

**Oracle Financial Services Fraud
Enterprise Edition (Real Time Fraud)**

User Guide

Release 8.1.2.6.0

October 2023

E98368-07

ORACLE®

Financial Services

OFS Fraud Enterprise Edition (Real Time Fraud)

Copyright © 2015, 2023, Oracle and/or its affiliates.

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

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

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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

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

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

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

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility

Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

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

Document Control

Table 1: Document Control

Version Number	Revision Date	Change Log
8.1.2.6.0	October 2023	There are no updates to this guide in this release.
8.1.2.5.0	June 2023	Added <i>Assigning the Alerts</i> section and details on <i>Alert Archival</i> in Managing OFS Enterprise Wire Fraud and Managing OFS Enterprise Card Fraud sections.
8.1.2.4.0	March 2023	Updated the Managing OFS Enterprise Wire Fraud section.
8.1.2.3.0	December 2022	Updated the details regarding ECM integration in sections Transaction Summary Details and Using Card Fraud Transaction Filters .
8.1.2.2.0	Created: September 2022	Created the first version of Fraud Enterprise Edition (Real Time Fraud Component) User Guide for 8.1.2.2.0 Release.

Table of Contents

1	About this Guide.....	5
1.1	Summary.....	5
1.2	Audience.....	5
1.3	Related Documents.....	5
1.4	Conventions Used in this Guide.....	5
1.5	Abbreviations Used in this Guide.....	6
2	About OFS Real Time Fraud.....	7
2.1	Overview.....	7
3	Getting Started.....	9
3.1	Access OFS Real Time Fraud.....	9
4	Managing OFS Enterprise Wire Fraud.....	11
4.1	Using Wire Fraud Transaction Filters.....	11
4.2	Managing Wire Fraud Transactions.....	12
4.3	Assigning the Alerts.....	14
4.3.1	<i>Bulk Assigning the Alerts</i>	15
4.4	Alert List Details.....	15
4.5	Alert Information.....	16
5	Managing OFS Enterprise Card Fraud.....	18
5.1	Using Card Fraud Transaction Filters.....	18
5.2	Managing Card Fraud Transactions.....	19
5.3	Assigning the Alerts.....	21
5.3.1	<i>Bulk Assigning the Alerts</i>	22
5.4	Alert List Details.....	22
5.5	Alert Information.....	23
6	OFSAA Support Contact Details.....	25
7	Send Us Your Comments.....	26

1 About this Guide

This guide explains the concepts for the Real Time Fraud component in the Oracle Financial Services (OFS) Enterprise Edition application. It provides step-by-step instructions for navigating through the Fraud application, analyzing suspicious transactions, and taking necessary actions/decisions on those transactions.

Topics:

- [Summary](#)
- [Audience](#)
- [Related Documents](#)
- [Conventions Used in this Guide](#)
- [Abbreviations Used in this Guide](#)

1.1 Summary

You can find the latest copy of this document on the [Oracle Help Center](#) Documentation Library which includes all the recent additions/revisions (if any) done till date.

1.2 Audience

This guide is intended for end users such as Fraud Analysts who analyze real-time transactions, identify and investigate fraudulent transactions, and make quick decisions to hold or release transactions.

1.3 Related Documents

This section identifies additional documents related to the OFS Real Time Fraud component. You can access the following documents from [Oracle Help Center](#) Documentation Library:

- Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud) Administration and Configuration Guide

1.4 Conventions Used in this Guide

[Table 1](#) lists the conventions used in this guide and their associated meanings.

Table 1: Conventions Used in this Guide

Convention	Meaning
Boldface	Boldface type indicates graphical user interface elements associated with an action (menu names, field names, options, button names) or terms defined in text or glossary.
<i>Italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Table 1: Conventions Used in this Guide

Convention	Meaning
monospace	Monospace type indicates the following: <ul style="list-style-type: none"> • Directories and subdirectories • File names and extensions • Process names • Code sample, that includes keywords, variables, and user-defined program elements within the text.
<variable>	Substitute input value.

1.5 Abbreviations Used in this Guide

Table 2 lists the abbreviations used in this guide.

Table 2: Abbreviations and their meaning

Abbreviation	Meaning
BIC	Bank Identifier Code
ECM	Enterprise Case Management
FCCM	Financial Crime and Compliance Management
IBAN	International Bank Account Number
IPE	Inline Processing Engine
OFS	Oracle Financial Services
OFSAA	Oracle Financial Services Analytical Applications

2 About OFS Real Time Fraud

This section details on Oracle Financial Services Real time fraud.

Topics:

- [Overview](#)

2.1 Overview

The Oracle Financial Services (OFS) Real Time Fraud solution provides a comprehensive set of fraud scenarios, sophisticated behavior detection, profiling techniques, and advanced risk scoring that drives targeted and effective fraud detection for current and future schemes.

Real Time Fraud application is built using Financial Crime and Compliance management (FCCM) Scoring Engine i.e., Inline Processing Engine (IPE), which evaluates and assesses scores of incoming transactions in real-time, near real-time, or batch to make quick decisions to hold or release transactions.

Real Time Fraud offers essentially two components namely Real Time Wire Fraud and Real Time Card Fraud. These components provides the information required to investigate suspicious wire/Card transactions. A transaction is identified as fraud based on certain rules configured in the IPE.

