Oracle® Banking Corporate Lending
Setup Plug-Ins

Release 14.8.0.0.0

ORACLE®

Oracle Banking Corporate Lending Setup Plug-Ins, Release 14.8.0.0.0

G29780-01

Contents

Preface

1   Set Up Plug-Ins

ORACLE®

Preface

This topic contains the following sub-topics:

- Purpose
- Audience
- Documentation Accessibility
- Critical Patches
- Diversity and Inclusion
- Related Resources
- Conventions
- Screenshot Disclaimer
- Acronyms and Abbreviations

Purpose

This guide describes the pre-deployment tasks to setup the Plug-in by manually before Oracle FLEXCUBE deployment. It provides detail information about the pre-deployment tasks based on the on the selected plug-ins.

Audience

This manual is intended for the following User/User Roles:

Table 1   Audience

Role	Function
Administrator	Who controls the system and application parameters and ensures smooth functionality and flexibility of the banking application.
Implementation team	Implementation of Oracle Banking Corporate Lending Solution
Pre-sales team	Install Oracle Banking Corporate Lending for demo purpose
Bank personnel	Who installs Oracle Banking Corporate Lending

The user of this manual is expected to have basic understanding of Oracle Banking Application installation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at https://www.oracle.com/corporate/accessibility/.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Corporate Lending User Guides.
- Oracle Banking Corporate Lending Installation Guides.

Conventions

The following text conventions are used in this document:

Table 2   Conventions

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

Acronyms and Abbreviations

The acronyms and abbreviations are listed in this below table:

Table 3   Acronyms and Abbreviations

Abbreviations or Acronyms	Definition
BAM	Business Activity Monitoring
BIP	Business Intelligence Publisher
BPEL	Business Process Execution Language
BPMN	Business Process Model and Notation
EAR	Enterprise Archive file
EM	Enterprise Manager
FTP	File Transfer Protocol
IMAP	Internet Message Access Protocol
JMS	Java Message Service
JDBC	Java Database Connectivity
JNDI	Java Naming and Directory Interface
SOA	Service-Oriented Architecture
SMTP	Simple Mail Transfer Protocol

ORACLE®

1

Set Up Plug-Ins

This topic contains the following sub-topics:

- Introduction
  This topic describes the pre-deployment tasks to set up plug-ins before Oracle FLEXCUBE deployment.

- Integrate Oracle FLEXCUBE UBS and BPEL
  This topic explains integration of Oracle FLEXCUBE UBS and BPEL.

- Integration of Oracle FLEXCUBE UBS and Scheduler
  This topic explains Integration of Oracle FLEXCUBE UBS and Scheduler.

- Integration of Oracle FLEXCUBE UBS and BIP Reports
  This topic explains integration of Oracle FLEXCUBE UBS and BIP Reports.

- Integration of Oracle FLEXCUBE UBS and MBean
  This topic explains to integrate Oracle FLEXCUBE UBS with MBean plug-in.

1.1 Introduction

This topic describes the pre-deployment tasks to set up plug-ins before Oracle FLEXCUBE deployment.

You need to carry out certain tasks manually before Oracle FLEXCUBE deployment. This guide provides the details of pre-deployment tasks based on the selected plug-ins.

1.2 Integrate Oracle FLEXCUBE UBS and BPEL

This topic explains integration of Oracle FLEXCUBE UBS and BPEL.

If you have created the EAR file with BPEL as a plug-in, the installer will create the **FCJJPSProvider.jar** file in the BPELbuild folder alongside the Oracle FLEXCUBE UBS EAR file. Before deploying the Oracle FLEXCUBE UBS EAR file, you must complete the following tasks.

This topic contains the following sub-topics:

- Configure Custom Authentication Provider
  This topic provides systematic instructions to configure the Custom Authentication Provider.

- Configure Libovd For Single Entity
  This topic provides the systematic instructions to configure libovd for a single entity.

- Configure Libovd for Multi Entity
  This topic provides the systematic instructions to configure libovd for multi entity.

- Configure Multiple Providers for Multiple Entities
  This topic explains to configure multiple providers for multiple entities.

- Configure DBAdapter
  This topic explains the steps to configure DBAdapter.

- Configure JMS Adapter
  This topic explains to configure JMS Adapter.

- Configure FTP Adapter
  This topic explains to configure FTP Adapter using the below steps.

- BAM Report Configuration settings
  This topic explains the configuration settings for BAM reports.

- Configure IPM to Edit Document
  This topic explains to edit the document using the IPM configuration.

- Configure Supervisor Roles in EM
  This topic explains to configure supervisor roles in the Oracle Enterprise Manager.

- Configure Email Driver
  This topics explains the steps to configure the Email Driver.

- Configure TimeOut Settings for BPEL
  This topic explains steps to configure TimeOut Settings for BPEL.

1.2.1 Configure Custom Authentication Provider

This topic provides systematic instructions to configure the Custom Authentication Provider.

FCUBS Custom Authenticator Provider configuration must be done through the Weblogic console of SOA or manually update the config.xml of the SOA domain.

Follow the below steps to setup Custom Authentication Provider:

1. Along with the FCUBS Ear file, the installer generates the **FCUBSAuthenticationProvider.jar** file in the **BPELbuild** folder. Copy this file in the following path on the application server host
   `<ORACLE_HOME>\wlserver\server\lib\mbeantypes`.

2. Restart the Admin Server.

3. Login to the Console.

4. Click **Security Realms**.

Figure 1-1   Oracle Weblogic Server - Security Realms

5. Click **myrealm**.

Figure 1-2   Oracle Weblogic Servers_SecurityRealm_myrealms

6. Click the **Providers** tab and then click the **New** button to create a new authentication provider.

Figure 1-3   Oracle Weblogic Server - Providers

7. Specify the Provider name as **FCJCustomProvider** and type as
   FCUBSUserAuthenticator and click **OK**.

**Figure 1-4   Oracle Weblogic Server - Providers - Create New Authentication
Provider**

8. Click the **Reorder** button.

Figure 1-5   Oracle Weblogic Server - Providers - Reorder

The **Reorder Authentication Providers** screen displays.

Figure 1-6   Oracle Weblogic Server - Settings for FCJCustomProvider

9. On the **Reorder Authentication Providers** screen, bring the newly created provider to the first of all providers and click **OK**.

10. Click **FCJCustomProvider**.

   The **Settings for FCJCustomProvider** screen displays.

Figure 1-7   Settings for FCJCustomProvider - Common

11. In the Common tab, change the **Control flag** to **SUFFICIENT** from the drop-down list.

12. In Provider Specific tab, perform one of the following actions:

    a. Set **JNDIName** as Flexcube JNDI Name.

    b. If external authentications are used in FCUBS, then specify the **LDAP/MSAD** related fields.

