Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud) Administration and Configuration Guide Release 8.1.2.5.0 June 2023 E98368-06



OFS Fraud Enterprise Edition (Real Time Fraud)

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

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

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

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

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

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

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

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

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

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

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

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

Document Control

Version Number	Revision date	Change Log
8.1.2.5.0	June 2023	 Added user roles to Mapping a User with a User Group section. Added Configuring Alert Archival section.
8.1.2.4.0	March 2023	Created the first version of Fraud Enterprise Edition (Real Time Fraud Component) Administration and Configuration Guide for 8.1.2.4.0 Release.
8.1.2.3.0	December 2022	Created the first version of Fraud Enterprise Edition (Real Time Fraud Component) Administration and Configuration Guide for 8.1.2.3.0 Release.
8.1.2.2.0	Created: September 2020	Created the 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 Al	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	
2.2	Post-Installation Configuration	
2.2	2.1 Configuring IPE for Real Time Wire Fraud	8
3 In	stalling OFS Card Fraud Enterprise Edition	24
3.1	Prerequisites	24
3.2	Post-Installation Configuration	24
3.2	2.1 Configuring IPE for Real Time Card Fraud	24
4 M	anaging User Administration and Security Configuration	41
4.1	About User Administration	41
4.2	User Provisioning Process Flow	41
4.3	Managing User Administration	42
4.3	3.1 Managing Identity and Authorization	
4.4	Adding Security Attributes	44
4.4	4.1 About Security Attributes	44
4.5	Mapping the Security Attributes	45
4.6	Enabling the Cron Job	47
4.7	Integrating with ECM	47
4.8	Configuring Alert Archival	48
4.8	8.1 Rolling Back Alert Archival	
5 Co	onfiguring Real Time Wire Fraud Scoring	50
5.1	Operating Real Time Wire Fraud Service	50
5.1	1.1 Real Time Wire Fraud Service Request	
5.1	1.2 Real Time Wire Fraud Service Response	53

5	5.2	Managing Real Time Wire Fraud Scenarios/Rules	. 53
	5.2.1	Modify Fraud Rules	. 54
6	Con	figuring Real Time Card Fraud Scoring	55
Ċ	5.1	Operating Real Time Card Fraud Service	55
	6.1.1	Real Time Card Fraud Service Request	. 55
Ċ	5.2	Managing Real Time Card Fraud Scenarios/Rules	. 58
	6.2.1	Modify Fraud Rules	. 58
7	Mar	naging Real Time Wire Administration	59
7	7.1	Accessing Real Time Wire Administration	. 59
7	7.2	Configuring Real Time Wire Administration	. 60
7	7.3	Configuring ECM User in Real Time Wire Administration	. 61
7	7.4	Configuring Alert Lock	. 62
7	7.5	Configuring Archival	. 62
8	Mar	naging Real Time Card Administration	63
8	3.1	Accessing Real Time Card Administration	. 63
8	3.2	Configuring Real Time Card Administration	. 64
8	3.3	Configuring ECM User in Real Time Card Administration	. 65
8	3.4	Configuring Alert Lock	. 66
8	3.5	Configuring Archival	. 66
9	Арр	endix-A: Mapping of RTF Wire JSON to ECM Columns	67
10	Арр	endix-B: Mapping of RTF Card JSON to ECM Columns	69
11	OFS	SAA Support Contact Details	71
12	Sen	d Us Your Comments	72

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 IPE for Real Time Wire Fraud
- Configuring IPE for Real Time Wire Fraud

2.2.1 Configuring IPE for Real Time Wire Fraud

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

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

2.2.1.1 Create the Source Entity Queue for RTF Wire

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

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

Table 4 shows a sample of JMS Queue configuration.

Name	Туре	JNDI Name	Sub Deployment	Targets
Cache Operation Message Destination Topic	Торіс	jms/ cacheOperationMessageDestinati on	RTISubdeploy	RTIServer
JMS Connection Factory	Connection Factory	jms/connectionFactory	Default Targeting	AdminServer
RTFWire Assessment Response Destination Topic	Торіс	jms/ RTFWireAssessmentResponseDes tination	RTISubdeploy	RTIServer
RTFWire Feedback Queue	Queue	jms/RTFWireFeedbackQueue	RTISubdeploy	RTIServer
RTFWire Hold JMS Queue	Queue	jms/ RTFWireTransactionActionQueue	RTISubdeploy	RTIServer
RTFWire Source Entity Queue	Queue	jms/RTFWireSourceEntityQueue	RTISubdeploy	RTIServer
Wire Transaction Source Entity Queue	Queue	jms/wireTrxnQueue	RTISubdeploy	RTIServer

Table 4: Sample JMS Queue configuration

2.2.1.2 Creating RTFWIRE.ear or RTFWIRE.war

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

- 1. Navigate to <FIC HOME>/RTFWireFraudIPEProcessing
- 2. Execute the following command:

./ant.sh.

Figure 1: Creating RTFWIRE.ear/ RTFWIRE.war

```
/scratch/ofsaaweb/BD812/BD812/RTFWireFraudIPEProcessing>./ant.sh
executing "merge"
Not TOMCAT
executing "ant"
Buildfile: /scratch/ofsaaweb/BD812/BD812/RTFWireFraudIPEProcessing/build.xml
copyrti:
createwar:
    [war] Building war: /scratch/ofsaaweb/BD812/BD812/RTFWireFraudIPEProcessing/RTFWIRE.war
createear:
    [ear] Building ear: /scratch/ofsaaweb/BD812/BD812/RTFWireFraudIPEProcessing/RTFWIRE.ear
BUILD SUCCESSFUL
Total time: 2 seconds
/scratch/ofsaaweb/BD812/RTFWireFraudIPEProcessing>
```

3. On successful execution, the RTFWIRE.ear and RTFWIRE.war files are generated under the <<FIC HOME>/RTFWireFraudIPEProcessing/ folder.

2.2.1.3 Configuring the JMS properties

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

1. 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. Refer to Appendix: B in OFS Inline Processing Engine Configuration Guide.
- b. Replace the **#**#JMS_PORT## with bootstrap port in WireTransactionsPost.jsp in the below path.

Path: \$FIC HOME/RTFWireFraudIPEProcessing/WebContent

2. Recreate and deploy the BD war.

2.2.1.4 Deploying RTFWIRE.ear



For more 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 RTFWIRE.ear.

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

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

2.2.1.4.1 Deploying RTFWIRE.ear in WebLogic

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

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

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

- 1. Start the WebLogic server.
- 2. Create an .ear folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/ <DOMAIN NAME>/applications.

- 4. Explode the RTFWIRE.ear file by executing the command:

jar -xvf RTFWIRE.ear

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

jar -xvf RTFWIRE.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>.

2.2.1.4.2 Installing RTFWIRE.ear in WebLogic using WebLogic Administrator Console

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

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

- 1. 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.



ORACLE WebLogic Server Ad	iministra	ation Console	14.1.1									9
Change Center		Home Log O	ut Prefere	nces 📐 Reco	ord Help		Q				Welcome, wel	Connected to: RTFE
View changes and restarts	Ho	ome >Summar	y of Deplo	ments								
Configuration editing is enabled. Future	Sum	nmary of Dep	oloyments									
modify, add or delete items in this domain.	Configuration Control Monitoring											
Domain Structure This page displays the list of Java EE applications and standalone application modules installed to this domain. B*:Environment You can update (redeploy) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the "services B*:Services To install a new application or module for deployment to targets in this domain, click Install. B*:Deployments Customize this table Deployments Customize this table						then using the co	ntrols on this page.					
		Install Upda	ate Dele	te							Showing	1 to 3 of 3 Previous Next
		🗆 Name 🚕						State	Health	Туре	Targets	Deployment Order
	C		8124					Active	🛩 ок	Enterprise Application	AdminServer	100
low do I 🗉	C		CARD					Active	🖋 ОК	Enterprise Application	AdminServer	100
Install an enterprise application Configure an enterprise application	C		WIRE					Active	🖋 ок	Enterprise Application	AdminServer	100
Update (redeploy) an enterprise application Monitor the modules of an enterprise application		Install Upda	ate Dele	te							Showing	1 to 3 of 3 Previous Nex
Deploy EJB modules Install a Web application	-											

