# Oracle® Banking Payments Payments Weblogic Configuration





Oracle Banking Payments Payments Weblogic Configuration, Release 14.8.0.0.0

G32382-01

Copyright © 2017, 2025, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

### Contents

face	
Purpose	1-1
Audience	1-1
Documentation Accessibility	1-1
Critical Patches	1-1
Diversity and Inclusion	1-2
Conventions	1-2
nfigure SSL on Oracle Weblogic	
Set up SSL on Oracle Weblogic	2-1
Certificates and Keypairs	2-1
ain the Identity Store	
Create Identity Store with Trusted Certificates Issued by CA	4-2
nfigure Identity and Trust Stores for Weblogic	
Enable SSL on Oracle Weblogic Server	5-:
Configure Identity and Trust Stores	5-2
SSL Attributes for Managed Servers	
SSL Attributes for Managed Servers  Set SSL Attributes for Private Key Alias and Password	6-:
t	Purpose Audience Documentation Accessibility Critical Patches Diversity and Inclusion Conventions  Infigure SSL on Oracle Weblogic Set up SSL on Oracle Weblogic Certificates and Keypairs  Dose the Identity and Trust Stores  Itain the Identity Store  Create Identity Store with Trusted Certificates Issued by CA Infigure Identity and Trust Stores  Enable SSL on Oracle Weblogic Server Configure Identity and Trust Stores



### 8 Create Resources on Weblogic

8.1	Reso	ource Administration	8-1
	8.1.1	Create Data Source	8-1
	8.1	1.1 XA Enabled Data Source	8-3
	8.1	1.2 Non-XA Enabled Data Source	8-12
	8.1.2	JMS Server Creation	8-21
	8.1.3	JMS Modules Creation	8-29
	8.1.4	Subdeployment Creation	8-35
	8.1.5	JMS Queue Creation	8-41
	8.1.6	JMS Connection Factory Creation	8-47
8.2	Conf	igure Weblogic for Oracle Banking Payments	8-55
8.3	Setu	p/Configure Mail Session in Weblogic	8-60
	8.3.1	Create JavaMail Session	8-60
	832	Configuration of the TLS/SSL Trust Store for Weblogic Server	8-65



1

### **Preface**

- Purpose
- Audience

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

- Documentation Accessibility
- Critical Patches
- · Diversity and Inclusion
- Conventions

### 1.1 Purpose

This guide is designed to help acquaint you with the Oracle Banking Payments application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

### 1.2 Audience

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

Table 1-1 User Roles

Role	Function
Implementation & IT Staff	Implementation & Maintenance of the Software

### 1.3 <u>Documentation Accessibility</u>

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

#### **Access to Oracle Support**

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

### 1.4 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 make sure effective security, as strongly recommended by Oracle Software Security Assurance.

### 1.5 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.

### 1.6 Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text.
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.



### Configure SSL on Oracle Weblogic

This topic explains to configure SSL on Oracle WebLogic.

This chapter details out the configurations for SSL on the Oracle Weblogic application server.

- Set up SSL on Oracle Weblogic
   This topic explains in setting up the SSL on Oracle Weblogic.
- Certificates and Keypairs
   This topic explains the Certificates and Keypairs used for validating the authenticity of the server.

### 2.1 Set up SSL on Oracle Weblogic

This topic explains in setting up the SSL on Oracle Weblogic.

To setup SSL on the Oracle Weblogic application server, you need to perform the following tasks:

- Obtain an identity (private key and digital certificates) and trust (certificates of trusted certificate authorities) for the Oracle Weblogic application server.
- 2. Store the identity and trust. Private keys and trust CA certificates are stored in key stores.
- **3.** Configure the identity and trust the key stores for the Oracle Weblogic application server in the administration console.
- Set SSL attributes for the private key alias and password in the Oracle Weblogic administration console.

### 2.2 Certificates and Keypairs

This topic explains the Certificates and Keypairs used for validating the authenticity of the server.

Certificates are used for validating the authenticity of the server. Certificates contain the name of the owner, certificate usage, duration of validity, resource location, or distinguished name (DN), which includes the common name (CN - website address or e-mail address depending on the usage) and the certificate ID of the person who certified (signs) this information. It also contains the public key and a hash to ensure that the certificate has not been tampered with. A certificate is insecure until it is signed. Signed certificates cannot be modified.

A certificate can be self-signed or obtained from a reputable certificate authority such as Verisign, Inc., Entrust.net, Thawte, GeoTrust, or InstantSSL.

SSL uses a pair of cryptographic keys - a **public key** and a **private key**. These keys are similar in nature and can be used alternatively. What one key encrypts can be decrypted by the other key of the pair. The private key is kept secret, while the public key is distributed using the certificate.

A key tool stores the keys and certificates in a keystore. The default keystore implementation implements it as a file. It protects private keys with a password. The different entities (key pairs

and the certificates) are distinguished by a unique 'alias'. Through its keystore, the Oracle Weblogic server can authenticate itself to other parties.

In Java, a keystore is a **java.security.KeyStore** instance that you can create and manipulate using the keytool utility provided with the Java Runtime.

There are two keystores to be managed by the Oracle Weblogic server to configure SSL.

- Identity Keystore: This contains the key pairs and the Digital certificate. This can also contain certificates of intermediate CAs.
- Trust Keystore: Contains the trusted CA certificates.



### Choose the Identity and Trust Stores

This topic explains to choose the identity and trust stores.

Oracle Financial Services Software recommends that the choice of Identity and Trust stores be made upfront. Oracle Weblogic server supports the following combinations of Identity and Trust stores:

- Custom Identity and Command Line Trust
- Custom Identity and Custom Trust
- · Custom Identity and Java Standard Trust
- Demo Identity and Demo Trust

Oracle Financial Services does not recommend choosing Demo Identity and Demo Trust for production environments.

It is recommended to separate the identity and trust stores since each Weblogic server tends to have its own identity but might have the same set of trust CA certificates. Trust stores are usually copied across Oracle Weblogic servers to standardize trust rules; it is acceptable to copy trust stores since they contain public keys and certificates of CAs. Unlike trust stores, identity stores contain private keys of the Oracle Weblogic server and hence should be protected against unauthorized access.

Command Line Trust, if chosen requires the trust store to be specified as a command-line argument in the Weblogic Server startup script. No additional configuration of the trust store is required in the Weblogic Server Administration Console.

Java Standard Trust would rely on the cacerts files provided by the Java Runtime. This file contains the list of trust CA certificates that ship with the Java Runtime and are located in the <code>JAVA\_HOME/jre/lib/security</code> directory. It is highly recommended to change the default Java standard trust store password and the default access permission of the file. Certificates of most commercial CAs are already present in the Java Standard Trust store. Therefore, it is recommended to use the Java Standard Trust store whenever possible. The rest of the document will assume the use of Java Standard Trust since most CA certificates are already present in it.

One can also create custom trust stores containing the list of certificates of trusted CAs.

For further details on identity and trust stores, please refer to the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server.

4

### Obtain the Identity Store

This topic explains in obtaining the identity store.

#### **Create Identity Store with Self-Signed Certificates**

Self-signed certificates are acceptable for use in a testing or development environment. Oracle Financial Services does not recommend the use of self-signed certificates in a production environment.

To create a self-signed certificate, the genkeypair option provided by the keytool utility of Sun Java 6 needs to be utilized.

#### **Creation of Self-signed Certificate**

Browse to the bin folder of JRE from the command prompt and type the following command.

keytool -genkeypair -alias alias -keyalg RSA -keysize 1024 -sigalg SHAlwithRSA -validity 365 -keystore keystore In the above command.

- 1. **alias** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
- 2. **keystore** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

- Keystore Password: Specify a password that will be used to access the keystore. This
  password needs to be specified later when configuring the identity store in Oracle
  Weblogic Server.
- Key Password: Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later when configuring the SSL attributes of the managed server(s) in the Oracle Weblogic Server.
- **3. First and Last Name (CN):** Enter the domain name of the machine used to access FLEXCUBE UBS, for instance, www.example.com
- 4. Name of your Organizational Unit: The name of the department or unit making the request, for example, BPD. Use this field to identify the SSL Certificate you are creating, for example, by department or by the physical server.
- 5. Name of your Organization: The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.
- Name of your City or Locality: The city in which your organization is physically located, for example. Mumbai.
- **7. Name of your State or Province:** The state/province in which your organization is physically located, for example, Maharashtra.
- **8. Two-Letter Country Code for this Unit:** The country in which your organization is physically located, for example, US, UK, IN, etc.

#### Figure 4-1 Stop image

The key generation algorithm has been specified as RSA, the key size as 1024 bits, the signature algorithm as SHA1withRSA, and the validity days as 365. These can be changed to suitable values if the need arises. For further details, please refer to the documentation of the keytool utility in the JDK utilized by the Oracle Weblogic Server.

Listed below is the result of a sample execution of the command:

```
D:\Oracle\weblogic11g\jrockit 160 05 R27.6.2-20\bin>keytool -
genkeypair -alias selfcert -keyalg RSA -keysize 1024 -sigalg
SHA1withRSA -validity 365 -keystore D:\keystores\FCUBSKeyStore.jks
Enter keystore password: < Enter a password to protect the keystore >
Re-enter new password: < Confirm the password keyed above>
What is your first and last name?
[Unknown]: cvrhp0729.i-flex.com
What is the name of your organizational unit?
  [Unknown]: BPD
What is the name of your organization?
  [Unknown]: Oracle Financial Services
What is the name of your City or Locality?
  [Unknown]: Mumbai
What is the name of your State or Province?
  [Unknown]: Maharashtra
What is the two-letter country code for this unit?
  [Unknown]: IN
Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services, L=Mumbai,
ST=Maharashtra, C=IN correct?
  [no]: yes
Enter key password for <selfcert>
(RETURN if same as keystore password): < Enter a password to protect the key>
Re-enter new password: < Confirm the password keyed above>
```

Create Identity Store with Trusted Certificates Issued by CA
 This topic explains to create identity store with trusted certificates issued by CA.

### 4.1 Create Identity Store with Trusted Certificates Issued by CA

This topic explains to create identity store with trusted certificates issued by CA.

#### Create Public and Private Key Pair

Browse to the bin folder of JRE from the command prompt and type the following command.

```
keytool -genkeypair -alias alias -keyalg keyalg -keysize keysize -
sigalg sigalg -validity valDays -keystore keystore
In the above command,
```

- 1. **alias** is used to identify the public and private key pair created. This alias is required later when configuring the SSL attributes for the managed servers in Oracle Weblogic Server.
- 2. **keyalg** is the key algorithm used to generate the public and private key pair. The RSA key algorithm is recommended.

- 3. **keysize** is the size of the public and private key pairs generated. A key size of 1024 or more is recommended. Please consult with your CA on the key size support for different types of certificates.
- 4. **sigalg** is the algorithm used to generate the signature. This algorithm should be compatible with the key algorithm and should be one of the values specified in the Java Cryptography API Specification and Reference.
- 5. valdays is the number of days for which the certificate is to be considered valid. Please consult with your CA on this period.
- 6. **keystore** is used to specify the location of the JKS file. If no JKS file is present in the path provided, one will be created.

The command will prompt for the following attributes of the certificate and keystore:

- 1. **Keystore Password:** Specify a password that will be used to access the keystore. This password needs to be specified later when configuring the identity store in Oracle Weblogic Server.
- 2. **Key Password:** Specify a password that will be used to access the private key stored in the keystore. This password needs to be specified later when configuring the SSL attributes of the managed server(s) in the Oracle Weblogic Server.
- 3. First and Last Name (CN): Enter the domain name of the machine used to access FLEXCUBE UBS, for instance, www.example.com
- 4. Name of your Organizational Unit: The name of the department or unit making the request, for example, BPD. Use this field to identify the SSL Certificate you are creating, for example, by department or by the physical server.
- 5. Name of your Organization: The name of the organization making the certificate request, for example, Oracle Financial Services. It is recommended to use the company or organization's formal name, and this name entered here must match the name found in official records.
- 6. Name of your City or Locality: The city in which your organization is physically located, for example, Mumbai.
- 7. Name of your State or Province: The state/province in which your organization is physically located, for example, Maharashtra.
- Two-Letter Country Code for this Unit: The country in which your organization is physically located, for example, US, UK, IN, etc.

D:\Oracle\weblogic11q\jrockit 160 05 R27.6.2-20\bin>keytool -

Listed below is the result of a sample execution of the command:

```
qenkeypair -alias cvrhp0729 -keyalq RSA -keysize 1024 -sigalq
SHA1withRSA -validity 365 -keystore D:\keystores\FCUBSKeyStore.jks
Enter keystore password: < Enter a password to protect the keystore >
Re-enter new password: < Confirm the password keyed above>
What is your first and last name?
[Unknown]: cvrhp0729.i-flex.com
What is the name of your organizational unit?
  [Unknown]: BPD
What is the name of your organization?
```

[Unknown]: Oracle Financial Services

What is the name of your City or Locality? [Unknown]: Mumbai

What is the name of your State or Province?

[Unknown]: Maharashtra

```
What is the two-letter country code for this unit?
  [Unknown]: IN
Is CN=cvrhp0729.i-flex.com, OU=BPD, O=Oracle Financial Services, L=Mumbai,
ST=Maharashtra, C=IN correct?
  [no]: yes
Enter key password for <cvrhp0729>
(RETURN if same as keystore password):<Enter a password to protect the key>Re-enter new password:<Confirm the password keyed above>
```

#### **Generate CSR**

To purchase an SSL certificate, one needs to generate a Certificate Signing Request (CSR) for the server where the certificate will be installed.

A CSR is generated from the server and is the server's unique **fingerprint**. The CSR includes the server's public key, which enables server authentication and secure communication.



If the keystore file or the password is lost and a new one is generated, the SSL certificate and the private key will no longer match. A new SSL Certificate will have to be requested.

The CSR is created by running the following command in the bin directory of the JRE:

keytool -certreq -alias alias -file certreq\_file -keystore keystore In the above command.

- alias is used to identify the public and private key pair. The private key associated with the alias will be utilized to create the CSR. Specify the alias of the key pair created in the previous step.
- 2. certreq\_file is the file in which the CSR will be stored.
- 3. **keystore** is the location of the keystore containing the public and private key pair.

Listed below is the result of a sample execution of the command.

```
D:\Oracle\Weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool -certreq - alias cvrhp0729 -file D:\keystores\certreq.csr - keystoreD:\keystores\FCUBSKeyStore.jks

Enter keystore password: [Enter the password used to access the keystore]
Enter key password for <cvrhp0729>
(RETURN if same as keystore password): [Enter the password used to access the
```

#### **Obtain Trusted Certificate from CA**

key in the keystorel

The processes of obtaining a trusted certificate vary from one CA to another. The CA might perform additional offline verification. Consult the CA issuing the certificate for details on the process to be followed for submission of the CSR and for obtaining the certificate.

