Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud)

Administration and Configuration Guide

Release 8.1.2.2.0

September 2023

E98368-01

ORACLE
Financial Services

OFS Fraud Enterprise Edition (Real Time Fraud)

Document Control

Table 1: Document Control

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

Table of Contents

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:

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	Italic 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>	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:

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.

2.2.1 Configuring install.properties File

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

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

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

sql.atomic.datasource.jndi.name=jdbc/<INFODOM_NAME>

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

system.infodom=<INFODOM_NAME>

system.domain=PFR

system.appid=OFS_FRAUD_EE

ipe.produce.hglights.results=true
```

2.2.2 Configuring IPE for Real Time Wire Fraud

You must install the RTFRAUD service to configure Inline Processing Engine (IPE) for Real Time Fraud.

To install the RTFRAUD service, follow these steps.

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

2.2.2.1 Creating RTFRAUD.ear or RTFRAUD.war

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

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

   Path: `<FIC_HOME>/ficapp/common/FICServer/bin/`

   Command : `./RTIImport.sh $FIC_HOME/RealTimeFraudIPEProcessing/IPEAssessmentImport/OFS_RTFRD_RTIExport_Fraud.xml <INFODOM> OFS_FRAUD_EE true`
3. Execute the following command:

   `./ant.sh`.

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

Figure 1: Creating RTFRAUD.ear/ RTFRAUD.war

```
/scratch/ofsaobie/AAAI_80/realtime_processing>ls
ant.sh  application.xml  build.xml  ILP.ear  ILP.war  ipesampleapp  WebContent
/scratch/ofsaobie/AAAI_80/realtime_processing>./ant.sh
executing "ant"
Buildfile: build.xml

createwar:

createear:

BUILD SUCCESSFUL
Total time: 0 seconds
/scratch/ofsaobie/AAAI_80/realtime_processing>
```

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

2.2.2.2 Deploying RTFRAUD.ear

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

2.2.2.2.1 Deploying RTFRAUD.ear in WebLogic

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

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

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

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

   ```
   jar -xvf RTFRAUD.ear
   ```

5. Delete the RTFRAUD.ear and RTFRAUD.war files.
6. Create an RTFRAUD.war folder in <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RTFRAUD.ear.
7. Copy <FIC_HOME>/RealTimeFraudIPEProcessing/RTFRAUD.war to <WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RTFRAUD.ear/RTFRAUD.war.
8. Explode the RTFRAUD.war file by executing the command:

   ```
   jar -xvf RTFRAUD.war
   ```

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

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

2.2.2.2.2 Installing RTFRAUD.ear in WebLogic using WebLogic Administrator Console

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

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

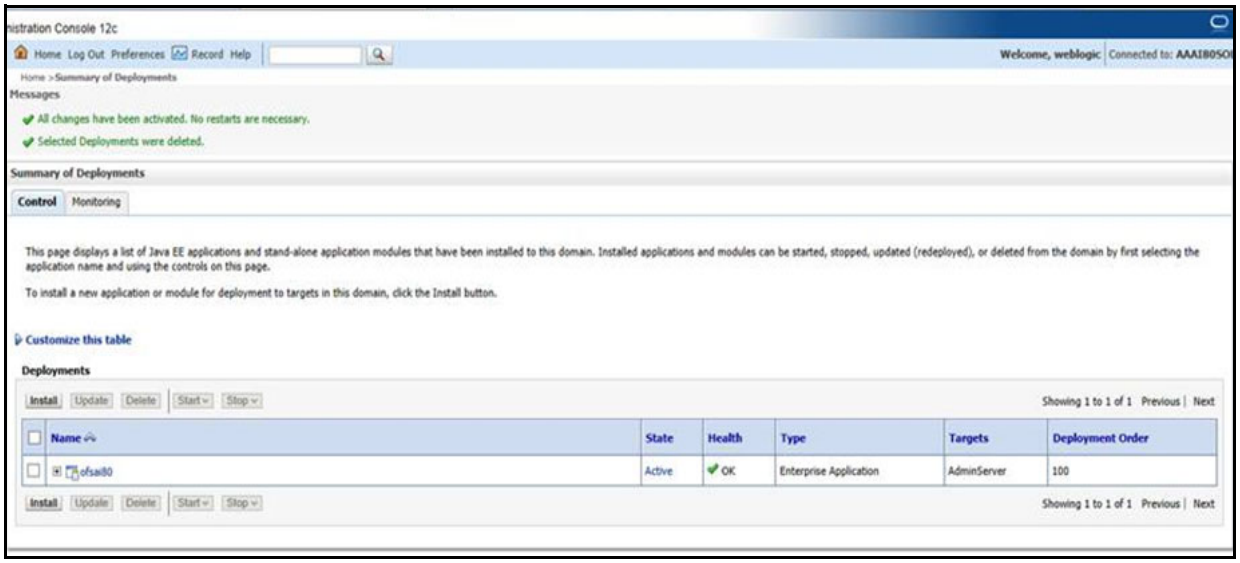
1. Navigate to the path <WebLogic Installation directory>/user_projects/domains/<domain name>/bin in the machine in which WebLogic is installed.
2. Start WebLogic by executing the following command:

   ```
   ./startWebLogic.sh -d64 file
   ```

3. Open the following URL in the browser window:

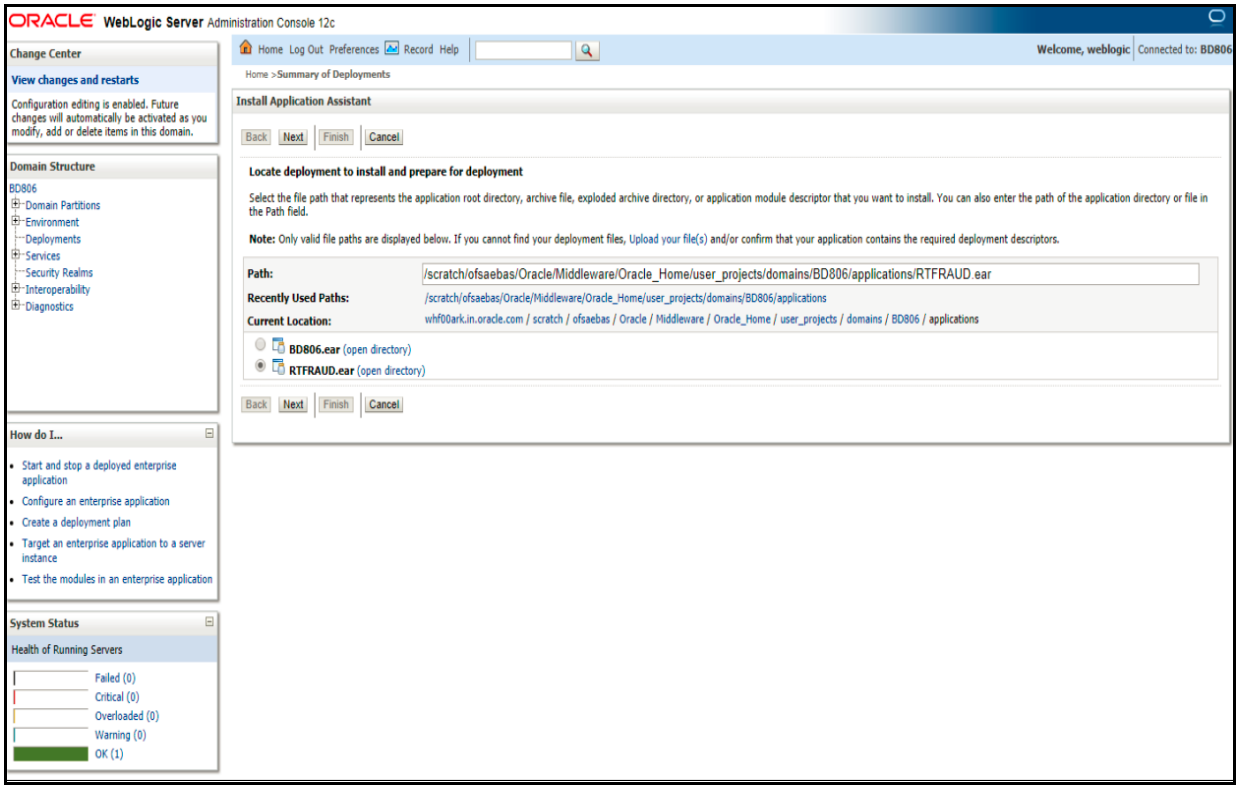
   http://<ipaddress>:<admin server port>/console (use https protocol if SSL is enabled). The Sign-in window of the WebLogic Server Administration Console is displayed.
4. Login with the Administrator **Username** and **Password**. The Summary of Deployment page is displayed.

Figure 2: Summary of Deployment



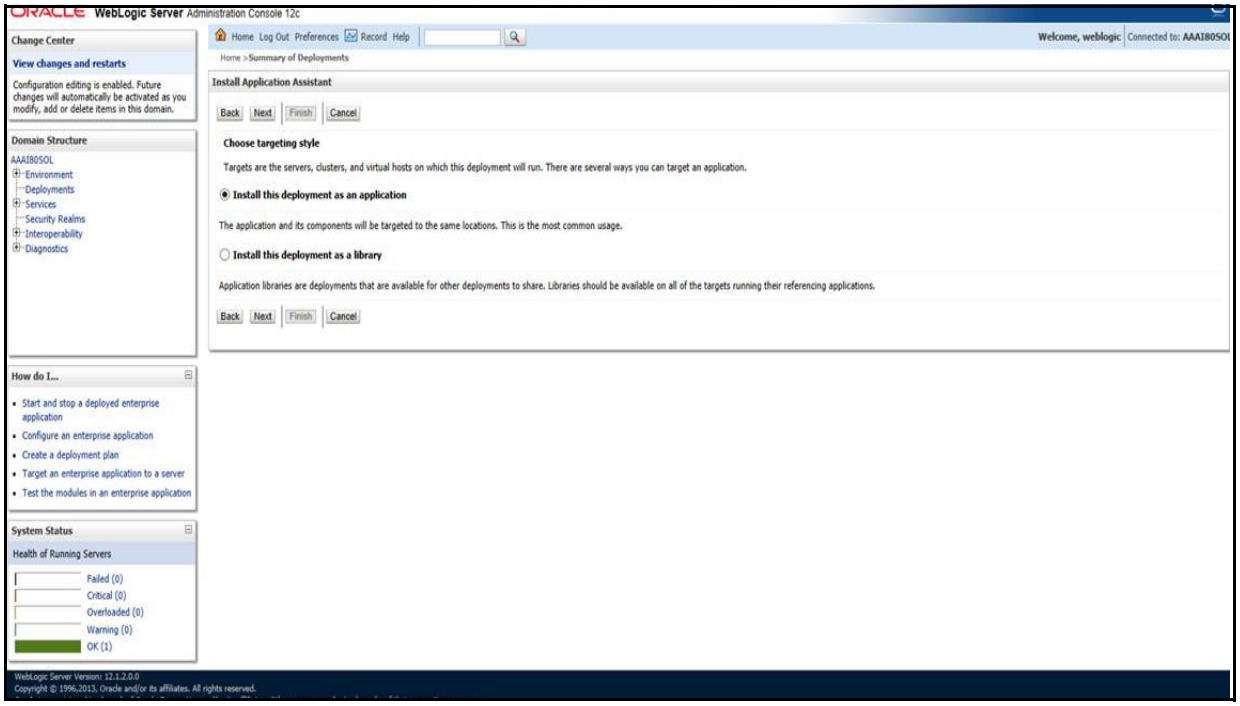
5. Click **Install**. The Install Application Assistance page is displayed.

Figure 3: Install Application Assistance Window



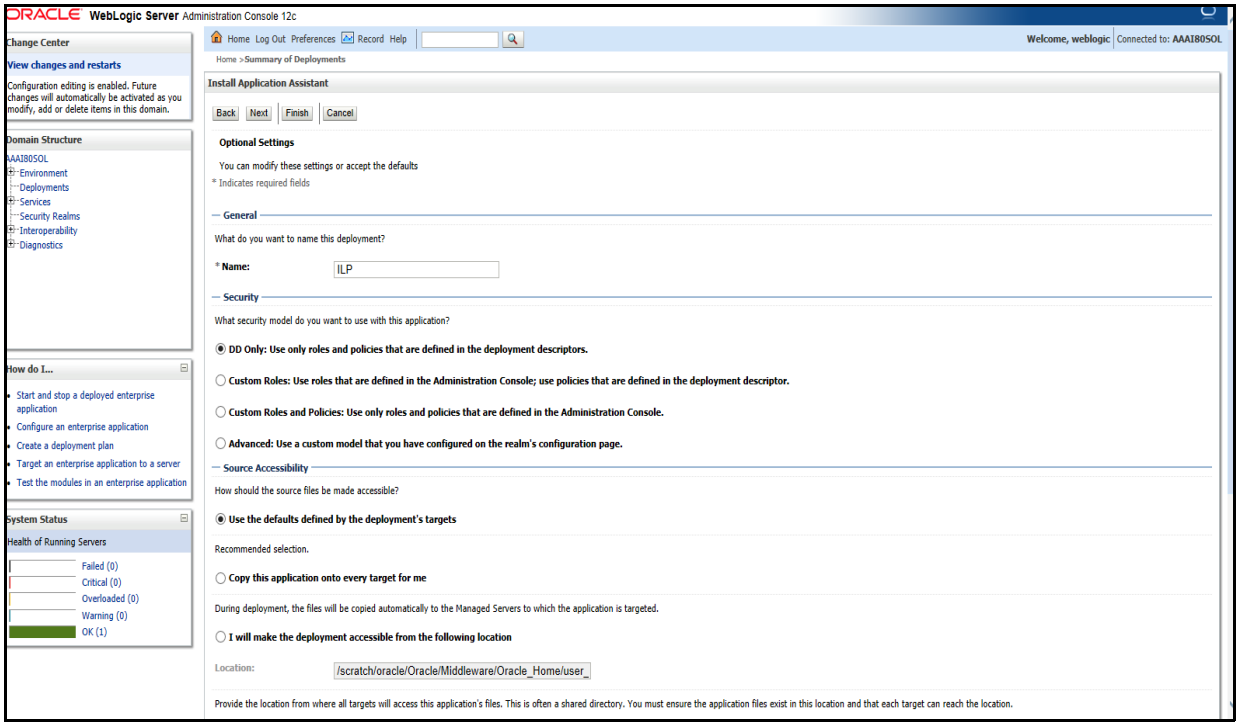
6. Select `RTFRAUD.ear` and click **Next**. This action displays the Install Application Assistance page with the Choose targeting style section.