13. For manual edit, browse the **config.xml** file from the following folder:

    `\Middleware\user_projects\domains\base_domain\config\`
    The following codes should be added at proper locations in the **config.xml** file.

    • Search for <realm> tag and add the following code between <realm> and </realm> tags. This should be the first child of the realm Node.

```
<sec:authentication-provider xmlns:n1="http://fcubs.ofss.com/security"
xsi:type="n1:fcubs-user-authenticatorType">
  <sec:name>FCJCustomProvider</sec:name>
  <sec:control-flag>SUFFICIENT</sec:control-flag>
  <n1:msad-or-ldap-login-required>true</n1:msad-or-ldap-login-required>
  <n1:external-password-required>true</n1:external-password-required>
  <n1:authentication-type>MSAD</n1:authentication-type>
  <n1:ldap-server-ip-and-port>LDAP://localhost:389</n1:ldap-server-ip-
and-port>
  <n1:ldap-ssl-enabled>true</n1:ldap-ssl-enabled>
  <n1:security-authentication-type>simple</n1:security-authentication-
type>
  <n1:ldap-domain-name>OFSS.COM</n1:ldap-domain-name>
  <n1:ldap-server-time-out-duration>0</n1:ldap-server-time-out-duration>
</sec:authentication-provider>
```

    • Make sure tag values matches the value given during Property file creation.

1.2.2 Configure Libovd For Single Entity

This topic provides the systematic instructions to configure libovd for a single entity.

Follow the steps below to configure the libovd details for a single entity:

1. Along with the **Oracle FLEXCUBE UBS EAR** file, the installer generates the **FCJJPSProvider.jar** file inside the **BPELbuild** folder under the SOURCE directory.

2. On the application server host, create a folder by the name **classes** at the following location `<MIDDLEWARE_HOME>soa\soa\modules\oracle.soa.ext_11.1.x.`

3. Extract the **FCJJPSProvider.jar** file and copy the **com** folder from the extracted content to the following location:
   `<MIDDLEWARE_HOME>soa\soa\modules\oracle.soa.ext_11.1.x\classes.`

4. Navigate to the location
   `<MIDDLEWARE_HOME>soa\soa\modules\oracle.soa.ext_11.1.x\classes\com\ofss\fcc\bpel\cac.`

5. Edit the properties file **CISProperties.properties** and update **JNDI.name** with the JNDI name same as Entity Name given in Multi Entity Names screen while creating property file **fcubs.properties**, example: jdbc/fcjdevDS.

6. Copy **FCJJPSProvider.jar** to `<MIDDLEWARE_HOME>/user_projects/domains/<domain_name>/config/fmwconfig/ovd/plu gins/lib.`

7. Create the directory structure if it does not exists.

8. Copy the **fcubs_adapter.xml** to the following location:

   `<MIDDLEWARE_HOME>/oracle_common/modules/oracle.ovd/templates/`

9. Search for **param name= DataSource** in fcubs_adapter.xml and update its value with FCUBS Datasource name, for example: The updated parameter would look like `<param_name="DataSource" value="jdbc/fcjdevDS"/>.`

10. Set environment variables in the command prompt, example: for Linux shell,

    `export ORACLE_HOME=/scratch/app/bpm12212(setting ORACLE_HOME) export WL_HOME=/scratch/app/bpm12212/wlserver(setting WL_HOME) export JAVA_HOME=/scratch/work_area/DBA/jdk1.8.0_144 (setting JAVA_HOME)`

11. Execute the **libovdadapterconfig** script which is available in `<MIDDLEWARE_HOME>/oracle_common/bin` with below parameters.

12. Specify the below arguments with values for admin server host name or IP that are:

    - Admin server port
    - WebLogic User ID
    - Domain Home
    - Fcubs datasource

    `./libovdadapterconfig.sh -adapterName fcubsadapter -adapterTemplate fcubs_adapter.xml -host <ADMIN_SERVER_HOST> -port <ADMIN_PORT> -userName <WEBLOGIC_USERID> -domainPath <DOMAIN_HOME> -dataStore DB -root ou=fcubs,dc=oracle,dc=com -contextName default - dataSourceJNDIName <FCUBS_DATASOURCE_JNDI>`

13. Once the above steps are completed, a message will displays and stating that **Adapter created successfully: fcubsAdapter**.

14. Restart the server.

1.2.3 Configure Libovd for Multi Entity

This topic provides the systematic instructions to configure libovd for multi entity.

Follow the steps given below to configure the libovd for multi entity.

1. Continue step 1 to step 5 from Configure Libovd For Single Entity

2. In the following steps, replace the <EntityId> tag with the proper Entity name.

3. Copy the fcubs_adapter_<EntityId>.xml to `<MIDDLEWARE_HOME>/oracle_common/modules/oracle.ovd/templates/`

4. Search for <FCUBSDATASOURCE> in fcubs_adapter_< EntityId>.xml and update it with fcubs Datasource with the mapped Datasource for the entity in the property file.

For example: `<param name="DataSource" value="<FCUBSDATASOURCE>"/>`

5. Search for UserIdPattern Parameter and update the value for OU to the entity name in lower case.

For example: `<param name="UserIdPattern" value="cn=%USERID%,ou=<EntityId>,dc=oracle,dc=com"/>`

6. Search for MultiEntityEnabled element and update the value to **true**.

For example: `<param name="MultiEntityEnabled" value="true"/>`

7. Search for EntityId element and update the value with the entity name in lower case which we have created.

For example: `<param name="EntityId" value=" <EntityId>"/>`

8. Search for ou=fcubs and update with entity id in lower case.

For example: ou= EntityId

9. Execute **libovdadapterconfig** script which is present in `<MIDDLEWARE_HOME>/oracle_common/bin` with below parameters.

10. Update the admin server host name or IP, admin server port, WebLogic user id, domain home, root, and fcubs datasource.

```
libovdadapterconfig.sh -adapterName fcubsAdapter -adapterTemplate
fcubs_adapter_< EntityId >.xml -host <ADMIN_SERVER_HOST> -port <ADMIN_PORT> -
userName <WEBLOGIC_USERID> - domainPath <DOMAIN_HOME> -dataStore DB -root
ou=<EntityId>,dc=oracle,dc=com -contextName default -dataSourceJNDIName
<FCUBSDATASOURCE name which we mapped in step4>
```

11. Repeat from step 2 to step 7 for each entity creation.

12. Once the above steps are completed, restart the server.

> ✎ **Note:**
>
> For any misconfiguration in libovd, delete the existing fcubsAdapter and re-run the **./libovdadapterconfig.sh**.

For deleting fcubsAdapter use the below command:

a. Log in to the WSLT console by running the WLST script.

