Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud) Administration and Configuration Guide Release 8.1.2.2.0 September 2023 E98368-01



OFS Fraud Enterprise Edition (Real Time Fraud)

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

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

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

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

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

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

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

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

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

For information on third party licenses, click here.

Document Control

Version Number	Revision date	Change Log
8.1.2.2.0	Created: September 2020	Created first version of Fraud Enterprise Edition (Real Time Fraud Component) Administration and Configuration Guide for 8.1.2.2.0 Release.

Table 1: Document Control

Table of Contents

1 A	bout this Guide	6
1.1	Summary	6
1.2	Audience	6
1.3	Related Documents	6
1.4	Conventions Used in this Guide	6
1.5	Abbreviations Used in this Guide	7
2 In	stalling OFS Wire Fraud Enterprise Edition	
2.1	Prerequisites	8
2.2	Post-Installation Configuration	8
2.2	2.1 Configuring install.properties File	8
2.2	2.2 Configuring IPE for Real Time Wire Fraud	8
3 In	nstalling OFS Card Fraud Enterprise Edition	
3.1	Prerequisites	24
3.2	Post-Installation Configuration	
3.2	2.1 Configuring IPE for Real Time Card Fraud	
4 M	lanaging User Administration and Security Configuration	40
4.1	About User Administration	40
4.2	User Provisioning Process Flow	40
4.3	Managing User Administration	41
4.	3.1 Managing Identity and Authorization	
4.4	Adding Security Attributes	42
4.	4.1 About Security Attributes	
4.5	Business Domain and Jurisdiction Mapping	43
5 Co	onfiguring Real Time Wire Fraud Scoring	46
5.1	Operating Real Time Wire Fraud Service	
5.1	1.1 Real Time Wire Fraud Service Request	
5.1	1.2 Real Time Wire Fraud Service Response	
5.2	Managing Real Time Wire Fraud Scenarios/Rules	
5.2	2.1 Modify Fraud Rules	

6	Configuring Real Time Card Fraud Scoring 48				
e	5.1	Operating Real Time Card Fraud Service	48		
	6.1.1	Real Time Card Fraud Service Request	.48		
ć	5.2	Managing Real Time Card Fraud Scenarios/Rules	. 51		
	6.2.1	Modify Fraud Rules	51		
7	Mai	naging Real Time Wire Administration	52		
7	7.1	Accessing Real Time Wire Administration	. 52		
7	7.2	Configuring Real Time Wire Administration	. 53		
8	Mai	naging Real Time Card Administration	55		
8	3.1	Accessing Real Time Card Administration	55		
8	3.2	Configuring Real Time Card Administration	56		
9	Арр	pendix-A: Wire Fraud Sample JSON	58		
10	0 Appendix-B: Card Fraud Sample JSON 61				
11	1 Appendix-C: Real Time Wire Fraud Request Attributes				
12	2 Appendix-D: Real Time Card Fraud Request Attributes				
13	OFS	SAA Support Contact Details	82		
14	Send Us Your Comments				

1 About this Guide

This guide explains the concepts for the Real Time Fraud component in the Oracle Financial Services (OFS) Fraud Enterprise Edition application and provides comprehensive instructions for configuration and system administration.

Topics:

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

1.1 Summary

Before you begin the installation, ensure that you have access to the Oracle Support Portal with valid login credentials to notify us of any issues at any stage quickly. You can obtain the login credentials by contacting Oracle Support. You can find the latest copy of this document in the Oracle Help Center Documentation Library.

1.2 Audience

This guide is intended for System Administrators. Their roles and responsibilities, as they operate within OFS Real Time Fraud, include the following:

• **System Administrator**: Configures and maintains the system, user accounts and roles. Monitors data management, archives data, loads data feeds, and performs post-processing tasks. In addition, the System Administrator also reloads cache.

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) User Guide.

1.4 Conventions Used in this Guide

Table 2 lists the conventions used in this guide and their associated meanings.

Table 2: 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	ltalic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.

Table 2: Conventions Used in this Guide

Convention	Meaning	
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 the text. 	
<variable></variable>	Substitute input value	

1.5 Abbreviations Used in this Guide

Table 3 lists the abbreviations used in this guide.

Table 3: Abbreviations and their meaning

Abbreviation	Meaning
AAI	Analytical Applications Infrastructure
BD	Behavior Detection
BIC	Bank Identifier Code
IBAN	International Bank Account Number
IPE	Inline Processing Engine
OFS	Oracle Financial Services

2 Installing OFS Wire Fraud Enterprise Edition

This chapter details on installing the Oracle Financial Services (OFS) Wire Fraud Enterprise Edition.

Topics:

- Prerequisites
- Post-Installation Configuration

2.1 **Prerequisites**

The prerequisites you must have before installing Oracle Financial Services (OFS) Wire Fraud Enterprise Edition are:

 OFS Behavior Detection (BD) Application Pack should be installed. For information on BD application pack installation, see Financial Services Behavior Detection (OFS BD) Application Pack Installation Guides.

2.2 Post-Installation Configuration

On successful installation of the OFS BD Application Pack, you must perform the following configurations for OFS Wire Fraud Enterprise Edition application.

- Configuring install.properties File
- Configuring IPE for Real Time Wire Fraud

2.2.1 Configuring install.properties File

You must configure the install.properties file to configure the Real Time Wire Fraud Component.

- Navigate to <FIC_HOME>/realtime_processing/WebContent/conf/ install.properties file.
- 2. Update the install.properties file as follows:

sql.config.datasource.jndi.name=jdbc/FICMASTER

sql.atomic.datasource.jndi.name=jdbc/<INFODOM NAME>

sql.metadom.datasource.jndi.name=jdbc/<INFODOM NAME>CNF

system.infodom=<INFODOM_NAME>

```
system.domain=PFR
```

system.appid=OFS_FRAUD_EE

ipe.produce.hglights.results=true

2.2.2 Configuring IPE for Real Time Wire Fraud

You must install the RTFRAUD service to configure Inline Processing Engine (IPE) for Real Time Fraud. To install the RTFRAUD service, follow these steps.

- 1. Creating RTFRAUD.ear or RTFRAUD.war
- 2. Deploying RTFRAUD.ear

2.2.2.1 Creating RTFRAUD.ear or RTFRAUD.war

It is mandatory to have the RTFRAUD.ear in the same profile or domain where the <contextname>.ear file of the OFS BD Application is deployed. To create RTFRAUD.ear or RTFRAUD.war, follow these steps:

- 1. Navigate to <FIC_HOME>/RealTimeFraudIPEProcessing.
- 2. Execute the below command to import IPE config

Path: <FIC HOME>/ficapp/common/FICServer/bin/

```
Command:./RTIImport.sh $FIC_HOME/RealTimeFraudIPEProcessing/
IPEAssessmentImport/OFS_RTFRD_RTIExport_Fraud.xml <INFODOM> OFS_FRAUD_EE
true
```

3. Execute the following command:

./ant.sh.

NOTE Execute the following command, if the server is Tomcat: ./ant.sh. Tomcat

Figure 1: Creating RTFRAUD.ear/ RTFRAUD.war



4. On successful execution, the RTFRAUD.ear and RTFRAUD.war files are generated under the <<FIC_HOME>/RealTimeFraudIPEProcessing/ folder.

2.2.2.2 Deploying RTFRAUD.ear

- Installing RTFRAUD.ear in WebLogic using WebLogic Administrator Console
- Deploying RTFRAUD.ear in WebSphere
- Deploying RTFRAUD.war in Tomcat

2.2.2.1 Deploying RTFRAUD.ear in WebLogic

This section defines how to deploy RTFRAUD.ear in WebLogic.

NOTE It is mandatory to have RTFRAUD.ear in the same domain where <contextname>.ear of the OFS BD Application is deployed.

To deploy RTFRAUD.ear in WebLogic, follow these steps:

- 1. Start the WebLogic server.
- 2. Create an RTFRAUD.ear folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/ <DOMAIN NAME>/applications.
- 4. Explode the RTFRAUD.ear file by executing the command:

jar -xvf RTFRAUD.ear

- 5. Delete the RTFRAUD.ear and RTFRAUD.war files.
- 6. Create an RTFRAUD.war folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/ <DOMAIN NAME>/applications/RTFRAUD.ear.
- 8. Explode the RTFRAUD. war file by executing the command:

jar -xvf RTFRAUD.war

9. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>config path, update config.xml with the below entry under <security-configuration>:

<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-authcredentials>.

2.2.2.2.2 Installing RTFRAUD.ear in WebLogic using WebLogic Administrator Console

This section defines how to deploy RTFRAUD.ear in WebLogic using WebLogic administrator console.

To deploy RTFRAUD.ear in WebLogic, follow these steps:

- Navigate to the path <WebLogic Installation directory>/user_projects/domains/ <domain name>/bin in the machine in which WebLogic is installed.
- 2. Start WebLogic by executing the following command:

./startWebLogic.sh -d64 file

3. Open the following URL in the browser window:

http://<ipaddress>:<admin server port>/console (use https protocol if SSL is enabled). The Sign-in window of the WebLogic Server Administration Console is displayed.

4. Login with the Administrator **Username** and **Password**. The Summary of Deployment page is displayed.

Figure 2: Summary of Deployment

Home Log Out Preferences Record Help Action > Summary of Deployments Messages Al changes have been activated. No restarts are necessary. Selected Deployments Control Monitoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Logated Teacter Teacter	Welcome, weblogic Connected to: AAA18050
Hone >Summary of Deployments Hessages All changes have been activated. No restarts are necessary. Selected Deployments Control Monitoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Listent Control Portion Control Control	
All changes have been activated. No restants are necessary. Selected Deployments Control Hontoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Linearing Treasment Treasment	
Selected Deployments were deleted. Summary of Deployments Control Montoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Listent Deployments Listent Deployment	
Summary of Deployments Control Monitoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments	
Control Monitoring This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. © Customize this table Deployments	
This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, application name and using the controls on this page. To install a new application or module for deployment to targets in this domain, click the Install button. Customize this table Deployments Uncerted Uncerted Uncerted Uncerted Uncerted Uncerted	
Deployments	
Televen Televen Foreine Foreine Televen	Showing 1 to 1 of 1 Previous Next
Name 🔅 State Health Type	Targets Deployment Order
C B Costando Active & OK Enterprise	and the second sec
anstall Updale Delete Start+) Stop+	lication AdminServer 100

5. Click Install. The Install Application Assistance page is displayed.

Figure 3: Install Application Assistance Window

ORACLE WebLogic Server Admi	inistration Console 12c				Q
Change Center	🏠 Home Log Out Preferences 🛃 Rec	ord Help	Q		Welcome, weblogic Connected to: BD806
View changes and restarts	Home >Summary of Deployments				
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Install Application Assistant Back Next Finish Cancel				
Domain Structure	Locate deployment to install and pr	epare for deployment			
BD806 Domain Partitions Environment Deployments	Select the file path that represents the a the Path field. Note: Only valid file paths are displayed	pplication root directory, arch d below. If you cannot find yo	hive file, exploded archive directory, or appli our deployment files, Upload your file(s) and	cation module descriptor that you want to inst /or confirm that your application contains the r	all. You can also enter the path of the application directory or file in required deployment descriptors.
Security Realms	Path:	/scratch/ofsaebas/Orac	cle/Middleware/Oracle Home/user p	roiects/domains/BD806/applications/R	TFRAUD ear
Interoperability	Recently Used Paths:	/scratch/ofsaebas/Oracle/M	iddleware/Oracle_Home/user_projects/doma	ains/BD806/applications	
the Diagnostics	Current Location:	whf00ark.in.oracle.com / sc	cratch / ofsaebas / Oracle / Middleware / Ora	cle_Home / user_projects / domains / BD806	/ applications
	BD806.ear (open directory) B RTFRAUD.ear (open directory)	r)			
How do I	Dack Next Fillish Calcel				
 Start and stop a deployed enterprise application 					
Configure an enterprise application					
Create a deployment plan					
Instance					
Test the modules in an enterprise application					
System Status					
Health of Running Servers					
Failed (0) Critical (0) Overloaded (0) Warning (0) OK (1)					

6. Select RTFRAUD.ear and click **Next**. This action displays the Install Application Assistance page with the Choose targeting style section.

ORACLE WebLogic Server Ad	ministration Console 12c	2
Change Center	🟦 Home Log Out Preferences 📨 Record Help	Welcome, weblogic Connected to: AAAI80501
View changes and restarts	Home >Summary of Deployments	,
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Install Application Assistant Back Next French Cancet	
Domain Structure	Choose targeting style	
AAA180SOL (D) Environment Deployments (D) Services Security Realms (D) Interoperability (D) Diagnostics	Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application. The application and its components will be targeted to the same locations. This is the most common usage. To target the foremarks a virtual hosts.	
	Instant time deployment as a unrary Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications. Back Next Printip Cancel	
How do I 🖂		
 Start and stop a deployed enterprise application 		
Configure an enterprise application		
Create a deployment plan		
Target an enterprise application to a server		
Test the modules in an enterprise application		
System Status		
Health of Running Servers		
Failed (0) Critical (0) Overloaded (0) Warning (0) OK (1)		
WebLogic Server Version: 12.1.2.0.0 Copyright © 1996,2013, Oracle and/or its affiliates. All	rights nearwed.	

Figure 4: Install Application Assistance with choose Target Style

7. By default, the **Install this deployment as an application** option in the Choose targeting style section is selected. Click **Next**. This action displays the Install Application Assistance page in the Optional Settings section.

