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

Administration and Configuration Guide

Release 8.0.8.0.0

E98368-01

November 2019

Administration and Configuration Guide, Release 8.0.8.0.0

E98368-01

Primary Author: Nethravathi G

Contributor: Anupama Srinivasa, Ruchi Tripathi, Swetha Yatham

Contents

1 Installing OFS Fraud Enterprise Edition

2 Managing User Administration and Security Configuration

3 Managing Administration for Real Time Fraud

4 Managing Real Time Administration

A Sample JSON

Document Control

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

About this Guide

This guide explains the concepts for the Real Time Fraud component in OFS Fraud Enterprise Edition. application and provides comprehensive instructions for configuration and system administration. This section focuses on the following topics:

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

Summary

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

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.

Related Documents

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

- *Oracle Financial Services Fraud Enterprise Edition (Real Time Fraud) User Guide*

Conventions Used in this Guide

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

Table 0–1 Conventions Used in this Guide

Convention	Meaning
Boldface	Boldface type indicates graphical user interface elements associated with an action (menu names, field names, options, button names), or terms defined in text or glossary.
Italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates the following: • Directories and subdirectories • File names and extensions • Process names • Code sample, that includes keywords, variables, and user-defined program elements within text
<variable>	Substitute input value

Abbreviations Used in this Guide

The following table lists the abbreviations used in this guide:

Table 0–2 Abbreviations and their meaning

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

1

Installing OFS Fraud Enterprise Edition

Prerequisites

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

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

Post Installation Configuration

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

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

Configuring install.properties File

You must configure the install.properties file in order to configure the Real Time 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

aai.auth.url=http://<host>:<port>/<Context
Name>/rest-api/idm/service/login
```

Configuring IPE for Real Time Fraud

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

To install RTFRAUD service, follow these steps:

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

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

Creating RTFRAUD.ear/ 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`/ `RTFRAUD.war`, follow these steps:

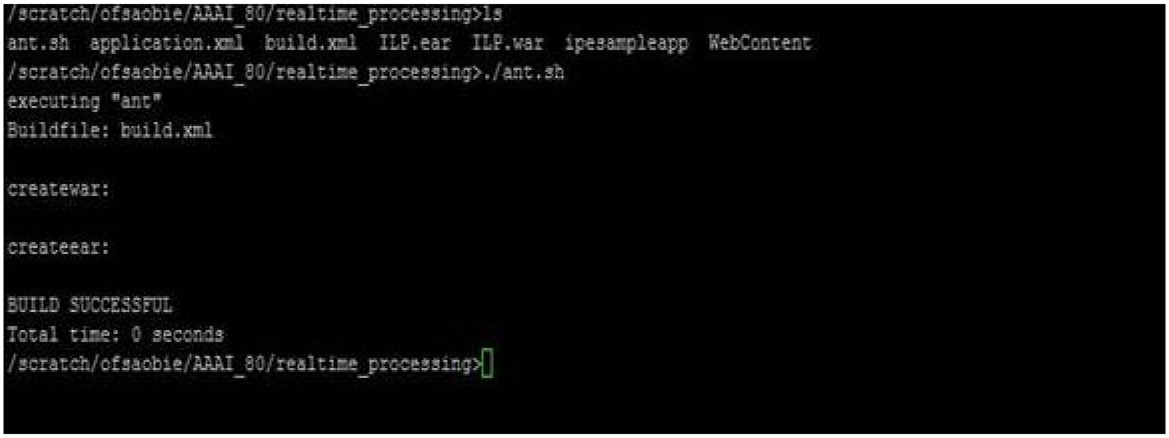
1. Navigate to `<FIC_HOME>/RealTimeFraudIPEProcessing`.
2. Execute the following command:

   ```
   ./ant.sh.
   ```

Note: Execute the following command, if the server is Tomcat:

```
./ant.sh. Tomcat
```

Figure 1–1 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>
```

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

Deploying RTFRAUD.ear

- Deploying RTFRAUD.ear in WebLogic
- Deploying RTFRAUD.ear in WebSphere
- Deploying RTFRAUD.war in Tomcat

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>.
   ```

Installing RTFRAUD.ear in WebLogic using WebLogic Administrator Console

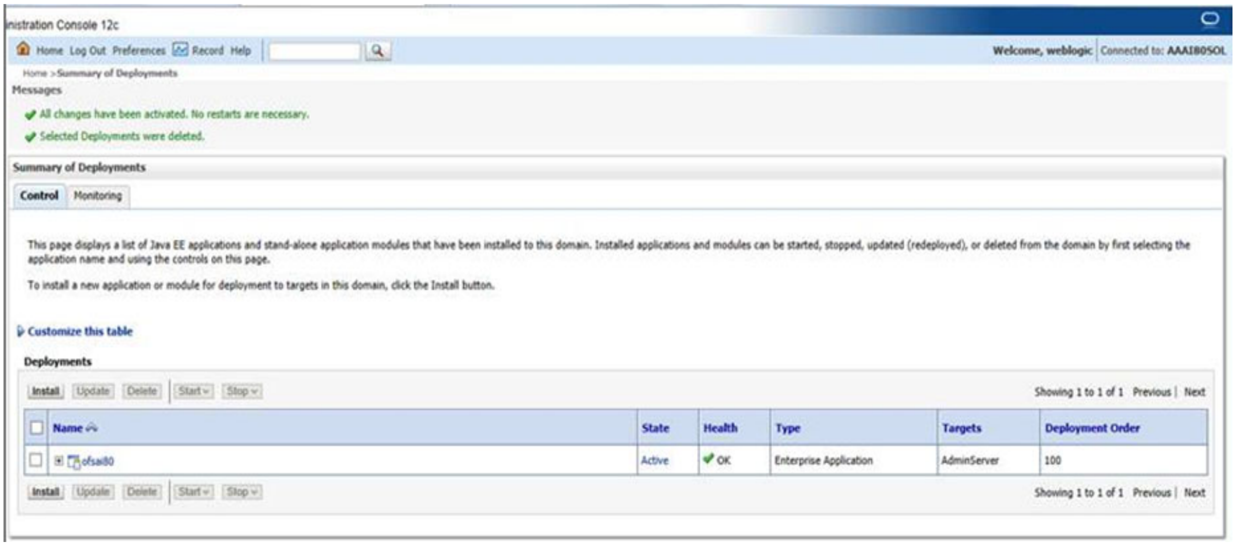
1. Navigate to the path `<WebLogic Installation directory>/user_projects/domains/<domain name>/bin` in the machine in which WebLogic is installed.
2. Start WebLogic by executing the following command:

   ```
   ./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 1–2 Summary of Deployment


nistration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: AAAI80SOL
Home >Summary of Deployments

Messages

✓ All changes have been activated. No restarts are necessary.

✓ Selected Deployments were deleted.

Summary of Deployments

This page displays a list of Java EE applications and stand-alone application modules that have been installed to this domain. Installed applications and modules can be started, stopped, updated (redeployed), or deleted from the domain by first selecting the application name and using the controls on this page.

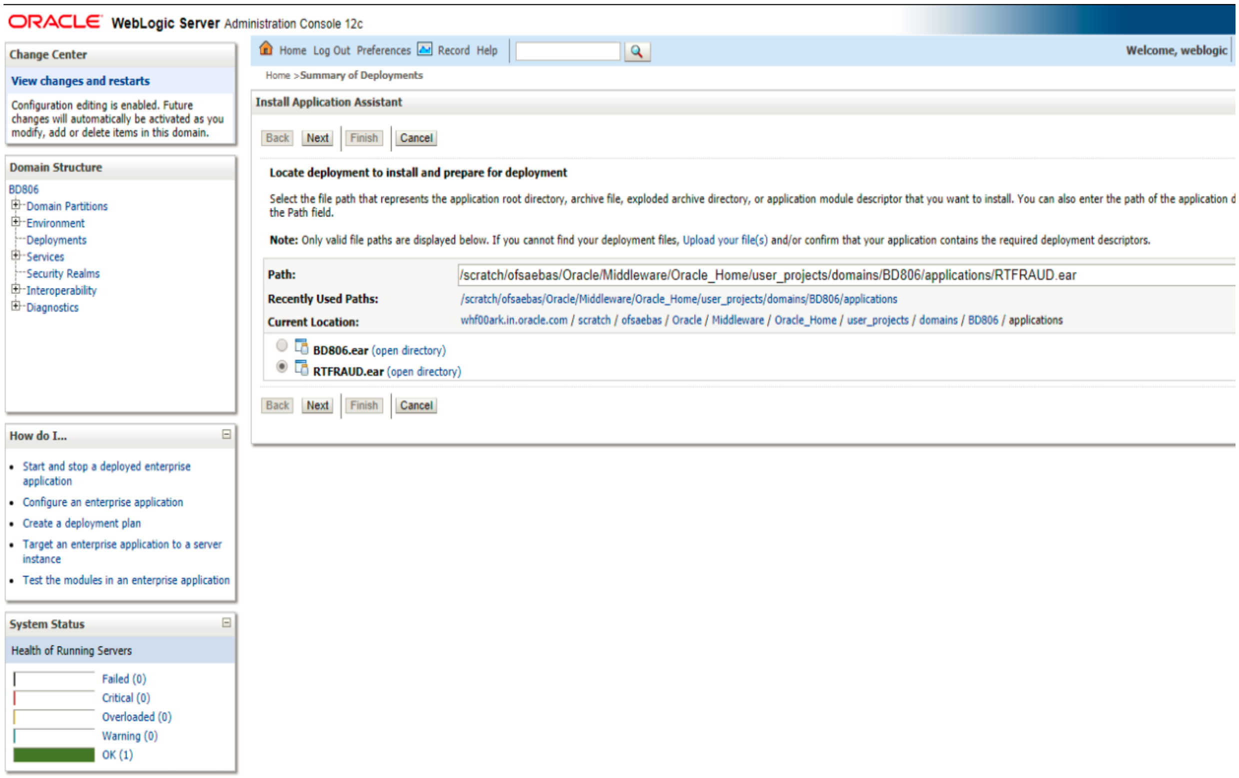
To install a new application or module for deployment to targets in this domain, click the Install button.

Deployments

□	Name	State	Health	Type	Targets	Deployment Order
□	ofsai80	Active	✓ OK	Enterprise Application	AdminServer	100

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

Figure 1–3 Install Application Assistance Window


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic
Home >Summary of Deployments

Change Center

View changes and restarts

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Domain Structure

BD806
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics

How do I...

- Start and stop a deployed enterprise application
- Configure an enterprise application
- Create a deployment plan
- Target an enterprise application to a server instance
- Test the modules in an enterprise application

System Status

Health of Running Servers

Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)

Install Application Assistant

Locate deployment to install and prepare for deployment

Select the file path that represents the application root directory, archive file, exploded archive directory, or application module descriptor that you want to install. You can also enter the path of the application d the Path field.

Note: Only valid file paths are displayed below. If you cannot find your deployment files, Upload your file(s) and/or confirm that your application contains the required deployment descriptors.

