWS data to be displayed by selecting the status criteria as mentioned in the Alert list Filter. For more information on filtering the alert list see Filtering the Alert List and for OWS status parameters see Alert Status.

For more information on data migration from OWS to CS, see OFS Customer Screening Administrator Guide.

Figure 3-9 Alert List for OWS Data



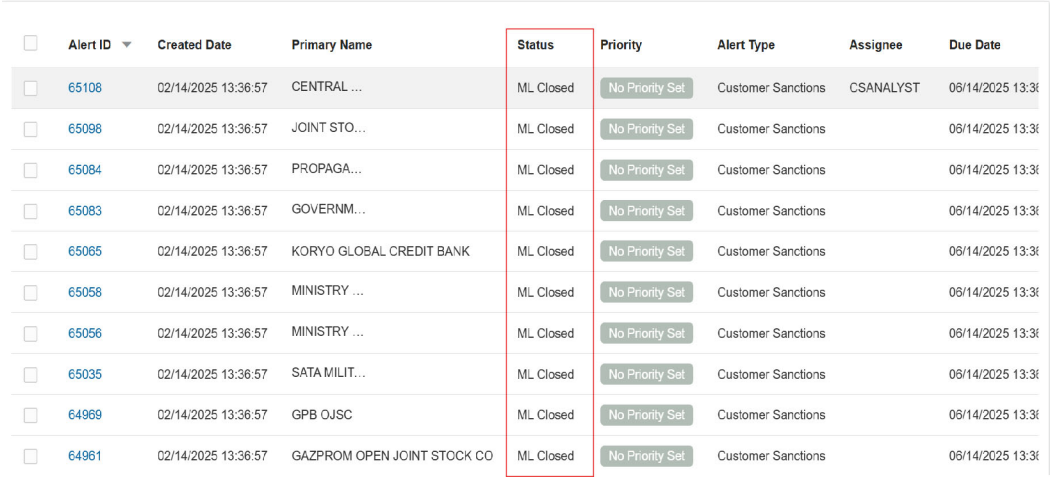
3.3.2 Alerts for ML decisioned Data

Once all ML related batches are configured and successfully executed, alerts decisioned by ML model are updated in the **Alert List** page on the **Status** column. Alert status is updated either ML Closed or ML escalated based on the ML auto threshold configuration. For more information, refer to the ML Integration with Customer Screening section in the Customer Screening Administration Guide

> **Note:**
>
> If any events ML score is **less than or equal** to threshold configured for auto closed score, the alert status is updated as **ML Closed**.
>
> If any events ML score is **greater than or equal** to threshold configured for auto escalated score, the alert status is updated as **ML Escalated**.
>
> If any events ML score is greater than threshold configured for auto closed score and less than auto escalated score threshold, the alert status updated as **New**.

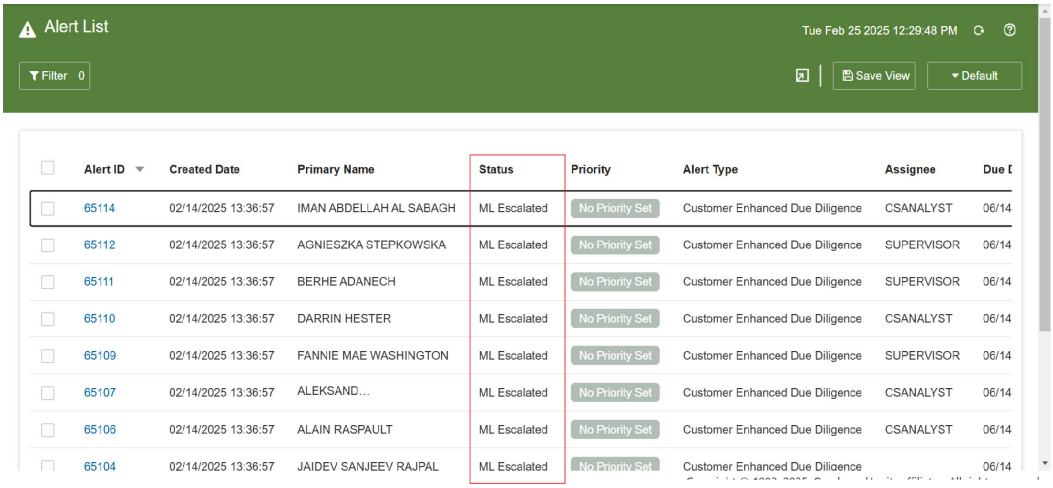
You can filter the ML decisioned data to be displayed by selecting the status criteria as mentioned in the Alert list Filter. For more information on filtering the alert list see the Filtering the Alert List section for the ML decisioned status parameters see Alert Status.

Figure 3-10 ML Closed Alert List for the ML decisioned data



Alert ID	Created Date	Primary Name	Status	Priority	Alert Type	Assignee	Due Date
65108	02/14/2025 13:36:57	CENTRAL ...	ML Closed	No Priority Set	Customer Sanctions	CSANALYST	06/14/2025 13:3
65098	02/14/2025 13:36:57	JOINT STO...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65084	02/14/2025 13:36:57	PROPAGA...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65083	02/14/2025 13:36:57	GOVERNM...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65065	02/14/2025 13:36:57	KORYO GLOBAL CREDIT BANK	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65058	02/14/2025 13:36:57	MINISTRY ...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65056	02/14/2025 13:36:57	MINISTRY ...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
65035	02/14/2025 13:36:57	SATA MILIT...	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
64969	02/14/2025 13:36:57	GPB OJSC	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3
64961	02/14/2025 13:36:57	GAZPROM OPEN JOINT STOCK CO	ML Closed	No Priority Set	Customer Sanctions		06/14/2025 13:3

Figure 3-11 ML Escalated Alert List for ML decisioned data



Alert ID	Created Date	Primary Name	Status	Priority	Alert Type	Assignee	Due D
65114	02/14/2025 13:36:57	IMAN ABDELLAH AL SABAGH	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	CSANALYST	06/14
65112	02/14/2025 13:36:57	AGNIESZKA STEPKOWSKA	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	SUPERVISOR	06/14
65111	02/14/2025 13:36:57	BERHE ADANECH	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	SUPERVISOR	06/14
65110	02/14/2025 13:36:57	DARRIN HESTER	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	CSANALYST	06/14
65109	02/14/2025 13:36:57	FANNIE MAE WASHINGTON	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	SUPERVISOR	06/14
65107	02/14/2025 13:36:57	ALEKSAND...	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	CSANALYST	06/14
65106	02/14/2025 13:36:57	ALAIN RASPAULT	ML Escalated	No Priority Set	Customer Enhanced Due Diligence	CSANALYST	06/14
65104	02/14/2025 13:36:57	JAIDEV SANJEEV RAJPAL	ML Escalated	No Priority Set	Customer Enhanced Due Diligence		06/14

3.3.3 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)
- Attaching a File to an Alert (Only Analyst/Supervisor/Senior Supervisor)
- Customizing the Field Columns
- Reordering the Columns
- Saving the View
- Managing Views
- Closed Alerts

- Exporting Alerts from the List
- Reload Grid for Alert List
- Bulk Action

3.3.3.1 Filtering the Alert List

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

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

- Customer/External Entity ID
- Alert Type
- Alert ID
- Primary Name
- Priority
- Assignment type
- Status
- Match Score
- Risk Score
- Decision
- Standard Comments
- Domain
- Jurisdiction
- Created Date Range
  - From Date
  - To Date
- Assignee
- Case ID
- WL Record ID
- Count of WL Record IDs
- Count of Events
- Count Of Event Types
  - SAN
  - EDD
  - PRB
- Is Bulk Actioned?
- Comments

3.3.3.2 Sorting the Alerts

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

- Click the sort icon available next to the column header.
- Right click on the field names and select **Sort Ascending** or **Sort Descending** options from the list.