Figure 5: Install the Application Assistance page with Optional Settings

ORACLE WebLogic Server Ad	tministration Console 12c	<u>S</u>					
Change Center	🔒 Home Log Out Preferences 🔤 Record Help	Welcome, weblogic Connected to: AAAI805OL					
View changes and restarts	Home >Summary of Deployments						
Configuration editing is enabled. Future	Install Application Assistant	Install Application Assistant					
modify, add or delete items in this domain.	Back Next Finish Cancel						
Domain Structure	Optional Settings						
AAAI80SOL	You can modify these settings or accept the defaults						
Deployments	* Indicates required fields						
B - Services							
Security Realms Triteroperability	- General -						
Diagnostics	What do you want to name this deployment?						
	*Name: ILP						
	- Security						
	What security model do you want to use with this application?						
	DD Only: Use only roles and policies that are defined in the deployment descriptors.						
How do I 🖻	Custom Roles: Use roles that are defined in the Administration Console: use policies that are defined in the deployment descriptor.						
Start and stop a deployed enterprise	2						
application	○ Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.						
Configure an enterprise application	○ Advanced: Use a custom model that you have configured on the realm's configuration page.						
Target an enterprise application to a server	- Source Arrestibility						
Test the modules in an enterprise application	Available to the second s						
System Status	Use the defaults defined by the deployment's targets						
Health of Running Servers	Recommended selection.						
Failed (0)	○ Convithis application onto every target for me						
Critical (0) Overloaded (0)							
Warning (0)	During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.						
OK (1)	\bigcirc I will make the deployment accessible from the following location						
	Location: //scratch/oracle/Oracle/Middleware/Oracle_Home/user_						
	Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each	arget can reach the location.					

8. Retain the default selections and click **Next**. The Install Application Assistance page is displayed with the Review your choices and click Finish section.

ORACLE WebLogic Server Administration Console 12c							
Change Center	Home Log Out Preference	es 🏊 Record Help	Welcome, weblogic Connected to: BD806				
View changes and restarts	Home >Summary of Deploym	Home >Summary of Deployments					
Configuration editing is enabled. Future	Install Application Assistant						
modify, add or delete items in this domain.	Back Next Finish	Cancel					
Domain Structure	Review your choices and click Finish						
80866 Girchaman Barthlone Click Finish to complete the deployment. This may take a few moments to complete.							
P-Environment	- Additional Configuration						
Deployments Services	In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?						
Security Realms	Yes, take me to the deployment's configuration screen.						
■ Diagnostics	No, I will review the configuration later.						
	- Summary						
	Deployment:	/scratch/ofsaebas/Oracle/Middleware/Oracle_Home/user_projects/domains/BD806/applications/RTI	RAUD.ear				
	Name:	RTFRAUD-1					
How do I	Staging Mode: Use the defaults defined by the chosen targets						
 Start and stop a deployed enterprise application 	Plan Staging Mode:	Use the same accessibility as the application					
 Configure an enterprise application 	Security Model: DDOnly: Use only roles and policies that are defined in the deployment descriptors.						
Create a deployment plan	Accenty more a log only one and ponces and are defined in the appropriate accentions.						
 Target an enterprise application to a server instance 	Scope: Global						
Test the modules in an enterprise application	Target Summary						
	Components 🐟		Targets				
System Status	a RTFRAUD.ear AdminServer						
Health of Running Servers							
Failed (0)	Back Nett Finsh Cancel						
Overloaded (0)							
Warning (0)							
OK (1)							

9. Select **No, I will review the configuration later** in the Additional Configuration section and click **Finish**. RTFRAUD is added in the Name section of the Summary of Deployment page with the following message: *The deployment has been successfully installed.*



ORACLE WebLogic Server Ad	inistration Console 12c							Q
Change Center	🔒 Home Log Out Preferences 🔤 Record H						Welcome, weble	ogic Connected to: BD806
View changes and restarts	Home >Summary of Deployments >RTFFAUD-1 >Summary of Deployments							
Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.	d Summary of Deployments d Configuration Control Monitoring							
Activate Changes	This page displays the list of Java EE applications and standalone application modules installed to this domain.							
Undo All Changes	You can usdate (redeolov) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this pape.							
Domain Structure	To install a new application or module for deployment to targets in this domain, click Install.							
BD806 ⊕- Domain Partitions ⊕- Environment Deployments	806 "Domain Partitions Customize this table "Environment Devolvement							
	Install Update Delete						Showing 1 to 2	2 of 2 Previous Next
P-Security Realms ⊡-Interoperability ⊡-Diagnostics	🔲 Name 🗞		State Hea	lth Type	Targets	Scope	Domain Partitions	Deployment Order
-	□ E BD806		Active 🖋 (K Enterprise Application	AdminServer	Global		100
			Active 🖋 (K Application	AdminServer	Global		100
	Install Update Delete						Showing 1 to 2	2 of 2 Previous Next
How do I 🖂								
Install an enterprise application								
Configure an enterprise application								
 Update (redeploy) an enterprise application 								
 Monitor the modules of an enterprise application 								
Deploy EJB modules								
 Install a Web application 								
System Status 🖂								
Health of Running Servers								
Failed (0)								
Critical (0)								

10. Restart all OFS Analytical Applications Infrastructure (AAI) servers.

2.2.2.3 Deploying RTFRAUD.ear in WebSphere

This section defines how to deploy RTFRAUD.ear in WebSphere.

NOTE It is mandatory to have RTFRAUD.ear in the same domain where <contextname>.ear of the OFS BD Application is deployed.

To deploy RTFRAUD.ear in WebSphere, follow these steps:

```
./startServer.sh server1
```

- 2. Create an RTFRAUD.ear folder in <WEBSPHERE_INSTALL_DIR>/RTFRAUD.ear.
- 3. Copy <FIC_HOME>/RealTimeFraudIPEProcessing/RTFRAUD.ear to <WEBSPHERE_INSTALL_DIR>/RTFRAUD.ear.
- 4. Open the following URL in the browser: http://<ipaddress>:<Administrative Console Port>/ibm/console. (use https protocol if SSL is enabled). The login screen is displayed.

Figure 8: WebSphere Login Window

WebSphere. softwa	ILE
	WebSphere Integrated Solutions Console User ID: admin Password: Log in
IBM.	Licensed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved. IBM, the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at <u>Copyright and trademark information</u> .

- 5. Enter the user credentials that have administrator rights and click **Log In**.
- 6. From the LHS menu, select **Applications** and click **New Application**. The New Application window is displayed.

Figure 9: New Application

lew Application						
New Application						
This page provides links to create new applications of different types.						
Install a New Application						
New Enterprise Application						
New Business Level Application						
New Asset						

7. Click **New Enterprise Application**. The **Preparing for the application installation** window is displayed.

Figure 10: Preparing for the Application Installation Window

rprise Applications	
paring for the application installation	2 -
Specify the EAR, WAR, JAR, or SAR module to upload and install.	
Path to the new application	
C Local file system Full path Choose File No file chosen	
Remote file system	
Full path Browse	
Next Cancel	

8. Select **Remote File System** and click **Browse**.

Figure 11: Browse Remote Filesystems Window

Enterprise Applications	Close page
Browse Remote Filesystems	E
Select the radio button next to the archive that you wish to install, or click on a directory name to view its contents.	
Contents of /scratch/IBM/WebSphere/AppServer/profiles/BD8123/installedApps/ofss-mum-889-Node3-Cell03/RTFRAUD.ear	
E parentDir	
RTFRAUD.ear	
OK Cancel	

9. Navigate through folders and select the EAR file generated for RTFRAUD to upload and install. Click **OK**.

Figure 12: Preparing for the application installation

Specify the EAR, WAR, JAR, or SAR module to upload and install.	
Path to the new application	
Choose File No file chosen	
Remote file system Full path /scratch/IBM/WebSphere/profiles/BD812/RTFRAUD.ear Browse	

10. Click Next.

Figure 13: Installation Options

Preparing for the application installation				
How do you want to install the application? Stat Path - Prompt only when additional information is required. Detailed - Show all installation options and parameters.				
Choose to generate default bindings and mappings Previous Next Cancel				

11. Select the Fast Path option and click Next. The Install New Application window is displayed.

Figure 14: Install New Application

nstall	stall New Application						
-							
Spe	city options for installing enterprise applications and modules.	Colort Installation ontions					
installation options		Sector instantiation options					
	Step 2 Map modules	speury the various options that are available for your application.					
*	Step 3 Map virtual	Precompile JavaServer Pages files					
	hosts for Web modules	Directory to install application					
	<u>Step 4</u> Summary	Distribute application					
		Use Binary Configuration					
		Deploy enterprise beans Application name					
		RTFRAUD					
		Create MBeans for resources					
		Override class reloading settings for Web and EJB modules					
		Reloau Interval In Seconds					
		Deploy Web services					
		Validate Input off/warn/fail warn					
		Process embedded configuration					
		File Permission					
		Allow all files to be read but not written to Allow executables to execute					
		Allow HTML and image files to be read by everyone					
		.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755					
		Application Build ID					
		Allow dispatching includes to remote resources					
		Allow servicing includes from remote resources					
		Business level application name					
		Asynchronous Request Dispatch Type					
		Disabled V					
		Allow EJB reference targets to resolve automatically					
		Deploy client modules Client deployment mode					
		Isolated					
		U Validate schema					
	lext Cancel						

12. Enter the required information and click **Next**. The Map Modules to Servers window is displayed.

Figure 15: Map Modules to Servers

Step 1 Select	Map modu	Map modules to servers					
→ Step 2: Map modules to servers ★ Step 2: Map modules to servers ★ Step 3: Map virtual hosts for Web modules Step 4: Summary Specify targets such as application servers or clusters of application servers where you want to instal the modules that are contained in your application. Modules can be installed on the same application server or dispersed among several application. Modules can be installed on the same application server or dispersed among several application. Modules can be installed on the same application server or dispersed among several application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based on the applications that are routed through. Clusters and servers: WebSphere:cell=ofss-mum-889-Node3-Cell03,node=ofss-mum-889-Node3,server=server1 Apply							
	Select	Module	URI	Server			
		Inline Processing RTFRAUD.war,WEB- INF/web.xml WebSphere:cell=ofss-mum-889-Node3- Cell03,node=ofss-mum-889- Node3,server=server1					

13. Select the **Inline Processing** check box and click Next. The Map Virtual hosts for the Web modules page are displayed.

nstall New Application							
Sp	ecify options for installing ente	rprise applications and modules.					
	<u>Step 1</u> Select	Map virtual hosts for Web modules					
	<u>Step 2</u> Map modules to servers	Specify the virtual host for the Web modules that are contained in your application. You can install Web modules on the same virtual host or disperse them among several hosts.					
→	Step 3: Map virtual hosts for Web modules	Apply Multiple Mappings					
	<u>Step 4</u> Summary	Select Web module Virtual host					
		✓ Inline Processing default_host ▼					
ļ	Previous Next Cancel						

Figure 16: Map Virtual hosts for Web modules page

- 14. Select the **Inline Processing** check box and click **Next**. The Metadata for the modules page is displayed.
- 15. Select the **Metadata-complete** attribute check box and click **Next**. The Summary page is displayed.

Figure 17: Summary page

Install New App

Step 1 Select	Summary				
	Summary of installation options				
<u>Step 2</u> Map modules to servers	Options	Values			
Step 3 Map virtual	Precompile JavaServer Pages files	No			
hosts for Web modules	Directory to install application				
Step 4: Summary	Distribute application	Yes			
	Use Binary Configuration	No			
	Application name	RTFRAUD			
	Create MBeans for resources	Yes			
	Override class reloading settings for Web and EJB modules	No			
	Reload interval in seconds				
	Deploy Web services	No			
	Validate Input off/warn/fail	warn			
	Process embedded configuration	No			
	File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755			
	Application Build ID	Unknown			
	Allow dispatching includes to remote resources	No			
	Allow servicing includes from remote resources	No			
	Business level application name				
	Asynchronous Request Dispatch Type	Disabled			
	Allow EJB reference targets to resolve automatically	No			
	Deploy client modules	No			
	Client deployment mode	Isolated			
	Validate schema	No			
	Cell/Node/Server	Click here			

16. Click **Finish**. On successful installation, the system displays a success message.

Figure 18: Installation Success

_			
Ins	tal	llin	g

there are enterprise beans in the application, the EJB deployment process can take several minutes. Do not save the configuration until the process completes.
check the SystemOut.log on the deployment manager or server where the application is deployed for specific information about the EJB deployment process as it occurs.
DMA5016I: Installation of RTFRAUD started.
DMA50671: Resource validation for application RTFRAUD completed successfully.
DMA5058I: Application and module versions are validated with versions of deployment targets.
DMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
DMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
DMA50811: The bootstrap address for client module is configured in the WebSphere Application Server repository.
DMA50531: The library references for the installed optional package are created.
DMA50051: The application RTFRAUD is configured in the WebSphere Application Server repository.
DMA50011: The application binaries are saved in /scratch/IBM8.5.5.9/WebSphere/AppServer/profiles/AppSrv03/wstemp/0/workspace/cells/whf00avgNode07Cell/applications/RTFRAUD.ear/RTFRAUD.ear
DMA50051: The application RTFRAUD is configured in the WebSphere Application Server repository.
ECJ0400I: Successfully updated the application RTFRAUD with the appContextIDForSecurity information.
DMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
DMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
DMA5113I: Activation plan created successfully.
DMA50111: The cleanup of the temp directory for application RTFRAUD is complete.
DMA5013I: Application RTFRAUD installed successfully.
Application RTFRAUD installed successfully.
o start the application, first save changes to the master configuration.
Changes have been made to your local configuration. You can:
<u>Save</u> directly to the master configuration.
 <u>Review</u> changes before saving or discarding.
o work with installed applications, click the "Manage Applications" link.
fanage Applications

17. Click **Save** and save the master file configuration. This action displays the details in the *Master File Configuration* page.

Figure 19: Master File Configuration page

Ente	terprise Applications										
E U G	Enterprise Applications Use this page to manage installed applications. A single application can be deployed onto multiple servers. Preferences										
Start Stop Install Uninstall Update Rollout Update Remove File Export DDL Export File Liberty Advisor •]						
	C (1 # \$									
s	elect	Name 🗘				Application Status	<u>.</u>			Liberty Advisor Sun	nmary ሷ
	You ca	n administer the fol	lowing resou	rces:							
ſ		BD812UP3WS				4				\oslash	
۱		DefaultApplication				÷				0	
ſ		RTFCARD				÷				0	
1	RTFRAUD			*		0					
۱				•				0			
ſ	guery			•				0			
	Total 6	,									

NOTE Make sure you take a backup of the Jersey Jar file to any folder and remove it by running the following command in the mentioned path.					
	Path: <deployed area="">/<rtfwire.ear>/ <rtfwire.war>/WEB-INF/LIB</rtfwire.war></rtfwire.ear></deployed>				
	Command: Delete jersey-bundler(jersey- bundle-1.6.jar) jar				

18. Select RTFRAUD and click **Start**. This action displays the Enterprise Application page with a confirmation message.

