

WebSphere Configuration
Oracle FLEXCUBE Investor Servicing
Release 14.5.0.0.0
[May] [2021]



Table of Contents

1.	CONFIGURING SSL ON WEBSPHERE.....	1-3
1.1	INTRODUCTION	1-3
1.2	CERTIFICATES.....	1-3
1.2.1	Creating SSL Connection between Application Server and Client	1-3
1.2.2	Creating Self Signed Certificate	1-3
1.2.3	Path Details	1-5
1.3	ADDING KEY STORE TO APPLICATION SERVER	1-6
1.4	CREATING SSL CONFIGURATION	1-8
1.5	MANAGING ENDPOINT SECURITY CONFIGURATIONS.....	1-10
1.6	RUNNING APPLICATION WITH SSL	1-14
1.7	CERTIFICATE EXCHANGE FOR TWO WAYS SSL.....	1-14
1.7.1	Extracting Certificate for Server1	1-14
1.7.2	Extracting Certificate for Server2	1-15
1.7.3	Importing Certificate into Keystore for Server1	1-16
1.7.4	Importing Certificate into Keystore for Server2	1-17
1.7.5	Importing Certificate into Truststore for Server1	1-18
1.7.6	Importing Certificate into Truststore for Server2.....	1-20
1.8	MANAGING ENDPOINT SECURITY CONFIGURATIONS.....	1-20
1.9	PROTECTION QUALITY	1-22
1.10	IMPORTING OR ADDING SERVER CERTIFICATES USING BATCH.....	1-23
2.	CREATING RESOURCES ON WEBSPHERE	2-1
2.1	INTRODUCTION	2-1
2.2	CREATING QUEUES ON WEBSPHERE MQ SERVER	2-1
2.2.1	Creating Queue Manager through Console.....	2-1
2.2.2	Creating Queues	2-11
2.3	CREATING QUEUE MANAGER AND QUEUE USING UNIX COMMANDS.....	2-13
2.3.1	Creating Queue Manager	2-13
2.3.2	Starting Queue Manager	2-14
2.3.3	Starting MQ Service to Create Queues under FC_QMGR.....	2-14
2.3.4	Creating Queues	2-14
2.3.5	Creating Channel.....	2-14
2.3.6	Ending MQSC.....	2-14
2.3.7	Creating Bindings.....	2-15
2.3.8	Creating QCF	2-15
2.3.9	MQ Channel Authentication	2-17
2.4	VIEWING IBM MQ QUEUES	2-17
3.	CREATING JDBC RESOURCES ON WEB SPHERE.....	3-1
3.1	INTRODUCTION	3-1
3.2	PREREQUISITE:	3-1
3.3	CREATING JDBC SOURCES	3-1
3.3.1	Creating Global Security.....	3-1
3.3.2	JDBC Provider for Non XA Data Source	3-4
3.3.3	Creating Non XA Data Source.....	3-7
3.3.4	Scheduler Data Source configuration.....	3-12
3.3.5	Testing Data Source.....	3-13
3.3.6	JDBC Provider for XA Data Source	3-14
3.3.7	Creating XA Data Source	3-17
3.3.8	Testing Data Source.....	3-21
3.4	CREATING JMS RESOURCES.....	3-22

3.4.1	<i>Creating Queue Connection Factory</i>	3-22
3.4.2	<i>Creating Queues</i>	3-30
3.5	CREATING MESSAGE LISTENER	3-34
4.	DEFAULT SETTINGS FOR WEB SPHERE	4-1
4.1	STANDALONE SCHEDULER CONFIGURATION	4-1
5.	CONFIGURING MAIL SESSION ON WEBSHERE	5-4
5.1	INTRODUCTION	5-4
5.2	CREATING JAVA MAIL SESSION.....	5-4
6.	ANNEXURE	6-1
6.1	IBM WEBSHERE SERVER - INCREASING HEAP SIZE	6-1
6.2	IBM WEBSHERE SERVER - TRANSACTION SERVICE PROPERTIES.....	6-1
6.3	IBM WEBSHERE SERVER – ORB SERVICE CONFIGURATION	6-1

1. Configuring SSL on Websphere

1.1 Introduction

This chapter guides you through the process of configuring SSL on IBM Websphere application server.

1.2 Certificates

1.2.1 Creating SSL Connection between Application Server and Client

To establish SSL connection between Websphere and client work stations, follow the steps given below:

- Create SSL certificate (this certificate is required during real time production)
- Self signed certificate (SSL) will be used for testing purpose

1.2.2 Creating Self Signed Certificate

To create a self signed certificate, you may use various tools including IBM (Keyman). For illustration purpose, this guide explains the method of generating SSL using a tool available in JAVA. The keytool is available in the folder 'JAVA_HOME\jdk\bin'.

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

```
keytool -genkeypair -alias alias -keyalg keyalg -keysize keysize -  
sigalg sigalg -validity valDays -keystore keystore
```



The texts highlighted in blue are placeholders. You need to replace them with the suitable values while running the command.

In the above command,

- ***alias*** is used to identify the public and private key pair created. This *alias* is required for configuring the SSL attributes for the managed servers in Oracle WebLogic application server.
- ***keyalg*** is the key algorithm to generate the public and private key pair. The RSA key algorithm is recommended.
- ***keysize*** is the size of the public and private key pair generated. A key size of 2048 or more is recommended. Consult your CA on the key size support for different types of certificates.
- ***sigalg*** is the algorithm used to generate the signature. This algorithm must be compatible with the key algorithm. This has to be one of the values specified in the Java Cryptography API Specification and Reference.
- ***valdays*** is the number of days for which the certificate is considered to be valid. Consult your CA on this period.
- ***keystore*** is to specify the location of the JKS file. If JKS file is not present in the path provided, this will create it.

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 Oracle WebLogic Server.
- **First and last name (CN):** Specify the domain name of the machine used to access Oracle FLEXCUBE INVESTOR SERVICING. For instance, www.example.com.
- **Name of your organizational unit:** Specify 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 physical server.
- **Name of your organization:** Specify the name of the organization making the certificate request. For example, Oracle Financial Services Software. It is recommended to use the formal name of the company or organization. This name must match the name in the official records.
- **Name of your City or Locality:** Specify the name of the city in which your organization is physically located. For example Mumbai.
- **Name of your State or Province:** Specify the state/province in which your organization is physically located. For example Maharashtra.
- **Two-letter country code for this unit:** Specify the country in which your organization is physically located. For example, US, UK, IN etc.