Figure 1: Real Time Wire Fraud Process Flow

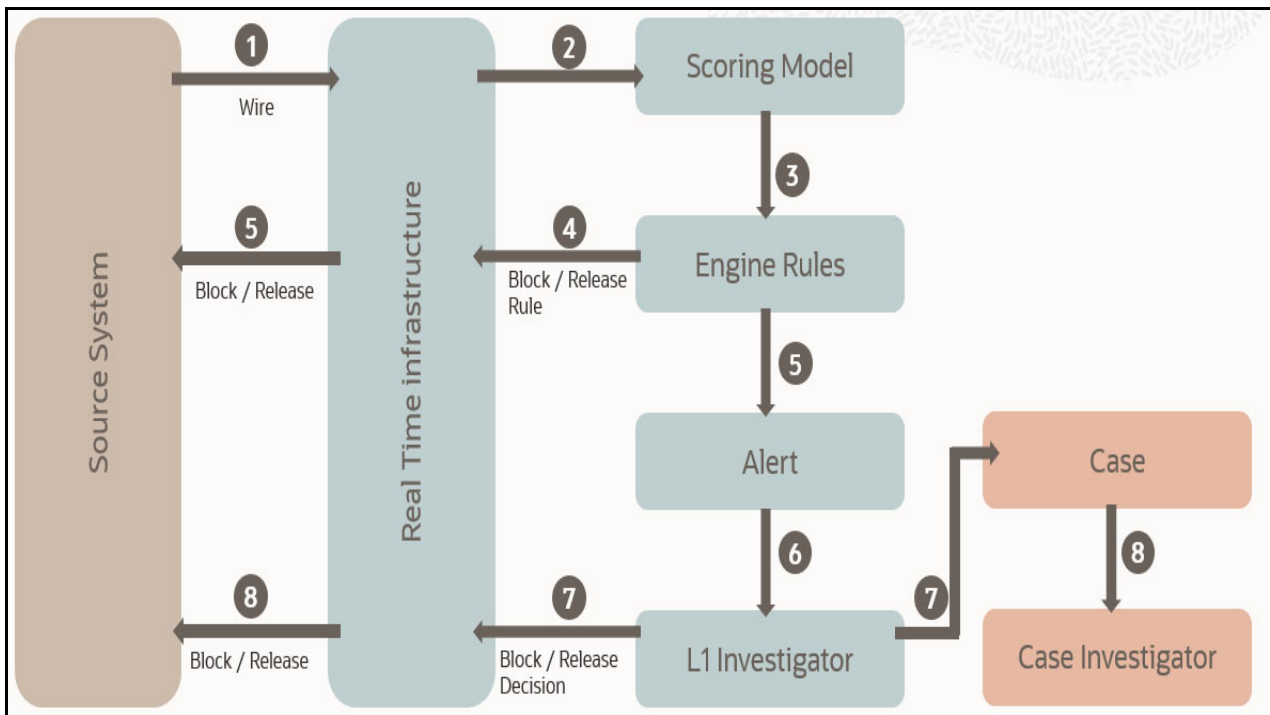
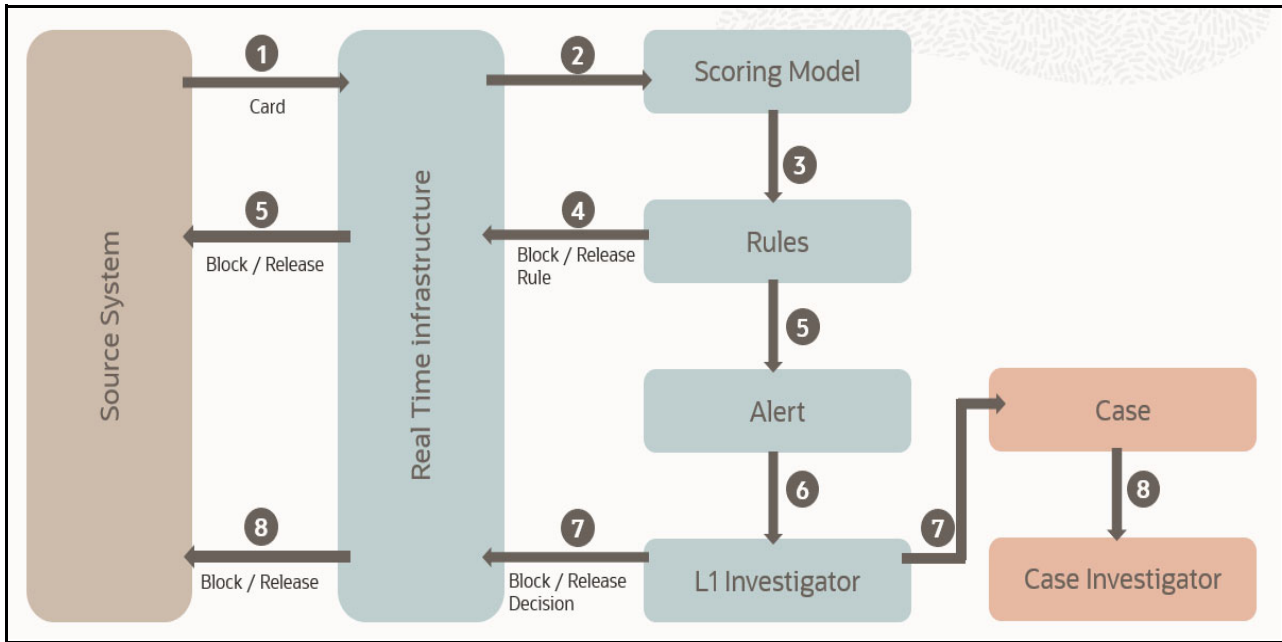


Figure 2: Real Time Card Fraud Process Flow



3 Getting Started

Getting Started introduces you to the Oracle Financial Services (OFS) Real Time Fraud component and provides the information you need to know to use the application.