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

Figure 3: Install Application Assistance Window

G Gmail 🕨 YouTube 🧿 OFS Behavio	or Detec 📙 Jira,Support,OIM	Pa <mark>-</mark> PaySlip, Caler	ndar 📙 Meeting ID's	Other bookmarks			
DRACLE WebLogic Server Adr	ninistration Console 14.1.1			Q [^]			
Change Center	A Home Log Out Preferences	Record Help	Q	Welcome, weblogic Connected to: RTF8124			
/iew changes and restarts	Home >Summary of Deployment	ts					
Configuration editing is enabled. Future	Install Application Assistant						
changes will automatically be activated as you nodify, add or delete items in this domain.	Back Next Finish Car	ncel					
Domain Structure	Locate deployment to insta	I and prepare for deploy	ment				
TF8124 ⊕-Environment ⊷-Deployments ⊕-Services ⊷-Servirk Realms	Select the file path that represe the application directory or file Note: Only valid file paths are	nts the application root dire in the Path field. displayed below. If you cann	ectory, archive file, exploded archive dire	ectory, or application module descriptor that you want to install. You can also enter the path of your file(s) and/or confirm that your application contains the required deployment descriptors.			
Interoperability	Path: //scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projects/domains/RTF8124/applications/RTFWIRE.ear						
t)-Diagnostics	Recently Used Paths:	/scratch/ofsaaweb/Orac	cle/Middleware/Oracle_Home/user_proje	iects/domains/RTF8124/applications			
	Current Location:	100.76.156.11 / scratch	n / ofsaaweb / Oracle / Middleware / Ora	racle_Home / user_projects / domains / RTF8124 / applications			
	Image: Control of the second secon	directory) directory) directory)					
łow do I 🗉	Back Next Finish Car	ncel					
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							

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

ORACLE' WebLogic Server Ad	ministration Console 14.1.1	Q ^
Change Center	🟦 Home Log Out Preferences 🔛 Record Help	Welcome, weblogic Connected to: RTF8124
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	Choose installation type	
tTF8124	Select if the deployment should be installed as an application or library. 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 Install this deployment as a library Back Next. Finish Cancel	e on all of the targets running their referencing applications.
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		

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

I text Test Optional Settings Two modely these settings or accept the defaults. I hadrates requested fades. Optional Settings Security What do you want to name this deployment? * Name: RTFWIRE Security What course only these settings or accept the defaults. Optional do you want to use with this application? I to Donly: Use only roles and policies that are defined in the deployment descriptors. I to Donly: Use only roles and policies that are defined in the defauinistration Console; use policies that are defined in the deployment descriptors. I to Donly: Use only roles and policies that are defined in the definistration Console; use policies that are defined in the deployment descriptors. I to the defaults defined by the deployment's target are defined in the deployment descriptor. I to Donly: Use only roles and policies that are defined in the deployment descriptor. I to the defaults defined by the deployment's target are defined in the deployment descriptor. I to Donly: Use only roles and policies that are defined in the deployment descriptor. I to the defaults defined by the deployment's target are defined in the deploy	Install Application Assist	tant
<pre>labe: tree: t</pre>	in a land land	lane a
Option Settings You can madify these settings or accest the defaults. * Indicates required fields. - General What de you want to ame the adeployment? * Name: RTFWIRE Socialy What de you want to use with this application? © DO Driv: to eonly roles and policies that are defined in the deployment descriptors. © Do Driv: to eonly roles and policies that are defined in the Administration Console. O Advanced: Use a cust model that you have configured on the realm's configuration page. > Socialy Work added for the deployment's targets > Socialy > Socialy > Custom Roles: Use a cust bild efford by the deployment's configuration page. > Socialy > Sociality > Social	Back Next Finish	Cancel
Two can modify these settings or accept the defaults. * Indicates required fields: Can modify these settings or accept the defaults. What do you want to name this deployment? * Name: RTFWIRE Security What sourchy model do you want to use with this application? O D Only: Use only roles and policies that are defined in the deployment descriptors. Outor Roles: Use roles that are defined in the defined in the deployment descriptors. Outor Roles: Use roles that are defined in the Administration Console: use policies that are defined in the deployment descriptor. Outor Roles: Use roles that are defined in the Administration Console: Outor Roles: Use roles that are defined in the deployment descriptors. Outor Roles: Use roles and policies that are defined in the deployment descriptor. Outor Roles: Use roles that outor Roles: and policies that are defined in the Administration Console. Outor Roles: Use roles and policies: Use only roles and policies that are defined in the deployment Console. Outor Roles: Use roles that you have configured on the realm's configuration page. Source Accessibility How should the source files be made accessible? Outor Roles: With application onto every target for me Durity description: Outor Roles: With role autoposition was and generation with the application is targeted. Outor Roles: Will make the deployment accessible policy files. This is often a shared directory. You must ensure the application files exist in this location and that each target will accessible? Pan Source Accessibility	Optional Settings	
Indicate regured helds General	You can modify these se	tings or accept the defaults.
General What do you want to name this deployment? What to you want to name this deployment? Name: RTFWIRE Security What security model do you want to use with this application? O Do My: Use only roles and policies that are defined in the deployment descriptors. Custom Roles: Use roles that are defined in the deployment descriptors. Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the Administration Console. Custom Roles: Use roles that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles that you have configured on the realm's configuration page. Custom Roles that source files be made accessible? Custom Roles that source files be made accessible? Custom Roles that source files be made accessible from the following location Lucation: Surce Accessibility How should the lans ource files the application 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 as the application 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 Sourc	 Indicates required fields 	
what do you want to name this deployment? * Name: RTFWIRE - Scurity What scurity model do you wont to use with this application? © DD Ohly: Use only roles and policies that are defined in the deployment descriptors. Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the Administration Console. Advanced: Use a custom wolel that you have configured on the realm's configuration page. - Source Accessibility How should the source files be made accessible? Ourse Accessibility Captom have a customed by the deployment's targets Recommended selection. Captom have be copied automatically to the Managed Servers to which the application is targeted. If your have be copied automatically to the Managed Servers to which the application is targeted. If your have be copied automatically to the Managed Servers to which the application is targeted. If your have be copied automatically to the Managed Servers to which the application is targeted. If your have be copied automatications (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 If we should dive application 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.	— General —	
* Name: RTEWIRE Security What security model do you want to use with this application? @ Do Dray: Use only roles and policies that are defined in the deployment descriptors. Outcom Roles: Use roles that are defined in the deployment descriptors. @ Castom Roles: Use roles that are defined in the deployment descriptors. Outcom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor. @ Castom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Outcom Roles and Policies: Use only roles and policies that are defined in the Administration Console. @ Castom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Outcom Roles and Policies: Use configuration page. > Source Accessibility Outcom Role as costom model that you have configuration page. > Source Accessibility Outcom Role as costom Role a	What do you want to nam	e this deployment?
Security What security model do you want to use with this application? Description Descri	* Name:	RTFWIRE
Security Se	E 11	
What security mode aby you want to use wint this application? Do Dry: Use only roles and policies that are defined in the deployment descriptors. 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; Source Accessibility How should the source files be made accessible? Outing deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. Porvide 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 as the application 	- Security	
DD Only: Use only roles and policies that are defined in the deployment descriptors. 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. Advanced: Use a custom model that you have configured on the realm's configuration page. Source Accessibility How should the source files be made accessible? Use the defaults defined by the deployment's targets Recommended selection. Cory this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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 as the 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.	what security model do y	ou want to use with this 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. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles: Use a custom model that you have configured on the realm's configuration page. Custom Roles: Use a custom model that you have configured on the realm's configuration page. Custom Roles: Use a custom model that you have configured on the realm's configuration page. Custom Roles: Use a custom role that deployment's targets Custom Roles: Use defaults defined by the deployment's targets Custom Roles: Use the defaults defined by the deployment's targets Custom Roles: Use a custom role every target for me Custom Roles: Use only automatically to the Managed Servers to which the application is targeted. Custom [stratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec] 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. Custom Recommended selection: Custom Role: Subject Selection: Custom Role: Subject Selection: Custom Role: Subject Role: Subject Selection: Custom Role: Subject Role: Subject Selection: Custom Role: Subject	OD Only: Use only r	oles and policies that are defined in the deployment descriptors.
Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console. Custom Roles and Policies: Use a custom model that you have configured on the realm's configuration page. Custom Roles and Policies: Use a custom model that you have configured on the realm's configuration page. Custom Roles and Policies: Use a custom model that you have configured on the realm's configuration page. Custom Roles and Policies: Use a custom model that you have configured on the realm's configuration page. Custom Roles and Policies: Use a custom Role accessibility Custom Roles and Education of the sequences and a consult of the policy of the sequence of the sequ	O Custom Roles: Use	roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
Advanced: Use a custom model that you have configured on the realm's configuration page. Source Accessibility How should the source files be made accessible? Use the defaults defined by the deployment's targets Recommended selection. Copy this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I viel make the deployment accessible from the following location Location: //scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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 Recommended selection. Come the power target source in the selection. //scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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 as the application Recommended selection.	Custom Roles and F	volicies: Use only roles and policies that are defined in the Administration Console.
Advanced: Use a custom model that you have configured on the realm's configuration page. Source Accessibility Source Sou	-	
Source Accessibility How should the source Accessibility How should the source Accessibility Use the defaults defined by the deployment's targets Recommended selection. Copy this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I will make the deployment accessible from the following location Location: //scratch/ofsa.aweb/Oracle/Middleware/Oracle_Home/user_projec 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 Recommended selection. Com this also note a users there the paper of the same accessible for the application Recommended selection.	Advanced: Use a cu	stom model that you have configured on the realm's configuration page.
How should the source files be made accessible? Use the defaults defined by the deployment's targets Recommended selection. Copy this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. To capty this application every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. To capty this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. To cation: To cation: 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? So Use the same accessibility as the application Recommended selection. Commended selection.	 Source Accessibility 	
Outse the defaults defined by the deployment's targets Recommended selection. Copy this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I will make the deployment accessible from the following location Location:	How should the source file	es be made accessible?
Recommended selection. Copy this application onto every target for me During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I will make the deployment accessible from the following location Location: /scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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? I will the plan source files be made accessible? It is the application files exist. Recommended selection. Commended selection.	O Use the defaults de	fined by the deployment's targets
Copy this application onto every target for me Uuring deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I will make the deployment accessible from the following location Location: /scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec //orde 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? //or the application //or the appl	Recommended selection.	
During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted. I will make the deployment accessible from the following location Location: /scratch/ofsa.aweb/Oracle/Middleware/Oracle_Home/user_projec 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? Very the same accessibility as the application Recommended selection. Coment the same accessibility	Copy this applicatio	in onto every target for me
Output deployment, the field will be copied automatcally to the Hanaged Servers to which the application is targeted. I will make the deployment accessible from the following location Location: /scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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? I Use the same accessibility as the application Recommended selection. — Coment the selection.		
I will make the deployment accessible from the following location Location: /_scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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? O Use the same accessibility as the application Recommended selection. Come the same accessibility	During deployment, the h	es will be copied automatically to the Managed Servers to Which the application is targeted.
Location: /scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec 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? I out the same accessibility as the application Recommended selection.	I will make the dep	loyment accessible from the following location
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? Superior accessibility as the application Recommended selection. Computed is also explane anone target for anone	Location:	/scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projec
Plan Source Accessibility How should the plan source files be made accessible? Source files be made accessibility as the application Recommended selection. Commended selection.	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.
How should the plan source files be made accessible?	— Plan Source Accessib	ility
Use the same accessibility as the application Recommended selection. Compute plane approximation approximat	How should the plan sour	ce files be made accessible?
Recommended selection.	Use the same acces	sibility as the application
	Recommended selection.	
	Copy this plan onto	every target for me