3.3.3.3 Updating the Alerts (Bulk Update)

You can bulk update the alerts from the list.

> **Note:**
>
> The Senior Supervisor only can **Bulk Update** the alerts on the Alerts List page.

To bulk update the alerts, follow these steps:

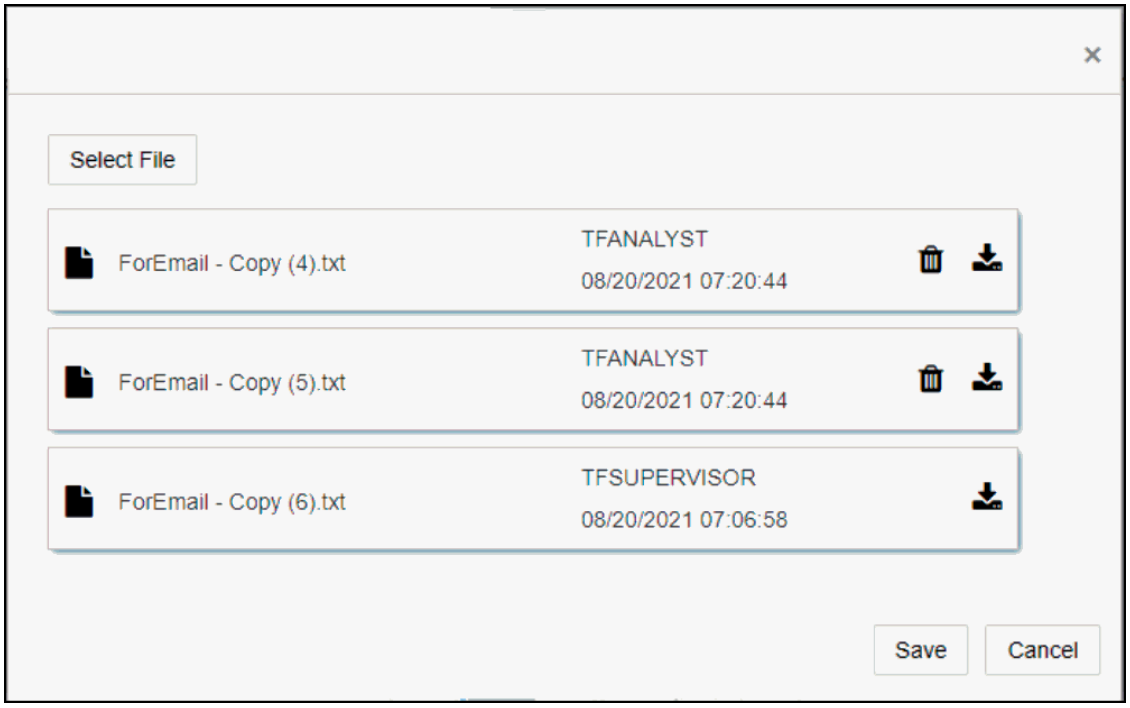
1. Select one or more alerts and click **Bulk Update**. The Bulk Update window is displayed
2. Provide the details for the following fields, and the alerts get updated based on the below action performed:
   - Due Date Time
   - Priority
   - Assignee
3. Click **Save**. The details related to the bulk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

3.3.3.4 Attaching a File to an Alert (Only Analyst/Supervisor/Senior Supervisor)

You can also attach a file to any alert.

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

Figure 3-12 Add Attachments



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

1. Select the alert from the list. The Attachment option is displayed.
2. Click **Attachment**. The Attachment window is displayed.
3. Click**Select Files** to select the files.
4. Click **Save**. The attachments are added to the list.
5. Click **Delete** icon next to the Attachment name to delete any of the attachments,
6. Click **Ok** to confirm. The file will be marked to delete. Click **Save** to delete the file.
7. Click **Download** icon next to the **Delete** icon to download the attachment.

> **Note:**
>
> - The maximum allowed size for the attachment is 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.

3.3.3.5 Customizing the Field Columns

You can customizing your field columns in the Alert list as per your requirement.

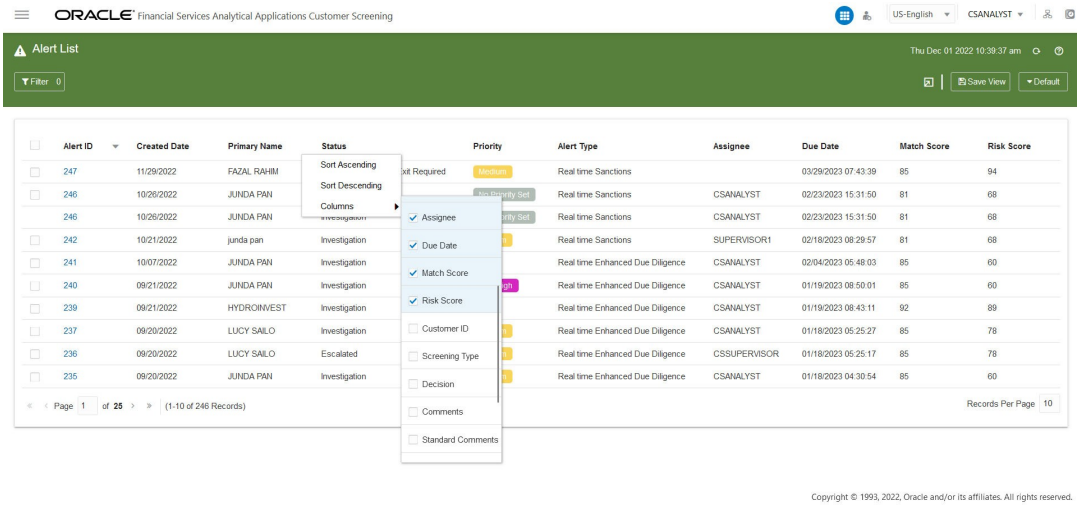
To customize the field columns, follow these steps:

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

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

   - Alert ID
   - Created Date
   - Primary Name
   - Status
   - Priority
   - Alert Type
   - Assignee
   - Due date
   - Match Score
   - Risk Score
   - Customer ID
   - Screening Type
   - Decision
   - Comments
   - Standard Comments
   - Domain
   - Jurisdiction
   - Case ID
   - Assignment Type
   - WL Record ID
   - Count of WL Record IDs
   - Count of Events
   - Count of Event Types
   - Is Bulk Actioned?
   - Count of ML Closed Events
   - Count of ML Escalated Events

Figure 3-13 Alert List Window- Columns



3.3.3.6 Reordering the Columns

You can reorder the column as per the priority and requirement.