#### Import Certificate into Identity Store

Store the certificate obtained from the CA in the previous step, in a file, preferably in PEM format. Other formats like the p7b file format would require conversion to the PEM format.

Details on performing the conversion are not listed here. Please refer to the Oracle Weblogic Server documentation on Securing Oracle Weblogic Server for details on converting a Microsoft **p7b** file to the **PEM** format.

The command to be executed for importing a certificate into the identity store depend on whether the trust store is chosen (in the earlier step; see section 2 of this document). It is highly recommended to verify the trust path when importing a certificate into the identity store. The commands provided below assume the use of the Java Standard Trust store.

#### Import the Intermediate CA certificate

Most Certificate Authorities do not use the root CA certificates to issue identity certificates for use by customers. Instead, Intermediate CAs issue identity certificates in response to the submitted CSRs.

If the Intermediate CA certificate is absent in the Java Standard Trust store, the trust path for the certificate will be incomplete for the certificate, resulting in warnings issued by Weblogic Server during runtime. To avoid this, the intermediate CA certificate should be imported into the identity keystore. Although the intermediate CA certificate can be imported into the Java Standard Trust store, this is not recommended unless the intermediate CA can be trusted.

The following command should be executed to import the intermediate CA certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file -trustcacerts -
keystore keystore
In the above command,
```

- 1. **alias** is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.
- cert\_file is the location of the file containing the intermediate CA certificate in a PKCS#7 format (PEM or DER file).
- 3. **keystore** is the location of the keystore containing the public and private key pair.

The trustcacerts flag is used to consider other certificates (higher intermediaries and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command.

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool - importcert -alias verisigntrialintermediateca - fileD:\keystores\VerisignIntermediateCA.cer -trustcacerts - keystoreD:\keystoreworkarea\FCUBSKeyStore.jks
```

Enter keystore password: < Enter the password used to access the keystore>

Certificate was added to keystore.

#### Import the Identity Certificate

The following command should be executed to import the identity certificate into the keystore.

```
keytool -importcert -alias alias -file cert_file -trustcacerts -
keystore keystore
In the above command.
```

 alias is used to identify the public and private key pair. Specify the alias of the key pair used to create the CSR in the earlier step.



- cert\_file is the location of the file containing the PKCS#7 formatted reply from the CA, containing the signed certificate.
- 3. **keystore** is the location of the keystore containing the public and private key pair.

The trustcacerts flag is used to consider other certificates (intermediate CAs and the root CA) in the chain of trust. If no chain of trust is established during verification, the certificate will be displayed and one would be prompted to verify it. It is recommended that due diligence be observed when the prompt is displayed to verify a certificate when a chain of trust is absent.

Listed below is a sample execution of the command.

```
D:\Oracle\weblogic11g\jrockit_160_05_R27.6.2-20\bin>keytool - importcert -alias cvrhp0729 -file D:\keystores\cvrhp0729.cer - trustcacerts -keystore D:\keystoreworkarea\FCUBSKeyStore.jks
```

Enter keystore password: <Enter the password used to access the keystore> Enter key password for <cvrhp0729>: <Enter the password used to access the private key>

#### Certificate was added to keystore.

The previous set of commands assumed the presence of the appropriate root CA certificate (in the chain of trust) in the Java Standard Trust store, i.e. in the cacerts file. If the CA issuing the identity certificate (for the Weblogic Server) does not have the root CA certificate in the Java Standard Trust store, one can opt to import the root CA certificate into cacerts, or the identity store, depending on factors including the trustworthiness of the CA, the necessity of transporting the trust store across the machine, among others.



## Configure Identity and Trust Stores for Weblogic

This topic explains to configure identity and trust stores for Weblogic.

- Enable SSL on Oracle Weblogic Server
   This topic explains the systematic instructions to enable SSL on Oracle Weblogic Server.
- Configure Identity and Trust Stores
   This topic explains the systematic instructions to configure identity and trust stores.

### 5.1 Enable SSL on Oracle Weblogic Server

This topic explains the systematic instructions to enable SSL on Oracle Weblogic Server.

To configure SSL on the Oracle Weblogic server, login into the Admin Console and follow the steps given below:

- 1. Click the Lock & Edit button under Change Center.
- 2. Expand the **Servers** node.
- **3.** Select the name of the server for which you want to enable SSL (example exampleserver).
- 4. Go to Configuration and select the General tab.
- 5. Select the option **SSL Listen Port Enabled** and specify the SSL listen port.
- Against Listen Address, specify the hostname of the machine in which the application server is installed.

### 5.2 Configure Identity and Trust Stores

This topic explains the systematic instructions to configure identity and trust stores.

To configure the Identity and Trust stores in Oracle Weblogic Server, login to the Admin Console of Weblogic Server.

- Click the Lock & Edit button under Change Center.
- 2. Expand the **Servers** node.
- Select the name of the server for which you want to configure the keystores (example exampleserver).
- 4. Go to **Configuration** and select the **Keystores** tab.
- 5. In the field **Keystores**, select the method for storing and managing private keys/digital certificate pairs and trusted CA certificates. This choice should match the one made in Section 2 of this document (Choosing the Identity and Trust Stores).
- **6.** In the **Identity** section, provide the following details:
  - a. Custom Identity Keystore File Name: Fully qualified path to the Identity keystore.

- b. Custom Identity Keystore Type: Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).
- c. Custom Identity Keystore PassPhrase: The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic Server only reads from the keystore. So whether or not you define this property depends on the requirements of the keystore.
- 7. In the **Trust** section, provide the following details:

If you choose **Java Standard Trust**, specify the password used to access the trust store.

If you choose **Custom Trust**, the following attributes have to be provided:

- a. Custom Trust Keystore: The fully qualified path to the trust keystore.
- **b. Custom Trust Keystore Type**: Set this attribute to JKS, the type of the keystore. If left blank, it defaults to JKS (Java KeyStore).
- c. Custom Trust Keystore Passphrase: The password you enter when reading or writing to the keystore. This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. Oracle Weblogic Server only reads from the keystore. So, whether or not you define this property depends on the requirements of the keystore.



When identity and trust stores are of the JKS format, the passphrases are not required.



6

### Set SSL Attributes for Managed Servers

This topic explains to set SSL attributes for managed servers.

Set SSL Attributes for Private Key Alias and Password
 This topic explais the systematic instruction to set SSL attributes for private key alias and password.

### 6.1 Set SSL Attributes for Private Key Alias and Password

This topic explais the systematic instruction to set SSL attributes for private key alias and password.

To configure the private key alias and password, login to the Oracle Weblogic Server Admin Console.

- 1. Click the Lock & Edit button under Change Center.
- 2. Expand the **Servers** node.
- Select the name of the server for which you want to configure the keystores (example exampleserver).
- 4. Go to **Configuration** and select the **SSL** tab.
- 5. Select **Keystores** from **Identity and Trust Locations**.
- 6. Under **Identity** section, specify the following details:
  - a. **Private Key Alias:** Set this attribute to the alias name defined for the key pair when creating the key pair in the Identity keystore.
  - **b. Private Key Passphrase:** The password defined for the key pair (alias\_password) at the time of its creation. Confirm the password.
- 7. Click Save.
- 8. Click Activate Changes button under Change Center.
- Go to the controls tab, check the appropriate server, and click Restart SSL. Confirm when it prompts.

7

### **Test Configuration**

This topic explains to test the configuration

Once the Oracle Weblogic has been configured for SSL, deploy the application in the usual manner. The application can be tested in SSL mode after deployment. To launch the application in SSL mode, enter the URL in the following format:

https://(Machine Name):(SSL\_Listener\_port\_no)/(Context\_root)



It is recommended that the Oracle Banking payments web application be accessed via the HTTPS channel instead of the HTTP channel.



### Create Resources on Weblogic

This topic explains the steps to deploy the FC payments application and gateway application in the application server.

#### Resource Administration

This section deals with the process of resource administration on Oracle Weblogic.

#### • Configure Weblogic for Oracle Banking Payments

This section explains the systematic instructions to configure the Oracle WebLogic application server for Oracle Banking Payments.

Setup/Configure Mail Session in Weblogic

This topic explains to setup/configure mail sessions in Weblogic.

### 8.1 Resource Administration

This section deals with the process of resource administration on Oracle Weblogic.

All the resources mention in **Resources To be Created** document are need to be created before deployment. One example for each category is explained in the following subsections.

#### Create Data Source

This topic helps to create data source.

#### JMS Server Creation

This topic explains the systematic instructions to create the JMS server in the Weblogic application server.

#### JMS Modules Creation

This topic explains the systematic instructions to create the JMS Modules in the Weblogic application server.

#### Subdeployment Creation

This topic explains the systematic instructions to create the subdeployment in the Weblogic application server.

#### JMS Queue Creation

This topic explains the systematic instructions to create the JMS Queue in the Weblogic application server.

#### JMS Connection Factory Creation

This topic explains the systematic instructions to create the JMS Connection Factory in the Weblogic application server.

#### 8.1.1 Create Data Source

This topic helps to create data source.

The method for creating data sources is explained under the following headings.

#### **Prerequisites**

To create the data source, the OCI needs to be enabled. For this, download Oracle Instant Client and install it. The details are given below:

Table 8-1 Oracle Instant Client

Package	Download Location	Remarks
Oracle Instant Client Package	https://www.oracle.com/ database/technologies/instant- client/downloads.html	Install Oracle Instant Client in a local directory. While configuring Weblogic for Windows or Unix/Linux box, the user needs to provide the directory path where Instant Client is installed.

The user needs to do the data source configuration with the OCI driver enabled. The configurations are given below.

- Oracle Weblogic on Windows Box:
  - Set {ORACLE HOME} in the environment variable.
  - Update the Environment Variable Path as {ORACLE\_HOME}/Instance Client. This
    is required to load all the .dll files.
  - Ensure that the ojdbc\*.jar file in {WL\_HOME}/server/lib/ojdbc\*.jar is the same as the file {ORACLE\_HOME}/jdbc/lib/ojdbc\*.jar. This is required for ensuring compatibility.
  - Update PATH in StartWebLogic.bat or setDomainEnv.bat. This must be the directory path where Oracle Instant Client is installed.
- Oracle Weblogic on Unix/Linux Box:
  - Set {ORACLE\_HOME} in the environment variable.
  - Update the environment variable LD\_LIBRARY\_PATH as {ORACLE\_HOME}/lib. This is to load all the .so files.
  - Ensure that the ojdbc\*.jar file in {WL\_HOME}/server/lib/ojdbc\*.jar is the same as the file {ORACLE\_HOME}/jdbc/lib/ojdbc\*.jar. This is to ensure compatibility.
  - Update LD\_LIBRARY\_PATH in StartWeblogic.sh or setDomainEnv.sh. This must be the directory path where Oracle Instant Client is installed.
  - If you are still not able to load the .so files, then you need to update the EXTRA\_JAVA\_PROPERTIES by setting Djava.library.path as {ORACLE\_HOME}/lib in StartWebLogic.sh or setDomainEnv.sh.
- XA Enabled Data Source

This topic explains the systematic instructions to create the XA enabled data source in the Weblogic application server.

Non-XA Enabled Data Source

This topic explains the systematic instructions to create the Non-XA enabled data source in the Weblogic application server.



#### 8.1.1.1 XA Enabled Data Source

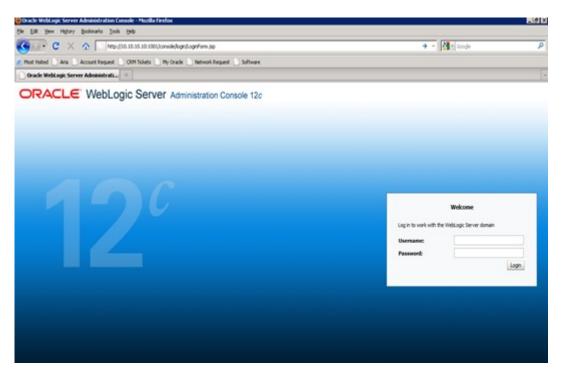
This topic explains the systematic instructions to create the XA enabled data source in the Weblogic application server.

To create the XA enabled data source, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser.

Oracle Weblogic Server - Welcome screen is displayed.

Figure 8-1 Oracle Weblogic Server - Welcome



2. Specify the WebLogic Administrator Username and Password, click **Log In**.

Oracle Weblogic Server - Home Page screen is displayed.



C Home Page - fcubs113\_domain - WLS Censole - Windows Internet Explorer **(3)** + (8) http://10.104.74.143.6 Be Edit Yes Figurities Josh Help O MOATERS -- E - - - - Den - Otok - " ORACLE WebLogic Server® Administration Console Mone Log Out Preferences ☑ Record Help Welcome, weblogic Corrected to: fcubs113 do 9 Click the Lock & Edit button to modify, add or delete items in this domain. - Information and Resources Lock & Est Configure applications
 Configure Shiturik for RAC Data Source
 Recent Task Status Common Administration Task Descript Read the documentation Ask a question on My Crade Support - Domain Configurations Messaging
 345 Servers
 Store and Forward Agents
 345 Modules
 Path Services Jolt Connection Fools • Senera Log Piles
 Diagnostic Modules
 Diagnostic Di Clusters
 Virtual Hosts Migratable Targets
 Coherence Servers Date Sources Persistent Stores
XML Registries
XML Bristy Caches
Foreign JICE Providers How do L Coherence Clusters • Archives Search the configuration
 Use the Change Center
 Record INLST Scripts . Startup And Shutdown Classes Work Contexts Change Console preferences
 Monitor servers Monitoring Deshboard Ø Health of Running Servers Falled (0) · Security Realing Ortical (III) Warning (0) OX (2)

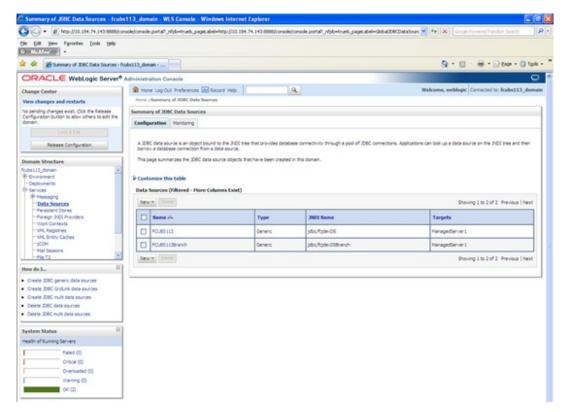
Figure 8-2 Oracle Weblogic Server - Home Page

- 3. Under the Change Center, click on the Lock & Edit button.
- Go to Data Sources.

Summary of JDBC Data Sources screen is displayed.



Figure 8-3 Summary of JDBC Data Sources



On the left pane, under Domain Structure, expand Services and then Data Sources under it. Click the Lock & Edit button.