Enterprise	Applications		2 =			
 Messages Application RTFRAUD on server server1 and node ofss-mum-889-Node3 started successfully. The collection may need to be refreshed to show the current status. 						
Enterp	prise Applications					
Use thi	is page to manage installed applications. A sir	gle application can be deployed onto multiple	e servers.			
🛨 Pref	ferences					
Star	t Stop Install Uninstall Update	Rollout Update Remove File Export E	xport DDL Export File Liberty Advisor			
D	6 # 9					
Select	Name 🗢	Application Status 🕸	Liberty Advisor Summary 🙅			
You ca	an administer the following resources:					
	BD812UP3WS	⇒	\oslash			
	DefaultApplication	\$	0			
□ RTFCARD ↔			0			
□ RTFRAUD �			0			
	□ ivtApp ◆					
	□ query � O					
Total	Total 6					

19. Restart all OFS AAAI servers.

2.2.2.4 Deploying RTFRAUD.war in Tomcat

To deploy RTFRAUD.war in Tomcat, follow these steps:

- 1. Create a data source for RTFRAUD context in Tomcat by editing server.xml in <TOMCAT HOME DIR>/conf directory.
- 2. Update database details as shown in the following sample:

```
maxTotal="100"
                  maxIdle="30"
                  maxWaitMillis="10000" removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"/>
      <Resource auth="Container"
                  name="jdbc/<infodom name>". For example, OFSAAAIINFO
                  type="javax.sql.DataSource"
        driverClassName="oracle.jdbc.driver.OracleDriver"
                  username="act obiatm"
                  password="password"
        url="jdbc:oracle:thin:@whf00aqr:1521/DEVUT08SPRINT"
                  maxTotal="100"
                  maxIdle="30"
                  maxWaitMillis="10000" removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"/>
 <Resource auth="Container"
                  name="jdbc/<infodom name>CNF". For example,
OFSAAAIINFOCNF
                  type="javax.sql.DataSource"
          driverClassName="oracle.jdbc.driver.OracleDriver"
                  username="act obiatm"
                  password="password"
          url="jdbc:oracle:thin:@whf00aqr:1521/DEVUT08SPRINT"
                  maxTotal="100"
                  maxIdle="30"
                  maxWaitMillis="10000" removeAbandoned="true"
removeAbandonedTimeout="60" logAbandoned="true"/>
      </Context>
```

- 3. Copy the RTFRAUD.war file to the <code>\$TOMCAT_HOME/webapps</code> directory.
- 4. Grant 755 (rwxr-xr-x) permissions to the RTFRAUD.war file
- 5. Start the Tomcat server.

3 Installing OFS Card Fraud Enterprise Edition

This chapter details on installing the Oracle Financial Services (OFS) Card Fraud Enterprise Edition.

Topics:

- Prerequisites
- Post-Installation Configuration

3.1 **Prerequisites**

The prerequisites you must have before installing OFS Card Fraud Enterprise Edition are:

• OFS Behavior Detection (BD) Application Pack should be installed. For information on BD application pack installation, see Financial Services Behavior Detection (OFS BD) Application Pack Installation Guides.

3.2 Post-Installation Configuration

On successful installation of the Oracle Financial Services BD Application Pack, you must perform the following configuration for OFS Card Fraud Enterprise Edition application.

Configuring IPE for Real Time Card Fraud

3.2.1 Configuring IPE for Real Time Card Fraud

You must install the RTFCARD service to configure IPE for Real Time Fraud.

The following sections show how to install the RTFCARD service.

- Create the Source Entity Queue for RTF Card
- Creating RTFCARD.ear or RTFCARD.war
- Configuring the JMS properties
- Deploying RTFCARD.ear
- Commands to Execute to Import IPE Configs

3.2.1.1 Create the Source Entity Queue for RTF Card

Create the source entity queue for RTF Card considering the following sample.

- Queue Name: RTI Source Entity Queue
- JNDI Name: jms/sourceEntityCardQueue
- Sub deployment: Select the Sub deployment as RTISubDeploy.

Table 4 shows a sample of JMS Queue configuration.

Table 4: Sample JMS Queue configuration

Name	Туре	JNDI Name	Sub Deployment	Targets
Cache Operation Message Destination Topic	Торіс	jms/ cacheOperationMessageDestinati on	RTISubdeploy	RTIServer

Name	Туре	JNDI Name	Sub Deployment	Targets
JMS Connection Factory	Connection Factory	jms/connectionFactory	Default Targeting	AdminServer
RTI Assessment Topic Response Destination Topic		jms/ assessmentResponseDestination	RTISubdeploy	RTIServer
RTI Feedback Queue	Queue	jms/feedbackQueue	RTISubdeploy	RTIServer
RTI Hold JMS Queue	Queue	jms/TransactionActionQueue	RTISubdeploy	RTIServer
RTI Source Entity Queue	Queue	jms/sourceEntityCardQueue	RTISubdeploy	RTIServer
sourceEntityQueue	Queue	jms/sourceEntityQueue	RTISubdeploy	RTIServer
Wire Transaction Source Entity Queue	Queue	jms/wireTrxnQueue	RTISubDeploy	RTIServer

Table 4: Sample JMS Queue configuration

3.2.1.2 Creating RTFCARD.ear or RTFCARD.war

It is mandatory to have the RTFCARD.ear in the same profile or domain where the <contextname>.ear file of the OFS BD Application is deployed. To create **RTFCARD.ear** or **RTFCARD.war**, follow these steps:

- 1. Navigate to <FIC_HOME>/RTFCardFraudIPEProcessing
- 2. Execute the following command:

./ant.sh.

3. On successful execution, the RTFCARD.ear and RTFCARD.war files are generated under the <<FIC_HOME>/RTFCardFraudIPEProcessing/ folder.

3.2.1.3 Configuring the JMS properties

Before deploying the RTFCARD.ear or RTFCARD.war file, perform the following steps.

1. Update RESTAPIConf.properties for card in the following path.

Path: \$FIC HOME/fiweb/webroot/conf

2. Replace the place holder ##WEB_IP## and ##WEB_PORT##.

For Webshpere:

- a. The ##WEB IP## and ##WEB PORT## values will be bootstrap IP address and port.
- b. Replace the ##JMS_PORT## with bootstrap port in CardTransactionsPost.jsp in the below path.

Path: \$FIC_HOME/RTFCardFraudIPEProcessing/WebContent

3. Recreate and deploy the BD war.

3.2.1.4 Deploying RTFCARD.ear

NOTE	For information on IPE configurations, such as JMS connection
	factory and JMS queue, see OFS inline Processing Engine
	Configuration Guide

The following sections detail the deployment of RTFCARD.ear.

- Deploying RTFCARD.ear in WebLogic
- Installing RTFCARD.ear in WebLogic using WebLogic Administrator Console
- Deploying RTFCARD.ear in WebSphere

NOTE	RTFCARD.ear deployment on Tomcat is not supported.
NOTE	Make sure that ipe.produce.hglights.results is false in the <deployed area="">/RTFCARD.ear/RTFCARD.war/conf/ install.properties path. You must update it to false if it is shown as true.</deployed>

3.2.1.4.1 Deploying RTFCARD.ear in WebLogic

This section defines how to deploy RTFCARD.ear in WebLogic.



It is mandatory to have RTFCARD.ear in the same domain where <contextname>.ear of the OFS BD Application is deployed.

To deploy RFTCARD.ear in WebLogic, follow these steps:

- 1. Start the WebLogic server.
- 2. Create an RTFCARD.ear folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/ <DOMAIN_NAME>/applications.
- 3. Copy <FIC_HOME>/RealTimeFraudIPEProcessing/RTFRAUD.ear to <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/ RTFRAUD.ear/.
- 4. Explode the RTFCARD.ear file by executing the command:

jar -xvf RTFCARD.ear

- 5. Delete the RTFCARD.ear and RTFCARD.war files.
- 6. Create an RTFCARD.war folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/ <DOMAIN NAME>/applications/RTFCARD.ear.
- 8. Explode the RTFCARD.war file by executing the command:

jar -xvf RTFCARD.war

9. In the <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<Domain Name>config
 path, update config.xml with the below entry under <security-configuration>:

```
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-
credentials>.
```

3.2.1.4.2 Installing RTFCARD.ear in WebLogic using WebLogic Administrator Console

This section defines how to deploy RTFCARD.ear in WebLogic using Weblogic administrator console.

To deploy RFTCARD.ear in WebLogic, follow these steps:

- Navigate to the path <WebLogic Installation directory>/user_projects/domains/ <domain name>/bin in the machine in which WebLogic is installed.
- 2. Start WebLogic by executing the following command:

./startWebLogic.sh -d64 file

3. Open the following URL in the browser window:

http://<ipaddress>:<admin server port>/console (use https protocol if SSL is enabled). The Sign in window of the WebLogic Server Administration Console is displayed.

4. Login with the Administrator **Username** and **Password**. The Summary of Deployment page is displayed.

Figure 21: Summary of Deployment

ORACLE WebLogic Server Ad	ministration Console 14.1.1					Ŏ
Change Center	A Home Log Out Preferences	s 🔤 Record Help	Q			Welcome, weblogic Connected to: BD812UT
View changes and restarts Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain. Domain Structure	Home >Summary of Deployment Messages Install operation cancelled Summary of Deployments	nts - no deployments installe	d.			
BOBI2UT ⊕ Environment ├─ Deployments ⊕ Security Realms ⊕ Interoperability ⊕ Diagnostics	This page displays the list of J You can update (redeploy) or To install a new application or Customize this table Deployments	ava EE applications and st delete installed application module for deployment to	tandalone application modu ns and modules from the d o targets in this domain, cli	les installed to this d omain by selecting th ck Install .	omain. e checkbox next to the applic	ation name and then using the controls on this page.
	Install Update Delete					Showing 0 to 0 of 0 Previous Next
How do I 🗉	🗆 Name 🗞	State	Health	Туре	Targets	Deployment Order
Install an enterprise application There are no items to display						
Configure an enterprise application	Install Update Delete Showing 0 to 0 of 0 Previous Next					
Update (redeploy) an enterprise application						
 Monitor the modules of an enterprise application 	ules of an enterprise					
Deploy E18 modules						
 Install a Web application 						

5. Click **Install**. The Install Application Assistance page is displayed.





6. Select RTFCARD.ear and click **Next**. This action displays the Install Application Assistance page with the Choose targeting style section.

Figure 23: Install Application Assistance with choose Target Style

ORACLE WebLogic Server Ad	ministration Console 14.1.1
Change Center	🏦 Home Log Out Preferences 🔤 Record Help
View changes and restarts	Home >Summary of Deployments >Summary of JMS Modules >RTI >Summary of Deployments >Summary of JMS Modules >Summary of Deployments
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Install Application Assistant Back Next Finish Cancel
Domain Structure	Choose installation type
BD812UT	Select if the deployment should be installed as an application or library.
Deployments Deployments Deployments Defloyments Defloyments Defloyments Deployments Deployme	The application and its components will be targeted to the same locations. This is the most common usage. Install this deployment as an application Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications. Install this deployment as a library Back Next Frish Cancel
Foreign JNDI ProvidersWork Contexts	
How do I 🗉	
 Start and stop a deployed enterprise application 	
Configure an enterprise application	
Create a deployment plan	
 Target an enterprise application to a server instance 	
Test the modules in an enterprise application	

7. By default, the **Install this deployment as an application** option in the Choose targeting style section is selected. Click **Next**. This action displays the Install Application Assistance page in the Optional Settings section.

Figure 24: Install the Application Assistance page with Optional Settings

Persistent Stores Foreign JNDI Providers Work Contexts	What security model do you want to use with this application?					
ow do I	D) only, use only roles and policies unit are defined in the deployment descriptors.					
Start and stop a deployed enterprise application	 Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. 					
Create a deployment plan	Advanced. Here a custom model that you have configured on the realm's configuration page					
Target an enterprise application to a server instance	Source Accessibility					
Test the modules in an enterprise application	How should the source files be made accessible?					
ystem Status 🖂	O Use the defaults defined by the deployment's targets					
ealth of Running Servers as of 2:14 PM	Recommended selection.					
Failed (0) Critical (0)	○ Copy this application onto every target for me					
Overloaded (0)	During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.					
Warning (0) OK (1)	I will make the deployment accessible from the following location					
	Location: /scratch/fccmapp/Oracle/Middleware/Oracle_Home/user_proj					
	Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.					
- Plan Source Accessibility						
	How should the plan source files be made accessible?					
	Use the same accessibility as the application					

8. Retain the default selections and click **Next**. The Install Application Assistance page is displayed with the Review your choices and click Finish section.

Figure 25: Install the Application Assistance page with Review your choices and click Finish section

DRACLE WebLogic Server Administration Console 14.1.1								
Change Center	🔒 Home Log Out	Preferences 🖉 Record Help	Icome, weblogic Connected to: BD812UT					
View changes and restarts	Home >Summary of	Deployments >Summary of JMS Modules >RTI >Summary of Deployments >Summary of JMS Modules >Summary of Deployments						
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	bled. Future Install Application Assistant be activated as you Isin this domain. Back Next Finish Cancel							
Domain Structure	Review your choices and click Finish							
3D812UT	Click Finish to com — Additional Conf	plete the deployment. This may take a few moments to complete. Iguration						
Services -Messaging -JMS Servers	In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?							
Store-and-Forward AgentsJMS ModulesPath Services BBridgesData Surges	 Yes, take me No, I will revie Summary — 	o the deployment's configuration screen. w the configuration later.						
Deployment: /scratch/fccmapp/Oracle/Middleware/Oracle_Home/user_projects/domains/BD812UT/applications/RTFCARD.ear								
How do I Start and stop a deployed enterprise	Staging Mode:	I will make the deployment accessible at /scratch/fccmaps/Oracle/Middleware/Oracle_Home/user_projects/domains/BD812UT/applications/RTFCARD.ear						
configure an enterprise application	Start and stop a deployed enterprise application Plan Staging Use the same accessibility as the application Configure an enterprise application Mode							
Create a deployment plan								
Target an enterprise application to a server instance Target Summary Target Summary								

9. Select **No**, **I will review the configuration later** in the Additional Configuration section and click **Finish**. RTFCARD is added in the Name section of the Summary of Deployment page with the following message: *The deployment has been successfully installed*.