Figure 4: Install Application Assistance with choose Target Style



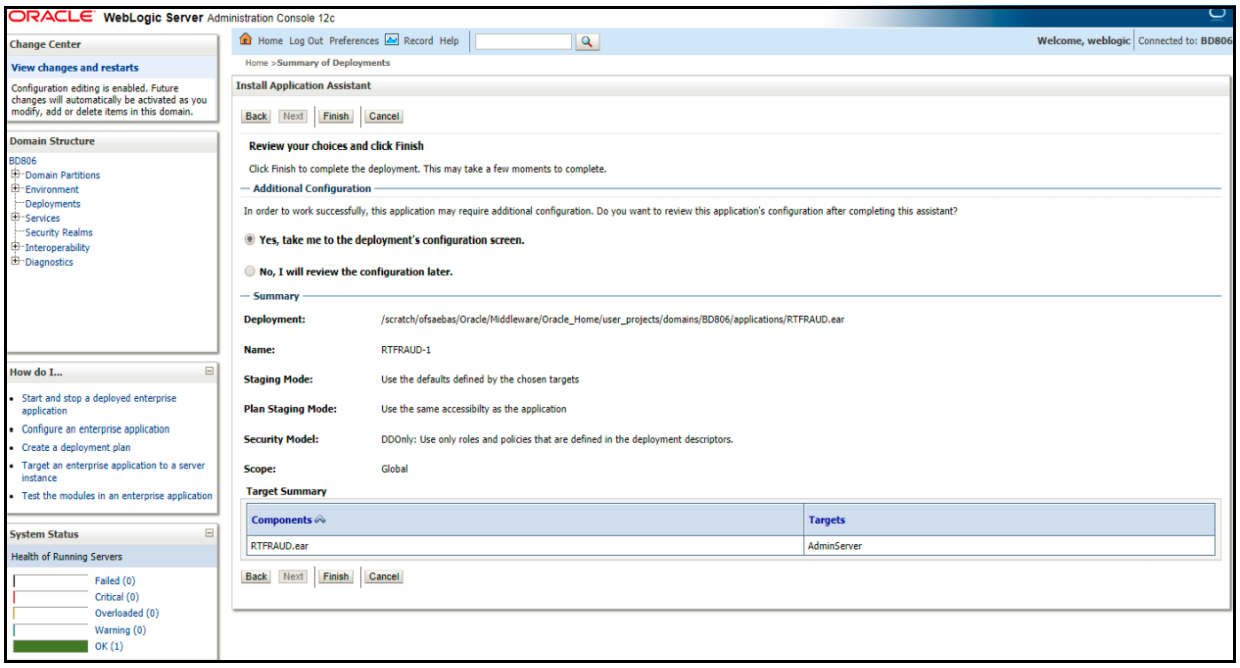
7. By default, the **Install this deployment as an application** option in the Choose targeting style section is selected. Click **Next**. This action displays the Install Application Assistance page in the Optional Settings section.

Figure 5: Install the Application Assistance page with Optional Settings



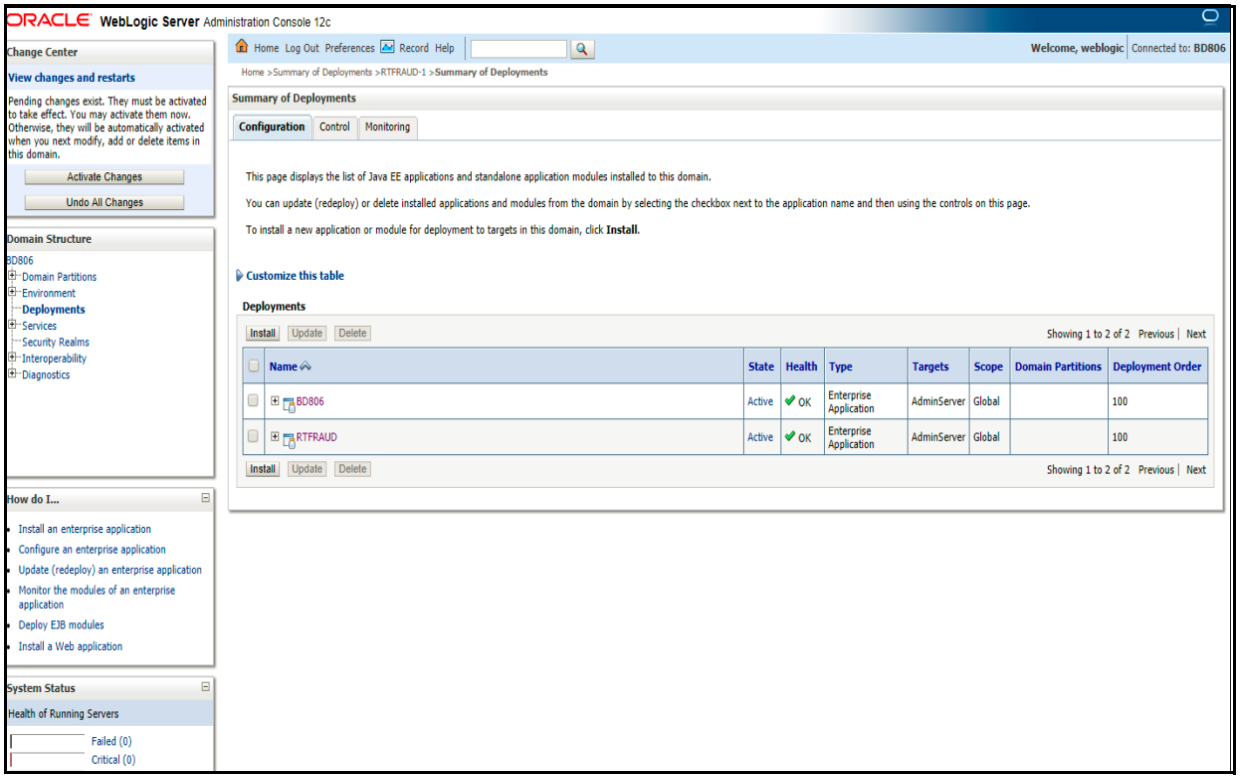
8. Retain the default selections and click **Next**. The Install Application Assistance page is displayed with the Review your choices and click Finish section.

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



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

Figure 7: Summary of Deployment page with RTFRAUD



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

2.2.2.2.3 Deploying RTFRAUD.ear in WebSphere

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

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

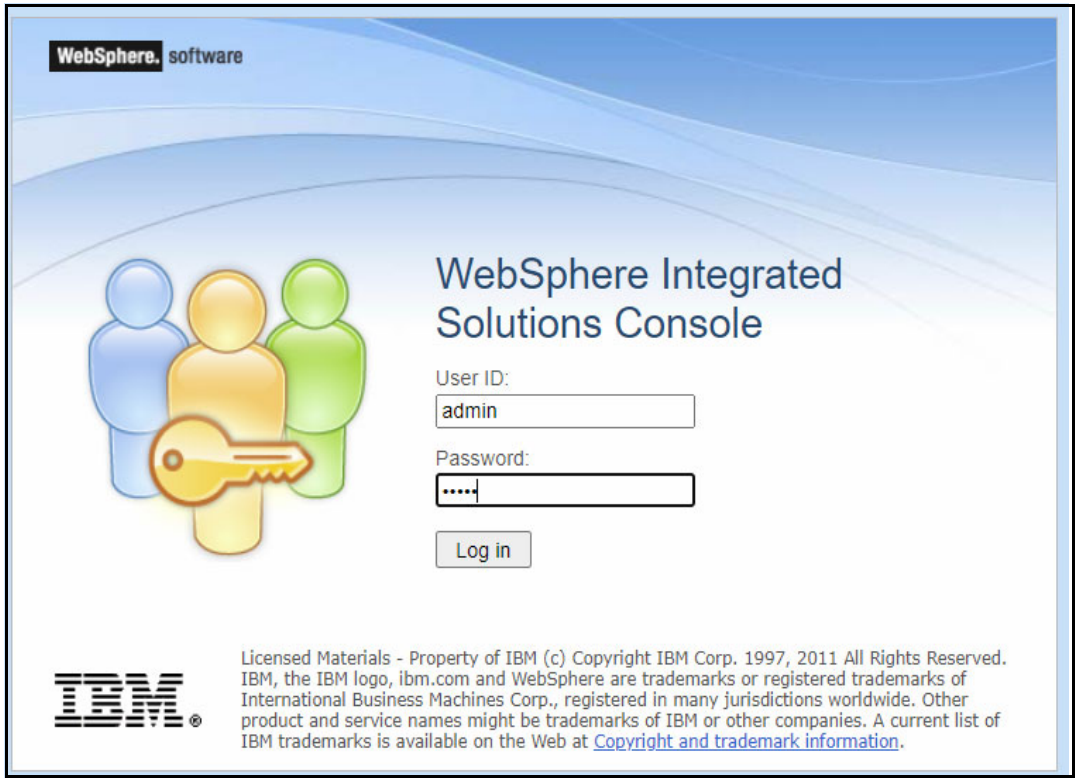
To deploy `RTFRAUD.ear` in WebSphere, follow these steps:

1. Start the WebSphere Profile by navigating to the path "`/<WebSphere_Installation_Directory>/IBM/WebSphere/AppServer/profiles/<Profile_Name>/bin/`" then execute the command:

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

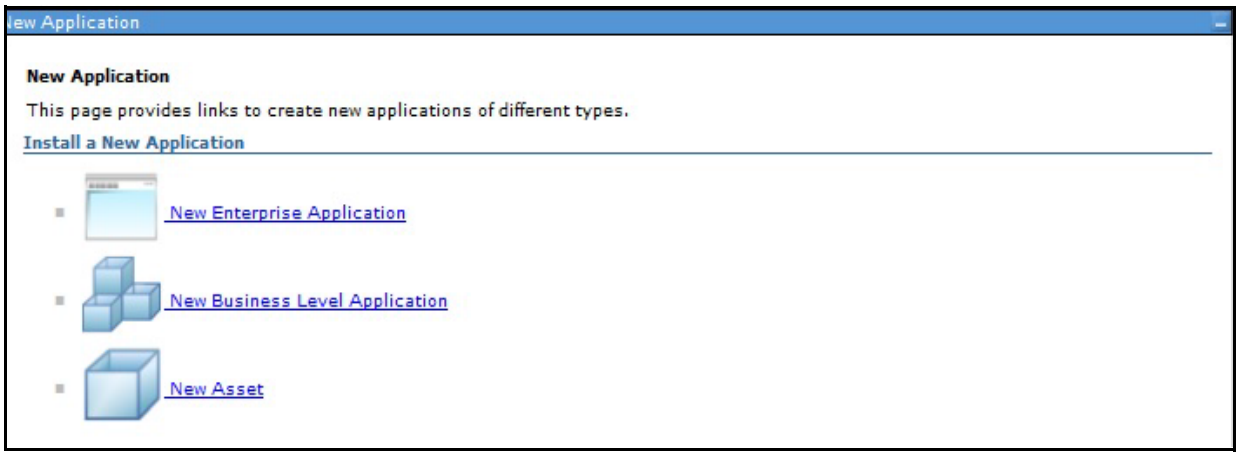
2. Create an `RTFRAUD.ear` folder in `<WEBSPHERE_INSTALL_DIR>/RTFRAUD.ear`.
3. Copy `<FIC_HOME>/RealTimeFraudIPEProcessing/RTFRAUD.ear` to `<WEBSPHERE_INSTALL_DIR>/RTFRAUD.ear`.
4. Open the following URL in the browser: `http://<ipaddress>:<Administrative Console Port>/ibm/console`. (use https protocol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

Figure 8: WebSphere Login Window



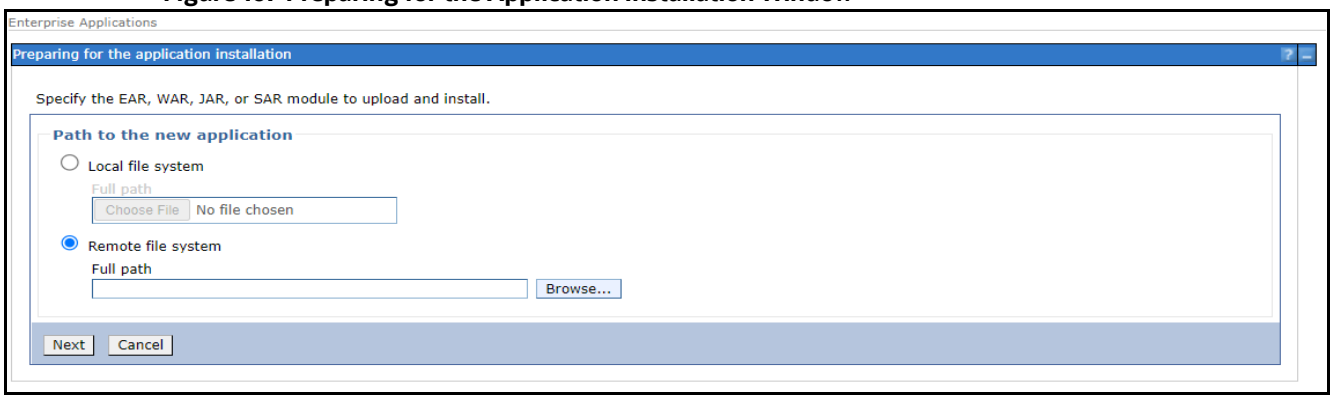
5. Enter the user credentials that have administrator rights and click **Log In**.
6. From the LHS menu, select **Applications** and click **New Application**. The New Application window is displayed.

Figure 9: New Application



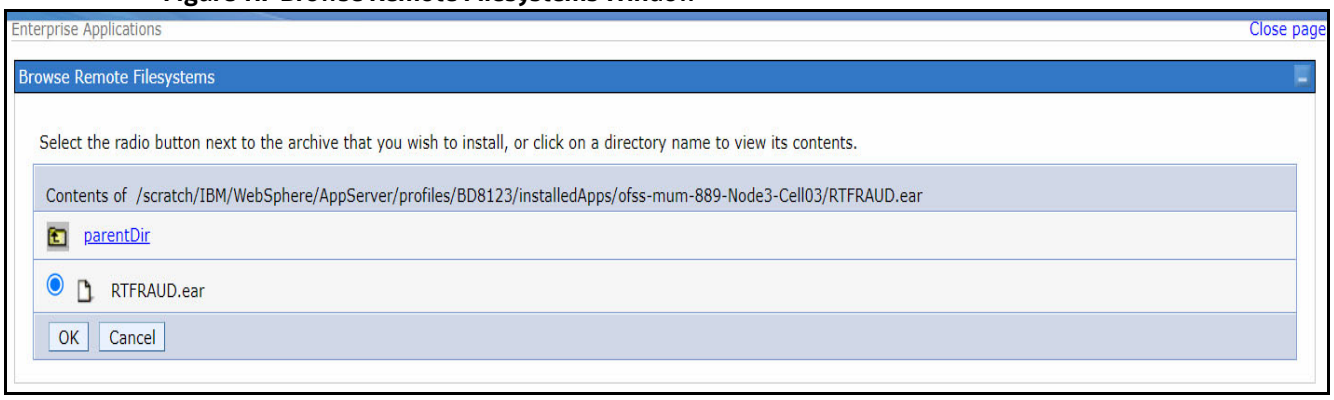
7. Click **New Enterprise Application**. The **Preparing for the application installation** window is displayed.

Figure 10: Preparing for the Application Installation Window