Topics:

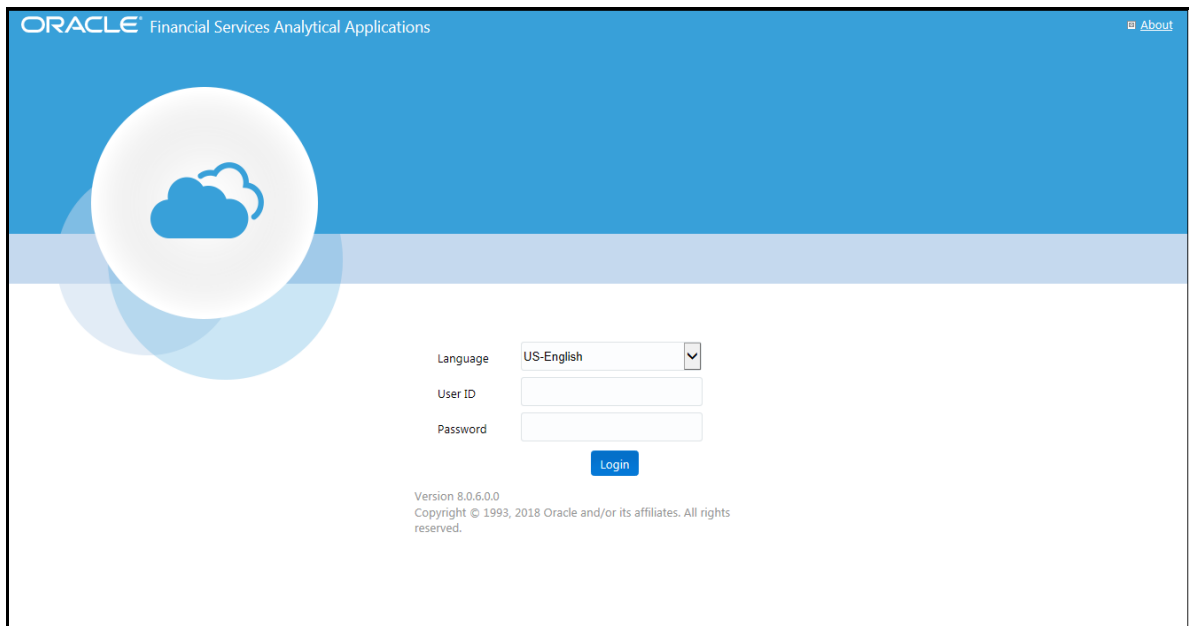
- [Access OFS Real Time Fraud](#)

3.1 Access OFS Real Time Fraud

To access OFS Real Time Fraud:

1. Enter the Oracle Financial Services Analytical Applications (OFSAA) URL in your browser.
This displays the OFSAA Login page.

Figure 3: OFSAA Login Page



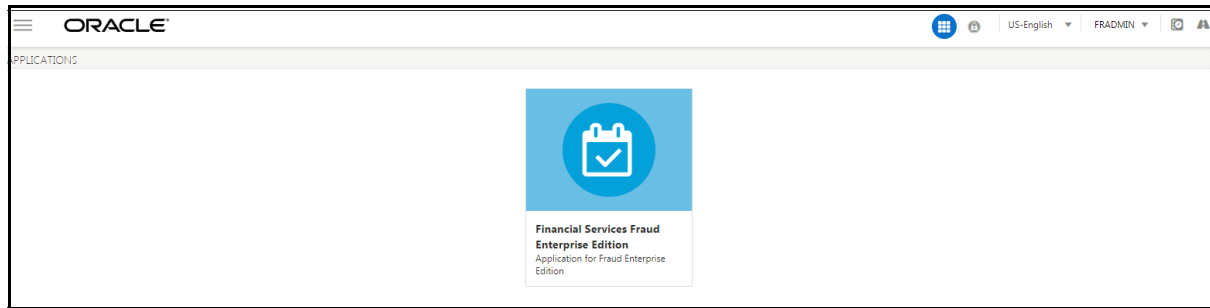
2. Select the **Language**.
3. Enter your **User ID** and **Password**.

NOTE

The User ID must have been already mapped to RT Fraud groups. For more information on mapping user to user groups, see [Oracle Financial Services Analytical Applications Infrastructure User Guide](#).

4. Click **Login**.
This action displays the **Applications** page.

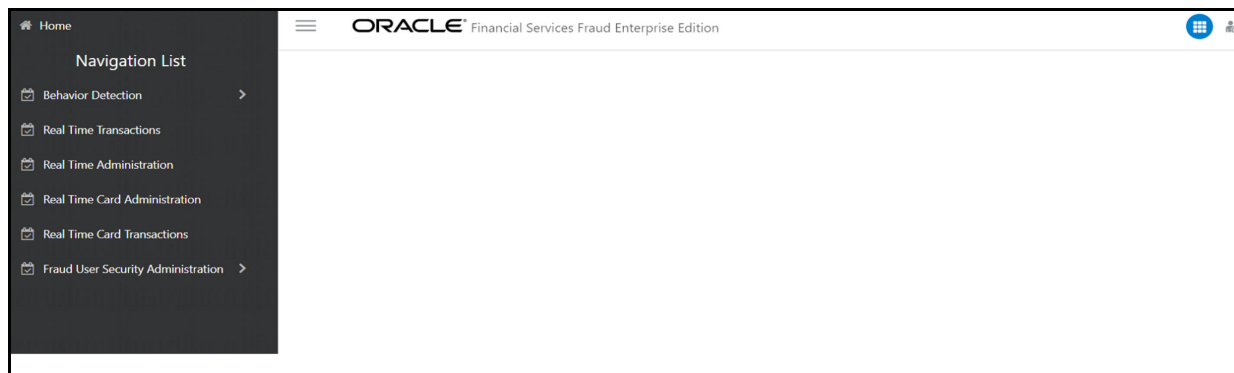
Figure 4: Fraud Enterprise Edition Applications Page



5. Click **Financial Services Fraud Enterprise Edition** from the Tiles menu.

This action displays the Financial Services Fraud Enterprise Edition Home page with the navigation list to the left.

Figure 5: Fraud Enterprise Edition Home Page



6. Click **Real Time Wire Transactions** or **Real Time Card Transactions** in the Navigation List based on your requirement.

This action displays the Wire or Card transactions page.

4 Managing OFS Enterprise Wire Fraud

This chapter details on how to manage the Oracle Financial Services (OFS) Enterprise Wire Fraud.