Figure 26: Summary of Deployment page with RTFCARD

View changes and restarts	Home >Summary of	of Deployments >Summary	of JMS Modules >RTI >Summary of Dep	loyments >Summary of JMS Moo	dules > Summa r	y of Deployments		
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Pressages							
Domain Structure	Structure Summary of Deployments							
Deployments	Configuration Control Monitoring							
Hessaging Masservers MS Servers MS Nodules MS Nodules	aging aging This page displays the list of Java EE applications and standalone application modules installed to this domain. MS Servers Store-and-Forward Agents MS Modules To install a new application or module for deployment to targets in this domain, click Install. To install a new application or module for deployment to targets in this domain, click Install. Sources Stores Ign JNDI Providers Contexts Listent Tores Listent T						ntrols on this page.	
How do I 🖂	🗆 Name 🐟			Stat	te Health	Туре	Targets	Deployment Order
Install an enterprise application Configure an enterprise application	□ E BD81	12UT		Activ	ve 🗸 OK	Enterprise Application	AdminServer	100
Update (redeploy) an enterprise application Monitor the modules of an enterprise		CARD		Activ	ve 🖋 OK	Enterprise Application	AdminServer	100
application Deploy EJB modules	C Enterprise Application AdminServer 100				100			
Install Update Delete Showing 1 to 3 of 3 Previous Next								

10. Restart all OFS Analytical Applications Infrastructure (AAI) servers.

3.2.1.4.3 Deploying RTFCARD.ear in WebSphere

This section defines how to deploy RTFCARD.ear in WebSphere.



To deploy RTFCARD.ear in WebSphere, follow these steps:

./startServer.sh server1

- 2. Create an RTFCARD.ear folder in <WEBSPHERE_INSTALL_DIR>/RTFCARD.ear.
- 3. Copy <FIC_HOME>/RTFCardFraudIPEProcessing/RTFCARD.ear to <WEBSPHERE_INSTALL_DIR>/RTFCARD.ear.
- 4. Open the following URL in the browser: http://<ipaddress>:<Administrative Console Port>/ibm/console. (use https protocol if SSL is enabled). The login screen is displayed.

Figure 27: WebSphere Login Window

WebSphere. software	
	WebSphere Integrated Solutions Console User ID: admin Password: Log in
Licen: IBM, Inter produ IBM t	sed Materials - Property of IBM (c) Copyright IBM Corp. 1997, 2011 All Rights Reserved. the IBM logo, ibm.com and WebSphere are trademarks or registered trademarks of national Business Machines Corp., registered in many jurisdictions worldwide. Other ct and service names might be trademarks of IBM or other companies. A current list of rademarks is available on the Web at <u>Copyright and trademark information</u> .

- 5. Enter the user credentials that have administrator rights and click **Log In**.
- 6. From the LHS menu, select **Applications** and click **New Application**. The New Application window is displayed.



ew App	lication						
New A	New Application						
This p	This page provides links to create new applications of different types.						
Instal	a New Application						
	New Enterprise Application						
	New Business Level Application						
	New Asset						

7. Click **New Enterprise Application**. The **Preparing for the application installation** window is displayed.

Figure 29: Preparing for the application installation

reparing for the application installation ?
Specify the EAR, WAR, JAR, or SAR module to upload and install.
Path to the new application
🔿 Local file system
Full path Choose File No file chosen
Remote file system
Full path Browse
Next Cancel

8. Select **Remote File System** and click **Browse**.

Figure 30: Browse Remote Filesystems Window

rowse Remote Filesystems -					
Select the radio button next to the archive that you wish to install, or click on a directory name to view its contents.					
Contents of /scratch/IBM/WebSphere/AppServer/profiles/BD8123/installedApps/ofss-mum-889-Node3-Cell03/RTFCARD.ear					
RTFCARD.ear					
OK Cancel					

9. Navigate through folders and select the EAR file generated for RTFRAUD to upload and install.

Figure 31: Preparing for the application installation

aring for the application ins	allation			
pecify the EAR, WAR, JAR,	or SAR module to up	load and install.		
Path to the new appl	cation			
U Local file system				
Choose File No file	chosen			
Remote file system				
Full path				
/scratch/IBM/WebSp	here/profiles/BD812	/RTFCARD.ear	Browse	
Next Cancel				

10. Click Next.

Figure 32: Installation Options

reparing for the application installation				
How do you want to install the application? Fast Path - Prompt only when additional information is required. Detailed - Show all installation options and parameters.				
Choose to generate default bindings and mappings Previous Next Cancel				

11. Select the **Fast Path** option and click **Next**. The Install New Application window is displayed.

Figure 33: Install New Application

E

Install New Application	
Specify options for installing enterprise applications and modules.	
Step 1: Select	Select installation options
Installation options	Specify the various options that are available for your application.
to servers	Precompile JavaServer Pages files
Step 3 Map virtual hosts for Web modules	Directory to install application
Step 4 Summary	Distribute application
	Use Binary Configuration
	Deploy enterprise beans
	Application name RTFCARD
	Create MBeans for resources
	Override class reloading settings for Web and EJB modules
	Reload interval in seconds
	Deploy Web services
	Validate Input off/wam/fail
	File Permission
	Allow all files to be read but not written to
	Allow HTML and image files to be read by everyone
	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755
	Application Build ID
	Allow dispatching includes to remote resources
	Allow servicing includes from remote resources
	Business level application name
	Asynchronous Request Dispatch Type
	Disabled 🗸
	Allow EJB reference targets to resolve automatically
	Deploy client modules Client deployment mode
	Isolated V
	Validate schema
Next Cancel	

12. Enter the required information and click **Next**. The Map Modules to Servers window is displayed.



installation options	Map modules to servers					
Step 2: Map modules to servers Step 3 Map virtual hosts for Web modules Step 4 Summary	Specify tar the module server or c serve as ro each Web Clusters a WebSphe Apply	gets such as es that are co lispersed amo uters for req server is gene ind servers: rre:cell=ofss-	application servers or clu ntained in your applicati ong several application se uests to this application. erated, based on the app mum-889-Node3-Cell03,	usters of application servers where you want to install on. Modules can be installed on the same application ervers. Also, specify the Web servers as targets that The plug-in configuration file (plugin-cfg.xml) for lications that are routed through. node=ofss-mum-889-Node3,server=server1		
	Select	Module Inline	URI RTFCARD.war,WEB-	Server WebSphere:cell=ofss-mum-889-Node3-		

13. Select the **Inline Processing** check box and click Next. The Map Virtual hosts for the Web modules page are displayed.

Insta	Il New Application	2							
s	Specify options for installing enterprise applications and modules.								
	Step 1 Select Map virtual hosts for Web modules								
	<u>Step 2</u> Map modules to servers	es Specify the virtual host for the Web modules that are contained in your application. You can install Web modules on the same virtual host or disperse them among several hosts.							
Step 3: Map virtual hosts for Web modules									
	<u>Step 4</u> Summary	Select Web module Virtual host Inline Processing default_host ▼							
	Previous Next Cancel								

Figure 35: Map Virtual hosts for Web modules page

- 14. Select the **Inline Processing** check box and click **Next**. The Metadata for the modules page is displayed.
- 15. Select the **Metadata-complete** attribute check box and click **Next**. The Summary page is displayed.

Figure 36: Summary page

nstall New Application						
Specify options for installing enterprise app	lications and modules.					
Step 1 Select	Summary					
	Summary of installation options					
<u>Step 2</u> Map modules to servers	Options	Values				
Stop 2 Map withual	Precompile JavaServer Pages files	No				
hosts for Web modules	Directory to install application					
→ Step 4: Summary	Distribute application	Yes				
y Step Hoummary	Use Binary Configuration	No				
	Deploy enterprise beans	No				
	Application name	RTFCARD				
	Create MBeans for resources	Yes				
	Override class reloading settings for Web and EJB modules	No				
	Reload interval in seconds					
	Deploy Web services	No				
	Validate Input off/warn/fail	warn				
	Process embedded configuration	No				
	File Permission	.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755				
	Application Build ID	Unknown				
	Allow dispatching includes to remote resources	No				
	Allow servicing includes from remote resources	No				
	Business level application name					
	Asynchronous Request Dispatch Type	Disabled				
	Allow EJB reference targets to resolve automatically	No				
	Deploy client modules	No				
	Client deployment mode	Isolated				
	Validate schema	No				
	Cell/Node/Server	Click here				
Previous Finish Cancel						

16. Click **Finish**. On successful installation, the system displays a message.
Figure 37: Installation Success

Installing...

there are enterprise beans in the application, the EJB deployment process can take several minutes. Do not save the configuration until the process completes.
theck the SystemOut.log on the deployment manager or server where the application is deployed for specific information about the EJB deployment process as it occurs.
DMA5016I: Installation of RTFCARD started.
DMA5067I: Resource validation for application RTFCARD completed successfully.
DMA5058I: Application and module versions are validated with versions of deployment targets.
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
DMA50811: The bootstrap address for client module is configured in the WebSphere Application Server repository.
DMA5053I: The library references for the installed optional package are created.
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
DMA50011: The application binaries are saved in /scratch/IBM/WebSphere/AppServer/profiles/BD8123/wstemp/92668751/workspace/cells/ofss-mum-889-Node3-Cell03/applications/RTFCARD.ear/RTFCARD.ear
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
ECJ0400I: Successfully updated the application RTFCARD with the appContextIDForSecurity information.
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
DMA5005I: The application RTFCARD is configured in the WebSphere Application Server repository.
DMA5113I: Activation plan created successfully.
DMA5011I: The cleanup of the temp directory for application RTFCARD is complete.
DMA5013I: Application RTFCARD installed successfully.
Application RTFCARD installed successfully.
o start the application, first save changes to the master configuration.
Changes have been made to your local configuration. You can: • <u>Save</u> directly to the master configuration.
Review changes before saving or discarding.
o work with installed applications, click the "Manage Applications" link.
lanage Applications

17. Click **Save** and save the master file configuration. This action displays the details on the *Master File Configuration* page.

Figure 38: Master File Configuration page

Enterprise Applications				
Enterprise Applications				
Use thi	s page to manage installed applications. A single applicati	on can be deployed onto multiple servers.		
Pret	rerences			
Star	t Stop Install Uninstall Update Rollout Updat	te Remove File Export Export DDL Export File	Liberty Advisor 🔻	
D	ē 👯 🖗			
Select	Select Name 🗘 Application Status 🖄 Liberty Advisor Summary 🖄			
You ca	an administer the following resources:			
	□ <u>BD812UP3WS</u> → Ø		0	
	DefaultApplication		0	
RTECARD * Ø		0		
	ivtApp	•	0	
	□ <u>auery</u>		0	
Total 5				

NOTE	Make sure you take a backup of the Jersey Jar file to any folder and remove it by running the following command in the mentioned path.	
	Path:< Deployed Area>/ <rtfcard.ear>/ <rtfcard.war>/WEB-INF/LIB</rtfcard.war></rtfcard.ear>	
	Command: Delete jersey-bundler(jersey- bundle-1.6.jar) jar	

18. Select RTFCARD and click **Start**. This action dsiplays the Enterprise Application page with a confirmation message.

Enterprise Applications				
Messages Application RTFCARD on server server1 and node ofss-mum-889-Node3 started successfully. The collection may need to be refreshed to show the current status.				
Enterp	rise Applications			
Use thi	s page to manage installed applications. A single applicati	on can be deployed onto multiple servers.		
Pref	erences			
Star	t Stop Install Uninstall Update Rollout Upda	te Remove File Export Export DDL Export Fi	le Liberty Advisor •	
	ā # #			
Select	Name 🗘	Application Status 位	Liberty Advisor Summary 堂	
You ca	an administer the following resources:			
	BD812UP3WS	\$	0	
	DefaultApplication	\$	0	
	RTFCARD	•	0	
	<u>ivtApp</u>	•	0	
	<u>query</u>	•	0	
Total 5				

Figure 39: Enterprise Application page with the Confirmation message

19. Restart all OFS AAAI servers.

3.2.1.5 Commands to Execute to Import IPE Configs

Execute the below command in the specified path to import IPE configs.

Path: <FIC HOME>/ficapp/common/FICServer/bin/

Command:./RTIImport.sh

\$FIC_HOME/RTFCardFraudIPEProcessing/IPEAssessmentImport/ OFS_RTFCARD_RTIExport_Fraud.xml <INFODOM> OFS_FRAUD_EE true

4 Managing User Administration and Security Configuration

This chapter provides instructions on managing user administration and configuring the security attributes for the Real Time Wire Fraud and Card Fraud components.

Topics:

- About User Administration
- User Provisioning Process Flow
- Managing User Administration
- Adding Security Attributes
- Business Domain and Jurisdiction Mapping
- Removing Security Attributes
- Business Domain and Jurisdiction Mapping

4.1 About User Administration

User administration enables you to create and manage users, and provide access rights based on their roles. This section discusses the following:

- Administrator permissions
- Creating and mapping users and user groups
- Mapping security attributes.

4.2 User Provisioning Process Flow

Figure 40: User Provisioning Process Flow



Table 5 lists the various actions and associated descriptions of the user administration process flow.

Table 5:	User	Provisioning	Process	Flow
----------	------	--------------	---------	------

Action	Description
Managing User Administration	Create and map users to user groups. This action allows Administrators to provide access, monitor, and administer users. This is applicable for both wire and card frauds.
Adding Security Attributes	Load security attributes. Security attributes are loaded using either Excel or SQL scripts. This is applicable only for card fraud.
Business Domain and Jurisdiction Mapping	Map security attributes to users. This action determines which security attributes control the user's access rights. This is applicable only for card fraud.

4.3 Managing User Administration

This section allows you to create, map, and authorize users to define a security framework that can restrict access to the Real Time Fraud component.

4.3.1 Managing Identity and Authorization

This section explains creating a user and providing access to the Real Time Fraud component.

This section covers the following topics:

- Managing Identity and Authorization Process Flow
- Creating and Authorizing a User
- Mapping a User with a User Group.