Example

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

```
keytool -genkeypair -alias cvrhp0729 -keyalg RSA -keysize 2048
-sigalg SHA256withRSA -validity 365 -keystore
D:\keystores\FCISKeyStore.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

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>

The self signed certificate needs to be added to the web server.

1.2.3 **Path Details**

You need to copy or move the keystore file *<name of the file>.jks* to the application server location given below:

/oracle1/WAS61/Appserver_ND/profiles/AppSrv01/config/cells/ips014dorCell01/nodes/ips014dorNode02

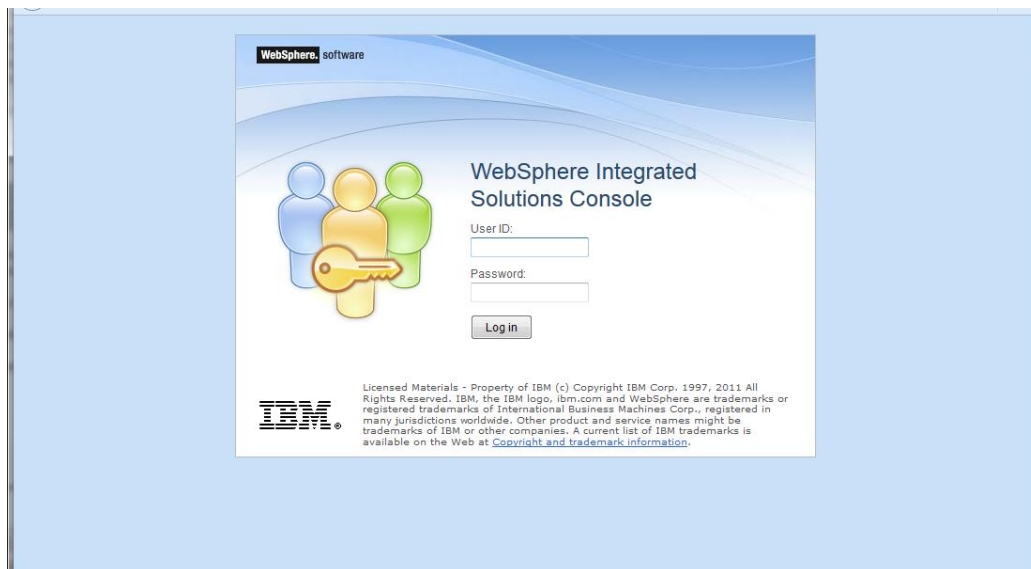
ips014dorCell01 --> <ips014dor> name of the machine and < Cell01>

ips014dorNode02 --> < ips014dorNode > name of the machine and <Node02>

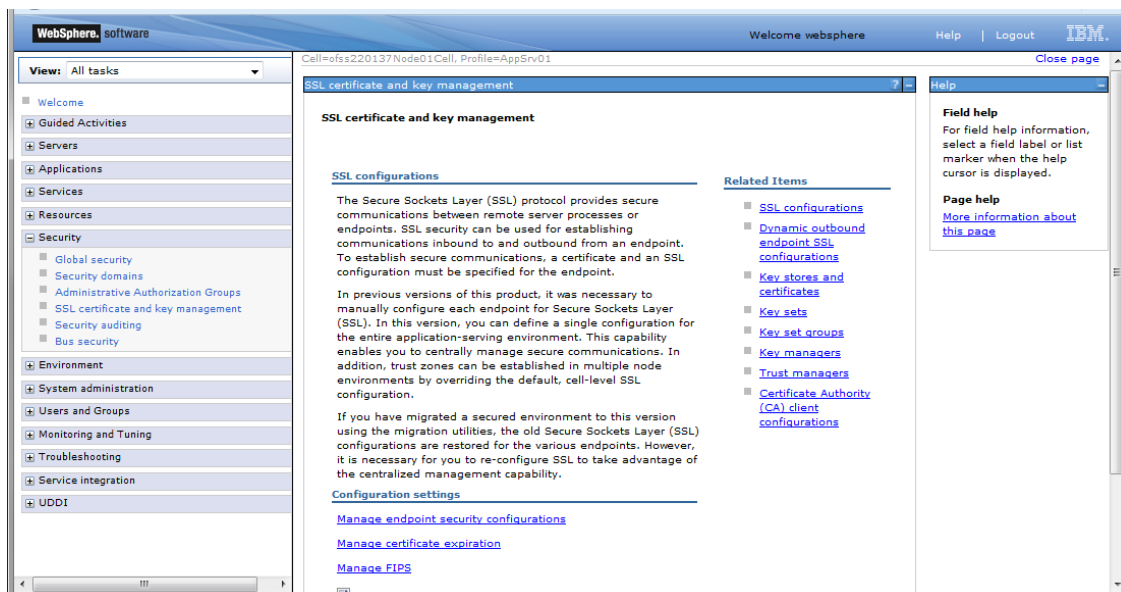
1.3 Adding Key Store to Application Server

To add keystore to the Websphere application server, follow the instructions given below.

1. Log in to the WAP console as the user 'admin'.

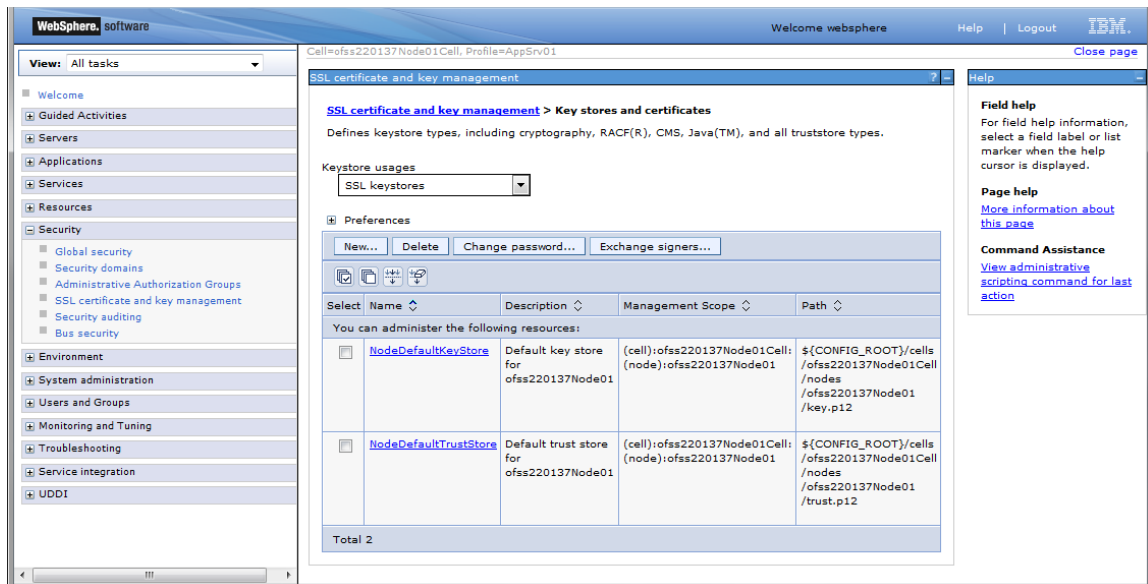


2. Specify the user ID of the administrator and the password set while installing the software. Click 'Log In'. The following screen is displayed:



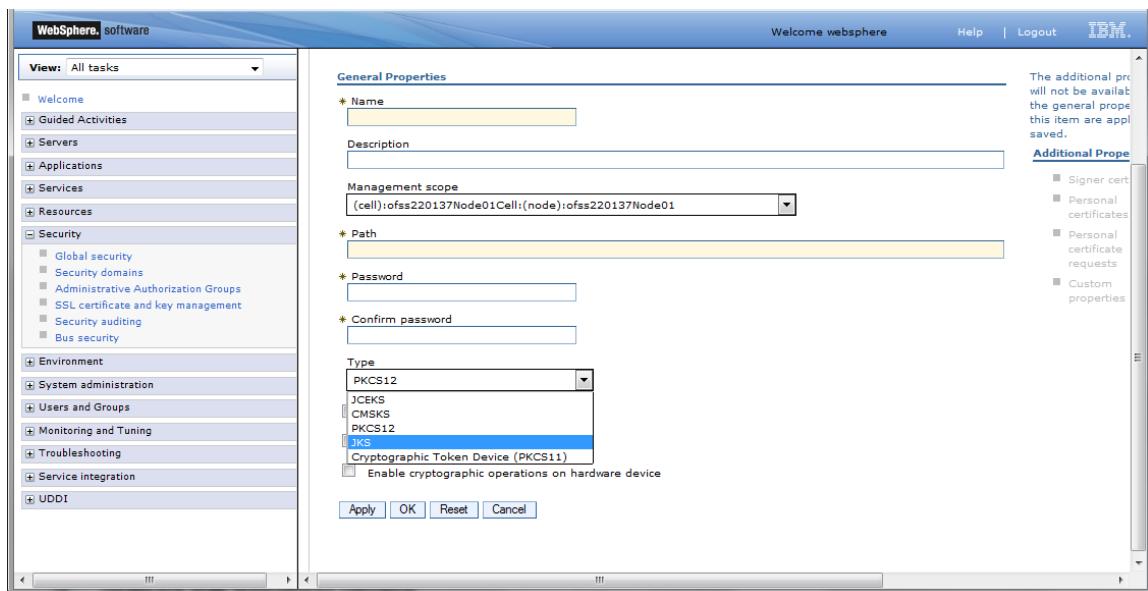
On the left pane, expand 'Security' and click 'SSL certificate and key management'. The screen displays the details of SSL.

3. Under 'Related items' on the right side, click 'Key stores and certificates'. The following screen is displayed:



This screen is used for attaching the key store to the application server.

4. Click 'New' button to add a new key to store.



5. Specify the following details:

Name

Specify the key store name.

Path

Specify the location of the key store generated.

This has to be a relative path.

Example

`${CONFIG_ROOT}/cells/ips014dorCell01/nodes/ips014dorNode02/jf3sslstore.jks`

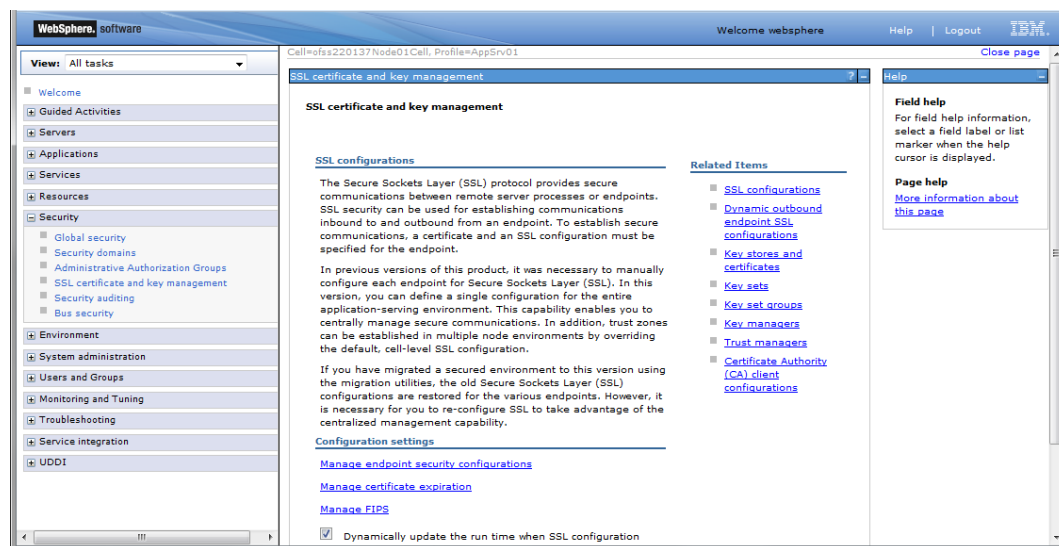
Password

Specify the password given in the 'store pass' parameter during key store generation.

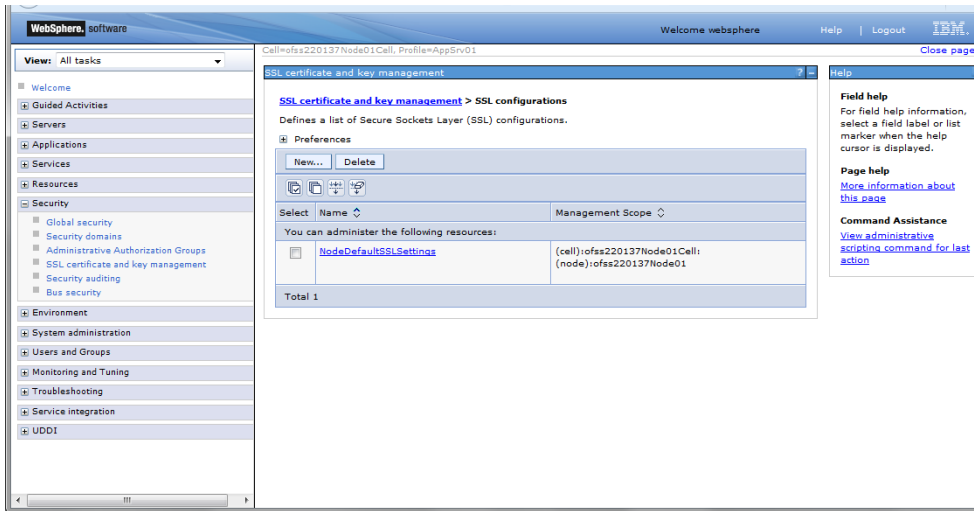
6. Click 'Apply' and save the changes.

1.4 **Creating SSL Configuration**

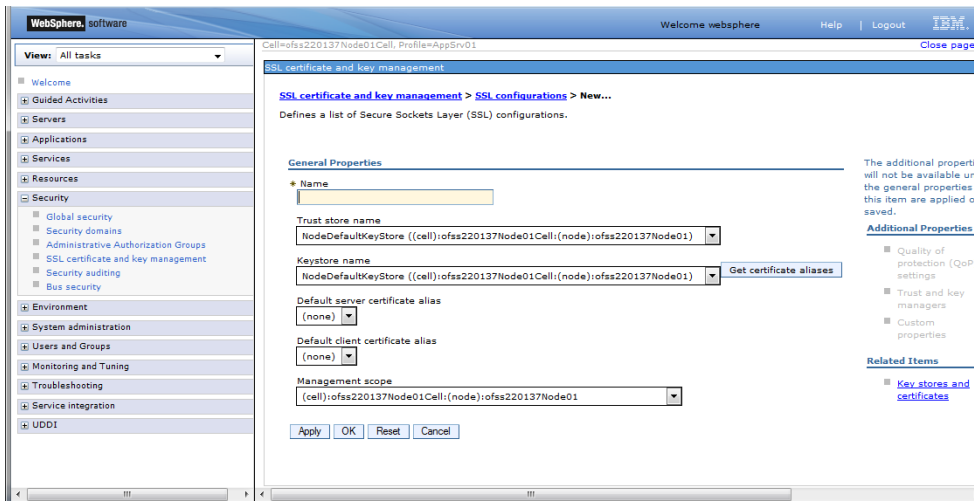
To create SSL configuration, on the left pane, click 'SSL certificate and key management'.



1. Under the section 'Related items', click 'SSL configurations'. The following screen is displayed:



2. Click 'New' button. The following screen is displayed.



3. Specify the following details:

Name

Specify the name of the SSL configuration.

Trusted Store Name

Select the added key store.

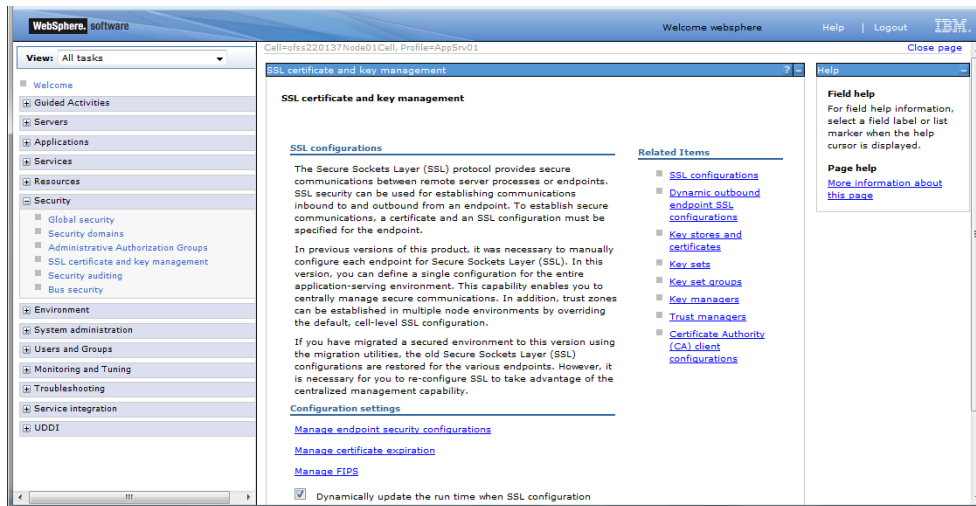
Key Store Name

Select the added key store.

4. Click the button 'Get Certificate aliases'. Further, click 'Apply' and save the changes.

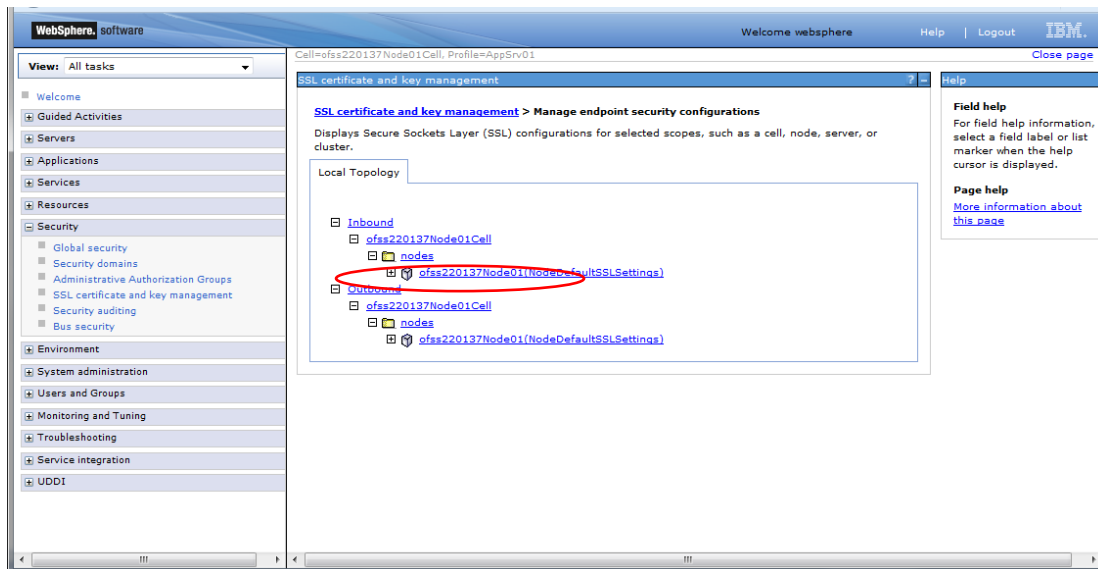
1.5 Managing Endpoint Security Configurations

This section explains the process of managing endpoint security configurations.

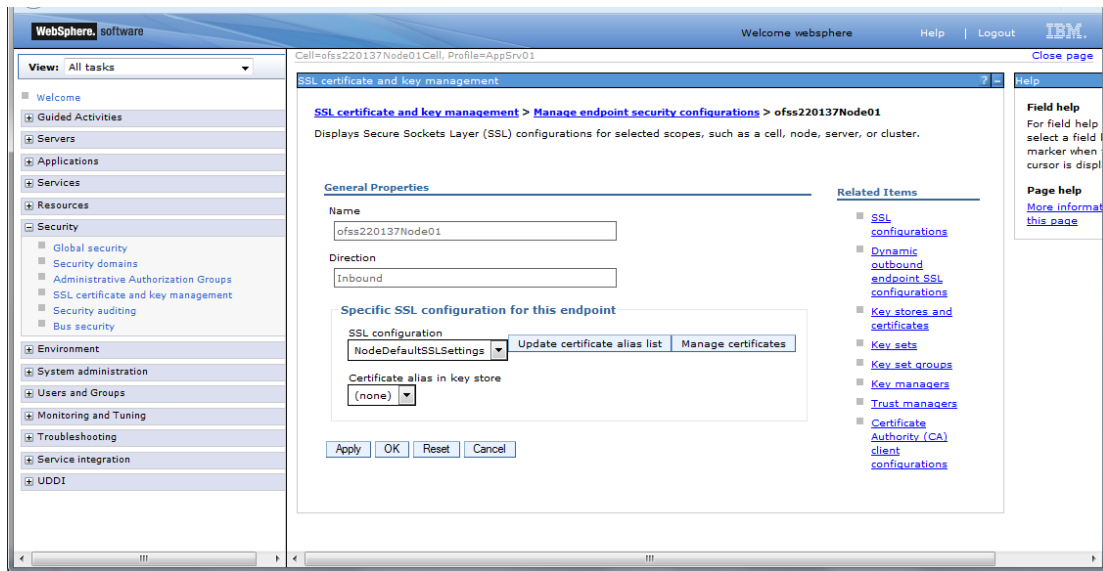


1. On the left pane, expand 'Security' and click 'SSL certificate and key management'. Under 'Configuration settings', click 'Manage endpoint security configurations'.

The following screen is displayed:



2. Click the first link under 'Inbound tree'. The following screen is displayed:

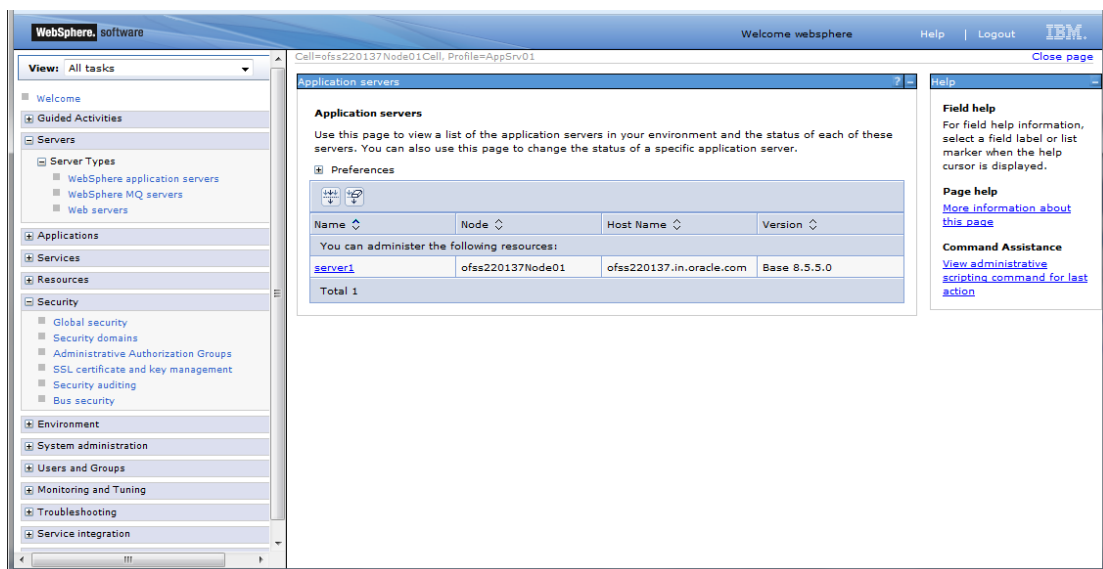


Under SSL configurations, select the configured SSL from the drop-down list.

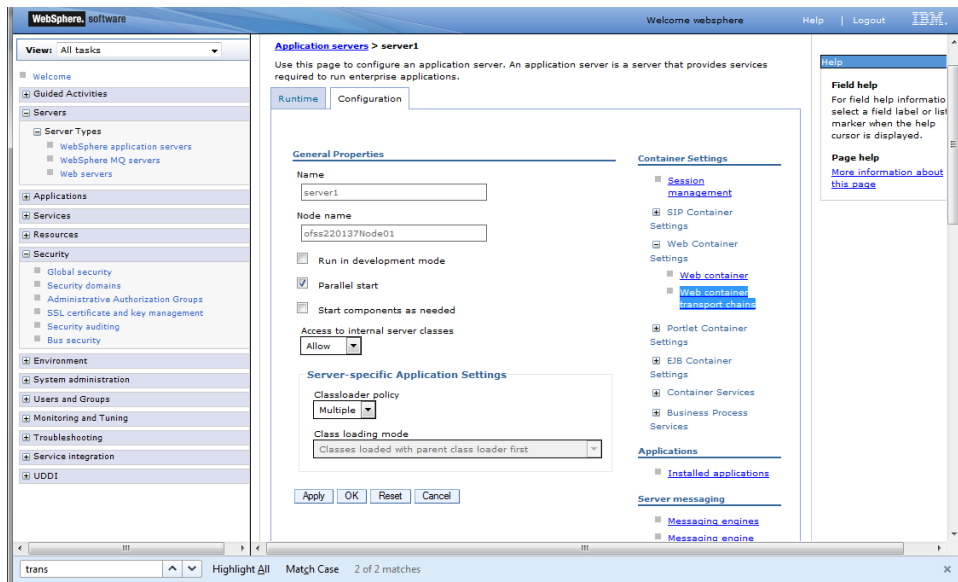
3. Click the button 'Update certificate alias list'. Click 'Apply' and save the changes.

4. SSL Settings at Application Server Level

Go to the servers available on the left and click the application servers link which will refresh the window on the right side to display the details pertaining to application servers

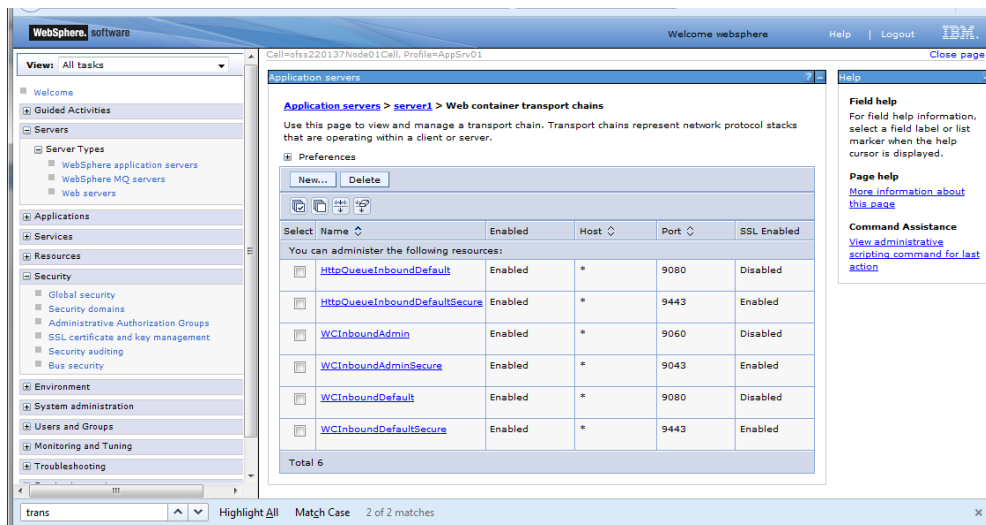


5. Click the server to which SSL configuration has to be applied. The following screen is displayed.

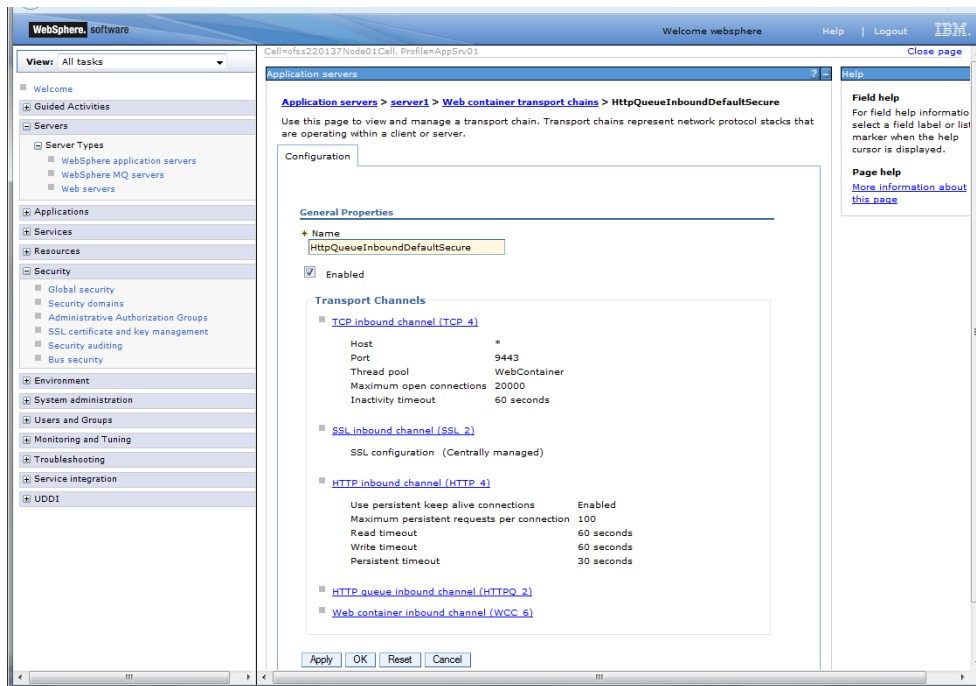


6. Go to Configuration tab and click 'Web container transport chains' under 'Container settings'.

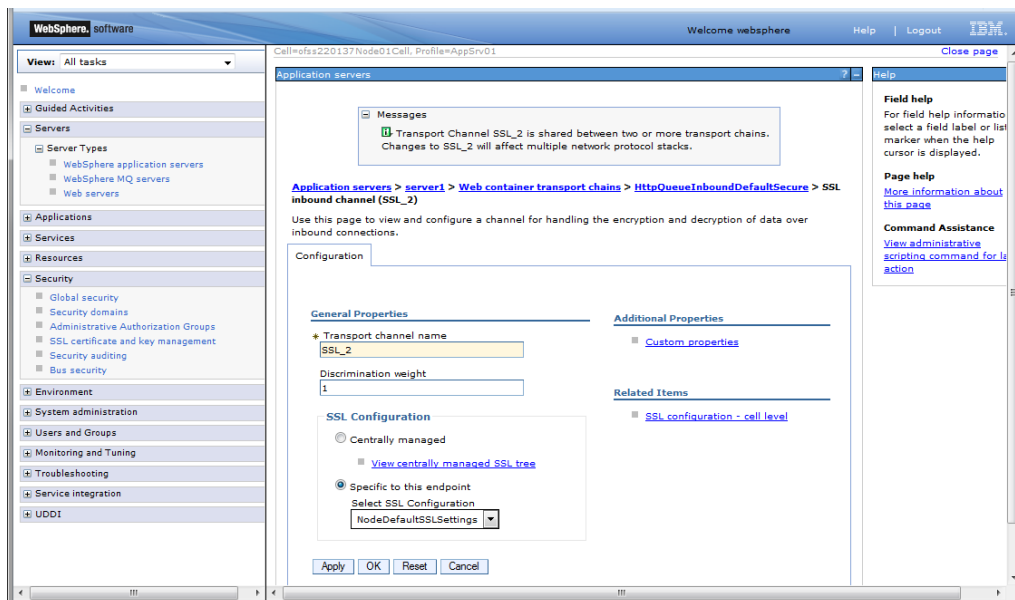
The following screen is displayed.



7. Against their respective names, the secured connection is available under the column 'SSL Enabled'. Click 'WCInboundDefaultSecure'. The following screen is displayed:



8. Click 'SSL Inbound channel (SSL 2)'.



9. Select the configured SSL from the list of SSL configurations. Click 'Apply' and save the changes.

1.6 Running Application with SSL

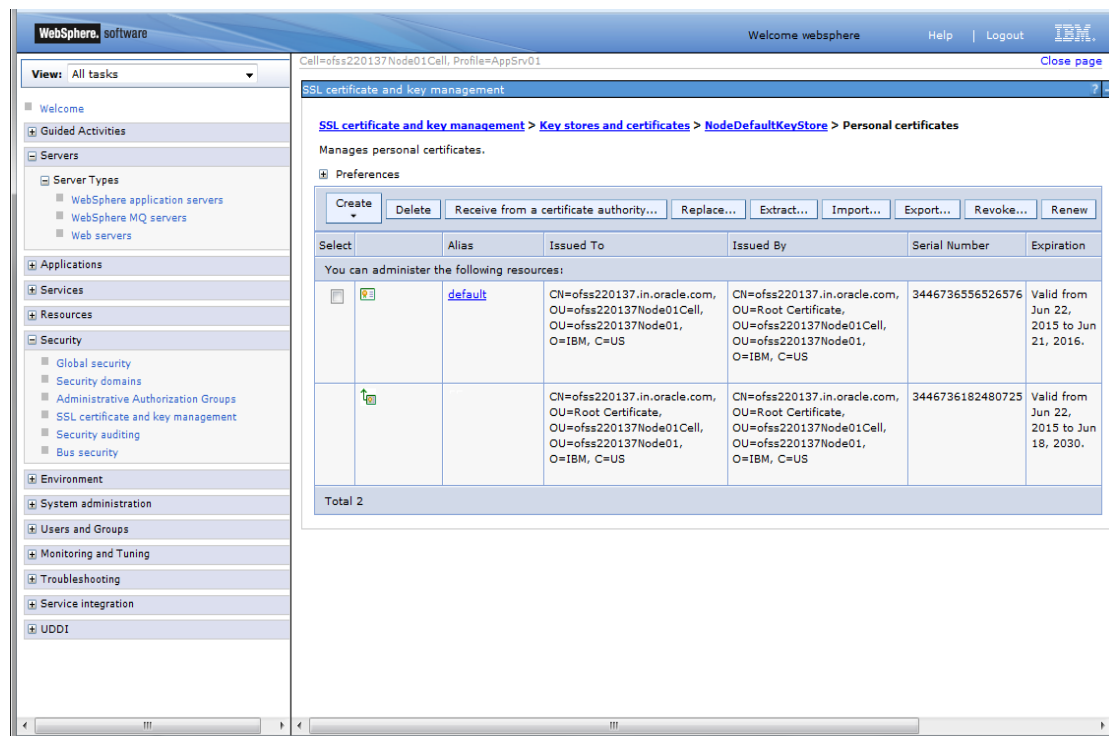
To run the application with SSL, use the following syntax:

https://<<ip address or host name>>:<<port number>>/<<context>>>

1.7 Certificate Exchange for Two Ways SSL

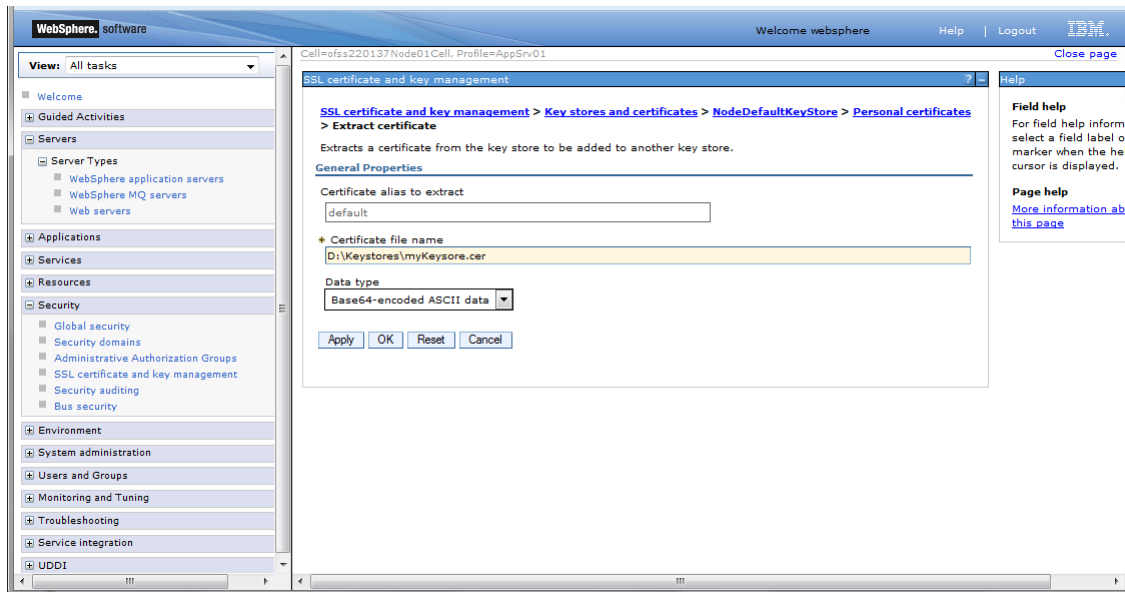
1.7.1 Extracting Certificate for Server1

The process of extracting certificate for Server 1 is described below.



1. On the left pane of the screen, expand 'Security'. Go to 'SSL certificate and key management' > Key stores and certificates > {YOUR KEYSTORE NAME} > Personal certificates.

2. Select the installed certificate and click 'Extract' button.



3. Specify the location to save the certificate. This will be used to add in the other server.
Ensure that the file has been created in the location.

Eg: \<localfolder>\<server1.cer>

4. Similarly extract the certificate for the second server.

Eg: \<localfolder>\<server2.cer>

1.7.2 Extracting Certificate for Server2

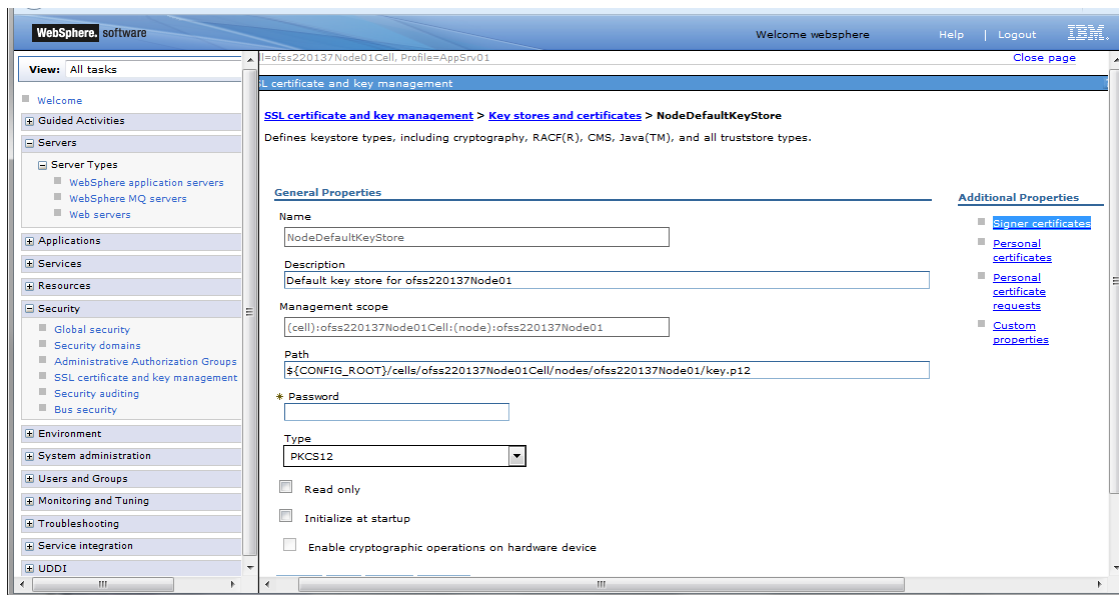
You can follow the steps for server 1 described under 'Extracting Certificate for Server1' to extract the certificate for Server2.

1.7.3 Importing Certificate into Keystore for Server1

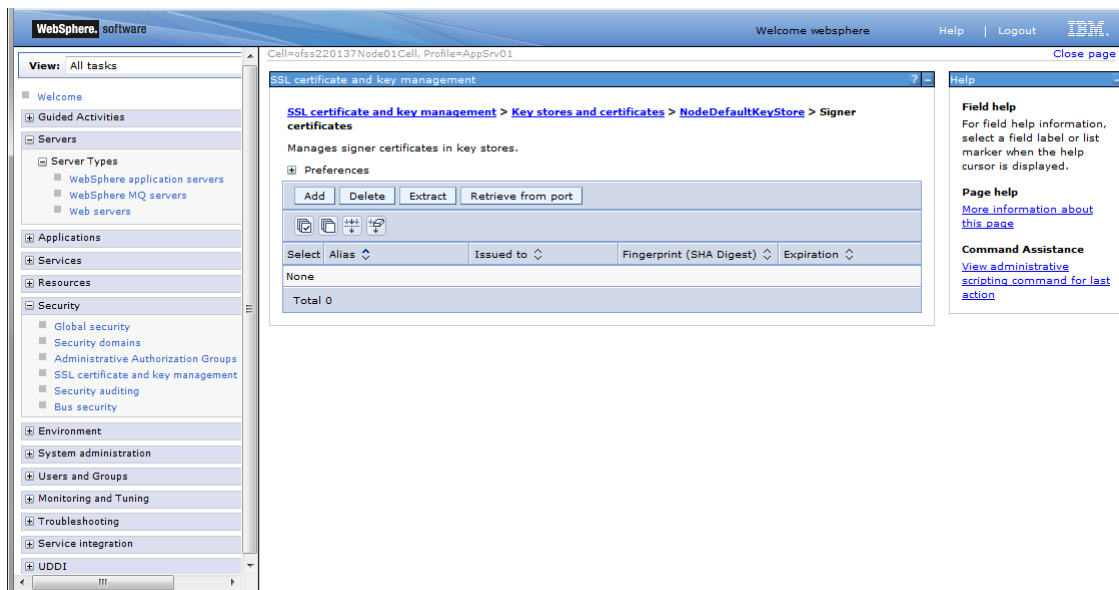


Note: The trust certificates also needs to be added in the **cacerts** of the Java Runtime Environment

Go to the other server. Expand 'Security > SSL certificate and key management > Key stores and certificates > Server7Keystore (which is created now).

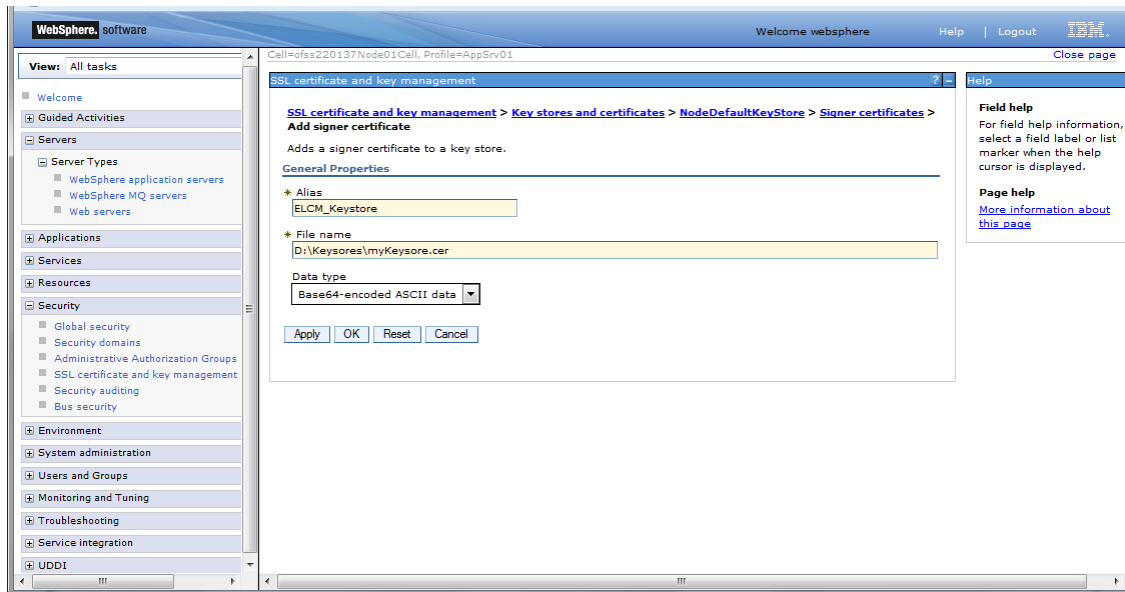


1. Click 'Signer Certificates'. The following screen is displayed:



2. Click 'Add' button to add the certificate of the other server.

The following screen is displayed:



3. The extracted certificate of the second server has to be imported to the key-store and trust-store of first server. This has to be done using the same local path where the extract certificate was generated for the first server.

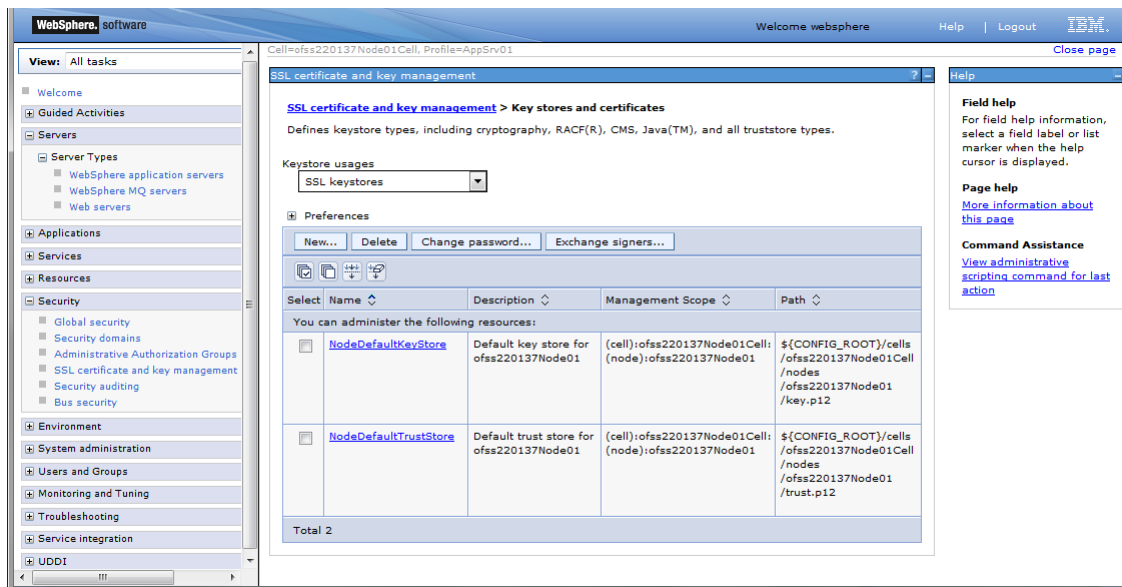
Eg: \<localfolder>\<server1.cer>

1.7.4 Importing Certificate into Keystore for Server2

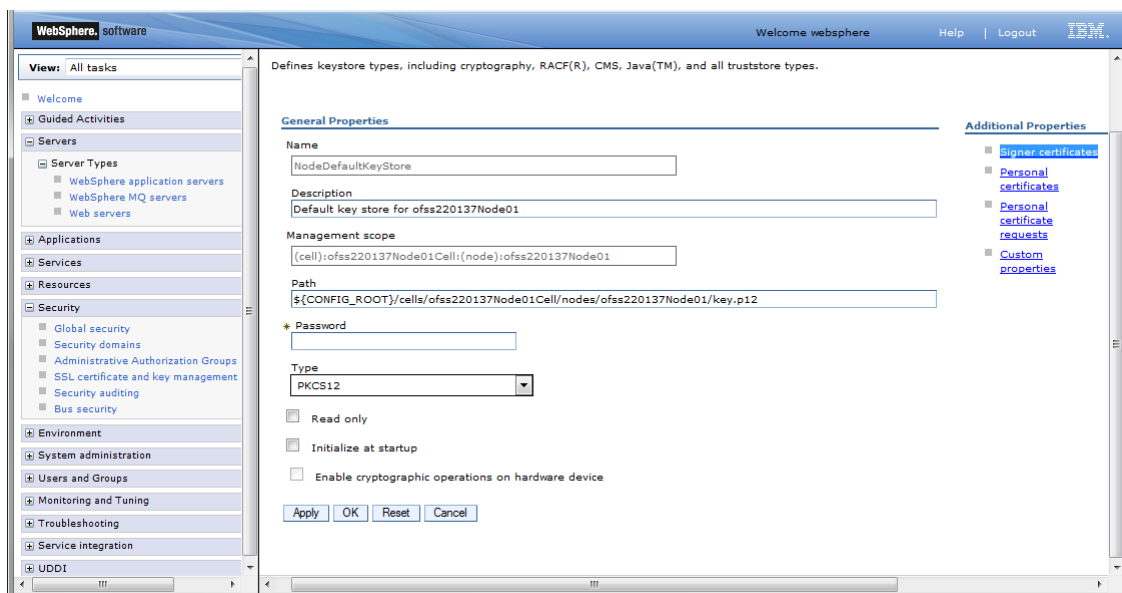
You can follow the steps for server 1 described under 'Importing Certificate into Keystore for Server1' to import the certificate into keystore for Server2.

1.7.5 Importing Certificate into Truststore for Server1

Expand 'SSL certificate and key management > Key stores and certificates and click 'NodeDefaultTrustStore'.

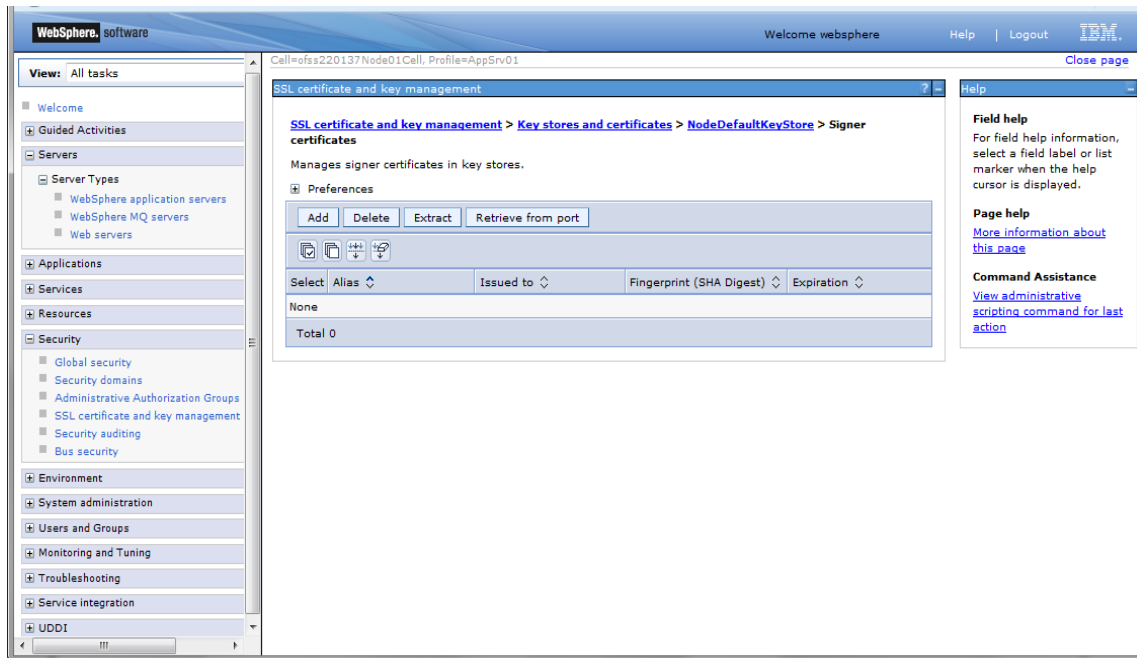


The following screen is displayed.

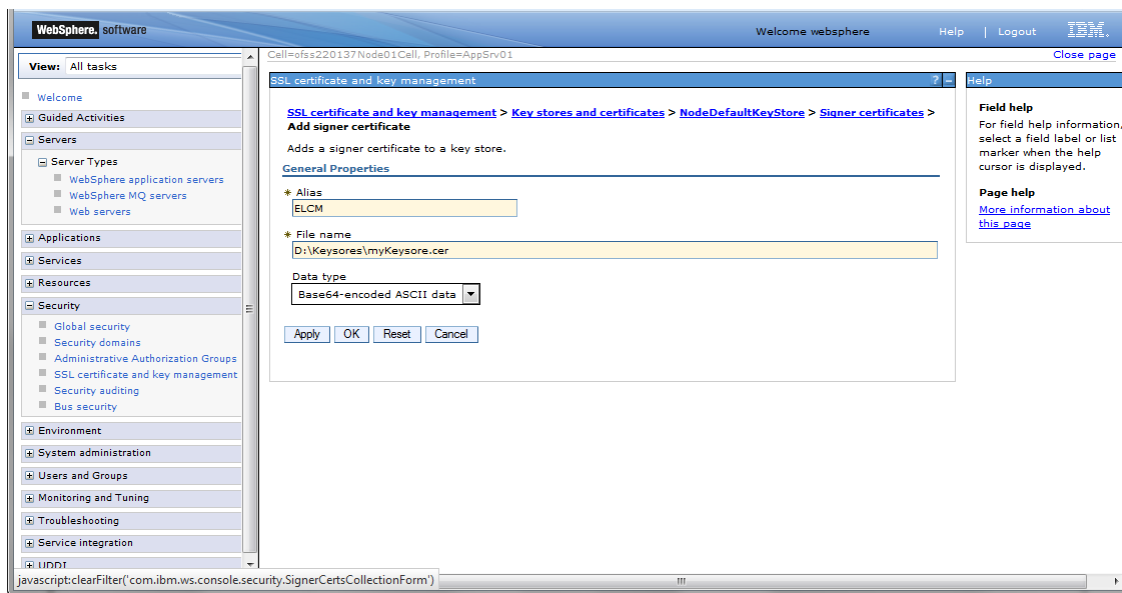


1. Click 'Signer Certificates'.

The following screen is displayed.



2. Click 'Add' button to add the extracted certificate of the second server. The following screen is displayed.



3. Specify the 'alias' name to identify the other server.

Eg: For server1, you can give the alias name 'server2Alias'.

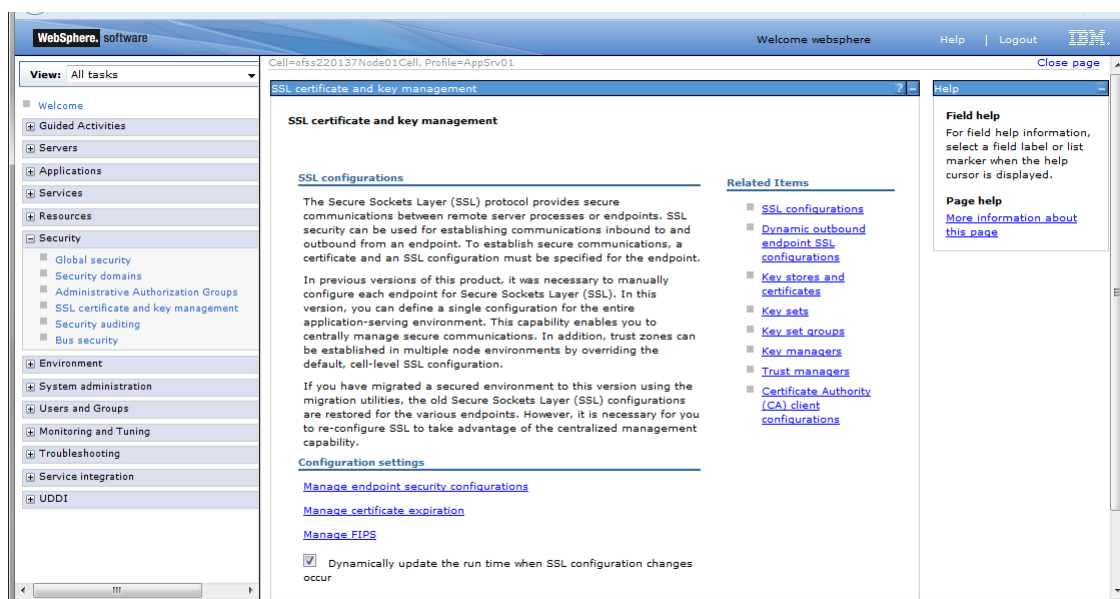
4. Further, specify the location of the extracted certificate.

1.7.6 Importing Certificate into Truststore for Server2

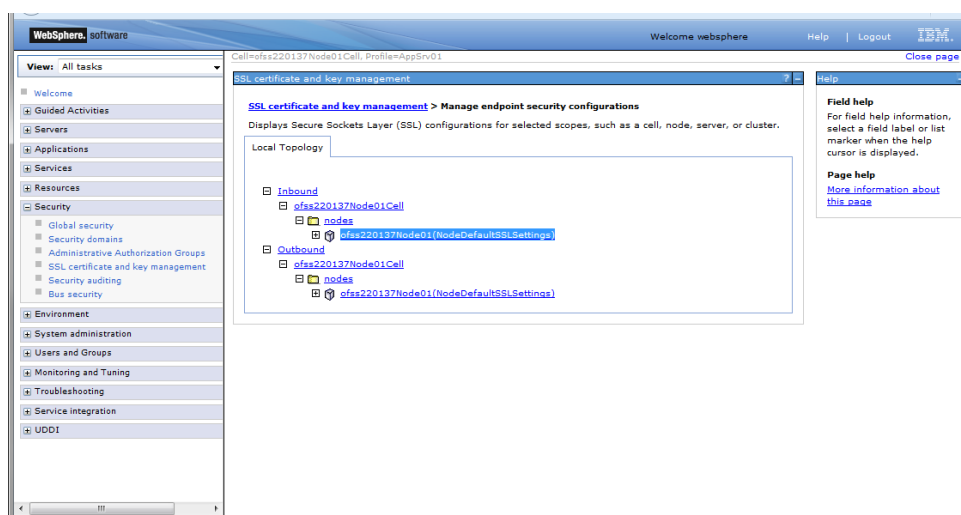
You can follow the steps for server 1 described under 'Importing Certificate into Truststore for Server2' to import the certificate into Truststore for Server2.

1.8 Managing Endpoint Security Configurations

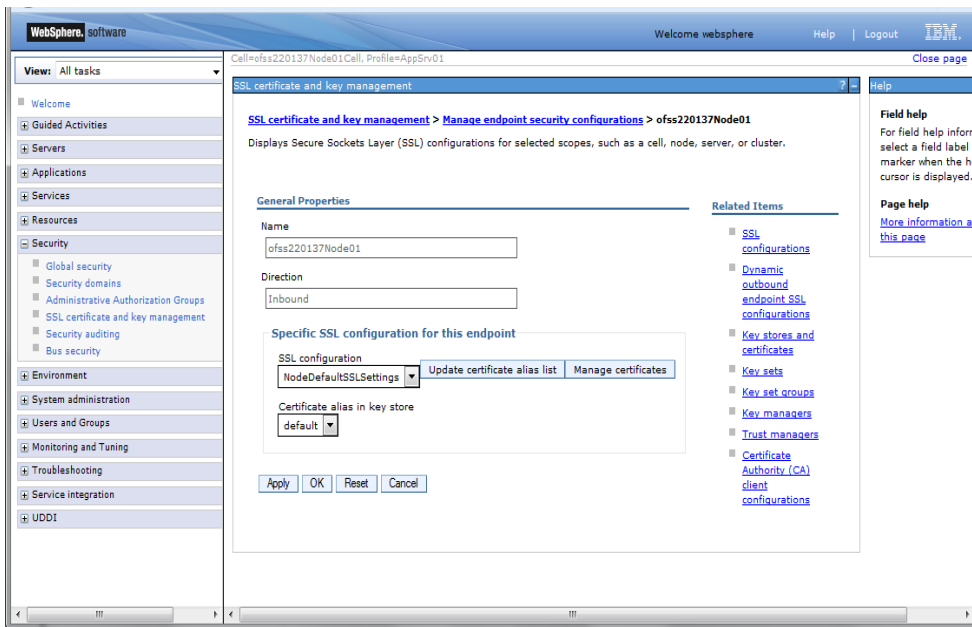
To manage the endpoint security configurations, follow the instructions given below.



1. Expand 'Security > SSL certificate and key management' and click 'Manage endpoint security configurations'.

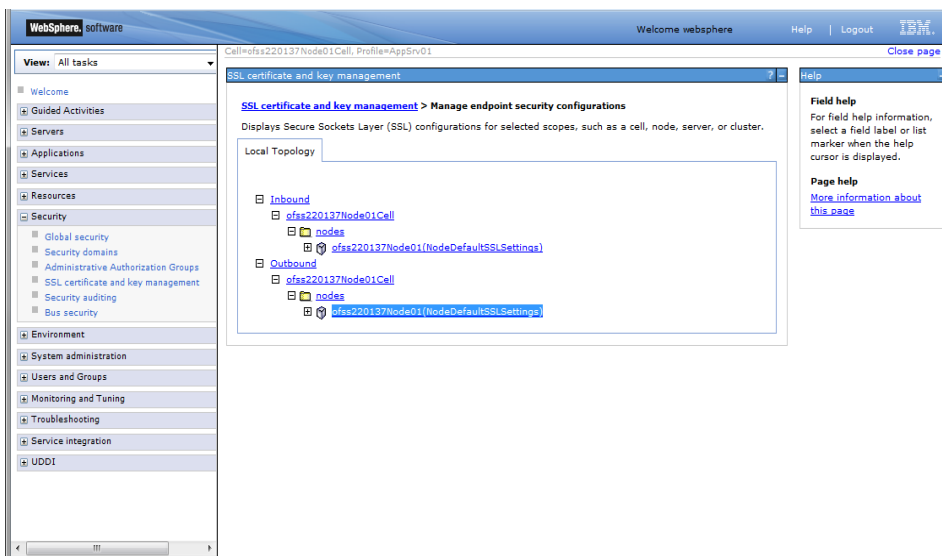


2. Change the inbound node settings. Expand 'Inbound' and click link highlighted in blue color. The following screen is displayed.



3. Select the 'SSL Configuration' created which you just created. Click 'Update certificate alias list' button.
4. Ensure that the proper certificate and SSL configuration are selected. Further, click 'Apply' and save the settings.

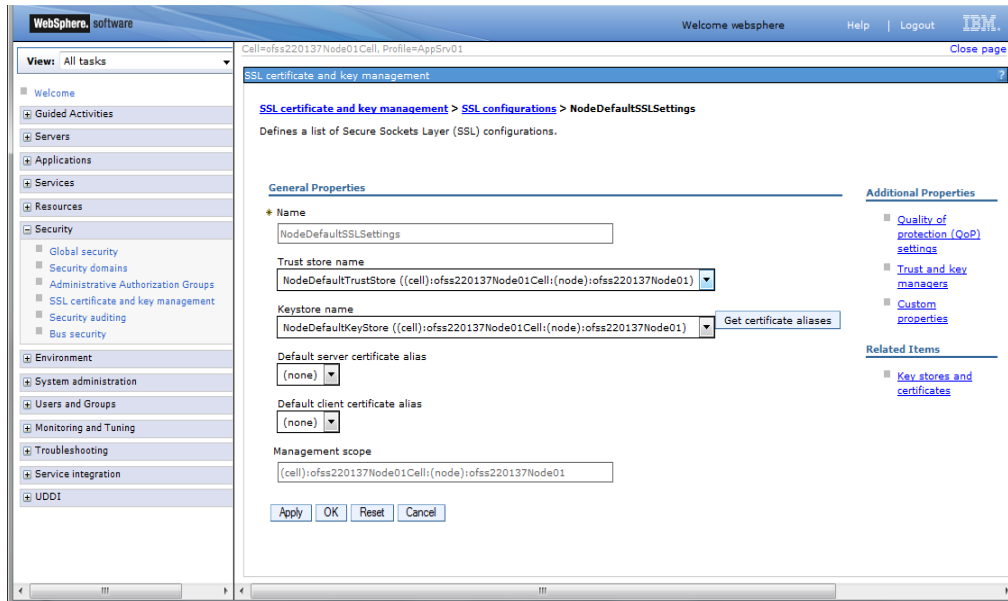
You can view the settings under 'Inbound'.



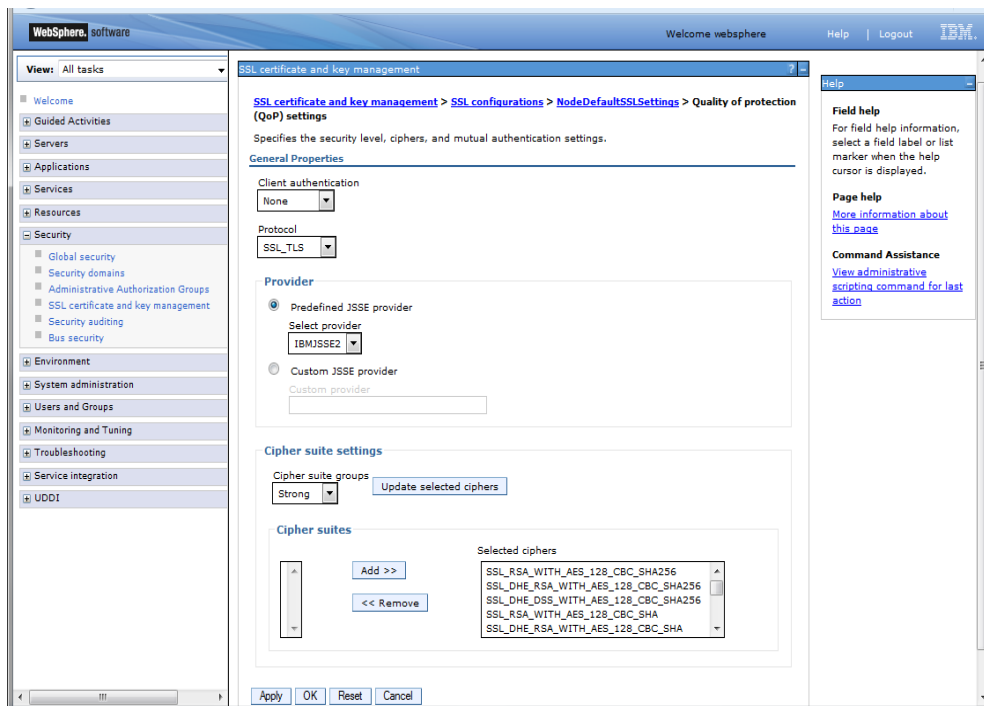
5. Repeat the above steps for 'Outbound' as well.
6. You need to repeat the above steps for server2 also.

1.9 Protection Quality

1. Expand 'SSL certificate and key management > SSL configurations > {YOUR SERVER CONFIG}'.



2. On the right side, click 'Quality of protection (QoP) settings'. The following screen is displayed.