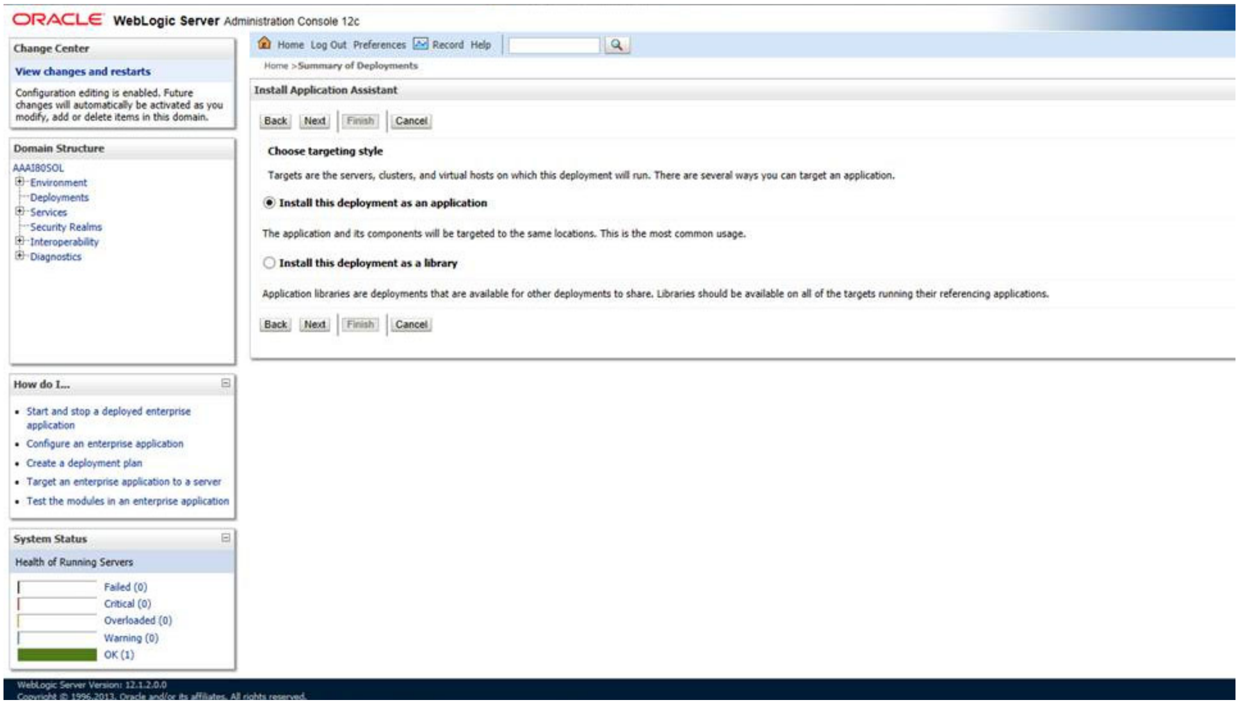
Path:	/scratch/ofsaebas/Oracle/Middleware/Oracle_Home/user_projects/domains/BD806/applications/RTFRAUD.ear
Recently Used Paths:	/scratch/ofsaebas/Oracle/Middleware/Oracle_Home/user_projects/domains/BD806/applications
Current Location:	whf00ark.in.oracle.com / scratch / ofsaebas / Oracle / Middleware / Oracle_Home / user_projects / domains / BD806 / applications

○ **BD806.ear** (open directory)

● **RTFRAUD.ear** (open directory)

6. Select `RTFRAUD.ear` and click **Next**. The Install Application Assistance page is displayed with the Choose targeting style section.

Figure 1–4   Install Application Assistance with choose Target Style


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Domain Structure
AAAI80SOL
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed enterprise application
Configure an enterprise application
Create a deployment plan
Target an enterprise application to a server
Test the modules in an enterprise application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Home Log Out Preferences Record Help
Home >Summary of Deployments
Back Next Finish Cancel
WebLogic Server Version: 12.1.2.0.0
Copyright © 1996,2013, Oracle and/or its affiliates. All rights reserved.

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Choose targeting style

Targets are the servers, clusters, and virtual hosts on which this deployment will run. There are several ways you can target an application.

● **Install this deployment as an application**

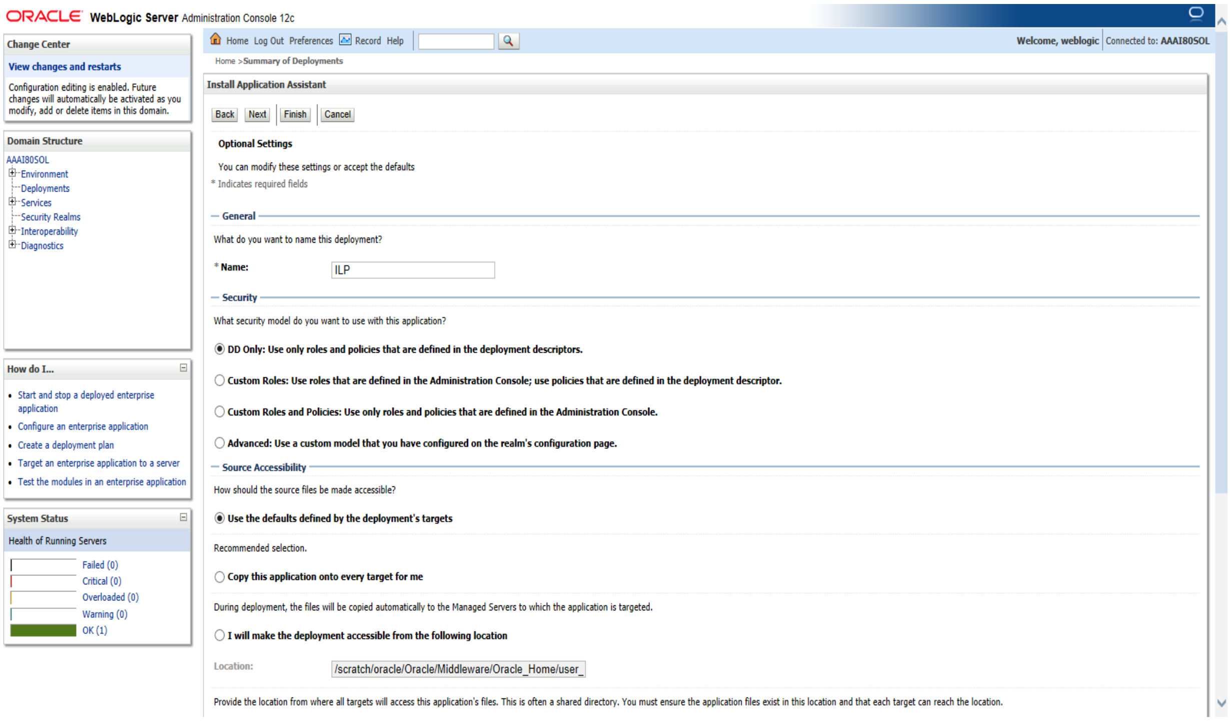
The application and its components will be targeted to the same locations. This is the most common usage.

○ **Install this deployment as a library**

Application libraries are deployments that are available for other deployments to share. Libraries should be available on all of the targets running their referencing applications.

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

Figure 1–5   Install Application Assistance page with Optional Settings


ORACLE WebLogic Server Administration Console 12c
Change Center
View changes and restarts
Domain Structure
AAAI80SOL
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed enterprise application
Configure an enterprise application
Create a deployment plan
Target an enterprise application to a server
Test the modules in an enterprise application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: AAAI80SOL
Home >Summary of Deployments
Back Next Finish Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Optional Settings

You can modify these settings or accept the defaults

* Indicates required fields

— General

What do you want to name this deployment?

* **Name:** ILP

— Security

What security model do you want to use with this application?

● **DD Only: Use only roles and policies that are defined in the deployment descriptors.**

○ **Custom Roles: Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.**

○ **Custom Roles and Policies: Use only roles and policies that are defined in the Administration Console.**

○ **Advanced: Use a custom model that you have configured on the realm's configuration page.**

— Source Accessibility

How should the source files be made accessible?

● **Use the defaults defined by the deployment's targets**

Recommended selection.

○ **Copy this application onto every target for me**

During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.

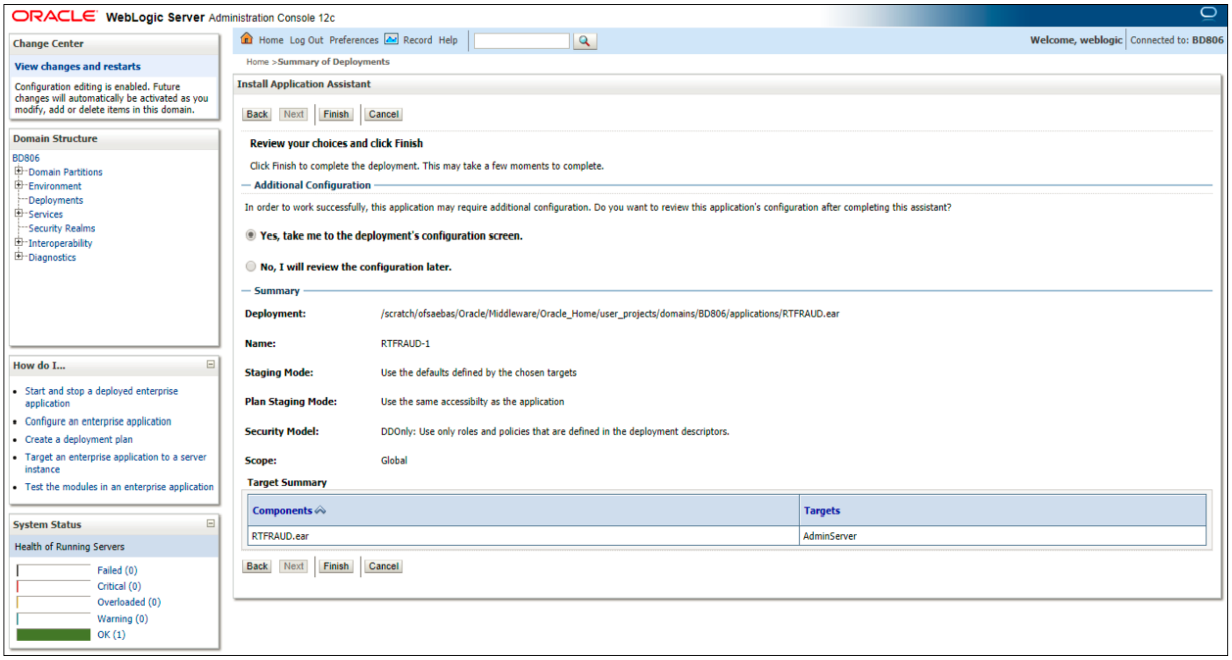
○ **I will make the deployment accessible from the following location**

Location: /scratch/oracle/Oracle/Middleware/Oracle_Home/user_

Provide the location from where all targets will access this application's files. This is often a shared directory. You must ensure the application files exist in this location and that each target can reach the location.

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

Figure 1–6 Install Application Assistance page with Review your choices and click Finish section


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic | Connected to: BD806
Home >Summary of Deployments
Change Center
View changes and restarts
Domain Structure
BD806
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop a deployed enterprise application
Configure an enterprise application
Create a deployment plan
Target an enterprise application to a server instance
Test the modules in an enterprise application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
OK (1)
Back Next Finish Cancel

Configuration editing is enabled. Future changes will automatically be activated as you modify, add or delete items in this domain.

