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

User Guide

Release 8.0.8.0.0

E98368-01

November 2019

ORACLE®

User Guide, Release 8.0.8.0.0

E98368-01

Primary Author: Nethravathi G

Contributor: Anupama Srinivasa, Ruchi Tripathi, Swetha Yatham

Contents

Document Control

Version Number	Revision Date	Changes Done
8.0.8.0.0	Created: November 2019	Created first version of Fraud Enterprise Edition (Real Time Fraud Component) User Guide for 8.0.8.0.0 Release.

About this Guide

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

- Summary
- Audience
- Related Documents
- Conventions Used in this Guide
- Abbreviations Used in this Guide

Summary

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

Audience

This guide is intended for end users such as Fraud Analysts who are responsible for analyzing real-time transactions, identifying and investigating fraudulent transactions, and taking quick decisions to hold or release transactions.

Related Documents

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

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

Conventions Used in this Guide

The following table lists the conventions used in this guide and their associated meanings:

Table 0–1   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.
Italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Monospace type indicates the following: • Directories and subdirectories • File names and extensions • Process names • Code sample, that includes keywords, variables, and user-defined program elements within text
<variable>	Substitute input value

Abbreviations Used in this Guide

The following table lists the abbreviations used in this guide:

Table 0–2   Abbreviations and their meaning

Abbreviation	Meaning
OFS	Oracle Financial Services
BIC	Bank Identifier Code
IBAN	International Bank Account Number
IPE	Inline Processing Engine

1

About OFS Real Time Fraud

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 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 take quick decisions to hold or release transactions.

Real Time Fraud offers a single page real-time user interface that displays details of all the transactions that has been identified as suspicious transactions. It also provides the information required to investigate suspicious transactions. A transaction is identified as fraud based on certain rules configured in the IPE.