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

🔒 Home Log Out Prefe	rrences 🔤 Record Help	Welcome, weblogic Connected to: RTF8124				
Home >Summary of Dep	loyments					
Install Application Assis	tant					
Back Next Finish	Cancel					
Review your choices	and click Finish					
Click Finish to complete	the deployment. This may take a few moments to complete.					
— Additional Configura	tion					
In order to work success	ully, this application may require additional configuration. Do you want to review this application's configuration after complet	ing this assistant?				
○ Yes, take me to the	e deployment's configuration screen.					
No, I will review the second secon	e configuration later.					
— Summary —						
Deployment:	/scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projects/domains/RTF8124/applications/RTFWIRE.ear					
Name:	RTFWIRE					
Staging Mode:	g Mode: I will make the deployment accessible at /scratch/ofsaaweb/Oracle/Middleware/Oracle_Home/user_projects/domains/RTF8124/applications/RTFWIRE.ear					
Plan Staging Mode:	in Staging Mode: Use the same accessibility as the application					
Security Model:	ecurity Model: DDOnly: Use only roles and policies that are defined in the deployment descriptors.					
Target Summary						
Components 🗞	onents A					
RTFWIRE.ear	WIREear AdminServer					
Back Next Finish Cancel						

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

Figure 7: Summary of Deployment page with RTFWIRE

10 million (10 mil						
Home_Log Out_Preferences 🛃 Record Help	Q				We	elcome, weblogic Connected to: RTF
me >Summary of Deployments						
ages						
All changes have been activated. No restarts are necessar	<i>l.</i>					
The deployment has been successfully installed.						
imary of Deployments						
nfiguration Control Monitoring						
ou can update (redeploy) or delete installed applications an	d modules from the domain by selecting the checkbox ne	ext to the application name an	d then using th	e controls on this page.		
ou can update (redeploy) or delete installed applications an o install a new application or module for deployment to targ customize this table eployments Install Update Delete	d modules from the domain by selecting the checkbox ne ets in this domain, click Install .	ext to the application name an	d then using th	e controls on this page.		Showing 1 to 3 of 3 Previous Nex
u can update (redeploy) or delete installed applications an install a new application or module for deployment to targ ustomize this table ployments Istall Update Delete	d modules from the domain by selecting the checkbox ne	ext to the application name an state state	Health	e controls on this page.	Targets	Showing 1 to 3 of 3 Previous Nex Deployment Order
u can update (redeploy) or delete installed applications an install a new application or module for deployment to targ ustomize this table ployments Istall Update Delete Name A T RTF8124	d modules from the domain by selecting the checkbox ne	ext to the application name an state Active	Health	e controls on this page. Type Enterprise Application	Targets AdminServer	Showing 1 to 3 of 3 Previous Nex Deployment Order 100
pu can update (redeploy) or delete installed applications an p install a new application or module for deployment to targ ustomize this table sployments nstall Update Delete Name D CRTF6124 D CRTFCARD	d modules from the domain by selecting the checkbox ne	ext to the application name an State Active Active	Health V OK V OK	controls on this page. Type Enterprise Application Enterprise Application	Targets AdminServer AdminServer	Showing 1 to 3 of 3 Previous Nex Deployment Order 100 100
You can update (redeploy) or delete installed applications an To install a new application or module for deployment to targ Sustomize this table eployments Install Update Delete Name B RTFR124 B RTFCARD B RTFWIRE	d modules from the domain by selecting the checkbox ne	ext to the application name an State Active Active Active Active	Health Control of the second s	e controls on this page. Type Enterprise Application Enterprise Application Enterprise Application	Targets AdminServer AdminServer AdminServer	Showing 1 to 3 of 3 Previous Nex Deployment Order 100 100 100

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

2.2.1.4.3 Deploying RTFWIRE.ear in WebSphere

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

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

To deploy **RTFWIRE**.ear in WebSphere, follow these steps:

./startServer.sh server1

- 2. Create an RTFWIRE.ear folder in <WEBSPHERE_INSTALL_DIR>/RTFWIRE.ear.
- 3. Copy <FIC_HOME>/RTFWireFraudIPEProcessing/RTFWIRE.ear to <WEBSPHERE_INSTALL_DIR>/RTFWIRE.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	re
	Mich Cash and Intermeted
	VvebSphere 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

Interprise Applications	
Preparing for the application installation	2
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 11: Browse Remote Filesystems Window