Topics:

- [Using Wire Fraud Transaction Filters](#)
- [Managing Wire Fraud Transactions](#)
- [Assigning the Alerts](#)
- [Alert Information](#)

4.1 Using Wire Fraud Transaction Filters

You can use the filter fields to search for a wire transaction. To view the filter fields follow these steps:

1. Login to the Real Time Fraud Application as a fraud administrator.
2. Click **Financial Services Fraud Enterprise Edition** and select **Real Time Wire Transactions**.
3. On the **Alert List** page, click **Filter**.
4. Enter the values in any of the following fields.

Table 3: Wire Fraud Transaction Filter Fields

Field	Description
Originator	Enter the name of the originator.
Originator Account	Enter the account number of the originator.
Alert ID	Enter the alert ID of the transaction.
Transaction ID	Enter the transaction ID.
Customer ID	Enter the customer ID.
Business Domain	Enter the business domain of the account holder.
Beneficiary	Enter the name of the transaction beneficiary.
Location	Enter the IP address of the transaction country
Direction	Enter the direction of the transaction message.
Decision	Enter the decision made during the alert.
Status	Select a status of the transactions from the following: <ul style="list-style-type: none"> • Assigned • Assigned To Me • Hold • Block • Release
Assignee	Select the assignee from the drop-down list.
Currency	Select the currency type of the transaction.
Jurisdiction	Select the jurisdiction of the transaction.

Table 3: Wire Fraud Transaction Filter Fields

Field	Description
Risk Score	You can filter the transactions based on the risk associated with it. Select a logical operator (=, >, <, >=, <=) from the drop-down list and enter the risk score.
Amount	You can filter the transactions based on the amount of the transactions. Select a logical operator (=, >, <, >=, <=) from the drop-down list and enter the amount.
Created Date	Enter the date on which the transaction entry is created.

4.2 Managing Wire Fraud Transactions

The following steps shows how to manage the OFS wire fraud transactions.

1. Navigate to the OFS Enterprise Fraud Real Time Wire Transactions page.

Figure 6: OFS Enterprise Fraud Real Time Wire Transactions Page

Alert ID	Transaction ID	Status	SLA	Assignee	Assign	Direction	Amount	Currency	Risk Score
383890	518381	H	-7499m:36s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10
383891	518384	H	-6135m:25s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10
383892	518382	H	-6135m:24s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10
383893	518383	H	-6135m:23s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10
383894	518385	H	-6135m:23s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10
383895	518386	H	-6135m:23s		<input type="checkbox"/>	OUTGOING	15000	DOLLAR	10

2. This section displays the details of all the identified suspicious transactions, and allows you to take necessary actions. All the suspicious transactions are in Held status. By default, this section displays the transactions in Held Status. For more information, see [Assigning the Alerts](#).
 - Click **Export** on the top-right of the page to download the alert list.
 - To update the columns shown on the **Alert List** page, click **Columns** on the top-right of the page. Select the required columns that you wish to see and click **Save**.
 - To view the archived alerts, turn on the **Show Archived**.

NOTE

The **Show Archived** button is available only if the Archival Configuration is enabled. For more information on Configuring Alert archival, see [Configuring Alert Archival](#) section in [OFS Real Time Fraud Administration Guide](#).

- Click on any Alert ID on the **Alert List** page to view more details. For more information, see [Alert Information](#).

NOTE While a user is viewing an Alert ID details, the alert will be locked for some time interval. Hence any other user wont be able to able to take any actions against that Alert ID. However the Supervisor has the required permissions to assign the locked alert to a different user.

Figure 7: Alert details Page

The screenshot shows the Oracle Financial Services Enterprise Fraud interface. At the top, it displays 'Alert 458790'. Below this is the 'Alert Summary' section, which contains a table with the following data:

Transaction ID	Status	Case ID	Case Status	Originator	Orig. Account	Beneficiary	Benef. Account	Direction	Amount	Currency	Location
627785	Blocked	CA15850	Confirmed Fraud Action	Oct12Test10	EXMLNHRTH RCP-3804	Jokovic	ACPOTCHKFRA C-6540	OUTGOING	999888	DOLLAR	India

Below the table, there are sections for 'Historical Transactions' with a filter and 'Sync Horizontal Scroll' option, and a summary bar showing: Held: 1, Assigned: 4, Blocked - Case Created: 12, Released: 1. The 'Score Card' section shows a Risk Score of 10 and a 'Wire Cross Border Transaction' indicator. The 'Transaction Risk Information' section includes session details like IP Address (12.56.23.86) and Channel (SWIFT).

- If ECM application is integrated, you can click on the **Case ID** in **Alert Summary** section to view the case details.
 - Scroll the Alert details page for additional Customer details and the Alert decision.
- The following figure shows the customer details without Enterprise Case Management (ECM) integration.

Figure 8: Customer Details in Alert Details Page without ECM Integration

The screenshot shows the 'Customer details' section of the alert details page. It contains a form with the following fields:

- Customer ID: XXXXCUSPAGERISKTLAC-4500-RB
- Name: Oct12Test10
- Date of birth: xxx
- Alternate name: xxx
- Address Purpose: xxx
- Address: xxx
- Phone purpose: xxx
- Phone: xxx
- Phone extension: xxx
- ID Number: xxx
- ID Jurisdiction: xxx
- Country of Citizenship: xxx

Below the customer details is the 'Alert Decision' section. It has two radio buttons: 'Release' (selected) and 'Block'. There is a 'Comments' field with the text 'adding comments wire'. To the right, there is an 'Attachments' section showing '1 Items'. At the bottom right, there are two buttons: 'Save and Next' and 'Save and Close'.

The following figure shows the customer details with ECM integration.