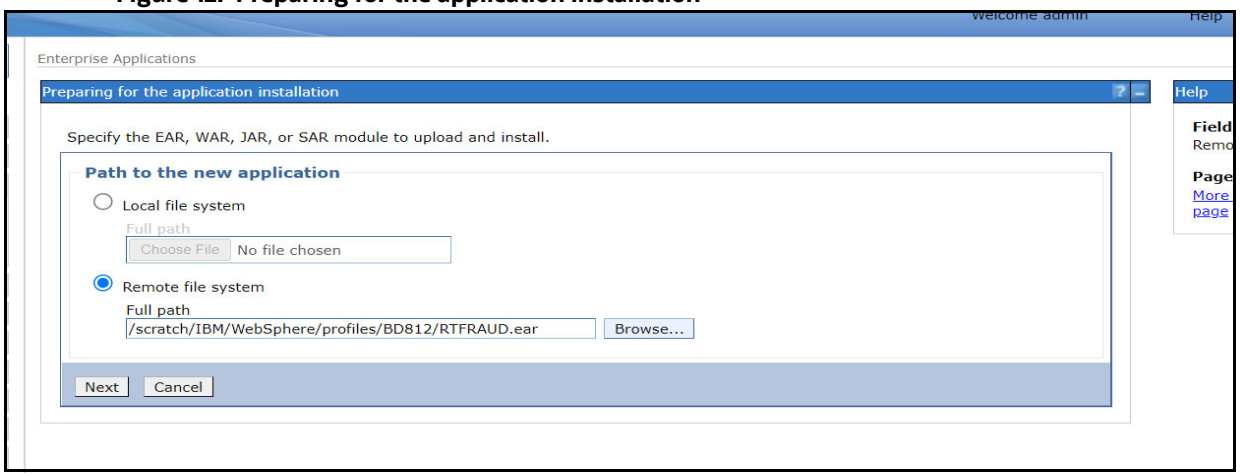
8. Select **Remote File System** and click **Browse**.

Figure 11: Browse Remote Filesystems Window



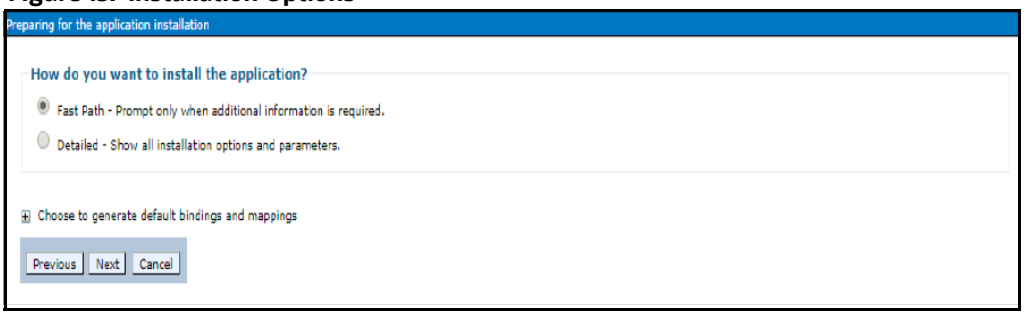
9. Navigate through folders and select the EAR file generated for RTFRAUD to upload and install. Click **OK**.

Figure 12: Preparing for the application installation



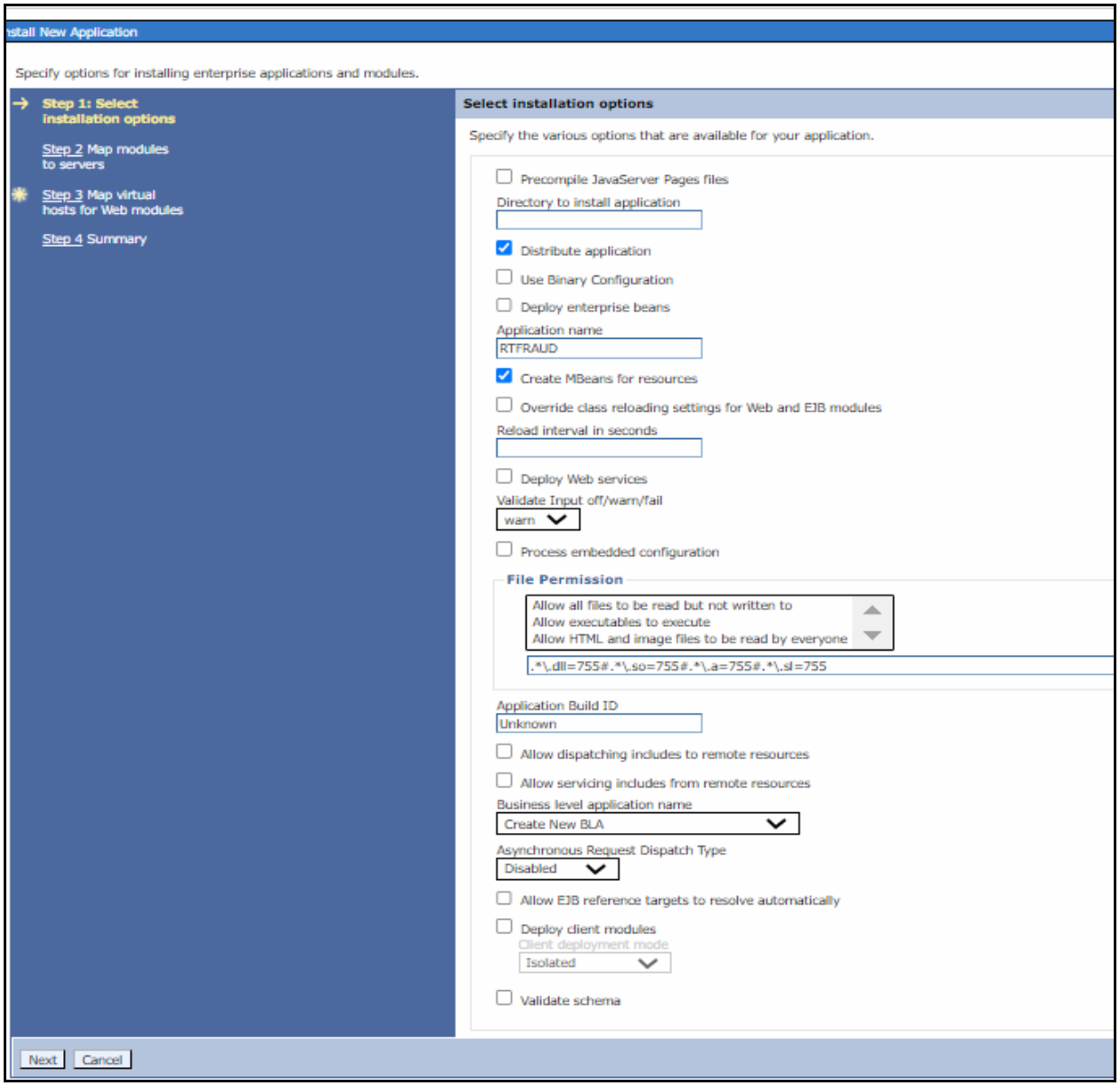
10. Click **Next**.

Figure 13: Installation Options



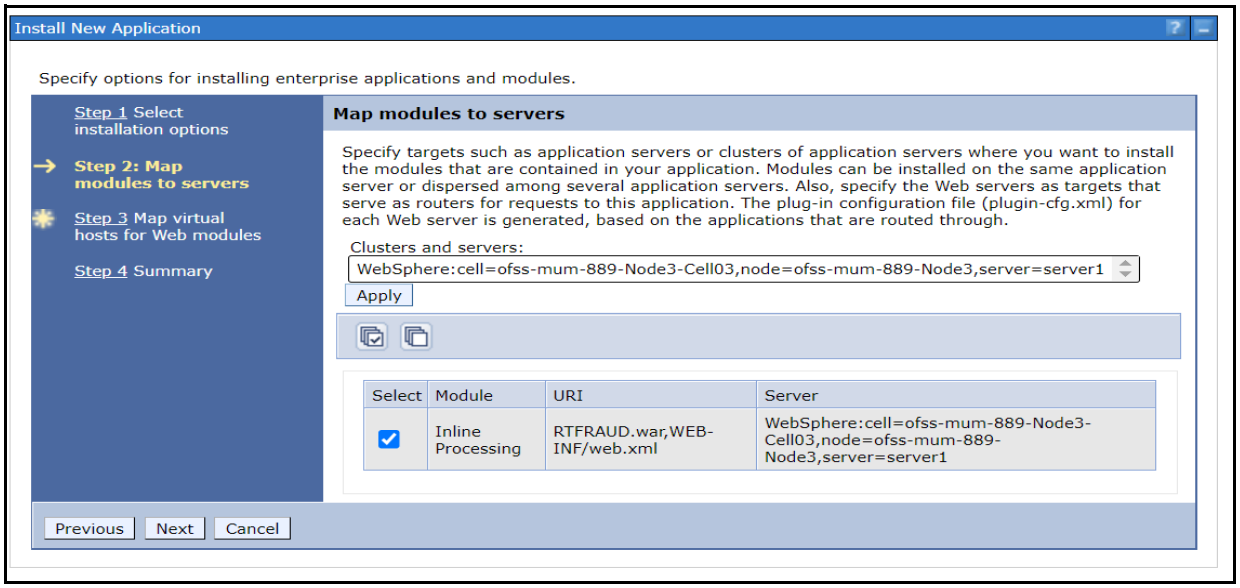
11. Select the **Fast Path** option and click **Next**. The Install New Application window is displayed.

Figure 14: Install New Application



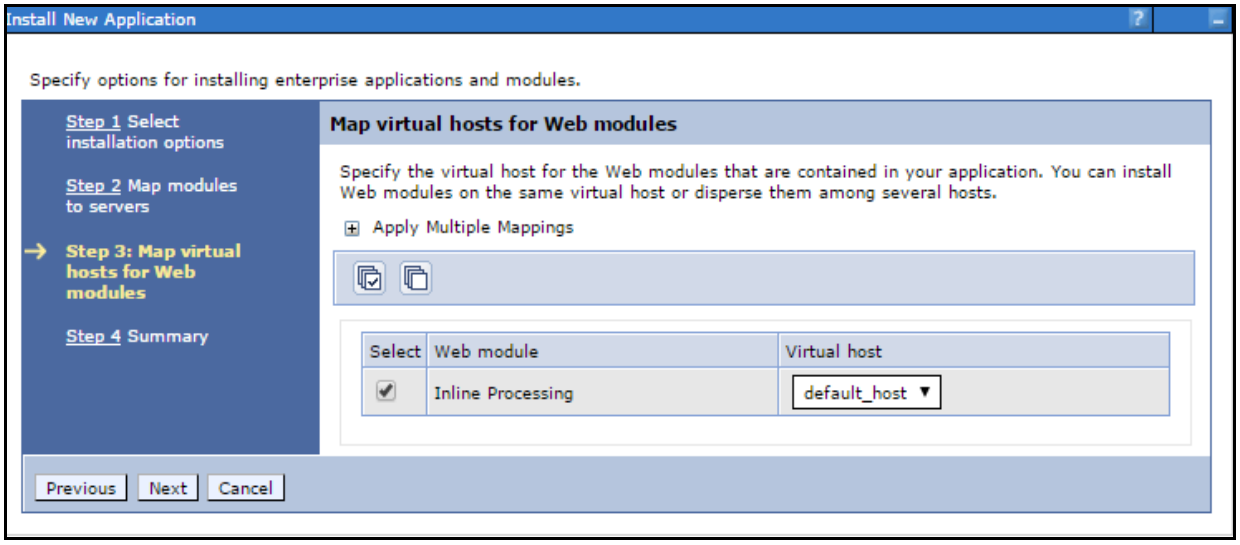
12. Enter the required information and click **Next**. The Map Modules to Servers window is displayed.

Figure 15: Map Modules to Servers



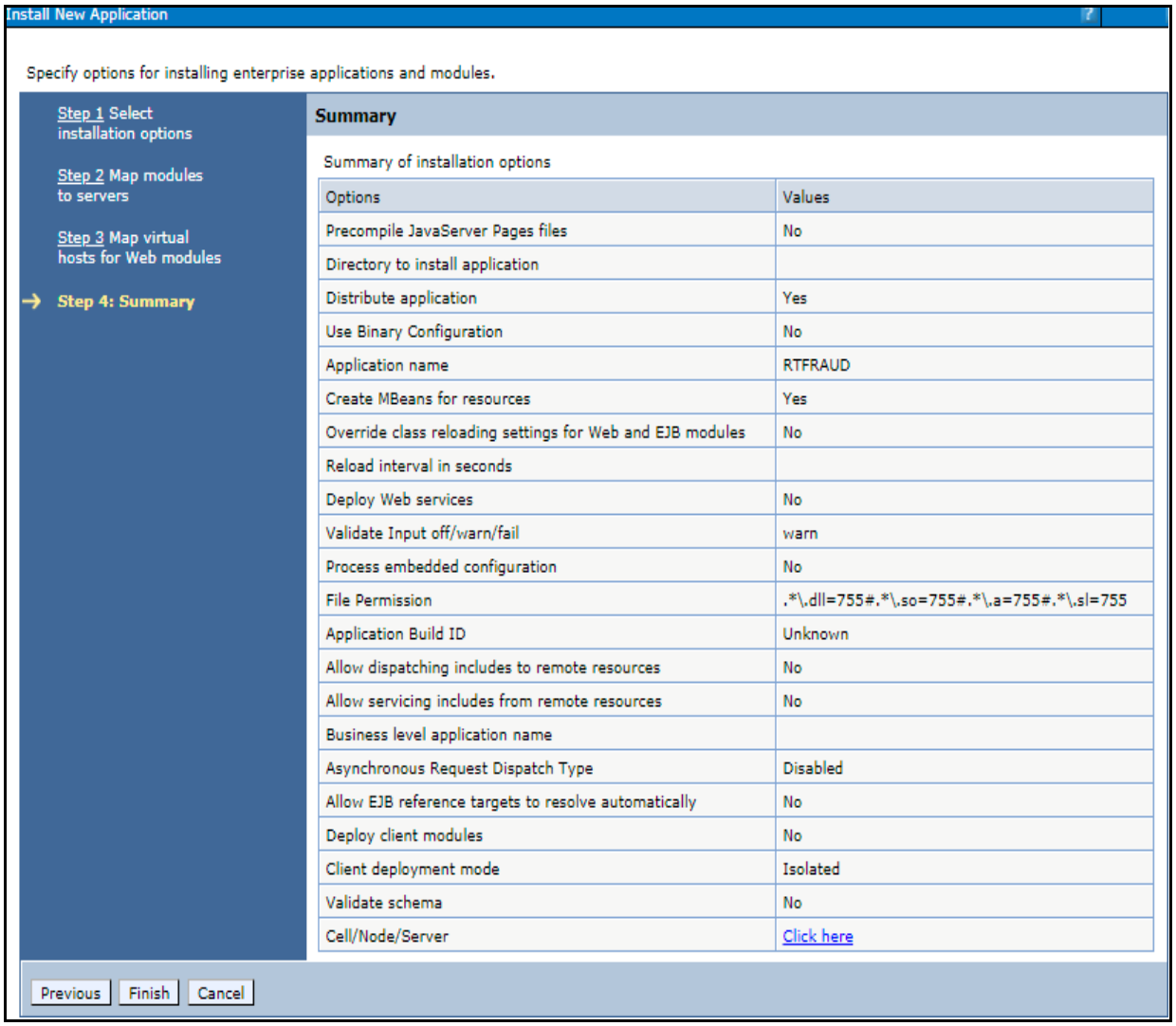
13. Select the **Inline Processing** check box and click Next. The Map Virtual hosts for the Web modules page are displayed.

Figure 16: Map Virtual hosts for Web modules page



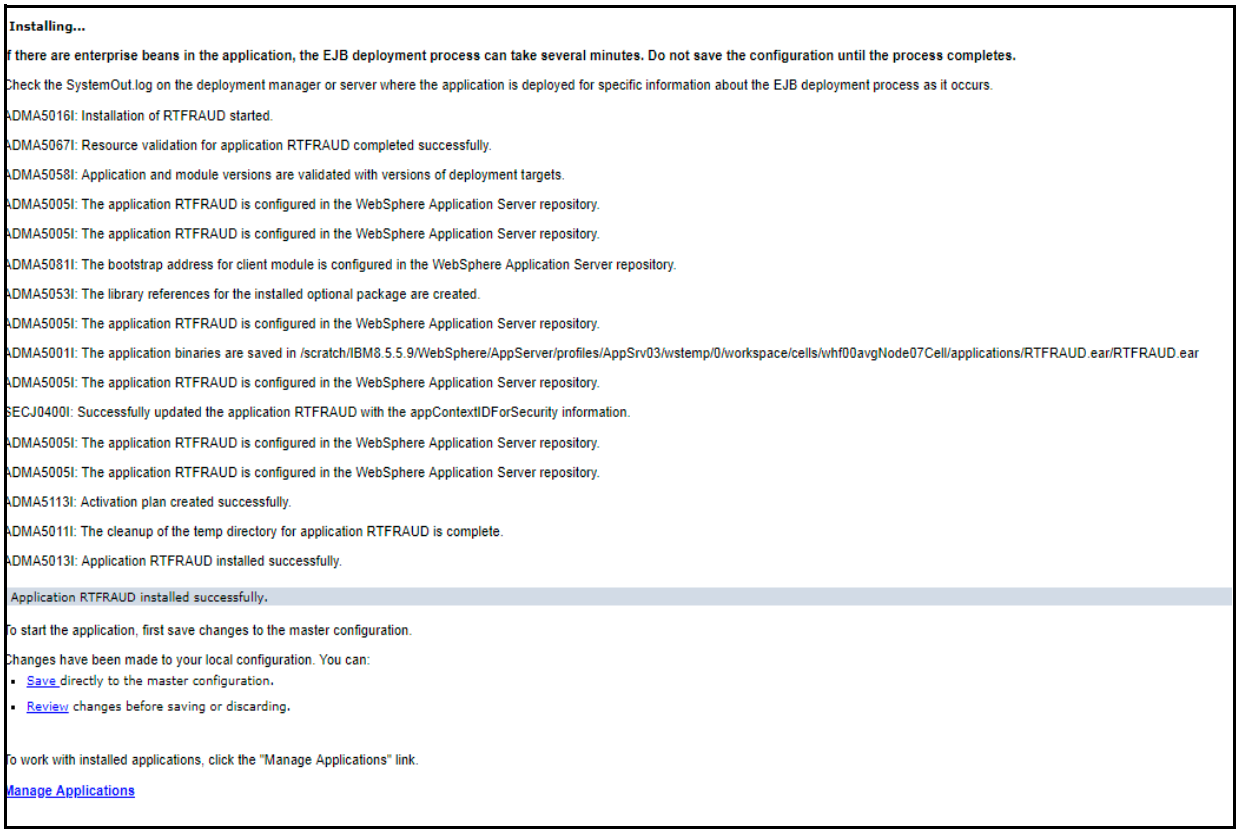
14. Select the **Inline Processing** check box and click **Next**. The Metadata for the modules page is displayed.
15. Select the **Metadata-complete** attribute check box and click **Next**. The Summary page is displayed.

Figure 17: Summary page



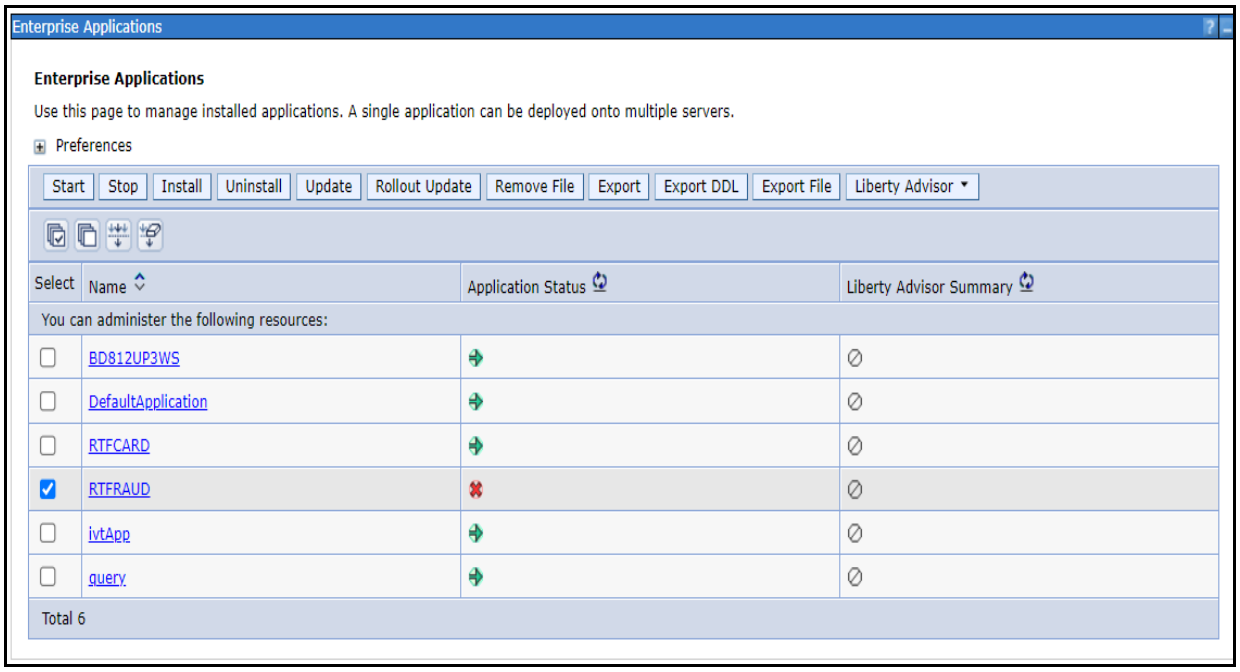
16. Click **Finish**. On successful installation, the system displays a success message.

Figure 18: Installation Success



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



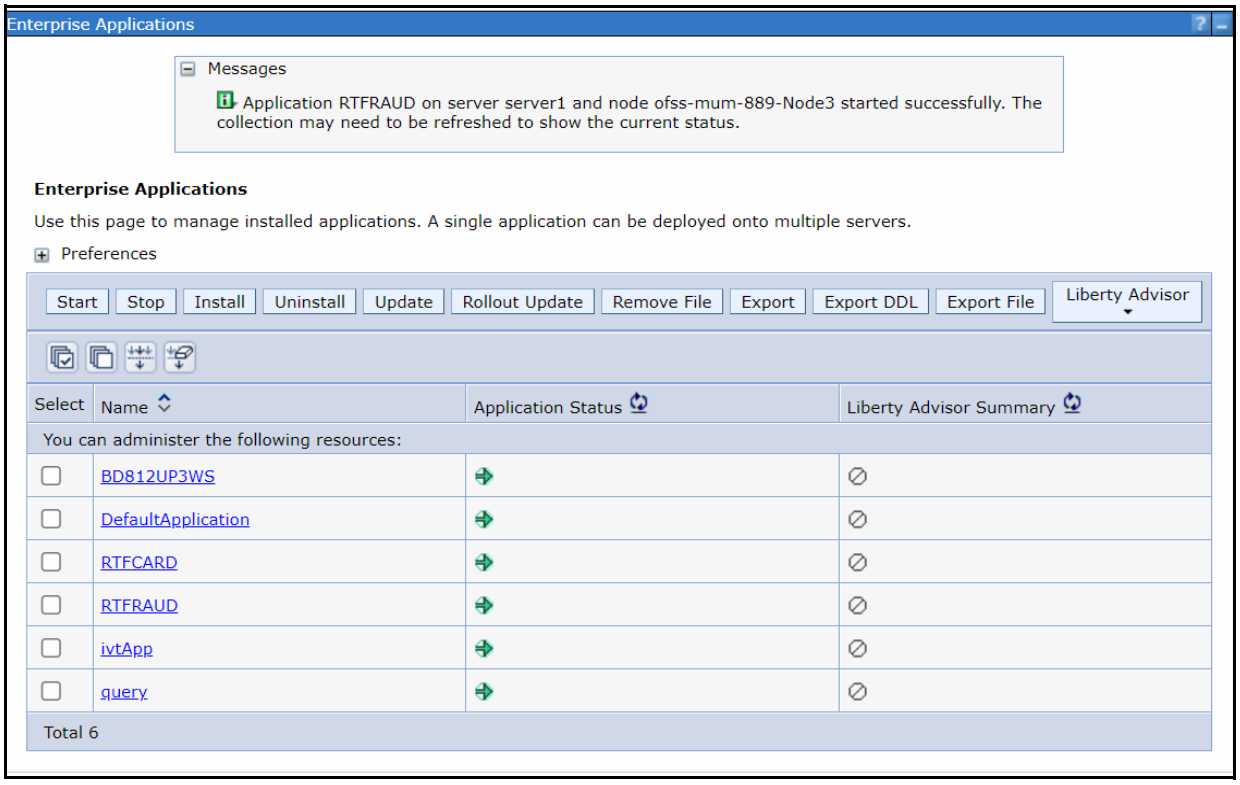
NOTE Make sure you take a backup of the Jersey Jar file to any folder and remove it by running the following command in the mentioned path.

Path: `<Deployed Area>/<RTFWIRE.ear>/<RTFWIRE.war>/WEB-INF/LIB`

Command: `Delete jersey-bundler(jersey-bundle-1.6.jar) jar`

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

Figure 20: Enterprise Application page with Confirmation message



19. Restart all OFS AAAI servers.

2.2.2.2.4 Deploying RTFRAUD.war in Tomcat

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

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

> **NOTE** Context name must be the directory name under `webapps`.