Summary of JDBC Data Sources - Configuration screen is displayed.



sary of JOBC Data Sources - fcubs113\_domain - WLS Console - Windows Internet Explorer Gie Edit View Figurates Iools Help Com/193/1990 \* Summary of XXEC Data Sources - foubst(13\_domain - ... 💁 \* 🔯 \* 🖟 \* 🖸 Enge \* 🔘 Tgols \* ORACLE WebLogic Server® Administration Console none Log Out Preferences ☑ Record Help Welcome, weblogic Corrected to: fcubs113\_do No pending changes exist. Click the Release Configuration button to allow others to edit the Summary of JOBC Data Sources Configuration Monitoring A 2000 data source is an object bound to the 2000 tree that provides database connectivity through a pool of 2000 connections. Applications can look up a data source on the 2000 tree and then borrow a database connection from a data source. Release Configuration Dismain Structure
Tubes 13, donain
Temperat
Deployment
Deployment
Service
B Hessaging
Data Sources
Persistent Stores
Persistent Stores
Persistent Stores
(No. Contexts
Vol. Registers
Vol. This page summarizes the 2000 data source objects that have been created in this domain. P Customize this table Shoring 1 to 2 of 2 Previous | Next New Y. Conne Generic Data Source 3NDI Name Targets GridLink Data Source denend struttgde/05 Manageddenier ( XM, Entry Caches
-ycox
-Mai Sessions
-Fig 12 CUBS 1138 with stoc/figde/058rands Generic ManagedServer1 New M. Delete Showing 1 to 2 of 2 Previous | Next How do I... Create XBC generic data sources
 Create XBC Gvd.rd data . Create XBC nulti data sources Delete 306C data sources
 Delete 306C multi data sources

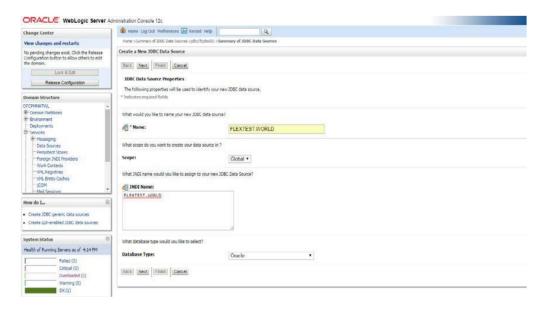
Figure 8-4 Summary of JDBC Data Sources - Configuration

To create a new data source, click New and select Generic Data Source from the dropdown.

Create a New JDBC Data Source screen is displayed.



Ortical (II)
Overloaded (II)
Illiaming (II)
Ox (II)



7. On the **Create a New JDBC Data Source** screen, specify the fields.

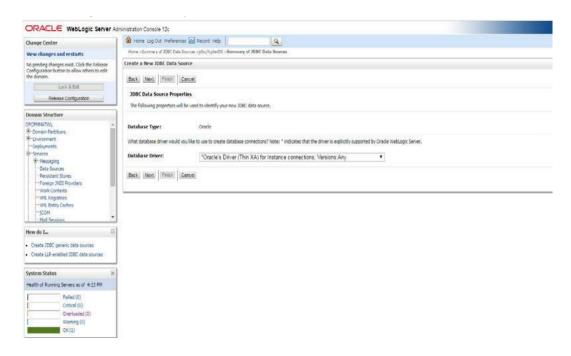
Table 8-2 Create a New JDBC Data Source

Field	Description
JDBC Datasource Name	Name of the data source.
JNDI Name	JNDI name which will be used for lookup.
Database Type	Specify the database type as Oracle from the drop-down list.

8. Click Next.

Create a New JDBC Data Source - JDBC Data Source Properties screen is displayed.

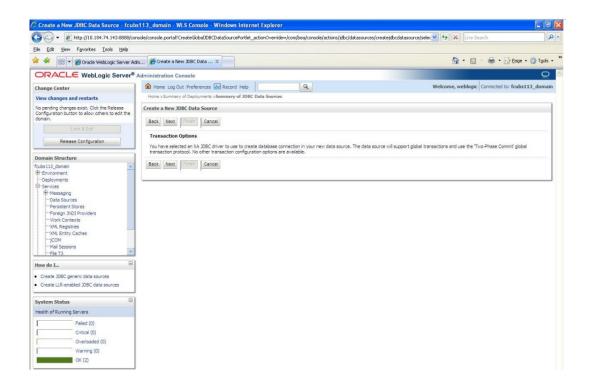
Figure 8-6 Create a New JDBC Data Source - JDBC Data Source Properties



9. Select the database driver from the drop-down list and click **Next**.

Create a New JDBC Data Source - Transaction Options screen is displayed.

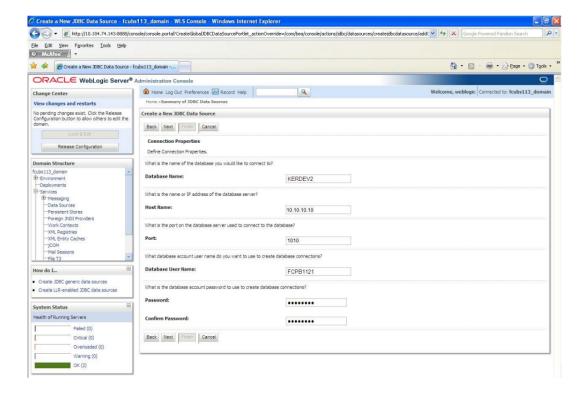
Figure 8-7 Create a New JDBC Data Source - Transaction Options



10. On the Create a New JDBC Data Source - Connection Properties screen, specify the Database Name, Host Name, Port of the database server to connect, Database User Name, Password and Confirm password.

Create a New JDBC Data Source - Connection Properties screen is displayed.

Figure 8-8 Create a New JDBC Data Source - Connection Properties

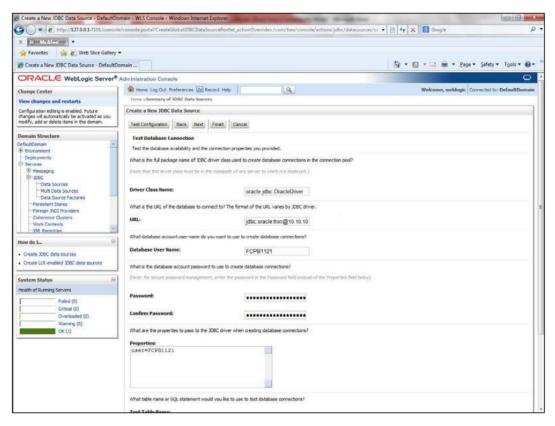




#### 11. Click Next.

Create a New JDBC Data Source - Test Database Connection screen is displayed.

Figure 8-9 Create a New JDBC Data Source - Test Database Connection



- 12. Specify the Driver Class Name (Eg: oracle.jdbc.OracleDriver).
- 13. Specify the URL as jdbc:oracle:thin:@10.10.10.10:1001<INSTANCE NAME>.
- 14. Specify the Database Username (Eg: FCPB1121) and password.
- 15. Confirm the password.
- 16. Click on **Test Configuration** button.
- 17. If the connection is established successfully, the message Connection test succeeded is displayed.

Create a New JDBC Data Source - Messages screen is displayed.



a New JOEC Data Source - fcubs113\_domain - WLS Console - Windows Internet Explorer the tok year figurities look tok Committeens -😭 🍲 🌋 Create a New XXXC Data Source - Frubel 13\_damain -... - D · B · Depr · O Tyck · ORACLE WebLogic Server® Administration Console Change Center

Wew changes and restarts

When changes and restarts

Change Center

One Change Code Storage

One Changes Code Storage

One Change C Sed Configuration | Back | Seed | Freeh | Carcel Test the database availability and the connection properties you provided. tithat is the full package name of 2000 driver class used to create displace connections in the connection pool? oracle jdbc OracleDriver What is the URL of the detabase to connect to? The format of the URL varies by 2000 driver. jdbc oracle oci @10.10.10. What is the database account password to use to create database connections? realth of Running Servers Feled (0) Overbaded (0) What are the properties to pass to the 2060 driver when cleating database con OK (0) Properties user=PCP01121 S Local intranet

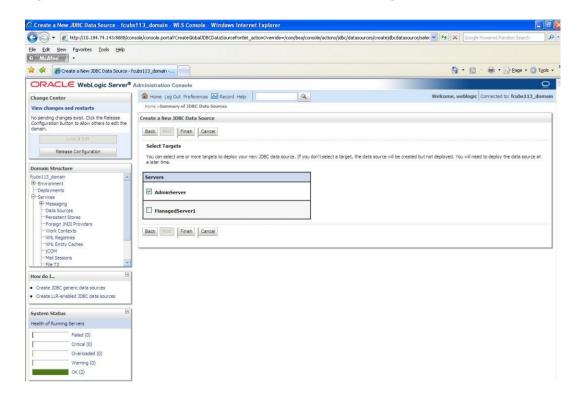
Figure 8-10 Create a New JDBC Data Source - Messages

#### 18. Click Next.

Create a New JDBC Data Source - Select Targets screen is displayed.



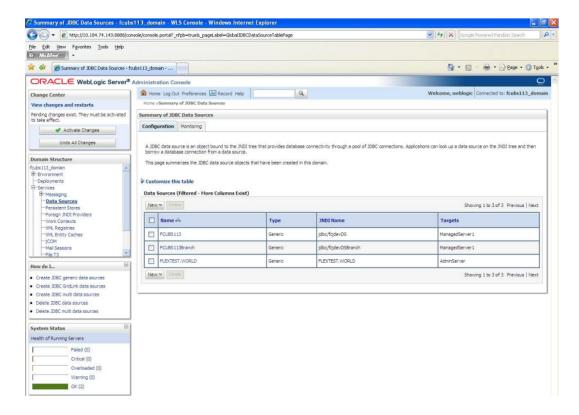
Figure 8-11 Create a New JDBC Data Source - Select Targets



19. Check the boxes against the required servers and click **Finish**.

Summary of JDBC Data Sources - New Data Source screen is displayed.

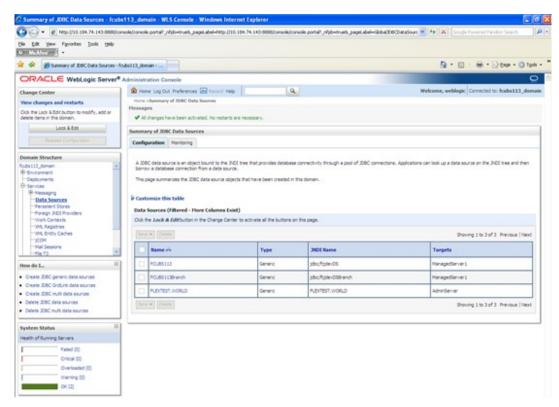
Figure 8-12 Summary of JDBC Data Sources - New Data Source



20. Click the Activate Changes button on the left pane. The message All the changes have been activated. No restarts are necessary is displayed.

Summary of JDBC Data Sources - Activate Changes Message screen is displayed.

Figure 8-13 Summary of JDBC Data Sources - Activate Changes Message



21. Refer to Resources\_To\_ Be\_Created.doc for the list of XA data sources to be created.

New Data Source is created.

#### 8.1.1.2 Non-XA Enabled Data Source

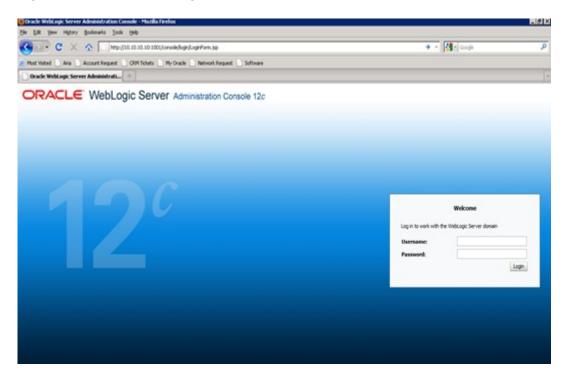
This topic explains the systematic instructions to create the Non-XA enabled data source in the Weblogic application server.

To create the Non-XA enabled data source, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser.

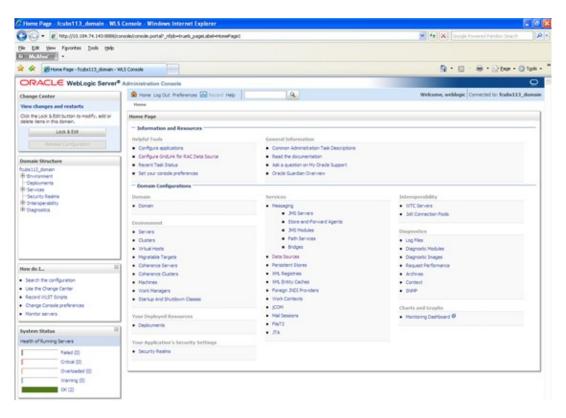
Oracle Weblogic Server - Welcome screen is displayed.

Figure 8-14 Oracle Weblogic Server - Welcome



Specify the WebLogic Administrator Username and Password, click Log In.
 Oracle Weblogic Server - Home Page screen is displayed.

Figure 8-15 Oracle Weblogic Server - Home Page

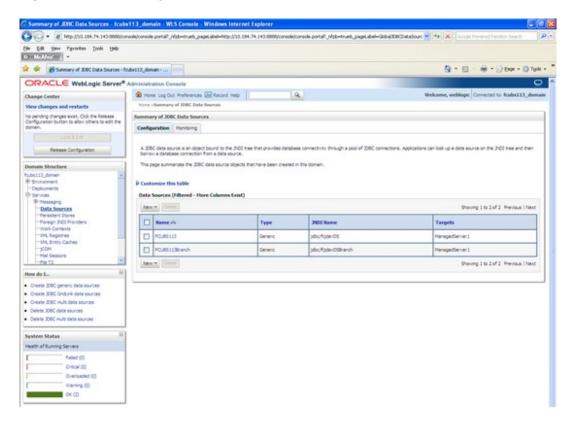




Go to Data Sources.

Summary of JDBC Data Sources screen is displayed.

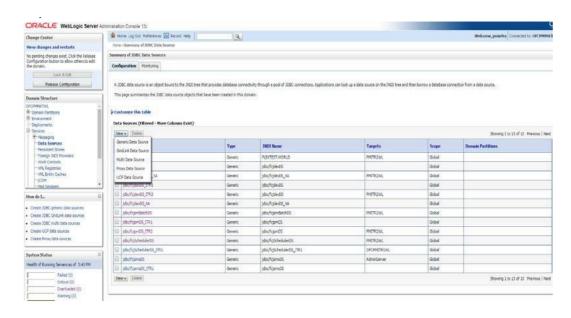
Figure 8-16 Summary of JDBC Data Sources



4. On the left pane, under **Domain Structure**, expand **Services** and then **Data Sources** under it. Click the **Lock & Edit** button.