To reorder the column, follow these steps:

1. Click and select the **Column**.
2. Drag, and drop in the required order.

3.3.3.7 Saving the View

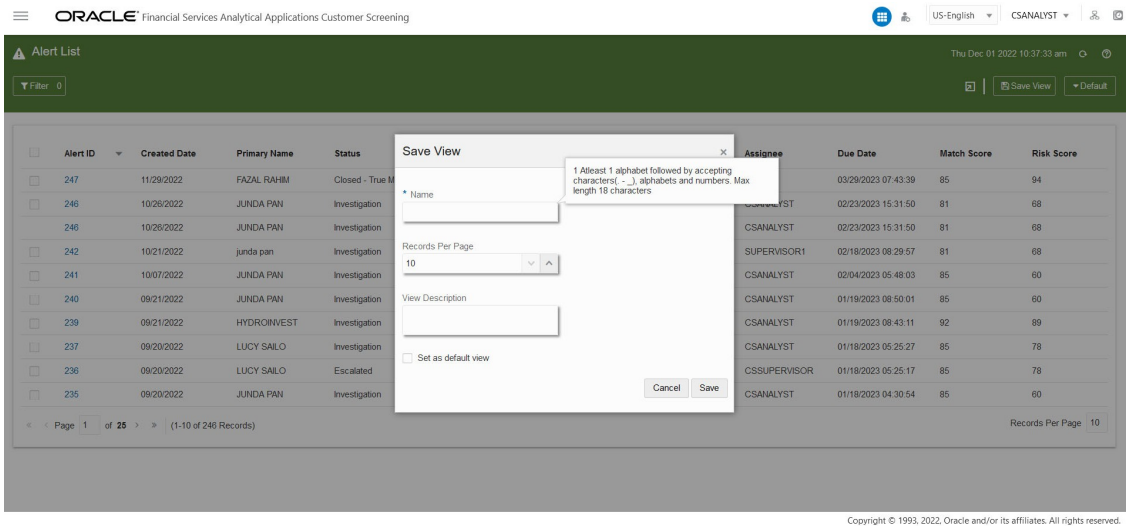
You can add the Customized View to the Views List by saving it.

To save and add the customized view, follow these steps:

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

Saving the view includes applied filters, column sort, column re-order, selected columns, view description (optional) and records per page data.
You can find the saved views list from the **Views** menu by selecting the **DEFAULT** option next to the **Save View** button. You can also use the Search bar in the **View** window to search for the views.

Figure 3-14 Save View



3.3.3.8 Managing Views

You can edit, delete, set as default or remove default the saved Views.

To manage the views, follow these steps:

1. Select the **DEFAULT** button. The Views window is displayed.
2. Use the Search bar to search for the views and select to apply or click the **Manage Views** bottom in the right corner to view the complete list of available views. You can view all the list of user created views in the Manage Views window.
3. To edit, delete, set as default or remove default, select the view from the list and click the **More Actions** icon and select the required action from the drop down.

   To edit the View follow these steps:

   a. Click **Edit**. The Update View window displays.

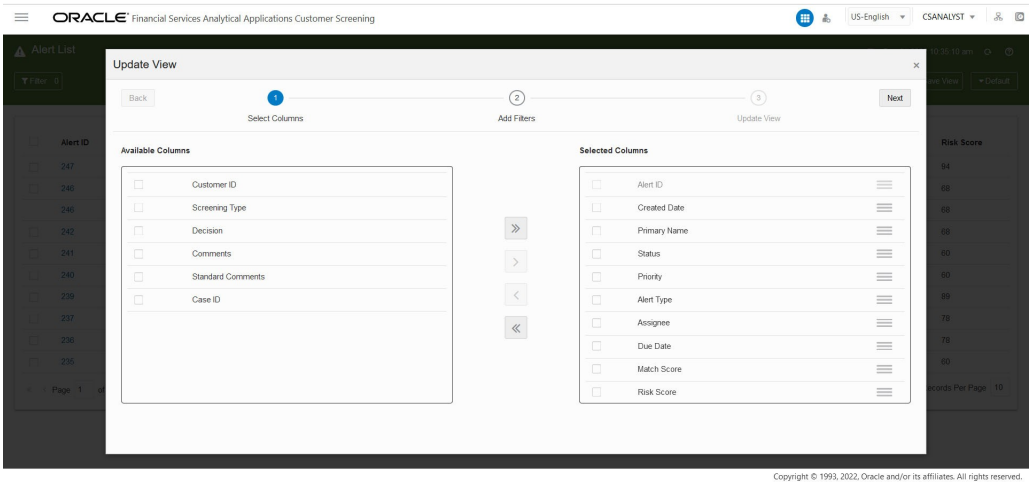
   b. To add new column to the View or delete the column from the View, select the required column from the **Available Column** list or **Selected Column** list and use the following icon to move columns:

   - Use icon to move all Columns from the **Available Columns** list to the **Selected Columns** list to add new columns.
   - Use icon to move the selected Columns from the **Available Columns** list to the **Selected Columns** list to add new columns.
   - Use icon to move the selected Columns from the **Selected Columns** list to the **Available Columns** list to delete the columns.

- Use  icon to move All Columns except Alert ID from **Selected Columns** list to the **Available Columns** list to delete the columns.

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

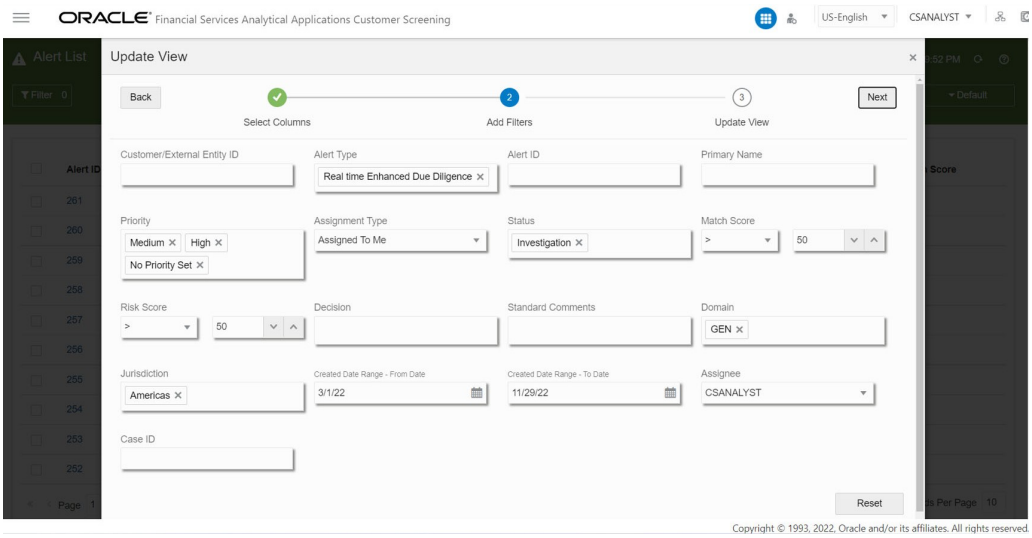
Figure 3-15 Select Columns



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

> **Note:**
>
> Use the **Reset** option to reset all the filter values.