4.3.1.1 Managing Identity and Authorization Process Flow

The following figure shows the process flow of identity management and authorization:

Figure 41: Managing Identity and Authorization Process Flow



Table 6 lists the various actions and associated descriptions of the user administration process flow.

Table 6: Administration Process Flow

Action	Description
Creating and Authorizing a User	Create a user. This involves providing a user name, user designation, and the dates between which the user is active in the application.
Mapping a User with a User Group	Map a user to a user group. This enables the user to have certain privileges that the mapped user group has.

4.3.1.2 Creating and Authorizing a User

The SYSADMN user creates a user and the SYSAUTH user authorizes a user in Real Time Fraud. For more information on creating and authorizing a user, see Oracle Financial Services Analytical Applications Infrastructure User Guide.

4.3.1.3 Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user can access the privileges as per the role. The SYSADMN user maps a user to a user group in Real Time Fraud.

Table 7 describes the predefined Fraud User Roles and corresponding User Groups.

Role	Privileges	User Group
Fraud Admin	Perform Batch Access	Fraud Admin
	Perform Batch Advanced	
	Perform Batch Authorize	
	Perform Batch Phantom	
	Perform Batch Read Only	
	Perform Batch Write	
	Manage User Preferences	
	Perform IPE Write	
	• Access Fraud applications and take action on transactions.	
Card Fraud Analyst	Access Fraud applications and take action on transactions.	Fraud Analyst

Table 7: Fraud Roles and User Groups

4.4 Adding Security Attributes

This section explains security attributes, the process of uploading security attributes, and mapping security attribute to users in the Real Time Card Fraud.

4.4.1 About Security Attributes

Security Attributes help an organization classify their users based on their geographical location, jurisdiction, and business domain to restrict access to the data they can view.

You need to map the roles with access privileges. Since these roles are associated with user groups, the users associated with the user groups can perform activities throughout various functional areas in Real Time Fraud.

4.4.1.1 Types of Security Attributes

The types of security attributes are as follows:

Jurisdiction

Fraud solutions use Jurisdictions to limit user access to data in the database. Records from the Oracle client that the Ingestion Manager loads must be identified with a jurisdiction and users of the system must be associated with one or more jurisdictions. In the Fraud application, users can view only data or alerts associated with jurisdictions to which they have access. You can use a jurisdiction to divide data in the database. For example:

- **Geographical**: Division of data based on geographical boundaries, such as countries, states, and so on.
- **Organizational**: Data division based on legal entities that compose the client's business.
- Other: Combination of geographic and organizational definitions. In addition, it is client driven and can be
- customized.
- Business Domain

Business domains are used for data access controls similar to jurisdiction but have a different objective. The business domain can identify records of different business types such as Private Clients verses Retail customers, or provide more granular restrictions to data such as employee data.

4.5 Business Domain and Jurisdiction Mapping

This section allows you to map Business Domains and Jurisdictions to User Groups for Real Time Card Fraud.

To map Business Domain and Jurisdiction, follow these steps:

1. Add entries for Business Domain in the KDD_BUS_DMN table in the atomic database

```
INSERT INTO KDD_BUS_DMN(
    BUS_DMN_CD,
    BUS_DMN_DESC_TX,
    BUS_DMN_DSPLY_NM,
    MANTAS_DMN_FL
)
VALUES
(
    'a',
    'General',
    'GEN',
    'Y'
)
```

2. Add entries for Jurisdiction in the KDD_JRSDCN table in the atomic database.

```
INSERT INTO KDD JRSDCN (
    JRSDCN CD,
    JRSDCN NM,
    JRSDCN DSPLY NM,
    JRSDCN DESC TX
)
VALUES
(
    'E',
    'East',
    'EAST',
    'EASTERN'
)
```

```
3. Add entries in FCC_FR_CARD_GROUP_SEC_ATTR_MAP to map the Business Domain to the
```

```
Groups.
```

)

)

)

```
INSERT INTO FCC_FR_CARD_GROUP SEC ATTR MAP (
    V_GROUP_CD,
    V_SEC_ATTR_CD,
    V SEC ATTR VAL
VALUES (
    'CARDFRAUDADMINGR',
    'BUSDMN',
    'a'
```

4. Add entries in FCC_FR_CARD_GROUP_SEC_ATTR_MAP to map the Jurisdiction to the Groups.

```
INSERT INTO FCC FR CARD GROUP SEC ATTR MAP (
```

```
V_GROUP_CD,
    V SEC ATTR CD,
    V SEC ATTR VAL
VALUES (
```

```
'CARDFRAUDADMINGR',
```

'JRSDCN', 'E'

)

5 Configuring Real Time Wire Fraud Scoring

This chapter provides information about configuring the Real Time Wire Fraud.

Topics:

- Operating Real Time Wire Fraud Service
- Managing Real Time Wire Fraud Scenarios/Rules

5.1 Operating Real Time Wire Fraud Service

The following sections explain about the Real Time Wire Fraud Service.

- Real Time Wire Fraud Service Request
- Real Time Wire Fraud Service Response

5.1.1 Real Time Wire Fraud Service Request

The client must provide input to the Real Time Wire Fraud service by posting relevant attributes into the IPE REST Service using either of the following:

<WEB PROTOCOL>://<WEB IP>:<WEB PORT>/RTFRAUD/service/json/score

The attributes must be in JSON format. For sample JSON input, see Appendix-A: Wire Fraud Sample JSON.

Table 8 shows the structure of the Real Time Wire Fraud message attributes.

Message Attributes	Description
type	Indicates the business name of the activity in Real Time Wire Fraud.
domain	Indicates the Inline Processing Segment Code for Real Time Wire Fraud.
appID	Indicates the application ID for Real Time Wire Fraud.

Table 8: Real Time Wire Fraud Message Attributes

See Appendix-C: Real Time Wire Fraud Request Attributes for the list of Real Time Wire Fraud request attributes.

5.1.2 Real Time Wire Fraud Service Response

Any input given to the Real Time Wire Fraud service will have a response or feedback message. The client must configure a REST Service feedback URL and expose that URL to the Real Time Fraud service to receive the response from Real Time Fraud service.

You must configure the REST Service feedback URL in the action.json.response.url parameter in the <RTFraud.war Deployed Path>/RTFRAUD/conf/install.properties file and then restart the webserver for the configuration to take effect.

5.2 Managing Real Time Wire Fraud Scenarios/Rules

In Real Time Wire Fraud, certain out-of-the-box fraud scenarios or rules are configured in IPE. You can modify existing rules or create new ones in IPE per customer requirements.

Table 9 shows the sample out-of-the-box wire fraud risk rules configured for real-time delectation.

Wire Fraud Scenarios/Rules	Description
Cross Border Transaction	This risk rule is used to assign risk score when source country and destination country are different in a transaction.
First Transaction to a new Beneficiary & AMT> Threshold	This risk rule is used when a customer initiates a transaction to a new beneficiary for the first time. This rule checks first time transaction along with amount threshold and then assigns the risk score.
Largest Transaction for the Customer	This risk rule is used to assign risk score when a customer initiates a transaction with largest amount. Current transaction amount is compared with the average of last 10 transactions multiplied by 1.3.
Multiple Transactions from the Same IP and different Account	This risk rule is used to assign risk score when a customer initiates multiple transactions from same IP but from different customer accounts within a lookback period of 30 minutes. The lookback period is configurable.
Multiple Transactions from the multiple IP for the same Account	This risk rule is used to assign risk score when a customer initiates multiple transactions from multiple IPs and from different customer accounts within a lookback period of 30 minutes. The lookback period is configurable.
Transaction to a new Beneficiary	This risk rule is used to assign risk score when a new beneficiary is introduced for the financial institutions across customers.
Transaction to suspicious beneficiary and amount > Threshold	This risk rule is used to assign risk score when a transaction occurs with suspicious beneficiary with exceeding amount threshold. This risk rule is based on exclude list.

Table 9: Fraud Risk Rules

5.2.1 Modify Fraud Rules

You can modify existing fraud rules or create new rules in IPE as per requirement.

Perform the following to modify fraud rules.

- 1. Navigate to the Inline Processing Home Page.
- 2. Click **Evaluations**. The Evaluations page is displayed.
- 3. Add or modify the evaluation rules.

For more information, see Inline Processing Engine User Guide.

6 Configuring Real Time Card Fraud Scoring

This chapter provides information about configuring the Real Time Card Fraud.

Topics:

- Operating Real Time Card Fraud Service
- Managing Real Time Card Fraud Scenarios/Rules

6.1 Operating Real Time Card Fraud Service

The following sections explain about the Real Time Card Fraud Service.

- Real Time Card Fraud Service Request
- Real Time Card Fraud Service JMS Response Details

6.1.1 Real Time Card Fraud Service Request

The client must provide input to the Real Time Card Fraud service by posting relevant attributes into the IPE REST Service using either of the following:

• API:

```
<WEB_PROTOCOL>://<WEB_IP>:<WEB_PORT>/<DOMAIN>/rest-api/FRAUDREST/
CardIPEService/postMessageToQueue
```

• JSP:

<host>:<port>/RTFCARD/CardTransactions.jsp

- IPE JMS Client:
 - To configure the JMS Client, follow the steps mentioned in chapters Configuring IPE Sample Application Client for Real Time Mode and Running the IPE Client for Real Time in the OFS Inline Processing Engine Sample Application Installation Guide.
 - Copy the following jars to the mentioned path.

Table 10 shows the jars to be copied along with paths for conguring IPE JMS Client.

Table 10: Jars and Paths to Configure IPE JMS Client

Jars	To Path
<pre>\$FIC_HOME/RTFCardFraudIPEProcessing/ IPEJMSTestClient/realtime-client- test.jar</pre>	<pre>/scratch/fccmapp/BD8123/BD8123/ realtime_processing/ipesampleapp/ client/lib</pre>
<pre>\$FIC_HOME/ficweb/webroot/WEB-INF/ lib/commons-math3-3.6.1.jar</pre>	<pre>\$FIC_HOME/realtime_processing/ ipesampleapp/client/lib</pre>

The attributes must be in JSON format. For sample JSON input, see Appendix-B: Card Fraud Sample JSON.

Table 11 shows the structure of the Real Time Card Fraud message attributes.

Message Attributes	Description
type	Indicates the business name of the activity in Real Time Card Fraud.
domain	Indicates the Inline Processing Segment Code for Real Time Card Fraud.
appID	Indicates the application ID for Real Time Card Fraud.

Table 11: Real Time Card Fraud Message Attributes

See Appendix-D: Real Time Card Fraud Request Attributes for the list of Real Time Card Fraud request attributes.

6.1.1.1 Real Time Card Fraud Service JMS Response Details

This section shows the details related to the Real Time Card Fraud Service JMS Response.

Table 12 shows the Real Time Card Fraud Service JMS Response Details.

JMS Response	Alert Action	Alert Description	Response
Alert Not Created	Clean	This response is generated on the hold queue if the posted transaction is clean, i.e., it does not match any of the given IPE rules in the application. This action doesn't generate any alert.	<pre>{ "Transaction ID" : 2781, "Message Reference" : Message Reference, "Status" : CLEAN }</pre>
Alert Not Created	Error	This response is generated on the hold queue if the posted transaction gives an error because of bad data, bad network, server issues or any such cases.	<pre>{ "Transaction ID" : 2787, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : Failed to Evaluate, "Assessment ID" : "", "Score" : "", "Decision" : "" }</pre>
			}

Table 12: Real Time Card Fraud Service JMS Response Details

JMS Response	Alert Action	Alert Description	Response
Alert Created	Held	This response is created on the hold queue if the posted transaction fails at any IPE rules provided in the application. An alert in held status gets generated and the users can view it in the UI.	<pre>{ "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10.0, "Decision" : "" }</pre>
Alert Created	Release	This response is created on the hold queue if the posted transaction is released from the UI or auto-closed by Card Administrator SLA settings.	<pre>{ "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : CLEAN, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Released } </pre>
Alert Created	Blocked	This response is created on the hold queue if the posted transaction is blocked from the UI or auto-closed by Card Administrator SLA settings.	<pre>{</pre>

Table 12: Real Time Card Fraud Service JMS Response Details

6.2 Managing Real Time Card Fraud Scenarios/Rules

In Real Time Card Fraud, certain out-of-the-box fraud scenarios or rules are configured in IPE. You can modify existing rules or create new ones in IPE per customer requirements.

Table 13 shows the sample out-of-the-box fraud risk rules configured for real-time delectation.

Table 13: Fraud Risk Rules

Card Fraud Scenarios/Rules	Description
sudden surge in credit utilization	Assigns risk score if the user suddenly has high card usage in a short period

6.2.1 Modify Fraud Rules

You can modify existing fraud rules or create new rules in IPE as per requirement.

Perform the following to modify fraud rules.

- 1. Navigate to the Inline Processing Home Page.
- 2. Click **Evaluations**. The Evaluations page is displayed.
- 3. Add or modify the evaluation rules.

For more information, see Inline Processing Engine User Guide.

7 Managing Real Time Wire Administration

Real Time Wire Administration enables you to configure SLA, a set of rules, conditions, and time for SLA. SLA defines the cut-off time period from the moment when payment is held by the Fraud application, within which the user must take necessary action.

Whenever a transaction satisfies the rules configured for the SLA, the user must take necessary action on that transaction within the specified cut-off time. The system automatically takes action on the transactions that are not acted upon before.

Topics:

- Accessing Real Time Wire Administration
- Configuring Real Time Wire Administration

7.1 Accessing Real Time Wire Administration

To configure Real Time Wire Administration, you must log in to the Fraud Enterprise Edition application as an Administrator.

1. Enter the OFSAA URL in your browser.

The OFSAA Login page is displayed.

Figure 42: OFSAA Login Page

ORACLE Financial Services Analytical Applications	⊠ <u>About</u>
Language US-English 🗸	
User ID	
Password	
Login	
Version 8.0.6.0.0 Conviright © 1092 2018 Oracle and/or its affiliates. All rights	
reserved.	

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



Ensure to login as an Administrator.

4. Click Login.

This action displays the **Applications** page.