3. Under 'Client authentication' choose 'Supported' from the drop-down list.

4. Click 'Apply' and save the changes.
5. You need to repeat these steps for the second server. Once you have made the changes to both the servers, restart the servers. It is recommended to restart the servers after making the changes.

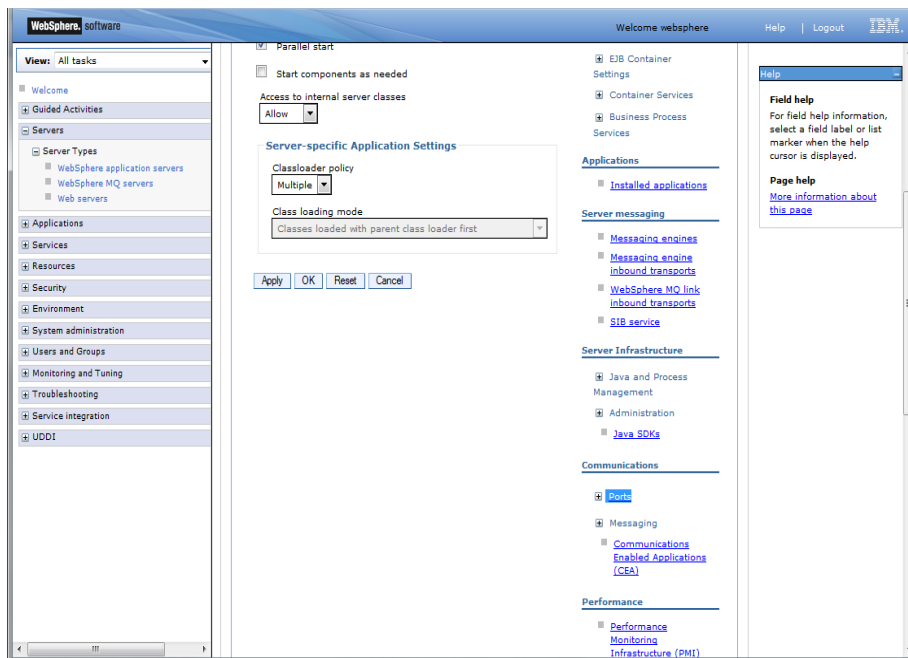
1.10 Importing or Adding Server Certificates using Batch

Alternatively, you can import or add the server certificates using *ikeyman.bat*. This batch is available at the following location:

<InstalledLocatio>\IBM\Websphere\AppServer\bin

For security reasons, change the password for 'defaultTruststore' (trust.p12). The default password is 'WebAS'.

SSL port information is available in the following screens.



Click 'Ports'. The details are displayed as follows.

WebSphere, software

Welcome websphere Help | Logout IBM

View: All tasks

- Welcome
- Guided Activities
- Servers
 - Server Types
 - WebSphere application servers
 - WebSphere MQ servers
 - Web servers
- Applications
- Services
- Resources
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Communications

Ports

Port Name	Port	Details
BOOTSTRAP_ADDRESS	2809	
SOAP_CONNECTOR_ADDRESS	8880	
ORB_LISTENER_ADDRESS	9100	
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS	9401	
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS	9403	
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS	9402	
WC_adminhost	9060	
WC_defaulthost	9080	
DCS_UNICAST_ADDRESS	9353	
WC_adminhost_secure	9043	
WC_defaulthost_secure	9443	
SIP_DEFAULTHOST	5060	
SIP_DEFAULTHOST_SECURE	5061	
SIB_ENDPOINT_ADDRESS	7276	
SIB_ENDPOINT_SECURE_ADDRESS	7286	
SIB_MQ_ENDPOINT_ADDRESS	5558	
SIB_MQ_ENDPOINT_SECURE_ADDRESS	5578	
IPC_CONNECTOR_ADDRESS	9633	
OVERLAY_UDP_LISTENER_ADDRESS	11003	
OVERLAY_TCP_LISTENER_ADDRESS	11004	

Messaging

[Communications Enabled Applications \(CEA\)](#)

Performance

[Performance Monitoring Infrastructure \(PMI\)](#)

2. Creating Resources on Websphere

2.1 Introduction

This document explains the steps to create resources on Websphere application server and Queues in Websphere MQ server.

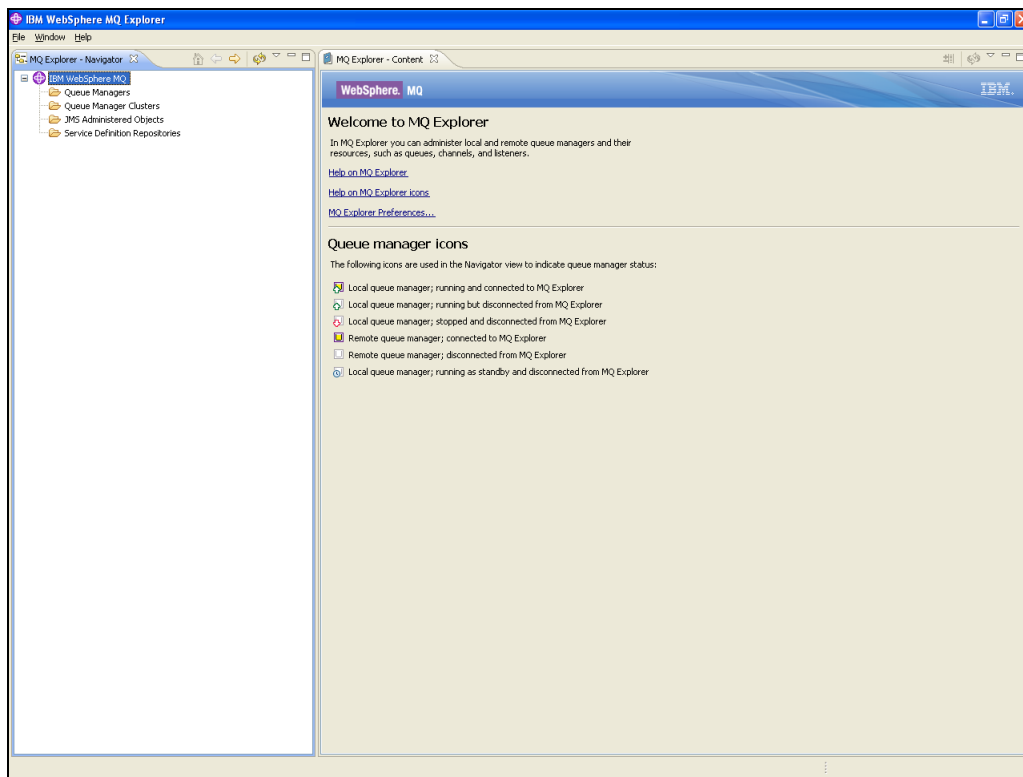
2.2 Creating Queues on Websphere MQ Server

The process of creation of queues on Websphere is explained under the following headings.

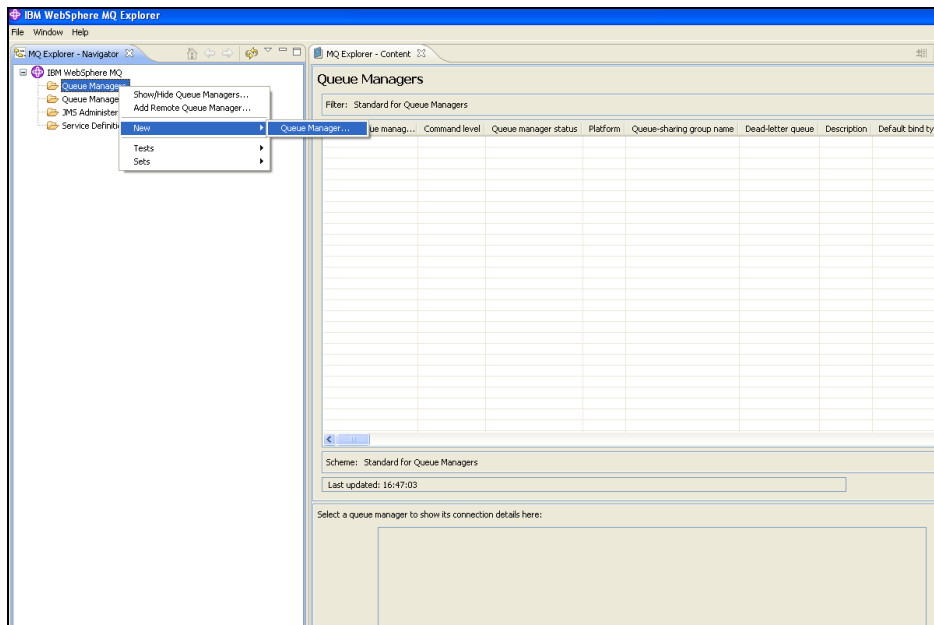
2.2.1 Creating Queue Manager through Console

To create queue manager through console, follow the steps given below:

1. Start MQ server console.



2. On the left pane, go to 'IBM Websphere MQ > Queue Manager > New > Queue Manager' as shown below:



The following screen is displayed:

Create Queue Manager

Queue Manager
Enter basic values

Queue manager name: QM_DDHP0520

☒ Make this the default queue manager

Default transmission queue:

Dead-letter queue:

Max handle limit: 256

Trigger interval: 999999999

Max uncommitted messages: 10000

? < Back Next > Finish Cancel

3. Specify the 'Queue manager name'. Check the box 'Make this the default queue manager'.

4. Click 'Next'. The following screen is displayed:

Create Queue Manager

Queue Manager
Enter data and log values

Queue manager name: QM_DDHP0520

☒ Use circular logging
☐ Use linear logging

Log file size: (x4KB) 4096

Log primary files: 3

Log secondary files: 2

Data and Log paths

☒ Use default paths:

Data path: D:\Program Files\IBM\WebSphere MQ\qmgrs Browse...

Log path: D:\Program Files\IBM\WebSphere MQ\log Browse...

? < Back Next > Finish Cancel

5. Click 'Next'.

The following screen is displayed:

Create Queue Manager

Queue Manager
Enter configuration options

Queue manager name:

☒ Start queue manager after it has been created

Multi-instance Queue Manager:

☐ Permit a standby instance

Select type of queue manager startup

☒ Automatic
☐ Service (manual)
☐ Interactive (manual)

Configures the queue manager to start automatically when the machine starts up.

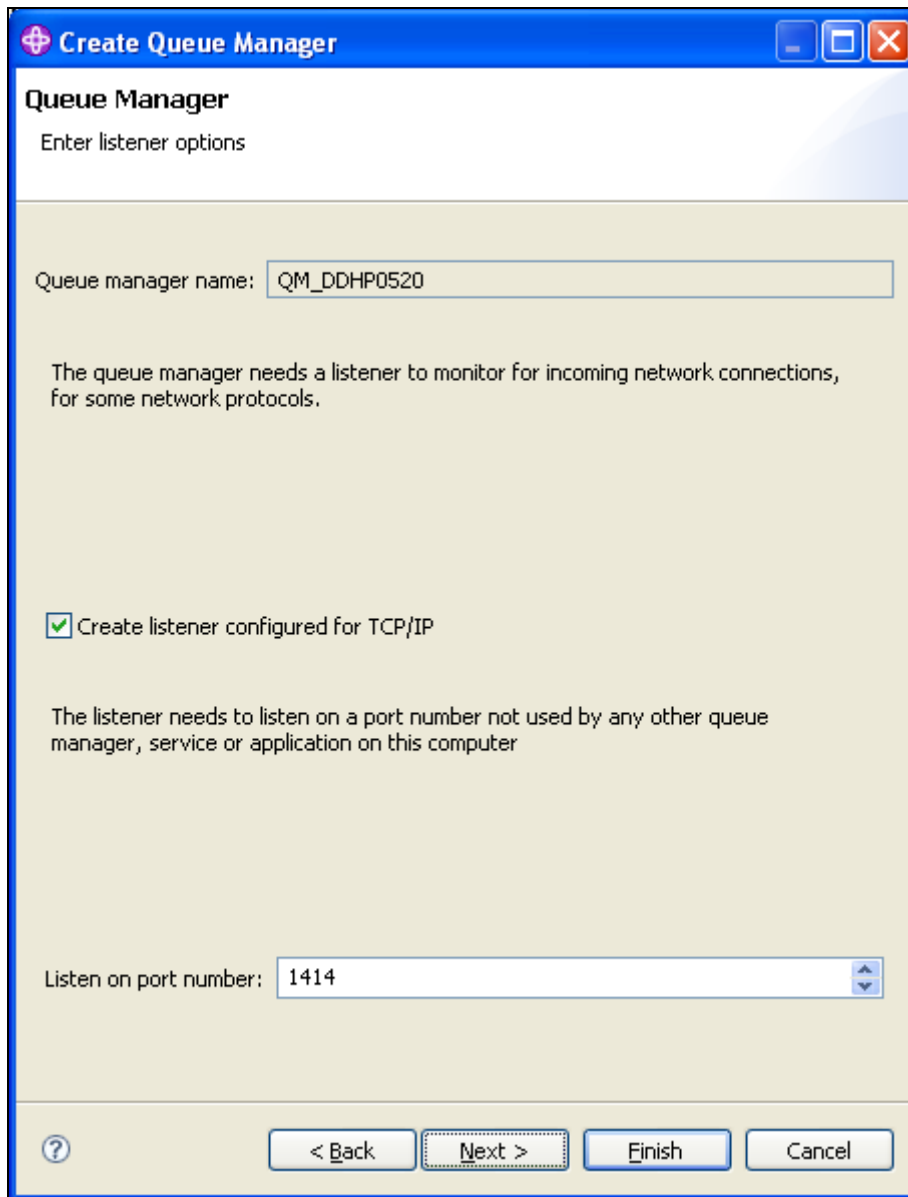
Create server-connection channel to allow remote administration of the queue manager over TCP/IP

☐ Create server-connection channel

? < Back Next > Finish Cancel

6. Click 'Next'.

The following screen is displayed:



The image shows a Windows-style dialog box titled "Create Queue Manager". The title bar is blue with standard minimize, maximize, and close buttons. The main area has a light beige background. At the top, the text "Queue Manager" is followed by "Enter listener options". Below this, there is a text input field for "Queue manager name:" containing the text "QM_DDHP0520". A paragraph of text states: "The queue manager needs a listener to monitor for incoming network connections, for some network protocols." Below this is a checked checkbox labeled "Create listener configured for TCP/IP". Another paragraph of text states: "The listener needs to listen on a port number not used by any other queue manager, service or application on this computer". At the bottom, there is a "Listen on port number:" label followed by a spin box containing the value "1414". The bottom of the dialog features a help icon (question mark in a circle) on the left and four buttons: "< Back", "Next >", "Finish", and "Cancel".

Create Queue Manager

Queue Manager
Enter listener options

Queue manager name: QM_DDHP0520

The queue manager needs a listener to monitor for incoming network connections, for some network protocols.

☒ Create listener configured for TCP/IP

The listener needs to listen on a port number not used by any other queue manager, service or application on this computer

Listen on port number: 1414

? < Back Next > Finish Cancel

7. Specify the 'Listen on port number' as '1414' (default). Click 'Next'. The following screen is displayed:

Create Queue Manager

Queue Manager
Enter explorer options

Queue manager name: QM_DDHP0520

☒ Autoreconnect

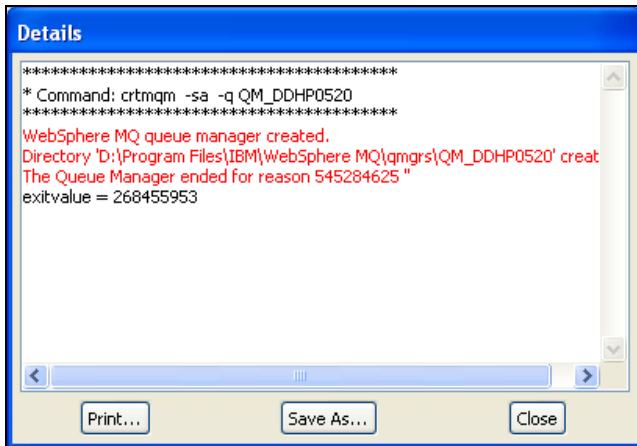
Automatic Refresh

☒ Automatically refresh information shown for this queue manager

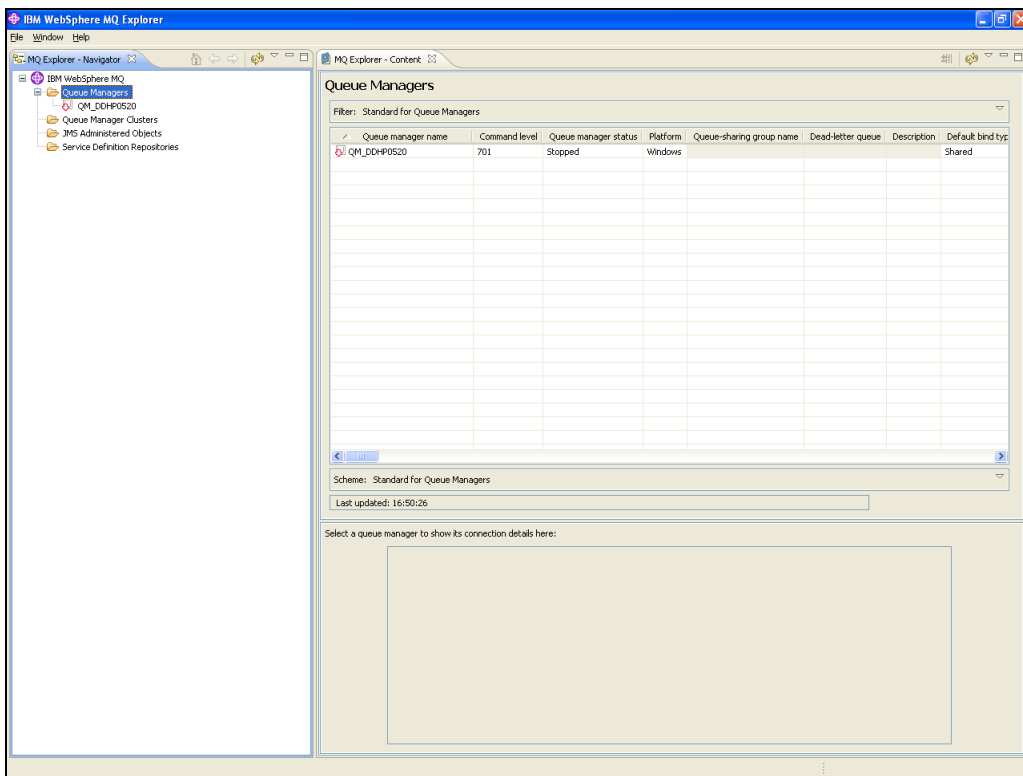
Interval (seconds): 15

? < Back Next > Finish Cancel

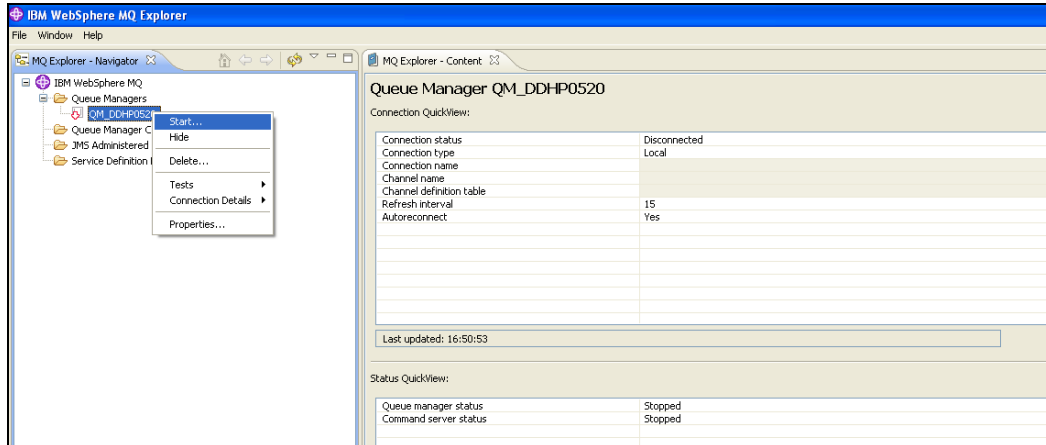
8. Click 'Finish'. The following screen is displayed:



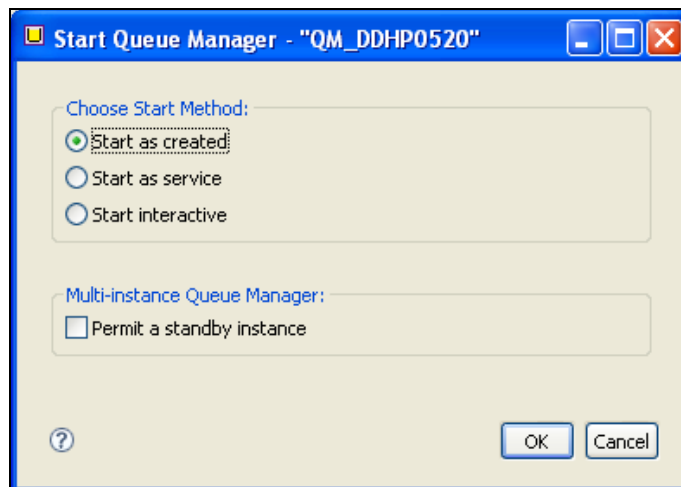
9. Close the message. The following screen is displayed:



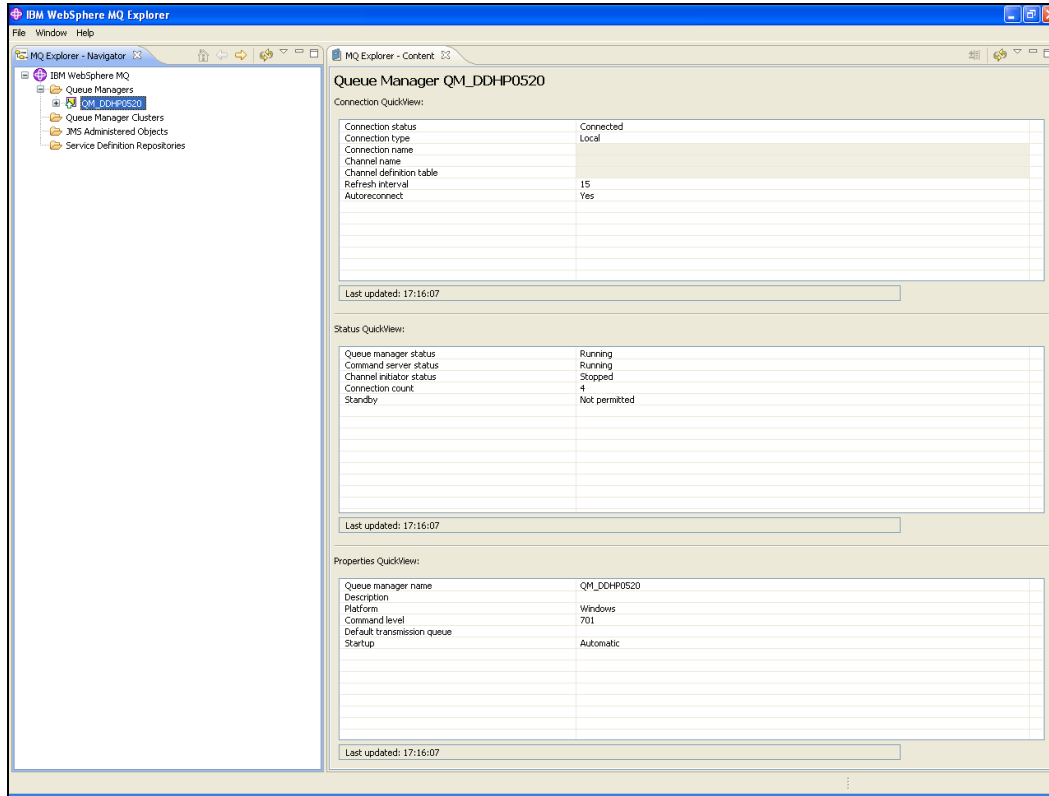
10. Right click 'Queue Manager' and select 'Start'. The following screen is displayed:



11. Right click 'Queue Manager QM_DDHP0520' and select 'Start'. The following screen is displayed:



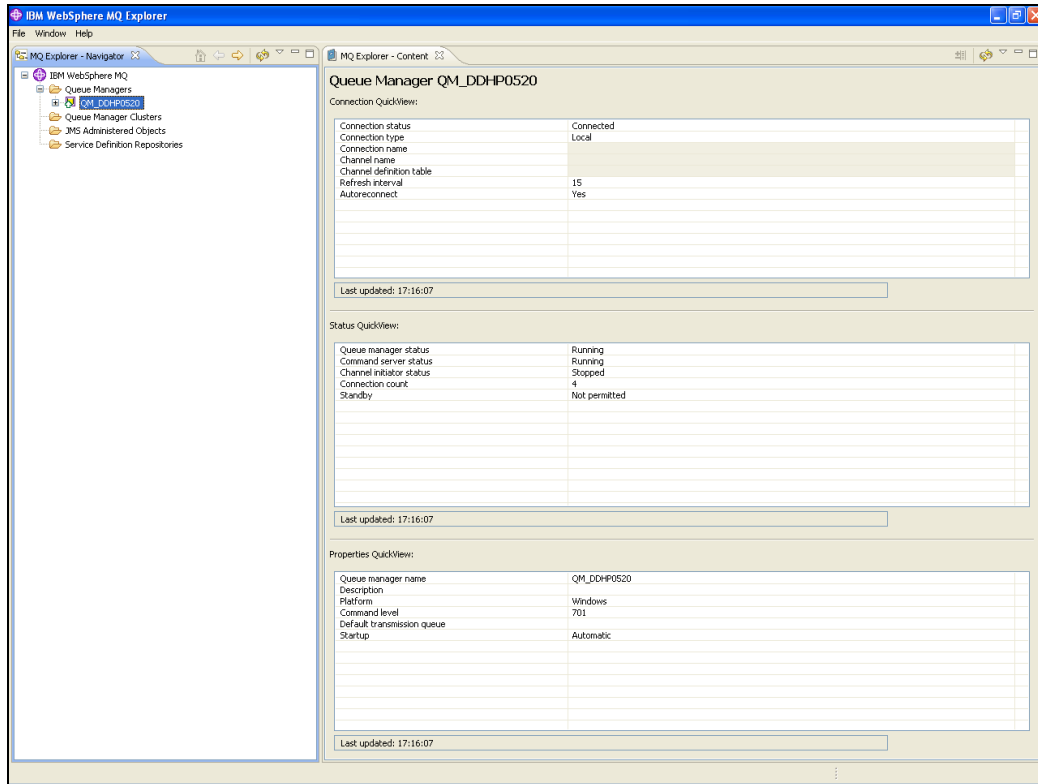
12. Click 'OK'. The following screen is displayed:



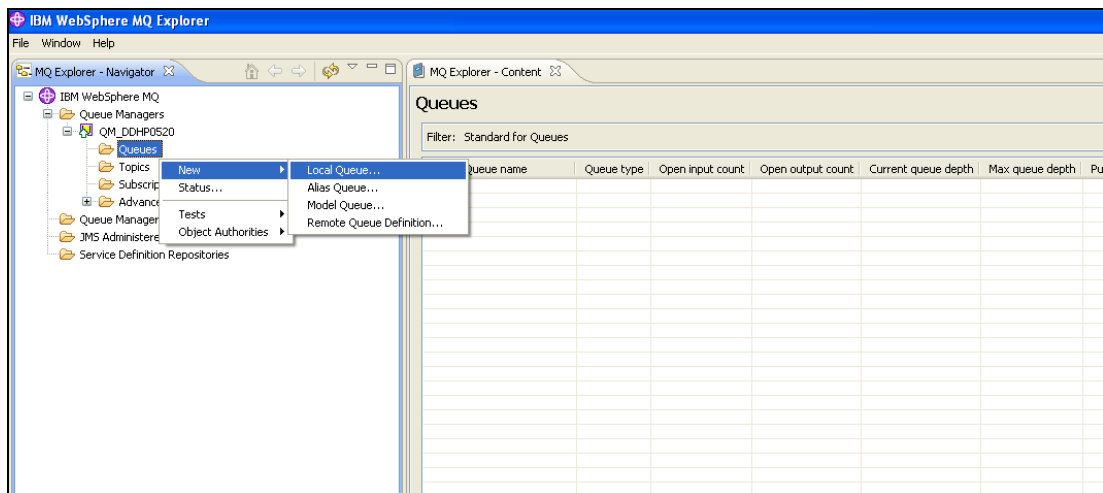
2.2.2 Creating Queues

To create queues, follow the steps given below:

1. Start MQ server console.



2. On the left pane, go to 'IBM Websphere MQ > Queue Managers > QM_DDHP0520 > Queues > New > Local Queue' as shown below.



The following screen is displayed:



Queue Name should be ALL CAPS, else issue will occur at listener level in WAS.

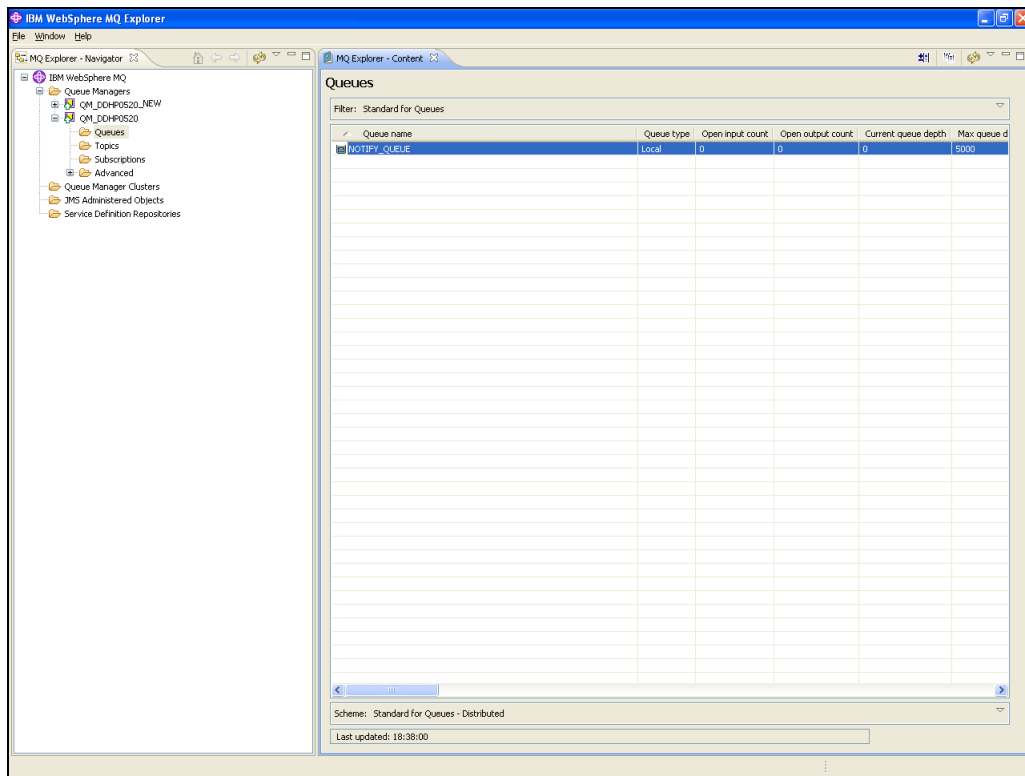
The 'New Local Queue' dialog box, titled 'Create a Local Queue', prompts the user to 'Enter the details of the object you wish to create'. It features a text field for 'Name' containing 'NOTIFY_QUEUE'. Below this, a section for selecting an existing object shows 'SYSTEM.DEFAULT.LOCAL.QUEUE' in a dropdown menu, with a 'Select...' button to its right. A checkbox labeled 'Start wizard to create a matching JMS Queue' is present and unchecked. The bottom of the dialog includes a help icon, a '< Back' button, a 'Next >' button, and 'Finish' and 'Cancel' buttons.

3. Specify the queue name. Click 'Next'. The following screen is displayed:

The 'New Local Queue' dialog box, titled 'Change properties', prompts the user to 'Change the properties of the new Local Queue'. On the left is a tree view with 'General' selected. The main area displays the 'General' properties: 'Queue name' (NOTIFY_QUEUE), 'Queue type' (Local), 'Description' (NOTIFY_QUEUE), 'Put messages' (Allowed), 'Get messages' (Allowed), 'Default priority' (0), 'Default persistence' (Persistent), 'Scope' (Queue manager), and 'Usage' (Normal). The bottom of the dialog includes a help icon, a '< Back' button, a 'Next >' button, and 'Finish' and 'Cancel' buttons.

4. Specify the description. Select 'Persistent' as the 'Default persistence'.

Select 'Queues' on the left pane.



5. You can find the new queue name in the list.

2.3 Creating Queue Manager and Queue using UNIX Commands

You need to create, configure, post and view messages in IBM MQ queues. The method is described under the following headings.

For this, first you need to open 'Putty' and connect it to the MQ server installed box.

2.3.1 Creating Queue Manager

Change the directory to '<Websphere_MQ_HOME>'. Here, 'Websphere_MQ_HOME' is the MQ server software installation directory.

The command to create Queue Manager is given below:

```
crtmqm <queue_manager_name>
```

Example

```
crtmqm FC_QMGR
```

This command creates the queue manager 'FC_QMGR' in the MQ server.

2.3.2 **Starting Queue Manager**

Once the queue manager is created, you need to start the queue manager using the following command:

```
strmqm <queue_manager_name>
```

Example

```
strmqm FC_QMGR
```

This command starts the 'FC_QMGR' queue manager.

2.3.3 **Starting MQ Service to Create Queues under FC_QMGR**

After starting the queue manager, run the MQSC service (for creating queues and other objects) of queue manager. You can use the following command:

```
runmqsc <queue_manager_name>
```

Example

```
runmqsc FC_QMGR
```

This command starts the MQ service for 'FC_QMGR'.

2.3.4 **Creating Queues**

After starting the MQSC issue, you need to create the required queues using the following command:

```
DEFINE QLOCAL (<QUEUE_NAME>)
```

Example

```
DEFINE QLOCAL (EMSOUT_QUEUE)
```

This command creates all the necessary queues.

2.3.5 **Creating Channel**

After creating the queues, you need to create a channel for queue manager using the following command:

```
DEFINE CHANNEL (<CHNL_NAME>) CHLTYPE(<CHANNEL_TYPE>)
```

Here, 'CHNL_NAME' is the name of the channel and 'CHANNEL_TYPE' is the type of channel such as server connection, sender, receiver, etc. You can create the server connection channel using the following command:

```
DEFINE CHANNEL (FC_CNL) CHLTYPE (SVRCONN)
```

Here, SVRCONN stands for the 'Server Connection' channel type.

2.3.6 **Ending MQSC**

You can use the command 'END' to end the MQSC service.

2.3.7 Creating Bindings

After creating the queues and the channel, you need to bind them using the JMSAdmin. To do this, start Putty and connect it to the MQ server installed box.

Move to the directory '<Websphere_MQ_HOME>/java/bin'. Here, 'Websphere_MQ_HOME' is the MQ server software installation path.

In this folder, you will find the file 'JMSAdmin.config'. You need to give the PROVIDER_URL to which the .bindings files need to be created.

PROVIDER_URL=file: <Websphere_MQ_HOME>/JNDI

Example

PROVIDER_URL=file: /var/mqm/JNDI

Below environment variables need to be set before creating queue/connection factory configurations.