Figure 9: Customer Details in Alert Details Page with ECM Integration

Customer details		
Customer ID XXXCUSPAGERISKTOCAC-4500-RB	Address Purpose	ID Number xxx
Name Oct12Test10	Address	ID Jurisdiction xxx
Date of birth	Phone purpose xxx	Country of Citizenship
Alternate name xxx	Phone	
	Phone extension xxx	

Alert Decision		
Decision	Comments	Attachments
Release Block - Potential Fraud - Create a case Block - Non Fraud	adding comments wire	1 Items
		Save and Next Save and Close

- The Audit History table records historic actions on a specific Alert. This would include details like when the alert was created, blocked or unblocked etc.

Figure 10: Audit History Page

ORACLE Financial Services Enterprise Fraud

Audit History Tue Feb 21 2023 1:45:00 PM

Type to Filter


Updated By	User Role	Alert ID	Action Details	Assignee Full Name	Assignee Employee ID	Assignee Role	Comment	Action Date
WIREADMIN	WIREFRAUDADMIN	3784	Release	WIREADMIN	WIREADMIN	CARDFRAUDADMIN	adding comments wire	2023-02-17 13:41:20
WIREADMIN	WIREFRAUDADMIN	3784	Comment Added	WIREADMIN	WIREADMIN	CARDFRAUDADMIN	adding comments wire	2023-02-17 13:40:23
WIREADMIN	WIREFRAUDADMIN	3784	Assigned	WIREADMIN	WIREADMIN	CARDFRAUDADMIN	Assigned to WIREADMIN	2023-02-15 21:19:38
WIREADMIN	WIREFRAUDADMIN	3784	Held	WIREADMIN	WIREADMIN	CARDFRAUDADMIN	De-assigned by WIREADMIN	2023-02-15 20:19:36
WIREADMIN	WIREFRAUDADMIN	3784	Assigned	WIREADMIN	WIREADMIN	CARDFRAUDADMIN	Assigned to WIREADMIN	2023-02-15 18:50:47
SYSTEM		3784	Held				Alert created	2023-02-15 16:49:55

Page 1 of 1 (1-6 of 6 Items) < 1 >

4.3 Assigning the Alerts

The **Alert List** page allows the users to assign an alert to self.

To assign an alert to self, follow these steps:

- Login to **Fraud Enterprise Edition** using your **User ID** and **Password**.
- Click **Financial Services Fraud Enterprise Edition**  to open the **Navigation List**.
- Click **Real Time Wire Transactions**. This opens the **Alert List**.
- To assign an alert to self, turn **ON** the toggle button under **Assign** of the respective alert.

This action assigns the alert to self.

4.3.1 Bulk Assigning the Alerts

The **Alert List** page allows the Senior Supervisor to bulk assign alerts to any user.

To bulk assign alerts, follow these steps:


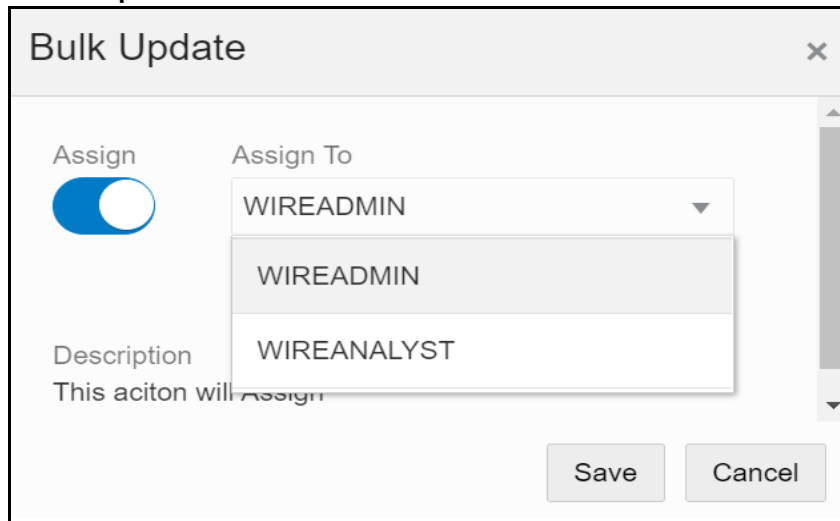
1. Login to **Fraud Enterprise Edition** as a Wire Senior Supervisor. For more information on the user roles and privileges, see **Mapping a User with A User Group** section in *OFS Real Time Fraud Administration Guide*.
2. Click **Financial Services Fraud Enterprise Edition**  to open the **Navigation List**.
3. Click **Real Time Wire Transactions**. This opens the **Alert List**.
4. To bulk assign alerts, select the alerts that you want to assign to any user using the check boxes.
5. Click **Bulk Update** to open the **Bulk Update** window.

Figure 11: Bulk Update Window



6. Turn **ON** the **Assign** toggle button and select the user from the **Assign To** drop-down.
7. Click **Save** to assign the alerts.

This action assigns the alerts to the selected user.

4.4 Alert List Details

Table 4 shows the Alert List details:

Table 4: Alert List Details

Column Name/ Field Name/Icon	Description
Alert ID	Unique identifier for the Alert
Transaction ID	The sequence ID number of the Transaction.
Status	The status of the Alert

Table 4: Alert List Details

Column Name/ Field Name/Icon	Description
SLA	This is the Service Level Agreement for the Alert (in minutes).
Assignee	The assignee of the Alert.
Assign	Used for assigning the Alert.
Direction	The direction of the message.
Amount	The original amount of the Transaction.
Currency	The original currency in which the Transaction was conducted.
Risk Score	The risk score assigned to the Transaction.
Created Date	The date when the Transaction was initiated.
Decision	The decision code of the Alert.
Jurisdiction	The jurisdiction of the Alert.
Business Domain	The business domain code of the Alert.
Customer ID	Customer unique identifier.
Originator	The identifier of the originating party of the Transaction.
Originator Account	The IBAN of the originating party of the Transaction.
Beneficiary	The IBAN of the beneficiary party of the Transaction.
Location	The source country of the IP address.