Install Application Assistant

Review your choices and click Finish

Click Finish to complete the deployment. This may take a few moments to complete.

Additional Configuration

In order to work successfully, this application may require additional configuration. Do you want to review this application's configuration after completing this assistant?

● Yes, take me to the deployment's configuration screen.

○ No, I will review the configuration later.

Summary

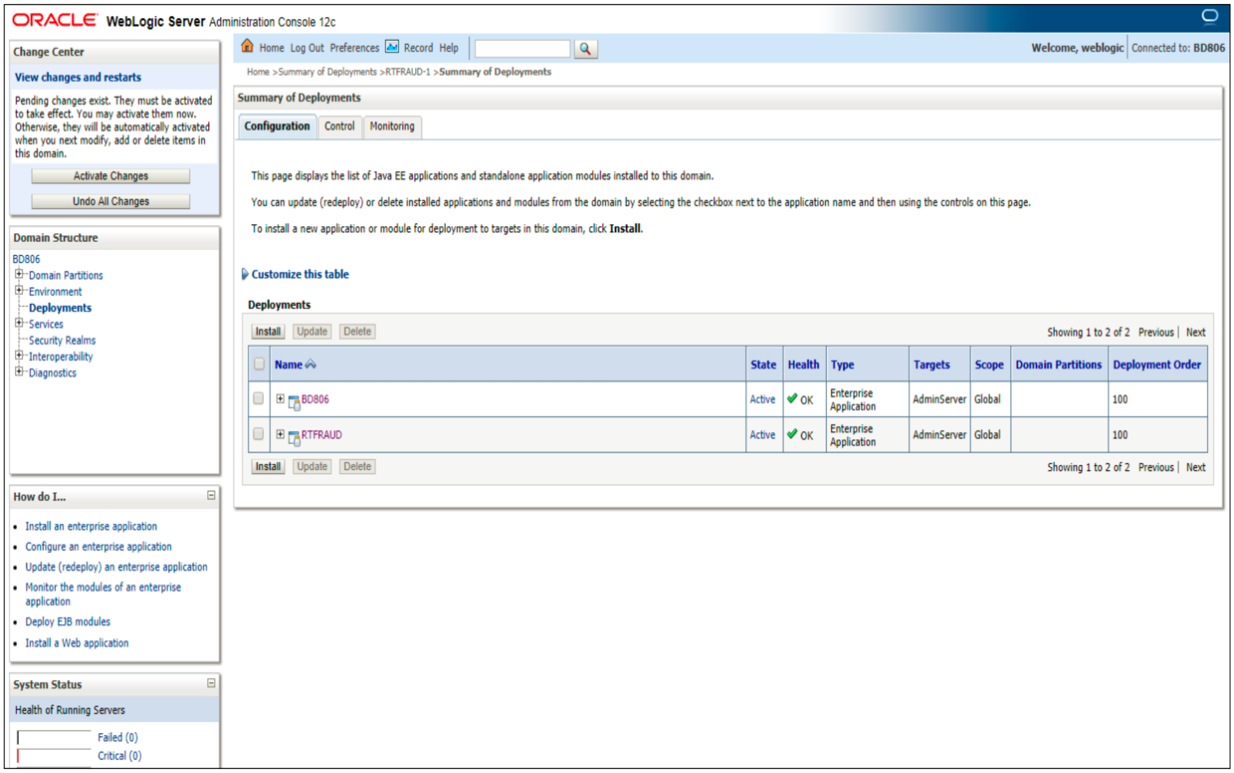
Deployment:	/scratch/ofsaebas/Oracle/Middleware/Oracle_Home/user_projects/domains/BD806/applications/RTFRAUD.ear
Name:	RTFRAUD-1
Staging Mode:	Use the defaults defined by the chosen targets
Plan Staging Mode:	Use the same accessibilty as the application
Security Model:	DDOnly: Use only roles and policies that are defined in the deployment descriptors.
Scope:	Global

Target Summary

Components	Targets
RTFRAUD.ear	AdminServer

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 following message: *The deployment has been successfully installed.*

Figure 1–7 Summary of Deployment page with RTFRAUD


ORACLE WebLogic Server Administration Console 12c
Home Log Out Preferences Record Help
Welcome, weblogic
Connected to: BD806
Home >Summary of Deployments >RTFRAUD-1 >Summary of Deployments
Change Center
View changes and restarts
Activate Changes
Undo All Changes
Domain Structure
BD806
Domain Partitions
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Install an enterprise application
Configure an enterprise application
Update (redeploy) an enterprise application
Monitor the modules of an enterprise application
Deploy EJB modules
Install a Web application
System Status
Health of Running Servers
Failed (0)
Critical (0)
Summary of Deployments
Configuration
Control
Monitoring
Customize this table
Install
Update
Delete
Showing 1 to 2 of 2 Previous | Next

Pending changes exist. They must be activated to take effect. You may activate them now. Otherwise, they will be automatically activated when you next modify, add or delete items in this domain.

This page displays the list of Java EE applications and standalone application modules installed to this domain.

You can update (redeploy) or delete installed applications and modules from the domain by selecting the checkbox next to the application name and then using the controls on this page.

To install a new application or module for deployment to targets in this domain, click **Install**.

Deployments

□	Name	State	Health	Type	Targets	Scope	Domain Partitions	Deployment Order
□	BD806	Active	✓ OK	Enterprise Application	AdminServer	Global		100
□	RTFRAUD	Active	✓ OK	Enterprise Application	AdminServer	Global		100

10. Restart all OFS AAAI servers.

Deploying 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.

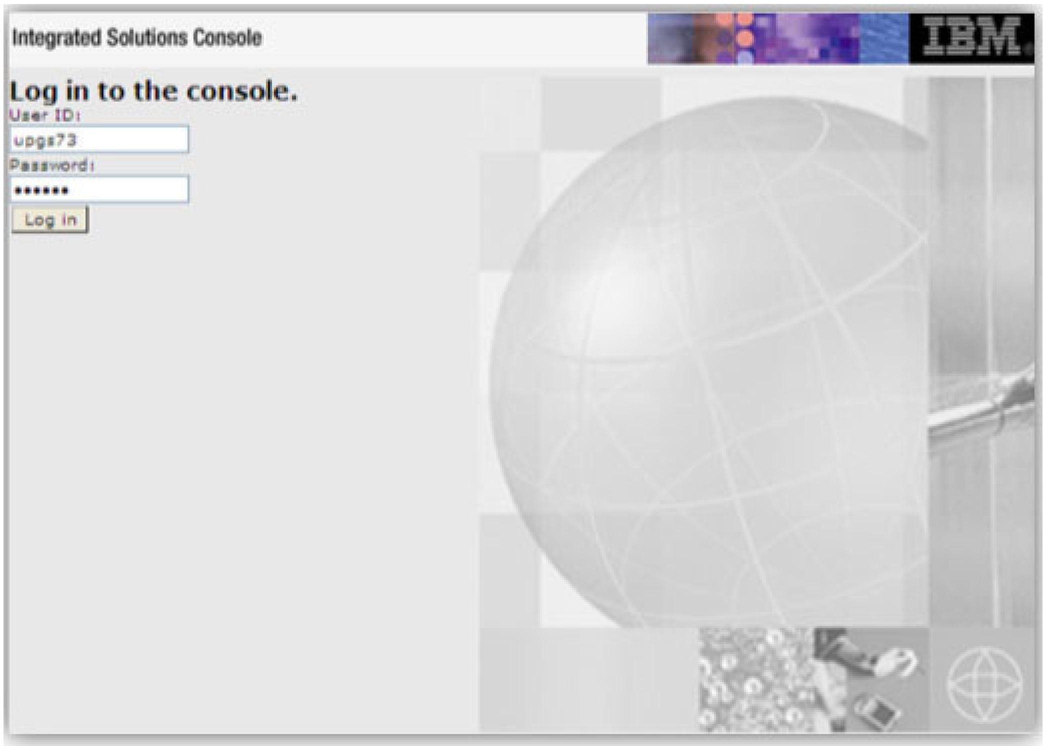
To deploy `RTFRAUD.ear` in WebSphere, follow these steps:

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
   ```

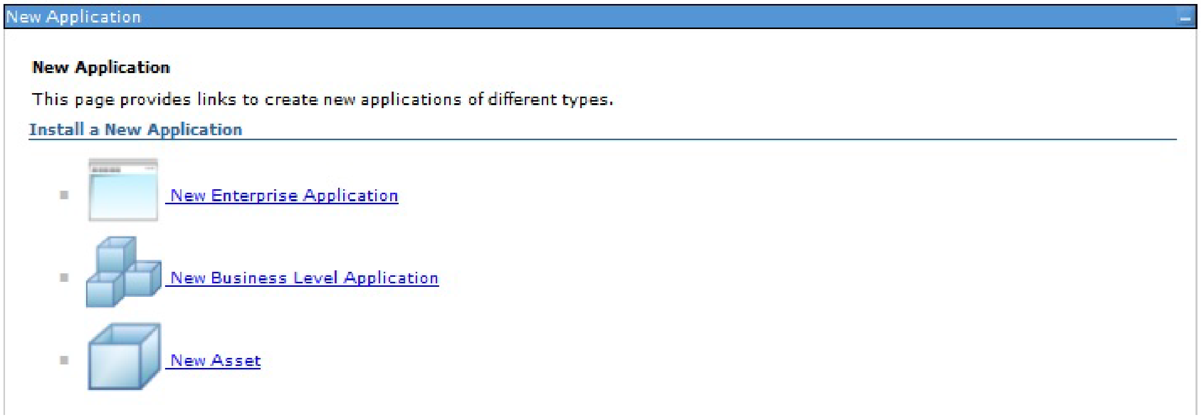
2. Open the following URL in the browser: `http://<ipaddress>:<Administrative Console Port>/ibm/console`. (use https protocol if SSL is enabled). The login screen is displayed.

Figure 1–8 WebSphere Login Window



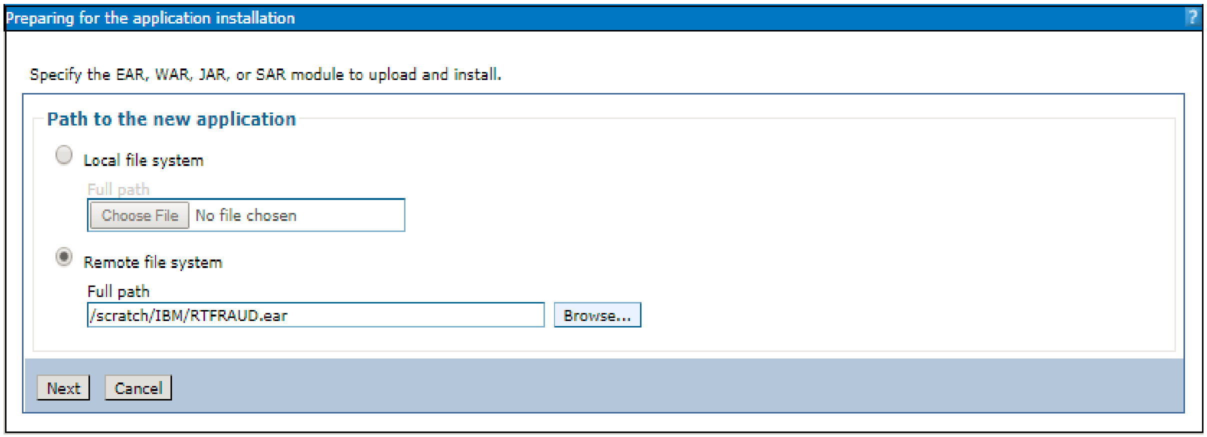
3. Enter the user credentials which has administrator rights and click **Log In**.
4. From the LHS menu, select **Applications** and click **New Application**. The New Application window is displayed.

Figure 1–9 New Application


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

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

Figure 1–10 Preparing for the application installation



Preparing for the application installation

Specify the EAR, WAR, JAR, or SAR module to upload and install.

Path to the new application

○ Local file system

Full path

Choose File No file chosen

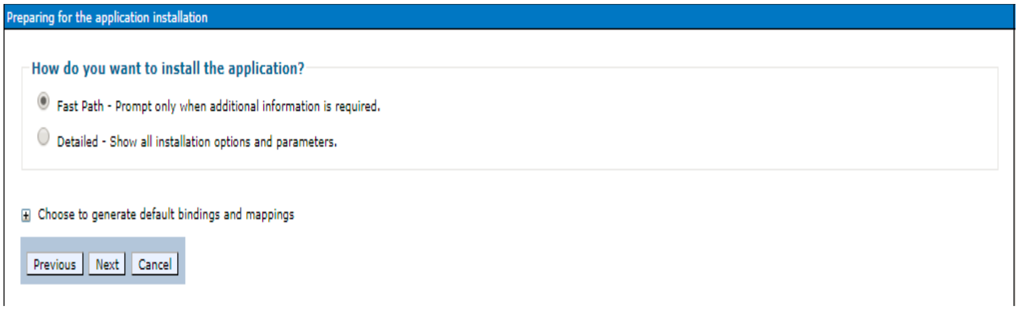
● Remote file system

Full path

/scratch/IBM/RTFRAUD.ear

6. Select **Remote File System** and click **Browse**. Select the EAR file generated for RTFRAUD to upload and install. Click **Next**.

Figure 1–11 Installation Options



Preparing for the application installation

How do you want to install the application?

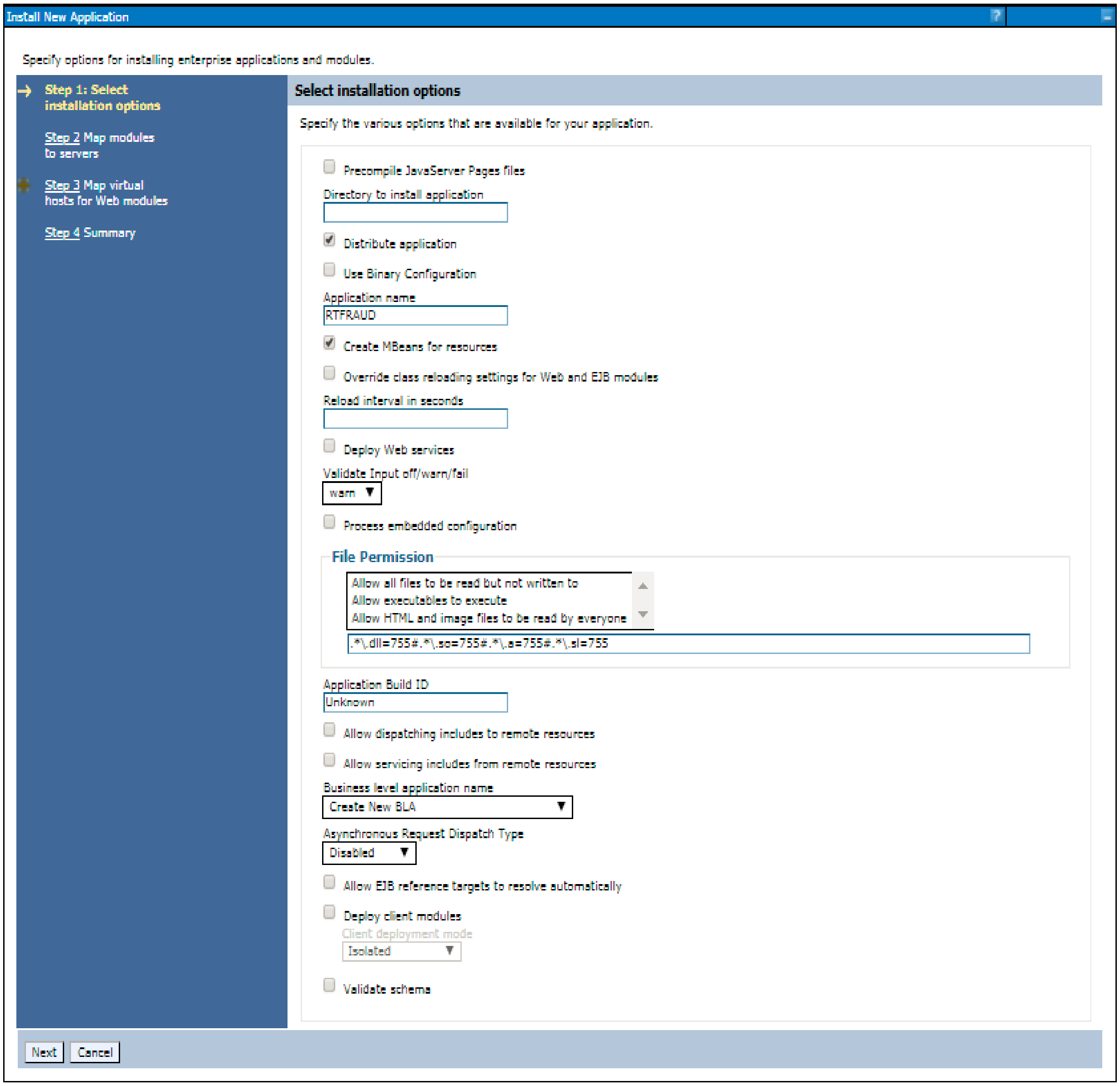
● Fast Path - Prompt only when additional information is required.

○ Detailed - Show all installation options and parameters.

⊞ Choose to generate default bindings and mappings

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

Figure 1–12 Install New Application


Install New Application
?
Step 1: Select installation options
Step 2 Map modules to servers
Step 3 Map virtual hosts for Web modules
Step 4 Summary
Next
Cancel

Specify options for installing enterprise applications and modules.

Select installation options

Specify the various options that are available for your application.

□ Precompile JavaServer Pages files

Directory to install application:

☑ Distribute application

□ Use Binary Configuration

Application name: RTFRAUD

☑ Create MBeans for resources

□ Override class reloading settings for Web and EJB modules

Reload interval in seconds:

□ Deploy Web services

Validate Input off/warn/fail: warn

□ Process embedded configuration

File Permission

Allow all files to be read but not written to
Allow executables to execute
Allow HTML and image files to be read by everyone

.*\.dll=755#.*\.so=755#.*\.a=755#.*\.sl=755

Application Build ID: Unknown

□ Allow dispatching includes to remote resources

□ Allow servicing includes from remote resources

Business level application name: Create New BLA

Asynchronous Request Dispatch Type: Disabled