```
PATH=$PATH:$HOME/bin
export MQ_JAVA_INSTALL_PATH=/opt/mqm/java
export MQ_JAVA_DATA_PATH=/var/mqm
export MQ_JAVA_LIB_PATH=/opt/mqm/java/lib
L=$MQ_JAVA_INSTALL_PATH/lib
CLASSPATH=$CLASSPATH:$L/com.ibm.mq.jar:$L/com.ibm.mqjms.jar
export
CLASSPATH=$CLASSPATH:/opt/mqm/samp/jms/samples:/opt/mqm/samp/wmqjava/samp
export PATH
```

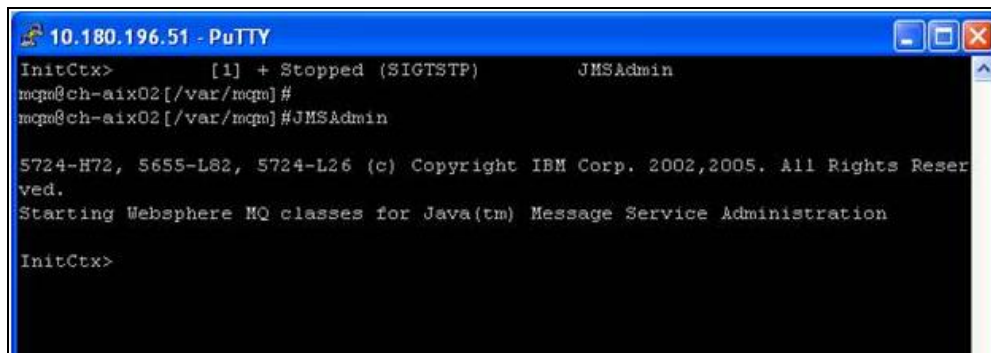
Launch JMSAdmin



You should have read-write access on this folder.

2.3.8 Creating QCF

After creating the queues and channel, you need to create a queue connection factory in the MQ server. Complete the above steps and make above changes to the 'JMSAdmin.config' file. Move to the directory '<Websphere_MQ_HOME>/java/bin' in Putty. Type 'JMSAdmin' as shown in the figure.



```
10.180.196.51 - PuTTY
InitCtx> [1] + Stopped (SIGTSTP) JMSAdmin
mqm@ch-aix02 [/var/mqm] #
mqm@ch-aix02 [/var/mqm] # JMSAdmin

5724-H72, 5655-L82, 5724-L26 (c) Copyright IBM Corp. 2002,2005. All Rights Reserved.
Starting Websphere MQ classes for Java(tm) Message Service Administration

InitCtx>
```

This will take you to the 'InitCtx>' section. Use the following command to create queue connection factory:


```
define qcf (<qcf_name>) qmgr(<queue_mgr_name>) host (<ip-address>) port(1010)
tran(CLIENT)
```

Example

```
define qcf (fc_qcf) qmgr(FC_QMGR) host (10.10.10.10) port(1010) tran(CLIENT)
```

This creates the queue connection factory for the queue manager 'FC_QMGR' in 10.10.10.10 server.

Now, you need to create the bindings for each queue. Use the following command in 'InitCtx>'.

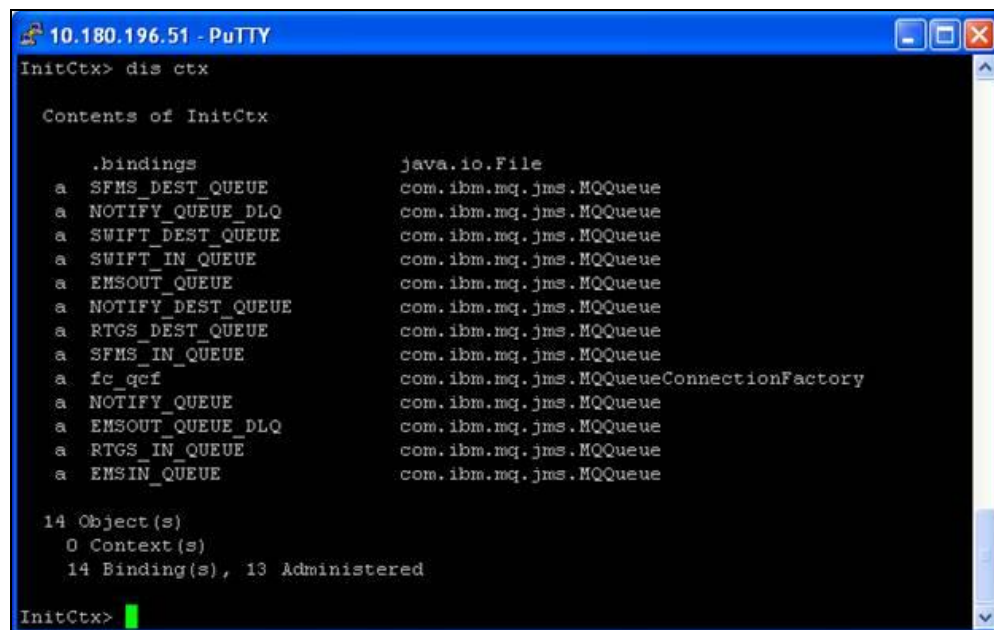
```
DEFINE Q(EMSOUT_QUEUE) QUEUE(EMSOUT_QUEUE) QMGR(FC_QMGR)
```

Use the same command for other queues also.

You can use the following command to view the binding details:

```
InitCtx> display ctx
```

The binding details are displayed as shown in the figure below.



```
10.180.196.51 - PuTTY
InitCtx> dis ctx

Contents of InitCtx

    .bindings                                java.io.File
a SFMS_DEST_QUEUE                          com.ibm.mq.jms.MQQueue
a NOTIFY_QUEUE_DLQ                        com.ibm.mq.jms.MQQueue
a SWIFT_DEST_QUEUE                        com.ibm.mq.jms.MQQueue
a SWIFT_IN_QUEUE                          com.ibm.mq.jms.MQQueue
a EMSOUT_QUEUE                            com.ibm.mq.jms.MQQueue
a NOTIFY_DEST_QUEUE                       com.ibm.mq.jms.MQQueue
a RTGS_DEST_QUEUE                         com.ibm.mq.jms.MQQueue
a SFMS_IN_QUEUE                           com.ibm.mq.jms.MQQueue
a fc_qcf                                 com.ibm.mq.jms.MQQueueConnectionFactory
a NOTIFY_QUEUE                            com.ibm.mq.jms.MQQueue
a EMSOUT_QUEUE_DLQ                       com.ibm.mq.jms.MQQueue
a RTGS_IN_QUEUE                           com.ibm.mq.jms.MQQueue
a EMSIN_QUEUE                             com.ibm.mq.jms.MQQueue