We	elcome admin	Help	Logout	IBM.
ise Applications				Close page
se Remote Filesystems				
lect the radio button next to the archive that you wish to install, or click on a directory name to view its contents.				
ontents of /scratch/IBM/WebSphere/AppServer/profiles/BECS8124WS/installedApps/ofss-mum-889-Node3-Cell08/RTFWI	RE.ear			
parentDir				
RTFWIRE.ear				
OK Cancel				
lect the radio button next to the archive that you wish to install, or click on a directory name to view its contents. ontents of /scratch/IBM/WebSphere/AppServer/profiles/BECS8124WS/installedApps/ofss-mum-889-Node3-Cell08/RTFWII parentDir D RTFWIRE.ear OK Cancel	RE.ear			

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

Figure 12: Preparing for the application installation

	Welcome admin	Help Logout IBM ,
Enterprise Applications		Close page
Preparing for the application installation	2 =	Help
Specify the EAR, WAR, JAR, or SAR module to upload and install. Path to the new application Cocal file system Full path Choose File No file chosen Remote file system Full path /scratch/IBM/WebSphere/AppServer/profiles/BECS8124WS/ins Browse		Field help Remote file system path Page help More information about this page
Next Cancel		

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

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

Figure 15: Map Modules to Servers

Install New Application			7 .	
Specify options for installing enterprise applications and modules.				
Step 1 Select	Map modules to servers			
→ Step 2: Map modules to servers	Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispensed among several application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-dg.xm) for each Web server is generated, based on the applications that are routed through.			
Step 3 Map virtual hosts for Web modules	Clusters and servers: WebSphere.cell=ofss-mum-889-Node3-Cell08,node=ofss-mum-889-Node3,server=server1 🔶 Apply			
<u>Step 4</u> Summary				
	Select Module	URI	Server	
	Inline Processing	RTFWIRE.war,WEB-INF/web.xml	WebSphere:cell=ofss-mum-889-Node3-Cell08,node=ofss-mum-889-Node3,server=server1	
Previous Next Cancel				

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

Install New Application		2
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	Specify the virtual host for the Web modules that are contained in your application. You can i Apply Multiple Mappings	stall Web modules on the same virtual host or disperse them among several hosts.
→ Step 3: Map virtual hosts for Web	0 0	
modules <u>Step 4</u> Summary	Select Web module Inline Processing	Virtual host default_host
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

<u>Step 1</u> Select installation options	Summary	
Step 2 Map modules	Summary of installation options	
to servers	Options	Values
Sten 3 Man virtual	Precompile JavaServer Pages files	No
hosts for Web modules	Directory to install application	
Ston A: Summary	Distribute application	Yes
Step 4. Summary	Use Binary Configuration	No
	Deploy enterprise beans	No
	Application name	RTFWIRE
	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/wam/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 dient 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

Insta	llin	a

Installing
If 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.
ADMA5016I: Installation of RTFWIRE started.
ADMA5067I: Resource validation for application RTFWIRE completed successfully.
ADMA5058I: Application and module versions are validated with versions of deployment targets.
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
ADMA5081I: The bootstrap address for client module is configured in the WebSphere Application Server repository.
ADMA5053I: The library references for the installed optional package are created.
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
ADMA50011: The application binaries are saved in /scratch/IBM/WebSphere/AppServer/profiles/BECS8124WS/wstemp/92668751/workspace/cells/ofss-mum-889-Node3-Cell08/ap
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
SECJ04001: Successfully updated the application RTFWIRE with the appContextIDForSecurity information.
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
ADMA5005I: The application RTFWIRE is configured in the WebSphere Application Server repository.
ADMA5113I: Activation plan created successfully.
ADMA50111: The cleanup of the temp directory for application RTFWIRE is complete.
ADMA5013I: Application RTFWIRE installed successfully.
Application RTFWIRE installed successfully.
To 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.
To work with installed applications, click the "Manage Applications" link.
Manage 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

Enterprise	Applications		
Enter	prise Applications		
Use th	is page to manage installed applications. A single application can be deployed onto multiple	e servers.	
± Pre	ferences		
Sta	rt Stop Install Uninstall Update Rollout Update Remove File Export	Export DDL Export File Liberty Advisor 🔻	
D			
Select	Name 🗘	Application Status 🙅	Liberty Advisor Summary 👲
You c	an administer the following resources:		
	BECS8124WS	◆	\oslash
	CommonGatewayService	⊕	\oslash
	DefaultApplication	•	\oslash
	FEDTFLT	*	\oslash
	GenerateCaseInputService	•	\oslash
	InitiateOnboardingService	♦	\oslash
	JSONToTablePersistenceUtility	♦	\oslash
	RAOR		\oslash
	RTFCARD		\oslash
	RTFWIRE	*	\oslash
	SEPATFLT	8	\oslash
	SMLiteWeb	\$	\oslash
	TFLT	*	\oslash
	TabletoJSONService	•	\oslash
	ivtApp		\oslash
	guery	•	\oslash
Total	16		

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

Figure 20: Enterprise Application page with Confirmation message

nterprise Applications						
 Messages Application RTFWIRE on server server1 and node ofss-mum-889-Node3 started successfully. The collection may need to be refreshed to show the current status. 						
Enterprise Applications						
Use this page installed applications. A single application can be deployed onto multiple servers.						
Preferences						
Start Stop Install Uninstall Update Rollout Update Remove File Export Expo	rt DDL Export File Liberty Advisor 🔻					
C C # \$						
Select Name 🗘	Application Status 👲	Liberty Advisor Summary 👲				
You can administer the following resources:						
BECS8124WS	⇒	0				
CommonGatewayService	⇒	0				
DefaultApplication	*	0				
EDTFLT	8	0				
GenerateCaseInputService	÷	0				
InitiateOnboardingService	•	0				
JSONToTablePersistenceUtility	•	0				
RAOR	÷	0				
RTFCARD	•	0				
RTFWIRE	÷	0				
SEPATFLT	*	0				
SMLiteWeb	*	0				
	8	0				
TabletoJSONService	*	0				
	•	0				
	à	0				
Total 16						

19. Update the key realtime: name=StatsManager to realtime: name=StatsManagerWIRE in the following file.

Path: <Deployed Area>/<RTFWIRE.ear>/ <RTFWIRE.war>/conf/
applicationContext-jmx.xml

20. Restart all OFS AAAI servers.

2.2.1.5 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/RTFWireFraudIPEProcessing/IPEAssessmentImport/ OFS_RTWIREFRAUD_RTIExport_Fraud.xml <INFODOM> OFS_FRAUD_EE true

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
- Enabling Feedback Message

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 5 shows a sample of JMS Queue configuration.

Name	Туре	JNDI Name	Sub Deployment	Targets
Cache Operation Message Destination Topic	Торіс	jms/ cacheOperationMessageDestinati on	RTISubdeploy	RTIServer
JMS Connection Factory	Connection Factory	jms/connectionFactory	Default Targeting	AdminServer
RTFCARD Assessment Response Destination Topic	Торіс	jms/ RTFCardAssessmentResponseDes tination	RTISubdeploy	RTIServer
RTFCARD Feedback Queue	Queue	jms/RTFCardFeedbackQueue	RTISubdeploy	RTIServer
RTFCARD Hold JMS Queue	Queue	jms/ RTFCardTransactionActionQueue	RTISubdeploy	RTIServer
RTFCARD Source Entity Queue	Queue	jms/RTFCardSourceEntityQueue	RTISubdeploy	RTIServer
Wire Transaction Source Entity Queue	Queue	jms/wireTrxnQueue	RTISubdeploy	RTIServer

Table 5: 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 RTFIPE_CONFIG.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. Refer to Appendix: B in OFS Inline Processing Engine Configuration Guide.
- 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 more 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.
- 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