For example:

- **UNIX**: `MW_HOME/oracle_common/common/bin/wlst.sh`

- **Windows**: `MW_HOME\oracle_common\common\bin\wlst.cmd`

b. Connect to your Administration Server using the following syntax:
`connect ('<WLS admin user name>','<WLS admin password>','t3://<admin server host>:<admin server port>')`

For Example: `connect('weblogic','weblogic','t3://myserver:7001')`

c. Delete the misconfigured adapter using the following syntax:
`deleteAdapter(adapterName='fcubsAdapter')`

> **Note:**
>
> - In the case of Multi Entity, all data sources must be created separately for each entity. The JNDI name will be differentiated by suffixing the entity name.
>
>   Example: If Data source is **jdbc/fcjDevDs** then **jdbc/fcjDevDs+entity name** will be lookup the application. **(jdbc/fcjDevDs+entity name) jndi** should be presented in application server.
>
> - For multi tenant deployment, BPMN support will be available only for the logged entity.

1.2.4 Configure Multiple Providers for Multiple Entities

This topic explains to configure multiple providers for multiple entities.

1. Login to the Adminserver.

2. Click **Security Realms**.

The **Oracle Weblogic Server** screen displays.

Figure 1-8　Oracle Weblogic Server

3. Click **myrealms**.

   The **Summary of Security Realms** screen displays.

Figure 1-9　Summary of Security Realms

4. Click the **Providers** tab.

   The **Settings for myrealms - Providers** screen displays.

Figure 1-10   Settings for myrealms - Providers

5. Click **New**.

Figure 1-11   Settings for myrealms - Authentication Providers

6. Specify the Name with proper Entity Name (entity name you mapped in property file) and select the type as **FCUBSUserAuthenticator** and click **OK**.

The **Create a New Authentication Provider** screen displays.

Figure 1-12   Create a new authentication Provider

7. Click **Reorder**. Bring the **Authenticatiorprovider** to the first in the order and click **OK**.

   The **Reorder Authentication Providers** screen displays.

Figure 1-13   Reorder Authentication Providers

8. Click the Provider that you have created.

   The **Settings for myrealms - Providers - New Provider** screen displays.

Figure 1-14   Settings for myrealms - Providers - New Provider

9. In the **Common** tab, select the control flag as SUFFICIENT from the list and click **Save**.

   The **Settings for ENTITYID - common tab** screen displays.

Figure 1-15   Settings for ENTITY ID - Common

10. Select the **Provider Specific** tab.

    The **Settings for ENTITYID - Provider Specific** screen displays.

Figure 1-16   Settings for ENTITYID - Product Specific

11. Change the **JNDIName** to the Datasource JNDI name, which has mapped to the entity in the property file level, and select the **Multi Entity enabled** checkbox.

Figure 1-17   Settings for ENTITYID - Provider Specific - Multi Entity

12. Specify the **Entity ID** with the Entity name which you have created in the property file level and click **Save**.

Figure 1-18   Settings for ENTITYID - Provider Specific - Entity Id

13. Create the new datasource for each entity with the JNDI name, which you mapped in the property file.

14. Restart the Admin Server.

15. Continue step 1 to step 15 for each provider creation in a multi-entity scenario.

1.2.5 Configure DBAdapter

This topic explains the steps to configure DBAdapter.

To configure DBAdapter, follow the steps given below:

1. Log in to **Weblogic Console** and click **Deployment** under **Domain Structure**.

   The **Summary of Deployments** screen displays.

Figure 1-19   Summary of Deployments

2. In the Deployments table, select **DbAdapter** and you will be navigated to **Settings for DbAdapter** screen.

3. Click the **Configuration** tab and select **Outbound Connection Pools**.

   The **Settings for DBAdapter** screen displays.

Figure 1-20   Settings for DBAdapter

4. Under **Groups and Instances**, click and expand **javax.resource.cci.ConnectionFactory**.

5. Click **New** and select **javax.resource.cci.ConnectionFactory** in Outbound Connection Group.

6. Define **JNDI Name** as eis/DB/FCCDEV and click **Finish**.

   The jndi name should be the same as the one in the **Dbutility sub-process**.

7. Click the **DbAdapter** again.

8. Click the **Configuration** tab and select **Outbound Connection Pools**.

9. Under **Groups and Instances**, click and expand **javax.resource.cci.ConnectionFactory**.

   The new JNDI name is listed.

10. Click on the `eis/DB/FCCDEV` link.

    The **Settings for javax.resource.cci.ConnectionFactory** screen displays.

Figure 1-21   Settings for javax.resource.cci.ConnectionFactory

11. Click the **Property Value** field for the **DataSourceName** and update the application JNDI reference (given in fcubs.properties file), and press the **Enter** key.

12. Click **Save** and restart the Admin server.

1.2.6 Configure JMS Adapter

This topic explains to configure JMS Adapter.

To configure JMS Adapter, follow the steps given below.

1. Log in to **Weblogic Console** and click on **JMS Servers** under **Domain Configurations - Services**.

   The **Weblogic Console Home Page** displays.

Figure 1-22   Oracle Weblogic Console Home Page

2. Click **New**.

    The **Summary of JMS Servers** screen displays.

Figure 1-23   Summary of JMS Servers

3. Specify the **Name** as FCUBSJMSServer for JMS Server, select the **Persistent Store** as
    SOAJMSFileStore from the dropdown list and click **Next**.

The **Create a New JMS Server** screen displays.

Figure 1-24   Create a New JMS Server

4. Select the **Target** as SOAServer from the dropdown list.

   The **Create a New JMS Server - Target** screen displays.

Figure 1-25   Create a New JMS Server - Target

5. Click **Finish**.

   Two messages displays on the **Summary of JMS Servers** screen.

Figure 1-26   Summary of JMS server - Messages

6. Go back to **Weblogic Console** and click **JMS Modules** under **Domain Configurations - Services**.

    The **Weblogic Console - JMS Module** screen displays.

Figure 1-27   Weblogic Console - JMS Module

The **Summary of JMS Modules** screen displays.

Figure 1-28   Summary of JMS Modules

7. On the **Summary of JMS Modules** screen, click **New**.

The **Create JMS System Module** screen displays.

Figure 1-29   Create JMS System Module

8. Specify the **Name** as FCUBSJMSModule.

The **Create JMS System Module - Select Target** screen displays.

Figure 1-30   Create JMS System Module - Select Target

9. Click **Next**.

10. Select the **Target** as SOAServer and click **Finish**.

    Two messages displays on the **Summary of JMS Modules** screen.

Figure 1-31   Summary of JMS Modules - Messages

11. Go back to **JMS Modules**, click on **FCUBSJMSModule**.

    The **Settings for FCUBSJMSModule** screen displays.

Figure 1-32   Settings for FCUBSJMSModule

12. Click **New**.

The **Create a New JMS System Module Resource** screen displays.

Figure 1-33   Create a New JMS System Module Resource

13. On the **Create a New JMS System Module Resource** screen, select **Connection Factory** and click **Next**.

The **Create a New JMS System Module Resource - Connection Factory Properties** screen displays.