14 Object(s)
  0 Context(s)
 14 Binding(s), 13 Administered

InitCtx>
```

Once this is created, you need to check whether the *.bindings* file is available in the path given in 'JMSAdmin.config' (PROVIDER_URL).

Now, you need to create JMS queues for DIRECT queues to post messages. DIRECT queues require connection to Oracle FLEXCUBE application. Please refer the document "Resource To be Created" for queue names list.

You need to create JMS queues for the queues mentioned in the document “Resource To be Created”.

Queue name	Queue type	Open input count	Open output count	Current queue depth
DEFERRED_DEST_QUEUE	Local	0	0	0
EL_NOTIFY_DLQ	Local	0	0	0
EL_NOTIFY_REQ_Q	Local	0	0	0
EL_NOTIFY_RES_Q	Local	0	0	0
ELMDB_DLQ	Local	0	0	0
ELMDB_REQ_Q	Local	0	0	0
ELMDB_RES_Q	Local	0	0	0
EMS_EXTQUEUE	Local	0	0	0
EMS_INQUEUE	Local	2	0	0
EMS_OUTQUEUE	Local	1	0	0
MDB_QUEUE	Local	0	0	0
MDB_QUEUE_DLQ	Local	0	0	0
MDB_QUEUE_RESPONSE	Local	0	0	0
NOTIFY_DEST_QUEUE	Local	0	0	0
NOTIFY_QUEUE	Local	1	0	0
NOTIFY_QUEUE_DLQ	Local	0	0	0
RTGS_INQUEUE	Local	1	0	0
SFMS_INQUEUE	Local	1	0	0

2.3.9 MQ Channel Authentication

MQ Channel Authentication can be managed using following set of MQSC Commands

- Enable Channel Authentication

>ALTER QMGR CHLAUTH(ENABLE)

- Allow MQ Privileged Users to access Channel

>SET CHLAUTH(*) TYPE(BLOCKUSER) USERLIST(*MQADMIN) ACTION(REMOVE)

- Allow all client addresses to access Channel

>SET CHLAUTH(SYSTEM.*) TYPE(ADDRESSMAP) ADDRESS(*) ACTION(REMOVE)

2.4 Viewing IBM MQ Queues

Through MQ explorer, you can view the queues created in IBM MQ. If the IBM MQ server sits on a Unix box, an MQ client needs to be setup in a client machine in Windows operating system.

Follows the below steps to view the queues created in server, from an MQ client:

1. Install IBM MQ client in a client terminal.
2. Open the client MQ explorer.
3. Right click 'Queue Managers' on the left pane and select 'Show/Hide Queue Managers'.
4. Click 'Add' in the Show/Hide Queue Managers window.
5. Specify the name of Queue Manager which is created in the MQ server. Click 'Next'.
6. Specify the IP address of the IBM MQ server in the Host name or IP address field.

7. Specify the Port number in which the Queue manager is created in MQ server.
8. Specify the server connection channel created in the MQ server. Click 'Finish'.

Under the Queue Manager menu, the queue manger created in the server is displayed with its IP address and port number in braces.

The screenshot shows the IBM WebSphere MQ Explorer interface. The left pane displays the 'Queue Managers' tree, with 'FC_QMGR on '10.180.196.51'(1415)' selected. The right pane shows the 'Queues' tab, which contains a table of queues. The table has columns for Queue name, Queue type, Definition type, Open input count, Open output count, Current queue depth, Max queue depth, and Put messages.

Queue name	Queue type	Definition type	Open input count	Open output count	Current queue depth	Max queue depth	Put messages
EMSI_IN_QUEUE	Local	Predefined	1	0	0	5000	Allowed
EMSI_OUT_QUEUE	Local	Predefined	1	0	12	5000	Allowed
EMSI_OUT_QUEUE_DLQ	Local	Predefined	0	0	0	5000	Allowed
FC_QMGR	Local	Predefined	0	0	0	5000	Allowed
MDI_QUEUE	Local	Predefined	1	0	0	999999999	Allowed
MDI_QUEUE_DLQ	Local	Predefined	0	0	6	999999999	Allowed
MDI_QUEUE_RESPONSE	Local	Predefined	0	0	12	999999999	Allowed
NOTIFY_DEST_QUEUE	Local	Predefined	0	0	1	5000	Allowed
NOTIFY_QUEUE	Local	Predefined	3	0	0	5000	Allowed
NOTIFY_QUEUE_DLQ	Local	Predefined	0	0	19	5000	Allowed
RTGS_DEST_QUEUE	Local	Predefined	0	0	0	5000	Allowed
RTGS_IN_QUEUE	Local	Predefined	1	0	0	5000	Allowed
SPMS_DEST_QUEUE	Local	Predefined	0	0	32	5000	Allowed
SPMS_IN_QUEUE	Local	Predefined	1	0	3	5000	Allowed
SPMS_OUT_QUEUE	Local	Predefined	1	0	3	5000	Allowed

3. Creating JDBC Resources on Web Sphere

3.1 Introduction

This chapter guides you through the process of JDBC resource creation on IBM Websphere application server.

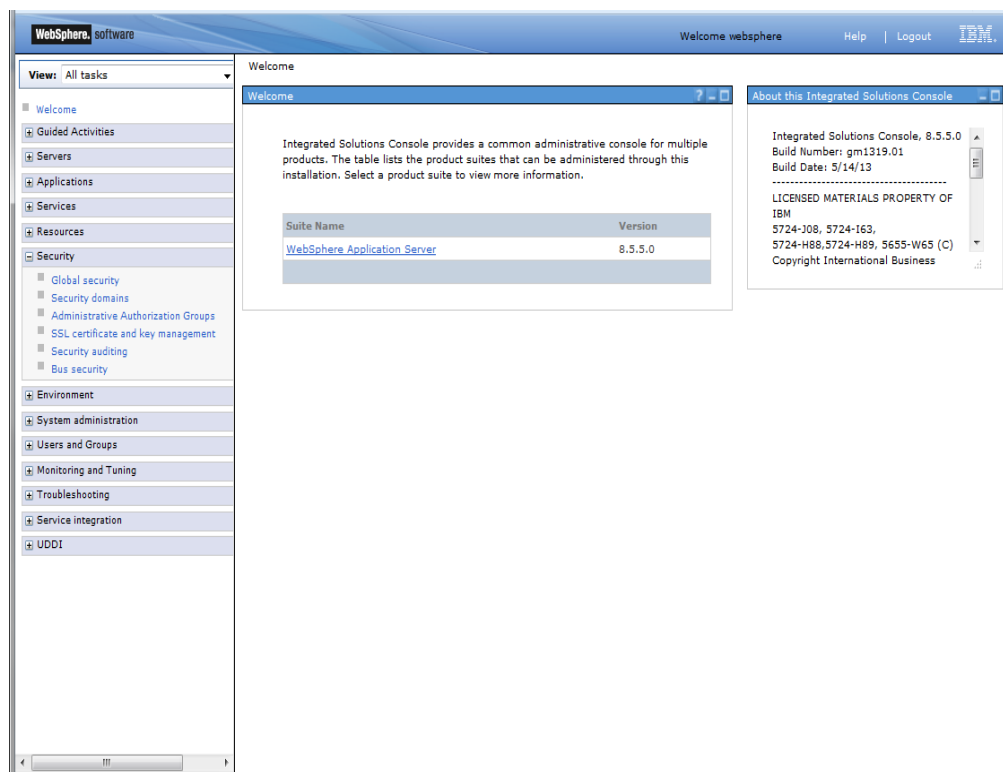
3.2 Prerequisite:

If OCI needs to be used in data sources, please refer the vendor specific support manual and make the configuration changes before creating datasources.

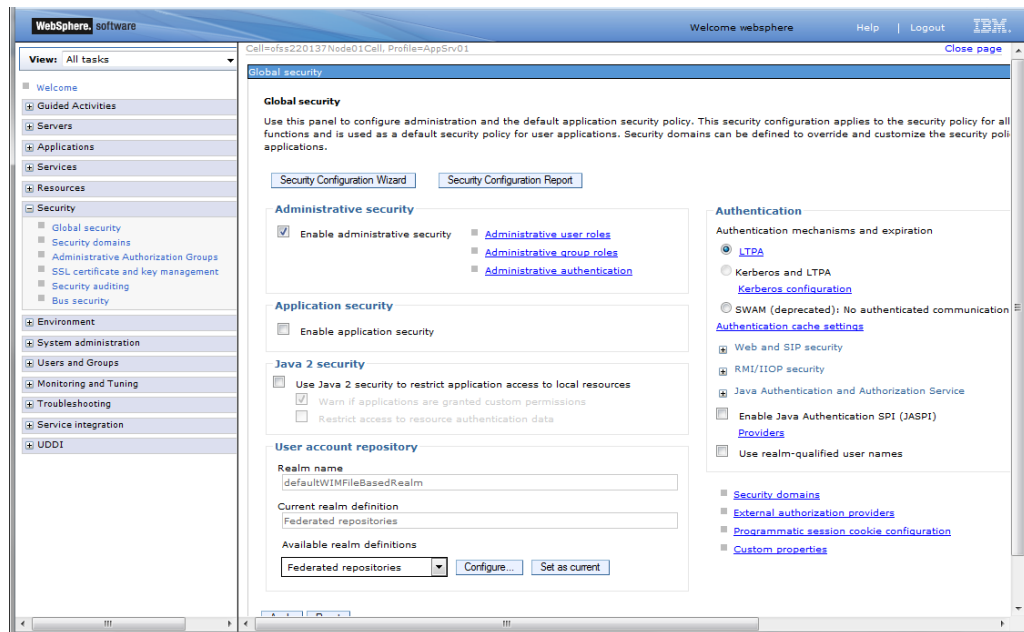
3.3 Creating JDBC Sources

3.3.1 Creating Global Security

1. Specify the Websphere administrator username and password.
2. Click 'Log In'.
3. Navigate to Websphere home page.

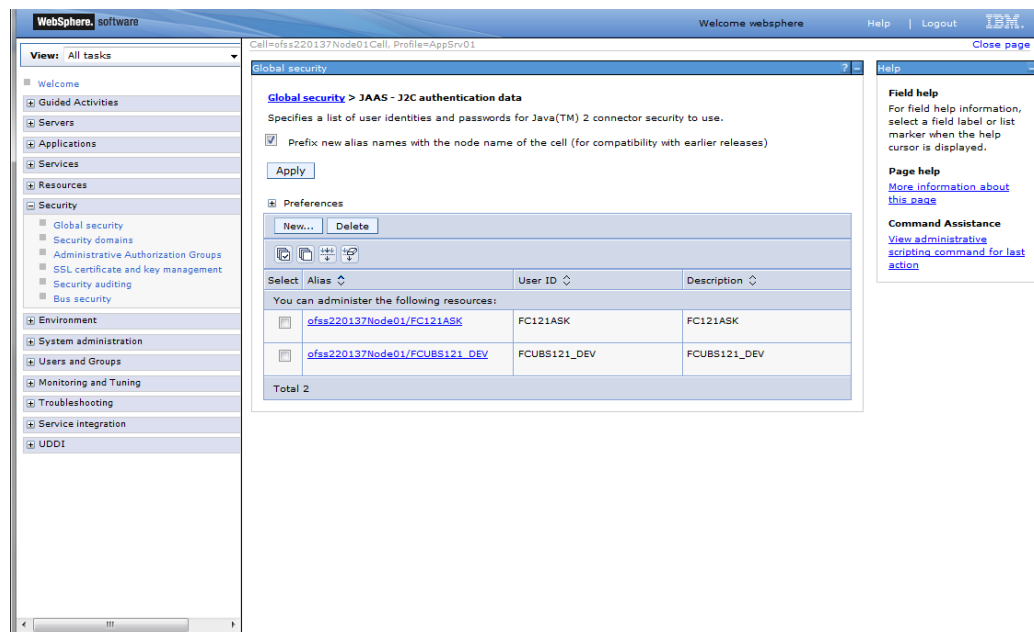


4. Expand 'Security' and select 'Global Security'. The following screen is displayed.



5. Expand 'Java Authentication', go to 'Authorization Service' and click 'J2C authentication data'.

The following screen is displayed.



6. Click 'New'.

The following screen is displayed.

WebSphere software | Welcome websphere | Help | Logout | IBM | Close page

Cell=ofss220137Node01Cell, Profile=AppSrv01

Global security

Global security > JAAS - J2C authentication data > New...

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

General Properties

Alias: FCITR2

User ID: FCITR2

Password: *****

Description: FCITR2

Apply OK Reset Cancel

Field help: For field help information, select a field label or list marker when the help cursor is displayed.

Page help: [More information about this page](#)

Command Assistance: [View administrative scripting command for last action](#)

7. You need to define the connection properties. Specify the following details.

- Alias
- User ID of the Database
- Password of the Database
- Description

8. Once you have specified the above details, click 'Apply' and then click 'Save' link.

The following screen is displayed.

WebSphere software | Welcome websphere | Help | Logout | IBM | Close page

Cell=ofss220137Node01Cell, Profile=AppSrv01

Global security

Global security > JAAS - J2C authentication data

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

☒ Prefix new alias names with the node name of the cell (for compatibility with earlier releases)

Apply

Preferences

New... Delete

Select	Alias	User ID	Description
<input type="checkbox"/>	ofss220137Node01/FC121ASK	FC121ASK	FC121ASK
<input type="checkbox"/>	ofss220137Node01/FCUBS121_DEV	FCUBS121_OEV	FCUBS121_DEV

Total 2

Field help: For field help information, select a field label or list marker when the help cursor is displayed.

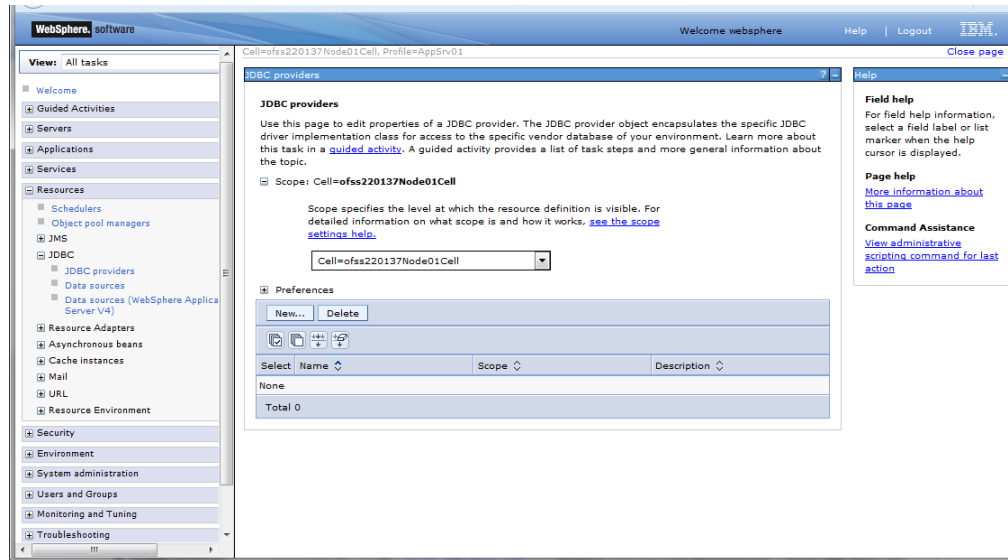
Page help: [More information about this page](#)

Command Assistance: [View administrative scripting command for last action](#)

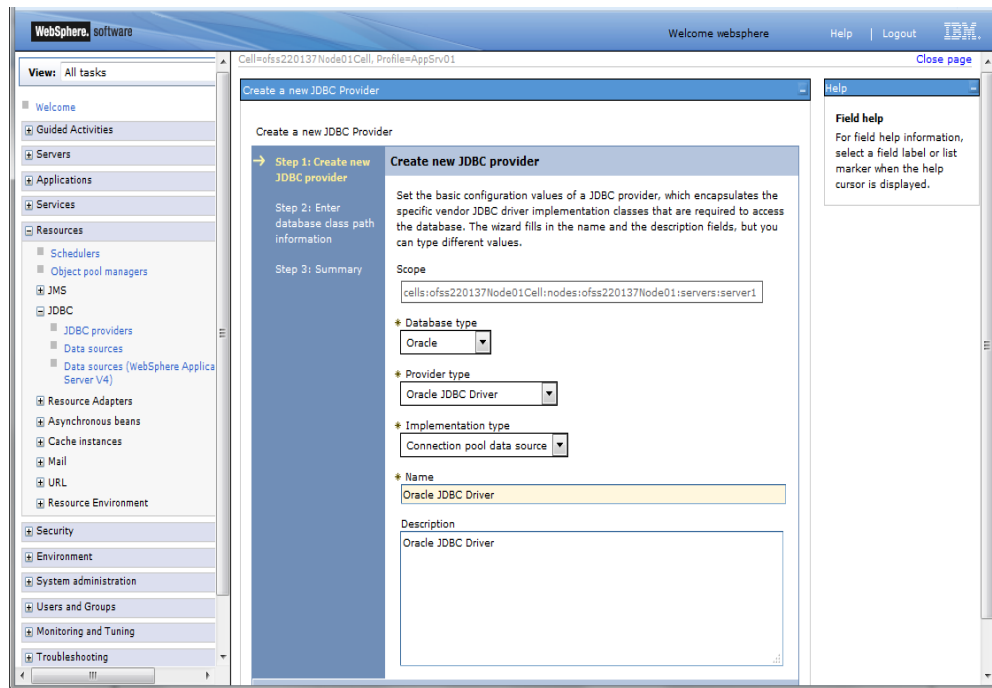
3.3.2 JDBC Provider for Non XA Data Source

Follow the steps given below:

1. Login to the application server administration console.
2. Expand 'Resources > JDBC' and select 'JDBC Providers'.



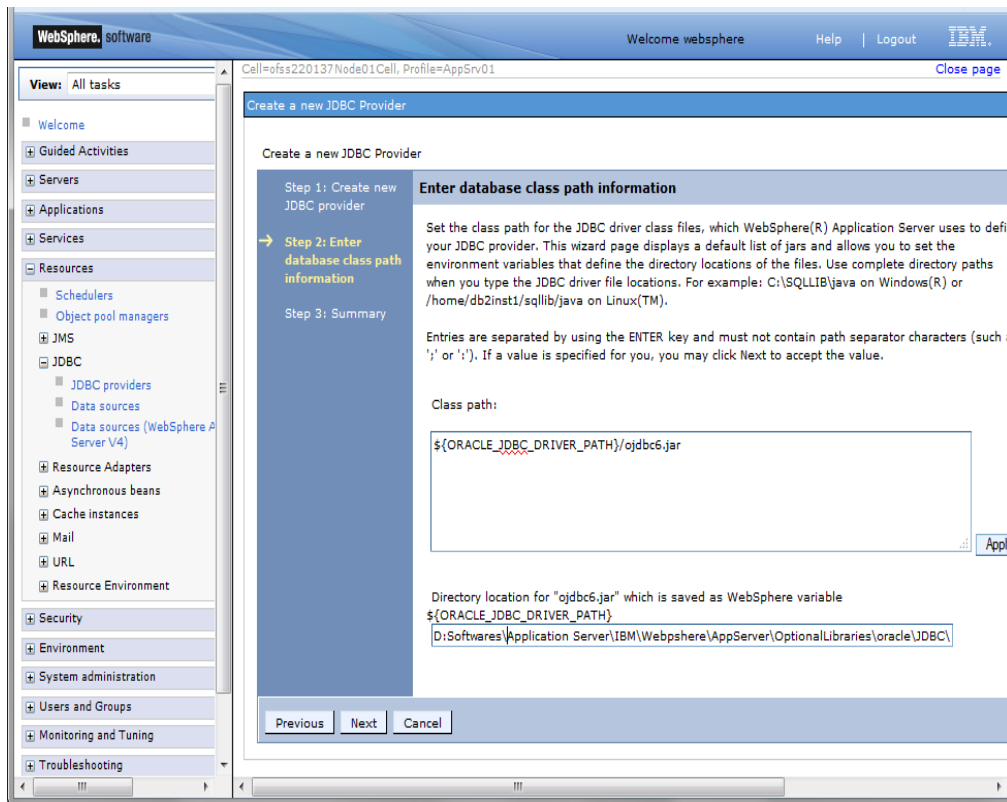
3. Select 'Node' from the dropdown list.
4. Click New, The following screen is displayed:



5. Specify the following details:

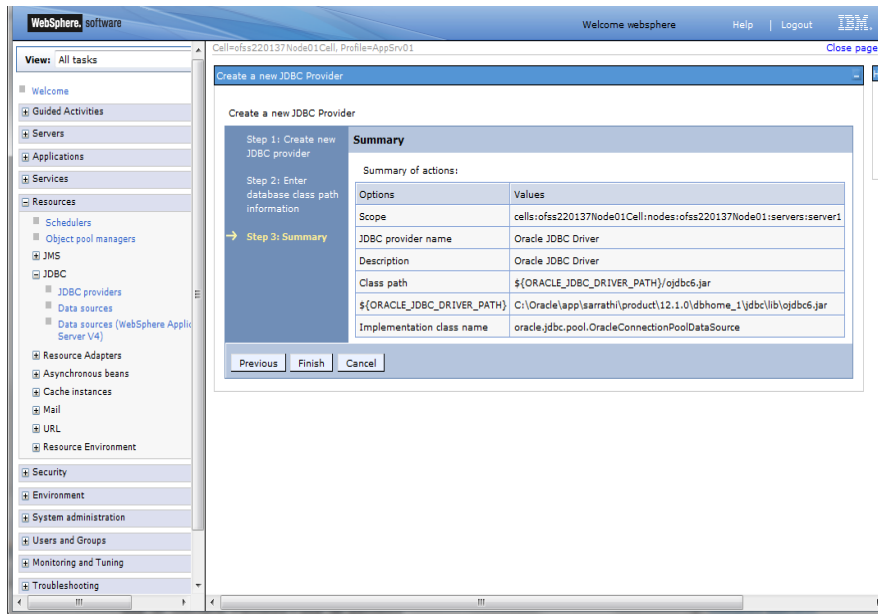
Database Type	Oracle
Provider Type	Oracle JDBC Driver
Implementation Type	Connection pool data source
Name	FCIS
Description	FCIS JDBC Driver

6. Click 'Next'. The following screen is displayed:

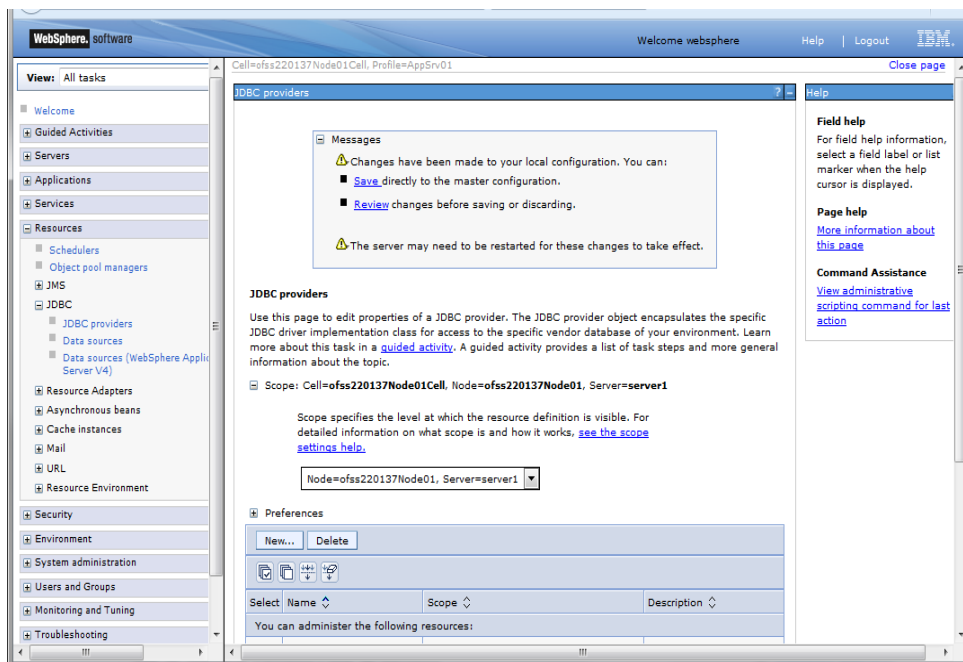


7. Provide the location of ojdbc6.jar. Click 'Next'.

The following screen is displayed.



8. Click 'Finish'. The following screen is displayed.



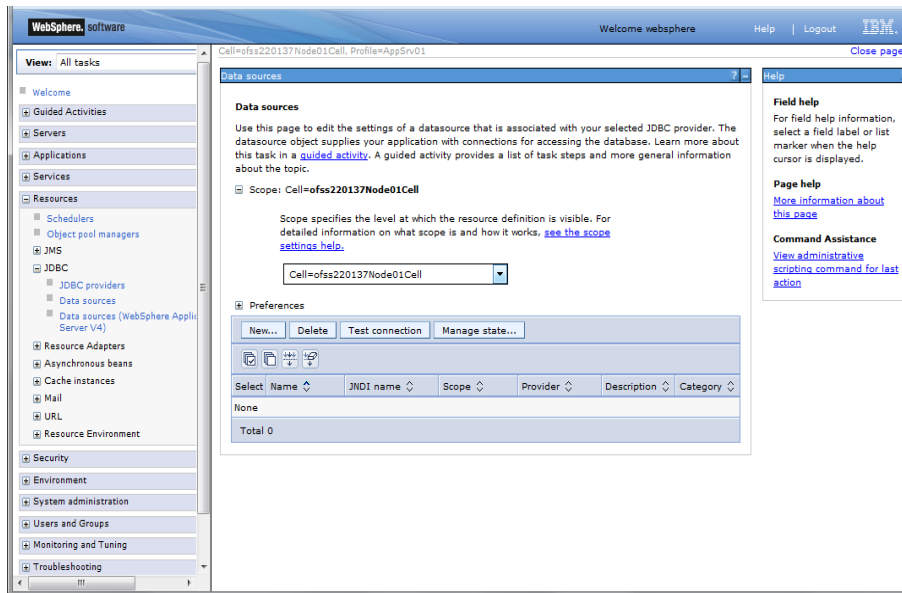
9. Click 'Save'.

3.3.3 Creating Non XA Data Source

Follow the steps given below:

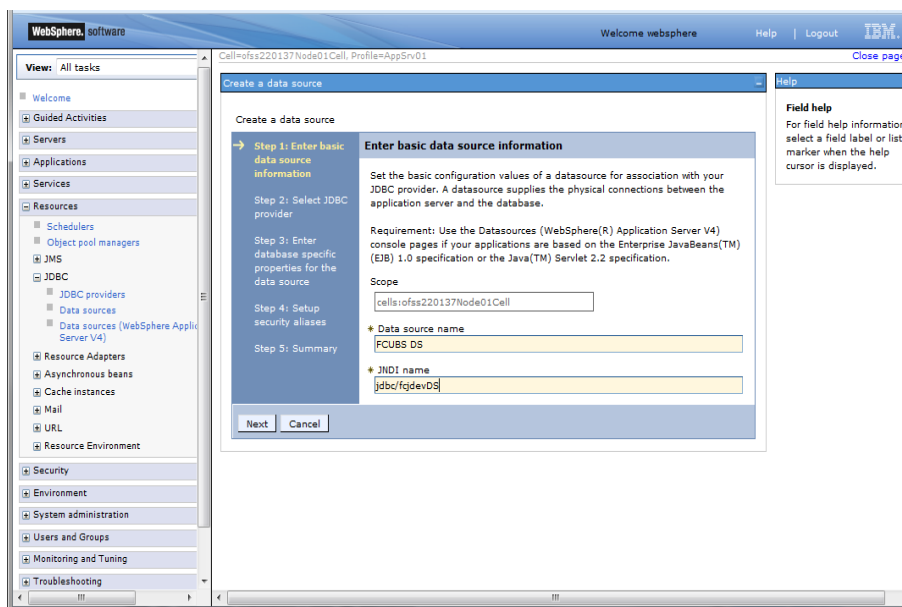
10. Login to the application server administration console.
11. Expand 'Resources > JDBC' and click 'Data sources'.

The following screen is displayed.



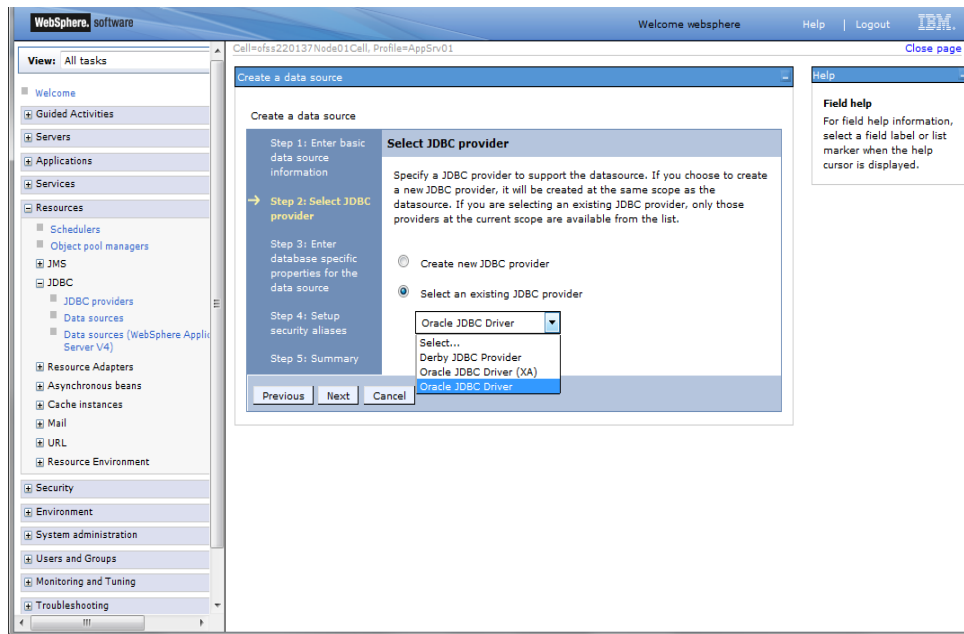
12. Select 'Node' from the drop-down list.

Click New, The following screen is displayed.

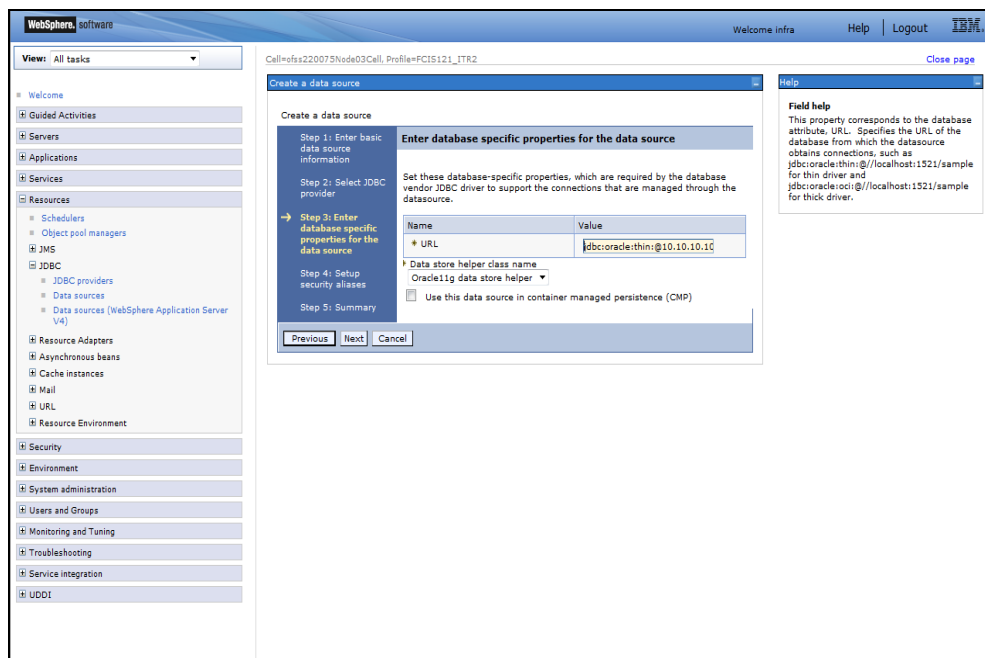


13. Specify the data source name as 'FCIS DS'.
14. Specify the JNDI name as 'jdbc/fcjdevDS'.
15. Click 'Next'.

The following screen is displayed.



16. Select the option 'Select an existing JDBC provider'. From the drop-down list, choose 'Oracle JDBC Driver' and click next. The following screen will be displayed:



17. Specify the URL of the Database

Uncheck “Use this data source in container managed persistence (CMP)”

Example

`jdbc:oracle:thin:@10.10.10.10:1010:KERDEV2`

Here, *10.10.10.10* is the *hostname* where the database is installed, *1010* the *port number* and *KERDEV2* the *instance name*.

18. Select the data store helper class as ‘Oracle11g data store helper’.

19. Click ‘Next’.

The following screen is displayed.

Select user alias from Component-managed authentication alias and Container-managed authentication alias dropdown.

The screenshot shows the 'Create a data source' wizard in the WebSphere Administration Console. The left sidebar contains a navigation tree with categories like Welcome, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The 'Resources' category is expanded, showing 'JDBC' and 'Data sources (WebSphere Application Server V4)'. The main panel displays the 'Setup security aliases' step. It includes a 'Component-managed authentication alias' dropdown set to 'ofsa220075Node03/R2SMS', a 'Mapping-configuration alias' dropdown set to '(none)', and a 'Container-managed authentication alias' dropdown set to 'ofsa220075Node03/R2SMS'. A note at the bottom states: 'Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost.' Below the note are two links: 'Global J2C authentication alias' and 'Security domains'. At the bottom of the wizard are 'Previous', 'Next', and 'Cancel' buttons. A 'Field help' popup is visible on the right side of the wizard.

20. Click 'Next'. The following screen is displayed.

WebSphere software

Cell=ofss220075Node03Cell, Profile=FCIS121_ITR2

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

→ Step 5: Summary

Summary of actions:

Options	Values
Scope	cells/ofss220075Node03Cell:nodes/ofss220075Node03
Data source name	FCIS DS
JNDI name	jdbc/fjdevDS
Select an existing JDBC provider	Oracle JDBC Driver
Implementation class name	oracle.jdbc.pool:OracleConnectionPoolDataSource
URL	jdbc:oracle:thin:@10.10.10.10:KERDEV2
Data store helper class name	com.ibm.websphere.rsadapter.Oracle11gDataSourceHelper
Use this data source in container managed persistence (CMP)	false
Component-managed authentication alias	ofss220075Node03/R2SMS
Mapping-configuration alias	(none)
Container-managed authentication alias	ofss220075Node03/R2SMS

Previous Finish Cancel

Field help
For field help information, select a field label or list marker when the help cursor is displayed.

21. Click 'Finish'. The following screen is displayed.

WebSphere software

Cell=ofss220137Node01Cell, Profile=AppSrv01

Data sources

Messages

- Changes have been made to your local configuration. You can:
 - Save directly to the master configuration.
 - Review changes before saving or discarding.
- The server may need to be restarted for these changes to take effect.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=ofss220137Node01Cell, Node=ofss220137Node01, Server=server1

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Node=ofss220137Node01, Server=server1

Preferences

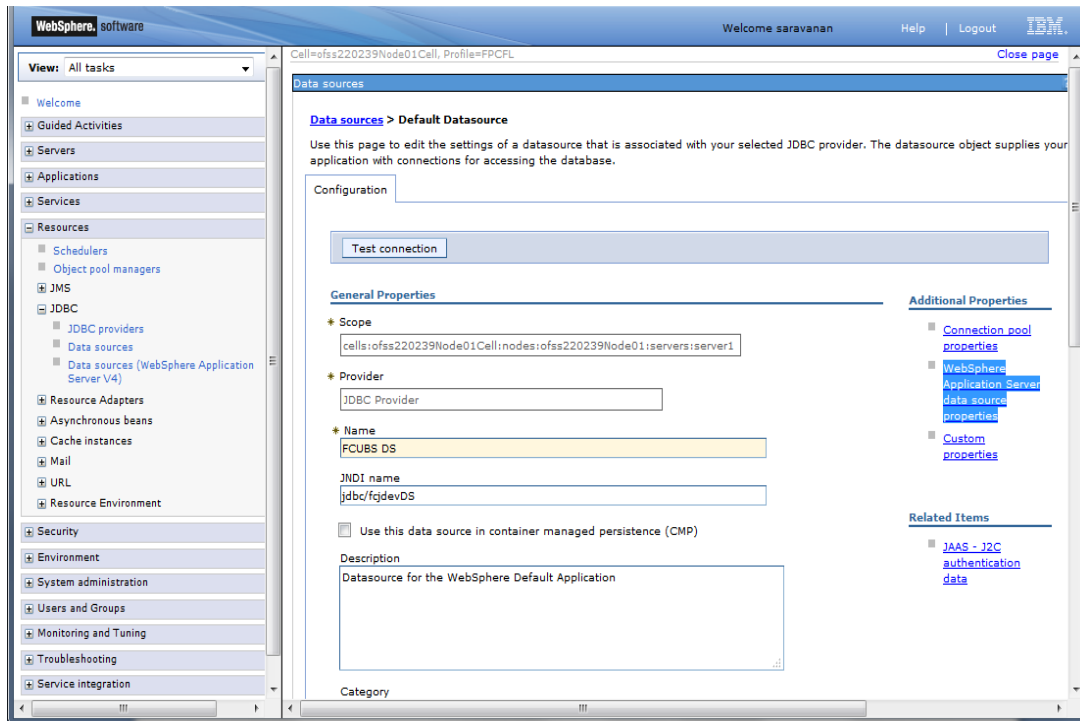
New... Delete Test connection Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	FCIS_DS	jdbc/fjdevDS1	Node=ofss220137Node01,Server=server1	Oracle JDBC	New JDBC DataSource	

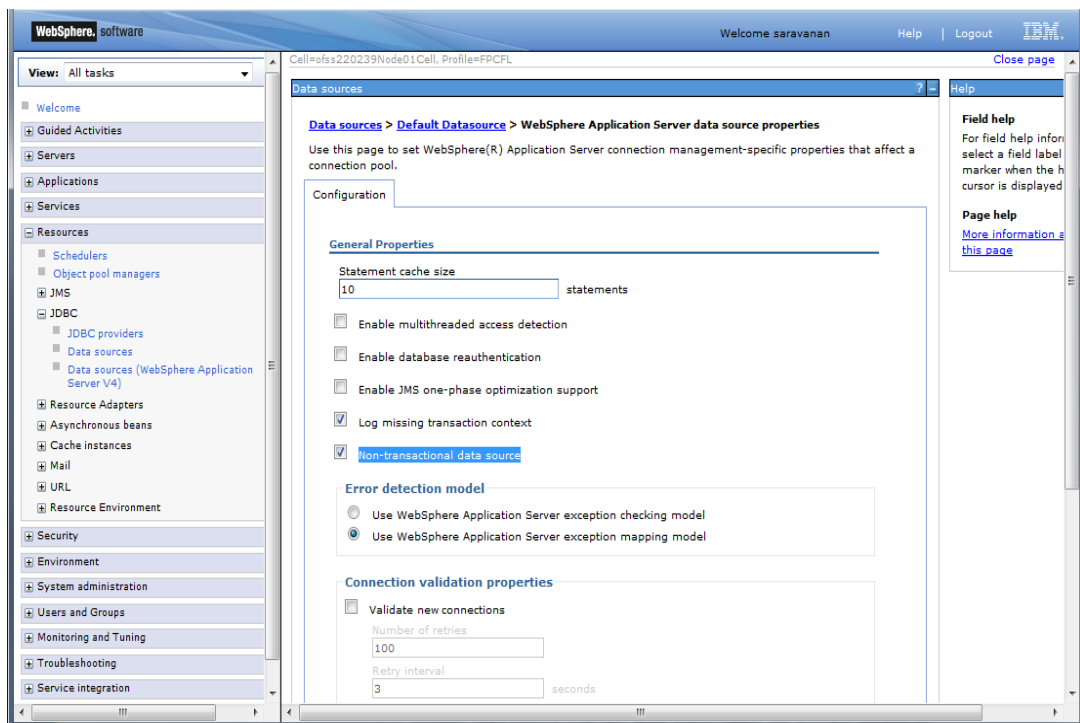
22. Click 'Save'.

23. Following steps need to be followed only for Non-XA datasources

24. Click on the newly created Non-XA datasource, in our example “FCIS DS”. The following screen is displayed