OFS Behavior Detection Installatic ×	Oracle BD Application Pack Docu × O FCCM_RTF_Administration_and_C × S	ummary of	Deployme	nts - BDR 🗙 🕂		\sim	_	٥	\times
$\leftarrow \rightarrow \mathbf{C}$ A Not secure http:/	// 100.76.156.11 :5680/console/console.portal?_nfpb=true&_pageLabel=AppDeploy					☆	*		
🌀 Gmail 📭 YouTube 🧧 OFS Behavio	or Detec 📕 Jira,Support,OIM,Pa 📕 PaySlip, Calendar 📕 Meeting ID's						. 🗖	Other boo	okmarks
ORACLE WebLogic Server Adr	ninistration Console 14.1.1								õ
Change Center	🔒 Home Log Out Preferences 🔤 Record Help			We	lcome, weblogi	Conne	ected to:	BDRTF_	8124
View changes and restarts	Home >Summary of Deployments								_
Configuration editing is enabled. Future	Summary of Deployments								
changes will automatically be activated as you modify, add or delete items in this domain.	Configuration Control Monitoring								
Domain scructure Domain scructure Be-Environment - Sectorments - Secontry Realms - Secontry Realms - Secontry Realms - Diagnostics	in Structure This page displays the list of Java EE applications and standalone application modules installed to this domain. 'splay You can update (redeplay) or delete installed applications and standalone application modules installed to this domain. You can update (redeplay) 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 page. To install a new application or module for deployment to targets in this domain, click Install. Customize this table Deployments Install Update Delete Name State Health Type Targets Deployment Order						e. ous Ne	×t	
	□	Active	🛩 ок	Enterprise Application	AdminServer	100			11
How do I Install an enterprise application Configure an enterprise application Update (redeploy) an enterprise application Monitor the modules of an enterprise application	Instati Update Delete			1	Showing 1	to 1 of	1 Previ	ous Nex	đ
Deploy EJB modules Install a Web application	- o o - o - o - o - o - o - o - o - o -		-	×1 ⋛ 33°C	~ 🖼	۲	») 4 :	05 PM	

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

Figure 22: Install Application Assistance Window



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 A	Select if the deployment should be installed as an application or library.
Deployments Deployments Deployments Deployments Defloyments Defloymen	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 Revel Next Company Company
Persistent StoresForeign 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

ORACLE WebLogic Server Adm	inistration Console 14	.1.1	õ		
Change Center	🔒 Home Log Out	Preferences 🖉 Record Help	Icome, weblogic Connected to: BD812UT		
View changes and restarts	CLE: WebLogic Server Administration Console 14.1.1 enter inges and restarts ion edition is enabled. Future attained as youd or delete terms in this domain. tructure intert innerts ssaging iNS Servers Stores S "Ores, take me to the deployment's configuration screen. "Witcher "Ores, take me to the deployment's configuration later. "Stores"				
Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Back Next	Assistant inish Cancel			
Domain Structure	Review your cho	ices 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 su	ccessfully, this application may require additional configuration. Do you want to review this application's configuration after completing the	nis 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.			
Persistent Stores	Deployment:	$/scratch/fccmapp/Oracle/Middleware/Oracle_Home/user_projects/domains/BD812UT/applications/RTFCARD.ear/interval and interval and inter$			
Work Contexts	Name:	RTFCARD			
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	Plan Staging Mode:	Use the same accessibility as the application			
Create a deployment plan					
Target an enterprise application to a server instance Tart the server instance	Security Model: Target Summary	UDUNIY: Use only roles and policies that are defined in the deployment descriptors.			

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*.



ORACLE WebLogic Server A	dministration Console 14.1.1					ç
Change Center	🏫 Home Log Out Preferences 🔤 Record Help				Welcome, webl	ogic Connected to: BDRTF_8
View changes and restarts Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.	Home >Summary of Deployments >RTFCARD >Roles >Summary of Deployments >RTFCARD >Summary of Deployments Messages # All changes have been activated. No restarts are necessary. # The deployment has been successfully installed.					
Domain Structure	Summary of Deployments					
BORTF_B124 ⊕ Environment ⊕ Services ⊕	Configuration Control Monitoring This page displays the list of Java EE applications and standalone application modules installed to this domain. You can update (redeplay) or delete installed applications and modules from the domain by selecting the checkber. To install a new application or module for deployment to targets in this domain, click Install. Customize this table Deployments Deployments	ix next to the	application na	ime and then using the controls	on this page.	
How do I	Install Update Delete				Showin	ng 1 to 2 of 2 Previous Next
How do I	Name 🗞	State	Health	Туре	Targets	Deployment Order
Install an enterprise application Configure an enterprise application	BDRTF_8124	Active	🛩 ок	Enterprise Application	AdminServer	100
Update (redeploy) an enterprise application Monitor the modules of an enterprise		Active	🛩 ок	Enterprise Application	AdminServer	100
application Deploy EJB modules Install a Web application	Install Update Delete			·	Showin	ng 1 to 2 of 2 Previous Next
System Status Health of Running Servers as of 10:43 AM				wa 崎		

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 RTFCARD to upload and install.

Figure 31: Preparing for the application installation

paring for the application installation	
Specify the EAR, WAR, JAR, or SAR module to upload and install.	
Path to the new application	
O Local file system	
Full path	
Choose File No file chosen	
Remote file system	
Eull nath	
/scratch/IBM/WebSphere/profiles/BD812/RTFCARD.ear Browse	
Next Concel	
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

F

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	Netribute annination		
	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		
	Process embedded configuration 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 form 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 V		
	Validate schema		
Next Cancel			

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



Step 1 Select	Map modu	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 in the modules that are contained in your application. Modules can be installed on the same applicat server or dispersed among several application servers. Also, specify the Web servers as targets the 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			Installation 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.		
	Select	Module	URI RTFCARD.war,WEB-	Server WebSphere:cell=ofss-mum-889-Node3-	
		Processing	INF/web.xml	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.

Insta	istall 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	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 ▼				
	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 applications and modules.					
Step 1 Select	t Summary				
	Summary of installation options				
<u>Step 2</u> Map modules to servers	Options	Values			
Stop 2 Map virtual	Precompile JavaServer Pages files	No			
hosts for Web modules	Directory to install application				
→ Sten 4: Summary	Distribute application	Yes			
y Step H Summary	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		7 =				
Enterp	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							
Select	Name 🗘	Application Status 💁	Liberty Advisor Summary 💁				
You ca	an administer the following resources:						
	BD812UP3WS	\$	0				
	DefaultApplication	\$	0				
	RTFCARD	*	0				
	ivtApp	•	0				
	<u>query</u>	•	0				
Total	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.

nterprise	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.										
nter	rise Applicati	ons									
e th	s page to mana	ige in	stalled applie	cations. A	single applicati	on can be deployed	onto mul	tiple servers.			
🗄 Pre	erences										
Sta	t Stop In	stall	Uninstall	Update	Rollout Upda	e Remove File	Export	Export DDL	Export File	Liberty Advisor 🔹	
Ø											
Select	Name 🗘					Application Status	٥			Liberty Advisor Sum	mary 🗳
You c	an administer t	he foll	lowing resou	rces:							
	BD812UP3WS					€				0	
	DefaultApplic	ation				€)				0	
	RTFCARD					•				0	
	<u>ivtApp</u>					•				0	
	<u>query</u>					•				0	
Total	5										

Figure 39: Enterprise Application page with the Confirmation message

19. Update the key realtime: name=StatsManager to realtime: name=StatsManagerCARD in the following file.

Path: <Deployed Area>/<RTFCARD.ear>/ <RTFCARD.war>/conf/
applicationContext-jmx.xml

20. 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

3.2.1.6 Enabling Feedback Message

If the Card IPE rules are imported, don't re run the IPE import and follow below steps to enable the Feedback message posting for Card Transactions.

- 1. Login with **Card Admin** user.
- 2. Navigate to Inline Processing Engine page.
- 3. Go to assessments Tab, Select Card Fraud Assessment.
- Select Send Card IPE Response Clean and update Score Lower Limit and Score Upper Limit to 0.

- 5. Select Send Card IPE Response Hold and update Score Lower Limit to 10.
- 6. Save Assessment outcome.

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
- Mapping the Security Attributes
- Enabling the Cron Job
- Integrating with ECM

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

Table 6:	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.
Mapping the Security Attributes	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 7 lists the various actions and associated descriptions of the user administration process flow.

Table 7:	Administration	Process	Flow
14010 /1	/		

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 8 describes the predefined Fraud User Roles and corresponding User Groups.