```
<Context path="/RTFRAUD" docBase="/scratch/ofsaaapp/apache-tomcat-
8.0.32/webapps/RTFRAUD" debug="0" reloadable="false"
crossContext="true"><Loader delegate="true"/>
     <Resource auth="Container"
                 name="jdbc/FICMASTER"
                 type="javax.sql.DataSource"
               driverClassName="oracle.jdbc.driver.OracleDriver"
                 username="act_obiconf"
                 password="password"
          url="jdbc:oracle:thin:@whf00aqr:1521/DEVUT08SPRINT"
```

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

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

3 Installing OFS Card Fraud Enterprise Edition

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

Topics:

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.

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.

3.2.1.1 Create the Source Entity Queue for RTF Card

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

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

  Table 4 shows a sample of JMS Queue configuration.

Table 4: Sample JMS Queue configuration

Name	Type	JNDI Name	Sub Deployment	Targets
Cache Operation Message Destination Topic	Topic	jms/cacheOperationMessageDestination	RTISubdeploy	RTIServer

Table 4: Sample JMS Queue configuration

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

3.2.1.2 Creating RTFCARD.ear or RTFCARD.war

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

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

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

3.2.1.3 Configuring the JMS properties

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

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

   Path: `$FIC_HOME/fiweb/webroot/conf`
2. Replace the place holder `##WEB_IP##` and `##WEB_PORT##`.

   For Webshpere:

   a. The `##WEB_IP##` and `##WEB_PORT##` values will be bootstrap IP address and port.

   b. Replace the `##JMS_PORT##` with bootstrap port in `CardTransactionsPost.jsp` in the below path.

      Path: `$FIC_HOME/RTFCardFraudIPEProcessing/WebContent`
3. Recreate and deploy the BD war.

3.2.1.4 Deploying RTFCARD.ear

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

The following sections detail the deployment of RTFCARD.ear.

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

> **NOTE** RTFCARD.ear deployment on Tomcat is not supported.

> **NOTE** Make sure that `ipe.produce.hglights.results` is **false** in the `<deployed area>/RTFCARD.ear/RTFCARD.war/conf/install.properties` path. You must update it to **false** if it is shown as **true**.

3.2.1.4.1 Deploying RTFCARD.ear in WebLogic

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

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

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

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

   ```
   jar -xvf RTFCARD.ear
   ```

5. Delete the `RTFCARD.ear` and `RTFCARD.war` files.
6. Create an `RTFCARD.war` folder in `<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RTFCARD.ear.`
7. Copy `<FIC_HOME>/RTFCardFraudIPEProcessing/RTFCARD.war` to `<WEBLOGIC_INSTALL_DIR>/user_projects/domains/<DOMAIN_NAME>/applications/RTFCARD.ear/RTFCARD.war.`
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:

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:

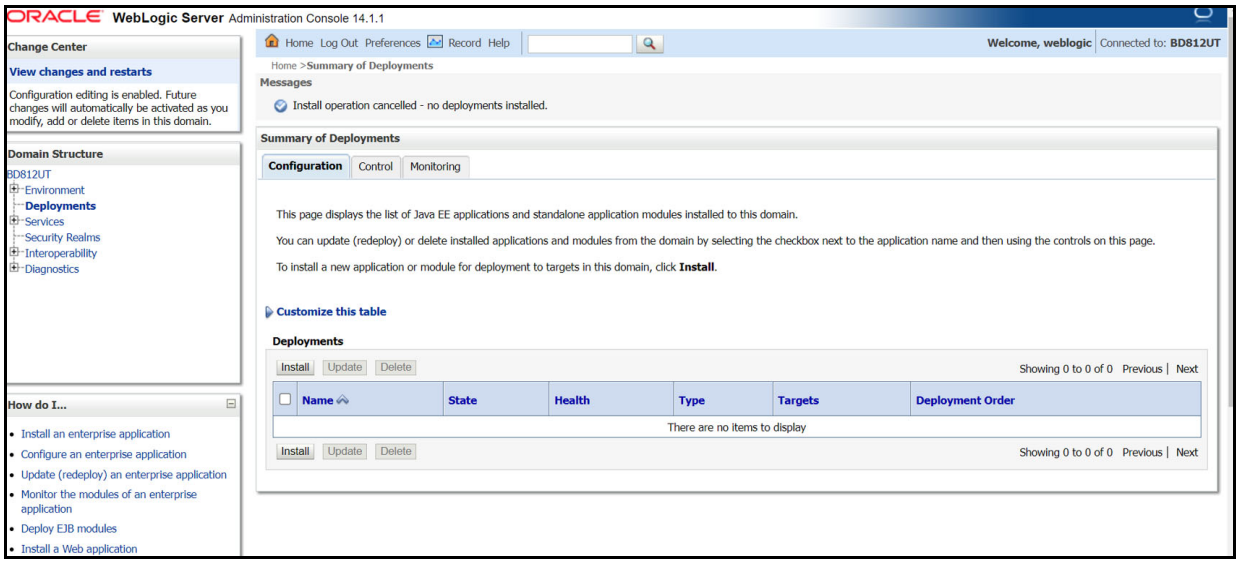
   `./startWebLogic.sh -d64 file`

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.

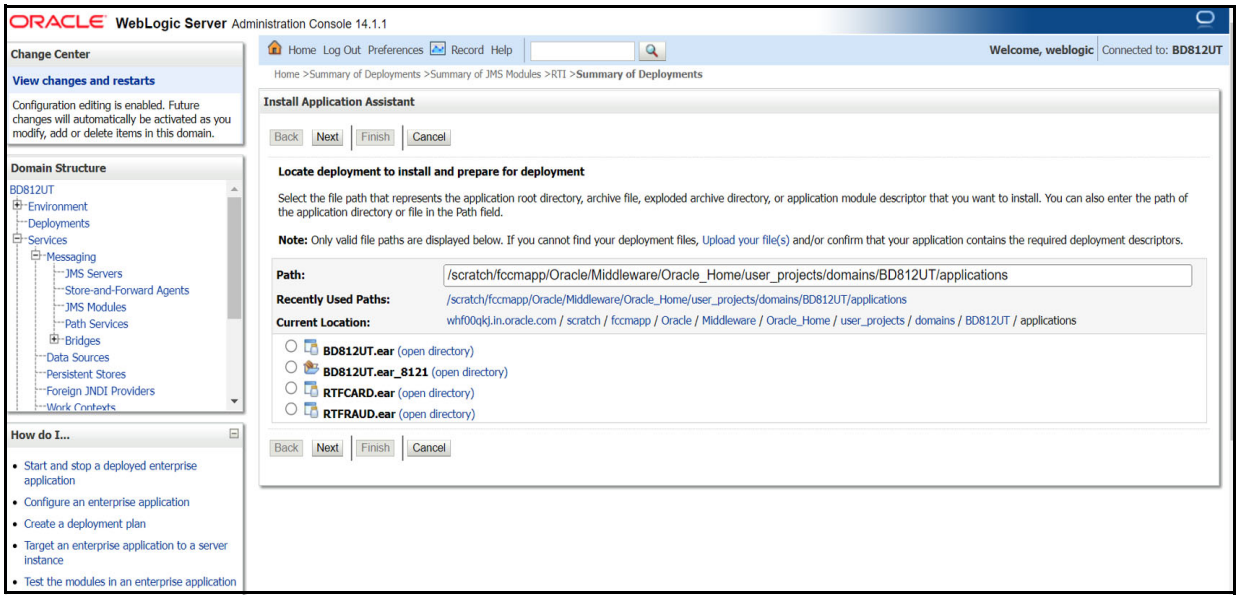
4. Login with the Administrator **Username** and **Password**. The Summary of Deployment page is displayed.

Figure 21: Summary of Deployment



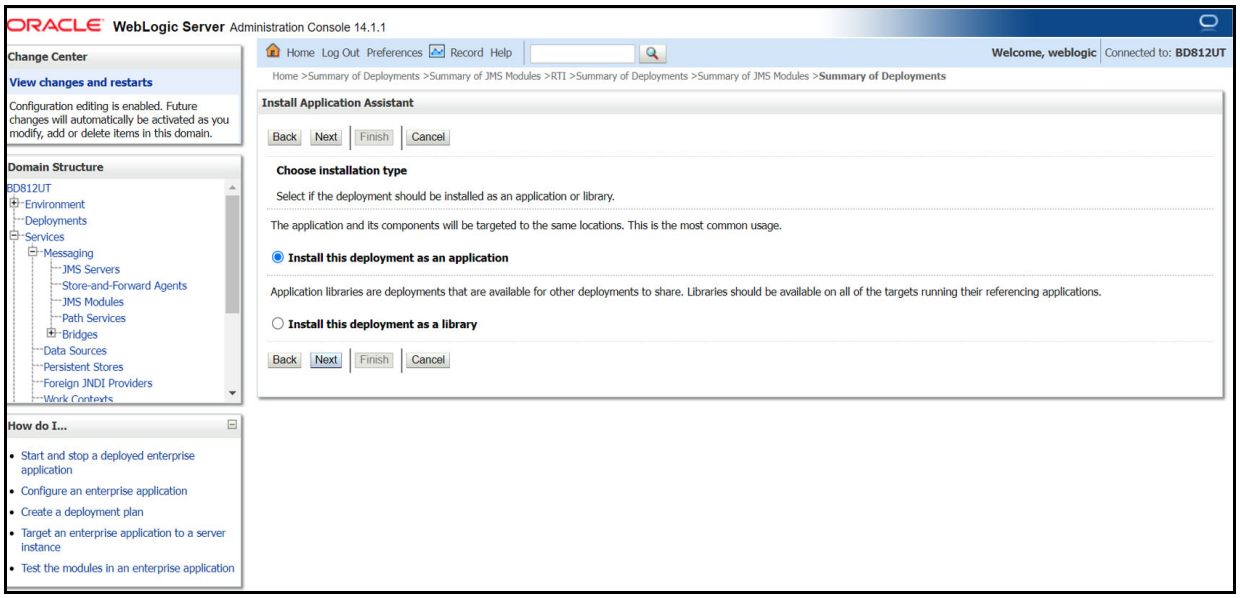
5. Click **Install**. The Install Application Assistance page is displayed.

Figure 22: Install Application Assistance Window



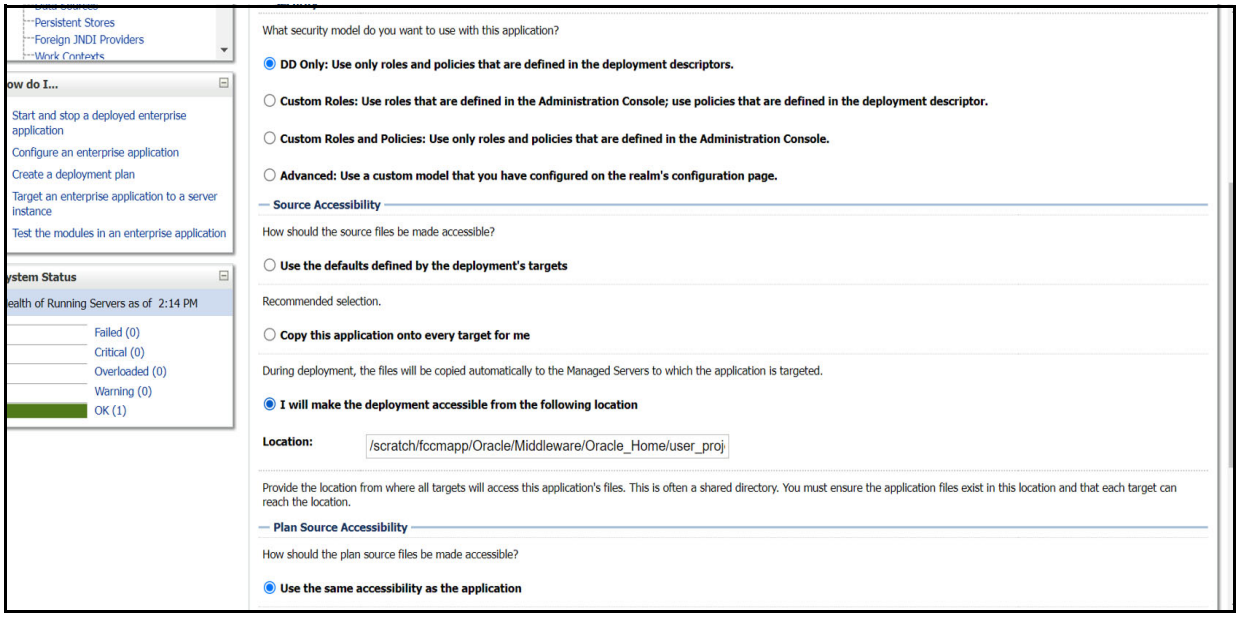
6. Select `RTFCARD.ear` and click **Next**. This action displays the Install Application Assistance page with the Choose targeting style section.

Figure 23: Install Application Assistance with choose Target Style



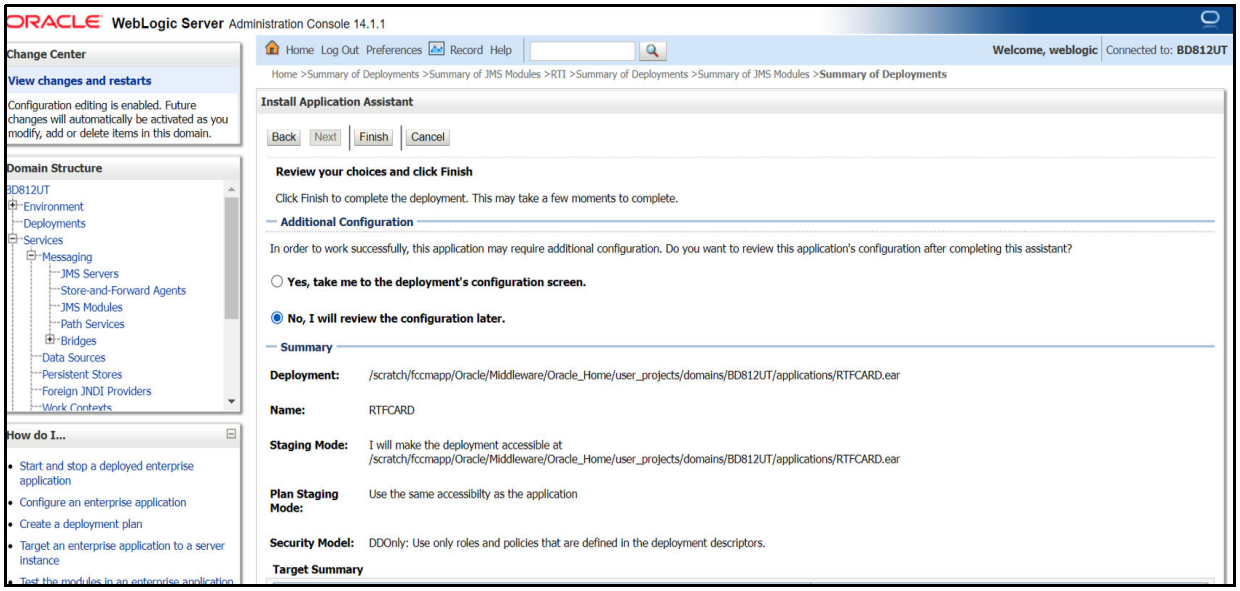
7. By default, the **Install this deployment as an application** option in the Choose targeting style section is selected. Click **Next**. This action displays the Install Application Assistance page in the Optional Settings section.

Figure 24: Install the Application Assistance page with Optional Settings



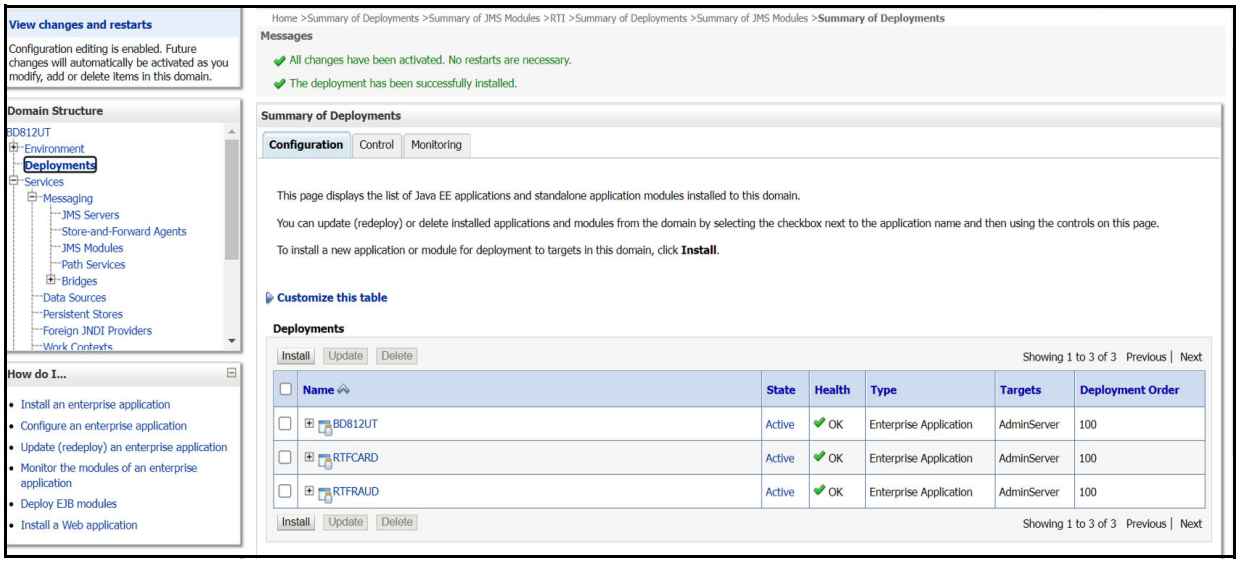
8. Retain the default selections and click **Next**. The Install Application Assistance page is displayed with the Review your choices and click Finish section.

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



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

Figure 26: Summary of Deployment page with RTFCARD



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.

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

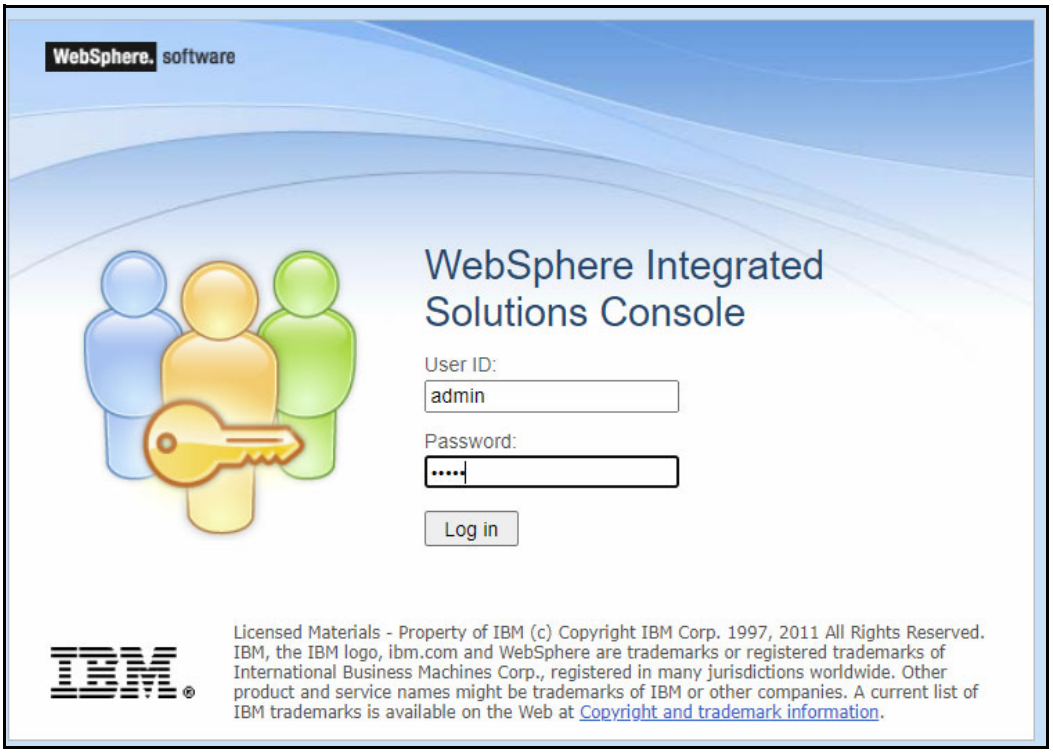
To deploy `RTFCARD.ear` in WebSphere, follow these steps:

1. Start the WebSphere Profile by navigating to the path "`/<WebSphere_Installation_Directory>/IBM/WebSphere/AppServer/profiles/<Profile_Name>/bin/`" then execute the command:

   ./startServer.sh server1

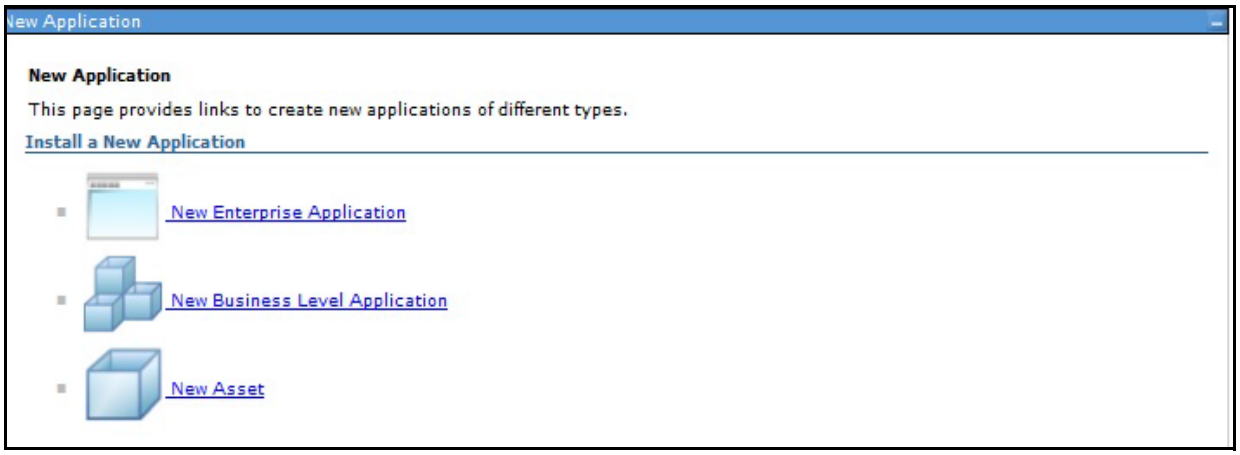
2. Create an `RTFCARD.ear` folder in `<WEBSPHERE_INSTALL_DIR>/RTFCARD.ear`.