4.5 Alert Information

Upon clicking an Alert in the **Alert List** section, additional details of that alert are displayed. These details provide further insight into an alert and can be used for further investigation.

Table 5 shows the alert details.

Table 5: Alert Details

Column Name	Description
Alert Summary	Provides key Alert details to help an Analyst make faster decisions. This includes Alert ID (in the header), Transaction ID, Created Date, Jurisdiction, Business Domain, Amount, Currency, Direction, Assignee, Decision, Comments, Attachments, Risk Score, Status and SLA .
Score card	Provides the Score and highlights for the Analyst to understand what triggered the Alert.
Transaction Details	Provides the transaction details to help an Analyst with faster decisions. This includes Date and Time, Direction, Amount, Currency, Channel, Status, Risk Score, Originator, Originator account, Beneficiary and Location.

Table 5: Alert Details

Column Name	Description
Client Details	<p>The client details have three sections that provide the below details.</p> <p>Customer details - Provides customer details associated with an alert. This includes Name, Alternate Name, User name, Customer number, Date they became customer, Tax ID, ID number, ID jurisdiction, Country of citizenship, Date of birth, Job title, Employer name, Annual income, Credit score, Risk score, Address purpose, Address, Phone purpose, Phone, Phone extension, Most recent login, Most recent IP address, Most recent failed login, and Last password change.</p> <p>Account Details - Provides account details associated with an alert. This includes Account type, Opened, Last updated, Current status/since, Balance, Available, Credit limit/since, Delinquent, Linked payment account, and Added date.</p> <p>Card Details - Provides card details associated with an alert. This includes Card on account, Authorized users, Card number (related to the transaction), Name, Status, Role, Since, Issue date, PIN updated, and Last reject.</p>
Alert Decision	The Analyst provides the decision about an alert here to close the Alert analysis.
Decision Explanation	The Analyst can support the decision on an alert with comments and attachments. Attachment file types supported are image, audio, word, excel and video. The file size should be within 9 MB. Multiple attachments can be included.

5 Managing OFS Enterprise Card Fraud

This chapter details on how to manage the Oracle Financial Services (OFS) Enterprise Card Fraud.

Topics:

- [Using Card Fraud Transaction Filters](#)
- [Managing Card Fraud Transactions](#)
- [Assigning the Alerts](#)
- [Alert Information](#)

5.1 Using Card Fraud Transaction Filters

You can use the filter fields to search for a card transaction. To view the filter fields follow these steps:

1. Login to the Real Time Fraud Application as a fraud administrator.
2. Click **Financial Services Fraud Enterprise Edition** and select **Real Time Card Transactions**.
3. On the **Alert List** page, click **Filter**.
4. Enter the values in any of the following fields.

Table 6: Card Fraud Transaction Filter Fields

Field	Description
Originator	Enter the name of the originator.
Originator Account	Enter the account number of the originator.
Alert ID	Enter the alert ID of the transaction.
Transaction ID	Enter the transaction ID.
Customer ID	Enter the customer ID.
Business Domain	Enter the business domain of the account holder.
Beneficiary	Enter the name of the transaction beneficiary.
Location	Enter the IP address of the transaction country
Direction	Enter the direction of the transaction message.
Decision	Enter the decision made during the alert.
Status	Select a status of the transactions from the following: <ul style="list-style-type: none"> • Assigned • Assigned To Me • Hold • Block • Release
Assignee	Select the assignee from the drop-down list.
Currency	Select the currency type of the transaction.
Jurisdiction	Select the jurisdiction of the transaction.

Table 6: Card Fraud Transaction Filter Fields

Field	Description
Risk Score	You can filter the transactions based on the risk associated with it. Select a logical operator (=, >, <, >=, <=) from the drop-down list and enter the risk score.
Amount	You can filter the transactions based on the amount of the transactions. Select a logical operator (=, >, <, >=, <=) from the drop-down list and enter the amount.
Created Date	Enter the date on which the transaction entry is created.

5.2 Managing Card Fraud Transactions

The following steps shows how to manage the OFS card fraud transactions.

1. Navigate to the OFS Enterprise Fraud Real Time Card Transactions page.

Figure 12: OFS Enterprise Fraud Real Time Card Transactions Page

Alert ID	Transaction ID	Status	SLA	Assignee	Assign	Direction	Amount	Currency	Risk Score
373186	554263	H	-	CARDSRSUPERVISOR	<input checked="" type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10
373187	554264	H	-18793m:53s	CARDSRSUPERVISOR	<input checked="" type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10
373188	554265	H	-18793m:51s		<input type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10
373189	554266	H	-18793m:49s		<input type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10
383884	554284	H	-8846m:10s		<input type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10
383885	554285	H	-8846m:7s		<input type="checkbox"/>	713Ho7BKawWITffD9	30000	INR	10

2. This section displays the details of all the identified suspicious transactions, and allows you to take necessary actions. All the suspicious transactions are in Held status. By default, this section displays the transactions in Held Status. For more information, see [Assigning the Alerts](#).
 - Click **Export** on the top-right of the page to download the alert list.
 - To update the columns shown on the **Alert List** page, click **Columns** on the top-right of the page. Select the required columns that you wish to see and click **Save**.
 - To view the archived alerts, turn on the **Show Archived**.

NOTE The **Show Archived** button is available only if the Archival Configuration is enabled. For more information on Configuring Alert archival, see [Configuring Alert Archival](#) section in [OFS Real Time Fraud Administration Guide](#).

- Click on any Alert ID on the **Alert List** page to view more details. For more information, see [Alert Information](#).

NOTE While a user is viewing an Alert ID details, the alert will be locked for some time interval. Hence any other user wont be able to able to take any actions against that Alert ID. However the Supervisor has the required permissions to assign the locked alert to a different user.