Role	Privileges	User Group
Wire Admin	Perform Batch Access	Wire 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 Admin	Perform Batch Access	Card 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.	
Wire Fraud Analyst	Access Fraud applications and take action on transactions.	Wire Analyst
Card Fraud Analyst	Access Fraud applications and take action on transactions.	Card Analyst

Table 8: Fraud Roles and User Groups

Role	Privileges	User Group
Wire Senior Supervisor	View and act on alerts that fall under their function, business domain or jurisdiction.	WIRESRSUPER VISORGRP
	The following actions are allowed:	
	View alert	
	Assign or reassign alert	
	Set alert decision	
	Search alert	
	View attachment	
	Add attachment	
	Bulk decision on an alert list.	
Card SeniorView and act on alerts that fall under their function, businessSupervisordomain or jurisdiction.		CARDSRSUPER VISORGRP
	The following actions are allowed:	
	View alert	
	Assign or reassign alert	
	Set alert decision	
	Search alert	
	View attachment	
	Add attachment	
	Bulk decision on an alert list.	
Wire Auditor	View the alerts that fall under their function, business domain or jurisdiction.	WIREFRAUDAU DITORGRP
Card Auditor	View the alerts that fall under their function, business domain or jurisdiction.	CARDFRAUDA UDITORGRP

Table 8: 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 Mapping the Security Attributes

This section allows you to map the security attributes that include Business Domains, Jurisdictions, and Asignee groups to User Groups for Real Time Fraud.

To map Business Domain, 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 in FCC_FR_GROUP_SEC_ATTR_MAP to map the Business Domain to the Groups.

```
INSERT INTO FCC_FR_GROUP_SEC_ATTR_MAP (
```

```
V_GROUP_CD,
V_SEC_ATTR_CD,
```

```
V_SEC_ATTR_VAL
)
VALUES (
    'CARDFRAUDADMINGRP',
    'BUSDMN',
    'a'
)
```

To map Jurisdictions, follow these steps:

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

```
INSERT INTO KDD_JRSDCN (
    JRSDCN_CD,
    JRSDCN_DSPLY_NM,
    JRSDCN_DESC_TX
)
VALUES
(
    'E',
    'East',
    'EAST',
    'EASTERN'
)
```

2. Add entries in FCC_FR_GROUP_SEC_ATTR_MAP to map the Jurisdiction to the Groups.

```
INSERT INTO FCC_FR_GROUP_SEC_ATTR_MAP (
    V_GROUP_CD,
    V_SEC_ATTR_CD,
    V_SEC_ATTR_VAL
)
VALUES (
    'CARDFRAUDADMINGRP',
    'JRSDCN',
    'E'
)
```

4.6 Enabling the Cron Job

Execute the following script in Atomic schema to enable user defined rules Cron Job.

• Update FCC_FR_ADMIN_CONF SET V_PARAM_VALUE='Y' where V_PARAM_NAME ='ENABLE_USER_RULES_EXECUTION'

4.7 Integrating with ECM

Real Time Fraud is integrated with Enterprise Case Management (ECM) to perform the following tasks.

- Create and Investigate the cases
- Close the cases

To know which Real Time Fraud JSON columns are moved to ECM, See Appendix-C: Mapping of RTF JSON to ECM Columns.

NOTE

Message Reference, Customer Internal Id, Account Number are mandatory for ECM integration in the Card Fraud JSON. See Appendix-B: Card Fraud Sample JSON for a sample.

To integrate Real Time Fraud with Enterprise Case Management (ECM), follow these steps:

1. Execute the following command in the Atomic database.

```
UPDATE FCC_FR_ADMIN_CONF
SET V_PARAM_VALUE = 'true'
WHERE V_PARAM_NAME = 'IS_L2_ANALYSIS_REQUIRED'
```

- 2. Go to \$FIC_HOME/RealTimeFraudCommonScripts and execute ECM_L1_ACTION_STATUS.sql in Atomic db.
- 3. For PMF update execute the following in Config Schema:

Wire: \$FIC_HOME/RealTimeFraudCommonScripts/RTF_Wire/ WIRE_PMF_WORKFLOW_L2_ANALYSIS.sql

Card: \$FIC_HOME /RealTimeFraudCommonScripts/RTF_Card/ CARD_PMF_WORKFLOW_L2_ANALYSIS.sql

4. Execute the following in Atomic schema.

Wire: \$FIC_HOME/RealTimeFraudCommonScripts/RTF_Wire/WIRE_TRXN_CASEID.sql

Card: \$FIC_HOME /RealTimeFraudCommonScripts/RTF_Card/CARD_TRXN_CASEID.sql

5. In the Real Time Card Administration tab, add the ECM URL (http://host:port/ContextName), ECM user name and password and click **Save**.

Figur	Figure 42: Oracle Financial Services Enterprise Fraud Page						
🛕 Not secure whf00qk	çin.orade.com :7780/8D8123/RealTimeFr	aud/RTFCardAdmin.jsp					
ORACLE' Fina	ancial Services Enterprise Fraud						
	Configuration Enable	SLA(minutes) 5					Save
	Rule ID	Rule Name	Priority	Actions	Edit	Enable	
			No data to disp	lay.			
			Page 1 (0 of 0 items) K	 C 1 (Σ ≤ X) 			
	O Create New Rule						
	ECM User Configuration						
	ECM URL http://whf00qkj.in.oracle.c	Username	supervisor	Password			Save

- 6. To integrate ECM for security attributes, mapping, and case assignment, see Adding Security Attributes and Configuring Case Allocation sections in Oracle Financial Services Enterprise Case Management Administration and Configuration Guide.
- 7. Restart the Oracle Financial Services Analytical Applications (OFSAA) servers to refresh the changes.

4.8 Configuring Alert Archival

Users can archive the alerts based on conditions as required.

To configure the archiving of the alerts, follow these steps:

1. Navigate to \$FIC_HOME/RealTimeFraudCommonScripts/ArchivalScripts.

NOTE Replace the ##SCHEMA NAME## with the actual schema name before executing the following in Atomic Database.

- 2. Update the condition for the archival as required and execute FCC_ARC_METADATA.sql in the Atomic Database.
- 3. Execute FCC ARC CHILD METADATA.sql in the Atomic Database.
- 4. Execute the following script in the Atomic Database.

```
set serveroutput on size 100000;
begin
FOR i IN (SELECT * FROM FCC_ARC_METADATA WHERE V_APP_ID='RTF')
LOOP
PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.p_fcc_archival_proc('RTF','##SCHEMA_NA
ME##',i.V_TABLE_NAME);
END LOOP;
end ;
/
```

5. To enable the Alert Archival, refer to Configuring Archival for Wire and Configuring Archival for Card.

4.8.1 Rolling Back Alert Archival

User can roll back archival process even after configuring it.

To roll back Alert Archival, follow these steps:

- 1. Navigate to the **Real Time Wire Administration** page.
- 2. Under Archival Configuration, turn OFF the Enable button.
- 3. Click Save.
- 4. Similarly, turn OFF the **Archival Configuration** for Card using the **Real Time Card Administration** page and **Save** the changes.
- 5. Replace ##SCHEMA_NAME## and execute the following command in the Atomic Schema.

```
set serveroutput on size 100000;
begin
FOR i IN (SELECT * FROM FCC_ARC_METADATA WHERE V_APP_ID='RTF')
LOOP
PKG_FCC_ARCHIVAL_COMPRESS_UTILITY.P_FCC_ROLL_BACK_ARCHIVE_PROC('RTF','##
SCHEMA_NAME##',i.V_TABLE_NAME, 'Y');
END LOOP;
end ;
/
```

This action rolls back the Archival Process.

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 Card Fraud service by posting relevant attributes into the IPE REST Service using either of the following:

• JSP:

<host>:<port>/RTFWIRE/WireTransactions.jsp

- IPE JMS Client:
 - a. 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.
 - b. Copy \$FIC_HOME/RTFWireFraudIPEProcessing/IPEJMSTestClient/lib/ RTFJMSClientTest.jar file to \$FIC_HOME/realtime_processing/ipesampleapp/ client/lib path.
 - c. Take a copy of IPEJMSClient.sh and rename it as IPEFraudJMSClient.sh. Modify the IPEFraudJMSClient.sh file as follows.
 - Update MAIN_JAVA_CLASS=com.ofs.aai.realtime.test.JmsGatewayTest to

MAIN JAVA CLASS=com.ofss.fccm.fraud.realtime.wire.test.JmsGatewayTest

— Update \$JAVA_BIN/java \$X_ARGS_GEN -classpath \$_CLASSPATH \$MAIN_JAVA_CLASS \$1 \$2 \$3 \$4 \$5 to \$JAVA_BIN/java \$X_ARGS_GEN classpath \$ CLASSPATH \$MAIN JAVA CLASS \$1 \$2 \$3 \$4 \$5 \$6

Additional parameter is the number of threads to run parallel.

