Websphere Configuration
Oracle FLEXCUBE Investor Servicing
Release 12.0.3.0.0
[April] [2014]

Table of Contents

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 1024 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:

```
C:\Program Files\IBM\Websphere\AppServer\bin>keytool -
genkeypair -alias cvrhp0729 -keyalg RSA -keysize 1024 -sigalg
SHA1withRSA -validity 365 -keystore D:\keystores\FCINSTALLER
SERVICINGKeyStore.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>
```

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

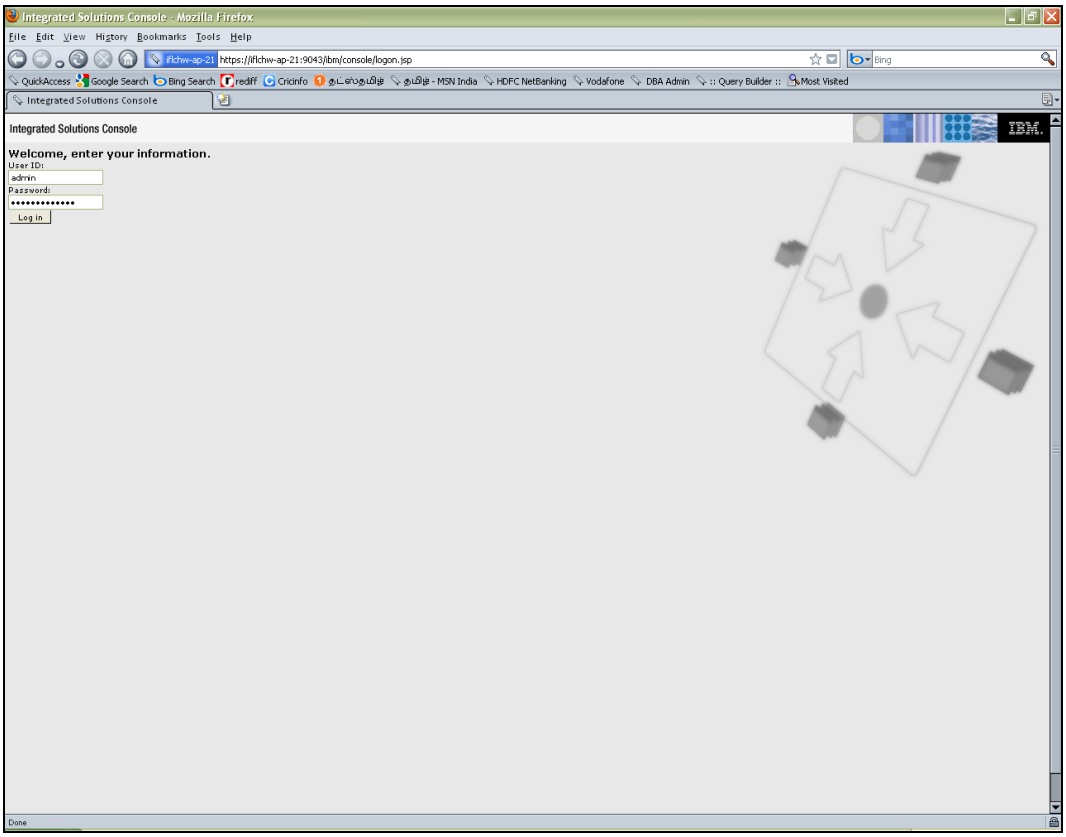
ips014dorCell01 --> <ips014dor> name of the machine and < Cell01>