Figure 43: Fraud Enterprise Edition Applications Page

		🔠 🖰 US-English 🔻 FRADMIN 🔻 🔟 🕼
APPLICATIONS		
	Financial Services Fraud Enterprise Edition	
	Application for Fraud Enterprise Edition	

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 44: Fraud Enterprise Edition Home Page

🖀 Home	=	ORACLE [®] Financial Services Fraud Enterprise Edition	(1)
Navigation List			
🖄 Behavior Detection	>		
🖾 Real Time Transactions			
🖄 Real Time Administration			
Real Time Card Administration			
🖄 Real Time Card Transactions			
Fraud User Security Administration	>		
DEEFERICAS EL CERTIS CONTRACTO			
herestellerer differenzetikenne			

6. Click **Real Time Wire Administration** in the Navigation List.

This action displays the Real Time Wire Administration page.

7.2 Configuring Real Time Wire Administration

On the Real Time Wire Administration page, you can configure SLA by creating new rules and conditions for each rule, configuring SLA cut-off time and priority for each rule, enabling the SLA, and so on.

Perform the following to configure SLA:

- 1. Navigate to the Real time Wire Administration page.
- 2. Click Create New Rule.

The **Create New Rule** section expands and displays the fields required to create a new rule.

3. Enter the following details in the **Create New Rule** section.

Table 14 shows the details regarding the create new rule section.

Table 14: Create New Rule

Field	Description
Rule ID	Indicates the Rule ID.
Rule Name	Indicates the rule name.

Table 14: Create New Rule

Field	Description
Priority	Indicates the priority given for a rule.
Actions	Indicates the action configured for a rule.

4. Click Create New Condition in the Create New Rule section.

The **Create New Condition** section expands and displays the fields required to create a new condition.

5. Enter the following details in the **Create New Condition** section.

Table 15 shows the details regarding the create new condition section.

Table 15: Create New Condition

Field	Description
Attribute Name	Select the attribute name for which you want to create a new condition.
Comparator	Select the comparator.
Value	Enter a value for the condition.

6. Click Save.

The new rule is created with the added conditions and displayed in the **Configuration** section.

7. Click **Configuration**.

The Configuration section expands.

8. Turn on the **Enable** button to enable the SLA.

You can also enable individual rule by turning on the **Enable** button corresponding to each rule in the **Configurations** section.

- 9. Enter a cut-off time period in **SLA (minutes)** field.
- 10. Click Save.

NOTE

This action configures the SLA for the Real Time Fraud.

8 Managing Real Time Card Administration

Real Time Card Administration enables you to configure SLA, a set of rules, conditions, and time for SLA. SLA defines the cut-off time period from the moment when payment is held by the Fraud application, within which the usermust take necessary action.

Whenever a transaction satisfies the rules configured for the SLA, the user must take necessary action on that transaction within the specified cut-off time. The system automatically takes action on the transactions that are not acted upon before.

Topics:

- Accessing Real Time Card Administration
- Configuring Real Time Card Administration
- This action configures the SLA for the Real Time Fraud.

8.1 Accessing Real Time Card Administration

To configure Real Time Card Administration, you must log in to the Fraud Enterprise Edition application as an Administrator.

1. Enter the OFSAA URL in your browser.

The OFSAA Login page is displayed.

ORACLE [®] Financial Services Analytical Applicat	ions	⊠ <u>About</u>
	Language US-English 🗸	
	User ID	
	Password	
	Login	
	Version 8.0.6.0. Copyright © 1993, 2018 Oracle and/or its affiliates. All rights reserved.	

Figure 45: OFSAA Login Page

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



Ensure to login as an Administrator.

4. Click Login.

The **Applications** page is displayed.

Figure 46: Fraud Enterprise Edition Applications Page

	US-English V FRADMIN V 🔝 🗛
Financial Services Fraud Enterprise Edition Application for Fraud Enterprise Edition	

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 47: Fraud Enterprise Edition Home Page

😤 Home	=	ORACLE [*] Financial Services Fraud Enterprise Edition	ch 💷
Navigation List			
😇 Behavior Detection	>		
🛱 Real Time Transactions			
🖄 Real Time Administration			
🗟 Real Time Card Administration			
觉 Real Time Card Transactions			
🛱 Fraud User Security Administration	>		
tereställere förstrestär met			

6. Click Real Time Card Administration in the Navigation List.

The Real Time Card Administration page is displayed.

8.2 Configuring Real Time Card Administration

On the Real Time card Administration page, you can configure SLA by creating new rules and conditions for each rule, configuring SLA cut-off time and priority for each rule, enabling the SLA, and so on.

Perform the following to configure SLA:

- 1. Navigate to the Real Time Card Administration page.
- 2. Click Create New Rule.

The **Create New Rule** section expands and displays the fields required to create a new rule.

3. Enter the following details in the Create New Rule section.

Table 16 shows the details regarding the create new rule section.

Table 16: Create New Rule

Field	Description
Rule ID	Indicates the Rule ID.

Table 16: Create New Rule

Field	Description
Rule Name	Indicates the rule name.
Priority	Indicates the priority given for a rule.
Actions	Indicates the action configured for a rule.

4. Click Create New Condition in the Create New Rule section.

The **Create New Condition** section expands and displays the fields required to create a new condition.

5. Enter the following details in the **Create New Condition** section.

Table 17 shows the details regarding the create new condition section.

Table 17: Create New Condition

Field	Description
Attribute Name	Select the attribute name for which you want to create a new condition.
Comparator	Select the comparator.
Value	Enter a value for the condition.

6. Click Save.

The new rule is created with the added conditions and displayed in the **Configuration** section.

7. Click **Configuration**.

The Configuration section expands.

8. Turn on the **Enable** button to enable the SLA.

NOTE

You can also enable individual rule by turning on the **Enable** button corresponding to each rule in the **Configurations** section.

- 9. Enter a cut-off time period in **SLA (minutes)** field.
- 10. Click Save.

This action configures the SLA for the Real Time Fraud.

9 Appendix-A: Wire Fraud Sample JSON

The JSON input data must be in the following format:

{

```
"type":"FCC_FR_TRANSACTIONS",
"domain":"PFR",
"appId":"OFS FRAUD EE",
"runtype":1,
"runParam":1,
"attributes":{
   "To Latitude":"40.73868",
   "From Latitude":"78.9629",
   "From Longitude":"20.5937",
   "To Longitude":"-73.93570",
   "Account Source UniqueID":"",
   "Authentication Mode":"",
   "Browse Type":"",
   "Current Date":"",
   "Customer Source UniqueID":"",
   "IP GEO Domain":"",
   "IP Address":"12.56.23.86",
   "IP Address City":"Delhi",
   "IP Address Country":"India",
   "IP GEO ISP":"",
   "IP Organisation Name":"",
   "IP Address State":"",
   "IP GEO Autonomous System Number":"",
   "IP GEO Autonomous System Organization":"",
   "IP GEO Is Anonymous Proxy":"",
   "IP GEO User Type":"",
   "OS Type":"",
   "Referrer Site":"",
   "Session ID":"",
   "Source System Code":"",
   "Time":"",
   "User Agent":"",
```

"Web Session Value":"ELISSA", "Login Time Session":"", "Session Number":"", "Channel Info":"SWIFT", "Payment Type":"", "Transaction Type Code":"TYPE1", "ACH Batch ID":"", "Reoccurring Flag":"", "Message Type":"", "Message Direction":"OUTGOING", "Payment International Flag":"", "Credit/Debit Code":"", "Transaction unique SIQ ID":"", "Message Reference": "MSG00079", "Sender":"", "Receiver": "BOFAUS6S", "Debited Branch":"", "Credited Branch":"", "Transaction Currency": "DOLLAR", "Transaction Amount":"999888", "Transaction Original Currency":"", "Transaction Original Amount":"", "Payment Value Date":"", "Originator Party AccountID/IBAN":"EXMLENHRTHRCP-3804", "Originator Party Name":"Sep1Test2", "Originator Party BIC":"", "Originator Party Countrycode":"US", "Originator Party Identifier":"XXXCUSPAGERISKTOLAC-4500-RB", "Counterparty AccountID/IBAN":"ACPOTCHKFRAC-6540", "Counterparty Name":"Drakeo", "Counterparty BIC":"", "Counterparty Country Code":"UK", "Counterparty Identifier":"CUMCT-ALT2-MLB-SAC-03-RFT", "Involved Party 1 Type":"", "Involved Party 1 AccountID/IBAN":"", "Involved Party 1 Name":"",

```
"Involved Party 1 BIC":"",
   "Involved Party 1 Country Code":"",
   "Involved Party 1 Identifier":"",
   "Involved Party 2 Type":"",
   "Involved Party 2 AccountID/IBAN":"",
   "Involved Party 2 Name":"",
   "Involved Party 2 BIC":"",
   "Involved Party 2 Country Code":"",
   "Involved Party 2 Identifier":"",
   "Involved Party 3 Type":"",
   "Involved Party 3 AccountID/IBAN":"",
   "Involved Party 3 Name":"",
   "Involved Party 3 BIC":"",
   "Involved Party 3 Country Code":"",
   "Involved Party 3 Identifier":"",
   "Source Country":"US",
   "Destination Country":"UK",
   "Payment Information":"",
   "Details of Charges":"",
   "Transaction Date Start":"01-FEB-2022",
   "Transaction Date End":"15-FEB-2022"
},
"additionalParams":{
}
```

}

10 Appendix-B: Card Fraud Sample JSON

The JSON input data must be in the following format

```
{
    "type": "FCC FR CARD TRANSACTIONS",
    "domain": "CFR",
    "appId": "OFS FRAUD EE",
    "runtype": 1,
    "runParam": 1,
    "attributes": {
        "AEVV Result Code": "2",
        "ATM Financial Institution ID/Teller terminal ID": "ATM Financial
Institution ID/Teller terminal ID",
        "AVS Address Response": "2",
        "AVS Postcode Response": "2",
        "AVV Result Code": "2",
        "Account Added Date": "2022-03-23",
        "Account Available Balance": "100000",
        "Account Balance Amount": "1000",
        "Account Balance Type": "Account Balance Type",
        "Account Billing Currency Code": "INR",
        "Account Country": "IND",
        "Account Credit Limit Amount": "10000",
        "Account Credit Limit Currency": "INR",
        "Account Currency Code": "INR",
        "Account Current Auth Amount": "5000",
        "Account Current Balance Amount": "10000",
        "Account Delinquency History": "Account Delinquency History",
        "Account Limit Type": "ALT",
        "Account Number": "3923287323",
        "Account Open Date": "2021-04-28",
        "Account Status Code": "A",
        "Account Type": "CHK:Checking",
        "Account branch ID": "Account branch ID",
        "Account postal code": "Account postal code",
        "Action": "",
```

"Action Time": "", "Annual Income": "3520000", "Assignee": "", "Authentication Method": "AuthMethod", "Authentication Mode": "Auth Mode", "Authorization Code": "Auth Code", "Available limit": "8000", "Biometric verification": "2", "Browse Type": "Browse Type", "CAVV Result Code": "2", "CVR result": "2", "CVV2 Response": "0", "Card Bin prefix": "1234567", "Card Block Code": "F", "Card DOB": "2021-04-28", "Card Issue Date": "2021-04-12", "Card Last 4 Digits": "0000", "Card Number": "123456123456123457", "Card POS entry Mode": "0", "Card Renewal Date": "2021-04-28", "Card account open date": "2021-04-28", "Card activation Date": "2021-04-28", "Card credit limit change date": "2021-04-28", "Card holder Address 1": "Card holder Address 1", "Card holder Address 2": "Card holder Address 2", "Card holder Address 3": "Card holder Address 3", "Card holder City": "Card holder City", "Card holder Country": "Card holder Country", "Card holder Home Phone": "Card holder Home Phone", "Card holder State": "Card holder State", "Card holder email ID": "Card holder email ID", "Card holder mobile phone": "Card holder mobile phone", "Card holder postal code": "Card holder postal code", "Card holder present Flag": "1", "Card holder work phone": "Card holder work phone", "Card last address change date": "2021-04-28",

"Card last pin change date": "2021-04-28", "Card last req date": "2021-04-28", "Card last status change date": "2021-04-28", "Card present Flag": "1", "Card sequence number": "12345", "Card status": "status", "Card verify Flag": "Y", "Cardholder Authentication Method": "1", "Cards Expiry Date": "2023-04-28", "Channel Amount Currency": "INR", "Channel Amount Limit": "20000", "Channel City": "Channel City", "Channel Country": "IND", "Channel Device ID": "Channel Device ID", "Channel Geographic Location": "Channel Geographic Location", "Channel Info": "Channel Info", "Channel Type": "CP", "Channel User ID": "Channel User ID", "Channel User ID Type": "Channel User ID Type", "Checking Account Customer Name": "Checking Account Customer Name", "Checking Account Number": "12345678322362", "Checking Account Sort Code": "Checking Account Sort Code", "Cheque Bounce Date": "2021-04-28", "Clearing Date": "2021-04-28", "Client Device Type": "Client Device Type", "Counterparty Name": "Counterparty Name", "Counterparty AccountID/IBAN": "Counterparty AccountID/IBAN", "Counterparty BIC": "Counterparty BIC", "Counterparty Country Code": "Counterparty Country Code", "Counterparty Identifier": "Counterparty Identifier", "Credit Utilization": "5004", "Credit/Debit Code": "Debit Code", "Credited Branch": "Credited Branch", "Current Date": "2021-04-28", "Cust Address verification Flag": "Y", "Customer Address Line 1": "Customer Address Line 1",

```
"Customer Address Line 2": "Customer Address Line 2",
"Customer Address Line 3": "Customer Address Line 3",
"Customer Address Line 4": "Customer Address Line 4",
"Customer Address Line 5": "Customer Address Line 5",
"Customer Address Line 6": "Customer Address Line 6",
"Customer Address Purpose Type Indicator": "B",
"Customer Alias": "Customer Alias",
"Customer City Of Residence": "Customer City Of Residence",
"Customer Country Code": "IND",
"Customer Country Of Residence": "IND",
"Customer Credit Score": "300",
"Customer Date of Birth": "2010-04-28",
"Customer Email Address 1": "Customer Email Address 1",
"Customer Email Address 2": "Customer Email Address 2",
"Customer Email Address Purpose Type 1": "B",
"Customer Email Address Purpose Type 2": "B",
"Customer First Name": "Customer First Name",
"Customer Last Name": "Customer Last Name",
"Customer Phone Extension 1": "12345",
"Customer Phone Extension 2": "12345",
"Customer Phone Number 1": "Customer Phone Number 1",
"Customer Phone Number 2": "Customer Phone Number 2",
"Customer Phone Purpose Type 1": "B",
"Customer Phone Purpose Type 2": "B",
"Customer Postal Code": "Customer Postal Code",
"Customer Region": "Customer Region",
"Customer Source UniqueID": "CustomerUniqueID",
"Customer State": "Customer State",
"Customer Type": "R",
"Customer global ID": "Customer global ID",
"Debited Branch": "Debited Branch",
"Depositing Date": "2022-03-23",
"Destination Country": "Destination Country",
"Details of Charges": "Details of Charges",
"Device ID": "Device ID",
"ECI Status": "02",
```