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

Table 9 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.

Table 9: Real Time Wire Fraud Message Attributes

Table 9: Real Time Wire Fraud Message Attributes

Message Attributes	Description
applD	Indicates the application ID for Real Time Wire Fraud.

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

5.1.1.1 Real Time Wire Fraud Service JMS Response Details

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

Table 10 shows the Real Time Wire 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.	{ "Transaction ID" : 2781, "Message Reference" : Message Reference, "Status" : CLEAN }
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 10: Real Time Wire 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" : "" } { Transaction ID" : 2788, "Message Reference" : </pre>
			Message Reference, "Status" : HOLD
Alert Created	Release	This response is created on the hold queue if the posted transaction is released from the UI or auto-closed by Wire Administrator SLA settings.	<pre>{ "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : CLEAN, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Released }</pre>

Alert Blocked This response is created { Created on the hold queue if the "Transaction ID":	JMS Response	Alert Action	Alert Description	Response
2789, blocked from the UI or auto-closed by Wire Administrator SLA settings. "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Blocked	Alert Created	Blocked	This response is created on the hold queue if the posted transaction is blocked from the UI or auto-closed by Wire Administrator SLA settings.	<pre>{ "Transaction ID" : 2789, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Blocked }</pre>

Table 10: Real Time Wire Fraud Service JMS Response Details

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 <RTFWIRE.war Deployed Path>/RTFWIRE/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 11 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.

Table 11: Fraud Risk Rules

Wire Fraud Scenarios/Rules	Description
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 11: 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:

• JSP:

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

- IPE JMS Client:
 - a. 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.
 - b. Copy \$FIC_HOME/RTFCardFraudIPEProcessing/IPEJMSTestClient/lib/ RTFJMSClientTest.jar file to \$FIC_HOME/realtime_processing/ipesampleapp/ client/lib path.
 - c. Take a copy of IPEJMSClient.sh and rename it as IPEFraudJMSClient.sh. Modify the IPEFraudJMSClient.sh file as follows.
 - Update MAIN JAVA CLASS=com.ofs.aai.realtime.test.JmsGatewayTest to

MAIN JAVA CLASS=com.ofss.fccm.fraud.realtime.card.test.JmsGatewayTest

— Update \$JAVA_BIN/java \$X_ARGS_GEN -classpath \$_CLASSPATH \$MAIN_JAVA_CLASS \$1 \$2 \$3 \$4 \$5 to \$JAVA_BIN/java \$X_ARGS_GEN classpath \$ CLASSPATH \$MAIN JAVA CLASS \$1 \$2 \$3 \$4 \$5 \$6

Additional parameter is the number of threads to run parallel.

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

Table 12 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.

Table 12: Real Time Card Fraud Message Attributes

Table 12: Real Time Card Fraud Message Attributes

Message Attributes	Description
appID	Indicates the application ID for Real Time Card Fraud.

See Appendix-E: Real Time Wire 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 13 shows the Real Time Card Fraud Service JMS Response Details.

Action	Alert Description	Response
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.	{ "Transaction ID" : 2781, "Message Reference" : Message Reference, "Status" : CLEAN }
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>
Err	or	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.

Table 13: 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" : "" } { "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : HOLD } </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>

Table 13: Real Time Card Fraud Service JMS Response Details

JMS Response	Alert Action	Alert Description	Response
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>{ "Transaction ID" : 2789, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Blocked }</pre>

Table 13: 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 14 shows the sample out-of-the-box fraud risk rules configured for real-time delectation.

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
Cash credit withdrawal suppression	Assign risk score if the user has made frequent cash withdrawals than usual.
Previous Card Transaction from different Country	Assign risk score if the user has made high card transactions from different locations in a short period of time.

Table 14: Fraud Risk Rules

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.

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:

7

- Accessing Real Time Wire Administration
- Configuring Real Time Wire Administration
- Configuring ECM User in 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.

ORACLE [®] Financial Services Analytical Appl	ications		■ <u>About</u>
3			
	Language	US-English	
	User ID		
	Password		
		Login	
	Version 8.0.6.0.0 Copyright © 1993, reserved.	, 2018 Oracle and/or its affiliates. All rights	

Figure 43: OFSAA Login Page

- 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 44: 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 45: Fraud Enterprise Edition Home Page

A Home	ORACLE [®] Financial Services Fraud Enterprise Edition	r.
Navigation List		
🛱 Real Time Wire Transactions		
觉 Real Time Wire Administration		
🛱 Real Time Card Administration		
🛱 Real Time Card Transactions		
Processing Modelling Framework		
🛱 Operations >		
🛱 Financial Services Inline Processing >		
💆 Data Model Management >		

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 15 shows the details regarding the create new rule section.

Table	15:	Create New Rule	
iubic		cicate iten itale	

Field	Description
Rule ID	Indicates the Rule ID.
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 16 shows the details regarding the create new condition section.

Table 16: 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.

This action configures the SLA for the Real Time Fraud.

7.3 Configuring ECM User in Real Time Wire Administration

On the **Real Time Wire Administration** page, you can configure Enterprise Case Management (ECM) user details to integrate ECM with Real Time Wire.

To configure ECM user, follow these steps.

1. Navigate to the **Real Time Wire Administration** page.

2. Under ECM User Configuration, enter the details as mentioned.

Table 17 shows the ECM user configuration details.

Table 17: ECM User Configuration Details

Field	Description
ECM URL	Enter the ECM URL as shown in the following format.
	host:port/contextName
Username	Enter your ECM username.
Password	Enter your ECM user password.

3. Click Save.

7.4 Configuring Alert Lock

Alert Locking helps in locking a particular alert a user is viewing, for a specific interval. The locked alert won't allow other users to take any actions against it. However a supervisor can assign the locked alert to any other user as required.

On the Real Time Wire Administration page, you can configure the Alert Locking Time Interval.

To Configure Lock Interval (minutes), follow these steps.

- 1. Navigate to the **Real Time Wire Administration** page.
- 2. Under Alert Lock Configuration, update the Lock Interval(minutes) as required.
- 3. Click Save.

7.5 Configuring Archival

Alert Archival helps the users in archiving alerts based on the required condition. For more information on Alert Archival, refer to Configuring Alert Archival.

To configure alert archival, follow these steps.

- 1. Navigate to the **Real Time Wire Administration** page.
- 2. Under Archival Configuration, turn on the Enable button.
- 3. Click Save.

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
- Configuring ECM User in Real Time Card Administration

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 Applic	ations	⊠ <u>About</u>
3		
	Language US-English	
	User ID	
	Password	
	Login Version 8.0.6.0.0 Copyright © 1993, 2018 Oracle and/or its affiliates. All rights reserved.	

Figure 46: 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 47: Fraud Enterprise Edition Applications Page

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

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

Figure 48: Fraud Enterprise Edition Home Page

🖀 Home		ORACLE' Financial Services Fraud Enterprise Edition	
Navigation List			
Real Time Wire Transactions			
🖉 Real Time Wire Administration			
🖉 Real Time Card Administration			
🖄 Real Time Card Transactions			
Processing Modelling Framework	>		
🖉 Operations	>		
Financial Services Inline Processing	. >		
觉 Data Model Management	>		

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 18 shows the details regarding the create new rule section.

Table 18: Create New Rule

Field	Description
Rule ID	Indicates the Rule ID.
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 19 shows the details regarding the create new condition section.

Table 19: 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.

This action configures the SLA for the Real Time Fraud.

8.3 Configuring ECM User in Real Time Card Administration

On the **Real Time Card Administration** page, you can configure Enterprise Case Management (ECM) user deatils to integrate ECM with Real Time Card.

To Configure ECM user, follow these steps.

1. Navigate to the **Real Time Card Administration** page.

2. Under ECM User Configuration, enter the details as mentioned.

Table 20 shows the ECM user configuration details.

Table 20: ECM User Configuration Details

Field	Description	
ECM URL	Enter the ECM URL as shown in the following format.	
	host:port/contextName	
Username	Enter your ECM username.	
Password	Enter your ECM user password.	