Figure 1-34   Create a New JMS System Module Resource - Connection Factory Properties

14. Specify **Name** as FCUBSConnectionfactory and click **Next**.

The **Create a New JMS System Module Resource - Advanced Targeting** screen displays.

Figure 1-35   Create a New JMS System Module Resource - Advanced Targeting

15. Click the **Advanced Targeting** button.

The **Create a New JMS System Module Resource - Subdeployments** screen displays.

Figure 1-36   The Create a New JMS System Module Resource - Subdeployments

16. Click **Create New Sub Deployment** with the below name, and click **OK**.

17. Click **Next** and select the subdeployment you want to use.

18. If you not yet created a subdeployment, click **Create a New Subdeployment** and specify the **Subdeployment Name** and click **OK**.

The **Create a New Subdeployments** screen displays.

Figure 1-37   Create a New Subdeployments

19. Click **Next** and select **Targets** as FCUBSJMS Servers.

    The **Create a New JMS System Module Resource - Select Target** screen displays.

Figure 1-38   Create a New JMS System Module Resource - Select Target

20. Click **Finish**.

    Two messages displays on the **Settings for FCUBSJMSModule** screen.

Figure 1-39   Settings for FCUBSJMSModule - Messages

21. Go back to **Weblogic Console**, click on **JMS Modules**, click **New**, select **Queue**, and click on **Next**.

    The **Create a New JMS System - Queue** screen displays.

Figure 1-40   Create a New JMS System - Queue

22. Specify **Name** as NOTIFY_DEST_QUEUE and **JNDI Name** as jms/
NOTIFY_DEST_QUEUE and click **Next**.

The **JMS Destination Properties** screen displays.

Figure 1-41   JMS Destination Properties

23. Select the **Subdeployments** from the drop-down list that you created earlier, select the
Targets as JMS Servers.

The **Create a New JMS System Module Resource - Subdeployments and Select
Targets** screen displays.

Figure 1-42   Create a New JMS System Module Resource - Subdeployments and Targets

24. Click on **Finish**.

Two messages displays the **Settings for FCUBSJMSModule** screen.

Figure 1-43   Settings for FCUBSJMSModule - Messages

25. Create queue **MDB_QUEUE_RESPONSE** with JNDI name as **jms/ MDB_QUEUE_RESPONSE**, queue **eis/jms/ORGateway** with JNDI name as **eis/jms/ ORGateway**, and queue **FAULT_QUEUE_RESPONSE** with JNDI name as **jms/ FAULT_QUEUE_RESPONSE** as above in console within FCUBSJMSModule. (Repeat the steps from 14 to 21).

26. Go to **Weblogic Console**, click **Deployment**.

The **Summary of Deployment** screen displays.

Figure 1-44   Settings for JMSAdapter

27. Select **JMS Adapter**.

The **Settings for JMSAdapter - Configuration - Outbound Connection Pools** screen displays.

Figure 1-45   Settings for JMSAdapter - Outbound Connection Pools Configuration

28. Click **Configuration** tab, select **Outbound Connection Pools** and expand **oracle.tip.adapter.jms.IJmsConnectionFactory**.

    The **Create a New Outbound Connection** screen displays.

Figure 1-46   Create a New Outbound Connection

29. Click **New**.

30. Select the **Outbound Connection Group** and click **Next**.

    The **Create a New Outbound Connection - JNDI Name for Outbound Connection Instance** screen displays.

Figure 1-47   Create a New Outbound Connection - JNDI Name for Outbound Connection Instance

31. Specify the **JNDI Name** as eis/Queue/Notif and click **Finish**.

32. The eis/Queue/Notif is listed in the Outbound Connection Pool Configuration Table on the **Settings for JMSAdapter** screen.

    The **Settings for JMSAdapter - Table** screen displays.

Figure 1-48   Settings for JMSAdapter - Outbound Connection Pool Configuration Table

33. Click on the Outbound connection pool with **eis/Queue/Notif** and specify the connection factory location as **jndi/FCUBSConnectionfactory**, and press enter.

    The **Settings for oracle.tip.adapter.jms.IJmsConnectionFactory** screen displays.

Figure 1-49   Settings for oracle.tip.adapter.jms.IJmsConnectionFactory

34. Click on **Save**.

Two messages displays on the **Settings for oracle.tip.adapter.jms.IJmsConnectionFactory** screen.

Figure 1-50   Settings for oracle.tip.adapter.jms.IJmsConnectionFactory - Messages

35. Go to **Weblogic Console**, click **Deployment**, and select **JMS Adapter**.

The **Summary of Deployments** screen displays.

Figure 1-51   Summary of Deployments

36. Click **Update**.

The **Update Application Assistant** screen displays.

Figure 1-52   Update Application Assistant

37. Click **Next** and then click **Finish**.

   The two messages displays on the **Summary of Deployments** screen.

Figure 1-53   Summary of Deployments - Messages

38. Create the Outbound Connection Pool with the **eis/wls/Queue** name in the Deployments using Connection Factory **jndi/FCUBSConnectionfactory**.

1.2.7 Configure FTP Adapter

This topic explains to configure FTP Adapter using the below steps.

1. Login to **Weblogic Console**, click **Deployment**, and select **FTP Adapter**.

2. Click the **Configurations** tab and select **Outbound Connection Pool**.

   The **Outbound Connection Pool** screen displays.

Figure 1-54   Outbound Connection Pool

3. Click **New**.

    The **Create a New Outbound Connection** screen displays.

Figure 1-55   Create a New Outbound Connection

4. Specify eis/ftp/FtpAdapterLcl in the **JNDI Name** field.

5. Click **Finish** and **Save**.

    This topic contains the following sub-topic:

- BIP Interactive reports configuration
  This topic explains systematic instructions to configure the BIP Interactive reports with BPEL.

1.2.7.1 BIP Interactive reports configuration

This topic explains systematic instructions to configure the BIP Interactive reports with BPEL.

To configure BPEL with BIP interactive reports, follow the instructions below:

1. Login to the **BIP domain console**, http/s:<hostname>:<port>/console.

2. To add the FCJCustomProvider, refer to steps from *Configure Custom Authentication Provider* topic.

3. Navigate to **Security realms** and click **myrealm**, and then click **Users and Groups** tab.

   The **Settings for myrealm - Users and Groups** screen displays.

   Figure 1-56   Settings for myrealm - Users and Groups

> **Note:**
>
> Check if the users from the schema, display in the **Users** tab, and the roles from the schema are displayed under the **Groups** tab.

4. Login to the **Enterprise Manager** (em) http/s:<hostname>:<port>/em.

   - Right click the domain (in which BI suite is installed) under the WebLogic domain.

   - Go to **Security** and then navigate to **Application Roles**.