Figure 13: Alert details Page

The screenshot shows the Oracle Financial Services Enterprise Fraud interface. At the top, there's a navigation bar with 'Audit History' and a date/time stamp 'Fri Oct 06 2023 6:17:36 PM'. Below this, the alert ID 'Alert 373188' is displayed. The main section is titled 'Alert Summary' and contains a table with the following data:

Transaction ID	Status	Case ID	Case Status	Originator	Orig. Account	Beneficiary	Direction	Amount	Currency	Location	Start Date
554265	Blocked	CA4871	-	713Ho7BKawwWITfID9	713Ho7BKawwWITfID9	Lorem ipsum dolor sit amet	713Ho7BKawwWITfID9	30000	INR	IP Address Country	2021-05-23T14:13:12

Below the table, there are two sections: 'Score Card' and 'Transaction Risk Information'. The 'Score Card' shows a 'Risk Score' of 10 and a 'Sudden Surge in Revolving Credit Utilization' of 10, with sub-points: '> Account Credit Limit Amount: 10000' and '> Transaction Amount for a card per day: 90000'. The 'Transaction Risk Information' section is divided into 'Session details' and 'Merchant Details'. 'Session details' includes IP Address (10.232.23.34), IP Address Organization name (IP GEO Autonomous System Organization), and IP Address Location (City). 'Merchant Details' includes Device ID, Authentication type (Auth Mode), and Authentication Result.

- If ECM application is integrated, you can click on the **Case ID** in **Alert Summary** section to view the case details.
- Scroll the Alert details page for additional Customer details and the Alert decision.
 The following figure shows the customer details without Enterprise Case Management (ECM) integration.

Figure 14: Customer Details in Alert Details Page without ECM Integration

Customer details			
Customer ID CUST-123	Address Purpose B	ID Number Identifier Number	Credit Score 300
Name Customer First Name	Address Customer Address Line 1	ID Jurisdiction xxx	Risk Score xxx
Date of birth 2010-04-28T00:00:00	Phone purpose B	Country of Citizenship IN	Annual income 3520000
Alternate name Customer Alias	Phone Customer Phone Number 1		
	Phone extension 12345		
Account details		Cards details	
Account Type CL	Last updated xxx	Cards On Account 6	
Opened 2021-04-28T00:00:00	Last password Change 2021-04-28T00:00:00	Card Number 123456134243	Role 2
Balance 1000		Name Name on Card	Issue date 2021-04-12T00:00:00
Credit Limit 100000			
Alert Decision			
Decision	Comments	Attachments	
Release Block	Action taken by RT Fraud system on SLA breach	No attachment items found	
		Save and Next Save and Close	

The following figure shows the customer details with ECM integration.

Figure 15: Customer Details in Alert Details Page with ECM Integration

Customer details			
Customer ID CUST-123	Address Purpose B	ID Number Identifier Number	Credit Score 300
Name Customer First Name	Address Customer Address Line 1	ID Jurisdiction xxx	Risk Score xxx
Date of birth 2010-04-28T00:00:00	Phone purpose B	Country of Citizenship IN	Annual income 3520000
Alternate name Customer Alias	Phone Customer Phone Number 1		
	Phone extension 12345		
Account details		Cards details	
Account Type CL	Last updated xxx	Cards On Account 6	
Opened 2021-04-28T00:00:00	Last password Change 2021-04-28T00:00:00	Card Number 123456134243	Role 2
Balance 1000		Name Name on Card	Issue date 2021-04-12T00:00:00
Credit Limit 100000			
Alert Decision			
Decision	Comments	Attachments	
Block - Potential Fraud - Create a case Block - Non Fraud Release	Action taken by RT Fraud system on SLA breach	No attachment items found	
		Save and Next Save and Close	

- 6. The Audit History table records historic actions on a specific Alert. This would include details like when the alert was created, blocked or unblocked etc.


Figure 16: Audit History Page

Updated By	User Role	Alert ID	Action Details	Assignee Full Name	Assignee Employee ID	Assignee Role	Comment	Action Date
CARDADMIN	CARDFRAUDADMIN	2865	Assigned	CARDADMIN	CARDADMIN	CARDFRAUDADMIN	Assigned to CARDADMIN	2023-02-17 12:31:20
CARDADMIN	CARDFRAUDADMIN	2865	Hold	CARDADMIN	CARDADMIN	CARDFRAUDADMIN	De-assigned by CARDADMIN	2023-02-17 12:31:24
CARDADMIN	CARDFRAUDADMIN	2865	Assigned	CARDADMIN	CARDADMIN	CARDFRAUDADMIN	Assigned to CARDADMIN	2023-02-16 17:03:10
CARDADMIN	CARDFRAUDADMIN	2865	Hold	CARDADMIN	CARDADMIN	CARDFRAUDADMIN	De-assigned by CARDADMIN	2023-02-16 17:03:07
CARDPRDADMIN	CARDFRAUDADMIN	2865	Assigned	cardfraadmin	CARDPRDADMIN	CARDFRAUDADMIN	Assigned to CARDPRDADMIN	2023-02-16 12:44:35
CARDPRDADMIN	CARDFRAUDADMIN	2865	Hold	cardfraadmin	CARDPRDADMIN	CARDFRAUDADMIN	De-assigned by CARDPRDADMIN	2023-02-16 12:44:25
CARDPRDADMIN	CARDFRAUDADMIN	2865	Assigned	cardfraadmin	CARDPRDADMIN	CARDFRAUDADMIN	Assigned to CARDPRDADMIN	2023-02-14 11:11:50
SYSADMIN		2865	Block	System Administrator	SYSADMIN		Action taken by RT Fraud system on SLA breach	2023-02-01 16:46:33
SYSADMIN		2865	Block	System Administrator	SYSADMIN		Action taken by RT Fraud system on SLA breach	2023-02-01 16:46:33
SYSADMIN		2865	Block	System Administrator	SYSADMIN		Action taken by RT Fraud system on SLA breach	2023-02-01 16:46:33

5.3 Assigning the Alerts

The **Alert List** page allows the users to assign an alert to self.