□ Allow EJB reference targets to resolve automatically

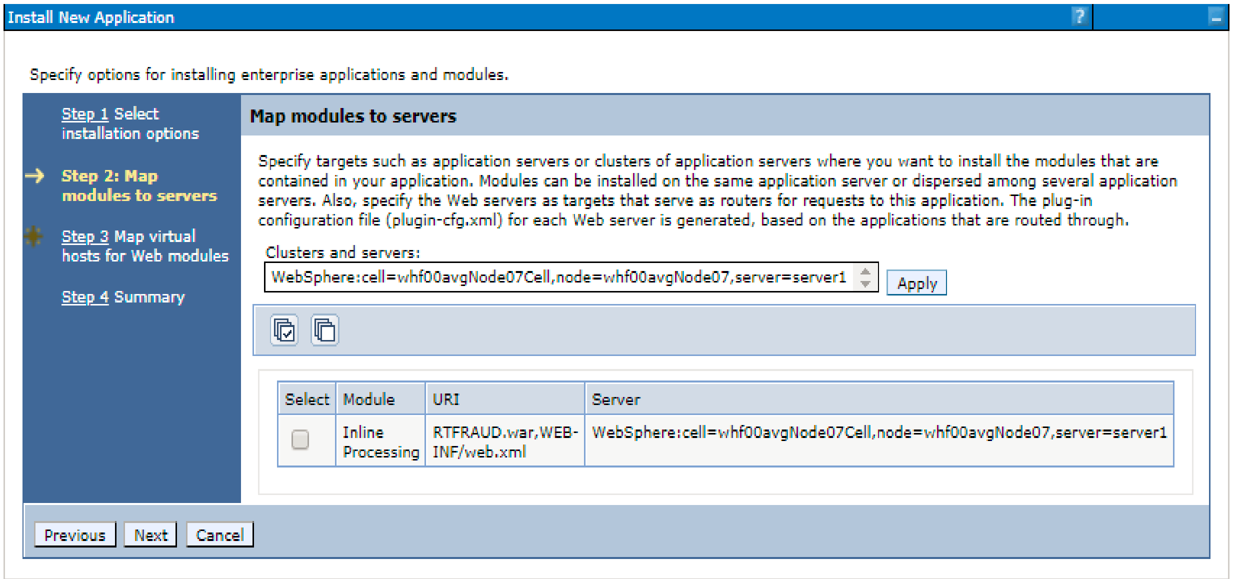
□ Deploy client modules

Client deployment mode: Isolated

□ Validate schema

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

Figure 1–13 Map Modules to Servers


Install New Application
?
Step 1 Select installation options
Step 2: Map modules to servers
Step 3 Map virtual hosts for Web modules
Step 4 Summary
Apply
Previous
Next
Cancel

Specify options for installing enterprise applications and modules.

Map modules to servers

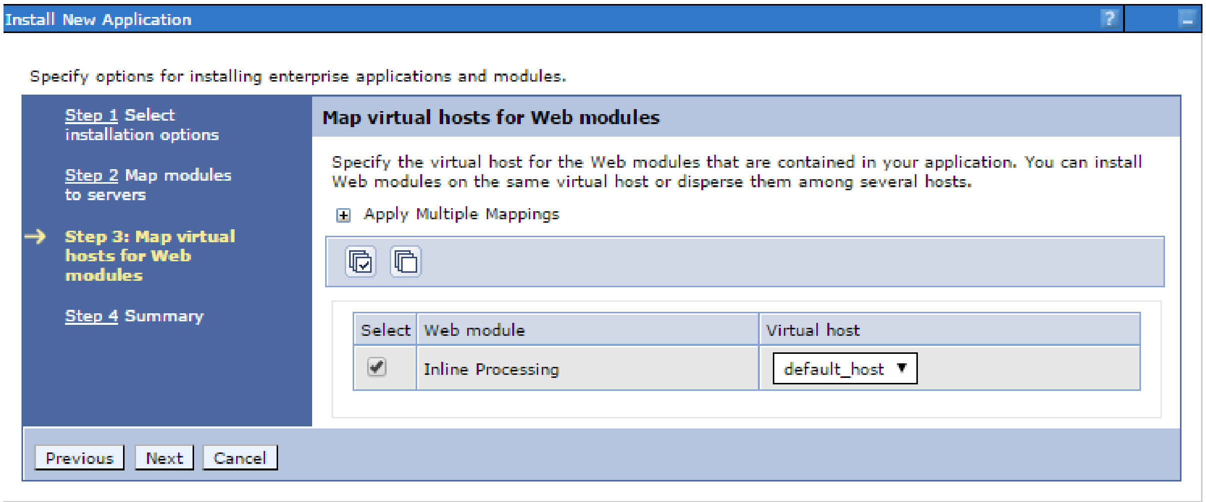
Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispersed among several application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based on the applications that are routed through.

Clusters and servers:
WebSphere:cell=whf00avgNode07Cell,node=whf00avgNode07,server=server1

Select	Module	URI	Server
☐	Inline Processing	RTFRAUD.war,WEB-INF/web.xml	WebSphere:cell=whf00avgNode07Cell,node=whf00avgNode07,server=server1

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

Figure 1–14 Map Virtual hosts for Web modules page


Install New Application
?
Step 1 Select installation options
Step 2 Map modules to servers
Step 3: Map virtual hosts for Web modules
Step 4 Summary
Previous
Next
Cancel

Specify options for installing enterprise applications and modules.

Map virtual hosts for Web modules

Specify the virtual host for the Web modules that are contained in your application. You can install Web modules on the same virtual host or disperse them among several hosts.

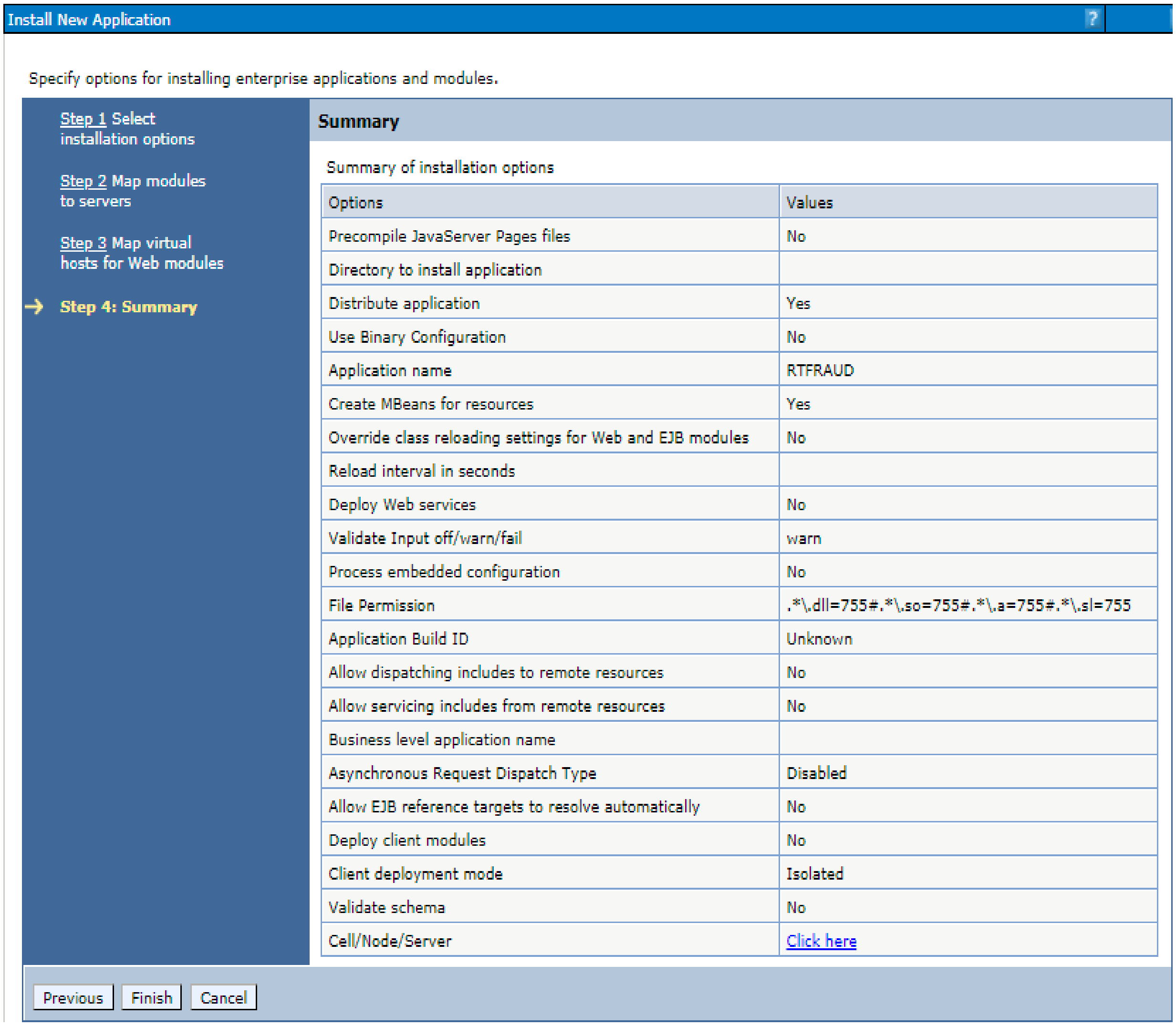
⊞ Apply Multiple Mappings

Select	Web module	Virtual host
☑	Inline Processing	default_host ▼

10. Select the **Inline Processing** check box and click **Next**. The Metadata for modules page is displayed.

11. Select the **Metadata-complete** attribute check box and click **Next**. The Summary page is displayed.

Figure 1–15 Summary page



Install New Application
?
Step 1 Select installation options
Step 2 Map modules to servers
Step 3 Map virtual hosts for Web modules
Step 4: Summary
Previous
Finish
Cancel

Specify options for installing enterprise applications and modules.

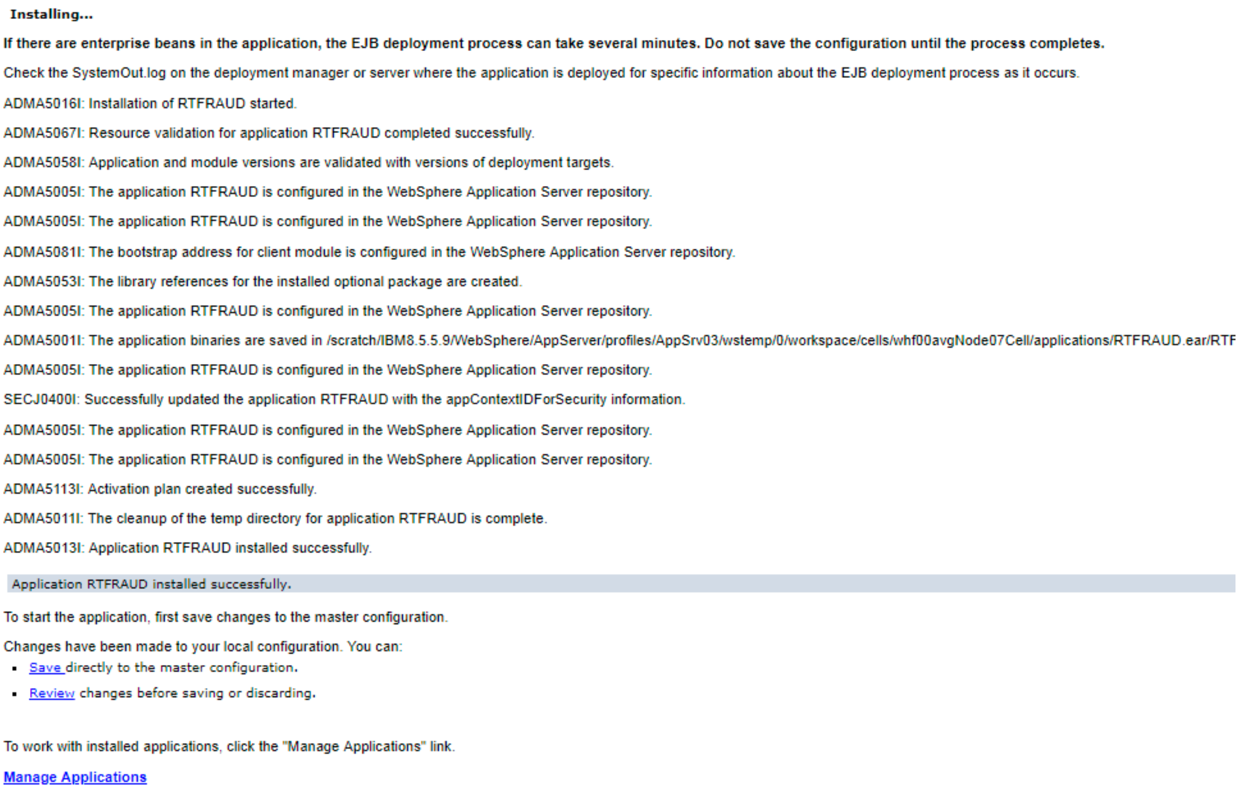
Summary

Summary of installation options

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

12. Click **Finish**. On successful installation, a message is displayed.

Figure 1–16 Installation Success



Installing...

If there are enterprise beans in the application, the EJB deployment process can take several minutes. Do not save the configuration until the process completes.

Check the SystemOut.log on the deployment manager or server where the application is deployed for specific information about the EJB deployment process as it occurs.