**Summary of JDBC Data Sources - Configuration** screen is displayed.

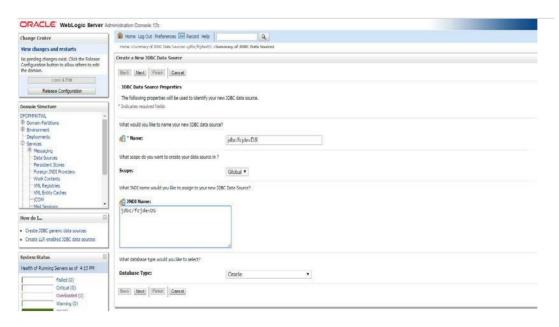
Figure 8-17 Summary of JDBC Data Sources - Configuration



To create a new data source, click New and select Generic Data Source from the dropdown.

Create a New JDBC Data Source screen is displayed.

Figure 8-18 Create a New JDBC Data Source



6. On the Create a New JDBC Data Source screen, specify the fields.

For more information on fields, refer to the field description table.

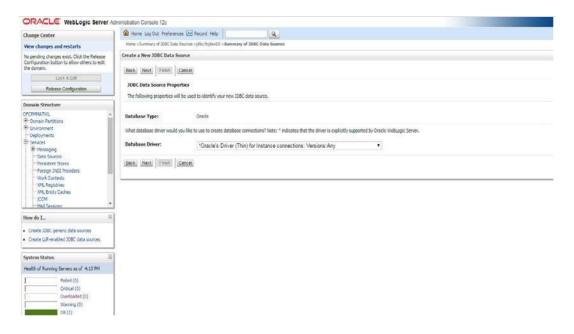
Table 8-3 Create a New JDBC Data Source

Field	Description
JDBC Datasource Name	Name of the Datasource.
JNDI Name	JNDI for lookup.
Database Type	Oracle

7. Click Next.

Create a New JDBC Data Source - JDBC Data Source Properties screen is displayed.

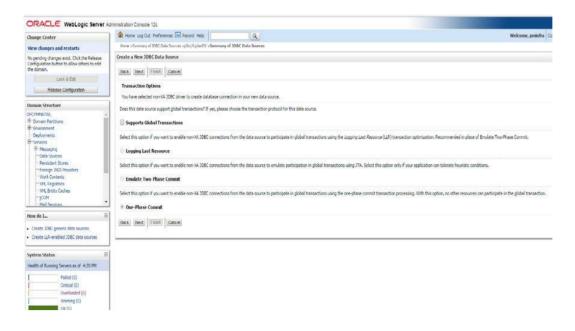
Figure 8-19 Create a New JDBC Data Source - JDBC Data Source Properties



8. Select the database driver as shown in the figure. For Payments Online datasource, check **Support Global Transactions** and Select **Logging Last Resource**.

Create a New JDBC Data Source - Transaction Options screen is displayed.

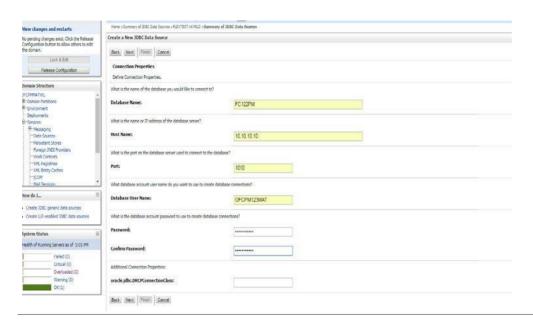
Figure 8-20 Create a New JDBC Data Source - Transaction Options



For other datasources, click Next. The following screen is displayed:

Create a New JDBC Data Source - Connection Properties screen is displayed.

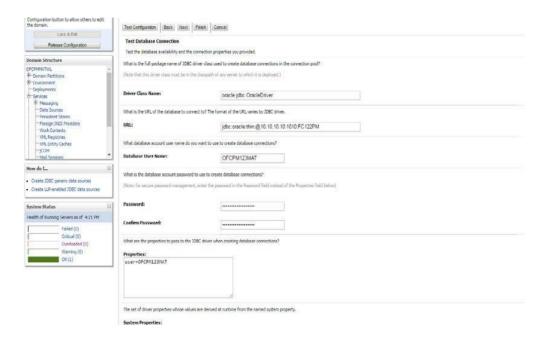
Figure 8-21 Create a New JDBC Data Source - Connection Properties



- The Create a New JDBC Data Source Connection Properties defines the connection properties.
- Specify the Database Name, Host Name, Port of the database server to connect, Database User Name, Password, and Confirm the password.
- 12. Click Next.

Create a New JDBC Data Source - Test Database Connection screen is displayed.

Figure 8-22 Create a New JDBC Data Source - Test Database Connection

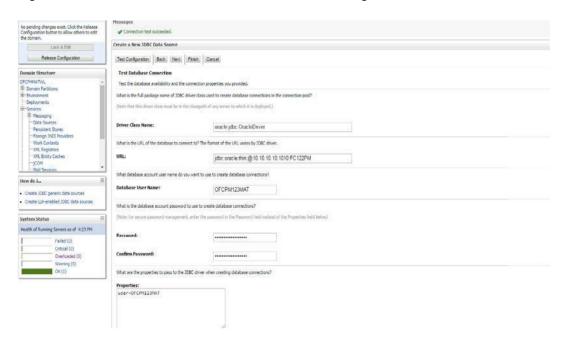


13. Specify the **Driver Class Name** (Eg: oracle.jdbc.OracleDriver).

- **14.** Specify the URL as jdbc:oracle:oci:@10.10.10.10:1010:<INSTANCE\_NAME> from jdbc:oracle:thin:@10.10.10.10.1001<INSTANCE\_NAME>.
- **15.** Specify the Database Username (Eg: testdb) and password.
- **16.** Confirm the password.
- 17. Click on Test Configuration button.
- **18.** If the connection is established successfully, the message Connection test succeeded is displayed.

Create a New JDBC Data Source - Messages screen is displayed.

Figure 8-23 Create a New JDBC Data Source - Messages

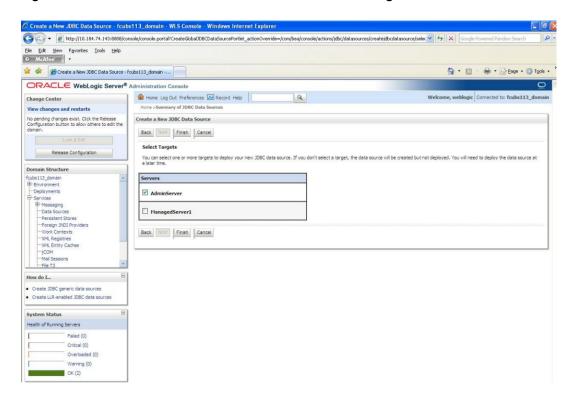


19. Click Next.

Create a New JDBC Data Source - Select Targets screen is displayed.



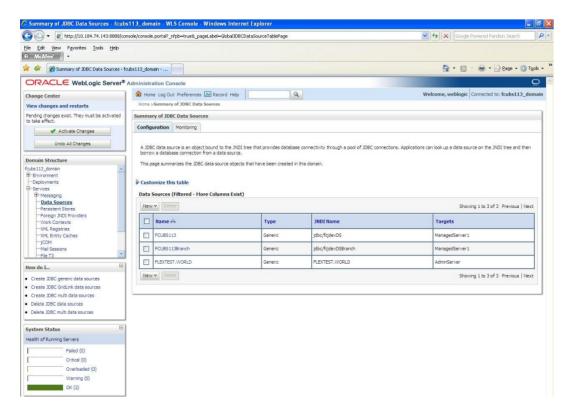
Figure 8-24 Create a New JDBC Data Source - Select Targets



20. Check the boxes against the required servers and click **Finish**.

Summary of JDBC Data Sources - New Data Source screen is displayed.

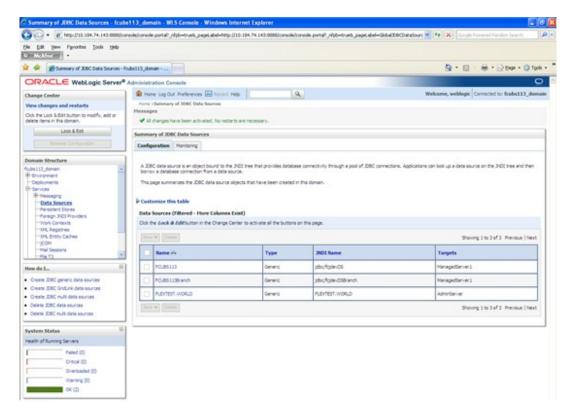
Figure 8-25 Summary of JDBC Data Sources - New Data Source



21. Click the Activate Changes button on the left pane. The message All the changes have been activated. No restarts are necessary is displayed.

Summary of JDBC Data Sources - Activate Changes Message screen is displayed.

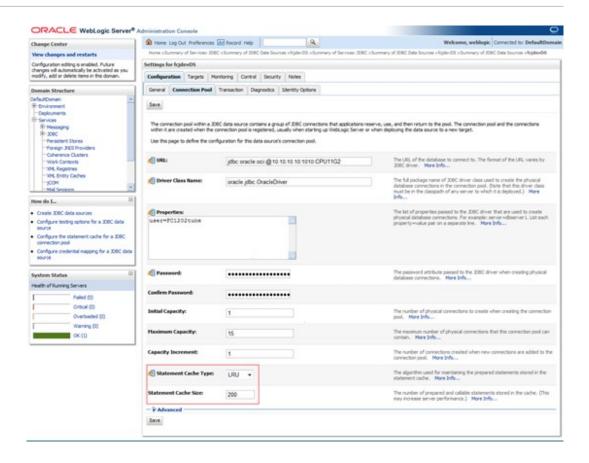
Figure 8-26 Summary of JDBC Data Sources - Activate Changes Message



- 22. The FCUBSDS datasource is created.
- 23. Click the **Datasource**, and then click on the **Connection Pool** tab.

**Settings for fcjdevDS - Connection Pool** screen is displayed.

Figure 8-27 Settings for fcjdevDS - Connection Pool



- 24. On the **Settings for fcjdevDS Connection Pool** screen, select the statement cache type as **LRU** from the drop-down list.
- 25. Specify the statement cache size as 200.
- 26. Click on Save button.
- Refer to Resources\_To\_ Be\_Created.doc for the list of Non-XA data sources to be created.

Note the following:

- You need to create another data source for Oracle FCpayments with the JNDI name '<Non-XA FCUBS HOST JNDI name>\_ASYNC' for the batch process. For example, if the Oracle FCUBS HOST Non-XA data source JNDI name is jdbc/fcjdevDS, then you need to create another data source for FCUBS with the JNDI name jdbc/ fcjdevDS\_ASYNC.
- While creating a branch using the Branch Parameters Maintenance (STDBRANC) screen, if you have created a data source for the branch, then you need to create a corresponding ASYNC data source with the JNDI name <Non-XA FCpayments BRANCH JNDI name>\_ASYNC.

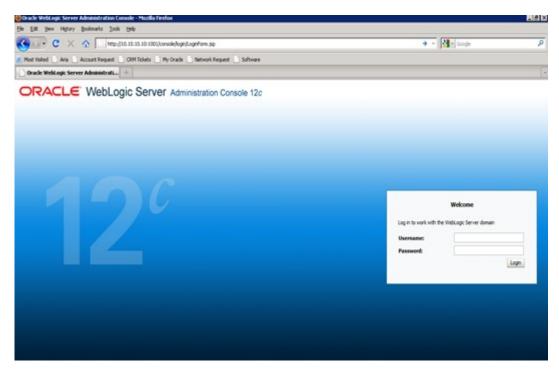
#### 8.1.2 JMS Server Creation

This topic explains the systematic instructions to create the JMS server in the Weblogic application server.

To create the JMS server, follow the steps given below:

 Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser. Oracle Weblogic Server - Welcome screen is displayed.

Figure 8-28 Oracle Weblogic Server - Welcome

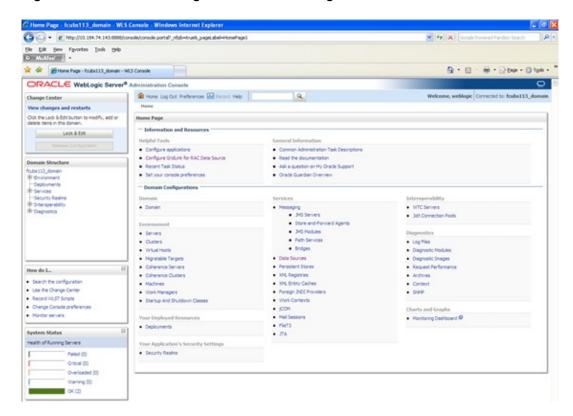


- Specify the WebLogic Administrator Username and Password. Click Login.
- 3. Navigate to Oracle Weblogic home page.

Oracle Weblogic Server - Home Page screen is displayed.



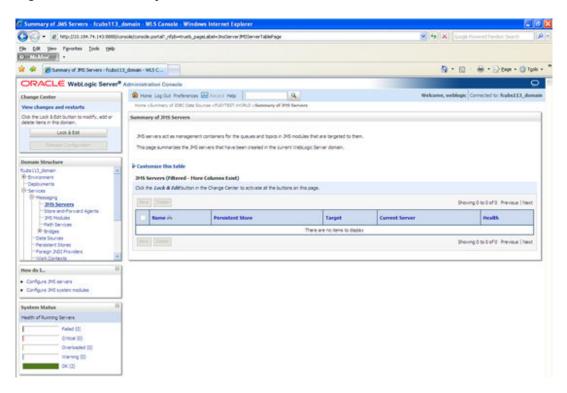
Figure 8-29 Oracle Weblogic Server - Home Page



4. Go to JMS Servers.

Summary of JMS Servers screen is displayed.

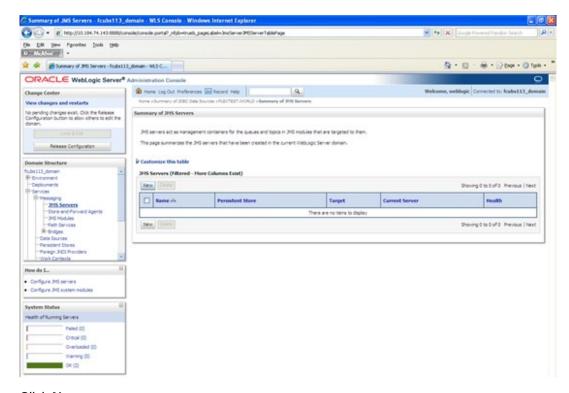
Figure 8-30 Summary of JMS Servers



 On the left pane, under Domain Structure, expand Services, Messaging and JMS Server under it. Click the Lock & Edit button.

Summary of JMS Servers screen is displayed.