3. Copy `<FIC_HOME>/RTFCardFraudIPEProcessing/RTFCARD.ear` to `<WEBSPHERE_INSTALL_DIR>/RTFCARD.ear`.
4. Open the following URL in the browser: `http://<ipaddress>:<Administrative Console Port>/ibm/console`. (use https protocol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

Figure 27: WebSphere Login Window



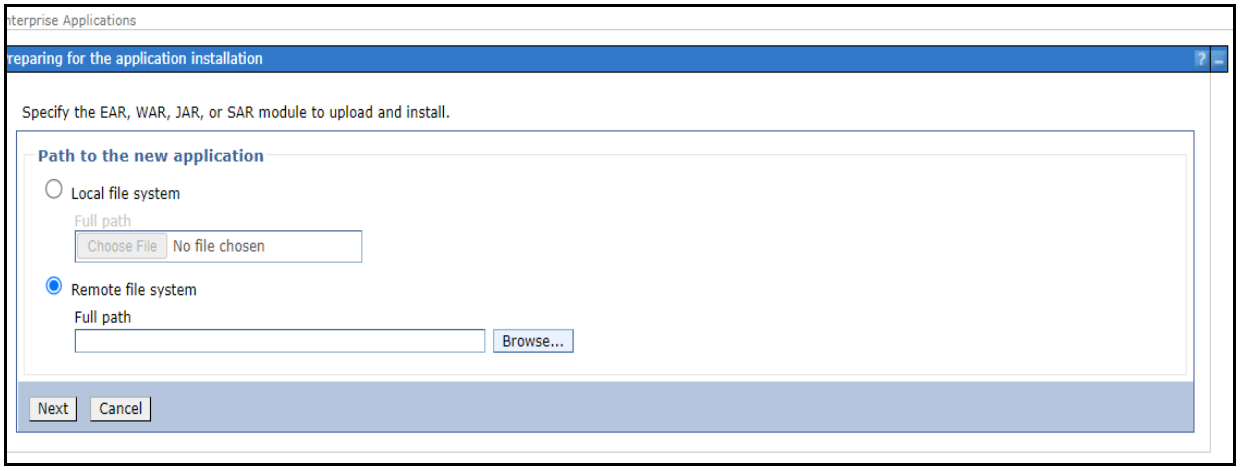
5. Enter the user credentials that have administrator rights and click **Log In**.
6. From the LHS menu, select **Applications** and click **New Application**. The New Application window is displayed.

Figure 28: New Application



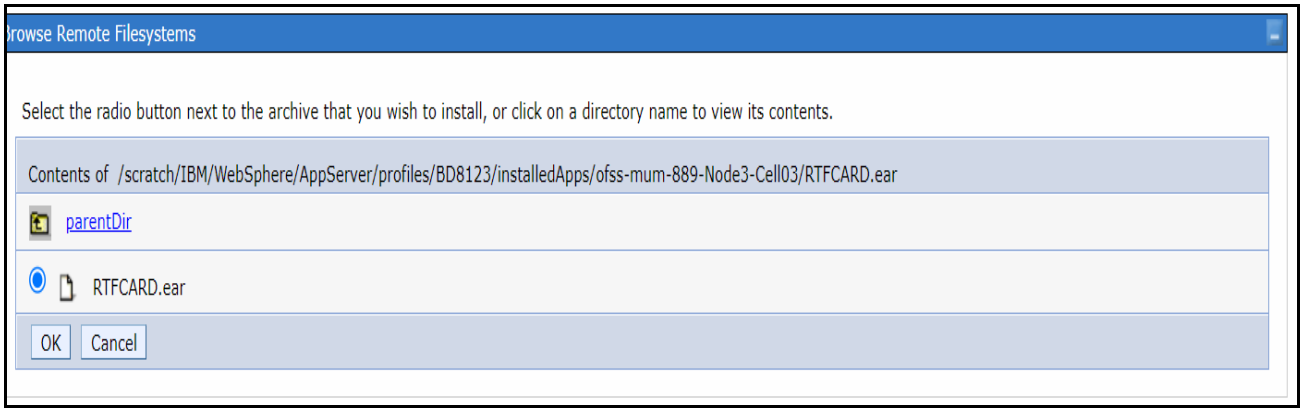
7. Click **New Enterprise Application**. The **Preparing for the application installation** window is displayed.

Figure 29: Preparing for the application installation



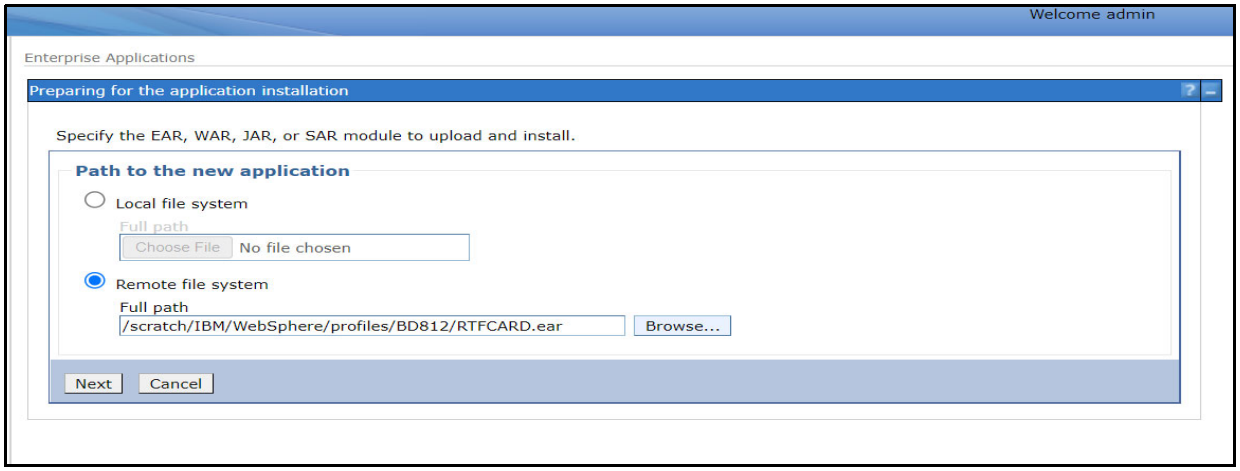
8. Select **Remote File System** and click **Browse**.

Figure 30: Browse Remote Filesystems Window



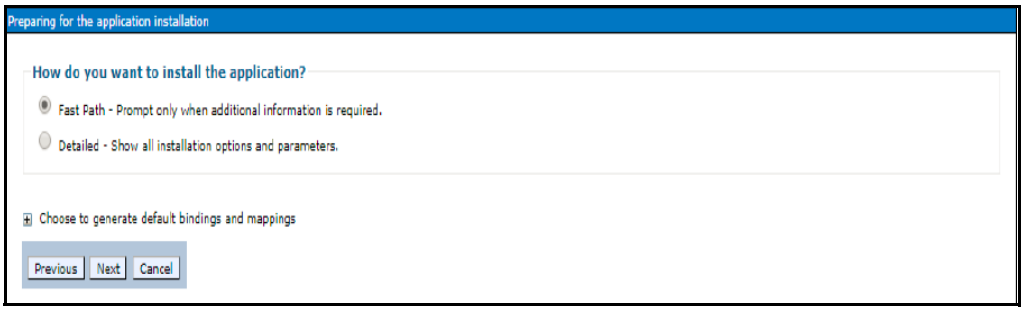
9. Navigate through folders and select the EAR file generated for RTFRAUD to upload and install.

Figure 31: Preparing for the application installation



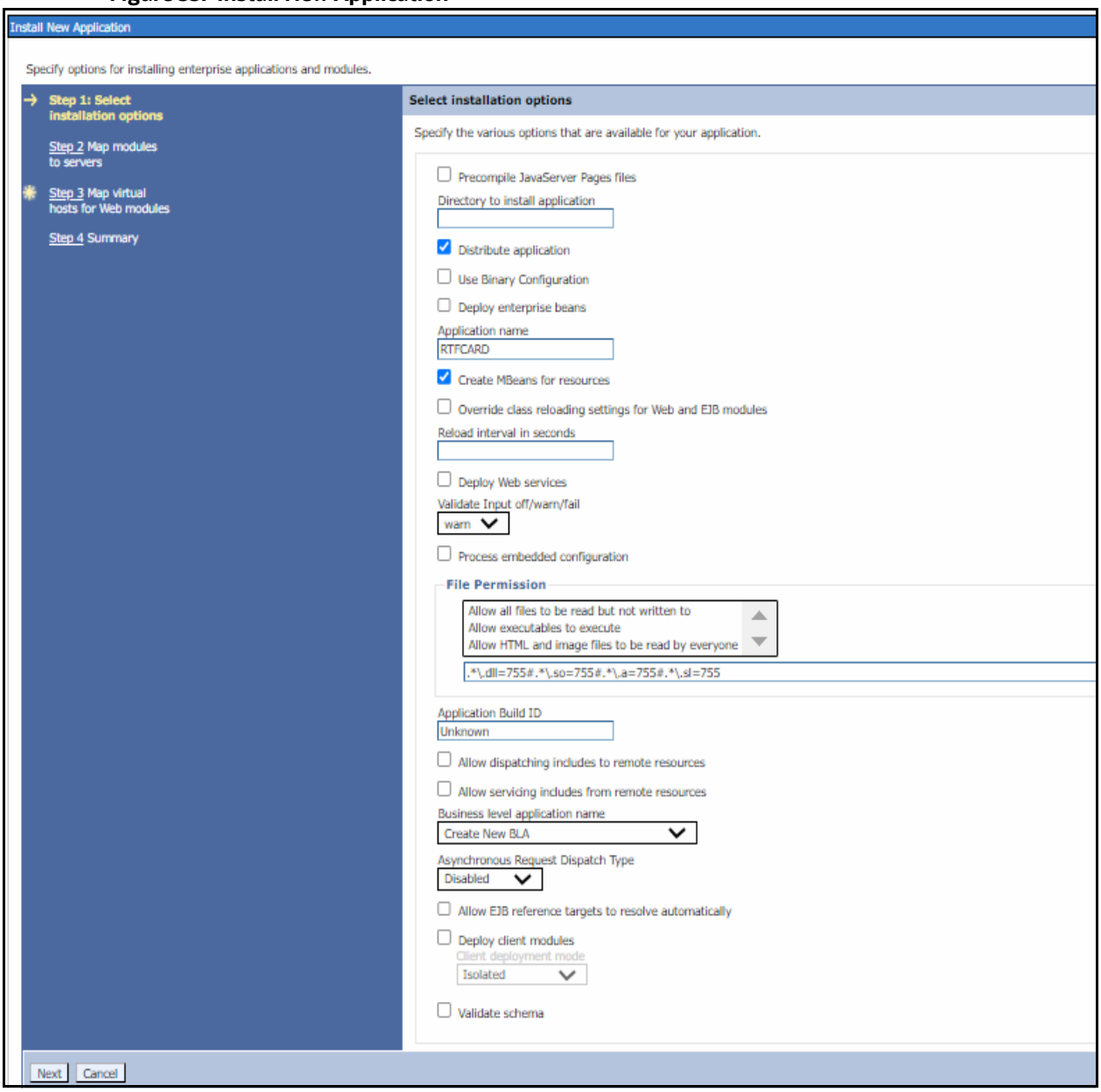
10. Click **Next**.

Figure 32: Installation Options



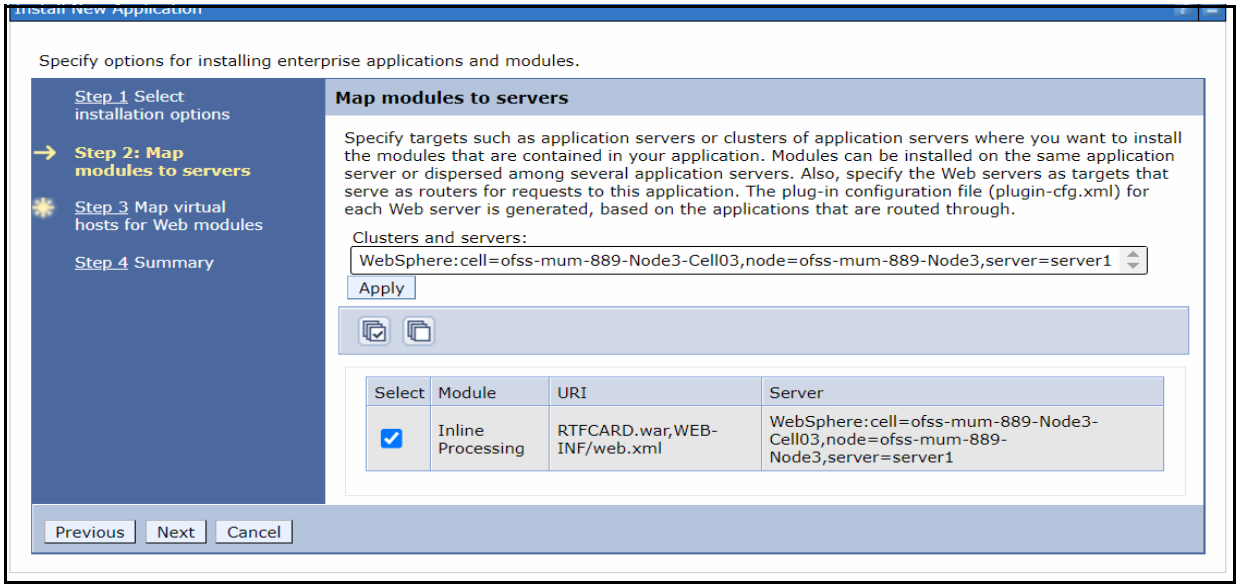
11. Select the **Fast Path** option and click **Next**. The Install New Application window is displayed.

Figure 33: Install New Application



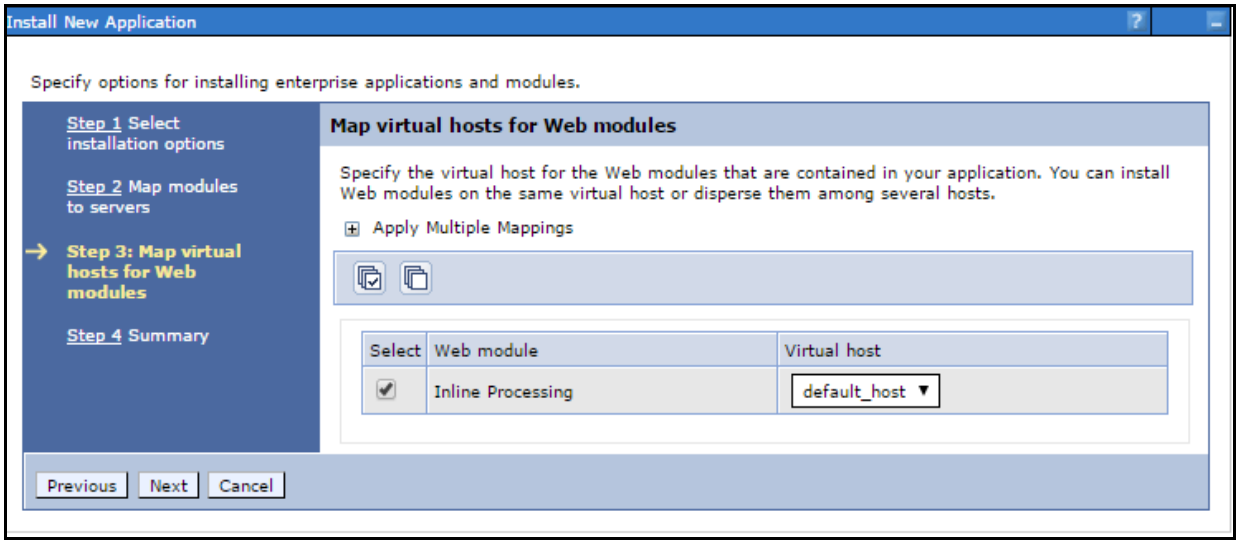
12. Enter the required information and click **Next**. The Map Modules to Servers window is displayed.

Figure 34: Map Modules to Servers



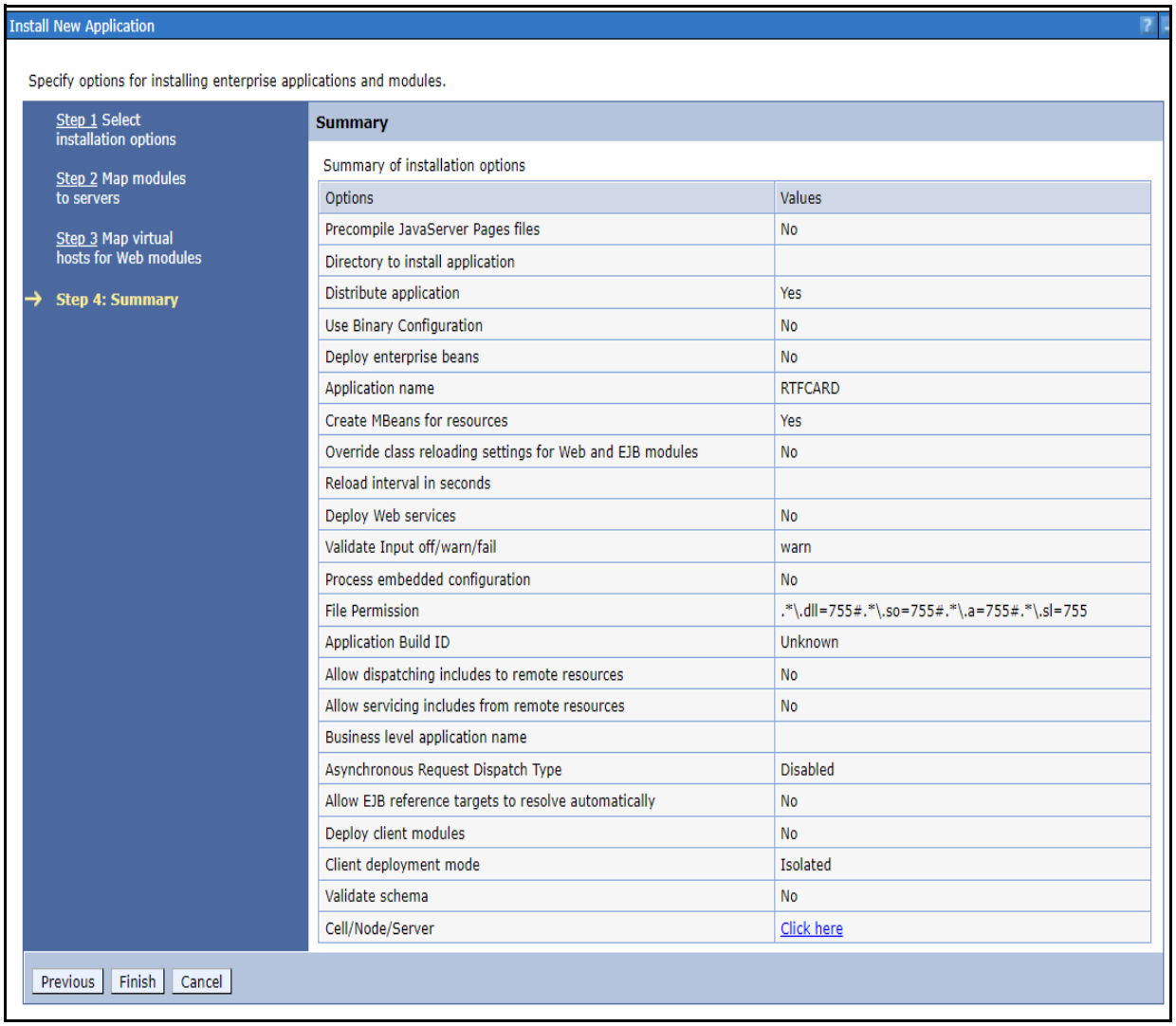
13. Select the **Inline Processing** check box and click Next. The Map Virtual hosts for the Web modules page are displayed.

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

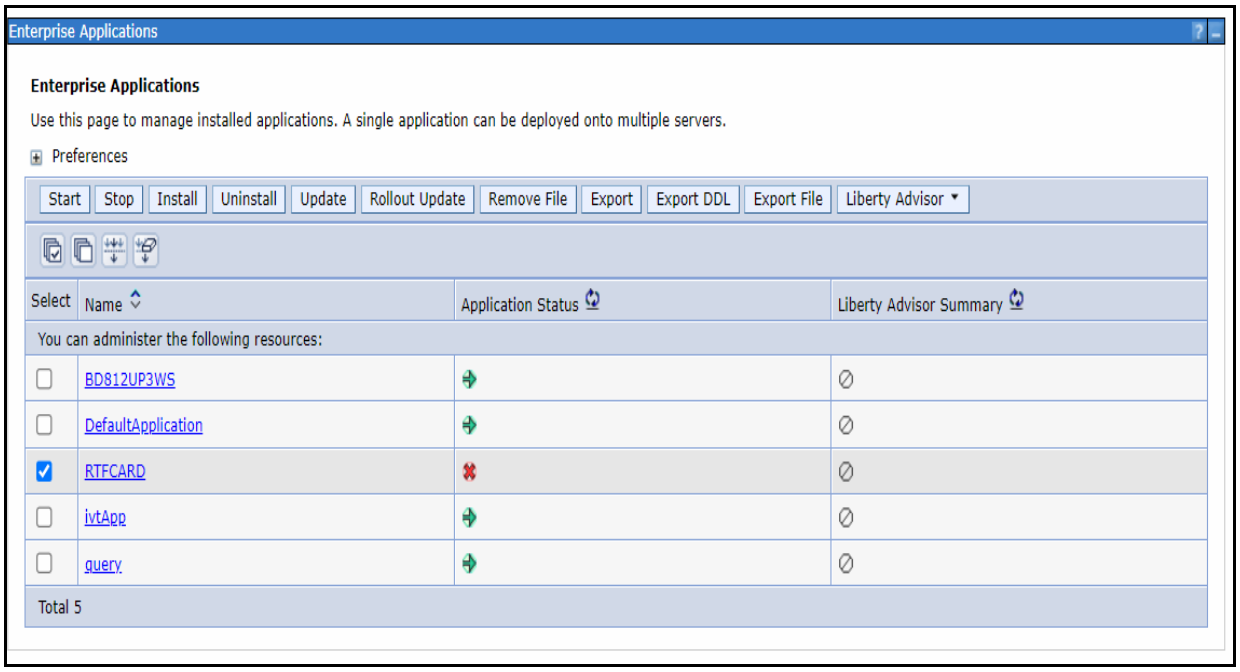


16. Click **Finish**. On successful installation, the system displays a message.

Figure 37: Installation Success

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



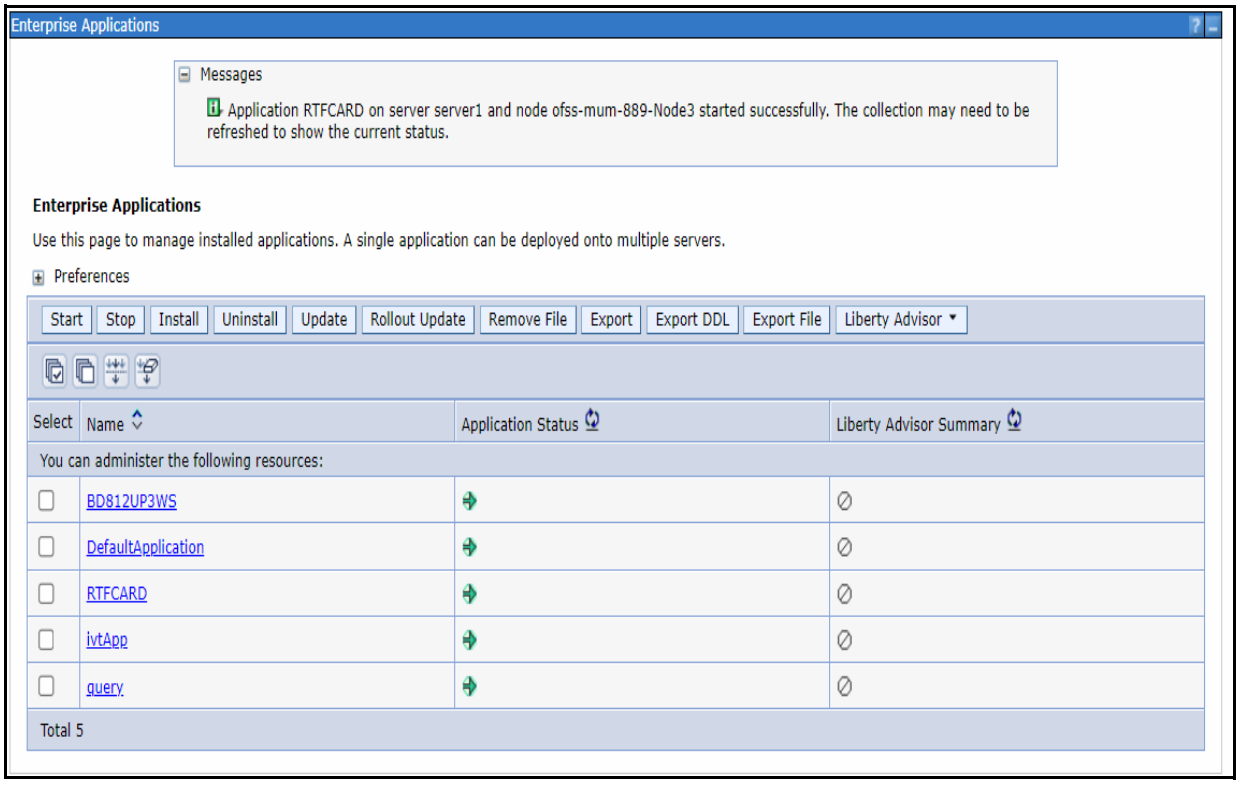
NOTE Make sure you take a backup of the Jersey Jar file to any folder and remove it by running the following command in the mentioned path.

Path: <`Deployed Area>/<RTFCARD.ear>/<RTFCARD.war>/WEB-INF/LIB`

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.

Figure 39: Enterprise Application page with the Confirmation message



19. Restart all OFS AAAI servers.

3.2.1.5 Commands to Execute to Import IPE Configs

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

Path: `<FIC_HOME>/ficapp/common/FICServer/bin/`

Command: `./RTIImport.sh`

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

4 Managing User Administration and Security Configuration

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

Topics:

4.1 About User Administration

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

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

4.2 User Provisioning Process Flow

Figure 40: User Provisioning Process Flow

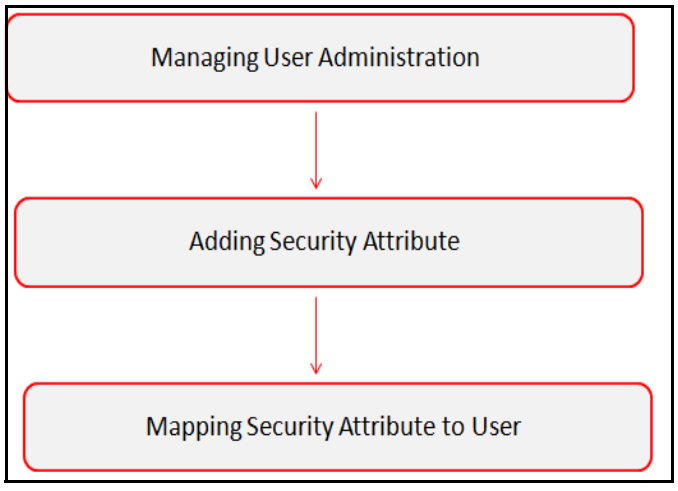


Table 5 lists the various actions and associated descriptions of the user administration process flow.

Table 5: User Provisioning Process Flow

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

4.3 Managing User Administration

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

4.3.1 Managing Identity and Authorization

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

This section covers the following topics:

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

4.3.1.1 Managing Identity and Authorization Process Flow

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

Figure 41: Managing Identity and Authorization Process Flow

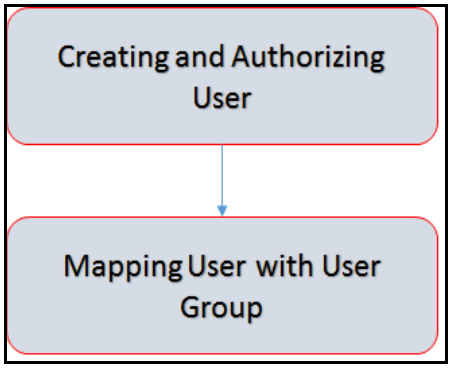


Table 6 lists the various actions and associated descriptions of the user administration process flow.

Table 6: Administration Process Flow

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

4.3.1.2 Creating and Authorizing a User

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

4.3.1.3 Mapping a User with a User Group

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

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

Table 7: Fraud Roles and User Groups

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

4.4 Adding Security Attributes

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

4.4.1 About Security Attributes

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

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

4.4.1.1 Types of Security Attributes

The types of security attributes are as follows:

- Jurisdiction

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

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

- Business Domain

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

4.5 Business Domain and Jurisdiction Mapping

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

To map Business Domain and Jurisdiction, follow these steps:

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

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

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

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

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