```
ADMA5016I: Installation of RTFRAUD started.
ADMA5067I: Resource validation for application RTFRAUD completed successfully.
ADMA5058I: Application and module versions are validated with versions of deployment targets.
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
ADMA5081I: The bootstrap address for client module is configured in the WebSphere Application Server repository.
ADMA5053I: The library references for the installed optional package are created.
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
ADMA5001I: The application binaries are saved in /scratch/IBM8.5.5.9/WebSphere/AppServer/profiles/AppSrv03/wstemp/0/workspace/cells/whf00avgNode07Cell/applications/RTFRAUD.ear/RTF
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
SECJ0400I: Successfully updated the application RTFRAUD with the appContextIDForSecurity information.
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
ADMA5005I: The application RTFRAUD is configured in the WebSphere Application Server repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application RTFRAUD is complete.
ADMA5013I: Application RTFRAUD installed successfully.
```

Application RTFRAUD installed successfully.

To start the application, first save changes to the master configuration.

Changes have been made to your local configuration. You can:

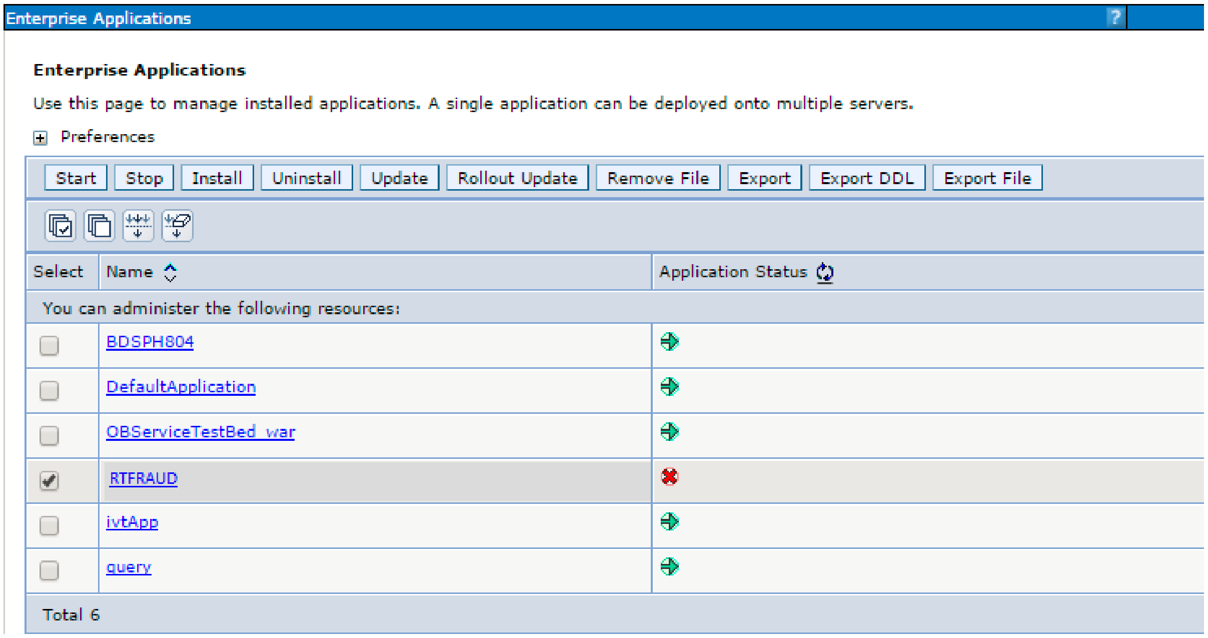
- Save directly to the master configuration.
- Review changes before saving or discarding.

To work with installed applications, click the "Manage Applications" link.

Manage Applications

13. Click **Save** and save the master file configuration. The details are displayed in the *Master File Configuration* page.

Figure 1–17 Master File Configuration page



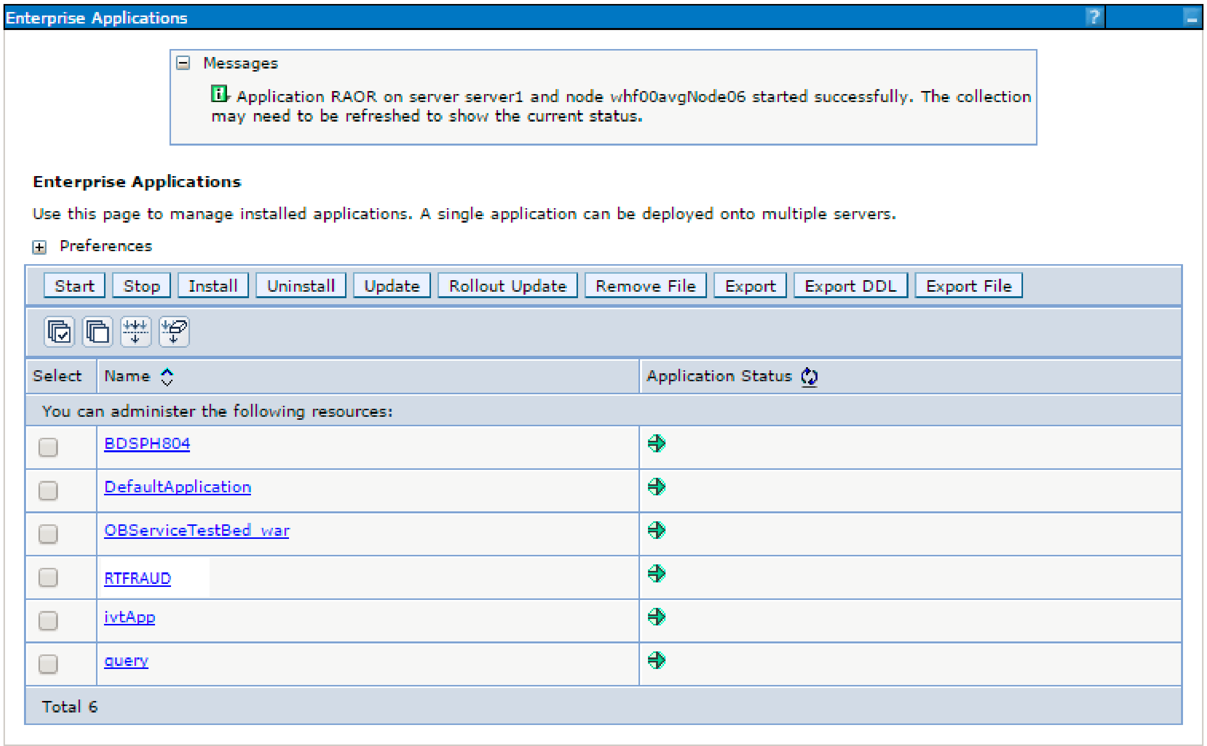
Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
☐	BDSPH804	➔
☐	DefaultApplication	➔
☐	OBServiceTestBed_war	➔
☑	RTFRAUD	✖
☐	ivtApp	➔
☐	query	➔
Total 6		

14. Select RTFRAUD and click **Start**. The Enterprise Application page is displayed with confirmation message.

Figure 1–18 Enterprise Application page with Confirmation message



Application RAOR on server server1 and node whf00avgNode06 started successfully. The collection may need to be refreshed to show the current status.

Enterprise Applications

Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Select	Name	Application Status
You can administer the following resources:		
□	BDSPH804	➔
□	DefaultApplication	➔
□	OBServiceTestBed_war	➔
□	RTFRAUD	➔
□	ivtApp	➔
□	query	➔
Total 6		

15. Restart all OFS AAAI servers.

Deploying RTFRAUD.war in Tomcat

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

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

2

Managing User Administration and Security Configuration

This chapter provides instructions for setting up and configuring Real Time Fraud component.

This chapter focuses on the following topics:

- About User Administration
- User Provisioning Process Flow
- Managing User Administration
- Adding Security Attributes
- Mapping Security Attributes to Organization and Users

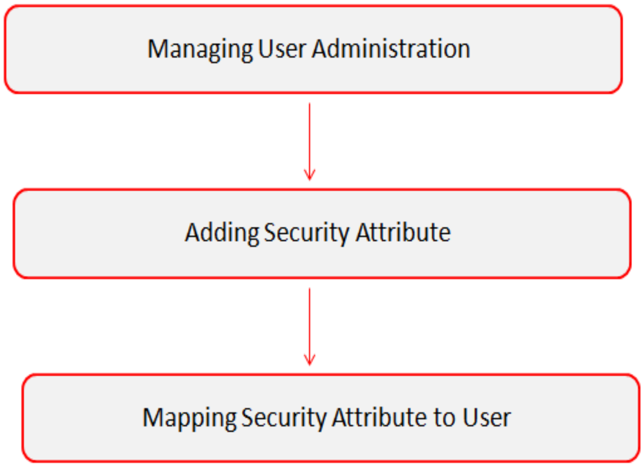
About User Administration

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

User Provisioning Process Flow

Figure 2–1 User Provisioning Process Flow


Managing User Administration
Adding Security Attribute
Mapping Security Attribute to User

The following table lists the various actions and associated descriptions of the user administration process flow:

Table 2–1 User Provisioning Process Flow

Action	Description
Managing User Administration	Create and map users to user groups. This allows Administrators to provide access, monitor, and administer users.
Adding Security Attributes	Load security attributes. Security attributes are loaded using either Excel or SQL scripts.
Mapping Security Attributes to Organization and Users	Map security attributes to users. This is done to determine which security attributes control the user's access rights.

Managing User Administration

This section allows you to create, map, and authorize users defining a security framework which has the ability to restrict access to the Real Time Fraud component.

Managing Identity and Authorization

This section explains how to create a user and provide access to the Real Time Fraud component.

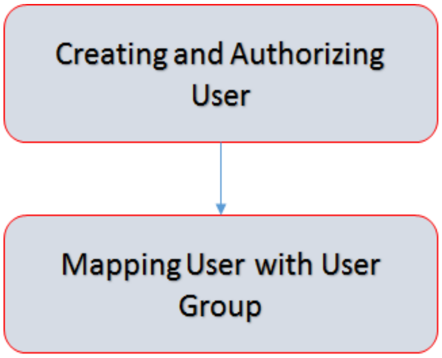
This section covers the following topics:

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

Managing Identity and Authorization Process Flow

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

Figure 2–2 Managing Identity and Authorization Process Flow



The following table lists the various actions and associated descriptions of the user administration process flow:

Table 2–2 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.

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*.

Mapping a User with a User Group

This section explains how to map Users and User Groups. With this, the user has access to the privileges as per the role. The SYSADMN user maps a user to a user group in Real Time Fraud. The following table describes the predefined Fraud User Roles and corresponding User Groups.

Table 2–3 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 application and take action on transactions	Fraud Admin
Fraud Analyst	Access Fraud application and take action on transactions	Fraud Analyst

Adding Security Attributes

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

About Security Attributes

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

You need to map the roles with access privileges, and 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.

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**: Division of data based on different 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 be used to identify records of different business types such as Private Client verses Retail customer, or to provide more granular restrictions to data such as employee data.

- **Scenario Group**

  Scenario groups are used for data access controls. A scenario group refers to a group of scenarios in the Real Time Fraud applications that identify a set of scenario permissions and to which a user has access rights.

- **Case Type/Sub Type**

  If your firm has implemented Real Time Fraud, you must establish access permissions associated with the available Case Types and Subtypes. The Case Type/Subtype is used for data access controls similar to business domains, but has a different objective. The Case Type/Subtype can be used to identify records of different case types or to provide more granular restrictions to data such as case data.

- **Organization**

  Organizations are used for data access controls. Organizations are user group to which a user belongs.

Mapping Security Attributes to Organization and Users

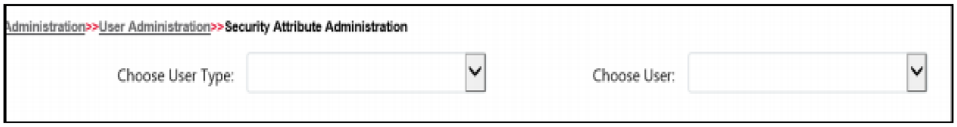
The Mapping Security Attributes to Users functionality section enables you to determine which security attribute controls a user's access. Using this UI, an Administrator can map both Organizations and Users to different Security attributes.

To map a Security Attribute, follow these steps:

1. Login as the Mantas Administrator. The OFSAAI Applications page is displayed.
2. Click Financial Services Money Laundering.
3. In the Navigation List, select Behavior Detection, then select Administration. The Anti Money Laundering page is displayed.
4. Hover mouse over the Administration menu, select the User Administration sub-menu, and click **Security Attribute Administration**. The Security Attribute Administration page is displayed.
5. Select user type from Choose User Type drop-down list. The following options are available:
   - Organization
   - User

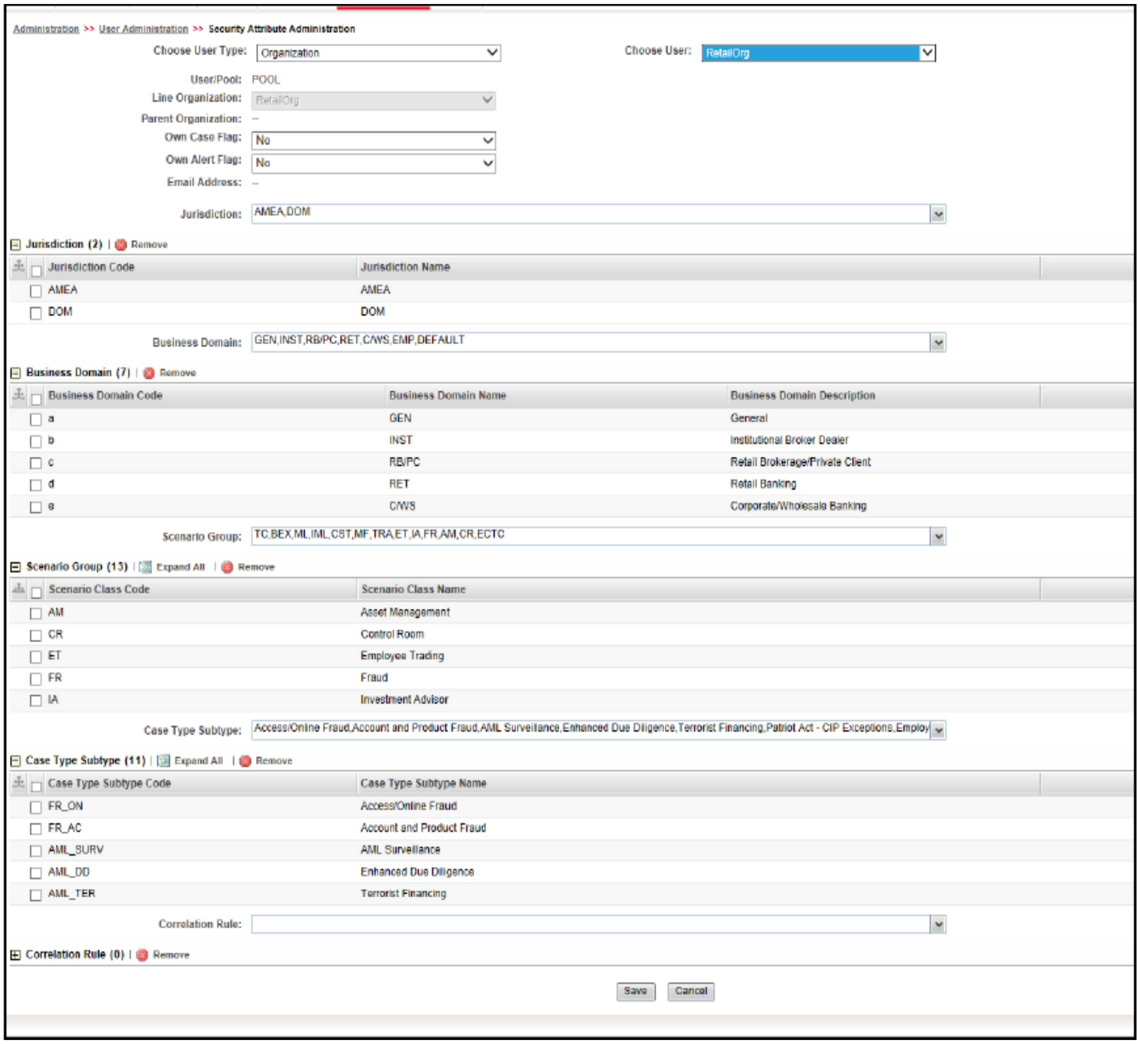