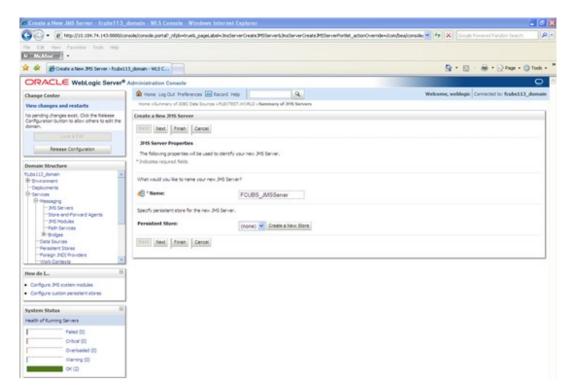
Figure 8-31 Summary of JMS Servers



6. Click New.

Create a New JMS Server screen is displayed.

Figure 8-32 Create a New JMS Server - Store Type



On Create a New JMS Server screen, specify the fields.

For more information on fields, refer to the field description table.

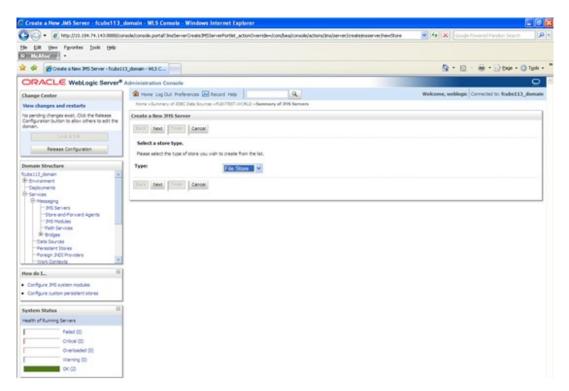
Table 8-4 Create a New JMS Server

Field	Description
JMS Server Name	Specify the name of JMS Server.

8. Click **Create a new Store** button.

Create a New JMS Server - Store Type screen is displayed.

Figure 8-33 Create a New JMS Server - File Store Properties



- 9. Select the **Type** as **File Store** from the drop-down.
- 10. Click Next.

Create a New JMS Server - File Store Properties screen is displayed.

Figure 8-34 Create a New JMS Server - File Store Properties

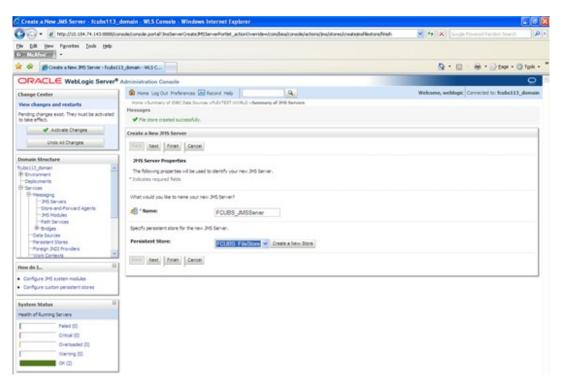


- **11.** To identify the new **File Store**, specify the following properties:
  - a. Specify the file store name as FCpayments\_FileStore.
  - b. Select a server. For this file store, you may select ManagedServer1 (created by the user).

- c. Specify the File store Directory path as C:/FCpayments FileStore.
- d. Click OK.
- 12. Click Next and the message File store created successfully is displayed.

Create a New JMS Server - Messages screen is displayed.

Figure 8-35 Create a New JMS Server - Messages



13. Click Next.

Create a New JMS Server - Select Targets screen is displayed.

C Create a New JMS Server - (cubs113\_domain - WLS Comole - Windows Internet Explorer (Se Edit Yew Figurities Josh (selp On Matthews) 😭 🔗 ② Greate a New 3HS Server - Foubs113\_domain - WLS C.... ORACLE WebLogic Server® Administration Console ★ Home Log Out Preferences 
 ☐ Record Help Welcome, weblogic Connected to: fcubs113 do Pending changes exist. They must be activated to take effect. Create a New 3HS Server Back Tirri From Cancel Undo All Changes Select targets Select the server instance or migratable target on which you would like to deploy this 345 Server. Domain Structure ManagedServer1 ≅ Back Hotel Finan Cancel Configure 345 system modules . Configure outton pensistent stores

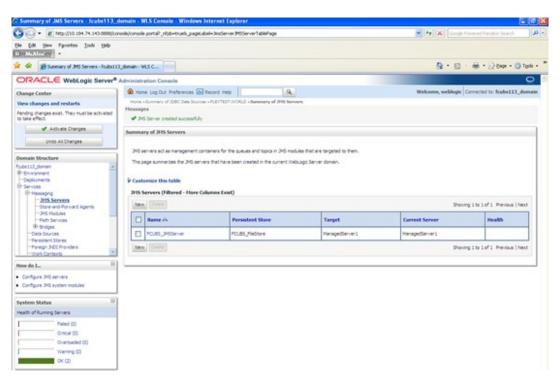
Figure 8-36 Create a New JMS Server - Select Targets

**14.** Select the **Target** as **ManagedServer1**.

System Status
Health of Running Servers
Failed (0)
Criscal (0)
Overloaded

15. Click on Finish and the message JMS Server created successfully is displayed.
Summary of JMS Servers - Messages screen is displayed.

Figure 8-37 Summary of JMS Servers - Messages





**16.** Click the Activate Changes button under Change Center. The message All the changes have been activated. No restarts are necessary is displayed.

JMS Server is created.

#### 8.1.3 JMS Modules Creation

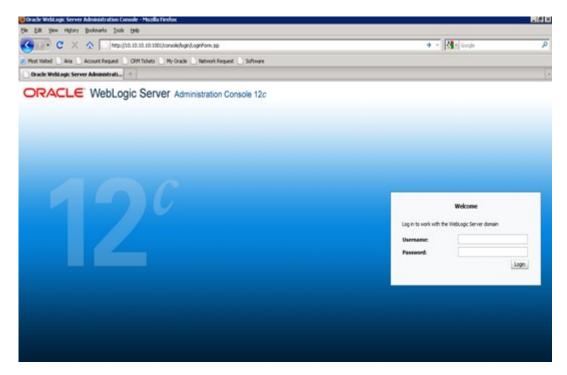
This topic explains the systematic instructions to create the JMS Modules in the Weblogic application server.

To create the JMS Modules, follow the steps given below:

 Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser.

Oracle Weblogic Server - Welcome screen is displayed.

Figure 8-38 Oracle Weblogic Server - Welcome

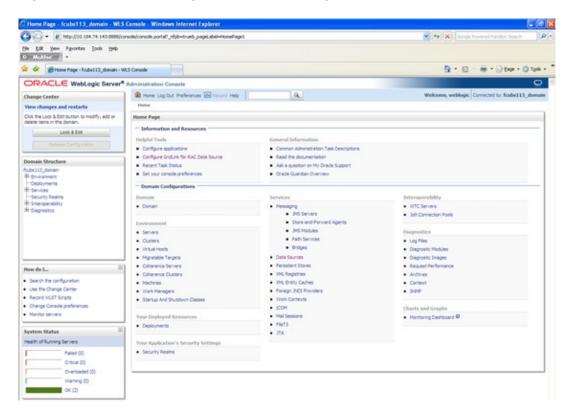


- Specify the WebLogic Administrator Username and Password. Click Log In.
- 3. Navigate to Oracle Weblogic home page.

Oracle Weblogic Server - Home Page screen is displayed.



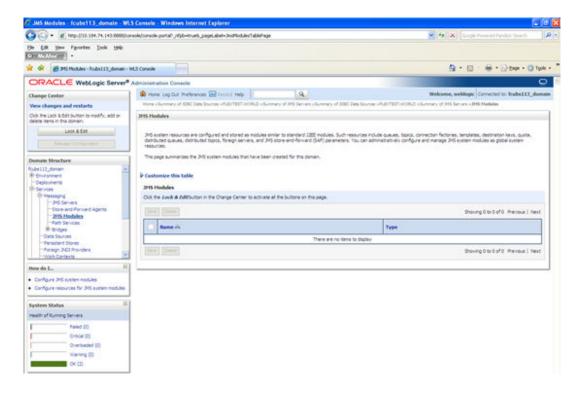
Figure 8-39 Oracle Weblogic Server - Home Page



4. On the left pane, under **Domain Structure**, expand **Services**, **Messaging** and **JMS Modules** under it.

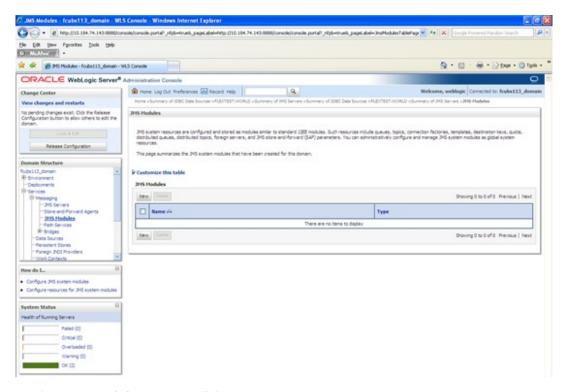
JMS Modules screen is displayed.

Figure 8-40 JMS Modules



To create new JMS Module, click the Lock & Edit button under the Change Center.
 JMS Modules - Change Center screen is displayed.

Figure 8-41 JMS Modules - Change Center

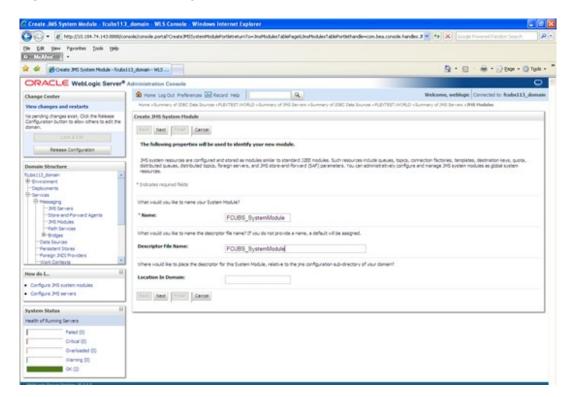


6. On the JMS Modules screen, click New.

Create JMS System Module screen is displayed.



Figure 8-42 Create JMS System Module



7. On Create JMS System Module screen, specify the fields.

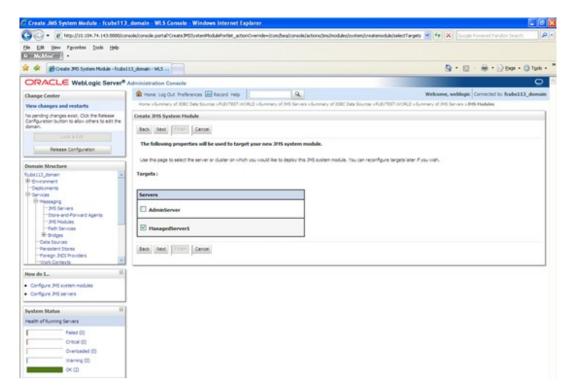
Table 8-5 Create JMS System Module

Field	Description
Name	Enter the System Module Name as FCUBS_SystemModule.
Description File Name	Enter the Description File Name as FCUBS_SystemModule.

8. Click Next.

Create JMS System Module - Targets screen is displayed.

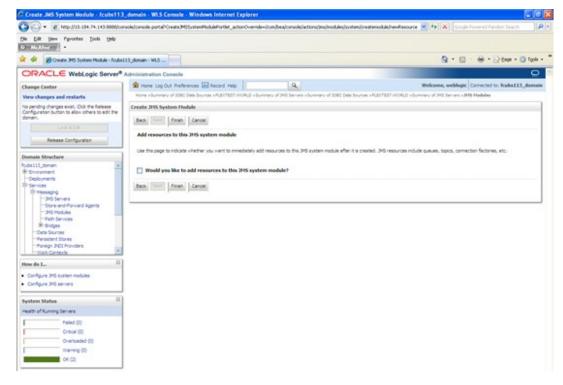
Figure 8-43 Create JMS System Module - Targets



9. Check the box against the server created and click **Next**.

Create JMS System Module - Add Resources screen is displayed.

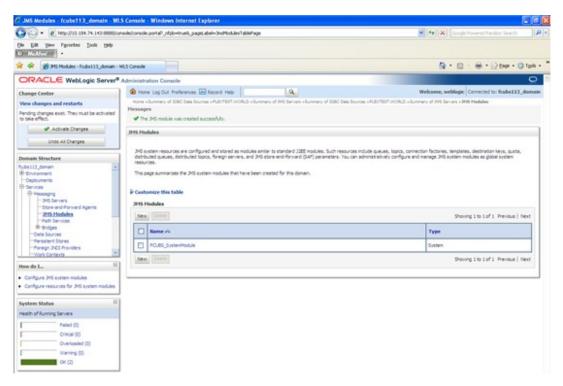
Figure 8-44 Create JMS System Module - Add Resources



10. Click on Finish button.

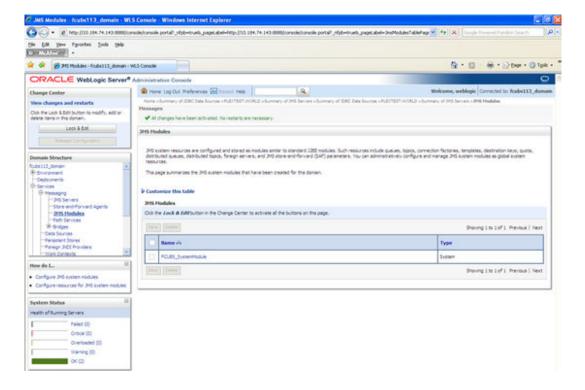
JMS Modules - New screen is displayed.

Figure 8-45 JMS Modules - New



11. Click the Activate Changes button under Change Center. The message All the changes have been activated. No restarts are necessary is displayed.

JMS Modules - Activate Changes screen displays.





The **JMS Module** is created.

## 8.1.4 Subdeployment Creation

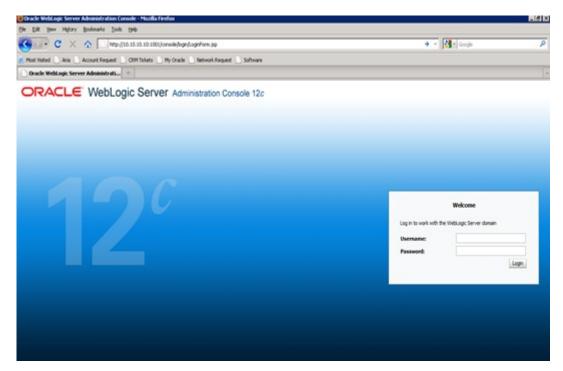
This topic explains the systematic instructions to create the subdeployment in the Weblogic application server.

To create the subdeployments, follow the steps given below:

1. Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser.

Oracle Weblogic Server - Welcome screen is displayed.