"Employer Name": "Employer Name", "Encrypted Card Number": "Encrypted Card Numb", "Eop Average Balance": "1004", "Execution Time": "", "Failed Login Attempts Count": "4", "Fraud Indicator": "Y", "Home Phone change last date": "2021-04-28", "IP Address": "10.232.23.34", "IP Address City": "IP Address City", "IP Address Country": "IP Address Country", "IP Address State": "IP Address State", "IP GEO Autonomous System Number": "IP GEO Autonomous System Number", "IP GEO Autonomous System Organization": "IP GEO Autonomous System Organization", "IP GEO Domain": "IP GEO Domain", "IP GEO ISP": "IP GEO ISP", "IP GEO Is Anonymous Proxy": "IP GEO Is Anonymous Proxy", "IP GEO User Type": "IP GEO User Type", "IP Organisation Name": "IP Organisation Name", "Identifier Issue Date": "2021-04-28", "Identifier Issue Place": "Identifier Issue Place", "Identifier Number": "Identifier Number", "Identifier Type": "Identifier Type", "Involved Party 1 Country Code": "IND", "Involved Party 1 Identifier": "Involved Party 1 Identifier", "Involved Party 1 AccountID//IBAN": "Involved Party 1 AccountID// IBAN", "Involved Party 1 BIC": "Involved Party 1 BIC", "Involved Party 1 Name": "Involved Party 1 Name", "Involved Party 1 Type": "Involved Party 1 Type", "Involved Party 2 Country Code": "IND", "Involved Party 2 Identifier": "Involved Party 2 Identifier", "Involved Party 2 AccountID\/IBAN": "Involved Party 2 AccountID\/ IBAN", "Involved Party 2 BIC": "Involved Party 2 BIC", "Involved Party 2 Name": "Involved Party 2 Name", "Involved Party 2 Type": "Involved Party 2 Type",

```
"Involved Party 3 Country Code": "IND",
        "Involved Party 3 Identifier": "Involved Party 3 Identifier",
        "Involved Party 3 AccountID/IBAN": "Involved Party 3 AccountID/IBAN",
        "Involved Party 3 BIC": "Involved Party 3 BIC",
        "Involved Party 3 Name": "Involved Party 3 Name",
        "Involved Party 3 Type": "Involved Party 3 Type",
        "Job Title": "Job Title",
        "Last Delinguent Date": "2021-04-28",
        "Login Time Session": "Login Time Session",
        "Mail Handling Instruction": "H",
        "Merchant Description": "Merchant Description",
        "Merchant Identifier": "12345",
        "Merchant MCC\/SIC": "Merchant MCC\/SIC",
        "Message Direction": "Message Direction",
        "Message Reference": "Message Reference",
        "Message Type": "Message Type",
        "Mobile Phone change last date": "2021-04-28",
        "Name on Card": "Name on Card",
        "No of Card consecutive txn": "10",
        "Number of cards on Account": "6",
        "OS Type": "OS Type",
        "Originator Party AccountID/IBAN": "Originator Party AccountID/IBAN",
        "Originator Party BIC": "Originator Party BIC",
        "Originator Party Countrycode": "IND",
        "Originator Party Identifier": "Originator Party Identifier",
        "Originator Party Name": "Originator Party Name",
        "Over Limit Balance": "500",
        "PIN Change Date": "2021-04-28",
        "PIN Tried count": "2",
        "POS Cardholder Authentication Capability": "POS Cardholder
Authentication Capability",
        "POS Merchant ID": "POS Merchant ID",
        "POS Terminal Capabilities": "POS Terminal Capabilities",
        "POS Terminal Entry Capability": "POS Terminal Entry Capability",
        "Password Change Date": "2021-04-28",
        "Past Due Flag": "Y",
```

```
"Payment Amount Bounced": "600",
        "Payment Information": "Payment Information",
        "Payment Instrument Routing Code": "123456",
        "Payment International Flag": "N",
        "Payment Instrument Number": "Instrument Number",
        "Payment Type": "Payment Type",
        "Payment Value Date": "2021-04-28",
        "Pin Verification Result": "2",
        "Purchase Amount": "5008",
        "Receipt Or Payment Indicator": "R",
        "Receiver": "Receiver",
        "Recent/Cycle Returns Count": "5",
        "Referrer Site": "Referrer Site",
        "Relationship Manager": "Relationship Manager",
        "Reoccurring Flag": "Reoccurring Flag",
        "Run Timestamp": "",
        "Sender": "Sender",
        "Session ID": "Session ID",
        "Session Number": "Session Number",
        "Source Country": "Source Country",
        "Status": "",
        "Terminal Acquirer Country": "IND",
        "Terminal ID": "Terminal ID",
        "Terminal Merchant/ATM/Teller Terminal City": "Terminal Merchant/
ATM/Teller Terminal City",
        "Terminal Acquirer Unique ID": "Terminal Acquirer Unique ID",
        "Terminal Merchant/FI Original script Name": "Terminal Merchant/FI
Original script Name",
        "Terminal Merchant/FI/Teller Terminal Name": "Terminal Merchant/FI/
Teller Terminal Name",
        "Terminal Postal Code": "Terminal Postal Code",
        "Terminal State": "Terminal State",
        "Time": "",
        "Total Amount Overdue": "7534",
        "Transacting Card Number": "8374734636435",
        "Transaction Amount": "6000",
        "Transaction Automated Flag": "Y",
```

```
"Transaction Currency": "INR",
    "Transaction Date End": "2021-03-23",
    "Transaction Date Start": "2021-05-23 14:13:12",
    "Transaction Original Amount": "7534",
    "Transaction Original Currency": "INR",
    "Transaction Phone Number": "Transaction Phone Number",
    "Transaction Reversal Date": "2021-03-23",
    "Transaction Type Code": "Transaction Type Code",
    "Transaction unique SIQ ID": "",
    "Username": "Username",
    "Work Phone change last date": "2021-03-23",
    "Business Domain": "d",
    "Jurisdiction": "E",
    "ID Issuer/Assigner": "ID Issuer",
    "Role": "01",
    "Card Age": "365",
    "Authentication Result": "Result"
    "Customer Internal Id": "CUST-123"
},
"additionalParams": {}
```

}

11 Appendix-C: Real Time Wire Fraud Request Attributes

Table 18 shows the Real Time Wire Fraud Request Attributes along with their descriptions.

Table 18: Real Time Wire Fraud Request Attributes

Request Attributes	Description
From Latitude	Indicates the latitude unit representing the geographic coordinates of the location where the transaction is initiated.
From Longitude	Indicates the longitude unit that represents the location's geographic coordinates from where the transaction is initiated.
To Latitude	Indicates the latitude unit that represents the geographic coordinates of the location where the transaction ends.
To Longitude	Indicates the longitude unit that represents the geographic coordinates of the location where the transaction ends.
Authentication Mode	Indicates the authentication mode used for the transaction.
Browse Type	Indicates the type of browser used for the transaction. For example, Internet Explorer and Safari.
Current Date	Indicates the date when the transaction is initiated.
Customer Source UniqueID	Indicates if the bank wants to supply the Customer Source Unique ID.
IP GEO Domain	Indicates the domain name associated with the IP used for the transaction.
IP Address	Indicates the IP address used for the transaction.
IP Address City	Indicates the city associated with the IP address used for the transaction.
IP Address Country	Indicates the country associated with the IP address used for the transaction.
IP GEO ISP	Indicates the GEO ISP used for the transaction.
IP Organization Name	Indicates the organization name associated with the IP address used for the transaction.
IP Address State	Indicates the state associated with the IP address used for the transaction.
IP GEO Autonomous System Number	Indicates the GEO autonomous system number associated with the IP address used for the transaction.
IP GEO Autonomous System Organization	Indicates the GEO autonomous system organization associated with the IP used for the transaction.
IP GEO Is Anonymous Proxy	Indicates the GEO anonymous proxy associated with the IP used for the transaction.
IP GEO User Type	Indicates the GEO user type associated with the IP used for the transaction.
OS Type	Indicates the operating system type used for the transaction.
Referrer Site	Indicates the referrer site used for the transaction.
Session ID	Indicates the session ID of the transaction.

Request Attributes	Description
Source System Code	Indicates the source system code of the transaction.
Time	Indicates the session timestamp of the transaction.
User Agent	Indicates the user agent of the transaction.
Web Session Value	Indicates the web session value of the transaction.
Login Time Session	Indicates the time when the user logged in to initiate the transaction.
Session Number	Indicates the session number of the transaction.
Channel Info	Indicates the channel name or channel number of the transaction.
Payment Type	Indicates the payment type used for the transaction. For example, Wire, ACH, INSTANT, etc.
Transaction Type Code	Indicates the transaction type code. The values are payment request, return request, and refund request.
ACH Batch ID	Indicates the Batch ID number if the transaction uses the ACH payment type.
Reoccurring Flag	Indicates if the transaction is recurring in nature.
Message Type	Indicates the message type in the transaction.
Message Direction	Indicates the direction of the message in the transaction. The values are Inbound and Outbound.
Payment International Flag	Indicates if the transaction is for international payments.
Credit/Debit Code	Indicates if the transaction is credit or debit.
Transaction unique SIQ ID	Indicates the unique transaction SIQ ID supplied by banks.
Message Reference	Indicates the message reference which is unique for each transaction.
Sender	Indicates the sender's BIC (Bank Identifier Code) in a transaction.
Receiver	Indicates the receiver's BIC (Bank Identifier Code) in a transaction.
Debited Branch	Indicates the bank's branch code where amount is debited in the transaction.
Credited Branch	Indicates the bank's branch code where amount is credited in the transaction.
Transaction Currency	Indicates the currency in which the transaction is performed.
Transaction Amount	Indicates the transaction amount.
Transaction Original Currency	Indicates the original currency in which a transaction is initiated.
Transaction Original Amount	Indicates the original amount in which a transaction is initiated.
Payment Value Date	Indicates the date on which the actual value of the transaction amount is determined.
Originator Party AccountID/IBAN	Indicates the Account ID or IBAN (International Bank Account Number) of the originator party.
Originator Party Name	Indicates the originator's party name.

Request Attributes	Description
Originator Party BIC	Indicates the BIC (Bank Identifier Code) of the originator party.
Originator Party Countrycode	Indicates the country code of the originator party.
Originator Party Identifier	Indicates the identifier of the originator party.
Counterparty AccountID/ IBAN	Indicates the Account ID or IBAN (International Bank Account Number) of the counter party.
Counterparty Name	Indicates the counter party name.
Counterparty BIC	Indicates the BIC (Bank Identifier Code) of the counter party.
Counterparty Country Code	Indicates the country code of the counter party.
Counterparty Identifier	Indicates the identifier of the counter party.
Involved Party 1 Type	Indicates the type of middleman involved in the transaction.
Involved Party 1 AccountID/IBAN	Indicates the Account ID or IBAN (International Bank Account Number) of the middleman involved in the transaction.
Involved Party 1 Name	Indicates the name of the middleman involved in the transaction.
Involved Party 1 BIC	Indicates the BIC (Bank Identifier Code) of the middleman involved in the transaction.
Involved Party 1 Country Code	Indicates the country code of the middleman involved in the transaction.
Involved Party 1 Identifier	Indicates the identifier of the middleman involved in the transaction.
Source Country	Indicates the source country in the transaction.
Destination Country	Indicates the destination country in the transaction.
Payment Information	Indicates the payment information of the transaction.
Details of Charges	Indicates the details of any charges applied to the transaction.
Transaction Date Start	Indicates the receiving date and time of the transaction in the source system.
Transaction Date End	Indicates the end date and time of the transaction in the source system until it is analyzed in IPE. After the end date, the source system automatically rejects the transaction. If the transaction is scheduled for the next day, the difference between the Transaction Start Date and the Transaction End Date is several hours.

12 Appendix-D: Real Time Card Fraud Request Attributes

Table 19 shows the Real Time Card Fraud Request Attributes along with their descriptions.