   The **Enterprise Manager** screen displays.

Figure 1-57   Enterprise Manager

5. Navigate to the **Application Roles** screen, specify the following details:

    a. Select **obi** from the **Application Stripe** drop-down.

    b. Click the **Search** button.

    c. Click the **Create** button to add a role.

    The **Application Roles** screen displays.

Figure 1-58   Application Roles

6. On the **Create Application Role** screen, specify the following details:

    a. Specify the **Role Name** (mandatory), **Display Name** (optional) and **Description** (optional).

b. Click the **Add** button.

The **Add Principal** pop-up displays.

Figure 1-59   Add Principal

c. Select Group from the **Type** drop-down.

d. Select the checkbox under the **Advanced Option** section and again select Group from the **Type** drop-down.

- Click the **Search** button, if the roles are listed then select the roles like ALLROLES-000, ADMINROLE-000 from the list.

- Specify the **Principal Name** (mandatory), which is the role present in the FCUBS (ex: ALLROLES-000, ADMINROLE-000), Display Name (optional).

e. Click the **OK** button in the **Add Principal** pop-up and then also in the **Create Application Role** screen.

A confirmation screen displays with a message stating that a new role added successfully.

7. Again, right click the domain (which BI suite is installed) under the **WebLogic domain** and select **Security** and then select **Application Policies**.

The **Application Policies** screen displays.

Figure 1-60   Application Policies

8. On the **Application Policies** screen, specify the following details:

   a. Select **obi** from the **Application Stripe** drop-down and also select **Application Role** in the **Principal Type** field.

   b. Click the **search** button.

   c. Select **BIConsumer** from the list and click the **Create** button.

   The **Application Policies** screen displays.

Figure 1-61   Application Policies

9. On the **Create Application Grant** screen, click the **Add** button.

    The **Add Principal** pop-up window displays.

Figure 1-62   Add Principal

10. On the **Add Principal** pop-up window, perform the following actions:

    a. Select **Application Role** from the **Type** drop-down list and click the **Search** button.

    b. From the **Searched Principals** list, select **ALLROLES** that has been created earlier in the **Application Role** screen.

    c. Click the **OK** button in the **Add Principal** pop-up window and also on the **Create Application Grant** screen.

11. Click the **Add** button under **Permissions** section and add the two permissions one by one as mentioned below.

- oracle.bi.publisher.runReportOnline

- oracle.bi.publisher.accessReportOutput

The **Create Application Grant - Permissions** screen displays.

Figure 1-63   Create Application Grant

The confirmation screen displays with a message stating that a security added successfully.

12. Login into the **BI Publisher** , http/s:<hostname>:<port>/xmlpserver.

13. Click **Administration**.

14. Click **Roles and Permission** under **Security Center** and check whether the added role (in em) is displayed or not, if not, restart the servers.

The **BIPublisher - Administration** screen displays.

Figure 1-64   BIPublisher - Administration

15. Click **Catalog**, select the folder that has been created.

    The **BIPublisher - Catalog** screen displays.

Figure 1-65   BIPublisher - Catalog

16. Click **Permissions** under the **Tasks**.

    The **Permissions** pop-up displays.

Figure 1-66   Permission

17. Delete all the roles if any present.

18. Click the **Add** button.

19. Click the **Search** button in the **Add Roles** pop-up window.

20. Select the role that has been created and click the **Move** button and then click **OK**.

    The role will be added in the **Permissions** pop-up window.

Figure 1-67   Permissions - Add Roles

21. Select the options that should be granted to the particular role and check if permissions are only granted to items in the folder if necessary.

    Now the reports in the folder will be accessed accordingly based on roles.

> **✎ Note:**
>
> Similarly, you can set the permissions at the report level also for a particular role.

22. Login in to **BI Publisher** http://server:port/xmlpserver.

23. Click **Administration**.

    The **Administration** screen displays.

Figure 1-68   Administration

24. Under **Data Sources**, click **JDBC Connection**.

    The **Administration - JDBC** screen displays.

Figure 1-69   Administration - JDBC

25. Click **Add Data Source** to create the data source with name as **FCSOA** and use SOA schema details to create the same.

The **Add Data Source** screen displays.

Figure 1-70   Add Data Source

26. Under **Security**, add FCUBS roles to Allowed Roles.

The **Add Data Source (Security)** screen displays.

Figure 1-71   Add Data Source (Security)

27. Click **Test Connection**.

28. Once the connection is established successfully, click **Apply**.

29. Follow steps 25 to 28 to create the data source for FCUBS Schema and specify the name as **FCBIPBPEL**.

1.2.8 BAM Report Configuration settings

This topic explains the configuration settings for BAM reports.

Generate a deployment plan for BAM Composer Application. If you want to configure BPEL with BAM reports, follow the steps below:

1. Generate a deployment plan for BAM Composer Application.

2. Log in to console `http://<hostname>:<port>/<console>`.

3. Under the **Domain Structure**, click **Deployments**.

   The **Summary of Deployments** screen displays.

Figure 1-72   Summary of Deployments

4. Click **BAM Composer**.

    The **Summary of BAM Composer** screen displays.

Figure 1-73   Summary of BAM Composer

5. On the **Summary of BAM Composer** screen, click the **Configuration** tab, select the **Application** tab and click the **Save** button.

6. Click the **Overview** tab and check the **Deployment Plan** location.

   The **Summary of BAM Composer - Overview** screen displays.

Figure 1-74   Summary of BAM Composer - Overview

7. Add variable and variable assignment as below to the Plan.xml in `<module-name>BamComposerWeb.war</module-name>`.

```
<variable>
 <name>oracle.adf.view.rich.security.FRAME_BUSTING</name>
 <value>never</value>
 </variable>
<module-descriptor external="true">
 <root-element>web-app</root-element>
 <uri>WEB-INF/web.xml</uri>
 <variable-assignment>
 <name>oracle.adf.view.rich.security.FRAME_BUSTING</name>
 <xpath>/web-app/context-param/
[paramname="oracle.adf.view.rich.security.FRAME_BUSTING"]/param-value</
xpath>
 <origin>planbased</origin>
 </variable-assignment> </module-descriptor>
```

8. On the **Summary of Deployments** screen, click the **Stop** button and the following options are displayed.

   • When work completes

- • Force Stop Now

- • Stop, but continue servicing administration requests

9. Click **Force Stop Now**.

10. To update the deployment plan, click **Deployment** and select the **BAM Composer** checkbox.

    The **Summary of Deployments - Update** screen displays.