Figure 3-16 Add Filters



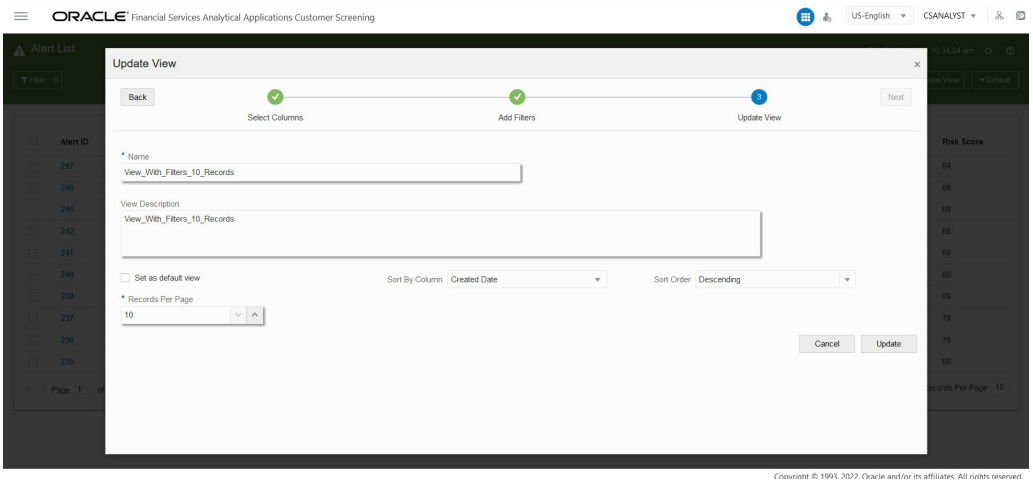
e. You can edit **Name**, **View Description** and **Records Per Page** field in the Update View page. To set the current view as the default view click **Set as default view** check box.

> **Note:**
>
> **Name** and **Records Per Page** are mandatory fields.

f. Click **Update**. A confirmation warning message is displayed.

g. To overwrite the existing view click **Yes**. To cancel click **No**.

Figure 3-17 Update View



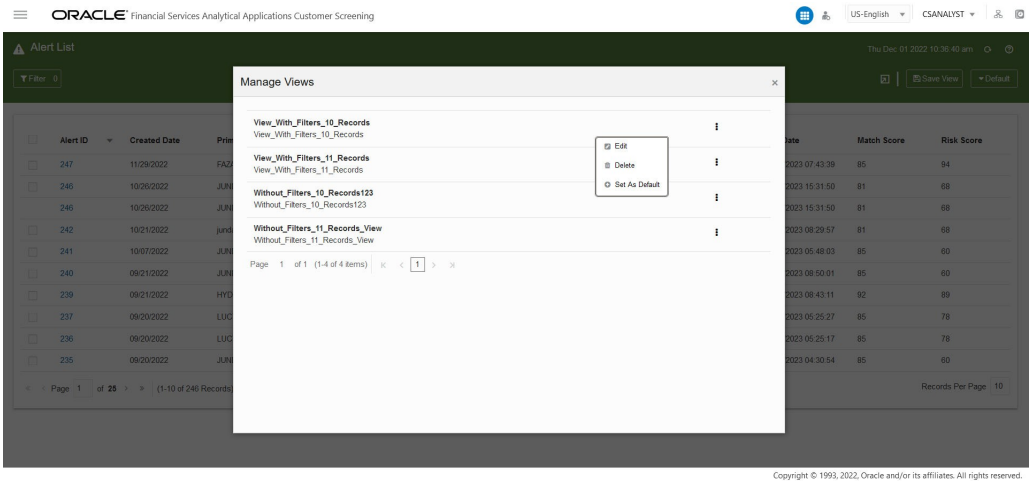
To delete the View, follow these steps:

a. Click **Delete**. A confirmation warning message is displayed.

b. To delete the selected View click **Yes**. To cancel, click **No**.

To set the view as default view click **Set as Default** and to remove the applied default view click **Remove Default**.

Figure 3-18 Manage Views



3.3.3.9 Closed Alerts

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

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

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

3.3.3.10 Exporting 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.

3.3.3.11 Reload Grid for Alert List

In the top right corner, click the Reload  icon to refresh the current view.

3.3.3.12 Bulk Action

You can take bulk action against alerts by selecting multiple alerts from the list.

To take bulk action on the alerts, follow these steps:

1. Select an alert or multiple alerts from the list. The Bulk Action feature is displayed.
2. Click **Bulk Action**. The Bulk Action window is displayed.

> **Note:**
>
> A Warning message pop-up is displayed with the list of selected alert IDs in the following scenarios:
>
> - If the selected alert IDs has any pending events.
> - If any alert is locked by other user.
>
> Click **Yes** to continue or **No** to cancel. If you click **Yes**, Alert ID locked by other user will be filtered and the **Bulk Action** window is displayed.
>
> The Bulk Action window will not be displayed if no common actions are available for selected alerts.

3. From the **Bulk Action** window, select the decision. The decisions common to all the selected alerts are only displayed in the list. Selecting the decision is a mandatory field. You can configure the alert decision to be displayed for the bulk action for the alerts. For more information on configuring alert decisions, see OFS Customer Screening Administrator Guide.

4. Select one or more Standard Comments from the drop-down list in the Standard Comments section. It is mandatory to provide a standard comment or a free text comment.
5. In the Comments section, enter your comments and click **Save**. A message pop-up window is displayed.

> **Note:**
>
> If the bulk action on the events are configured, events are updated as per the configuration. This feature allows you to make decisions on events in bulk in accordance with the bulk action feature that is currently available for alerts on the alert list page. This feature can be enabled or disabled, and the required event decision mapping for alert decisions can be performed in the backend. For more information on bulk action on the events configuration, see General Configurations section in OFS Customer Screening Administrator Guide.
> A Warning message pop-up is displayed in the following scenarios:
>
> - If you close the event as a **False Positive** if any one of the events is **True Positive**.
> - If you select as **Recommend True Match** if all the events are **False Positive**.
>
> You can review the alerts and change the event status for bulk action against these alert IDs or click **Yes** to complete bulk action for the remainder of the alert.

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

3.3.3.13 Field Descriptions for Alert List

The following table lists the Field Description for Alert List.

Table 3-3 Alert List - Field Description

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.