Table 19: Real Time Card Fraud Request Attributes

Request Attributes	Description
Transaction unique SIQ ID	The sequence ID number of the transaction.
Authentication Method	The method used to authorize the transaction.
Channel Type	The type of the transaction channel.
Channel Info	The name of the transaction channel.
Channel User ID	The user ID of the party involved in the transaction.
Channel User ID Type	The type of ID of the party involved in the transaction.
Channel Device ID	The device ID of the party involved in the transaction.
Channel Amount Limit	The maximum allowable transaction amount for the channel.
Channel Amount Currency	The currency type of the transaction amount for the channel.
Channel Geographic Location	The geo location from which the transaction was originated.
Channel Country	The country the transaction was initiated from for the channel.
Channel City	The city the transaction was initiated from for the channel.
Customer Country Code	The country code of the country in which the customer resides.
POS Merchant ID	The point of sale merchant identifier associated with the transaction.
ATM Financial Institution ID/ Teller terminal ID	The financial institution identifier associated with the ATM from which the transaction was made.
Merchant MCC/SIC	The unique code of the merchant category.
Terminal Acquirer Unique ID	The unique identifier of the merchant acquirer associated with the terminal.
Terminal Acquirer Country	The country code of the merchant acquirer associated with the terminal.
Terminal ID	The unique identifier associated the terminal from which the transaction was made.
Terminal Merchant/ATM/ Teller Terminal City	The city associated with the merchant owner of the terminal.
Terminal Merchant/Fl/Teller Terminal Name	The name of the merchant who owns the terminal.
Terminal Merchant/Fl Original script Name	The name of the financial institution.
Terminal Postal Code	The postal code component of the terminal location on which the transaction was made.
Request Attributes	Description
--	---
Terminal State	The state component of the terminal location on which the transaction was made.
Customer Source UniqueID	The unique identifier associated with the customer within the source system.
Customer Date of Birth	The customer's date of birth.
Customer First Name	The first name of the customer.
Customer Last Name	The last name of the customer.
Customer global ID	The global id of the customer.
Customer Alias	The alias of the customer.
Customer Address Purpose Type Indicator	The purpose type indicator for the address.
Customer Address Line 1	The address line 1 for the Location
Customer Address Line 2	The address line 2 for the Location
Customer Address Line 3	The address line 3 for the Location
Customer Address Line 4	The address line 4 for the Location
Customer Address Line 5	The address line 5 for the Location
Customer Address Line 6	The address line 6 for the Location
Customer City Of Residence	The city of residence of the customer.
Customer Country Of Residence	The country of residence of the customer.
Customer Postal Code	The postal code component of this address.
Customer Region	The region component of this address.
Customer State	The state component of this address.
Customer Email Address 1	The primary email address of the customer.
Customer Email Address Purpose Type 1	The email address type of the customer's primary email address.
Customer Email Address 2	The secondary email address of the customer.
Customer Email Address Purpose Type 2	The email address type of the customer's secondary email address.
Customer Phone Extension 1	The phone extension for the customer's primary phone number.
Customer Phone Number 1	The primary phone number of the customer.
Customer Phone Purpose Type 1	The phone number type for the customer's primary phone number.
Customer Phone Extension 2	The phone extension for the customer's secondary phone number.
Customer Phone Number 2	The secondary phone number of the customer.

Request Attributes	Description
Customer Phone Purpose Type 2	The phone number type for the customer's secondary phone number.
Customer Credit Score	The credit score of the customer.
Identifier Number	The number of the government issued identifier for the customer.
Identifier Type	The jurisdiction that issued the customer's identifier.
Mail Handling Instruction	The mail handling instruction for this address.
Job Title	The job title of the customer.
Employer Name	The name of the employer of the customer.
Annual Income	The income of the annual of the customer.
Account Available Balance	The available balance of the account
Account Balance Amount	The balance of the account at the time of the transaction.
Account Balance Type	The type of balance associated with the account.
Account Billing Currency Code	The billing currency code for the account.
Account branch ID	The branch identifier for the branch at which the account was opened.
Account Country	The country code associated with the account.
Account Credit Limit Amount	The credit limit amount of the account.
Account Credit Limit Currency	The currency of for the credit limit of the account.
Account Current Auth Amount	The maximum authorized transaction amount for the account.
Account Current Balance Amount	The current balance of the account.
Account Open Date	Date on which the account was opened in the financial institution.
Account Number	The number of the account
Account Status Code	The status code of the account
Account Limit Type	The limit type of the account
Account postal code	The postal code of the account
Account Type	The type of the account
Account Delinquency History	The delinquency history of the account
Account Added Date	The last date on which a linked payment account was added to the customer's profile.
Checking Account Customer Name	The name of the customer associated with the checking account.

Request Attributes	Description
Checking Account Sort Code	The sort code of checking account associated with the card number.
Checking Account Number	Unique identifier of the checking account number associated with the credit card number.
Failed Login Attempts Count	The number of failed logins which occurred before a successful attempt.
Password Change Date	The last date on which the customer's login password was changed.
Username	The username of the customer.
PIN Change Date	The last date on which the customer's PIN was changed.
ECI Status	The outcome of authentication attempted on the transaction enforced by 3DS.
AVS Postcode Response	The postcode verification response of the AVS.
AVS Address Response	The address verification response of the AVS.
CVV2 Response	The verification response of the cv2.
Authorization Code	The authorization result code associated with the transaction.
Biometric verification	The results of the biometric verification.
Card POS entry Mode	The point of sale entry mode of the transaction.
Card present Flag	Flag indicating that the card was present for the transaction.
Card verify Flag	The verify flag of the card
Card holder present Flag	Flag indicating that the card holder was present for the transaction.
Cust Address verification Flag	Flag indicating if the customer's address was verified.
Pin Verification Result	The result of the PIN verification attempted at the terminal.
PIN Tried count	The number of failed PIN entries attempted before the successful result.
Device ID	The device ID of the mobile device used to conduct the transaction.
Client Device Type	The type of device used to conduct the transaction.
Browse Type	The type of browser used to conduct the transaction.
IP Address	The IP address of the machine used to conduct the transaction.
IP Address City	The source city of the IP address.
IP Address Country	The source country of the IP address.
IP Address State	The source state of the IP address.
IP GEO Autonomous System Number	The Autonomous System Number of the IP address.
IP GEO Autonomous System Organization	The Autonomous System Organization of the IP address.
IP GEO Domain	The domain name associated with the IP address.

Request Attributes	Description
IP GEO Is Anonymous Proxy	Indicator that the IP address is an anonymous proxy.
IP GEO ISP	The internet service provider associated with the IP address.
IP GEO User Type	Indicates if the IP address is public, private, static, or dynamic.
IP Organisation Name	The organisation name associated with the IP address.
Login Time Session	The login type of the user session.
OS Type	The operating system of the machine used in the user session.
Session ID	The unique identifier associated with the user session.
Session Number	The number associated with the user session.
Time	The timestamp of the session.
Reoccurring Flag	Flag indicating that the transaction is recurring.
Counterparty Name	The name of the beneficiary party of the transaction.
Counterparty AccountID/ IBAN	The IBAN of the beneficiary party of the transaction.
Counterparty BIC	The BIC of the beneficiary party of the transaction.
Counterparty Country Code	The country code of the beneficiary party of the transaction.
Counterparty Identifier	The identifier of the beneficiary party of the transaction.
Credited Branch	The credited branch of the transaction.
Debited Branch	The debited branch of the transaction.
Destination Country	The destination country of the transaction.
Involved Party 1 Country Code	The country code of the first intermediary party of the transaction.
Involved Party 1 Identifier	The identifier of the first intermediary party of the transaction.
Involved Party 1 AccountID/ IBAN	The IBAN of the first intermediary party of the transaction.
Involved Party 1 BIC	The BIC of the first intermediary party of the transaction.
Involved Party 1 Name	The name of the first intermediary party of the transaction.
Involved Party 1 Type	The type of the first intermediary party of the transaction.
Involved Party 2 Country Code	The country code of the secondary intermediary party of the transaction.
Involved Party 2 Identifier	The identifier of the secondary intermediary party of the transaction.
Involved Party 2 AccountID/ IBAN	The IBAN of the secondary intermediary party of the transaction.
Involved Party 2 BIC	The BIC of the secondary intermediary party of the transaction.
Involved Party 2 Name	The name of the secondary intermediary party of the transaction.

Request Attributes	Description
Involved Party 2 Type	The type of the secondary intermediary party of the transaction.
Involved Party 3 Country Code	The country code of the tertiary intermediary party of the transaction.
Involved Party 3 Identifier	The identifier of the tertiary intermediary party of the transaction.
Involved Party 3 AccountID/ IBAN	The IBAN of the tertiary intermediary party of the transaction.
Involved Party 3 BIC	The BIC of the tertiary intermediary party of the transaction.
Involved Party 3 Name	The name of the tertiary intermediary party of the transaction.
Involved Party 3 Type	The type of the tertiary intermediary party of the transaction.
Message Direction	The direction of the message.
Message Reference	The reference number of the message.
Message Type	The type of the message.
Originator Party AccountID/ IBAN	The IBAN of the originating party of the transaction.
Originator Party BIC	The BIC of the originating party of the transaction.
Originator Party Countrycode	The country code of the originating party of the transaction.
Originator Party Identifier	Originator Party Identifier
Originator Party Name	The name of the originating party of the transaction.
Payment Information	The instructions associated with the payment.
Payment International Flag	Flag indicating that the transaction has crossed international borders.
Payment Type	The type of the payment
Payment Value Date	The date value of the payment
Receiver	The receiver of the message from the SWIFT network.
Referrer Site	The unique URL associated with the customer.
Sender	The sender of the message to the SWIFT network.
Source Country	The source country of the transaction.
Credit/Debit Code	The credit or debit code of the transaction.
Current Date	The current date.
Transaction Amount	The amount of the transaction.
Transaction Currency	The currency of the transaction.
Transaction Date End	The date the transaction was completed.
Transaction Date Start	The date the transaction was initiated.
Transaction Original Amount	The original amount of the transaction.

Request Attributes	Description
Transaction Original Currency	The original currency in which the transaction was conducted.
Transaction Type Code	The type code of the transaction.
Execution Time	The time on Execution Date at which this transaction was conducted.
Cheque Bounce Date	The date on which the check bounced.
Clearing Date	The time on clearing date at which the monetary instrument associated with this transaction was cleared by the clearing institution and is applicable for monetary instruments and checks
Depositing Date	The depositing time, for monetary instruments and checks, the time on Depositing Date at which the monetary instrument associated with this transaction was deposited at the depositing institution.
Payment Amount Bounced	The card payment amount that has bounced.
Payment Instrument Number	The Payment Instrument number. For monetary instruments, the serial number of the monetary instrument associated with this transaction (for example, the check number on checks).
Payment Instrument Routing Code	The Payment Instrument routing code. For monetary instruments, the routing code from the MICR line of the monetary instrument associated with this transaction.
Receipt Or Payment Indicator	The payment ind of the receipt
Recent/Cycle Returns Count	The number of returned transaction that occurred in the last billing cycle.
Merchant Identifier	This column stores the merchant number.
Merchant Description	This column stores the merchant description.
Purchase Amount	This column stores the amount paid for SOP 03-3 related exposures in natural currency.
Transacting Card Number	This column stores the unique card account number.
Details of Charges	The details of the charges.
Transaction Automated Flag	Flag indicating that the transaction is an automated payment.
Transaction Phone Number	The phone number which was used to conduct the transaction.
Transaction Reversal Date	This column stores date of the transaction which is a reversal entry that made to cancel out a specific entry.
Card Block Code	The block code of the card.
Card Issue Date	The date on which the transacting card was issued.
Card Bin prefix	The bin prefix of the card number.
Card Last 4 Digits	The last 4 digits of the card number.
Card Number	The number of the card
Card activation Date	Date on which the card is activated for usage.

Request Attributes	Description
Card Renewal Date	Date on which the card was renewed.
Credit Utilization	This column stores the utilization percent/utilization percent of the account.
Encrypted Card Number	The encrypted card number associated the card.
Eop Average Balance	This stores end of period balance which includes accrued interest.
Fraud Indicator	Indicator with flags the account as fraudulent.
Last Delinquent Date	This column stores the date when the loan was last delinquent.
Name on Card	The customer name as it appears on the plastic card.
Over Limit Balance	The balance amount which exceeds the customer's credit limit.
Past Due Flag	Flag to indicate whether the exposure is past due or not.
Total Amount Overdue	This column stores total amount of the principal, interest and any fee/ charges payment outstanding, which is contractually due and has not been paid.
Cards Expiry Date	This column stores the expiry date of the primary card issued to the customer.
Account Currency Code	This will be the account currency of the transaction.
Available limit	The available limit is the limit available to customer to carry out purchase transaction.
Card holder Address 1	The address line 1 associated with the card holder.
Card holder Address 2	The address line 2 associated with the card holder.
Card holder Address 3	The address line 3 associated with the card holder.
Card holder City	The address city associated with the card holder.
Card holder Country	The address country associated with the card holder.
Card holder State	The address state associated with the card holder.
Card holder postal code	The address postal code associated with the card holder.
Card DOB	The ate of birth of the card holder.
Card holder Home Phone	The home phone number of the card holder
Home Phone change last date	The last date on which the card holder's home phone number was changed.
Card holder work phone	The work phone number of the card holder
Work Phone change last date	The last date on which the card holder's work phone number was changed.
Card holder mobile phone	The mobile phone number of the card holder
Mobile Phone change last date	The last date on which the card holder's mobile phone number was changed.
Card holder email ID	The email address of the card holder.

Request Attributes	Description
Card last address change date	The last date on which the card holder's address was changed.
Card last pin change date	The last date on which the card holder's PIN was changed.
Card last req date	The last date on which the card holder requested as new card.
Card last status change date	The last date on which the card's status was changed.
Card sequence number	The sequence number of the card.
Card status	The status of the card.
Number of cards on Account	The number of cards associated with the account.
Card credit limit change date	The last date the credit limit was changed on the account.
Card account open date	The date on which the account associated with the card was opened.
No of Card consecutive txn	The number of consecutive transactions on the card.
Customer Type	The type of the customer involved in the transaction.
Authentication Mode	The mode of the authentication for the transaction.
CAVV Result Code	The code of the CAVV authentication result.
AVV Result Code	The code of the AVV authentication result.
AEVV Result Code	The code of the AEVV authentication result.
CVR result	The code the of the CVR authentication result.
POS Terminal Capabilities	The card data input capabilities of the point of sale terminal.
POS Terminal Entry Capability	The card data input modes of the point of sale terminal.
POS Cardholder Authentication Capability	The type of authentication used for the POS transaction.
Identifier Issue Date	The date on which the customer's identifier was issued.
Identifier Issue Place	The jurisdiction that issued the customer's identifier.
Relationship Manager	The relationship manager associated with the account.
Cardholder Authentication Method	The authentication method used by the card holder.
Assignee	The assignee of the alert.
Action	The action taken on the alert.
Run Timestamp	The timestamp of the action.
Status	The status of the alert
Action Time	The action taken on the alert by the assignee.
Jurisdiction	The jurisdiction of the alert.
Business Domain	The business domain code of the alert.

Request Attributes	Description
ID Issuer/Assigner	ID Issuer/Assigner
Role	Ownership role that this customer plays with respect to this account. Role can be; 01 - Primary Account Holder, 02 - Secondary Account Holder
Card Age	Number of days since the transacting card was issued.
Authentication Result	The result of the authentication method used for the transactions.

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.