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

1.3 Adding Key Store to Application Server

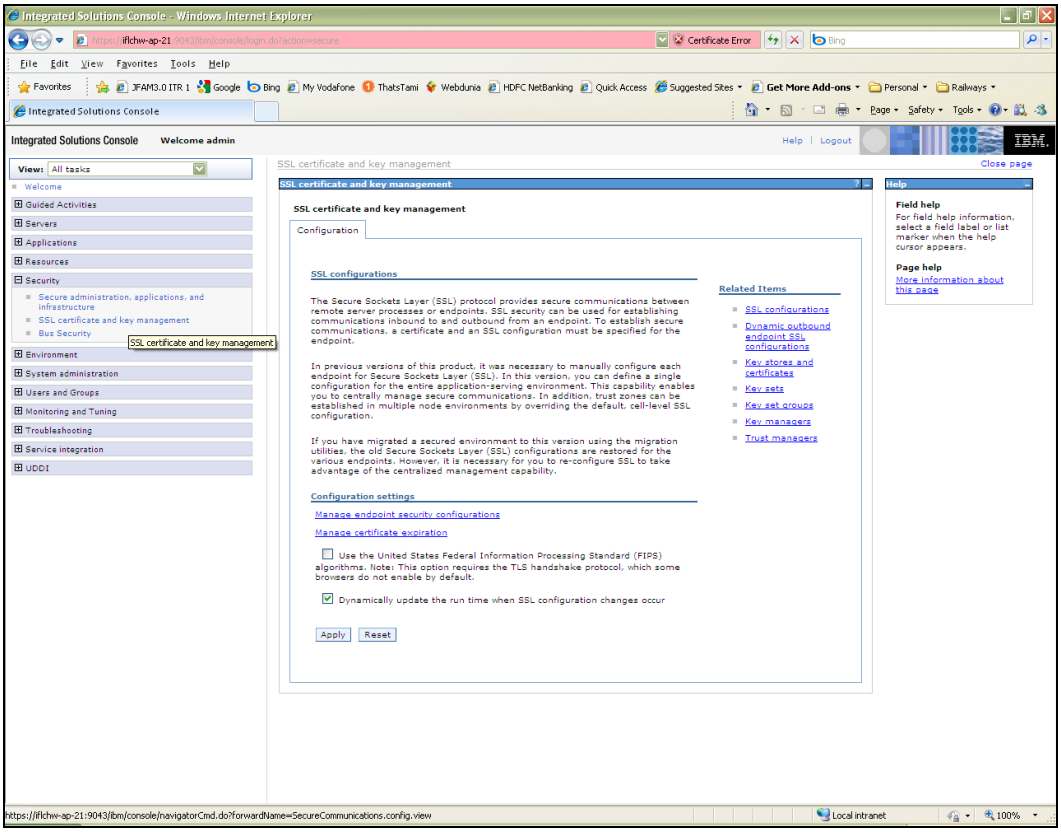
To add keystore to the Websphere application server, follow the instructions given below.

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’.

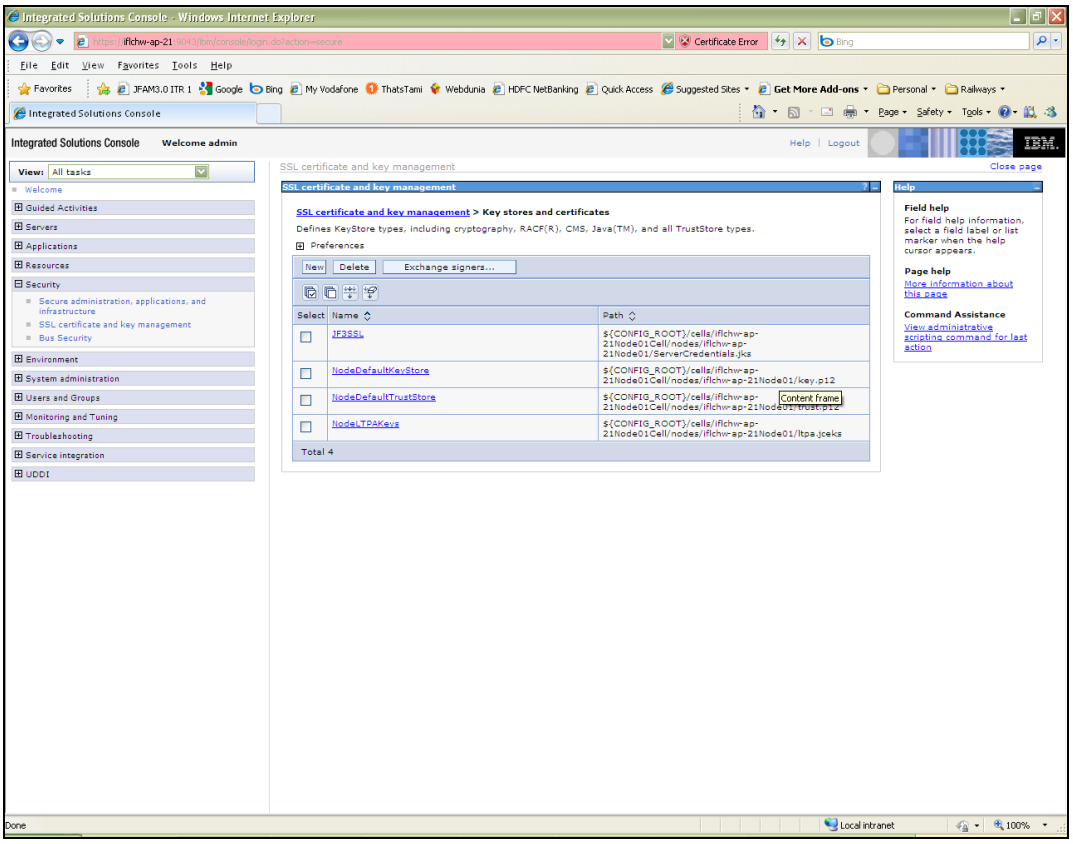
The following screen is displayed:



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

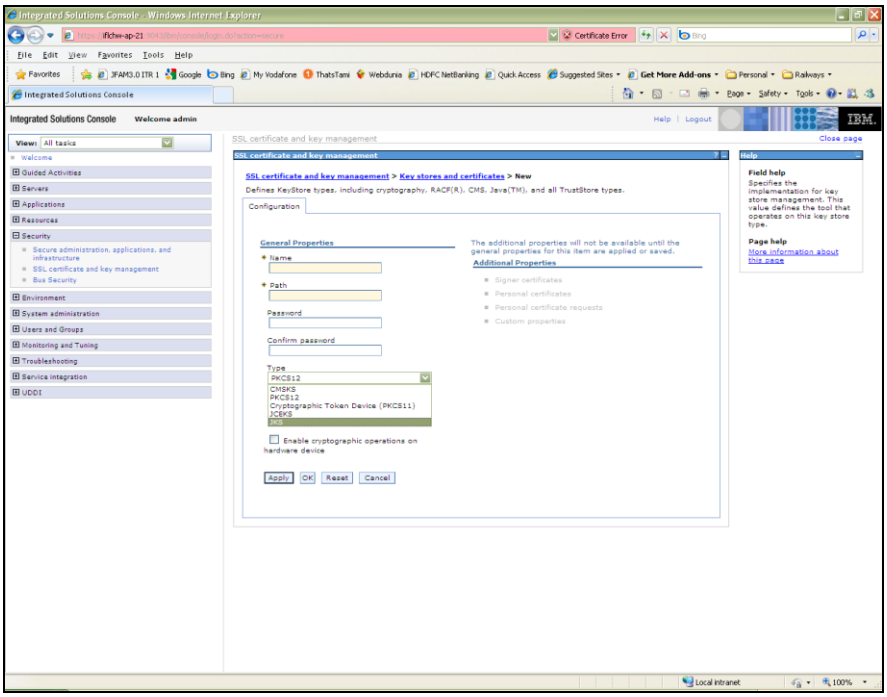
3. Under ‘Related items’ on the right side, click ‘Key stores and certificates’.