```
INSERT INTO FCC_FR_CARD_GROUP_SEC_ATTR_MAP (
    V_GROUP_CD,
    V_SEC_ATTR_CD,
    V_SEC_ATTR_VAL
)
VALUES (
    'CARDFRAUDADMINGR',
    'BUSDMN',
    'a'
)
```

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

```
INSERT INTO FCC_FR_CARD_GROUP_SEC_ATTR_MAP (
    V_GROUP_CD,
    V_SEC_ATTR_CD,
    V_SEC_ATTR_VAL
)
VALUES (
    'CARDFRAUDADMINGR',
```

```
    'JRSDCN',
    'E'
)
```

5 Configuring Real Time Wire Fraud Scoring

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

Topics:

5.1 Operating Real Time Wire Fraud Service

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

5.1.1 Real Time Wire Fraud Service Request

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

`<WEB_PROTOCOL>://<WEB_IP>:<WEB_PORT>/RTFRAUD/service/json/score`

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

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

Table 8: Real Time Wire Fraud Message Attributes

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

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

5.1.2 Real Time Wire Fraud Service Response

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

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

5.2 Managing Real Time Wire Fraud Scenarios/Rules

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

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

Table 9: Fraud Risk Rules

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

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:

6.1 Operating Real Time Card Fraud Service

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

6.1.1 Real Time Card Fraud Service Request

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

- **API:**

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

- **JSP:**

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

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

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

Table 10: Jars and Paths to Configure IPE JMS Client

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

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

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

Table 11: Real Time Card Fraud Message Attributes

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

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

6.1.1.1 Real Time Card Fraud Service JMS Response Details

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

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

Table 12: Real Time Card Fraud Service JMS Response Details

JMS Response	Alert Action	Alert Description	Response
Alert Not Created	Clean	This response is generated on the hold queue if the posted transaction is clean, i.e., it does not match any of the given IPE rules in the application. This action doesn't generate any alert.	{ "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.	{ "Transaction ID" : 2787, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : Failed to Evaluate, "Assessment ID" : "", "Score" : "", "Decision" : "" }

Table 12: Real Time Card Fraud Service JMS Response Details

JMS Response	Alert Action	Alert Description	Response
Alert Created	Held	This response is created on the hold queue if the posted transaction fails at any IPE rules provided in the application. An alert in held status gets generated and the users can view it in the UI.	{ "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10.0, "Decision" : "" }
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.	{ "Transaction ID" : 2788, "Message Reference" : Message Reference, "Status" : CLEAN, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Released }
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.	{ "Transaction ID" : 2789, "Message Reference" : Message Reference, "Status" : HOLD, "Error" : "", "Assessment ID" : 22258, "Score" : 10, "Decision" : Blocked }

6.2 Managing Real Time Card Fraud Scenarios/Rules

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

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

Table 13: Fraud Risk Rules

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

6.2.1 Modify Fraud Rules

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

Perform the following to modify fraud rules.

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

For more information, see Inline Processing Engine User Guide.

7 Managing Real Time Wire Administration

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

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

Topics:

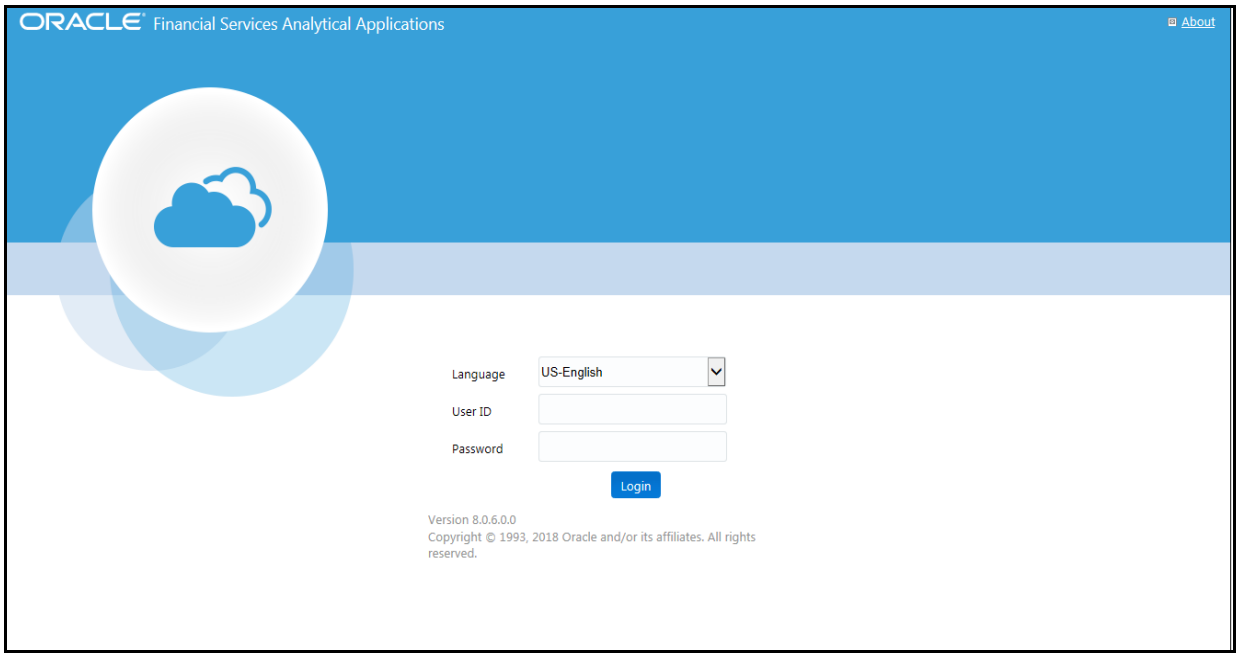
7.1 Accessing Real Time Wire Administration

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

1. Enter the OFSAA URL in your browser.

   The OFSAA Login page is displayed.

Figure 42: OFSAA Login Page



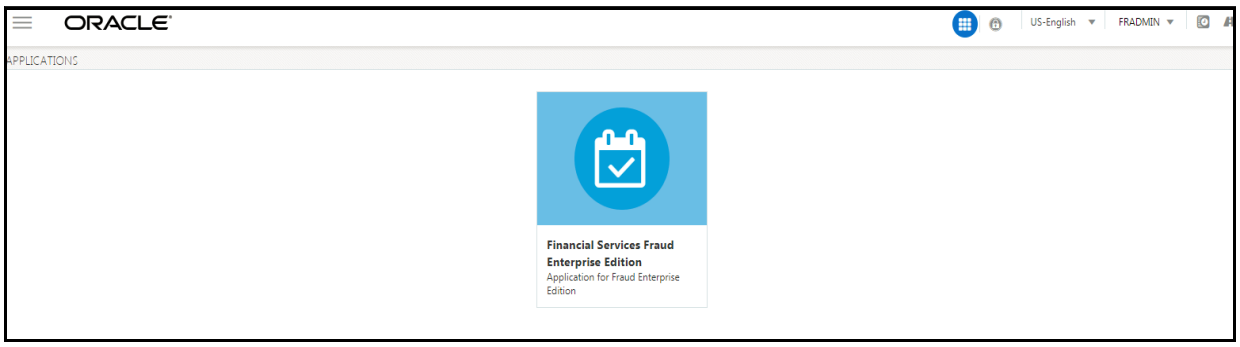
2. Select the **Language**.
3. Enter your **User ID** and **Password**.

   NOTE Ensure to login as an **Administrator**.

4. Click **Login**.

   This action displays the **Applications** page.

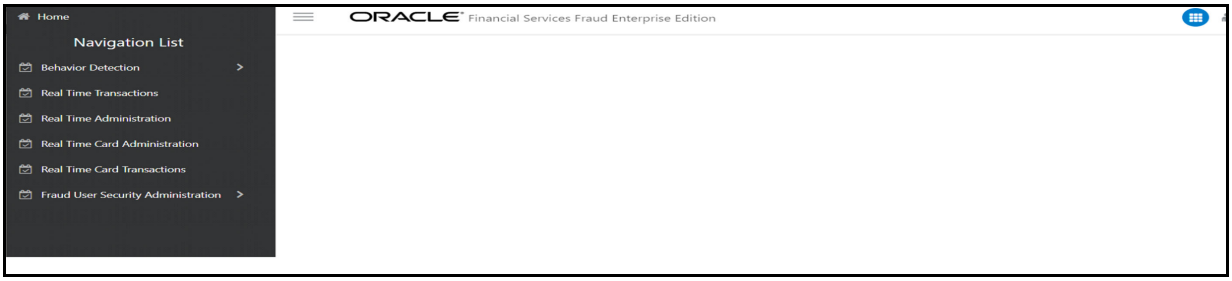
Figure 43: Fraud Enterprise Edition Applications Page



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 44: Fraud Enterprise Edition Home Page



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

   This action displays the Real Time Wire Administration page.

7.2 Configuring Real Time Wire Administration

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

Perform the following to configure SLA:

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

   The **Create New Rule** section expands and displays the fields required to create a new rule.
3. Enter the following details in the **Create New Rule** section.

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

Table 14: Create New Rule

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

Table 14: Create New Rule

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

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

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

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

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

Table 15: Create New Condition

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

6. Click **Save.**

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

7. Click **Configuration**.

   The Configuration section expands.

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

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

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

    This action configures the SLA for the Real Time Fraud.

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:

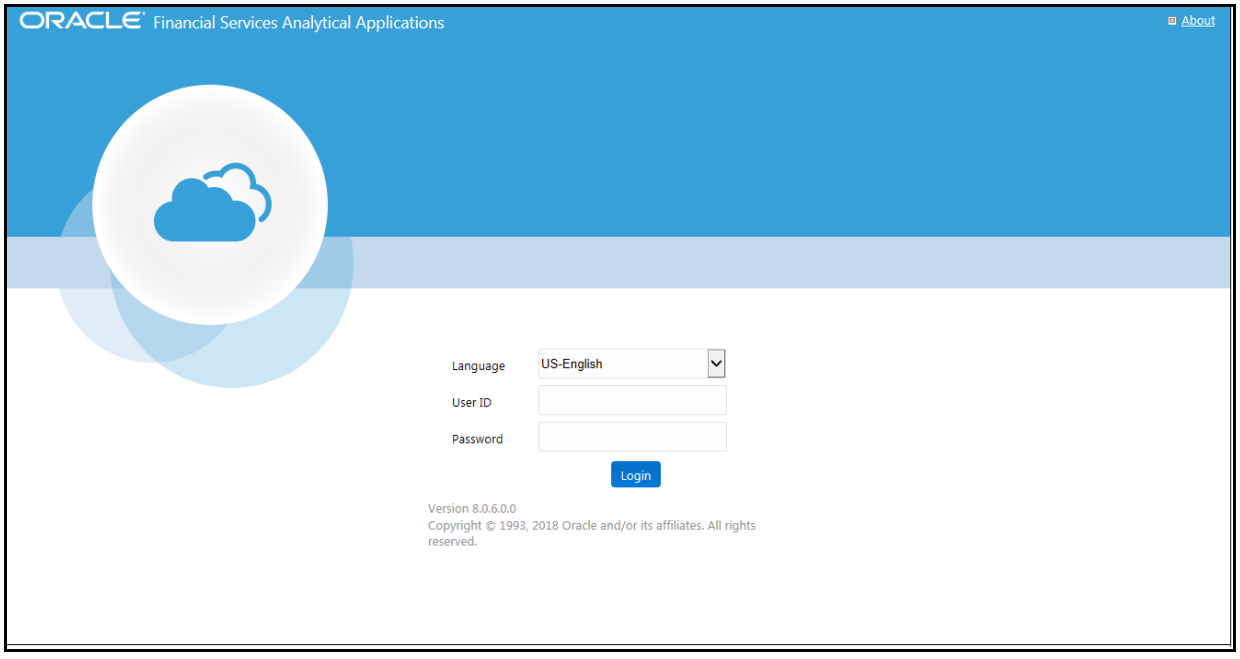
8.1 Accessing Real Time Card Administration

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.

Figure 45: OFSAA Login Page



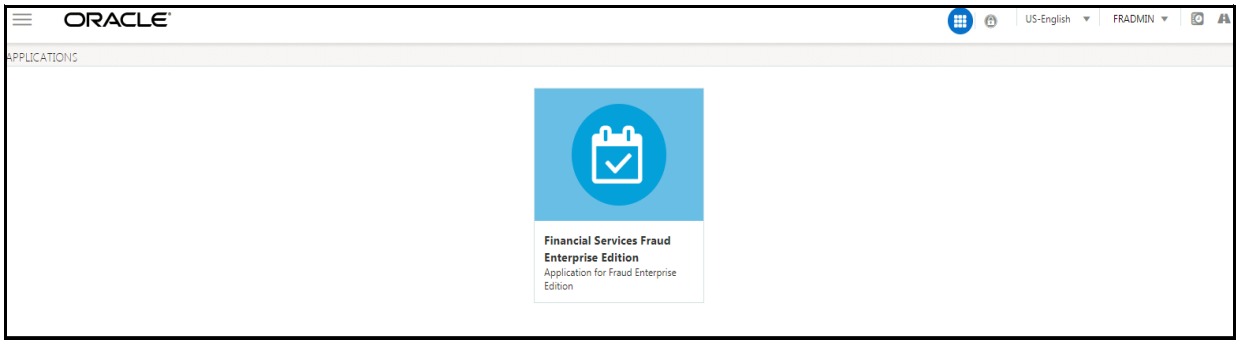
2. Select the **Language**.
3. Enter your **User ID** and **Password**.

   NOTE Ensure to login as an **Administrator**.

4. Click **Login**.

The **Applications** page is displayed.

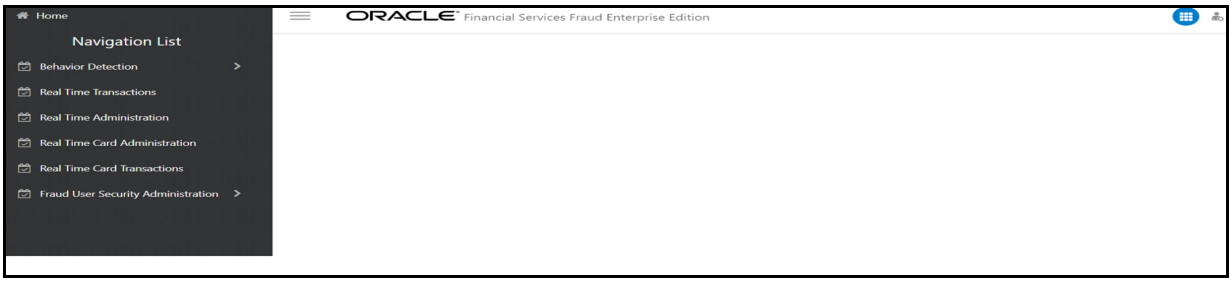
Figure 46: Fraud Enterprise Edition Applications Page



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 47: Fraud Enterprise Edition Home Page



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

   The Real Time Card Administration page is displayed.

8.2 Configuring Real Time Card Administration

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

Perform the following to configure SLA:

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

   The **Create New Rule** section expands and displays the fields required to create a new rule.
3. Enter the following details in the **Create New Rule** section.

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

Table 16: Create New Rule

Field	Description
Rule ID	Indicates the Rule ID.

Table 16: Create New Rule

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

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

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

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

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

Table 17: Create New Condition

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

6. Click **Save.**

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

7. Click **Configuration**.

   The Configuration section expands.

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

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

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

    This action configures the SLA for the Real Time Fraud.

9 Appendix-A: Wire Fraud Sample JSON

The JSON input data must be in the following format:


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

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

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

   }
}
```