Figure 1-75   Summary of Deployments - Update

11. Click the **Update** button.

    The **Update Application Assistant** screen displays.
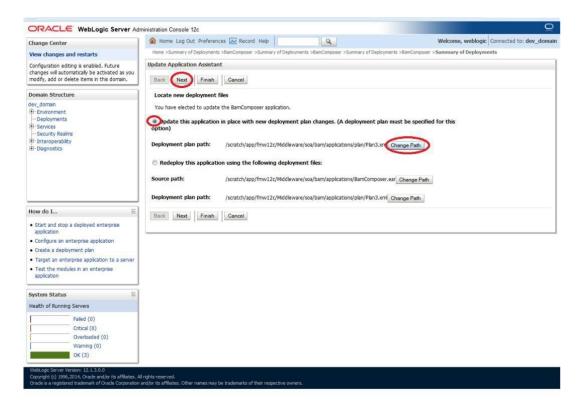
Figure 1-76   Update Application Assistant

12. On the **Update Application Assistant** screen, select the **Update this application in place with new deployment plan changes** option and click the **change path** button.

13. Select the latest plan.xml in the path, and click the **Next**.

   The **Update Application Assistant - Select a deployment plan** screen displays.
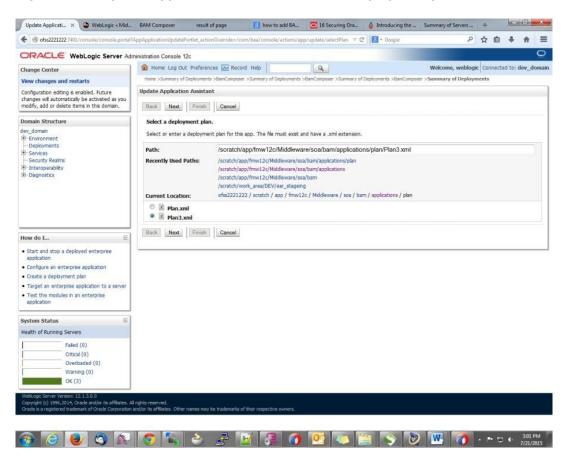
Figure 1-77   Update Application Assistant - Select a deployment plan

14. Click **Finish**.

    Two messages are displayed on the **Summary of Deployments** screen.

Figure 1-78   Summary of Deployments - Messages

15. Restart the BAM Composer application in the console.

The **Summary of Deployments - Restart BAM Composer** screen displays.

Figure 1-79   Summary of Deployments - Restart BAM Composer

16. Log in to Enterprise Manager console `http://hostname:port/em`.

17. Right click the **BAM Server**, and click **Security** and then click **Application Roles**.

    The **BAM Server - Application Roles** screen displays.

Figure 1-80   BAM Server - Application Roles

18. On the **Application Roles** screen, click the **Create** button to create application role with **ALL ROLES-000** name.

The **Create Application Role** screen displays.

Figure 1-81   Create Application Role

19. Click the **ADD** button under the **Members** section.

20. Select the **Group** from the **Type** drop-down list and add principle details.

21. Log in to BAM Composer `http://hostname:port/bam/composer`.

22. Click **Administrator**.

The **Oracle BAM Composer - Administrator** screen displays.

Figure 1-82   Oracle BAM Composer - Administrator

23. Under **Data Objects**, Right click **CUBE_INSTANCE** and select **Security**.

The **BAM Composer - Navigate to Security** screen displays.
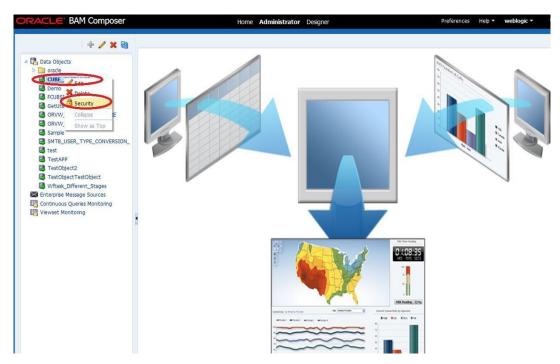
Figure 1-83   BAM Composer - Navigate to Security

24. Click the **Add** button under **Grant permission** and search the list based on the **Application Role**.

The **Security** screen displays.

Figure 1-84   Security

25. Move the **ALLROLES-000** to the Selected Members column.

The **Security - Add Application Roles, Groups and Users** screen displays.

Figure 1-85   Security - Add Application Roles, Groups and Users

26. Select **Read**, **Select**,and **Update** checkboxes and click the **Save** button.

The **Add Application Roles, Groups and Users - ALLROLES-000** screen displays.

Figure 1-86   Add Application Roles, Groups and Users - ALLROLES-000

27. Follow the steps 21 to 27 for other Data objects as listed below:

- cube_instance
- wftask_different_stages
- ORVW_TRACK_EXPOSURE
- ORVW_FACILITY_EXPOSURE
- GetUtilsDB
- SMTB_USER_TYPE_CONVERSION_VIEW
- FCUBSDATAOBJECTS

28. On the **Oracle BAM Composer**, click the **Designer**.

    The **Oracle BAM Composer Designer** screen displays.

Figure 1-87   Oracle BAM Composer Designer

29. Click **Open Project**.

    The **Open Project** pop-up window displays.

Figure 1-88   Designer - Open Project

30. On the **Open Project** pop-up window, click **FCUBS_BAM_Report**.

31. On the **Designer** screen, right click **FCUBS_BAM_Report** and select **Security**.

    The **FCUBS_BAM_Report - Security** screen displays.

Figure 1-89   FCUBS_BAM_Report - Security

32. On the **FCUBS_BAM_Report (Security)** screen, click the **ADD** icon under **Grant Permission**.

The **FCUBS_BAM_Report (Security)** screen displays.

Figure 1-90   FCUBS_BAM_Report (Security)

33. Search the list based on the **Application Roles** and select the **ALLROLES-000**.

The **Add Application Roles, Groups and Users - ALLROLES-000** pop-up window displays.

Figure 1-91   Add Application Roles, Groups and Users - ALLROLES-000

ORACLE

34. Move the **ALLROLES-000** to Selected Members column and click the **OK** button.

The **Add Application Roles, Groups and Users - ALLROLES-000 - Selected Members** pop-up window displays.

Figure 1-92   Add Application Roles, Groups and Users - ALLROLES-000 - Selected Members

35. Select the **Read** checkbox for **ALLROLES-000** and click the **Save** button.

The **FCUBS_BAM_Report (Security) - ALLROLES-000** screen displays.

Figure 1-93   FCUBS_BAM_Report (Security) - ALLROLES-000

1.2.9 Configure IPM to Edit Document

This topic explains to edit the document using the IPM configuration.

If you want to configure BPEL with IPM configuration, perform the following steps.

1. Login to the console, http/s:<hostname>:<port>/console with admin user.

2. To add the FCJCustomProvider, Refer to the Configure Custom Authentication Provider topic.

3. Navigate to **Security Realms**, click **myrealm**, and click **Users and Groups** tab.

   Check if the users from the schema are displayed in the **Users** tab, and roles from the schema are displayed under the **Groups** tab.