25. Make sure that the checkbox “Use this data source in container managed persistence (CMP)” is unchecked. Then click on the link “WebSphere Application Server data source properties” on the right side.



26. Select the checkbox “Non-transactional data source”.

27. Click Apply button and Click Save link.



Note the following

- You need to create another data source for Oracle FCIS with the JNDI name ‘<Non-XA FCIS HOST JNDI name>_ASYNC’. For example, if the Oracle FCIS HOST Non XA data source JNDI name is ‘jdbc/fcjdevDS’, then you need to create another data source for FCIS 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 FCIS BRANCH JNDI name>_ASYNC’.

3.3.4 Scheduler Data Source configuration

For all the LOB and SMS schema created for FCIS, Equivalent XA data sources are required for Scheduler with Jndi name as “jndi name of LOB/SMS schema”+ “_XA” (Standard naming convention)

Example

If there are three LOB schema’s for FCIS with below jndi names

- ✓ jdbc/BR1204R1
- ✓ jdbc/EN1204R1
- ✓ jdbc/AMC1204R1

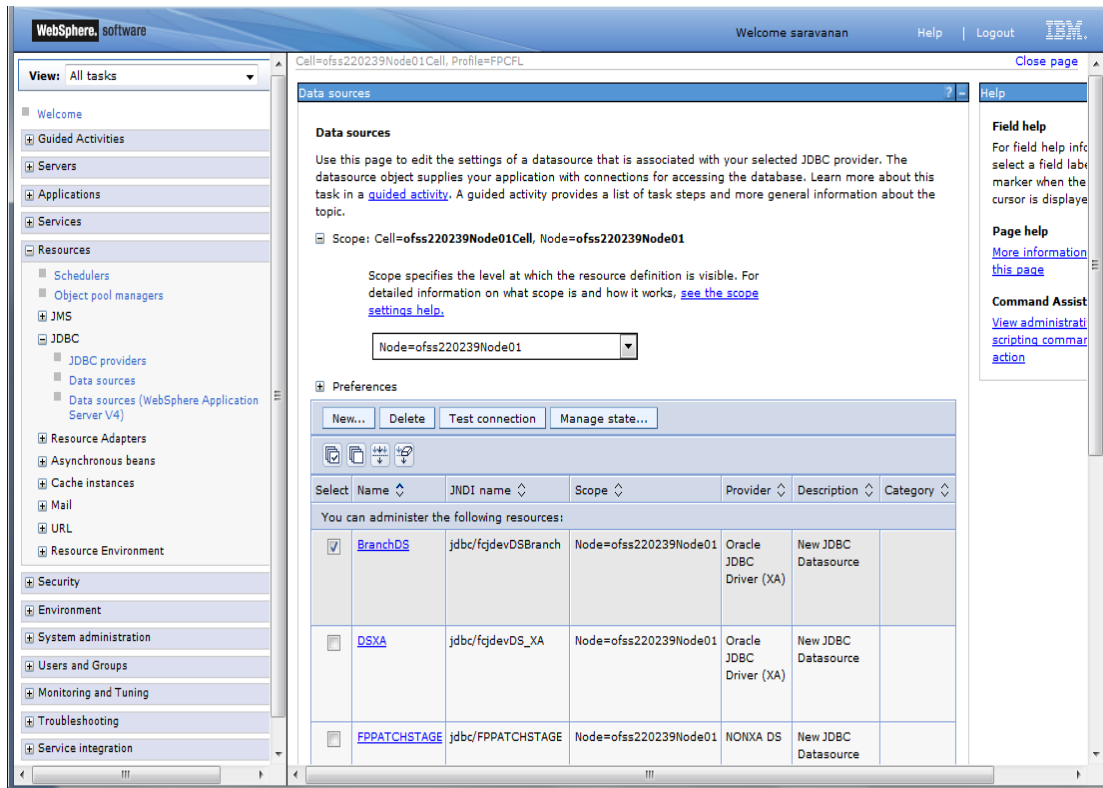
Equivalent Data source setup for scheduler will be

Data source name	Jndi Name
BR1204R1_XA	jdbc/BR1204R1_XA
EN1204R1_XA	jdbc/EN1204R1_XA
AMC1204R1_XA	jdbc/AMC1204R1_XA

3.3.5 Testing Data Source

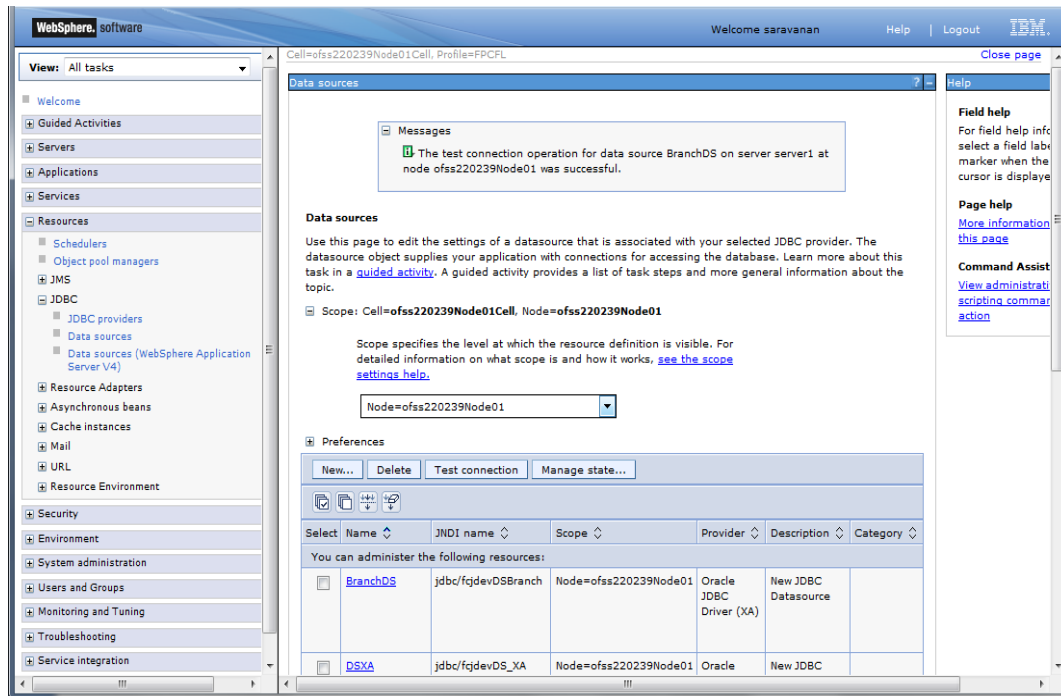
Follow the steps given below:

1. Select the data source as shown in the figure.



2. Click 'Test connection' button.

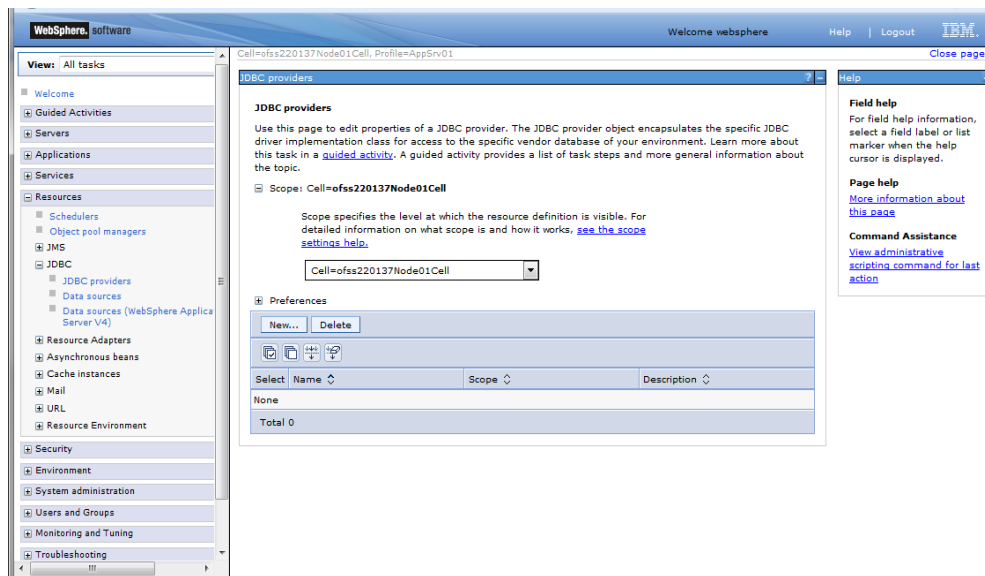
On successful creation, the following message is displayed.



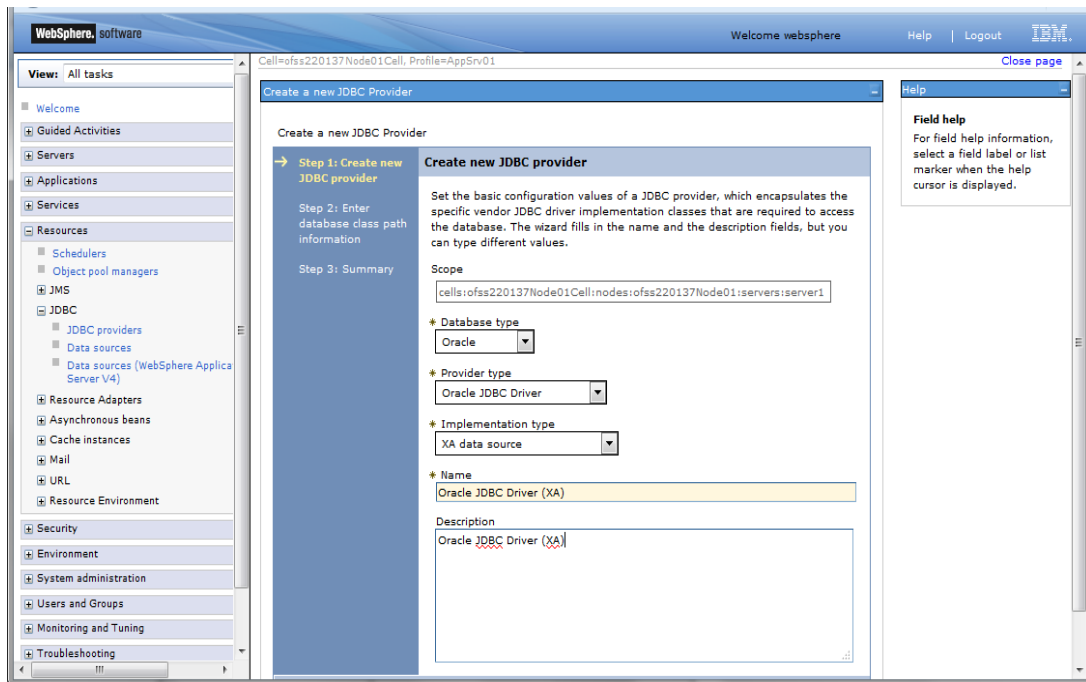
3.3.6 JDBC Provider for XA Data Source

Follow the steps given below:

1. Login to the application server administration console.
2. Expand 'Resources > JDBC' and click 'JDBC Providers'. The following screen is displayed.



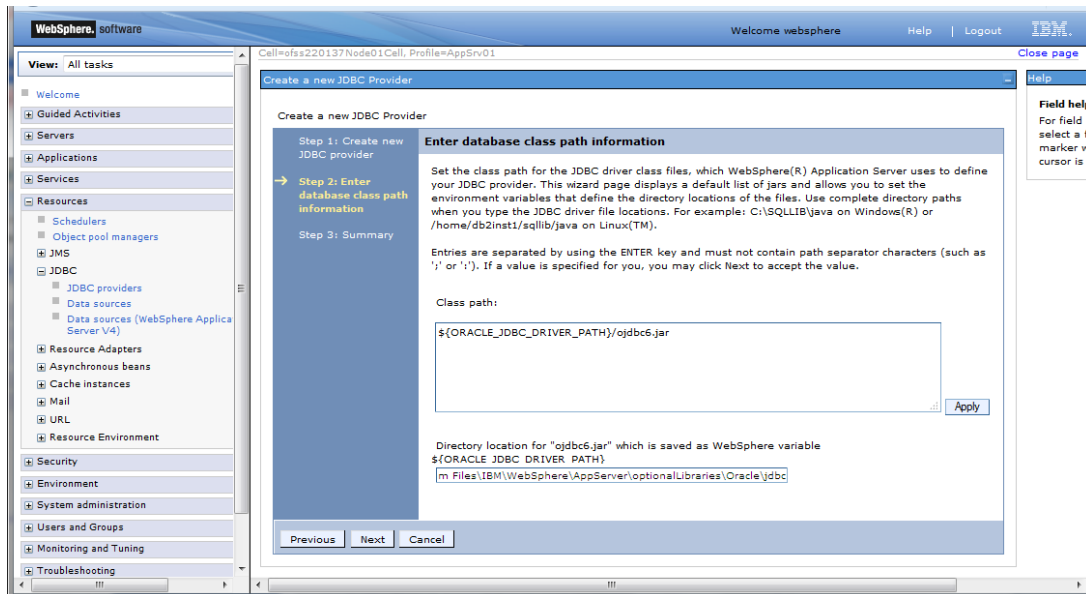
3. Select 'Node' from the drop-down list and click 'New' button. The following message is displayed.



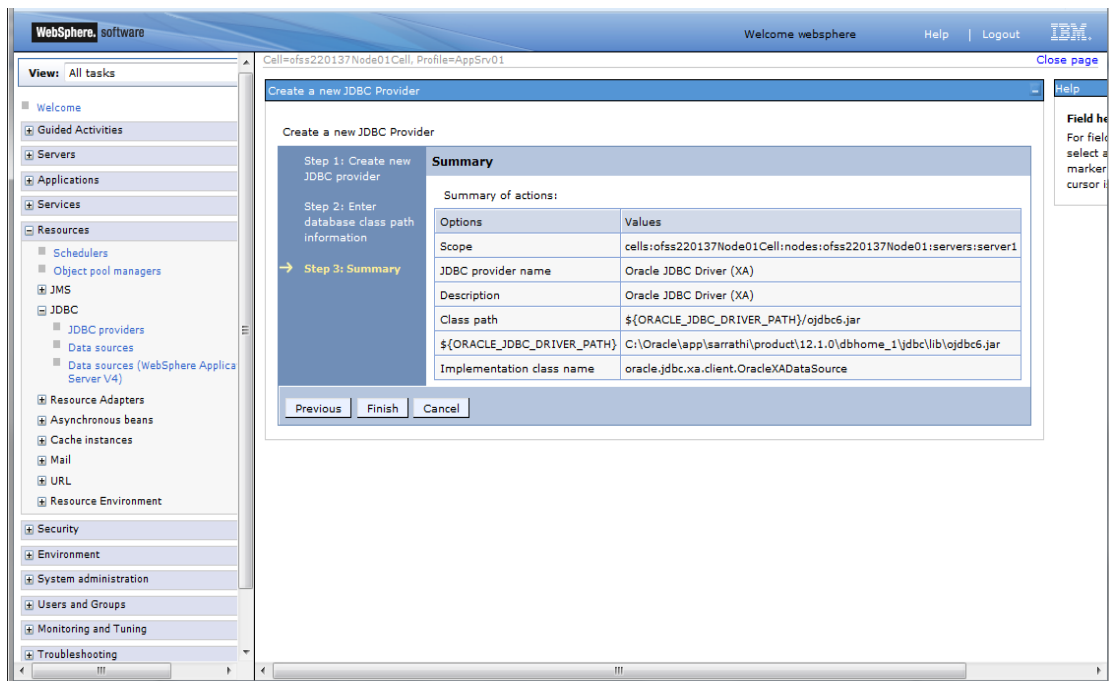
4. Specify the following details:

Database Type	Oracle
Provider Type	Oracle JDBC Driver
Implementation Type	XA data source
Name	FCIS Oracle JDBC Driver (XA)
Description	FCIS Oracle JDBC Driver (XA)

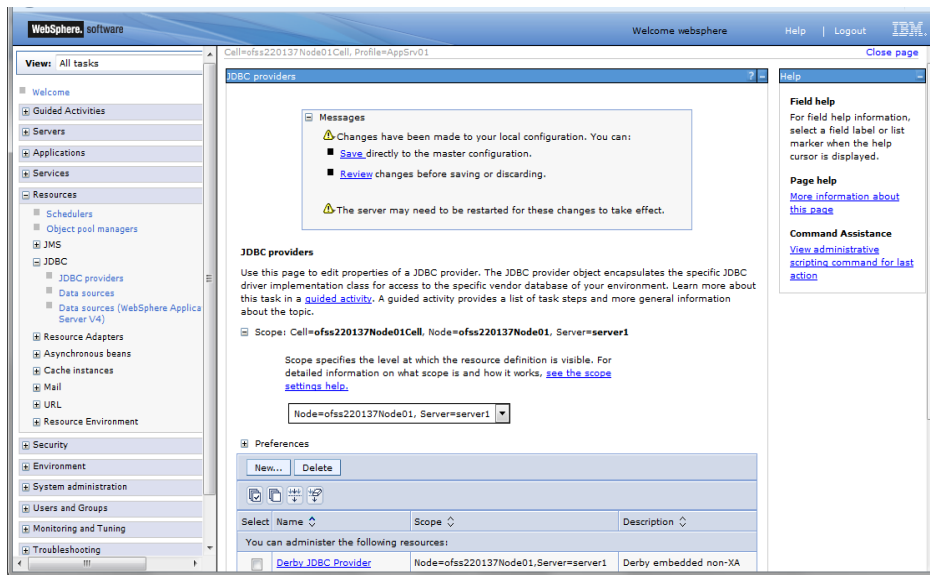
Click next, the following message is displayed.



5. Specify the location of ojdbc6.jar and click next. The following screen is displayed.



6. Click 'Finish'. The following screen is displayed.



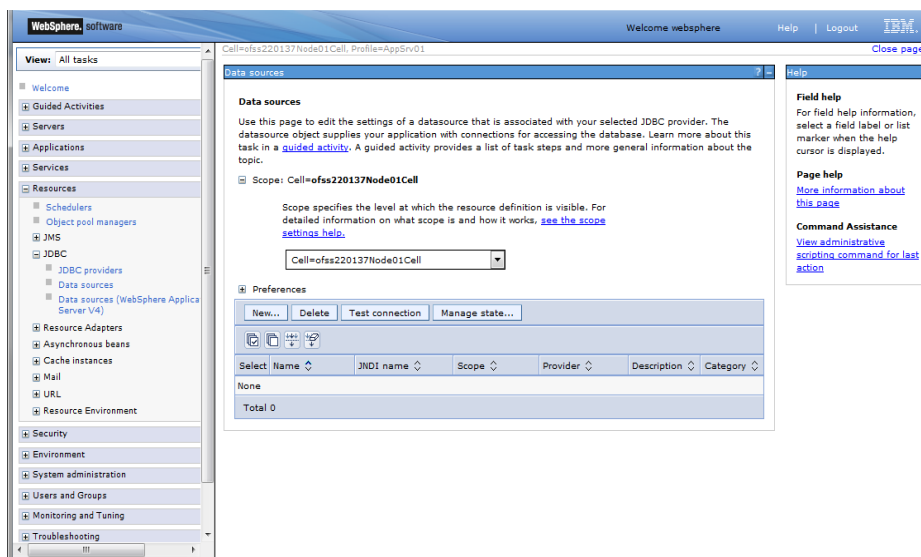
7. Click 'Save'.

3.3.7 Creating XA Data Source

Follow the steps given below:

1. Login to the application server administration console.
2. Expand 'Resources > JDBC' and click 'Data sources'.

The following screen is displayed.



3. Select 'Node' from the dropdown list and click 'New' button. The following screen is displayed.

WebSphere, software

Cell=cells220137Node01Cell, Profile=AppSrv01

Welcome websphere Help Logout IBM

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
 - Schedulers
 - Object pool managers
 - JMS
 - JDBC
 - JDBC providers
 - Data sources
 - Data sources (WebSphere Application Server V4)
 - Resource Adapters
 - Asynchronous beans
 - Cache instances
 - Mail
 - URL
 - Resource Environment
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting

Create a data source

Step 1: Enter basic data source information

Set the basic configuration values of a datasource for association with your JDBC provider. A datasource supplies the physical connections between the application server and the database.

Requirement: Use the Datasources (WebSphere(R) Application Server V4) console pages if your applications are based on the Enterprise JavaBeans(TM) (EJB) 1.0 specification or the Java(TM) Servlet 2.2 specification.

Scope

cells:ofss220137Node01Cell:nodes:ofss220137Node01:servers:server1

Data source name

FCIS DS

JNDI name

jdbc/fcjschedulerDS

Next Cancel

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

4. Specify the following details:

Data source name	FCIS Scheduler Data source
JNDI Name	jdbc/fcjschedulerDS

Click next, the following screen is displayed.

WebSphere, software

Cell=cells220137Node01Cell, Profile=AppSrv01

Welcome websphere Help Logout IBM

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
 - Schedulers
 - Object pool managers
 - JMS
 - JDBC
 - JDBC providers
 - Data sources
 - Data sources (WebSphere Application Server V4)
 - Resource Adapters
 - Asynchronous beans
 - Cache instances
 - Mail
 - URL
 - Resource Environment
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting

Create a data source

Step 2: Select JDBC provider

Specify a JDBC provider to support the datasource. If you choose to create a new JDBC provider, it will be created at the same scope as the datasource. If you are selecting an existing JDBC provider, only those providers at the current scope are available from the list.

Create new JDBC provider

Select an existing JDBC provider

Oracle JDBC Driver (XA)

Previous Next Cancel

Field help

For field help information, select a field label or list marker when the help cursor is displayed.

5. Select the option 'Select an existing JDBC provider' and choose 'FCIS Oracle JDBC Driver (XA)' from the drop-down list and click next. The following screen is displayed.

WebSphere software

Cell=ofss220075Node03Cell, Profile=FCIS121_1TR2

View: All tasks

Close page

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

→ Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

Step 5: Summary

Enter database specific properties for the data source

Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasourse.

Name	Value
URL	<code>jdbc:oracle:thin:@10.10.10.1</code>

Data store helper class name
Oracle11g data store helper

☐ Use this data source in container managed persistence (CMP)

Previous Next Cancel

Field help
This property corresponds to the database attribute, URL. Specifies the URL of the database from which the datasource obtains connections, such as `jdbc:oracle:thin:@//localhost:1521/sample` for thin driver and `jdbc:oracle:oci:@//localhost:1521/sample` for thick driver.

6. Specify the URL of the Database

Uncheck "Use this data source in container managed persistence (CMP)"

Example

`jdbc:oracle:thin:@10.10.10.10:1010:KERDEV2`

Here, *10.10.10.10* is the *hostname* where the database is installed, *1010* is the *port number*, *KERDEV2* is the *instance name*.

7. Select the 'Data store helper class' as 'Oracle11g data store helper'.
8. Click 'Next'. The following screen is displayed.

Select user alias from Authentication alias for XA Recovery, Component-managed authentication alias and Container-managed authentication alias dropdown.

The screenshot shows the 'Create a data source' wizard in WebSphere, specifically Step 4: Setup security aliases. The left sidebar contains a navigation tree with categories like Welcome, Guided Activities, Servers, Applications, Services, Resources, Security, Environment, System administration, Users and Groups, Monitoring and Tuning, Troubleshooting, Service integration, and UDDI. The main content area is titled 'Create a data source' and includes a progress bar with steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 3: Enter database specific properties for the data source, Step 4: Setup security aliases (current step), and Step 5: Summary. The 'Setup security aliases' section contains three dropdown menus: 'Authentication alias for XA recovery' (selected: ofss220075Node03/R2SMS), 'Component-managed authentication alias' (selected: ofss220075Node03/R2SMS), and 'Mapping-configuration alias' (selected: (none)). Below these is a 'Container-managed authentication alias' dropdown (selected: ofss220075Node03/R2SMS). A note states: 'Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost.' The links are 'Global J2C authentication alias' and 'Security domains'. At the bottom are 'Previous', 'Next', and 'Cancel' buttons. A 'Help' button is in the top right corner.

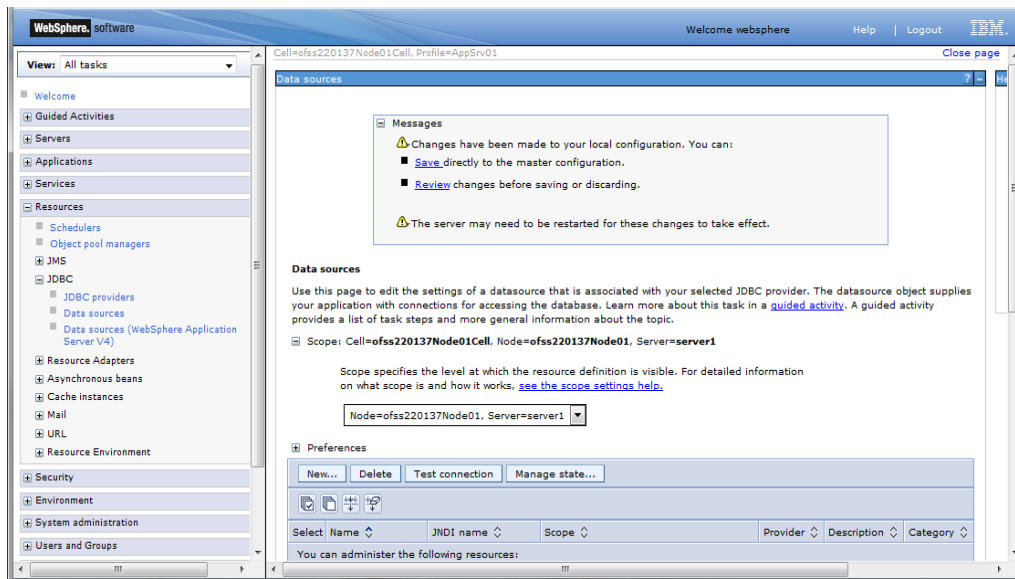
9. Click 'Next'.The following screen is displayed.

The screenshot shows the 'Create a data source' wizard in WebSphere, specifically Step 5: Summary. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Create a data source' and includes a progress bar with steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 3: Enter database specific properties for the data source, Step 4: Setup security aliases, and Step 5: Summary (current step). The 'Summary' section is titled 'Summary of actions:' and contains a table with the following data:

Options	Values
Scope	cells:ofss220137Node01Cell:nodes:ofss220137Node01:servers:server1
Data source name	FCUBS_DS
JNDI name	jdbc/fqSchedulerDS1
Select an existing JDBC provider	Oracle JDBC Driver (XA)
Implementation class name	oracle.jdbc.xa.client.OracleXADataSource
URL	jdbc:oracle:oci:@10.10.10.10:1010:KERDEV2
Data store helper class name	com.ibm.websphere.rsadapter.Oracle11gDataStoreHelper
Use this data source in container managed persistence (CMP)	true
Authentication alias for XA recovery	ofss220137Node01/FCUBS121_DEV

At the bottom are 'Previous', 'Next', and 'Cancel' buttons. A 'Help' button is in the top right corner.

Click finish, the following screen is displayed.

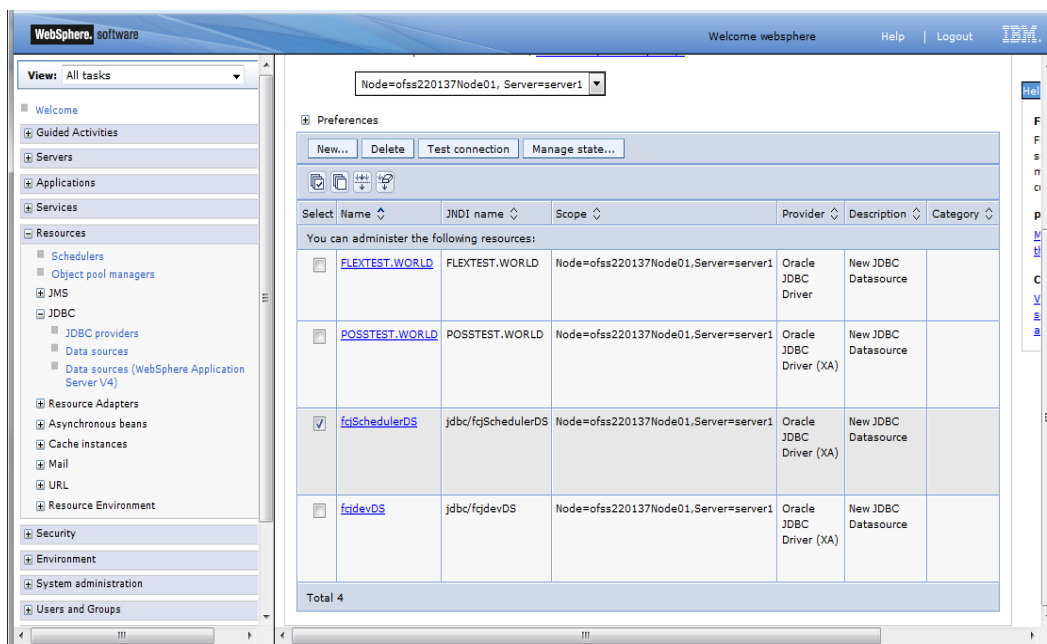


10. Click 'Save'.

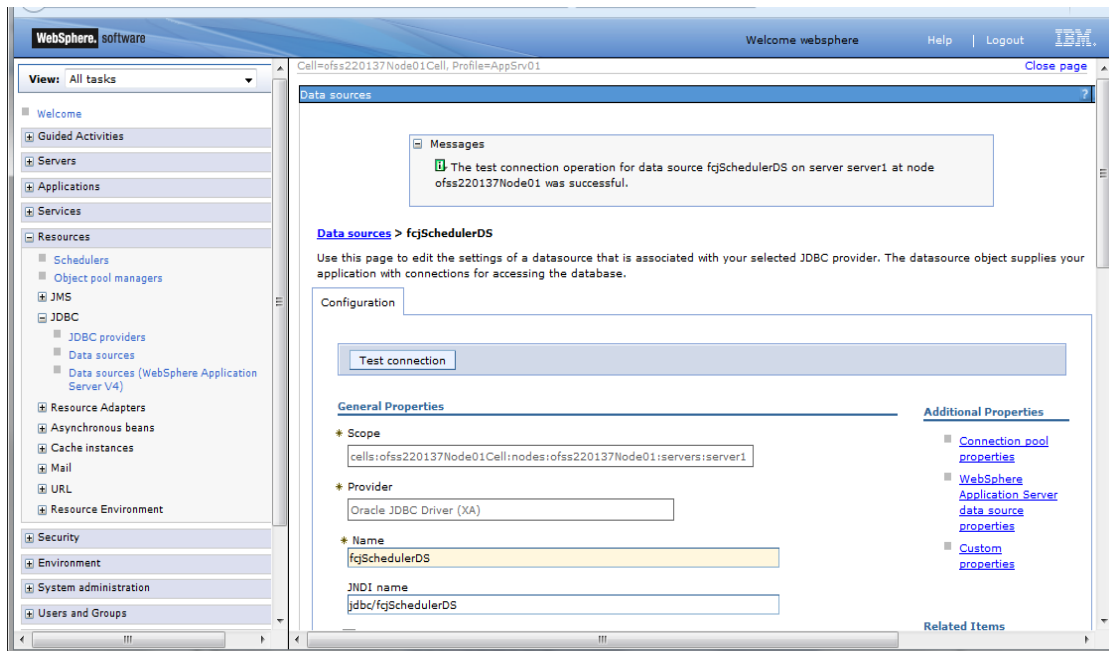
3.3.8 Testing Data Source

Follow the steps given below:

1. Select data source as given below.



2. Click 'Test connection' button. The following screen is displayed on successful creation.



3.4 Creating JMS Resources

3.4.1 Creating Queue Connection Factory

Follow the steps given below:

1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

`http://{Host}:{Port}/console`

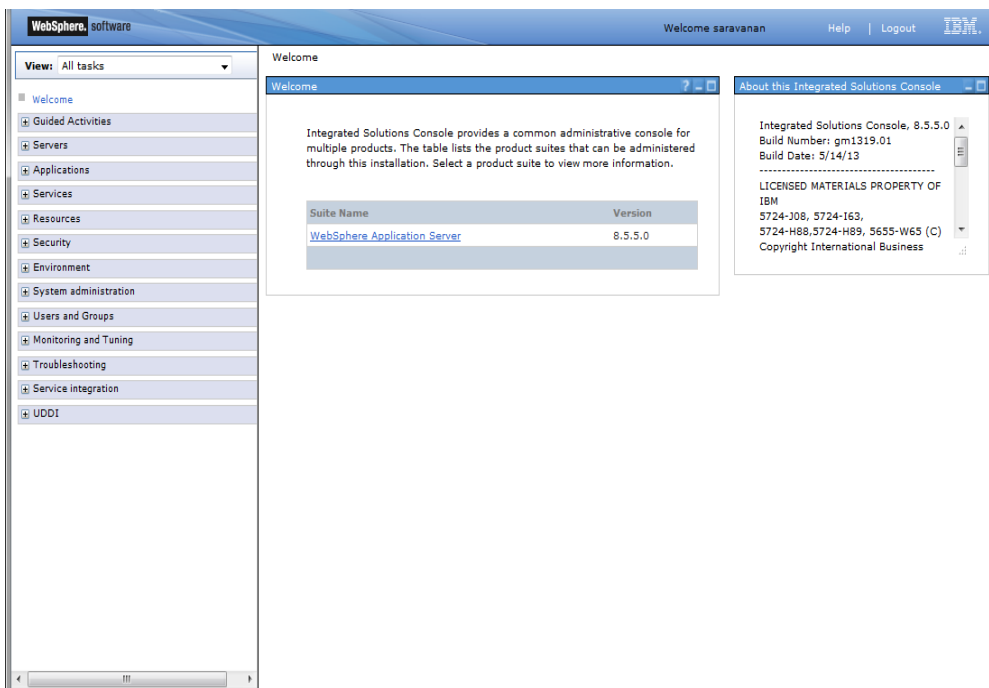
Eg: `https://10.10.10.10:1010/console`

In this example, 10.10.10.10 is the machine IP address on which Websphere is running.

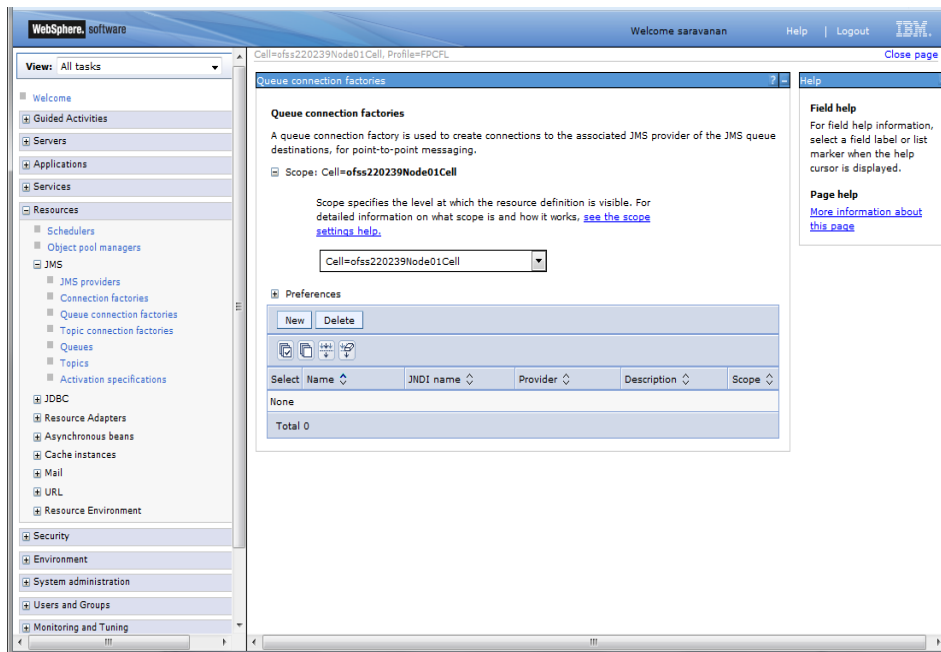
The following screen is displayed:



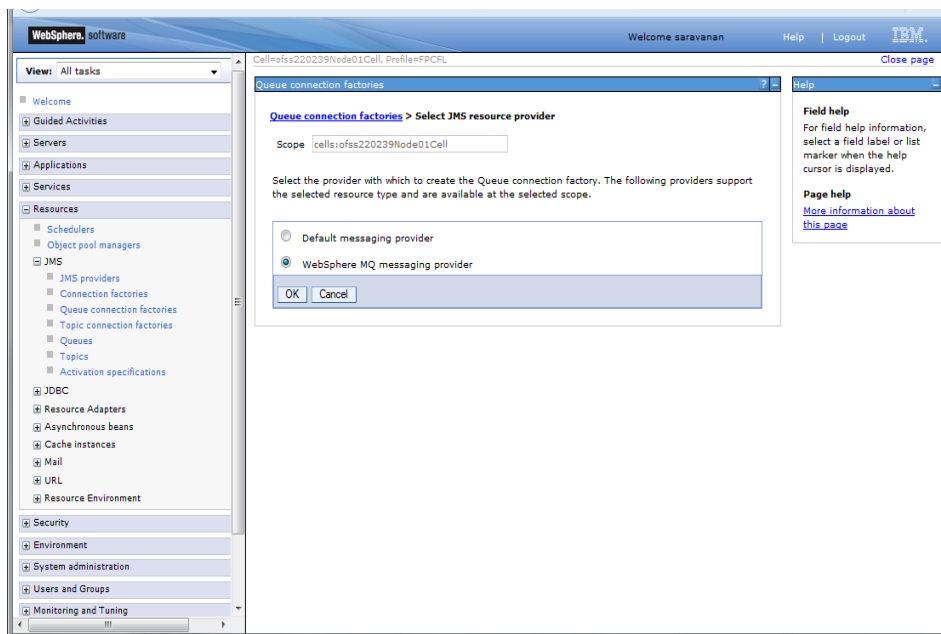
2. Specify the Websphere administrator username and password.
3. Click 'Log In'.
4. Navigate to Websphere home page.



5. Expand 'Resources' and select 'JMS'. Click 'Queue Connection Factories'. The following screen is displayed.



6. Select 'Node' from the drop down list and click 'New' button. The following screen is displayed.



7. Select 'WebSphere MQ messaging provider' and click 'OK'. The following screen is displayed.

The screenshot shows the 'Create WebSphere MQ JMS resource' wizard in the WebSphere software interface. The left sidebar contains a tree view with categories like Welcome, Guided Activities, Servers, Applications, Services, Resources, JMS, JDBC, Resource Adapters, Asynchronous beans, Cache instances, Mail, URL, Resource Environment, Security, Environment, System administration, Users and Groups, and Monitoring and Tuning. The main panel displays the wizard steps: Step 1: Configure basic attributes (selected), Step 2: Select connection method, Step 3: Test connection, and Step 4: Summary. The 'Configure basic attributes' section includes fields for Name (NotifyDestQCF), JNDI name (NotifyDestQCF), and Description (NotifyDestQCF). A 'Field help' box on the right explains that for field help information, a field label or list marker should be selected when the help cursor is displayed. 'Next' and 'Cancel' buttons are at the bottom.

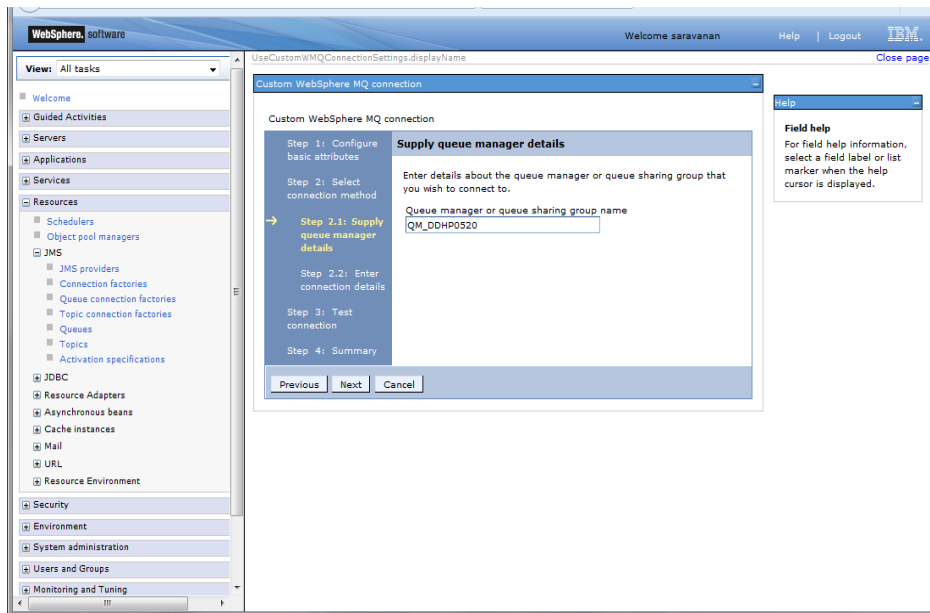
8. Specify the following details:

Name	NotifyDestQCF
JNDI Name	NotifyDestQCF
Description	NotifyDestQCF

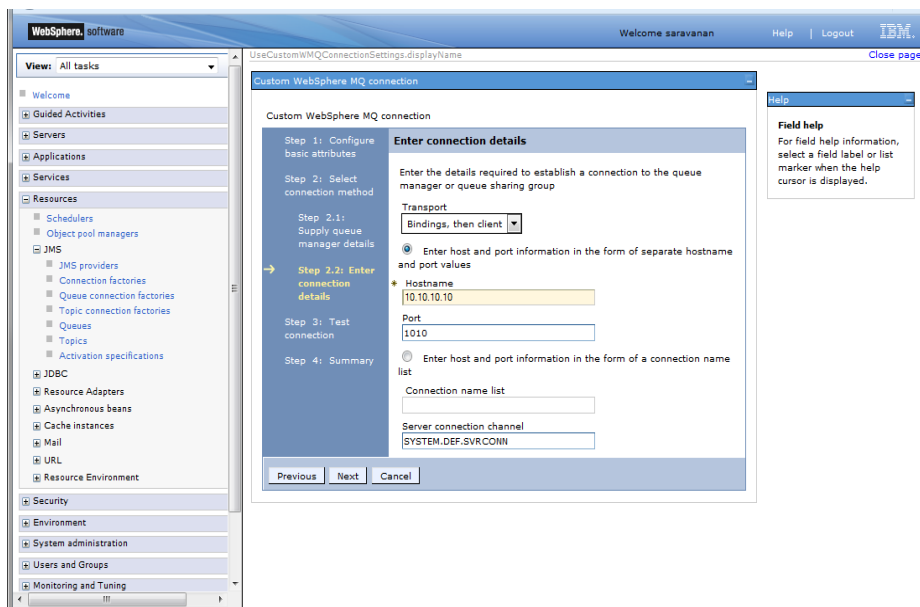
Click 'Next'. The following screen is displayed.