   Note: Before proceeding with providing a user access through this UI, ensure that you have created a user and all necessary data is available in the appropriate database tables.**:**

Figure 2–3 Security Attribute Administration


Administration>>User Administration>>Security Attribute Administration
Choose User Type:
Choose User:

Depending on the User Type you have selected, the available options in the Choose User drop down list is updated. Select the user from Choose User drop-down list. The relevant Security Attribute Administration page is displayed.

Figure 2–4 Security Attribute Administration



Administration >> User Administration >> Security Attribute Administration

Choose User Type: Organization

Choose User: RetailOrg

User/Pool: POOL

Line Organization: RetailOrg

Parent Organization: --

Own Case Flag: No

Own Alert Flag: No

Email Address: --

Jurisdiction: AMEA,DOM

⊟ Jurisdiction (2) | Remove

□	Jurisdiction Code	Jurisdiction Name
□	AMEA	AMEA
□	DOM	DOM

Business Domain: GEN,INST,RB/PC,RET,C/WS,EMP,DEFAULT

⊟ Business Domain (7) | Remove

□	Business Domain Code	Business Domain Name	Business Domain Description
□	a	GEN	General
□	b	INST	Institutional Broker Dealer
□	c	RB/PC	Retail Brokerage/Private Client
□	d	RET	Retail Banking
□	e	C/WS	Corporate/Wholesale Banking

Scenario Group: TC,BEX,ML,IML,CST,MF,TRA,ET,IA,FR,AM,CR,ECTC

⊟ Scenario Group (13) | Expand All | Remove

□	Scenario Class Code	Scenario Class Name
□	AM	Asset Management
□	CR	Control Room
□	ET	Employee Trading
□	FR	Fraud
□	IA	Investment Advisor

Case Type Subtype: Access/Online Fraud,Account and Product Fraud,AML Surveilance,Enhanced Due Diligence,Terrorist Financing,Patriot Act - CIP Exceptions,Employ

⊟ Case Type Subtype (11) | Expand All | Remove

□	Case Type Subtype Code	Case Type Subtype Name
□	FR_ON	Access/Online Fraud
□	FR_AC	Account and Product Fraud
□	AML_SURV	AML Surveillance
□	AML_DD	Enhanced Due Diligence
□	AML_TER	Terrorist Financing

Correlation Rule:

⊞ Correlation Rule (0) | Remove

Note: In order to update the user profiles before proceeding with mapping any security attributes, select User from the Choose User Type drop-down list. When chosen, all the updates made to all the user profiles through User Maintenance UI are imported from the CSSMS_USER_PROFILE table of the OFS AAI ATOMIC schema to the KDD_REVIEW_OWNER table of the ATOMIC schema.

If you delete a user through the Security Management application screen, you must come back to the Security Attribute Administration screen and select the value User from the Choose User Type drop-down list. Then the deleted user is updated in the KDD_REVIEW_OWNER table against the column actv_flg as N, and that user is inactive.

Table 2–4 Security Attributes

Fields	Description
Organization	Select an organization from the drop-down list. A User or Organization's access to other Organizations depends on the selection(s) made for this organization parameter, such as, if a user is mapped to Org1 and Org2, it implies that this user can access alerts which belong to these two organizations, provided other security attributes are also matching.
Own Case Flag	Select whether this user type will own a case flag from the drop-down list.
Own Alert Flag	Select whether this user type will own a alert flag from the drop-down list.
Note: The Own Alert and Case flag is required for taking ownership of the alerts and cases. If an alert user must perform a Promote To Case action, then the following prerequisites should be fulfilled. The user should be mapped to any one of the following user groups: • Case Supervisor • Case Analyst1 • Case Analyst2	
Business Organization	The default Business Organization is displayed, but you can select the business organization from the drop-down list.
Jurisdictions	Select the jurisdictions from the drop-down list. Mapping of one or more jurisdictions to a user or organization allows this user or organization to access cases, alerts, watch lists, and watch list members that belong to the mapped jurisdiction. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Business Domain	Select the business domains from the drop-down list. Mapping of one or more business domains to a user or organization allows this user or organization to access cases, alerts, watch lists, and watch list members that belong to the mapped business domains. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Scenario Group	Select the scenario group from the drop-down list. Mapping of one or more Scenario Groups to a user or organization allows this user or organization to access alerts that belong to the mapped scenario Group. The selected jurisdictions are displayed in Jurisdictions section after you save your selection.
Case Type/Subtype	Select the case type/subtype from the drop-down list. Mapping of one or more Case Types/Subtypes to a user or organization allows this user or organization to access cases that belong to the mapped Case Type/Subtype. The selected jurisdictions are displayed in Case Types/Subtypes section after you save your selection. This is only applicable if your firm has implemented Enterprise Case Management.
Correlation Rule	Select the correlation rule from the drop-down list. Mapping of one or more correlation rules allows the user to view the correlations generated based on the mapped correlation. The selected jurisdictions are displayed in correlation section after you save your selection.

6. Click **Save**. The following confirmation message displays: *Would you like to save this action?*
7. Click **OK**. The following confirmation message displays: *The update operation successful.*
8. Click **OK**. The updated *Security Attribute* page is displayed.

Removing Security Attributes

This section allows you to delete the mapped security with Users.

To remove security attributes, follow these steps:

1. Navigate to the *Security Attributes* page.
2. Select one or more check boxes in the respective security attributes such as Business Domain, Jurisdictions, and so on.
3. Click Remove. The following confirmation message displays: *Are you sure you want to delete this records?*
4. Click **OK**. The selected record is deleted from the list.
5. Click **Save**. The changes are updated.

3

Managing Administration for Real Time Fraud

This chapter provides information about administrator tasks required to set up Real Time Fraud component. This section includes the following:

- Operating RTFraud Service
- Manage RT Fraud Scenarios/Rules

Operating RTFraud Service

This section explains about RTFraud Service

- RTFraud Service Request
- RTFraud Service Response

RTFraud Service Request

The client must provide input to the RTFraud service by posting relevant attributes into the IPE REST Service using the following URL:

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

The attributes must be in JSON format. For sample JSON input, see Appendix A, "Sample JSON"

Following is the structure of the RTFraud message attributes:

Table 3–1 RTFraud Message Attributes

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

Following is the structure of the RTFraud request attributes:

Table 3–2 RTFraud Request Attributes

Request Attributes	Description
From Latitude	Indicates the latitude unit that represent geographic coordinates of the location from where the transaction is initiated.
From Longitude	Indicates the longitude unit that represent geographic coordinates of the location from where the transaction is initiated.

Table 3–2 RTFraud Request Attributes

Request Attributes	Description
To Latitude	Indicates the latitude unit that represent geographic coordinates of the location where the transaction ends.
To Longitude	Indicates the longitude unit that represent 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, 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 Organisation 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.