4. After adding the custom authenticator, perform the following actions:

   a. Navigate to **Security Realms**, click **myrealm**, click **Users and Groups** and click the **Groups** tab.

      The **Settings for myrealm** screen displays.

Figure 1-94   Setting for myrealm

b.   Click the **New** button.

The **Create a New Group** screen displays.

Figure 1-95   Create a New Group

5.   On the **Create a New Group** screen, specify the following details.

a.   Specify the name as **IPMUserGroup**.

b.   Specify the **Description** for the new group (optional).

c.   Select the **Provider** as **DefaultAuthenticator**.

d.   Click the **OK** button.

6.   Login to the Imaging using the following URL http/s:<hostname>:<port>/imaging with admin user.

The **Oracle Webcenter Content:Imaging** log in screen displays.

Figure 1-96   Oracle Webcenter Content:Imaging

7. Specify **User ID** and **Password** and click **Sign in**.

The **FLEXCUBE:Application Summary** screen displays.

Figure 1-97   FLEXCUBE:Application Summary

8. Navigate to **Manage Applications** on the left pane.

9. Click **FLEXCUBE**.

10. Click the **Modify** button on the right pane.

The **Create Application Document Security** screen displays.

Figure 1-98   Create Application Document Security

11. On the **Create Application Document Security** screen, perform the following steps:

    a. Click **Document Security** tab.

    b. Click the **Add** button.

        The **Add Security Member** pop-up window displays.

    c. Click the **Search** button in the **Add Security Member** pop-up window.

    d. Select the **IPMUserGroup**.

    e. Click **Add**.

        IPMUserGroup is listed in the panel.

    f. Select **View**, **Write**, **Annotate Standard**, **Annotate Restricted** and **Annotate Hidden** checkboxes.

    g. Click **Submit**.

        The **USER_ID:Search Summary** screen displays.

Figure 1-99   USER_ID:Search Summary

12. On the **USER_ID: Search Summary** screen, perform the following steps:

    a. Navigate to **Manage Searches**.

    b. Select the available search (ex: USER_ID in this doc).

    c. Click the **Modify** button.

        The **USER_ID:Search Security** screen displays.

Figure 1-100   USER_ID:Search Security

13. On the **USER_ID:Search Security** screen, perform the following steps:

    a. Click the **Security** tab.

b. Click the **Add** button.

The **Add Security Member** pop-up window displays.

c. Click the **Search** button in the **Add Security Member** pop-up window.

d. Select the **IPMUserGroup**.

e. Click **Add** button.

The **IPMUserGroup** will be listed in the panel; don't select any checkbox except the default **View** checkbox.

f. Click the **Submit** button on the right corner.

14. Copy the **FCJJPSProvider.jar** to location `<ORACLE_HOME`
`>\user_projects\domains\<domian name>\lib` .

15. Go to the location `<ORACLE_HOME>\`
`user_projects\domains\<Domain_created>\config\fmwconfig`.

a. Open **jps-config.xml** file and search <serviceProviders> tag and add the following code between <serviceProviders> and </serviceProviders> tags.

```
<serviceProvider
class="oracle.security.jps.internal.idstore.generic.GenericIdentityStore
Provider"
name="custom.generic.provider" type="IDENTITY_STORE">
<description>DB IdentityStore Provider</description>
</serviceProvider>
```

b. Similarly, search for <serviceInstances> tag and add the following code between <serviceInstances> and </serviceInstances> tags.

```
<serviceInstance location="dumb" name="idstore.custom"
provider="custom.generic.provider">
 <description>Custom Identity Store Service Instance</description>
 <property name="idstore.type" value="CUSTOM"/>
 <property name="ADF_IM_FACTORY_CLASS"
value="com.ofss.fcc.bpel.security.idm.providers.stddb.FCIdentityStoreFac
tory"/>
 <property name="DATASOURCE_NAME" value="jdbc/fcjdevDS"/>
 <property name="INTERNAL_CONTEXT_REQUIRED" value="true"/>
 <property name="INTERNAL_CONTEXT_NAME" value="internalstore"/>
 </serviceInstance>
```

Make sure that the JNDI (jdbc/fcjdevDS) matches the value given during property file creation.

c. Search for **<jpsContexts default="default">** tag and add the following code between **<jpsContexts default="default">** and **</jpsContexts>**, preferably after the default jpsContext.

```
<jpsContext name="internalstore">
 <serviceInstanceRef ref="credstore"/>
 <serviceInstanceRef ref="keystore"/>
 <serviceInstanceRef ref="policystore.xml"/>
 <serviceInstanceRef ref="audit"/>
 </jpsContext>
```

ORACLE

1.2.10 Configure Supervisor Roles in EM

This topic explains to configure supervisor roles in the Oracle Enterprise Manager.

1. Right click **soa-infra** and select **Security** and click **Application Roles**.

   The **Target Navigation of Application Roles** screen displays.

Figure 1-101   Target Navigation of Application Roles

2. Search the Application Roles with the **Starts With** option.

   The **Application Roles** screen displays.

Figure 1-102   SOA Infra - Application Roles

3. Select **SOA Admin** role and click the **Edit** option.

4. On the **Edit Application Roles : SOAAdmin** screen, click the **ADD** button.

The **Add Principal** pop-up window displays.

Figure 1-103   Add Principal

5. Select the **Group** from the **Type** drop-down.

6. Specify the **Principal Name** as (EX: ALLROLES-000) Param_val, which is mapped to the OR_ADMINROLE in the cstb_param table and search the role.

   The list of application roles is displayed based on the criteria specified.

Figure 1-104   Add Principal - ALLROLES-000

7. Click the **OK** button.

1.2.11 Configure Email Driver

This topics explains the steps to configure the Email Driver.

To configure the Email Driver in BPEL, follow the steps below:

1. Log in to EM console.

2. Navigate to **User Messaging Service** folder.

   The **User Messaging Service** target navigation folder displays.
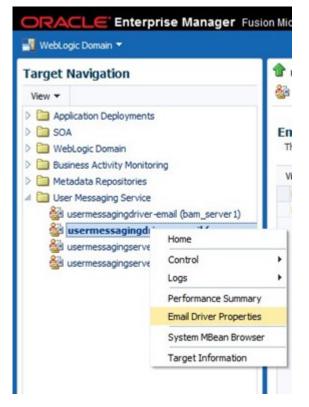
Figure 1-105   User Messaging Service

3. Right click **usermessagingdriver-email (soa_server1)**.

4. Click **Email Driver Properties**.

   The **usermessagingdriver-email** screen displays.

Figure 1-106   usermessagingdriver-email

5. Specify the **Sender Address** and **Default Sender Address** (This ID will be used as sender address).

6. Specify the supported protocols (SMTP).

7. Select the mail access protocol (IMAP) as per the mail server specification.

    The **Driver-Specific Configuration** screen displays.