Table 3-3 (Cont.) Alert List - Field Description

Field	Description
Assignment type	Displays the assignment type
WL Record ID	Displays the Watchlist record IDs
Count of WL Record IDs	Displays the count of Watchlist record IDs
Count of Events	Displays the count of Events
Count Of Event Types	Displays the count of event types
Is Bulk Actioned?	Displays whether the alert bulk actioned or not (Yes/No).
Count of ML Closed Events	Displays the count of ML Closed Events
Count of ML Escalated Events	Displays the count of ML Escalated Events

3.4 Alert Details

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

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

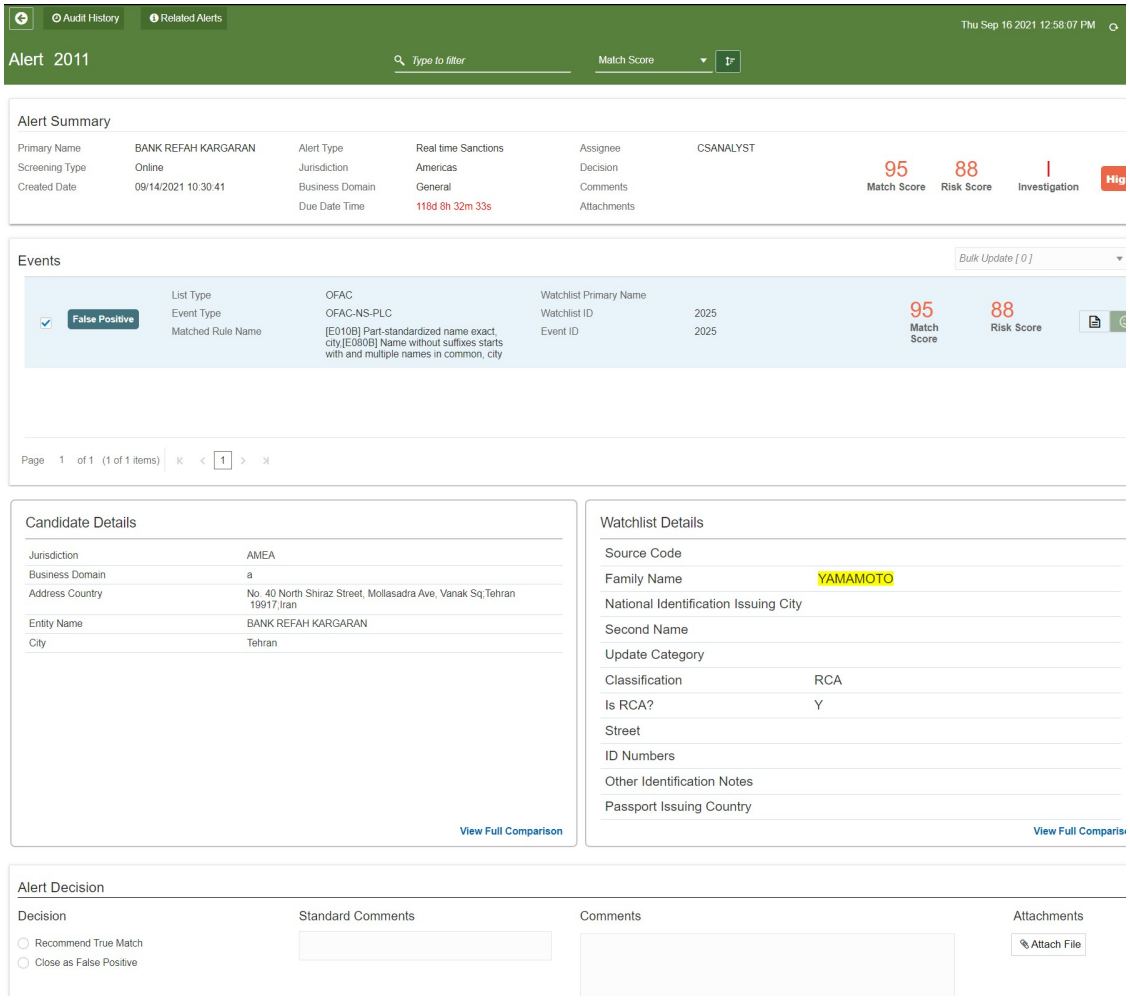
You can configure the functionality assigned to user group in the Alert Details page by assigning the required functional code to the user group. For more information on the list of functional codes configured for different user groups see the OFS Customer Screening Administrator Guide.

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

- Alert Summary
- 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 3-19 Alert Details



3.4.2 Navigating to Previous and Next Alert

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

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

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

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

3.4.3 Printing Alert Details

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

3.4.4 Reload Grid for Alert Details

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

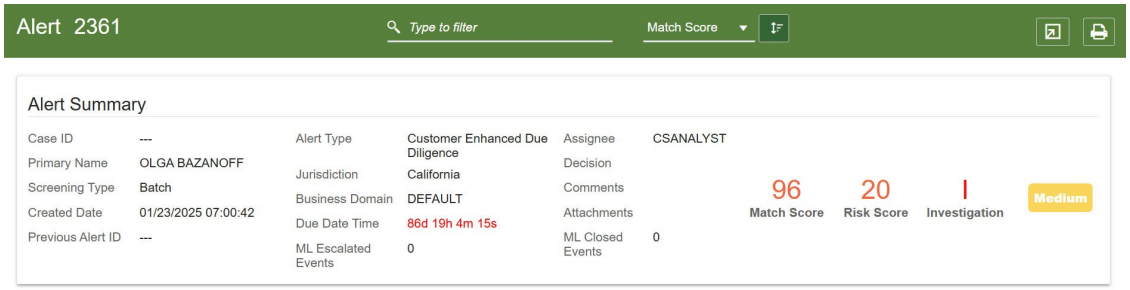
3.4.5 Alert Summary

This topic 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
- Comments
- Match Score
- Risk Score
- Status
- Priority

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

Figure 3-20 Alert Summary



3.4.6 Events

This topic 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

Click on the **Select All** check box to select all the event records for the bulk update. The **Select All** option is configurable. To enable and disable **Select All** option, see the Application Level Configuration section in OFS Customer Screening Administration Guide.

To Customize the number events records displayed per page in the event table, enter the number in the **Records Per Page** entry box. The value must be between 5 and 100.

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

You can save the preference by clicking the **Save** icon and click the **Clear** icon for the default view.

Click on **Match Details** to display all the matched parameters of the event listed in the events table.

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.

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**.

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 

.

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 

.

> **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.