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.

Table 3–2 RTFraud Request Attributes

Request Attributes	Description
ACH Batch ID	Indicates the Batch ID number if ACH payment type is used for the transaction.
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 BIC (Bank Identifier Code) of the sender in a transaction.
Receiver	Indicates the BIC (Bank Identifier Code) of the receiver in a transaction.
Debited Branch	Indicates the branch code of the bank where amount is debited in the transaction.
Credited Branch	Indicates the branch code of the bank 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 originators party name.
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 any 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.

Table 3–2 RTFraud Request Attributes

Request Attributes	Description
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 on 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 Transaction Start Date and Transaction End Date are several hours.

RTFraud Service Response

Any input given to the RTFraud service will have a response or feedback message. The client must configure a REST Service feedback URL and expose that URL to RTFraud service in order to receive the response from RTFraud 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.

Manage RT Fraud Scenarios/Rules

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

Below are the sample out of the box fraud risk rules configured for real-time delectation:

Table 3–3 Fraud Risk Rules

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.

Table 3–3 Fraud Risk Rules

Fraud Scenarios/Rules	Description
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.

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*.

4

Managing Real Time Administration

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

Whenever a transaction satisfies the rules configured for the SLA, the user is expected to take necessary action on that transaction within the specified cut-off time. If no action is taken, then the system automatically takes action on those transactions.

This section includes the following:

- Accessing Real Time Administration
- Configuring Real Time Administration

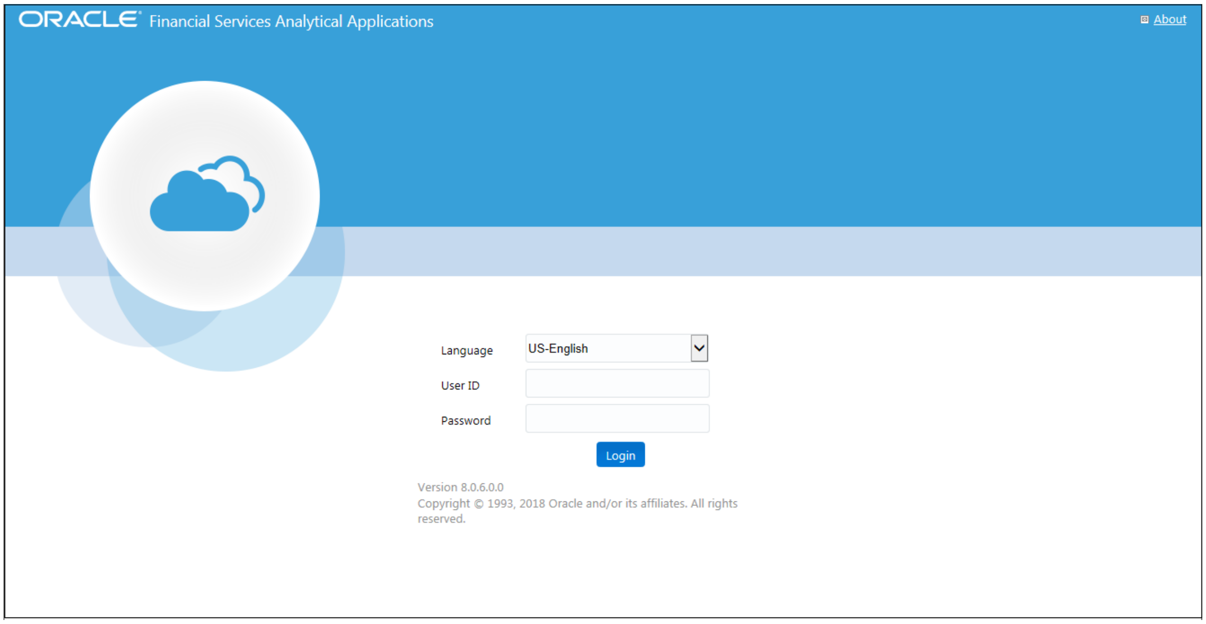
Accessing Real Time Administration

To configure Real Time Administration, you must login to Fraud Enterprise Edition application as an Administrator.

1. Enter the OFSAA URL in your browser.

   The OFSAA Login page is displayed.

Figure 4–1 OFSAA Login Page



Language: US-English

User ID

Password

Version 8.0.6.0.0
Copyright © 1993, 2018 Oracle and/or its affiliates. All rights reserved.

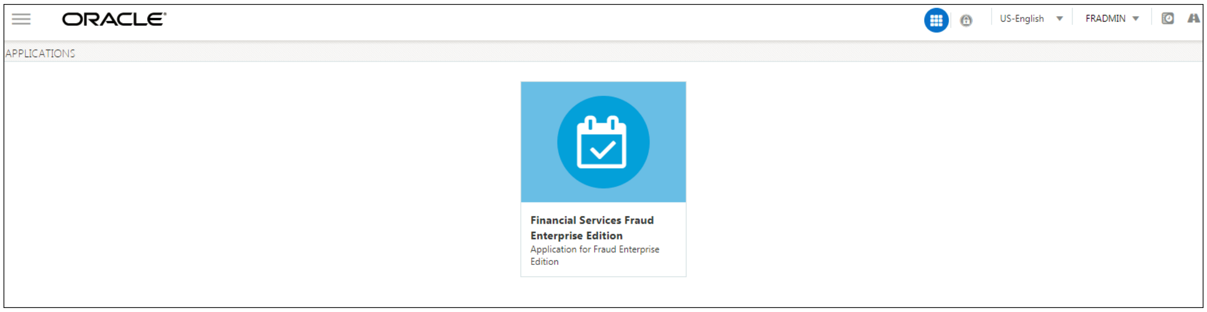
2. Select the **Language**.
3. Enter your **User ID** and **Password**.

> **Note:**
>
> Ensure to login as an Administrator.

4. Click **Login**.

   The **Applications** page is displayed.

Figure 4–2 Fraud Enterprise Edition Applications Page

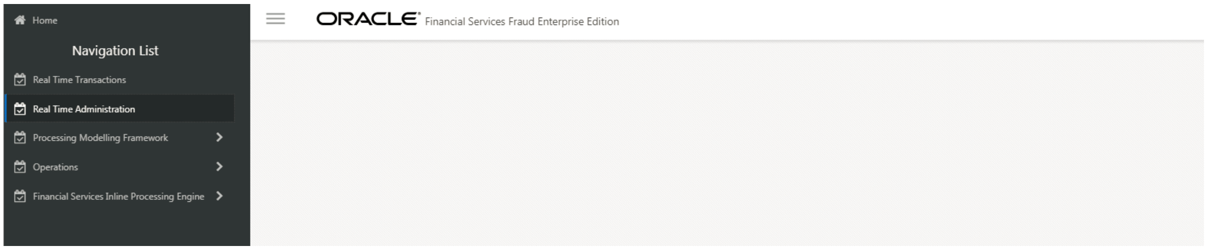


Financial Services Fraud Enterprise Edition
Application for Fraud Enterprise Edition

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

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

Figure 4–3 Fraud Enterprise Edition Home Page


Home
Navigation List
Real Time Transactions
Real Time Administration
Processing Modelling Framework
Operations
Financial Services Inline Processing Engine
ORACLE Financial Services Fraud Enterprise Edition

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

   The Real Time Administration page is displayed.

Configuring Real Time Administration

In Real Time Administration page, you can configure SLA by creating new rules and new 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 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 4–1 Create New Rule

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

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

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

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

Table 4–2 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**.

    The SLA is configured for the Real Time Fraud.

A

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": "<Input_Value>",
    "From Latitude": "<Input_Value>",
    "From Longitude": "<Input_Value>",
    "To Longitude": "<Input_Value>",
    "Account Source UniqueID": "<Input_Value>",
    "Authentication Mode": "<Input_Value>",
    "Browse Type": "<Input_Value>",
    "Current Date": "<Input_Value>",
    "Customer Source UniqueID": "<Input_Value>",
    "IP GEO Domain": "<Input_Value>",
    "IP Address": "<Input_Value>",
    "IP Address City": "<Input_Value>",
    "IP Address Country": "<Input_Value>",
    "IP GEO ISP": "<Input_Value>",
    "IP Organisation Name": "<Input_Value>",
    "IP Address State": "<Input_Value>",
    "IP GEO Autonomous System Number": "<Input_Value>",
    "IP GEO Autonomous System Organization": "<Input_Value>",
    "IP GEO Is Anonymous Proxy": "<Input_Value>",
"IP GEO User Type": "<Input_Value>",
"OS Type": "<Input_Value>",
"Referrer Site": "<Input_Value>",
"Session ID": "<Input_Value>",
"Source System Code": "<Input_Value>",
"Time": "<Input_Value>",
"User Agent": "<Input_Value>",
"Web Session Value": "<Input_Value>",
"Login Time Session": "<Input_Value>",
"Session Number": "<Input_Value>",
"Channel Info": "<Input_Value>",
"Payment Type": "<Input_Value>",
"Transaction Type Code": "<Input_Value>",
"ACH Batch ID": "<Input_Value>",
"Reoccurring Flag": "<Input_Value>",
"Message Type": "<Input_Value>",
"Message Direction": "<Input_Value>",
"Payment International Flag": "<Input_Value>",
"Credit/Debit Code": "<Input_Value>",
"Transaction unique SIQ ID": "<Input_Value>",
"Message Reference": "<Input_Value>",
"Sender": "<Input_Value>",
"Receiver": "<Input_Value>",
"Debited Branch": "<Input_Value>",
"Credited Branch": "<Input_Value>",
"Transaction Currency": "<Input_Value>",
"Transaction Amount": "<Input_Value>",
"Transaction Original Currency": "<Input_Value>",
"Transaction Original Amount": "<Input_Value>",
"Payment Value Date": "<Input_Value>",
"Originator Party AccountID/IBAN": "<Input_Value>",
"Originator Party BIC": "<Input_Value>",
"Originator Party Countrycode": "<Input_Value>",
"Originator Party Identifier": "<Input_Value>",
"Originator Party Name": "<Input_Value>",
"Counterparty AccountID/IBAN": "<Input_Value>",
"Counterparty  Name": "<Input_Value>",
    "Counterparty BIC": "<Input_Value>",
    "Counterparty Country Code": "<Input_Value>",
    "Counterparty Identifier": "<Input_Value>",
    "Involved Party 1 Type": "<Input_Value>",
    "Involved Party 1 AccountID/IBAN": "<Input_Value>",
    "Involved Party 1 Name": "<Input_Value>",
    "Involved Party 1 BIC": "<Input_Value>",
    "Involved Party 1  Country Code": "<Input_Value>",
    "Involved Party 1  Identifier": "<Input_Value>",
    "Involved Party 2 Type": "<Input_Value>",
    "Involved Party 2 AccountID/IBAN": "<Input_Value>",
    "Involved Party 2 Name": "<Input_Value>",
    "Involved Party 2 BIC": "<Input_Value>",
    "Involved Party 2  Country Code": "<Input_Value>",
    "Involved Party 2  Identifier": "<Input_Value>",
    "Involved Party 3 Type": "<Input_Value>",
    "Involved Party 3 AccountID/IBAN": "<Input_Value>",
    "Involved Party 3 Name": "<Input_Value>",
    "Involved Party 3 BIC": "<Input_Value>",
    "Involved Party 3  Country Code": "<Input_Value>",
    "Involved Party 3  Identifier": "<Input_Value>",
    "Source Country": "<Input_Value>",
    "Destination Country": "<Input_Value>",
    "Payment Information": "<Input_Value>",
    "Details of Charges": "<Input_Value>",
    "Transaction Date Start": "<Input_Value>",
    "Transaction Date End": "<Input_Value>"
  },
  "additionalParams": {}
}
```