10 Appendix-B: Card Fraud Sample JSON

The JSON input data must be in the following format


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

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

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

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

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

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

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

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

11 Appendix-C: Real Time Wire Fraud Request Attributes

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

Table 18: Real Time Wire Fraud Request Attributes

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

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

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

12 Appendix-D: Real Time Card Fraud Request Attributes

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

Table 19: Real Time Card Fraud Request Attributes

Request Attributes	Description
Transaction unique SIQ ID	The sequence ID number of the transaction.
Authentication Method	The method used to authorize the transaction.
Channel Type	The type of the transaction channel.
Channel Info	The name of the transaction channel.
Channel User ID	The user ID of the party involved in the transaction.
Channel User ID Type	The type of ID of the party involved in the transaction.
Channel Device ID	The device ID of the party involved in the transaction.
Channel Amount Limit	The maximum allowable transaction amount for the channel.
Channel Amount Currency	The currency type of the transaction amount for the channel.
Channel Geographic Location	The geo location from which the transaction was originated.
Channel Country	The country the transaction was initiated from for the channel.
Channel City	The city the transaction was initiated from for the channel.
Customer Country Code	The country code of the country in which the customer resides.
POS Merchant ID	The point of sale merchant identifier associated with the transaction.
ATM Financial Institution ID/ Teller terminal ID	The financial institution identifier associated with the ATM from which the transaction was made.
Merchant MCC/SIC	The unique code of the merchant category.
Terminal Acquirer Unique ID	The unique identifier of the merchant acquirer associated with the terminal.
Terminal Acquirer Country	The country code of the merchant acquirer associated with the terminal.
Terminal ID	The unique identifier associated the terminal from which the transaction was made.
Terminal Merchant/ATM/ Teller Terminal City	The city associated with the merchant owner of the terminal.
Terminal Merchant/FI/Teller Terminal Name	The name of the merchant who owns the terminal.
Terminal Merchant/FI Original script Name	The name of the financial institution.
Terminal Postal Code	The postal code component of the terminal location on which the transaction was made.

Request Attributes	Description
Terminal State	The state component of the terminal location on which the transaction was made.
Customer Source UniqueID	The unique identifier associated with the customer within the source system.
Customer Date of Birth	The customer's date of birth.
Customer First Name	The first name of the customer.
Customer Last Name	The last name of the customer.
Customer global ID	The global id of the customer.
Customer Alias	The alias of the customer.
Customer Address Purpose Type Indicator	The purpose type indicator for the address.
Customer Address Line 1	The address line 1 for the Location
Customer Address Line 2	The address line 2 for the Location
Customer Address Line 3	The address line 3 for the Location
Customer Address Line 4	The address line 4 for the Location
Customer Address Line 5	The address line 5 for the Location
Customer Address Line 6	The address line 6 for the Location
Customer City Of Residence	The city of residence of the customer.
Customer Country Of Residence	The country of residence of the customer.
Customer Postal Code	The postal code component of this address.
Customer Region	The region component of this address.
Customer State	The state component of this address.
Customer Email Address 1	The primary email address of the customer.
Customer Email Address Purpose Type 1	The email address type of the customer's primary email address.
Customer Email Address 2	The secondary email address of the customer.
Customer Email Address Purpose Type 2	The email address type of the customer's secondary email address.
Customer Phone Extension 1	The phone extension for the customer's primary phone number.
Customer Phone Number 1	The primary phone number of the customer.
Customer Phone Purpose Type 1	The phone number type for the customer's primary phone number.
Customer Phone Extension 2	The phone extension for the customer's secondary phone number.
Customer Phone Number 2	The secondary phone number of the customer.

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

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

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

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

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

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

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

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

OFSAA Support Contact Details

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

Send Us Your Comments

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

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

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

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