Figure 1-107   Driver-Specific Configuration

8. Specify the **Receive** folder in the mailbox (INBOX).

9. Specify the **Outgoing Mail Server hostname or IP**.

10. Specify the **Outgoing Mail Server Port**.

11. Specify the **Outgoing Default From Address**.

12. Specify the **Outgoing Username and Password** if required.

Figure 1-108   Driver-Specific Configuration

13. Navigate to **SOA** folder.

14. Right click **soa-infra (soa_server1)** and select **SOA Administration** and then click **Workflow Porperties**.

    The **Workflow Notification Properties** screen displays.

Figure 1-109   Workflow Notification Properties

15. Select **Email/ALL** from the **Notification Mode**drop-down list.

16. Specify the **From Address**, **Actionable Address**, and **Reply To Address**.

1.2.12 Configure TimeOut Settings for BPEL

This topic explains steps to configure TimeOut Settings for BPEL.

To configure TimeOut setting for BPEL, follow the below steps:

1. Login into Console (http://hostname:port/console).

    The **WebLogic Server** Home page displays.

Figure 1-110   WebLogic Server

2. Click **Deployments**.

The **Summary of Deployments** screen displays.

Figure 1-111   Summary of Deployments

3. Click **soa-infra** application under deployments.

4. Go to **EJBs**, click **BPELEngineBean**.

The **Summary of BPELEngineBean** screen displays.

Figure 1-112   Summary of BPELEngineBean

5. On the **BPELEngineBean** screen, click **Configuration** and set **Transaction TimeOut** to 300.

Figure 1-113   BPELEngineBean Configuration - Transaction TimeOut

6. Go to **EJBs**, click **BPELDeliveryBean**.

    The **Summary of BPELDeliveryBean** screen displays.

Figure 1-114   Summary of BPELDeliveryBean

7. On the **BPELDeliveryBean** screen, click **Configuration** and set **Transaction TimeOut** to 300.

Figure 1-115   BPELDeliveryBean Configuration - Transaction TimeOut

8. Login to Console and click **JTA** under **Services**.

9. Set the **JTA timeout** according to the below condition:

   BPELEngineBean + BPELDeliveryBean is <= JTA timeout (For example 300+300<=600).

   The **Settings for dev_domain JTA** screen displays.

Figure 1-116   Settings for dev_domain - JTA

10. Login to EM console (http://host:port/em).

11. Right click on the **soa-infra (SOAServer)**.

12. Select **SOA Administration** and then click the **BPEL Porperties**.

    The **soa-infra** screen displays.

Figure 1-117   SOA Infra

13. Click **MoreConfigpropeties** and then click **SyncMaxWaitTime**.

14. Change the **SyncMaxWaitTime** to 200 secs.

Figure 1-118   System MBean Browser

1.3 Integration of Oracle FLEXCUBE UBS and Scheduler

This topic explains Integration of Oracle FLEXCUBE UBS and Scheduler.

Before deploying the Oracle FLEXCUBE UBS EAR file, you must follow the tasks below.

- Running Backend Scripts
  This topic provides the systematic instructions to run the backend scripts in the schema.

1.3.1 Running Backend Scripts

This topic provides the systematic instructions to run the backend scripts in the schema.

You must compile specific tables related to the Scheduler in the schema that are pointed by the application. Use the latest qualified version of Quartz.

Follow the steps given below:

1. Download Quartz Latest Qualified **Version.gz** file from the following URL: `http://www.quartz-scheduler.org/download/download-catalog.html`.

2. Extract the **gz** file.

3. Open the **Quartz-Latest Qualified Version\docs\dbTables** folder and run the **tables_oracle.sql** (this is specific to Oracle Database) in the schema.

> ✎ **Note:**
>
> For more details on the latest version of the software qualified with Oracle FLEXCUBE, refer to the release certificate.

1.4 Integration of Oracle FLEXCUBE UBS and BIP Reports

This topic explains integration of Oracle FLEXCUBE UBS and BIP Reports.

For more details about integrate Oracle FLEXCUBE UBS and BIP reports, refer to the *BIP Web Service Reports* chapter in the *Oracle Analytics Publisher Web Service Reports* user manual.

- Deploy Application Through Application Server's Admin Console
  This topic explains deployment of application through Weblogic Administration Console.

1.4.1 Deploy Application Through Application Server's Admin Console

This topic explains deployment of application through Weblogic Administration Console.

For more details related to the deployment of Application using Weblogic Administration Console, refer to the *Deploying Oracle FLEXCUBE Application on WebLogic* user manual.

1.5 Integration of Oracle FLEXCUBE UBS and MBean

This topic explains to integrate Oracle FLEXCUBE UBS with MBean plug-in.

To integrate Oracle FLEXCUBE UBS and MBean, you must follow the below steps before deploying the Oracle FLEXCUBE UBS EAR file created with MBean as a Plugin.

- Startup Script Modification
  This topic explains the Startup Script Modification.

1.5.1 Startup Script Modification

This topic explains the Startup Script Modification.

By default, the TopLink used in MBean uses Oracle xml parser internally. However, Weblogic Server has to use JAXPlatform.
To change the system property, follow the steps below:

1. Go to the **Weblogic domain** home folder.

    a. Based on the operating system used, open **startWeblogic.cmd** (Windows) or **startWeblogic.sh** (Linux) from the **bin** folder.

    b. Search for **WLS_REDIRECT_LOG**. After **%JAVA_OPTIONS%** add the following code under **if and else** conditions.

       ```
       -Dtoplink.xml.platform=oracle.toplink.platform.xml.jaxp.JAXPPlatform
       ```
       Now, the details will look like this:

       ```
       if "%WLS_REDIRECT_LOG%"=="" (
       echo Starting WLS with line:
       echo %JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% -
       Dweblogic.Name=%SERVER_NAME% -
       ```

ORACLE

```
Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%JAVA_OPTIONS% %PROXY_SETTINGS% %SERVER_CLASS%
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% -
Dweblogic.Name=%SERVER_NAME% -
Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%JAVA_OPTIONS% -
Dtoplink.xml.platform=oracle.toplink.platform.xml.jaxp.JAXPPlatform
%PROXY_SETTINGS% %SERVER_CLASS%
) else (
echo Redirecting output from WLS window to %WLS_REDIRECT_LOG%
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% -
Dweblogic.Name=%SERVER_NAME% -
Djava.security.policy=%WL_HOME%\server\lib\weblogic.policy
%JAVA_OPTIONS% -
Dtoplink.xml.platform=oracle.toplink.platform.xml.jaxp.JAXPPlatform
%PROXY_SETTINGS% %SERVER_CLASS% >"%WLS_REDIRECT_LOG%" 2>&1
)
```

2. Restart the Weblogic server.

ORACLE