The screenshot shows the 'Create WebSphere MQ JMS resource' wizard in the WebSphere software interface, now at Step 2: Select connection method. The left sidebar is the same as in the previous screenshot. The main panel shows the wizard steps: Step 1: Configure basic attributes, Step 2: Select connection method (selected), Step 3: Test connection, and Step 4: Summary. The 'Select connection method' section includes a text box with the instruction 'Decide what information to enter to determine how to connect to WebSphere MQ' and two radio buttons: 'Enter all the required information into this wizard' (selected) and 'Use a client channel definition table'. 'Previous', 'Next', and 'Cancel' buttons are at the bottom. A 'Field help' box on the right is also present.

9. Set the options as shown in the figure. Click 'Next'. The following screen is displayed.



10. Specify the queue manager name 'QM_DDHP0520'. Click 'Next'.

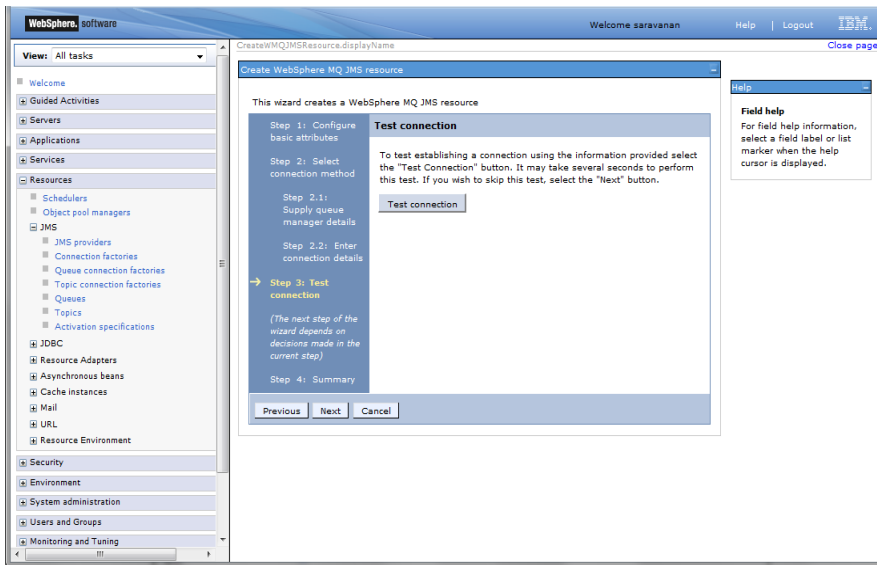


11. Specify the following details:

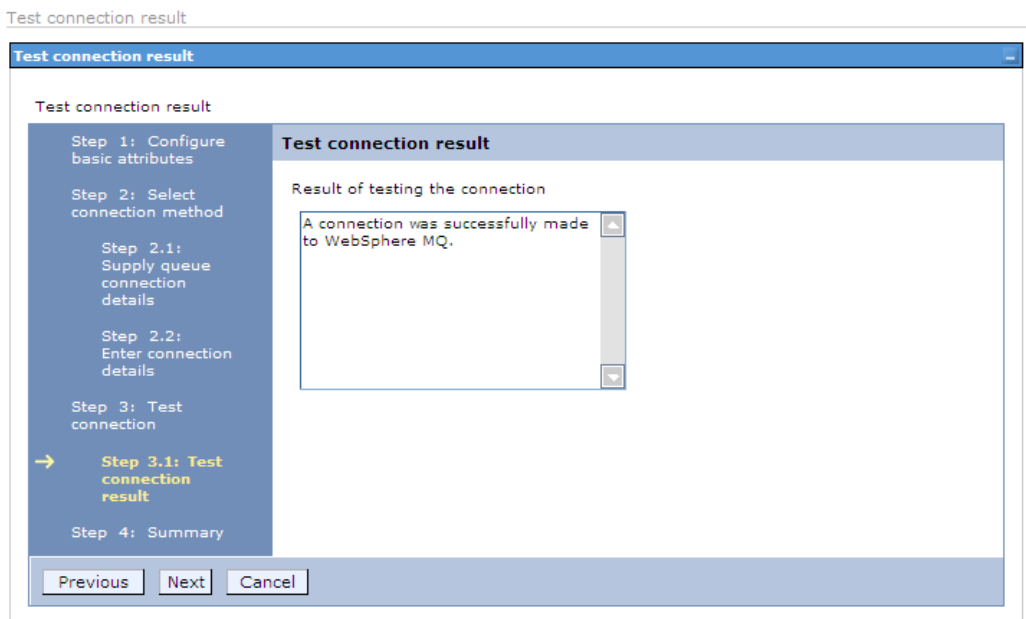
Host Name	10.10.10.10 (Host where Websphere MQ is installed)
Port	1010 (Web sphere MQ port)
Server Connection Channel	SYSTEM.DEF.SVRCONN

12.

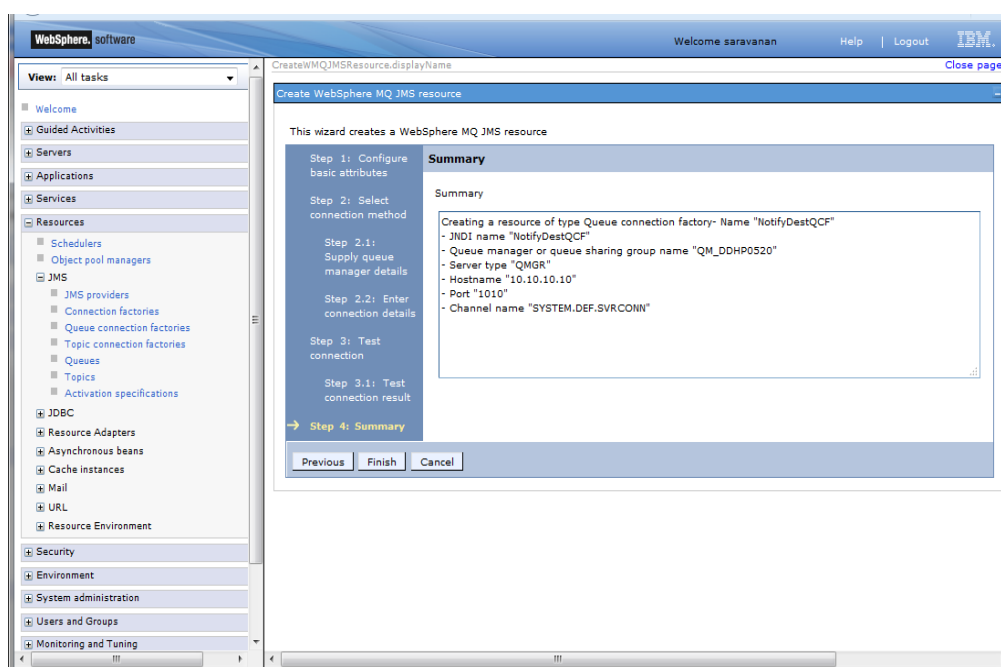
13. Click 'OK'. The following screen is displayed.



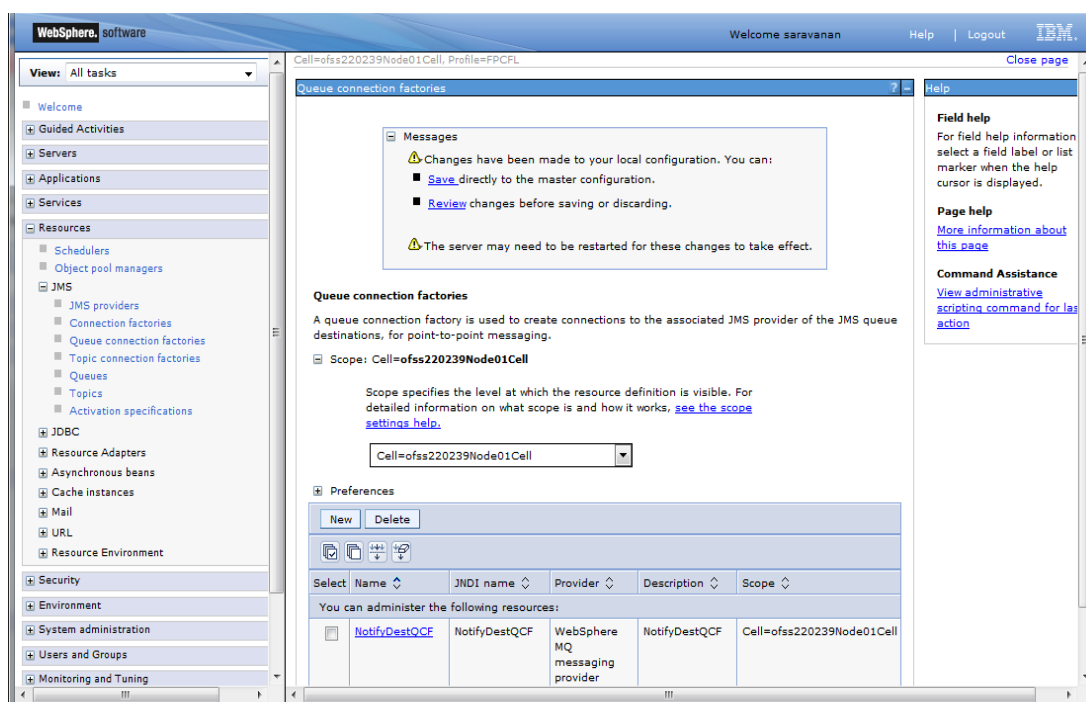
14. Click 'Test Connection' button. The following screen is displayed:



15. Click 'Next'. The following screen is displayed with a message in the summary field.



16. Click 'Finish'. The following screen is displayed.



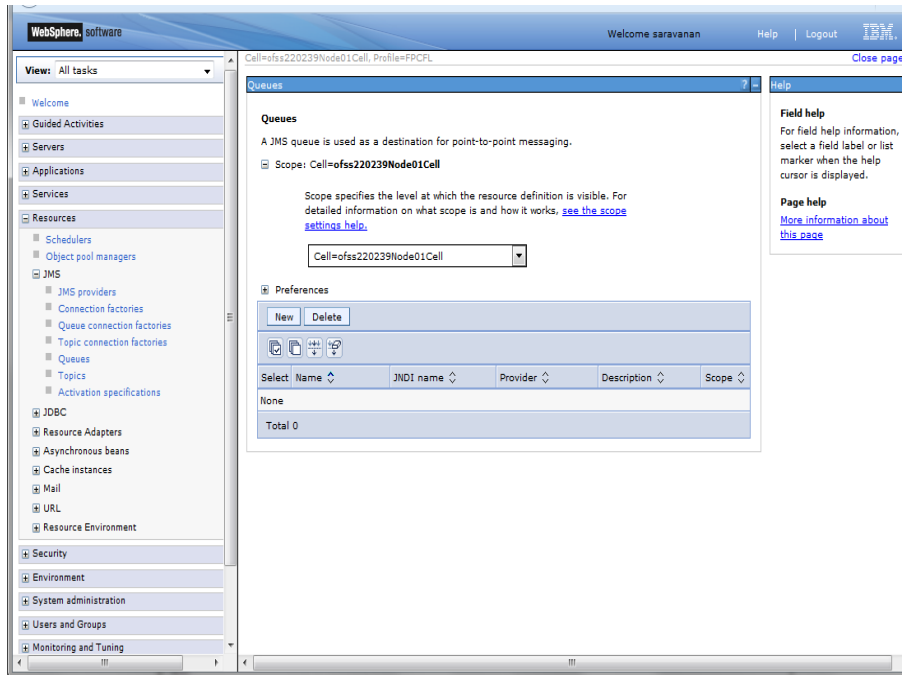
17. Click 'Save'.

18. Similarly, you need to create the all queue connection factories mentioned in the document "Resource To be Created"

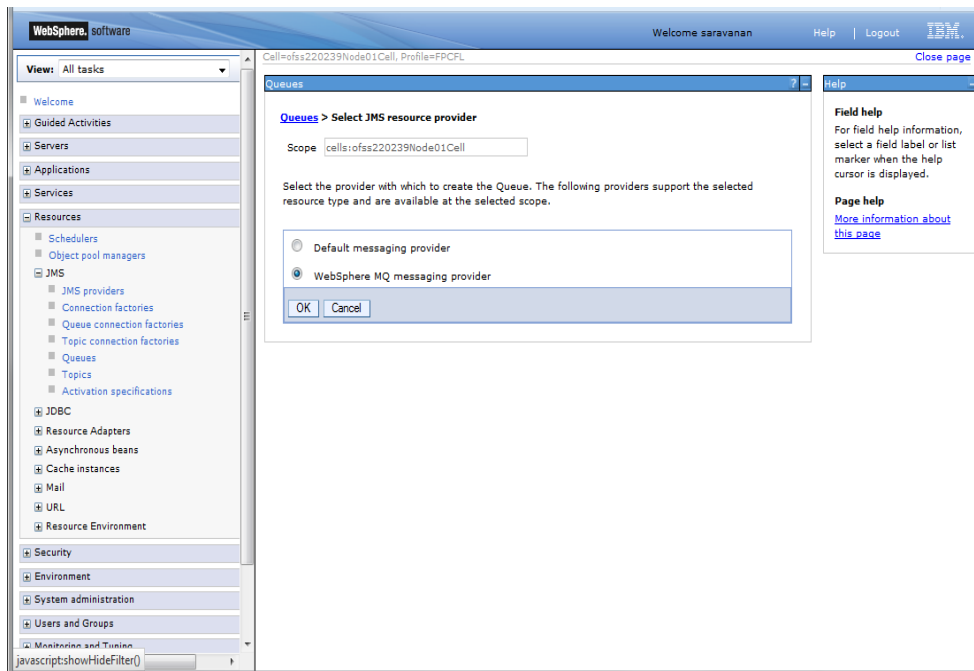
3.4.2 Creating Queues

Follow the steps given below:

1. Expand 'Resources > JMS' and click Queues.



2. Select 'Node' from the drop down list. Click 'New'. The following screen is displayed:



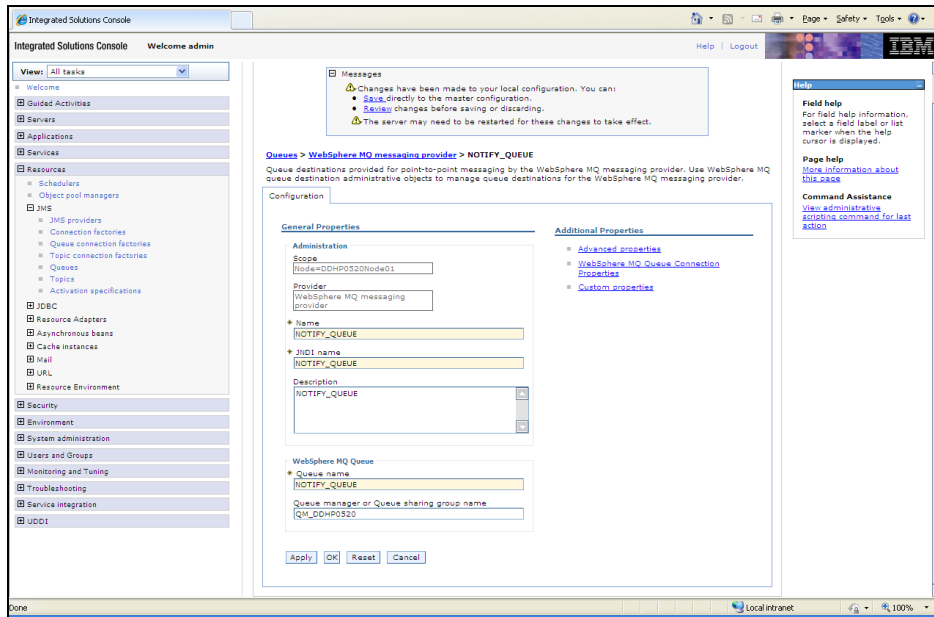
3. Select 'Websphere MQ messaging provider'. Click 'OK'. The following screen is displayed.

The screenshot shows the 'General Properties' dialog box in the WebSphere MQ Administration console. The left pane shows the navigation tree with 'Resources' expanded and 'JMS providers' selected. The main pane displays the configuration for a 'WebSphere MQ messaging provider'. The 'Administration' section contains fields for Scope, Provider, Name, JNDI name, and Description. The 'WebSphere MQ Queue' section contains fields for Queue name and Queue manager or Queue sharing group name. The 'OK' button is highlighted.

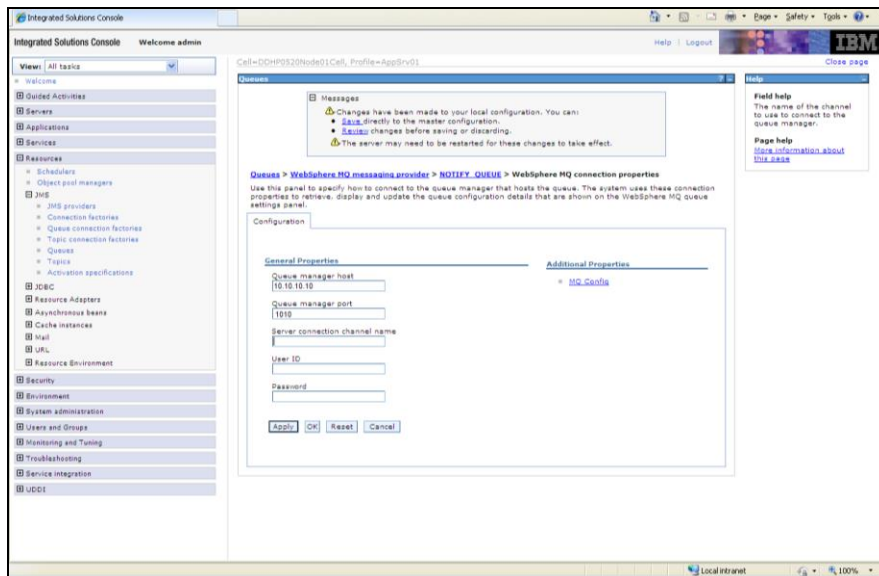
Specify the following details:

Name	NOTIFY_QUEUE
JNDI Name	NOTIFY_QUEUE
Description	NOTIFY_QUEUE
Queue Name	NOTIFY_QUEUE on Websphere MQ to which the queue needs to be mapped
Queue Manager or Queue sharing group name	QM_DDHP0520

4. Click 'Apply'. The following screen is displayed.



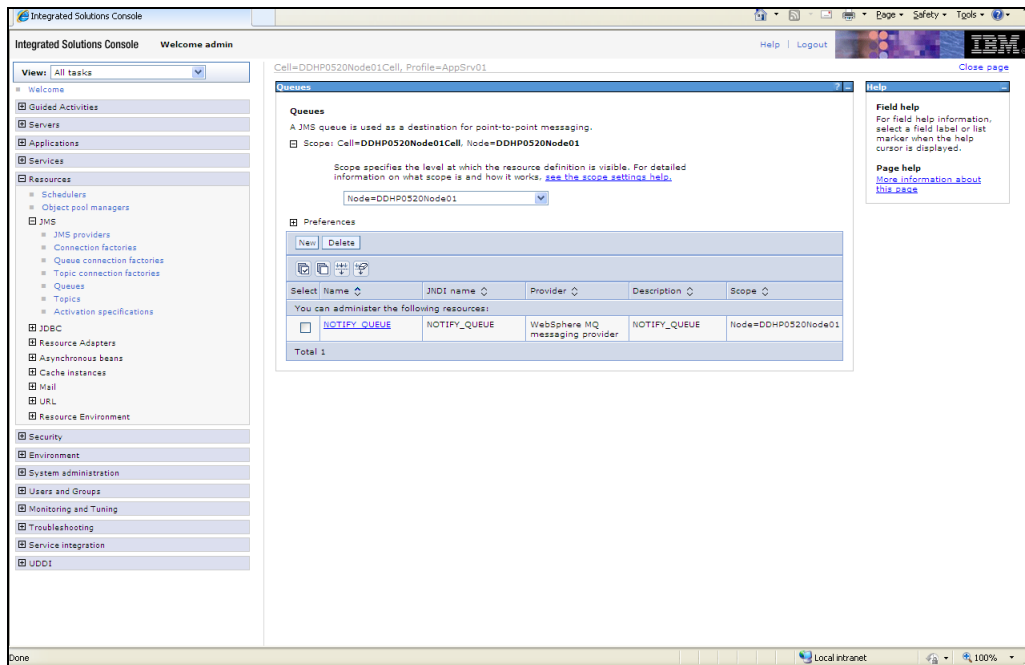
5. Click 'WebSphere MQ Queue Connection Properties'. The following screen is displayed.



6. Specify the following details:

Queue manager host	10.10.10.10 (IP address of the MQ server)
Queue manger port	1010
Server Connection Channel	SYSTEM.DEF.SVRCONN

7. Click 'Save'. The following screen is displayed.



8. Similarly, you need to create all the queues mentioned in the document "Resource To be Created".

3.5 Creating Message Listener

Follow the steps given below:

1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

`http://{Host}:{Port}/console`

Eg: `https://10.10.10.10:1010/console`

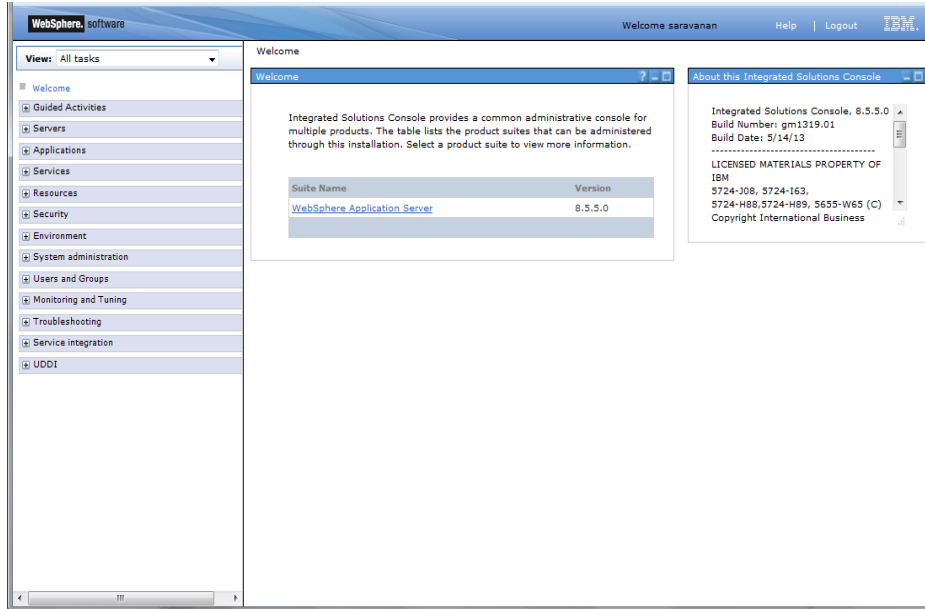
In this example, 10.10.10.10 is the machine IP address on which Websphere is running.

The following screen is displayed:

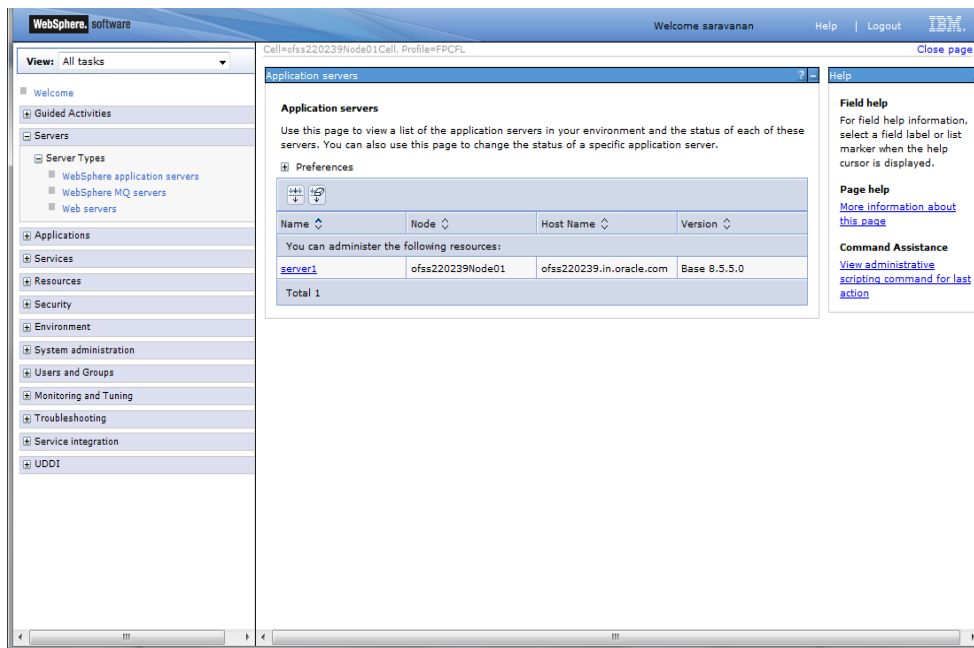


2. Specify the Websphere administrator username and password.
3. Click 'Log In'.

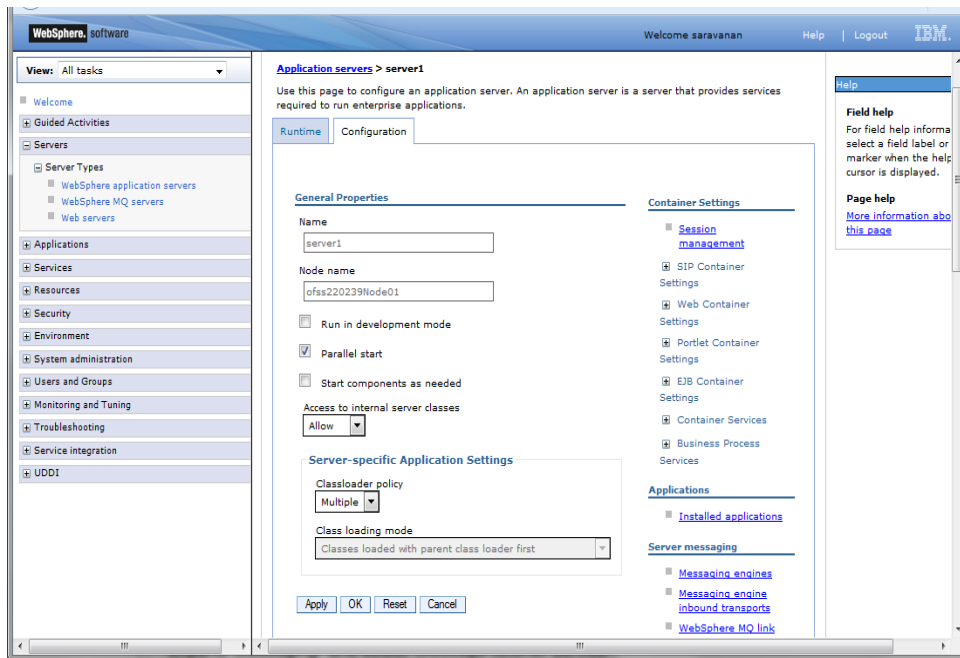
4. Navigate to Websphere home page.



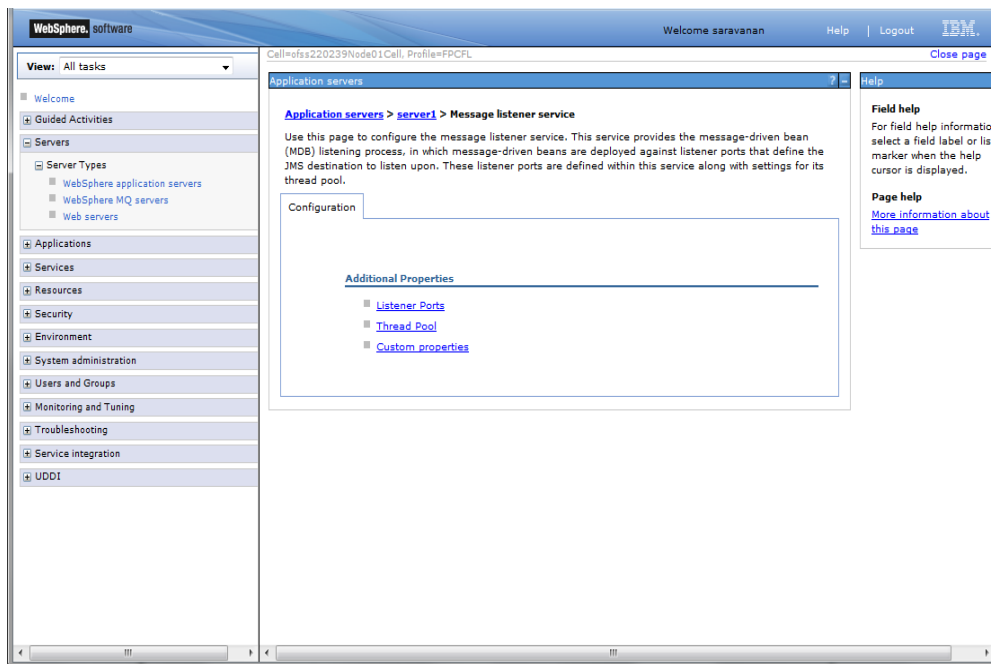
5. Expand 'Servers > Server Types' and click 'Websphere application servers'. The following screen is displayed.



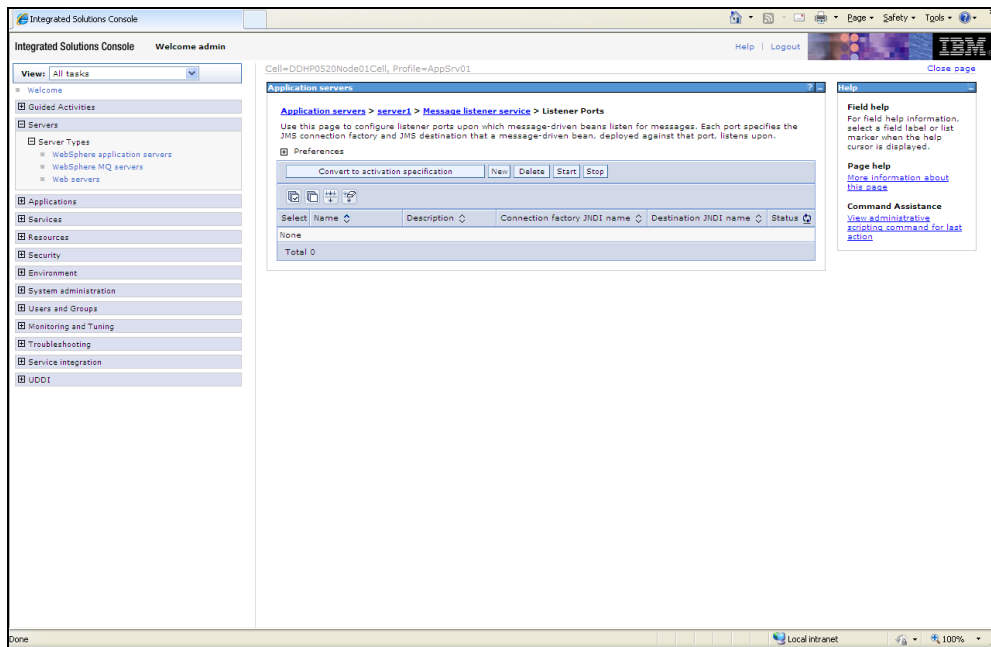
6. Click 'server1'. The following screen is displayed.



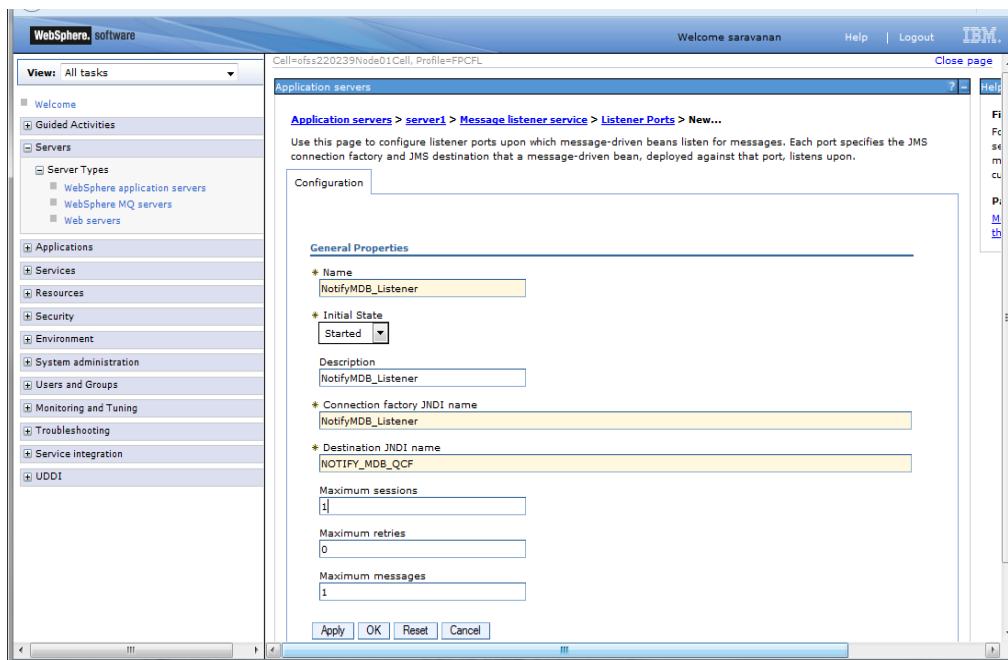
7. Expand 'Messaging' and select 'Message listener service'. The following screen is displayed.



8. Click 'Listener Ports'. The following screen is displayed.



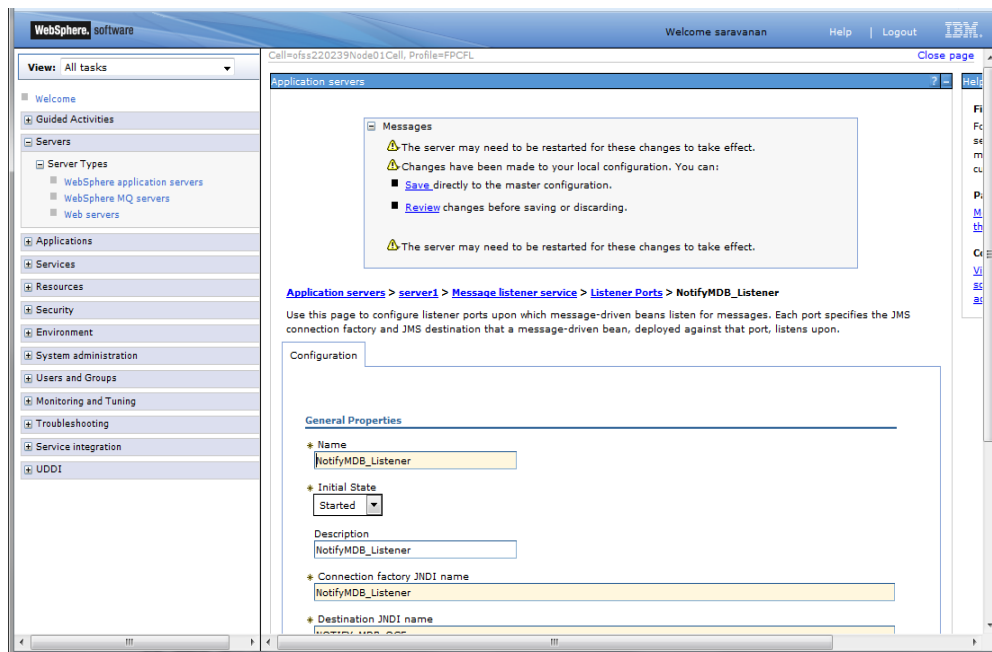
9. Click 'New'. The following screen is displayed.



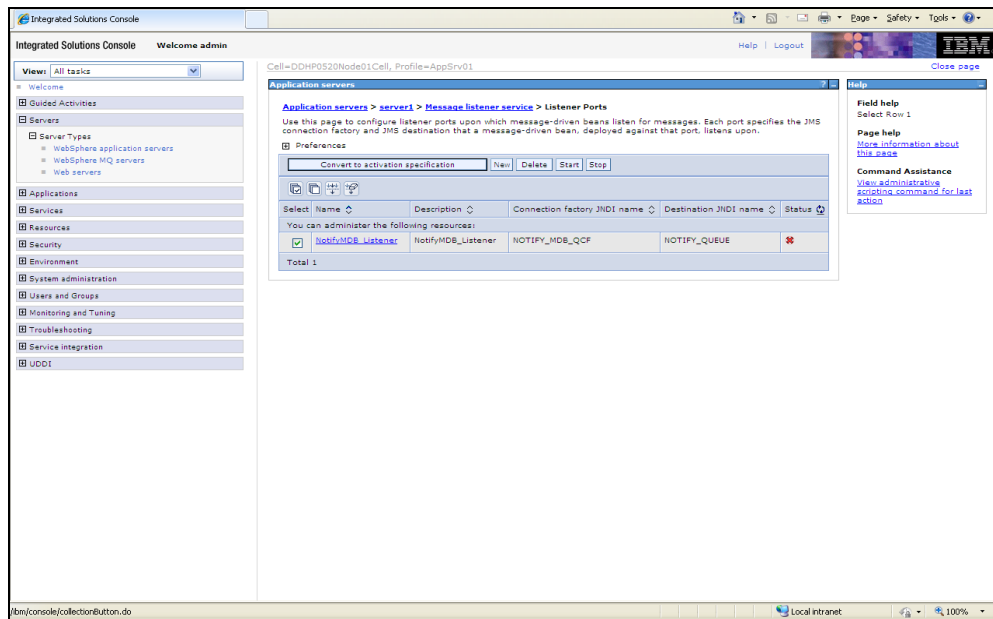
10. Specify the following details:

Name	NotifyMDB_Listener
Description	NotifyMDB_Listener
Connection factory JNDI name	NOTIFY_MDB_QCF
Destination JNDI name	NOTIFY_QUEUE
Maximum retries	1

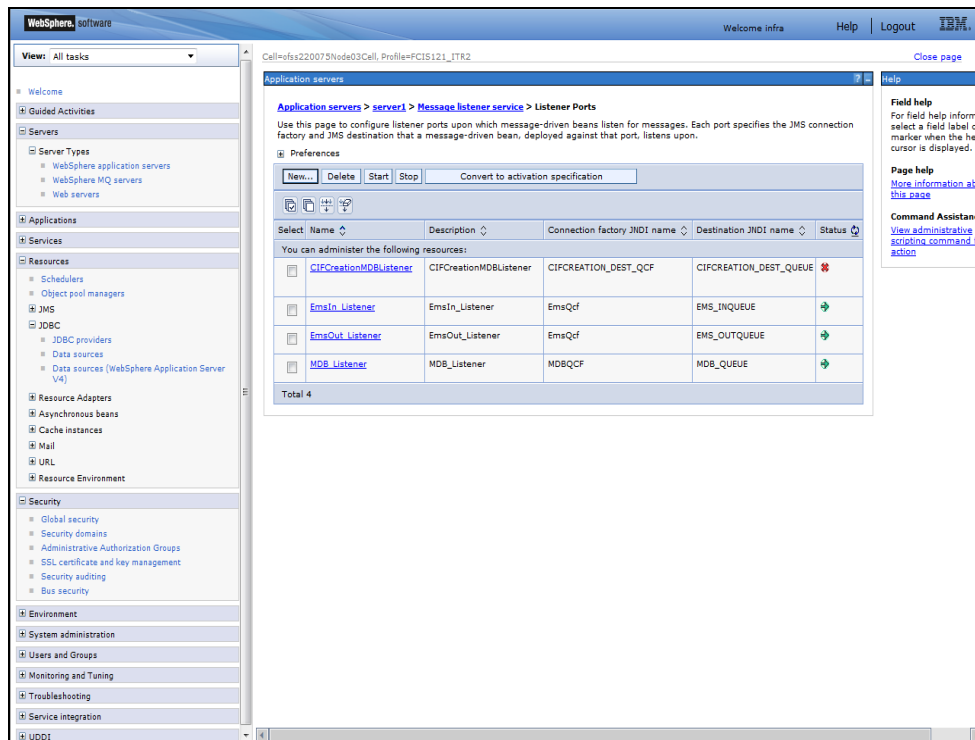
11. Click 'Apply'. The following screen is displayed.



12. Click 'Save'. The following screen is displayed.



13. Select 'NotifyMDB_Listener'. Click 'Start'. The following screen is displayed.



14. Similarly, you need to create the following listeners:

MDB_Listener
CIFCreationMDBListener
EmsIn_Listener
EmsOut_Listener

The complete list of listener queue and QCF to be created for Websphere is given below.

Application Name	Listener Name	Listener QCF	Listener QUEUE
<i>GWMDB</i>	<i>MDB_Listener</i>	<i>MDBQCF</i>	<i>MDB_QUEUE</i>
<i>EMSInMDB</i>	<i>EmsIn_Listener</i>	<i>EmsQcf</i>	<i>EMS_INQUEUE</i>
<i>EMSOOutMDB</i>	<i>EmsOut_Listener</i>	<i>EmsQcf</i>	<i>EMS_OUTQUEUE</i>
CIFCreationMDBListenerBean	<i>CIFCreationMDBListener</i>	<i>CIFCREATION_DEST_QCF</i>	<i>CIFCREATION_DEST_QUEUE</i>

Here,

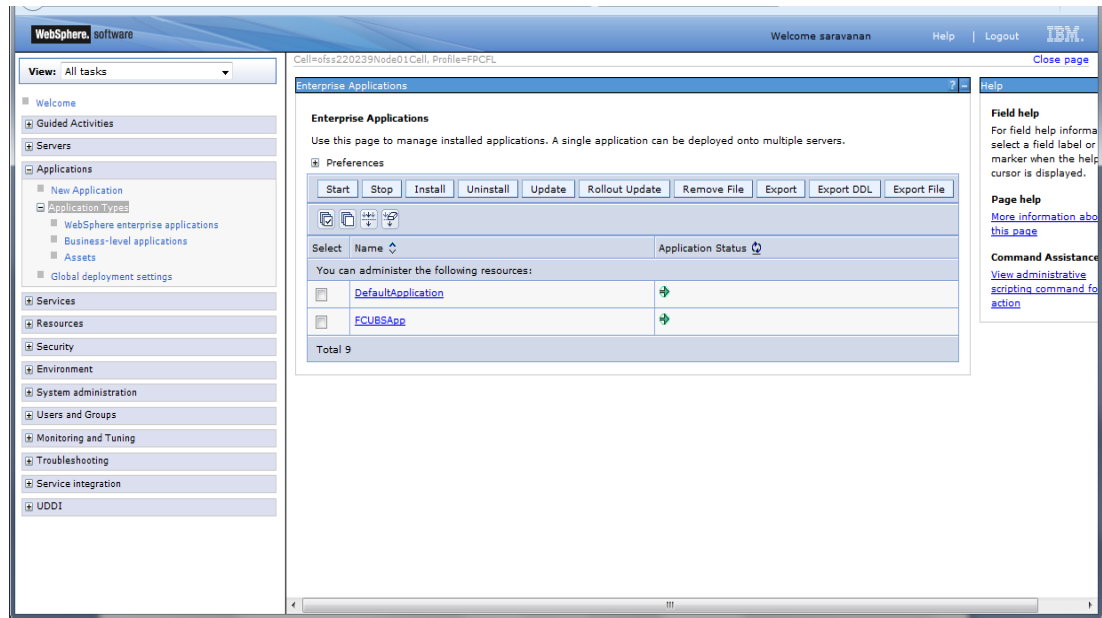
- MDB_Listener is mandatory for Gateway MDB applications
- All others are required for FCJ Applications embedded with Scheduler.

4. Default Settings for Web Sphere

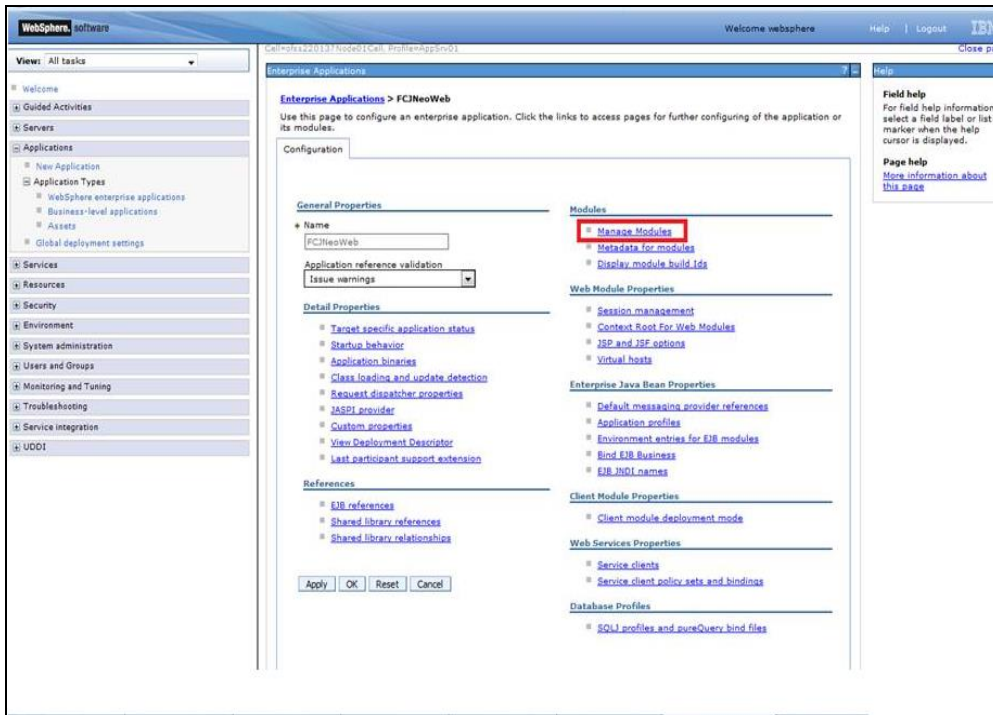
4.1 Standalone Scheduler Configuration

If standalone scheduler is enabled then below configuration should be done

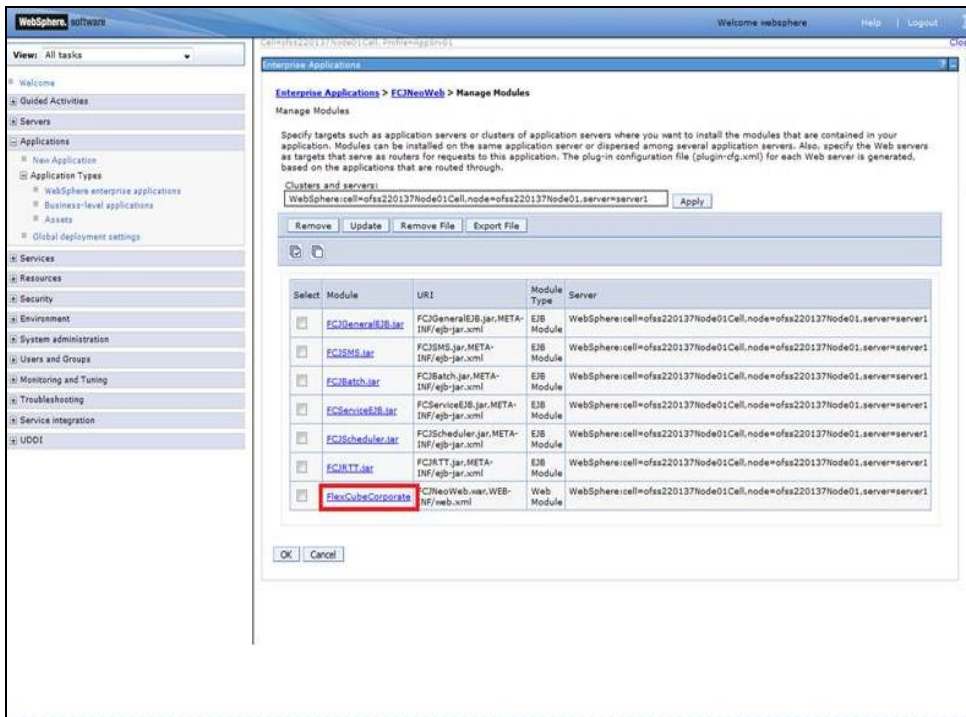
1. Login to websphere admin console. Expand 'Application > Application Types> WebSphere enterprise applications'. The following screen is displayed:



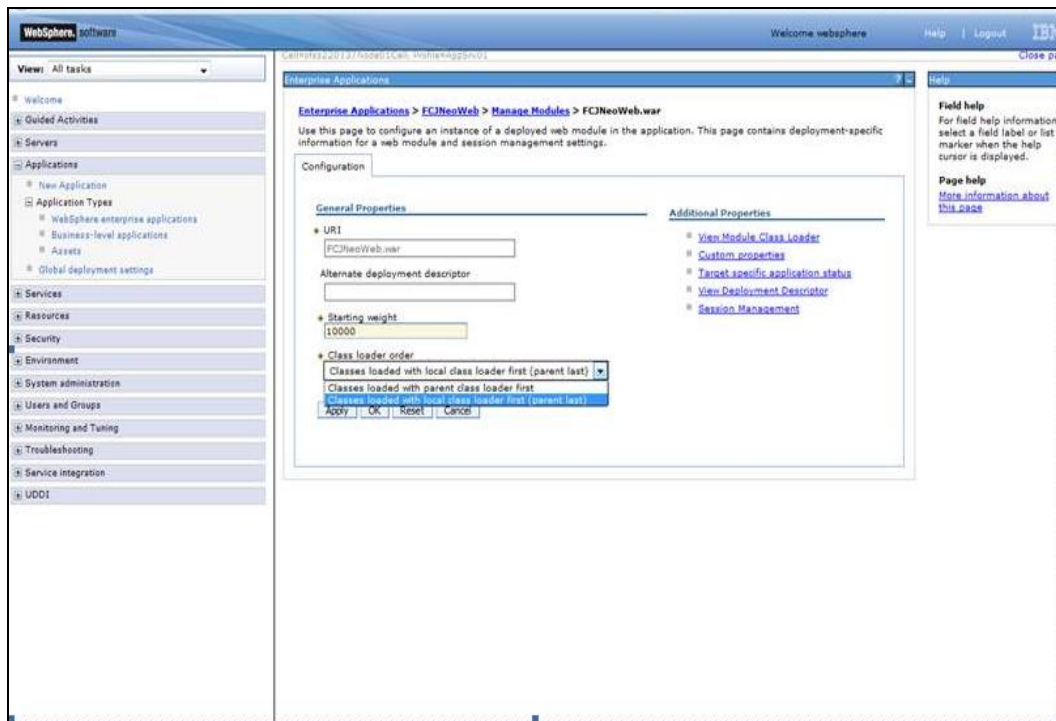
Click on the application 'FCISApp' below screen is displayed.



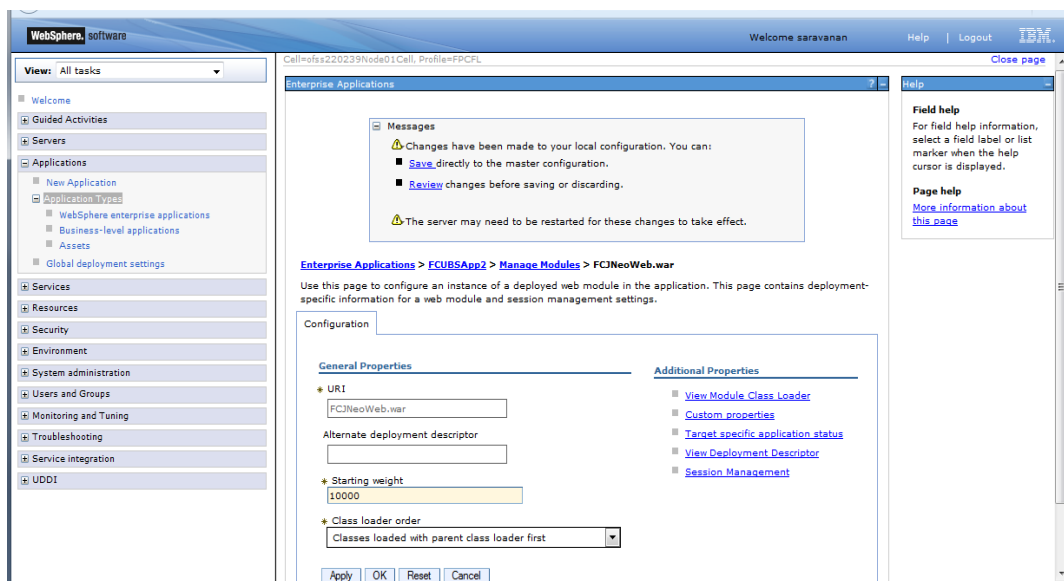
Click on 'Manage Modules'



Click on 'FlexCubeCorporate'



Select "Classes loaded with local class loader first (parent last)" from the dropdown 'Class loader order'. Click 'Apply' button



Click 'Save' link and restart the server.

5. Configuring Mail Session on Websphere

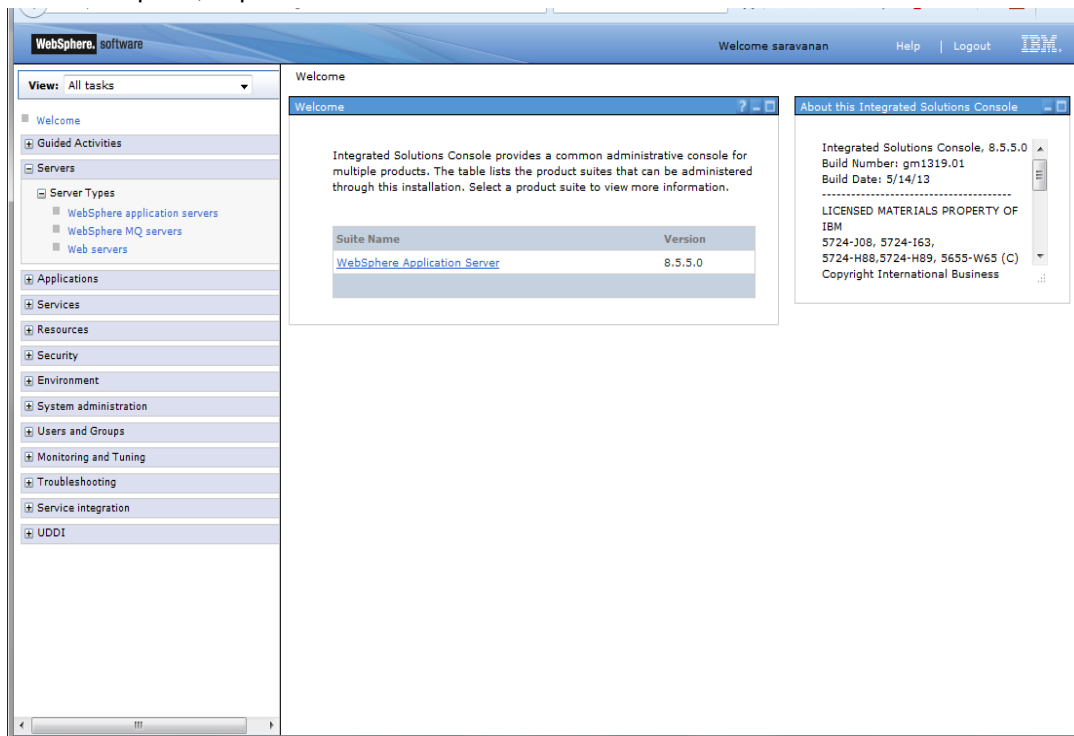
5.1 Introduction

This section describes the method to configure Websphere application server for Oracle FLEXCUBE IS to generate and send passwords to the users via e-mail.

5.2 Creating Java Mail Session

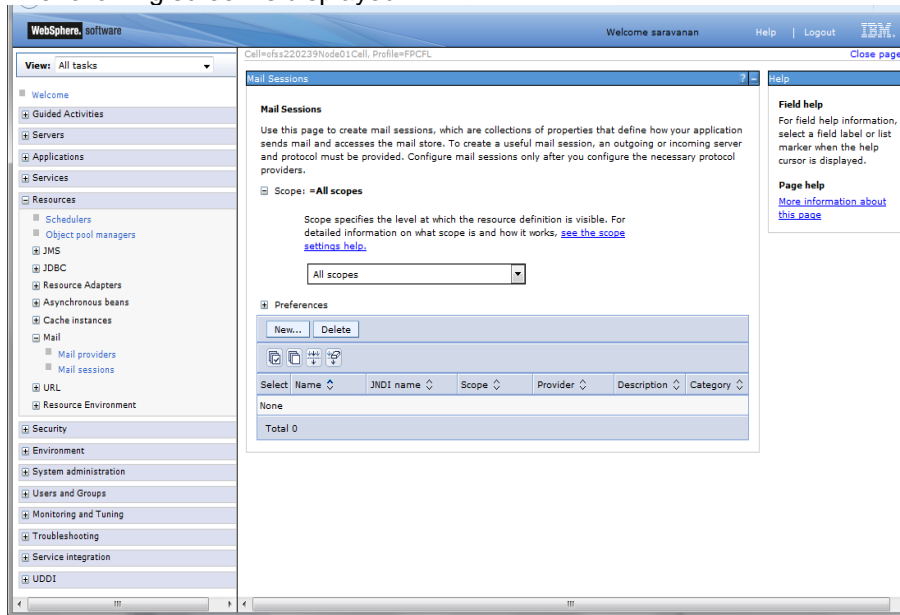
To create Java mail session, follow the steps given below:

1. On the left pane, expand 'Resources' and select 'Mail'.

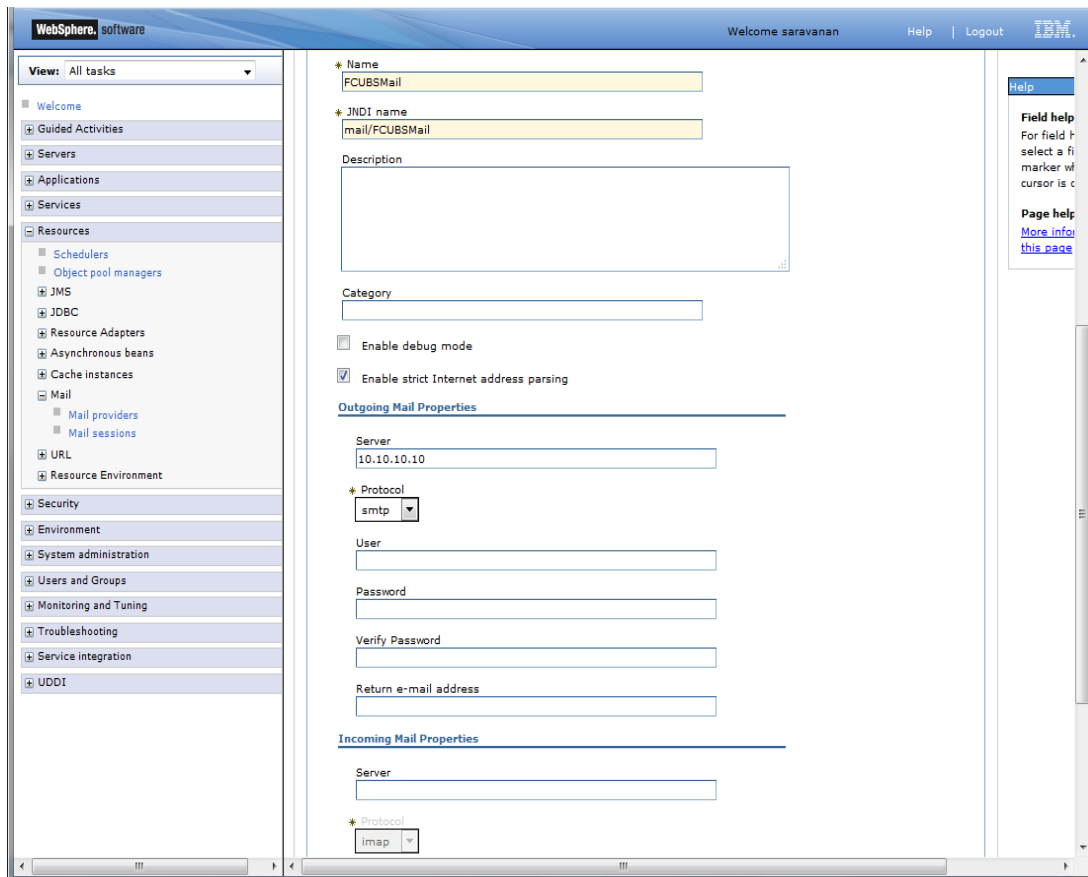


2. Click 'Mail Sessions' to invoke the 'Mail sessions' screen.

The following screen is displayed:



3. Click 'New' button to create a new mail session. The following screen is displayed:



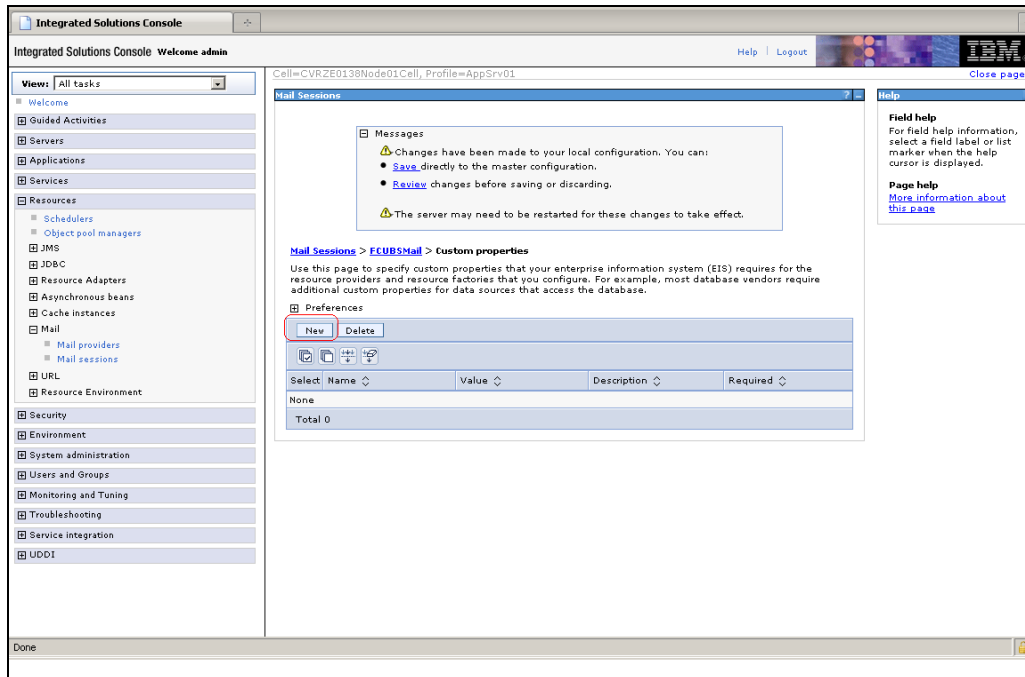
4. Provide the required information. Sample details are given below for your reference.

General Properties	
Name	FCUBSMail
JNDI Name	mail/FCUBSMail
N.B	This has to be maintained in the file 'fcubs.properties' in encrypted format
Outgoing Mail Properties	
Server	< HOST_MAIL_SERVER >
Protocol	smtps

5. Click 'Custom Properties' link to configure the custom properties.

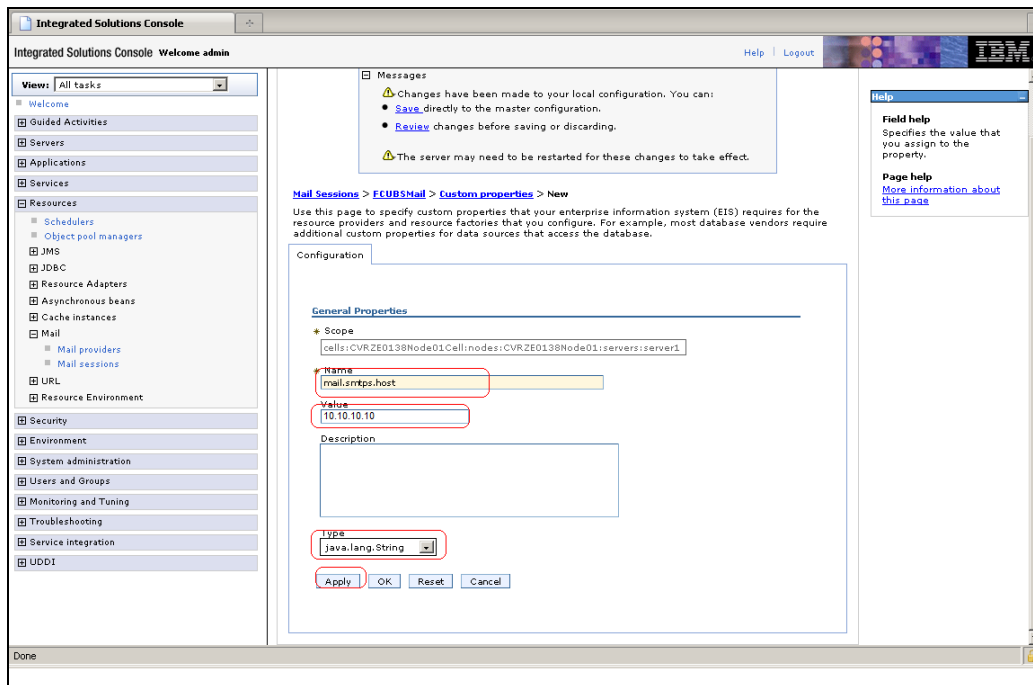
The screenshot shows the 'Integrated Solutions Console' interface. On the left is a navigation tree with categories like 'Welcome', 'Guided Activities', 'Servers', 'Applications', 'Services', 'Resources', 'Security', 'Environment', 'System administration', 'Users and Groups', 'Monitoring and Tuning', 'Troubleshooting', 'Service integration', and 'UDDI'. The main content area is titled 'Configuration' and contains two tabs: 'General Properties' and 'Additional Properties'. The 'General Properties' tab is active, showing fields for 'Scope' (cells:CVRZE0138Node01Cell:nodes:CVRZE0138Node01:servers:server1), 'Provider' (Built-in Mail Provider), 'Name' (FCUBSMail), 'JNDI name' (mail/FCUBSMail), and 'Description'. The 'Additional Properties' tab is also visible, showing a 'Custom properties' link. Below these tabs are checkboxes for 'Enable debug mode' and 'Enable strict Internet address parsing'. The 'Outgoing Mail Properties' section is also visible, showing fields for 'Server' (10.10.10.10), 'Protocol' (smtps), and 'User'. A 'Done' button is at the bottom left.

The following screen is displayed.



6. Click 'New' button to create new custom properties.

The following screen is displayed.

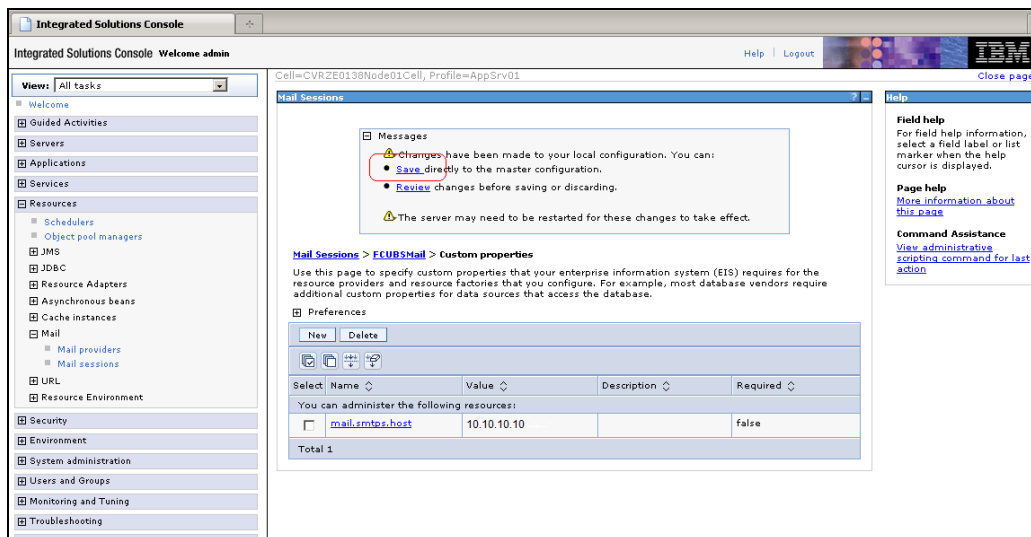


7. Specify the information required for creating custom properties. Sample details are given below:

Name	mail.smtps.host
Value	<HOST_SMTPS_MAIL_SERVER>
Type	java.lang.String

The custom properties are given below:

Name	Value	Type
mail.smtp.host	<HOST_SMTPS_MAIL_SERVER>	java.lang.String
mail.smtp.port	<SMTPS_SERVER_PORT>	java.lang.String
mail.host	<HOST_MAIL_SERVER>	java.lang.String
mail.smtps.auth	TRUE	java.lang.String



Click 'Save' to complete the configuration.



The file 'fcubs.properties' needs to be updated with the encrypted values of the following components

- SMTP_HOST
- SMTP_USER
- SMTP_PASSWORD
- SMTP_JNDI

You can update this using Oracle FLEXCUBE Investor Servicing Installer.

6. Annexure

Ensure the following settings before deploying the application:

6.1 IBM Websphere Server - Increasing Heap Size

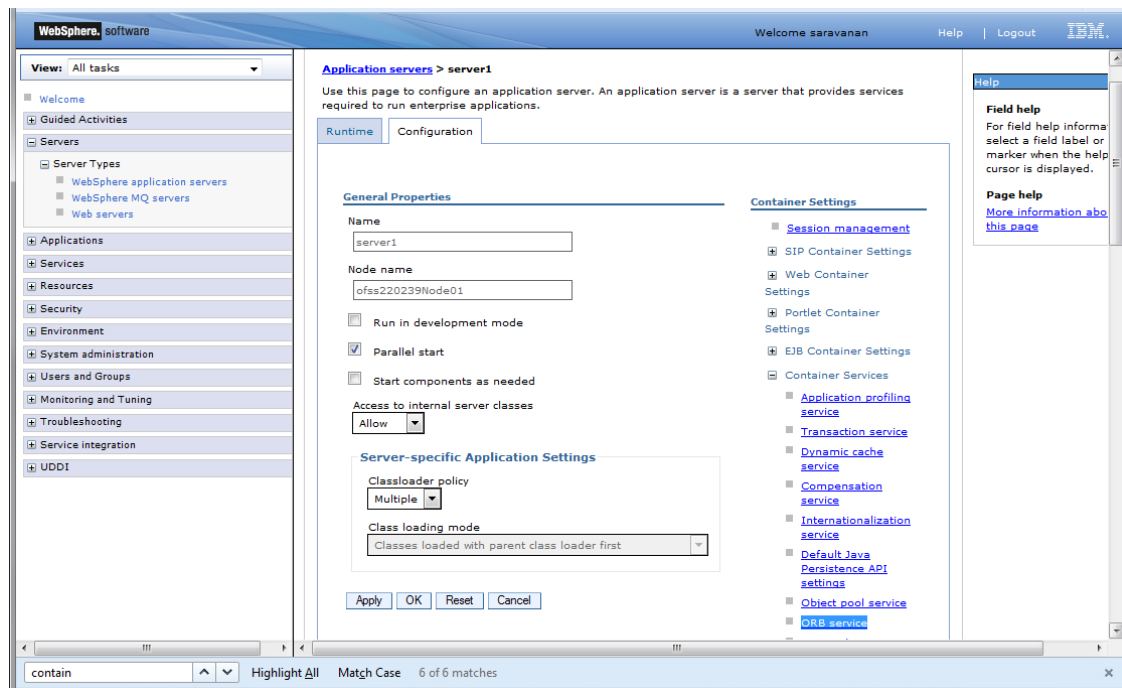
- Go to 'Server > Application Servers' and select the 'server_name'
- Under the Configuration tab, navigate to 'Server Infrastructure > Java(TM) and Process Management > Process Definition > Additional Properties: Java Virtual Machine'
- Modify the initial heap size and maximum heap size appropriately based on the load size

6.2 IBM Websphere Server - Transaction Service Properties

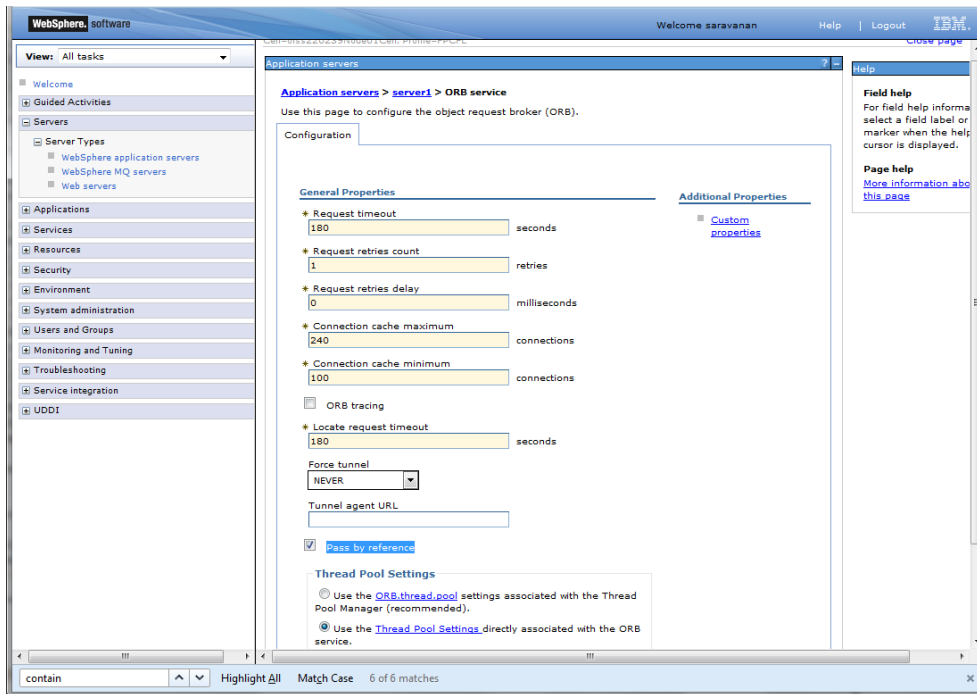
- Go to 'Server > Application Servers' and select the 'server_name'
- Choose 'Container Services > Transaction Service'
- Change the total transaction lifetime timeout appropriately
- Party content, products, or services.

6.3 IBM Websphere Server – ORB Service Configuration

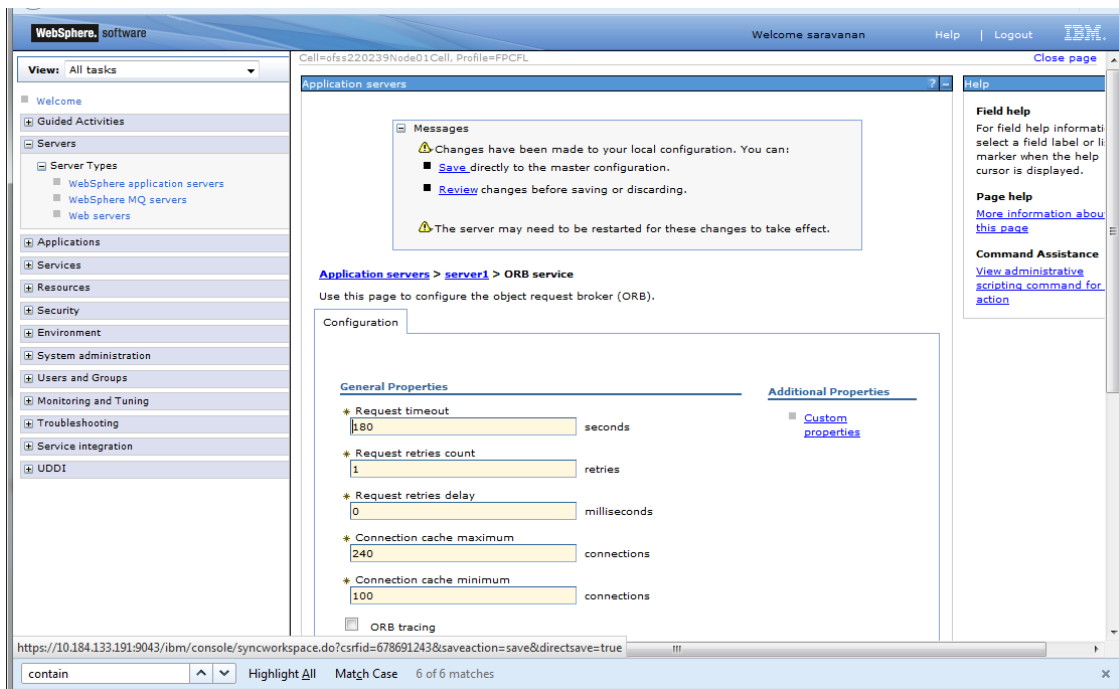
- Go to 'Server > Application Servers' and select the 'server_name'



- Expand 'Container Services' and click 'ORB Service'



Check 'Pass by reference' and click Apply



Click 'Save'.



Websphere Configuration
[May] [2021]
Version 14.5.0.0.0

Oracle Financial Services Software Limited
Oracle Park
Off Western Express Highway
Goregaon (East)
Mumbai, Maharashtra 400 063
India

Worldwide Inquiries:
Phone: +91 22 6718 3000
Fax: +91 22 6718 3001
www.oracle.com/financialservices/

Copyright © [2007], [2021], Oracle and/or its affiliates.

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

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" or "commercial computer software documentation" 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 failsafe, 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.

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.

This software or hardware and documentation may provide access to or information on 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. 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.