Figure 8-46 Oracle Weblogic Server - Welcome

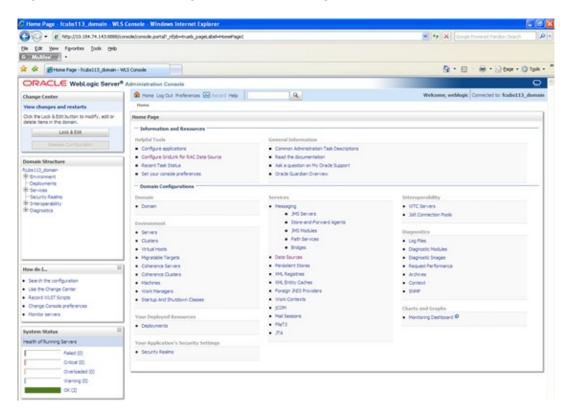


- Specify the WebLogic Administrator Username and Password. Click Log In.
- 3. Navigate to Oracle Weblogic home page.

Oracle Weblogic Server - Home Page screen is displayed.



Figure 8-47 Oracle Weblogic Server - Home Page



 On the left pane, under Domain Structure, expand Services, Messaging and JMS Modules under it.

JMS Modules screen is displayed.

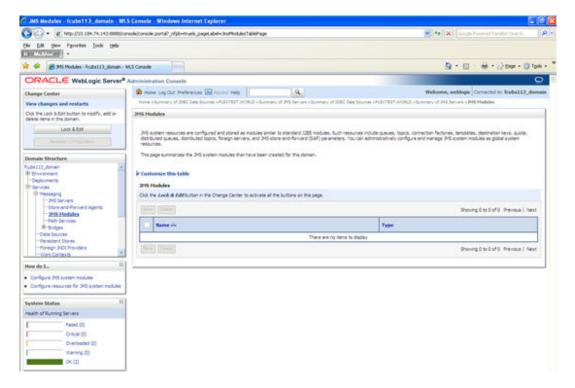
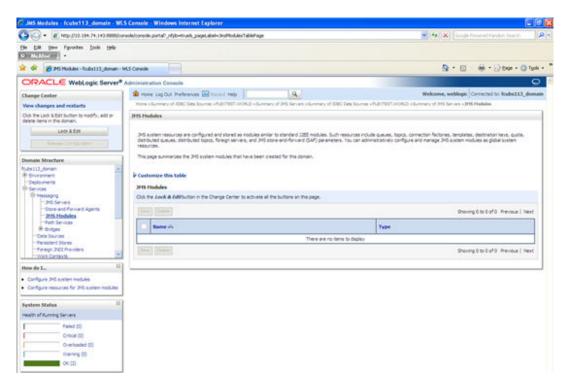


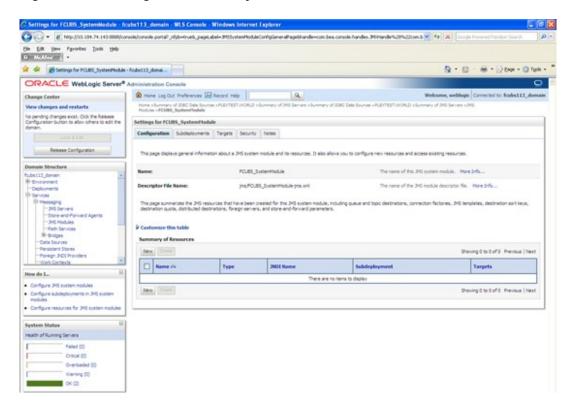
Figure 8-48 JMS Modules



- 5. Click the Lock & Edit button under the Change Center.
- 6. Select the JMS module created earlier.

**Settings for FCUBS\_SystemModule** screen is displayed.

Figure 8-49 Settings for FCUBS\_SystemModule





7. Click on Subdeployments tab.

Settings for FCUBS\_SystemModule - Subdeployments tab is displayed.

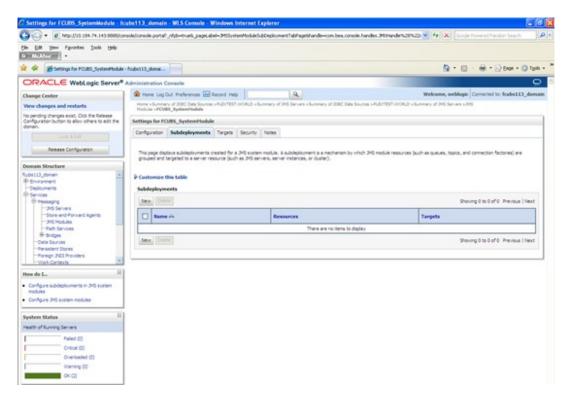
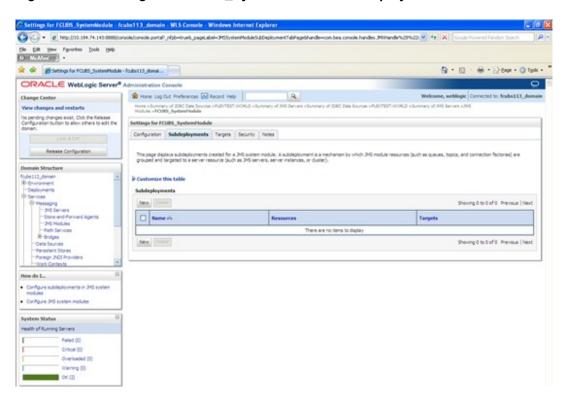


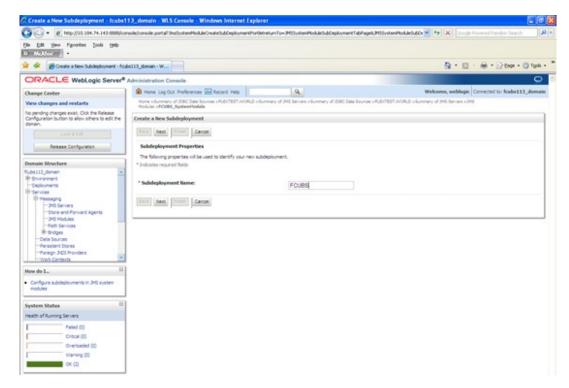
Figure 8-50 Settings for FCUBS\_SystemModule - Subdeployments



8. On the **Subdeployments** tab, click **New**.

Create a New Subdeployment screen is displayed.

Figure 8-51 Create a New Subdeployment

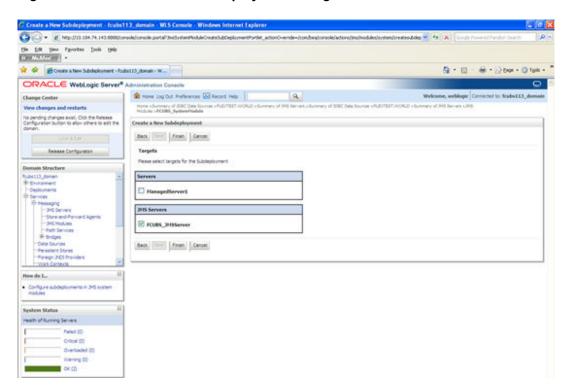


9. On Create a New Subdeployment screen, specify the Subdeployment Name as FCUBS and click Next.

Create a New Subdeployment - Targets screen is displayed.



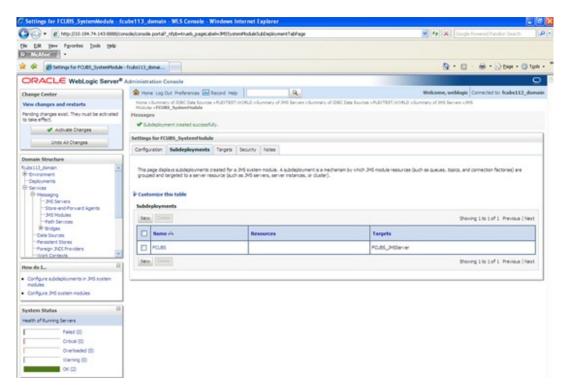
Figure 8-52 Create a New Subdeployment - Targets



- **10.** Select the **JMS Server** (as created by the user).
- 11. Click the Finish button.

FCUBS subdeployment is displayed in the Settings for FCUBS\_SystemModule screen.

Figure 8-53 FCUBS Subdeployment

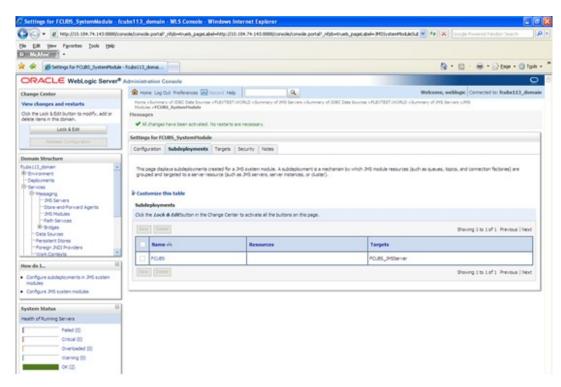




12. Click the Activate Changes button under Change Center. The message All the changes have been activated. No restarts are necessary is displayed.

Settings for FCUBS\_SystemModule - Messages tab is displayed.

Figure 8-54 Settings for FCUBS\_SystemModule - Messages



Subdeployment is created.

# 8.1.5 JMS Queue Creation

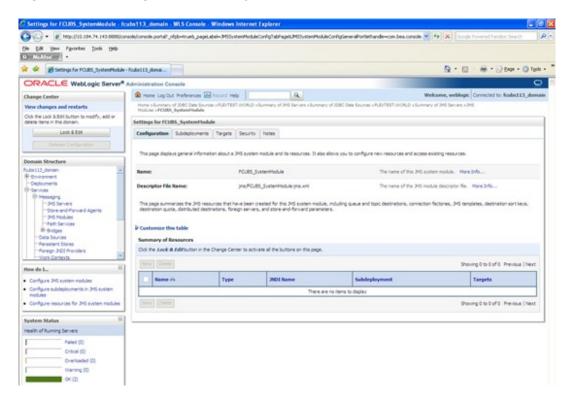
This topic explains the systematic instructions to create the JMS Queue in the Weblogic application server.

To create the JMS Queue, follow the steps given below:

1. Select the JMS Module created earlier.

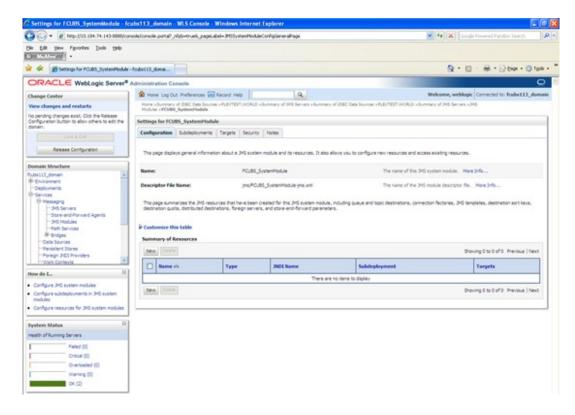
Settings for FCUBS\_SystemModule screen is displayed.

Figure 8-55 Settings for FCUBS\_SystemModule



Click on the Configuration tab and then click Lock & Edit button under Change Center.
 Settings for FCUBS\_SystemModule - Configuration tab is displayed.

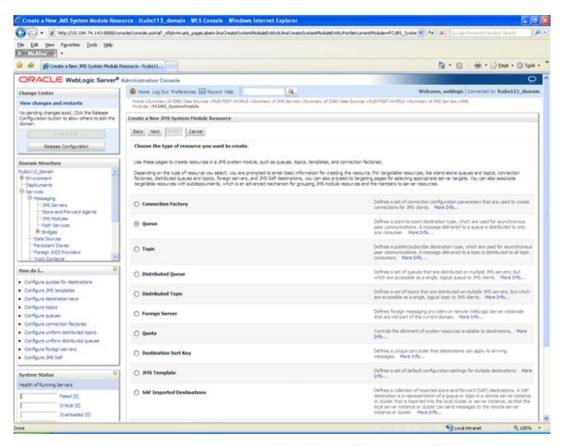
Figure 8-56 Settings for FCUBS\_SystemModule - Configuration





On the Settings for FCUBS\_SystemModule - Configuration tab, click New.
 Create a New JMS System Module Resource screen is displayed.

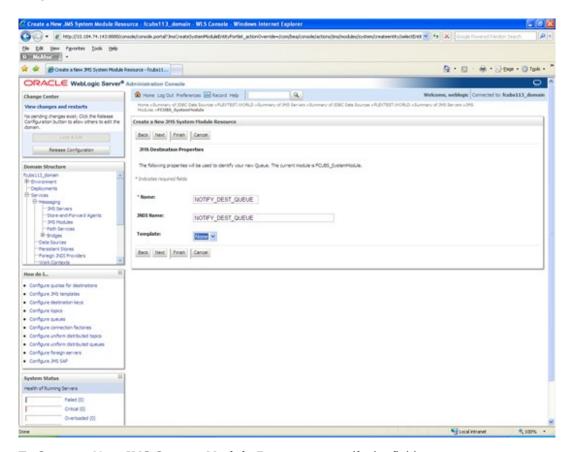
Figure 8-57 Create a New JMS System Module Resource



4. Select the **Queue** option and then click **Next**.

**Create a New JMS System Module Resource - JMS Destination Properties** screen is displayed.

Figure 8-58 Create a New JMS System Module Resource - JMS Destination Properties



5. To Create a New JMS System Module Resource, specify the fields.

**Table 8-6 JMS Destination Properties** 

Filed	Description
Name	Specify the Name of the Queue as NOTIFY_DEST_QUEUE.
JNDI Name	Specify the JNDI Name as NOTIFY_DEST_QUEUE
Template	Select the Template as <b>None</b> from the drop-down.