Figure 1–1   Real Time Fraud Process Flow

2
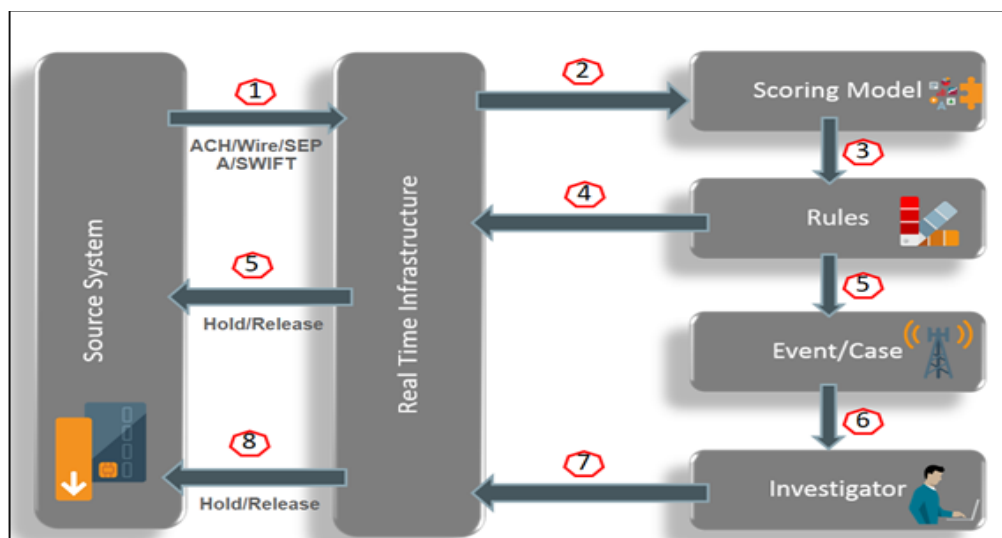
Getting Started

Getting Started introduces you to the OFS Real Time Fraud component and provides information that you need to know to use the application.
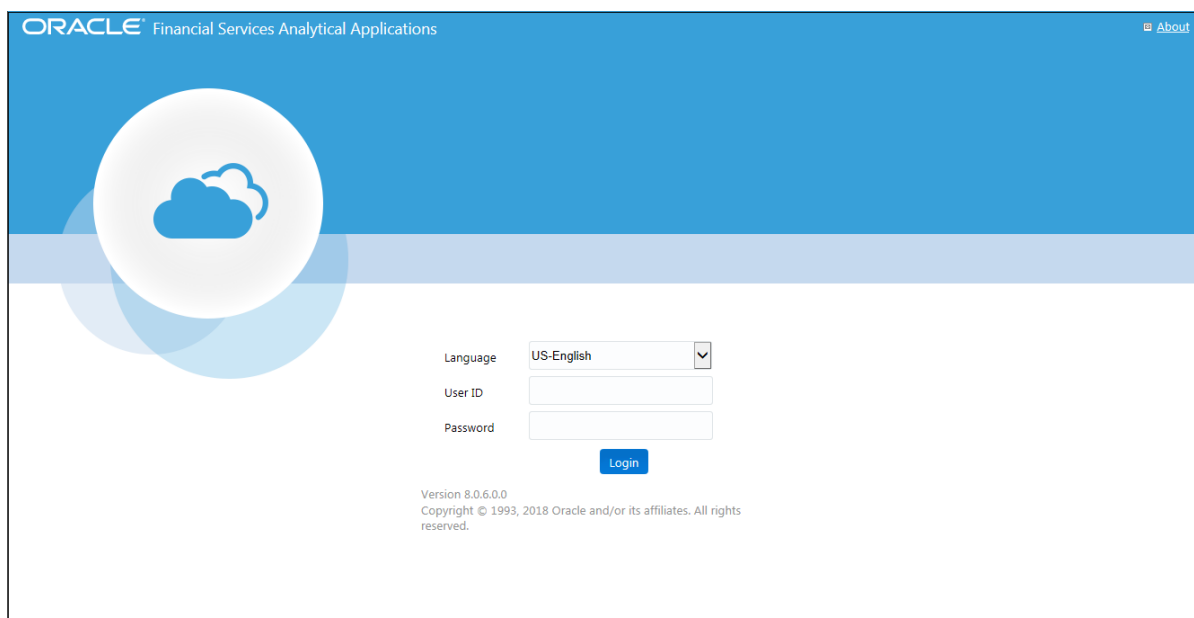
Access OFS Real Time Fraud

To access OFS Real Time Fraud:

1. Enter the OFSAA URL in your browser.

    The OFSAA Login page is displayed.

Figure 2–1   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**.

The **Applications** page is displayed.

Figure 2–2   Fraud Enterprise Edition Applications Page
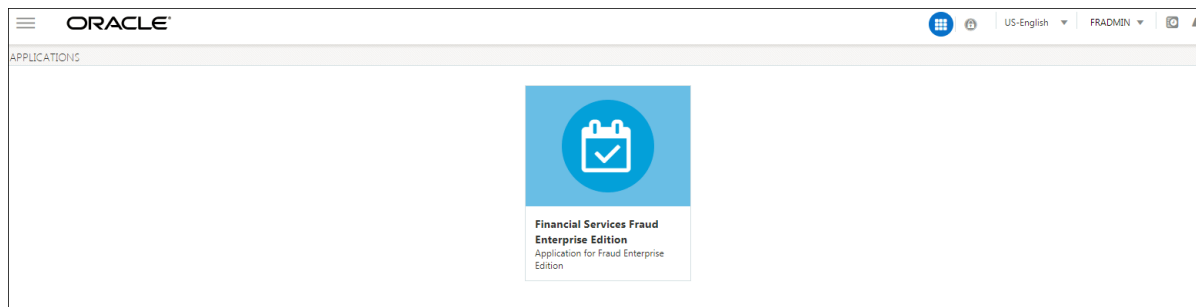
5. Click **Financial Services Fraud Enterprise Edition** from the Tiles menu.

The Financial Services Fraud Enterprise Edition Home page is displayed with the navigation list to the left.

Figure 2–3   Fraud Enterprise Edition Home Page
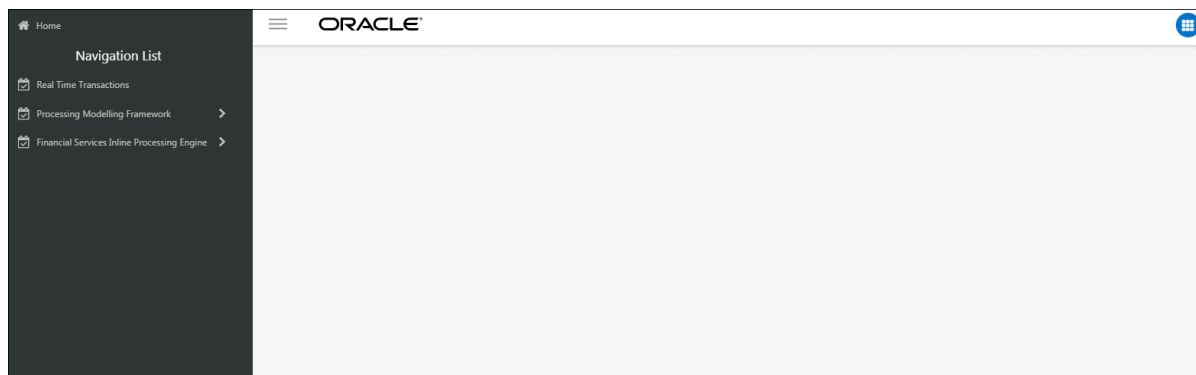
6. Click **Real time Transactions** in the Navigation List.