To assign an alert to self, follow these steps:

1. Login to **Fraud Enterprise Edition** using your **User ID** and **Password**.
2. Click **Financial Services Fraud Enterprise Edition**  to open the **Navigation List**.
3. Click **Real Time Card Transactions**. This opens the **Alert List**.
4. To assign an alert to self, turn **ON** the toggle button under **Assign** of the respective alert.

This action assigns the alert to self.

5.3.1 Bulk Assigning the Alerts

The **Alert List** page allows the Senior Supervisor to bulk assign alerts to any user.

To bulk assign alerts, follow these steps:


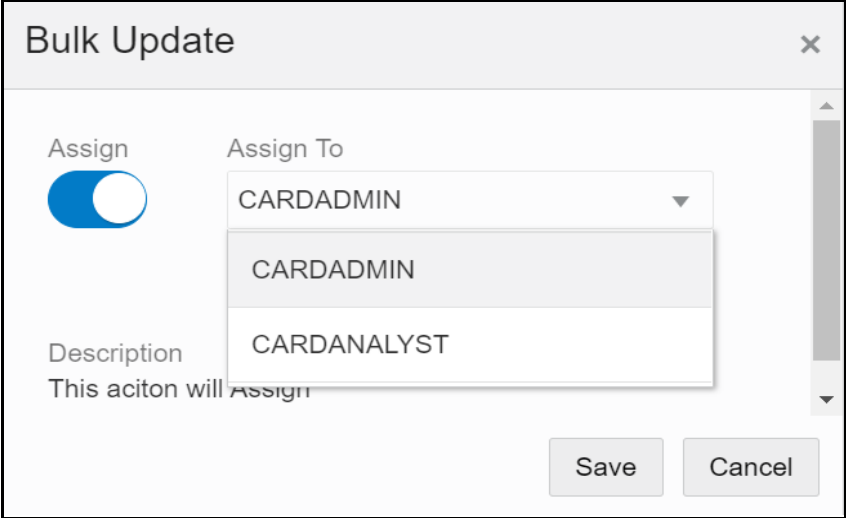
1. Login to **Fraud Enterprise Edition** as a Card Senior Supervisor. For more information on the user roles and privileges, see **Mapping a User with A User Group** section in **OFS Real Time Fraud Administration Guide**.
2. Click **Financial Services Fraud Enterprise Edition**  to open the **Navigation List**.
3. Click **Real Time Card Transactions**. This opens the **Alert List**.
4. To bulk assign alerts, select the alerts that you want to assign to any user using the check boxes.
5. Click **Bulk Update** to open the **Bulk Update** window.

Figure 17: Bulk Update Window



6. Turn **ON** the **Assign** toggle button and select the user from the **Assign To** drop-down.
7. Click **Save** to assign the alerts.

This action assigns the alerts to the selected user.

5.4 Alert List Details

Table 7 shows the Alert List details:

Table 7: Alert List Details

Column Name/ Field Name/Icon	Description
Alert ID	Unique identifier for the Alert
Transaction ID	The sequence ID number of the Transaction.
Status	The status of the Alert
SLA	This is the Service Level Agreement for the Alert (in minutes).
Assignee	The assignee of the Alert.
Assign	Used for assigning the Alert.
Direction	The direction of the message.
Amount	The original amount of the Transaction.
Currency	The original currency in which the Transaction was conducted.
Risk Score	The risk score assigned to the Transaction.
Created Date	The date when the Transaction was initiated.
Decision	The decision code of the Alert.
Jurisdiction	The jurisdiction of the Alert.
Business Domain	The business domain code of the Alert.

Table 7: Alert List Details

Column Name/ Field Name/Icon	Description
Customer ID	Customer unique identifier.
Originator	The identifier of the originating party of the Transaction.
Originator Account	The IBAN of the originating party of the Transaction.
Beneficiary	The IBAN of the beneficiary party of the Transaction.
Location	The source country of the IP address.

5.5 Alert Information

Upon clicking an Alert in the Alert List section, additional details of that alert are displayed. These details provide further insight into an alert and can be used for further investigation.

Table 8 shows the alert details:

Table 8: Alert Details

Column Name	Description
Alert Summary	Provides key Alert details to help an Analyst make faster decisions. This includes Alert ID (in the header), Transaction ID, Created Date, Jurisdiction, Business Domain, Amount, Currency, Direction, Assignee, Decision, Comments, Attachments, Risk Score, Status and SLA.
Score card	Provides the Score and highlights for the Analyst to understand what triggered the Alert.
Transaction Details	Provides the transaction details to help an Analyst with faster decisions. This includes Date and Time, Direction, Amount, Currency, Channel, Status, Risk Score, Originator, Originator account, Beneficiary and Location.
Client Details	<p>The client details have three sections that provide the below details.</p> <p>Customer details - Provides customer details associated with an alert. This includes Name, Alternate Name, User name, Customer number, Date they became customer, Tax ID, ID number, ID jurisdiction, Country of citizenship, Date of birth, Job title, Employer name, Annual income, Credit score, Risk score, Address purpose, Address, Phone purpose, Phone, Phone extension, Most recent login, Most recent IP address, Most recent failed login, and Last password change.</p> <p>Account Details - Provides account details associated with an alert. This includes Account type, Opened, Last updated, Current status/since, Balance, Available, Credit limit/since, Delinquent, Linked payment account, and Added date.</p> <p>Card Details - Provides card details associated with an alert. This includes Card on account, Authorized users, Card number (related to the transaction), Name, Status, Role, Since, Issue date, PIN updated, and Last reject.</p>
Alert Decision	The Analyst provides the decision about an alert here to close the Alert analysis.
Decision Explanation	The Analyst can support the decision on an alert with comments and attachments. Attachment file types supported are image, audio, word, excel and video. The file size should be within 9 MB. Multiple attachments can be included.

OFSAA Support Contact Details

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

Send Us Your Comments

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

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

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

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