Bulk Update the Events

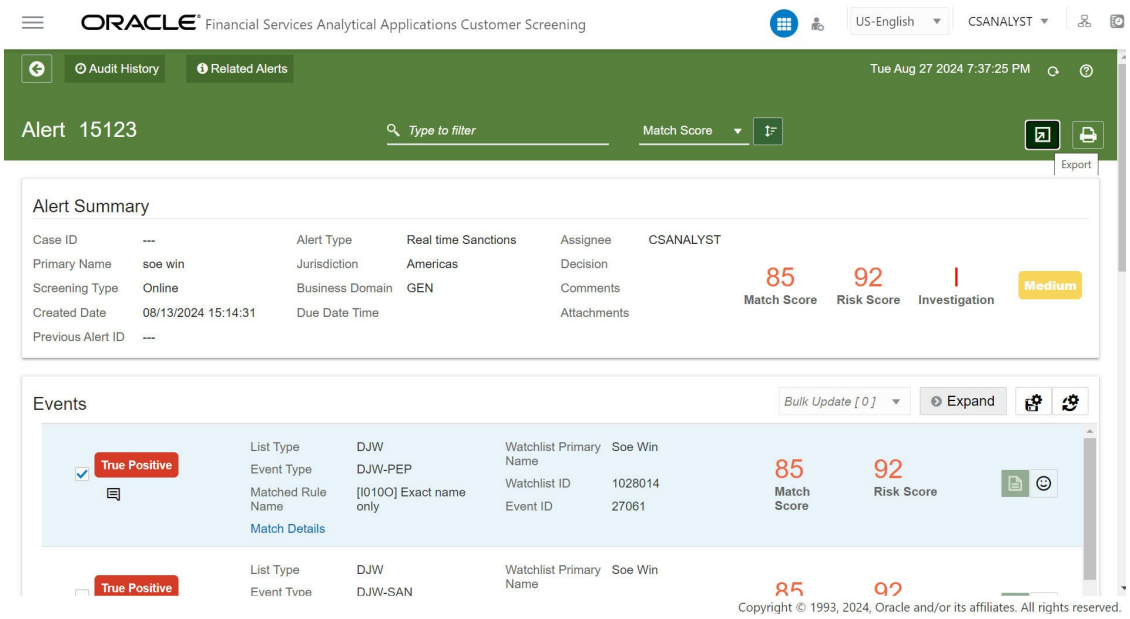
You can bulk update the status of the Events in the Alert. Follow these steps to Bulk update the status:

1. In the **Events** section, select one or more events or click **Select All** check box.
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.

Exporting Event Details

Once you click the export icon, the event details of the alert is exported into excel.

Figure 3-21 Exporting Event Details



Below is the list of columns that are available for Event export:

- Alert ID
- Screening Type
- Entity Type
- Jurisdiction
- Business Domain
- Event ID
- Customer/External Entity ID
- Given Names
- Family Name
- Full Name
- Source Request ID
- Date of Birth
- Primary Citizenship Code
- Secondary Citizenship Code
- Residency Country
- Taxation Country
- Country of Birth
- Country of Incorporation
- Operating Countries
- Employer Name
- Match Score

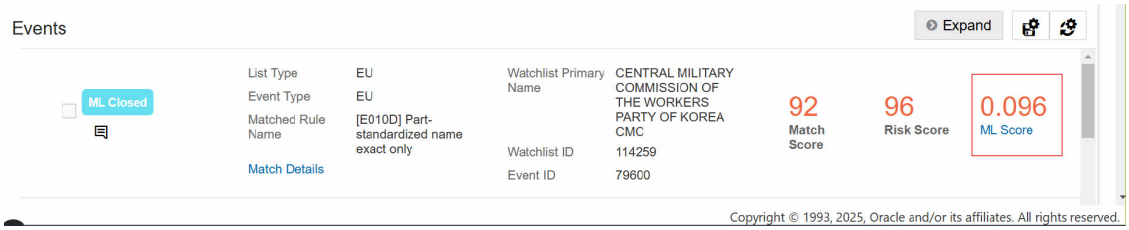
- Watchlist ID
- Watchlist Record Type
- Watchlist Key
- WL Given Names
- WL Family Name
- WL Full Name
- WL DOB
- WLYOB
- WL Country Of Birth
- WL Nationality Countries
- WL Operating Countries
- WL All Countries
- Event Decision
- Comments

3.4.7 ML Score

The ML Score is generated based on the deployed ML Models. For more information see ML Integration with Customer Screening section in the Customer Screening Administration Guide.

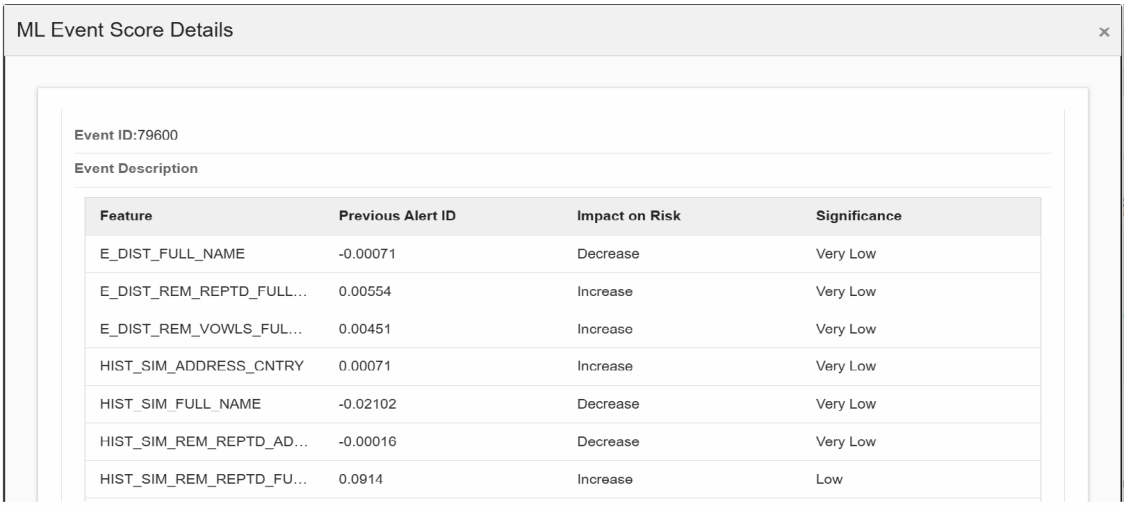
A sample event which is auto closed by ML model is displayed below. A new ML score option is added to display the ML score generated for the event.

Figure 3-22 ML Score



On the ML Alert event details, click **ML Score** to view the details of score. The **ML Event Score Details** window appears.

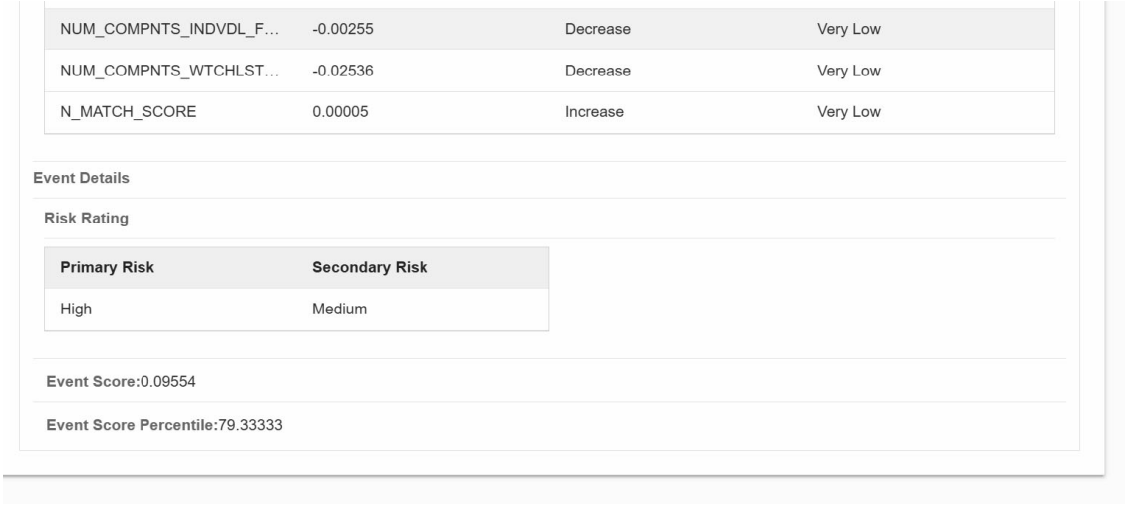
Figure 3-23 The ML Score Window



The ML Event Score Details window shows the list of features and their impact on risk and significance details.