The **Oracle Financial Services Enterprise Fraud** page is displayed.

Managing OFS Enterprise Fraud

This chapter includes the following details:

Managing OFS Fraud Transactions

1. Navigate to the Oracle Financial Services Enterprise Fraud page.

Figure 3–1   Oracle Financial Services Enterprise Fraud Page

2. You can view the **Transaction Summary** section on the top-left corner which displays all the transactions posted through JSON input.

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. You can change the filter in View

drop-down field to view transactions in other status. For more information, see Transaction Summary Details.

3. Click on any transaction in Transaction Summary section to view more details in the following sections:

    •   Transaction Information on the top-right corner of the page. For more information, see Transaction Information.

    •   Recent History at the bottom of the page. For more information, see Recent History.

Transaction Summary Details

The Transaction Summary details include the following:

Table 3–1   Transaction Summary Details

Column Name/ Field Name/Icon	Description
Status	Indicates the status of a transaction that is identified as a fraudulent transaction. The various statuses include Held, Blocked, Assigned, Released, and Clean.
Originator	Indicates the name of the originator who initiated the transaction.
Originator Account	Indicates the account details of the originator.
Beneficiary	Indicates the name of the beneficiary in a transaction.
Risk Score	Indicates the risk percentage scored by a transaction.
Received Date	Indicates the date on which the transaction amount is received by the beneficiary.
Amount	Indicates the total amount involved in a transaction.
Currency	Indicates the currency in which a transaction is performed.
IP Address	Indicates the IP address from which a transaction is initiated.
Channel	Indicates the channel of transaction.
Location	Indicates the location of a transaction.
Assign	Indicates if a transaction has been assigned to a user for further investigation. Upon assigning a transaction: • The transaction is assigned to the configured user role to take further action. • The status of the transaction is changed from Held to Assigned. • The assignee is expected to take action within the configured time period.
Actions	Indicates the various actions that can be performed on a transaction that has been assigned for further investigation. The available actions are as follows: • Release • Block Whenever an action is taken on a transaction, the RTFraud service sends a response or feedback to the REST Service feedback URL configured for the client.

Table 3–1   Transaction Summary Details

Column Name/ Field Name/Icon	Description
SLA	SLA defines the cut-off time period from the moment when a tranaction is held by the Fraud application, within which the user is expected to take necessary action.
	If SLA breach occurs and no action is taken within the stipulated time period, then the system will automatically take certain actions on the transaction.
	Admin can configure the SLA in the Real Time Administration page. For more information, see *Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud) Administration and Configuration Guide.*
	Indicates the total number of newly identified fraud transactions that are in queue and ready to be displayed on the Enterprise Fraud page. Click to refresh the page and display the new transaction on the Enterprise Fraud page
View	Select the required status from the View drop-down list to view only those transactions.

Transaction Information

The transaction Information section is displayed on the top right corner of the Fraud page. Upon clicking a transaction in the Transaction Summary section, additional details of that transaction are displayed in the transaction information. Additional details provide further insight into a transaction which is useful for further investigation.

The transaction information details include:

Table 3–2   Transaction Information Details

Column Name	Description
Score Card	Indicates the score gained by a transaction against various IPE rules configured for Real Time Fraud.
	The pre-configured rules are run on all the transactions posted using JSON input. Every rule that satisfies the rule is displayed along with actual values and the corresponding score.
Message	Provides details of a transaction such as originator and beneficiary details, name, identifier, Bank Identifier Code, Date and time of transaction, amount, currency, source and destination country, address, and so on.
Account Details	Provides the account details of the transaction.
Audit	Provides details of the activities performed on the transaction.

Recent History

The Recent History section displays the details of all the transactions performed by the concerned originator and originator account to various beneficiaries in different formats.

The details are displayed in various formats that include tabular, graphical, relationship graphs, and remittance flow map. The pictorial representation of data provides a birds eye view of the transaction pattern, sophisticated behavior detection that drives targeted and effective fraud detection for current and future schemes.