3. Click Save.

8.4 Configuring Alert Lock

Alert Locking helps in locking a particular alert a user is viewing, for a specific interval. The locked alert won't allow other users to take any actions against it. However a supervisor can assign the locked alert to any other user as required.

On the Real Time Card Administration page, you can configure the Alert Locking Time Interval.

To Configure Lock Interval (minutes), follow these steps.

- 1. Navigate to the **Real Time Card Administration** page.
- 2. Under Alert Lock Configuration, update the Lock Interval(minutes) as required.
- 3. Click Save.

8.5 Configuring Archival

Alert Archival helps the users in archiving alerts based on the required condition. For more information on Alert Archival, refer to Configuring Alert Archival.

To configure alert archival, follow these steps.

- 1. Navigate to the **Real Time Card Administration** page.
- 2. Under Archival Configuration, turn on the Enable button.
- 3. Click Save.

9 Appendix-A: Mapping of RTF Wire JSON to ECM Columns

This sections shows the Real Time Fraud (RTF) JSON columns that are used and mapped in the Enterprise Case Management (ECM) Environment.

Table 21 shows the RTF JSON and ECM Table column details.

Table 21: RTF Wire JSON and ECM Table Details

RTF Fraud JSON	ECM Table	ECM Column	Label
originatorPartyBIC	FCC_WIRE_TRXN_EVNT	SEND_INSTN_ID	Send FI ID
trxnOriginatorCurrenc y	FCC_WIRE_TRXN_EVNT	SEND_CRNCY_CD	with Base amount
originatorPartyAccoun tIdIBAN	FCC_WIRE_TRXN_EVNT	ORIG_ACCT_ID	Originating Account ID
trxnOriginatorAmount	FCC_WIRE_TRXN_EVNT	SEND_TRXN_ACTVY_AM	Send Amount
receiver	FCC_WIRE_TRXN_EVNT	RCV_INSTN_NM	Receiving FI Name
sender	FCC_WIRE_TRXN_EVNT	SEND_INSTN_NM	Send FI Name
trxnAmount	FCC_WIRE_TRXN_EVNT	TRXN_BASE_AM	Base Amount
trxnStartDate	FCC_WIRE_TRXN_EVNT	TRXN_EXCTN_DT	Date
counterPartyBIC	FCC_WIRE_TRXN_EVNT	RCV_INSTN_ID	Receiving FI ID
counterPartyName	FCC_WIRE_TRXN_EVNT	BENEF_NM	Beneficiary Name
counterPartyAccountl dIBAN	FCC_WIRE_TRXN_EVNT	BENEF_ACCT_ID	Beneficiary Account ID
originatorPartyName	FCC_WIRE_TRXN_EVNT	ORIG_NM	Originating Name
dataOrigin	FCC_WIRE_TRXN_EVNT	DATA_ORIGIN	Type/Source
trxnld	FCC_WIRE_TRXN_EVNT	TRXN_INTRL_REF_ID	Transaction Reference
addrPostalCode	FCC_ACCT_ADDR_EVNT	ADDR_POSTL_CD	Postal code
addrCityName	FCC_ACCT_ADDR_EVNT	ADDR_CITY_NM	City
addrStateCode	FCC_ACCT_ADDR_EVNT	ADDR_STATE_CD	State
addrCountryCode	FCC_ACCT_ADDR_EVNT	ADDR_CNTRY_CD	Country
addrStreetLine1	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE1_TX	Address Line 1
addrStreetLine2	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE2_TX	Address Line 2
addrStreetLine3	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE3_TX	Address Line 3
addrStreetLine4	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE4_TX	Address Line 4
addrStreetLine5	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE5_TX	Address Line 5
addrStreetLine6	FCC_ACCT_ADDR_EVNT	ADDR_STRT_LINE6_TX	Address Line 6
dataOrigin	FCC_ACCT_ADDR_EVNT	DATA_ORIGIN	Source

RTF Fraud JSON	ECM Table	ECM Column	Label
actld	FCC_ACCT_ADDR_EVNT	ACCT_INTRL_ID	Account ID
addrUsageCode	FCC_ACCT_ADDR_EVNT	ADDR_USAGE_CD	Description
custld	FCC_CUST_EVNT	CUST_INTRL_ID	Customer ID
custDOB	FCC_CUST_EVNT	BIRTH_DT	Date of Birth
custType	FCC_CUST_EVNT	CUST_TYPE_CD	Customer Type
jurisdiction	FCC_CUST_EVNT	JRSDCN_CD	Jurisdiction
businessDomain	FCC_CUST_EVNT	BUS_DMN_LIST_TX	Domain
actld	FCC_ACCT_EVNT	ACCT_INTRL_ID	Account ID
accName	FCC_ACCT_EVNT	ACCT_DSPLY_NM	Account Name
status	FCC_ACCT_EVNT	ACCT_STAT_CD	Status
dataOrigin	FCC_ACCT_EVNT	DATA_ORIGIN	Source
jurisdiction	FCC_ACCT_EVNT	JRSDCN_CD	Jurisdiction
businessDomain	FCC_ACCT_EVNT	BUS_DMN_LIST_TX	Domain

Table 21: RTF Wire JSON and ECM Table Details

10 Appendix-B: Mapping of RTF Card JSON to ECM Columns

This sections shows the Real Time Fraud (RTF) JSON columns that are used and mapped in the Enterprise Case Management (ECM) Environment.

Table 22 shows the RTF JSON and ECM Table column details.

RTF Fraud JSON	ECM Table	ECM Column	Label
Counterparty Name	FCC_CASH_TRXN	TRXN_LOC_NM	Name
Message Direction	FCC_CASH_TRXN	DBT_CDT_CD	Debit/Credit
Originator Party AccountID/IBAN	FCC_CASH_TRXN	CNDTR_ACCT_ID	Account
Originator Party Name	FCC_CASH_TRXN	CNDTR_NM	Name
Terminal ID	FCC_CASH_TRXN	TRXN_LOC_ID	ID
Terminal Merchant/Fl Original script Name	FCC_CASH_TRXN	TRXN_LOC_NM	Name
Transaction Amount	FCC_CASH_TRXN	TRXN_ACTVY_AM	Activity
Transaction Date Start	FCC_CASH_TRXN	TRXN_EXCTN_DT	Date
Account Status Code	FCC_ACCT	ACCT_STAT_CD	Status
Card status	FCC_ACCT	ACCT_STAT_CD	Status
Name on Card	FCC_ACCT	ACCT_DSPLY_NM	Account Name
Action	KDD_CASE_ACTIONS	ACTION_ID	Action:
Action Time	KDD_CASE_ACTIONS	ACTION_TS	Date and Time
Annual Income	KDD_CASE_CUSTOMERS	ANNL_INCM_BASE_AM	Estimated Annual Income
Assignee	KDD_CASES	ASSIGNED_TO_ID	Assignee
Status	KDD_CASES	STATUS_CD	Status
Account Added Date	FCC_CUST	CUST_ADD_DT	Added
Customer Address Line 1	FCC_CUST_ADDR	ADDR_STRT_LINE1_TX	Address
Customer Alias	FCC_CUST	ALIAS_NM	Alias
Customer Country Of Residence	FCC_CUST	RES_CNTRY_CD	Residence
Customer Credit Score	FCC_CUST	CUST_CDT_SCORE	Credit Score
Customer Date of Birth	FCC_CUST	BIRTH_DT	Date of Birth
Customer Phone Extension 1	FCC_CUST_PHON	PHON_EXT_NB	Extension

Table 22: RTF Card JSON and ECM Table Details

RTF Fraud JSON	ECM Table	ECM Column	Label
Customer Phone Number 1	FCC_CUST_PHON	PHON_NB	Phone
Employer Name	FCC_CUST	MPLYR_NM	Employer
Identifier Number	CUST_ID_DOC	CUST_INTRL_ID	Customer ID
Account Credit Limit Amount	FCC_LOAN	MAX_LOAN_LIMIT_BASE_ AM	Maximum Loan Limit
Account Number	FCC_LOAN	LOAN_INTRL_ID	ID
Account Open Date	FCC_LOAN	LOAN_ORIG_DT	Originating Date
Account Type	FCC_LOAN	LOAN_DESC_TX	Description

Table 22: RTF Card JSON and ECM Table Details

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.