Scroll down to the ML Event Score details window, it shows **Event Details**, **Event score** and **Event Score Percentile** for selected ML alert.

Figure 3-24 The ML Score Window



For more information about features, refer to the Feature Engineering section in latest OFS Compliance Studio Use Case Guide.

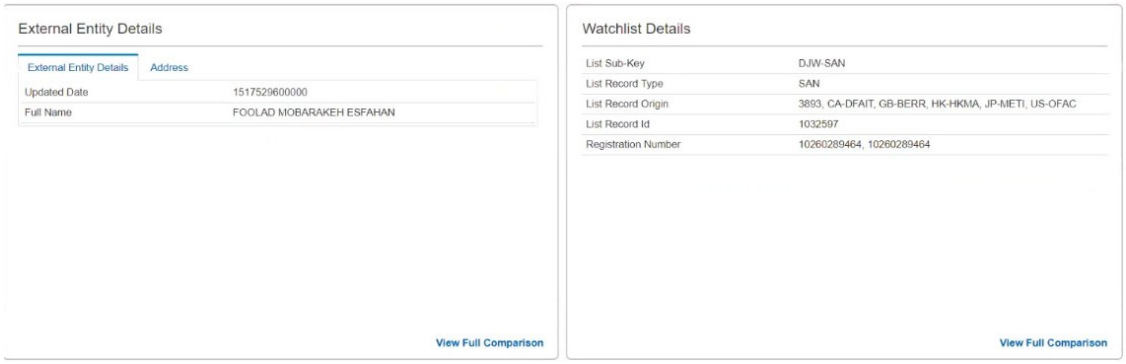
3.4.8 External Entity Details and Corresponding Watchlist Details

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 3-25 External Entity Details

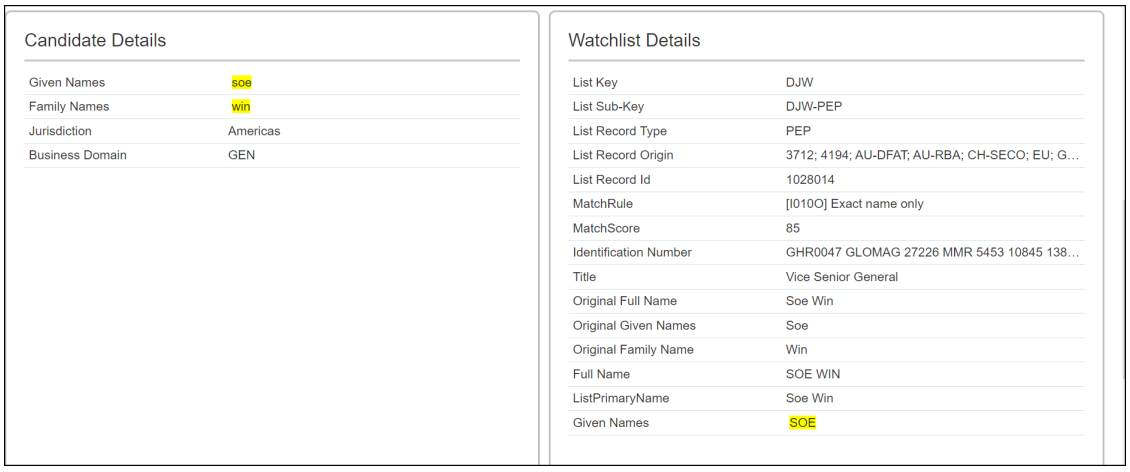


3.4.9 Candidate Details and Corresponding Watchlist Details

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.

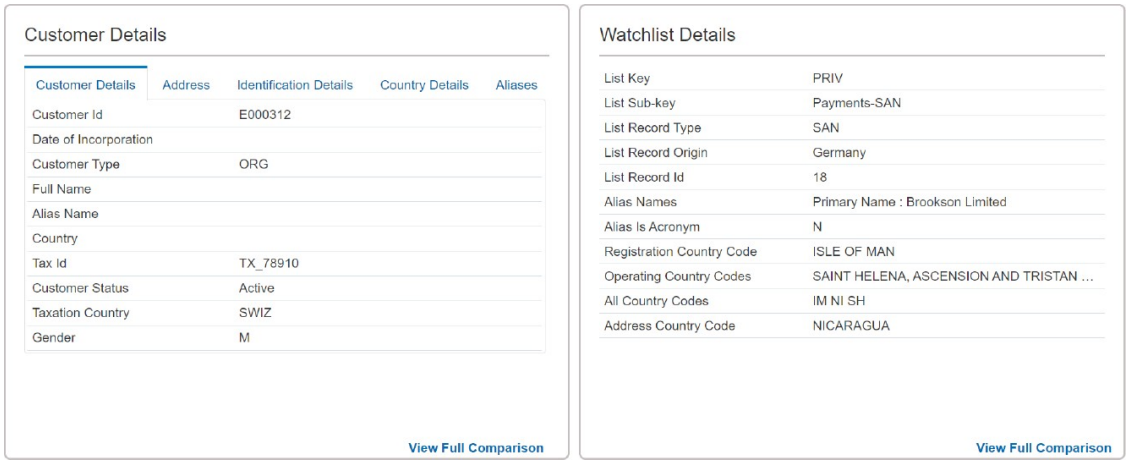
Figure 3-26 Candidate Details



3.4.10 Customer Details and Corresponding Watchlist Details

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

Figure 3-27 Customer Details



The details that are displayed in this section depend on the type of Customer data that is found. The Subsequent fields are displayed in the Customer Details UI:

- Customer Id
- Date of Incorporation
- Customer Type
- Full Name
- Alias Name
- Country
- Tax ID
- Customer Status
- Taxation Country
- Gender

> **Note:**
>
> You can accommodate a maximum of 12 fields in the Customer Details main page UI.

You can compare the Customer Details with the Watchlist Details. Click **View Full Comparison** at the bottom right corner of the section for the complete list of fields. 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.

You can add extra fields for comparison in the Alert Details page and configure the fields to display in the Customer Details main page UI. For more information on adding additional Fields in the Customer Details section, see OFS Customer Screening Administrator Guide.