6. Click Next.

**Create a New JMS System Module Resource - Select Subdeployment** screen is displayed.

Create a New JMS System Module Resource - Scubs113\_domain - WLS Comple - Windows Internet Explorer ( Nepul/10.104.74.140.00 Die Edit Verr Fgrorites Jods 19th Com/92/2019 -😭 🔅 Create a New JMS System Module Resource - Fouts 11... 💁 \* 🔯 - 🙀 \* 🔀 Enge + 🔘 Tgols + " ORACLE WebLogic Server® Administration Console Plone Log Out Preferences Record Help
 Record H Welcome, weblogic Corrected to: fcubs113\_dom Q. Home + Summery of JOSC Data Sources + PLEXTEST / IVORLD + So Hook/ws + PCORS, System Hodule No pending changes exist. Click the Release Configuration button to allow others to edit the Create a New JHS System Hodule Resource Back, Not Fran Carcel The following properties will be used to target your new 3HS system module resource Resease Configuration Use this page its select a subdishipment to assign this system module resource. A subdishipment is a mechanism by which 2HS resources are grouped and targeted to a server instance, duster, or SHP agent. Of necessary, you can create a new subdisplayment by cloting the Create a New Subdisplayment button. You can also reconfigure subdisplayment begins later by using the parent modular's subdisplayment amanagement ages. Domain Structure

Outs 13, Johan

B throwware

- Desponses

- Personnes

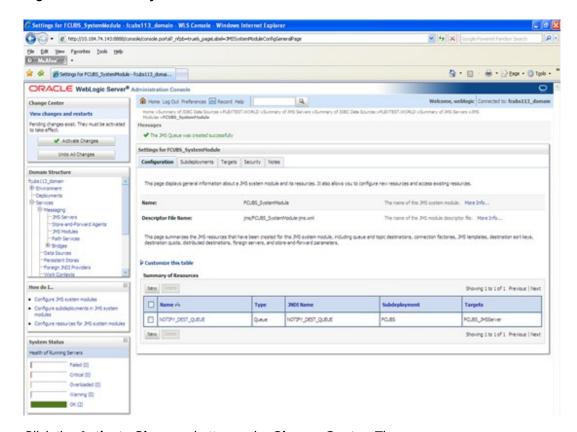
- Personne Select the subdeployment you want to use. If you select (hone), no targeting will occur. FCUBS V Create a New Subdeployment Tithet targets do you want to assign to this subdeployment? JP15 Servers Wark Contents ⊕ FCUBS\_3HSServer How do I... Configure quotes for destructions
Configure 3HS templates
Configure destruction keys
Configure topics
Configure queues Back Hot Fresh Cancel Configure connection factories
Gonfigure uniform distributed topics
Gonfigure uniform distributed queues Configure foreign servers
 Configure 3HS SAF Health of Running Servers CHINA (S) Overloaded (0) S Local Intranet

Figure 8-59 Create a New JMS System Module Resource - Select Subdeployment

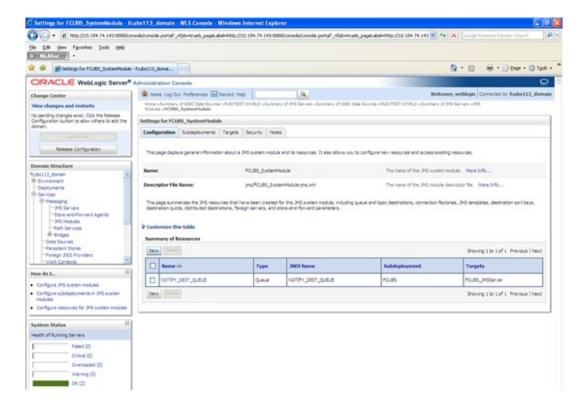
7. Select the managed server created and click **Finish** button.

New JMS System Module Resource is created.

Figure 8-60 JMS System Module Resource



8. Click the Activate Changes button under Change Center. The message All the changes have been activated. No restarts are necessary is displayed.



9. Click **New** to create more Queues. Follow the steps from 3 to 7.

The JMS Queue has been created successfully

### 8.1.6 JMS Connection Factory Creation

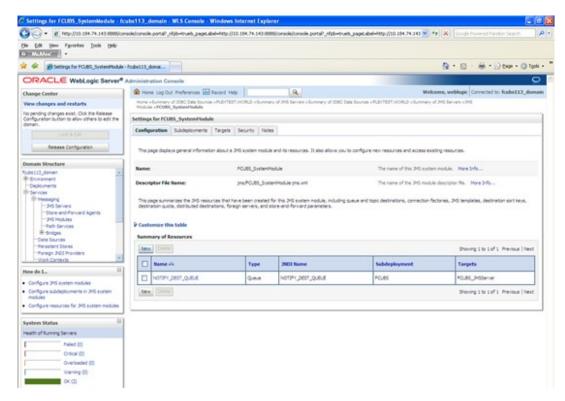
This topic explains the systematic instructions to create the JMS Connection Factory in the Weblogic application server.

After creating the queues, you need to create the connection factory. To create the JMS Connection Factory, follow the steps given below:

Select the JMS Module created earlier.

Settings for FCUBS\_SystemModule screen is displayed.

Figure 8-61 Settings for FCUBS\_SystemModule



- 2. Click on the Configuration tab and then click Lock & Edit button under Change Center.
- 3. On the **Settings for FCUBS\_SystemModule Configuration** tab, click **New**.

Create a New JMS System Module Resource screen is displayed.



C Create a New JMS System Module Resource - Scubs113\_domain - WLS Comple - Windows Internet Explorer Die Edit Verr Fgrorites Jods 19th On Malances -😭 🔅 Create a New 3HS System Module Resource - Fount11... 💁 \* 🔯 - 📾 \* 🖸 Enge + 🔘 Tgols + " ORACLE WebLogic Server® Administration Console Nome Log Out Preferences ☑ Record Help: Welcome, weblogic Corrected to: fcubs113\_don Q. Home > Summery of JOSC Data Sources > PLEXTEST. WORLD Hodules > PC0856, System Hodules No pending changes exist. Click the Release Configuration button to allow others to edit the Create a New 2015 System Hodule Resource Back Next From Canon Choose the type of resource you want to create. Release Configuration Use these pages to greate resources in a 2HS system module, such as queues, topics, templates, and connection factories. Domain Structure

Dost 11, domain

First woment

Grovers

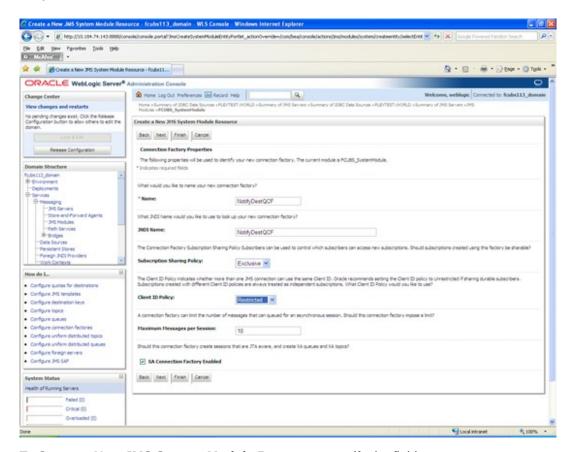
Grovers the resource. For targetable resources, like stand-alone queues and topics, cord to targeting pages for selecting appropriate server targets. You can also assistances and the members to server resources. Connection Factory O Queue Defines a publish/subscribe destination type, which are used for asynchronou peer communications. A message delivered to a topic is distributed to all topic community. More bris... O Topic Work Contents How do I... O Distributed Queue . Configure quotes for destinations Configure destination keys
 Configure topics
 Configure queues Defines foreign messaging providers or remote Webcopic Server instances that are not part of the current domain. More Info... O Foreign Server Configure connection factories
Gonfigure uniform distributed topics
Gonfigure uniform distributed queues Controls the allotment of system resources available to destinations. More 346... O Quota Defines a unique sort order that destinations can apply to arriving messages. More Info... Configure foreign servers
 Configure 345 SAF Defines a set of default configuration settings for multiple destinations. More linfo... O JHS Template CHINA (S) Overloaded (0) S Local Intranet

Figure 8-62 Create a New JMS System Module Resource

4. Select the Connection Factory option and then click Next.

Create a New JMS System Module Resource - Connection Factory Properties screen is displayed.

Figure 8-63 Create a New JMS System Module Resource - Connection Factory Properties



5. To Create a New JMS System Module Resource, specify the fields.

**Table 8-7 Connection Factory Properties** 

Filed	Description
Name	Specify the Name of the Connection factory as NotifyDestQCF.
JNDI Name	Specify the JNDI Name as NotifyDestQCF
Client ID Policy	Select the Client ID policy as <b>Restricted</b> from the drop-down.

- 6. Check the box XA Connection Factory Enabled.
- 7. Click Next.

Create a New JMS System Module Resource - Targets screen is displayed.

urce - fcubs113\_domain - WLS Console - Windows Internet Explorer A . III - A . Deser - O ton -😭 🔅 🌋 Create a New 245 System Module Resource - Frubs I I ... ORACLE WebLogic Server® Administration Console Change Center

Were changes and restarts

When changes and restarts

When changes and restarts .9. Welcome, weblogic Corre No pending changes exist. Clot the Ralesse Configuration button to allow others to edit the Back From Atherces Targeting Cancel The following properties will be used to target your new 2HS system module resource HanagedServer1 Seck From Advanced Tergeting Concel Configure quotas for destruct
Configure 345 templates
Configure destruction keys
Configure topics
Configure queues Configure queues
 Configure connection factories
 Configure curriors des bused topics
 Configure uniform des bused queues
 Configure foreign servers
 Configure 345 SAF Oreos (0) ¶Local intranet € 100% •

Figure 8-64 Create a New JMS System Module Resource - Targets

8. Click on the Advanced Targeting.

Create a New JMS System Module Resource - Advance Targeting screen is displayed.



e a New JMS System Module Resource - Scubs113\_domain - WLS Console - Windows Internet Explorer A . III - A . Deser - O ton -🙀 🍪 Create a New 245 System Module Resource - Fouls LL... ORACLE WebLogic Server® Administration Console Change Center

@ Home Log Out Preferences @ Record Indip

Wore changes and restarts

Type a Survey of JOSC One Source a PLOTEST work a No pending changes exist. Click the Release Configuration button to allow others to edit the Create a New 3HS System Hodule Re-Seck | Fren | Cancel The following properties will be used to target your new 24th system module re-Use this page to select a subdisplayment to assign the sinten module resource. A subdisplayment is a mechanism by which PIG resource are grouped and targeted to a server instance, duster, or SAR agent. Transcearry, not on create a new subdisplayment by clong the Create a New Subdisplayment output. Not can also reconfigure subdisplayment targets later by using the parent modulis's addisplayment management page. Select the subdeployment you want to use. If you select (none), no targeting will occur FCUBS V Create a New Subdeployment What targets do you want to assign to this subdeployment? ☐ Hanagediervert Configure quotas for destri
Configure 376 templates
Configure destruction keys
Configure topics
Configure queues compute quiture
 Configure connection factories
 Configure curriors destituted topics
 Configure uniform destituted quiture
 Configure foreign servers
 Configure 345 SAF Back Tirit From Cancel Oreos (0) ¶Local intranet € 100% •

Figure 8-65 Create a New JMS System Module Resource - Advance Targeting

- 9. Select the **Subdeployments** as **FCUBS** from the drop-down list.
- **10.** Under the JMS Servers, check the box against Managed Server.
- 11. Click on Finish and the message Connection Factory created successfully is displayed.

Settings for FCUBS\_SystemModule - Messages screen is displayed.

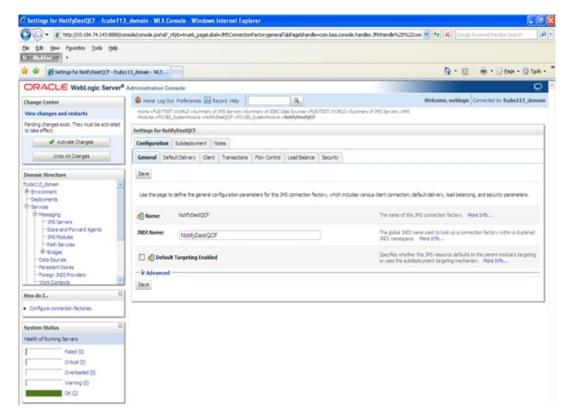
C Settings for FCURS\_SystemModule - fcubs113\_domain - WLS Console - Windows Internet Explorer He Edit Herr Figurites Indis Help Commissions -A . S - A . Stop - O Took - " ORACLE WebLogic Server® Administration Console none Log Out Preferences ☑ Record Help 9. Home >Summary of JOSC Cale Sources >FLEXTEST Hodules >FCVBS\_SystemHodule Pending changes exist. They must be activated to take effect. ◆ Connection factory created successfully ✓ Activate Changes Settings for PCUBS\_SystemPlodule Unite All Changes Configuration Subdeployments Targets Security Notes Domain Structure This page displays general information about a 2HS system module and its resources. It also allows you to configure new resources and access existing resources. PCUBS\_SystemModule Descriptor File Name: jns/PCLBS\_SystemPlodule-jns.xml The name of the 345 module descriptor file. More 346... This page summariors the 345 resources that have been created for this 345 system module, including queue and topic destinations, connection factories, 345 templates, destination sort keys, destination during destinations, distributed destinations, foreign servers, and store and forward parameters. Summary of Resources New Driver Configure 3/6 system modules
 Configure subdeployments in 3/6 system modules JNOS Name Targets ☐ Nest/DestQCF web/deeq0f Connection Factory FCLBS FOJES\_MSServer Configure resources for 345 system ☐ NOTSY\_DEST\_QUEUE PCUBS\_MSServer New Colors Falled (0) Creck (t) Overloaded (0) Harring (0)

Figure 8-66 Settings for FCUBS\_SystemModule - Messages

 To have the XA Connection Factory enabled, click on the Connection Factory NotifyDestQCF.

Settings for NotifyDestQCF screen is displayed.

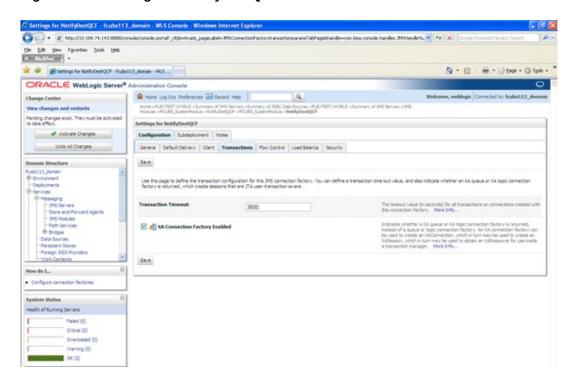
Figure 8-67 Settings for NotifyDestQCF



13. Click on the Transactions tab.

Settings for NotifyDestQCF - Transactions tab is displayed.

Figure 8-68 Settings for NotifyDestQCF - Transactions

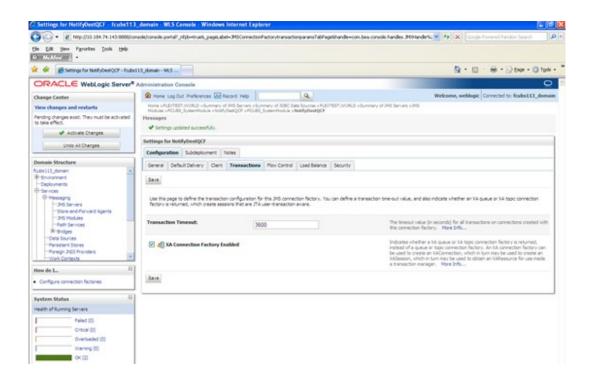




- **14.** Check the box **XA** Connection Factory Enabled.
- **15.** Click the **Save** button and the message Settings updated successfully is displayed.

**Settings for NotifyDestQCF - Messages** screen is displayed.

Figure 8-69 Settings for NotifyDestQCF - Messages



16. Click the Activate Changes button under Change Center. The message All the changes have been activated. No restarts are necessary is displayed.

Settings for NotifyDestQCF - Activate Changes screen is displayed.