3.4.11 Alert Decision

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

> **Note:**
>
> A Reviewer user cannot access the alert decision.

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

Alert Decision for (SAN and Prohibition) - Supervisor

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

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

Promoting to Case for SAN - Supervisor

The Promote to Case status is available when the Enterprise Case Management (ECM) L2 is enabled and status of the Alert is in Pending Review. See Promoting to case PMF work flow for the Process Modeling Framework (PMF) work flow.

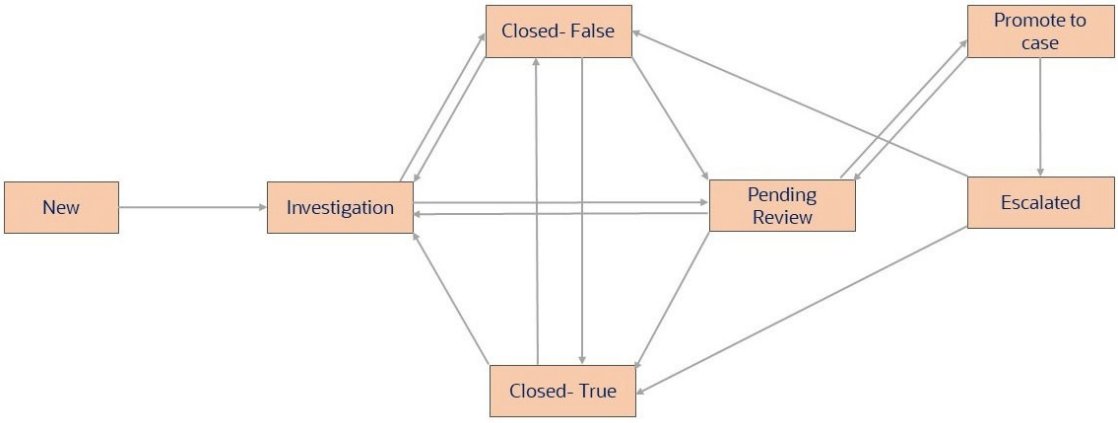
> **Note:**
>
> Bulk Alerts cannot be promoted to case.

To promote to case for SAN, follow these steps:

1. From the **Alert Decision**section, select the **Promote to Case**button.
2. Select the **Standard Comments** and then enter the comments to explain your analysis. Click **Clear** if you want to clear the comments.
3. Add the attachments, if any and, click **Save and Close** or Clear to **Clear** the attachment and details.

When you select Promote to Case, a new case will be created in ECM for the same Alert for the next level analysis.

Figure 3-28 Promoting to Case PMF Work Flow



> **Note:**
>
> To integrate TF alerts with ECM post promoting to case, see the **Configuring Sanctions Server Details for L2 Feedback** section in the ECM Administration and Configuration Guide.

3.4.12 Alert Status

Alert Status (For all Alert types) - Analyst

- New
- Investigation

Alert Status for (SAN and Prohibition) - Supervisor

- Pending Review
- Closed False Positive

- Closed - True Match Exit Required

Alert Status (PEP and EDD) - Supervisor

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

Alert Status for OWS migrated watchlist data

- Closed - False Positive - Migrated from OWS
- Closed - Migrated from OWS
- Closed - True Match Exit Required- Migrated from OWS
- Resolved - Migrated from OWS
- True Match Exit Required - Migrated from OWS

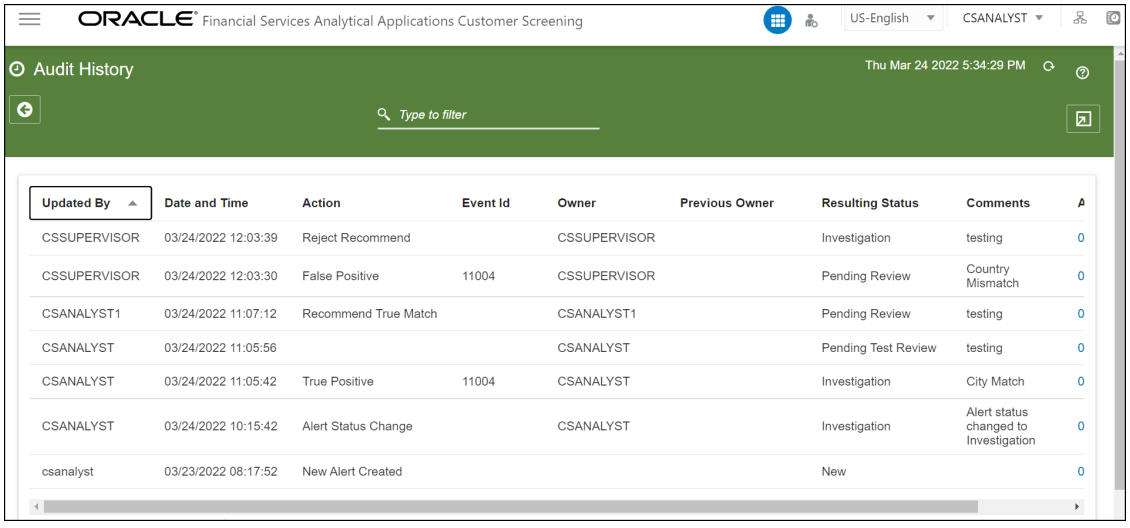
Alert Status for ML decision Data

- ML Closed
- ML Escalated

3.4.13 Audit History

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

Figure 3-29 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
- Is Bulk Actioned?

You can use the search filter in the top middle of the page to filter the Audit History list. Enter the search term in the search box to filter the list. Click the Reload icon next to the Last Modified Date Time to reload the Audit History list.

The following table lists the Field descriptions for Audit History.

Table 3-4 Audit History - Field Description

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.
Is Bulk Actioned?	Displays whether the alert bulk actioned or not (Yes/No).

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.

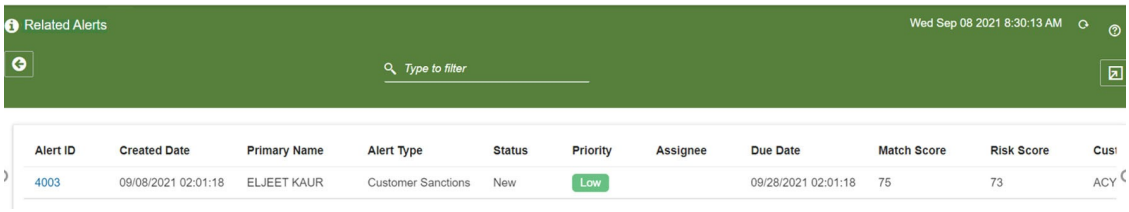
3.4.14 Related Alerts

This topic 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 3-30 Related Alerts



This topic 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.

The following table lists the field descriptions for Related Alerts.

Table 3-5 Related Alerts - Field Description

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.

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.

3.4.15 Field descriptions for Alert Details

The following table lists the Field descriptions for Alert Details.

Table 3-6 Alert Details - Field Description

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.