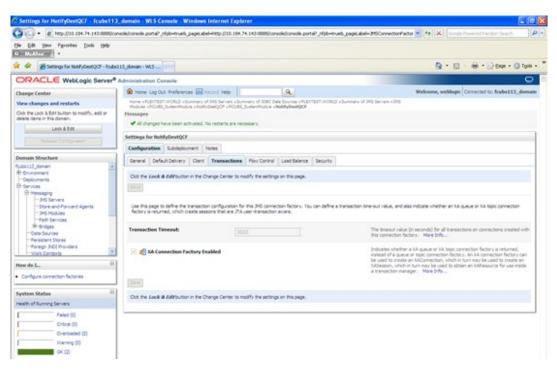


Figure 8-70 Settings for NotifyDestQCF - Activate Changes

The JMS Connection Factory is created.

## 8.2 Configure Weblogic for Oracle Banking Payments

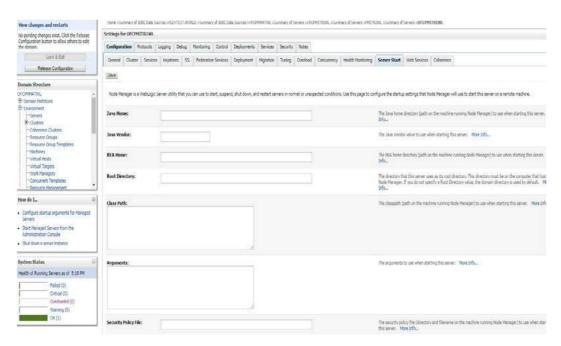
This section explains the systematic instructions to configure the Oracle WebLogic application server for Oracle Banking Payments.

To configure the Oracle WebLogic application server for Oracle Banking Payments, follow the steps given below:

1. SSelect the servers from domain structure shown below.

Domain Structure is displayed.

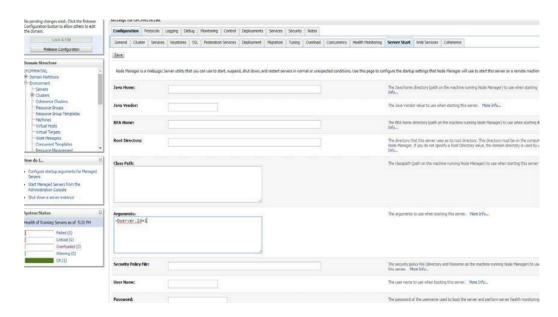
Figure 8-71 Domain Structure



Click Server Start tab and specify the Arguments as -Dserver.id=1', – in case of Manage server.

This attribute is used for Reference Number generation in payments module.

Figure 8-72 Arguments



Select the domain from the domain structure as shown below. (Eg: fcubs113\_domain).
 Settings for fcubs113\_domain screen is displayed.

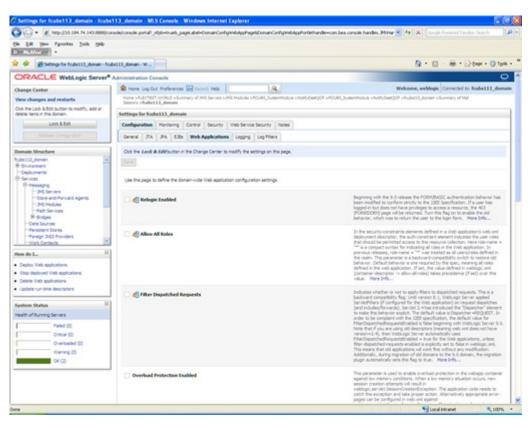


Figure 8-73 Settings for fcubs113\_domain

4. Under the **Configuration** tab, select **Web Applications**.

Settings for fcubs113\_domain - Web Applications tab is displayed.

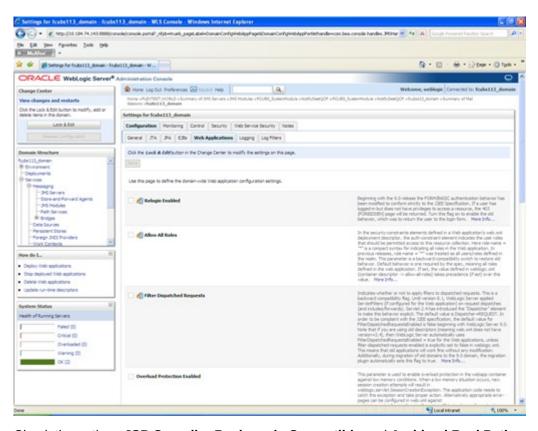
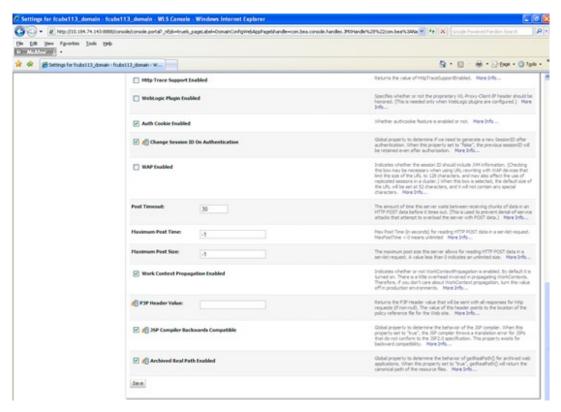


Figure 8-74 Settings for fcubs113\_domain - Web Applications

Check the options JSP Compiler Backwards Compatible and Archived Real Path Enabled.

Figure 8-75 Options



6. Click on Save button and the message Settings are updated successfully is displayed.

Settings for fcubs113\_domain - Messages screen is displayed.



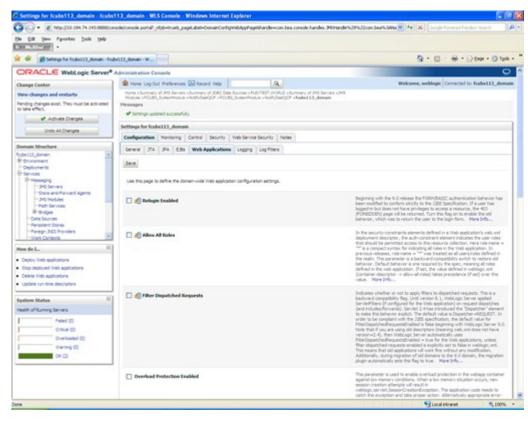


Figure 8-76 Settings for fcubs113\_domain - Messages

7. Click the Activate Changes button under the Change Center. The message All the changes have been activated. No restarts are necessary is displayed.

## 8.3 Setup/Configure Mail Session in Weblogic

This topic explains to setup/configure mail sessions in Weblogic.

This section describes the set of configurations changes required in the Oracle Weblogic Server when Oracle Banking Payments is configured to generate and send passwords to users via e-mail.

- Create JavaMail Session
   This topic explains the systematic instructions to create JavaMail session.
- Configuration of the TLS/SSL Trust Store for Weblogic Server
   This topic explains the configuration of the TLS/SSL Trust Store for Weblogic Server.

## 8.3.1 Create JavaMail Session

This topic explains the systematic instructions to create JavaMail session.

To configure the JavaMail session, follow the steps below.

 Start the Administrative Console of the WebLogic application server. Enter the Oracle WebLogic Admin Console URL in the address bar in an internet browser.

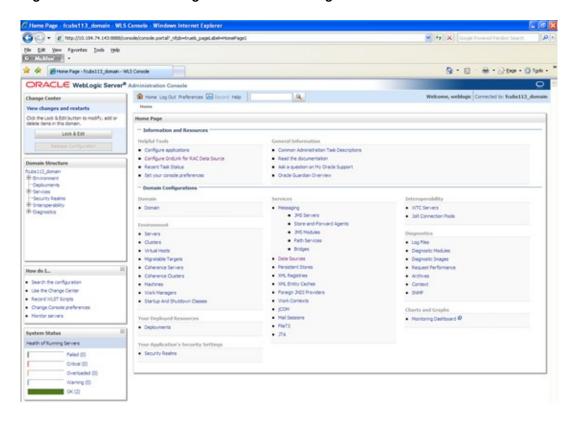
Oracle Weblogic Server - Welcome screen is displayed.

| Company | Server Administration Consoler - Notice (service) | Server Administration Consoler - Notice (service) | Server Administration Consoler | Server Administr

Figure 8-77 Oracle Weblogic Server - Welcome

Specify the WebLogic Administrator Username and Password, click Log In.
 Oracle Weblogic Server - Home Page screen is displayed.

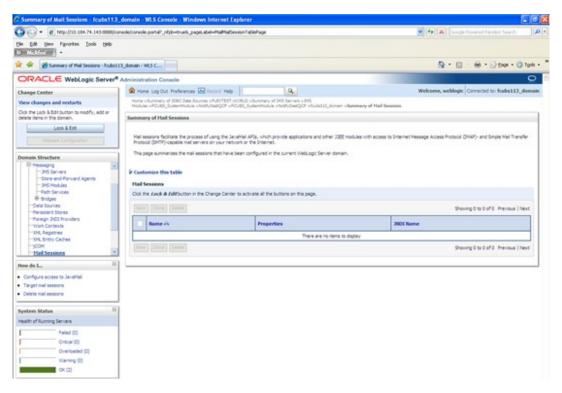
Figure 8-78 Oracle Weblogic Server - Home Page



- On the left pane, under Domain Structure, expand Services and Click Mail Sessions under it.
- Click the Lock & Edit button.

Summary of Mail Sessions screen is displayed.

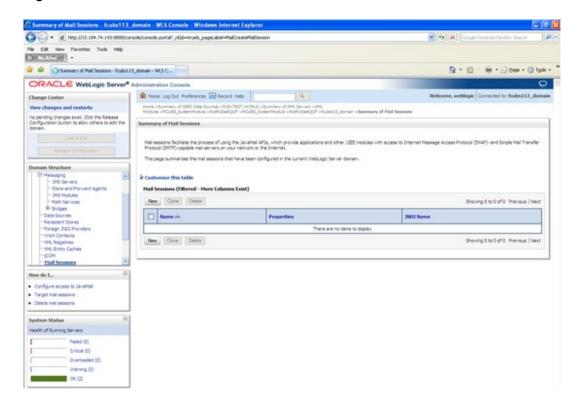
Figure 8-79 Summary of Mail Sessions



5. Click on the **New** button to create a new mail session.

Create a New Mail Session screen is displayed.

Figure 8-80 Create a New Mail Session



On the Create a New Mail Session screen, specify the fields.

Figure 8-81 Create a New Mail Session

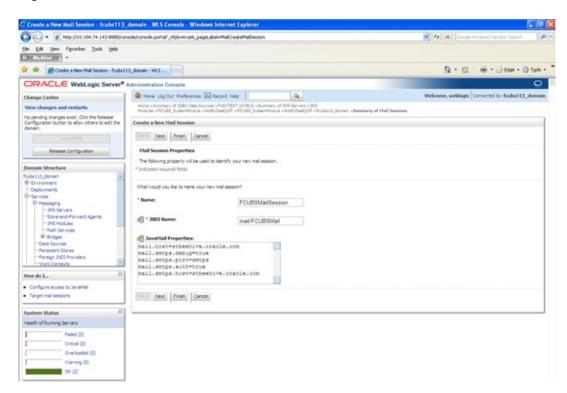


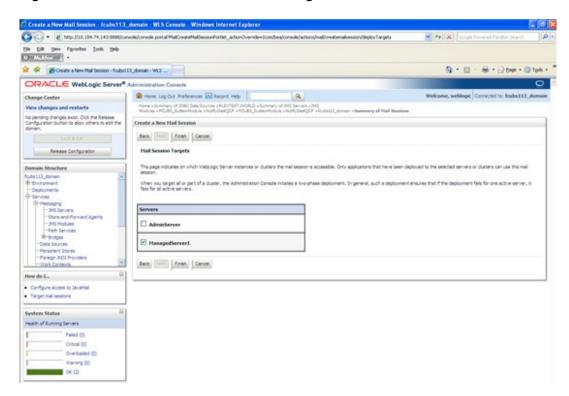
Table 8-8 Create a New Mail Session

Field	Description
Name	Specify the name as FCUBSMailSession.
JNDI Name	Specify the JNDI Name as mail/FCUBSMail.
	Note:  This JNDI name needs to be maintained in fcubs.properties file with encrypted format.
Java Mail Properties	Specify the following mail properties.  mail.host= <host_mail_server>  mail.smtps.port=<smtps_server_port> (For example: 1010)  mail.transport.protocol=<mail_transfer_protocol>(For Example: smtps)  mail.smtps.auth=true  mail.smtps.host==<host_smtps_mail_server></host_smtps_mail_server></mail_transfer_protocol></smtps_server_port></host_mail_server>

Click on Next.

Create a New Mail Session - Targets screen is displayed.

Figure 8-82 Create a New Mail Session - Targets



- 8. Check the box against the required servers and click **Finish** to complete the configuration. fcubs.properties file needs to be updated with the encrypted values of
  - SMTP\_HOST

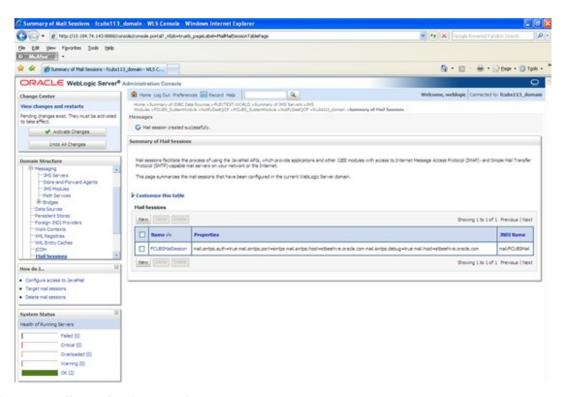
- SMTP USER
- SMTP PASSWORD
- SMTP\_JNDI

This can be achieved using the Oracle Banking UBS Installer.

9. Click the Activate Changes button under the Change Center to activate the current mail session settings. The message All the changes have been activated. No restarts are necessary is displayed.

Summary of Mail Session - Activate Changes Message screen is displayed.

Figure 8-83 Summary of Mail Session - Activate Changes Message



The JavaMail Session is created.

## 8.3.2 Configuration of the TLS/SSL Trust Store for Weblogic Server

This topic explains the configuration of the TLS/SSL Trust Store for Weblogic Server.

As described in the previous section, Oracle Banking Payments uses SMTPS to send outgoing mails. SMTPS uses SSL to ensure transport-level security of the mail messages and hence the certificate of the mail server needs to be imported into the trust store(s) of the Managed Servers where Oracle Banking Payments is deployed.

The certificate of the mail server needs to be specifically imported into the trust store configured for the Managed Server(s), as configured in the Oracle Banking Payments Installation guide titled SSL Configuration On Weblogic (SSL\_Configuration).

For further details on importing the certificate of the mail server into the trust store, refer to the documentation for the Sun Java keytool utility (Key and Certificate Management tool).