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

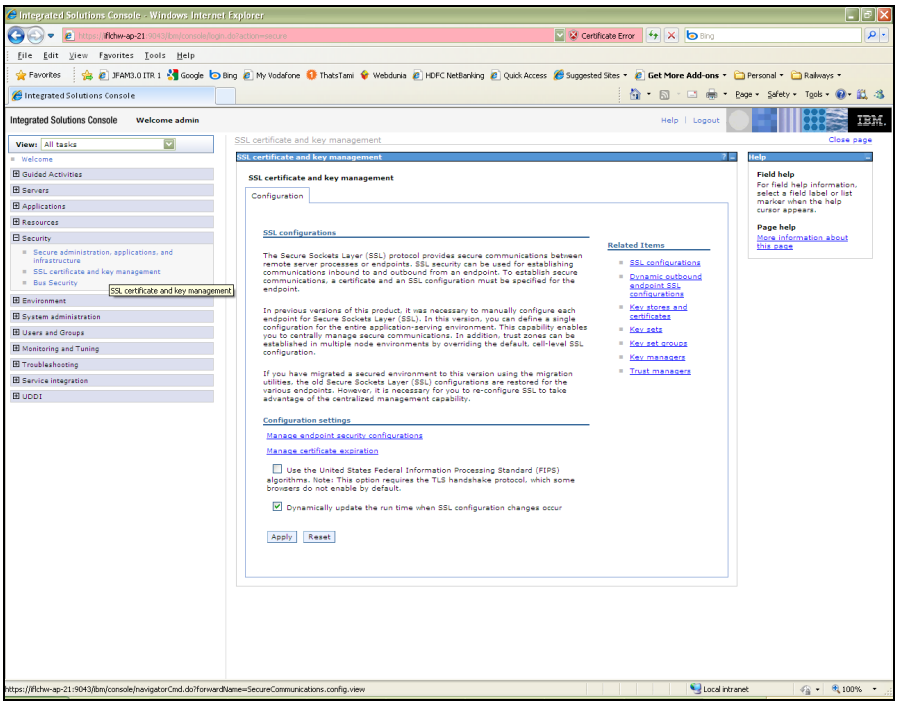
Password

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

6. Click ‘Apply’ and save the changes.

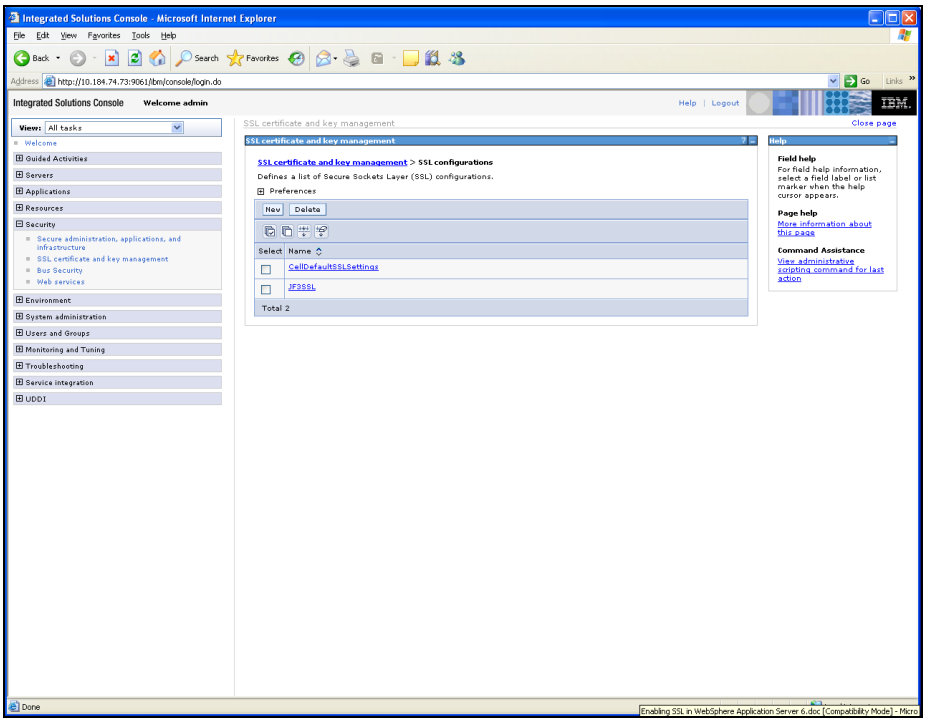
1.4 Creating SSL Configuration

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

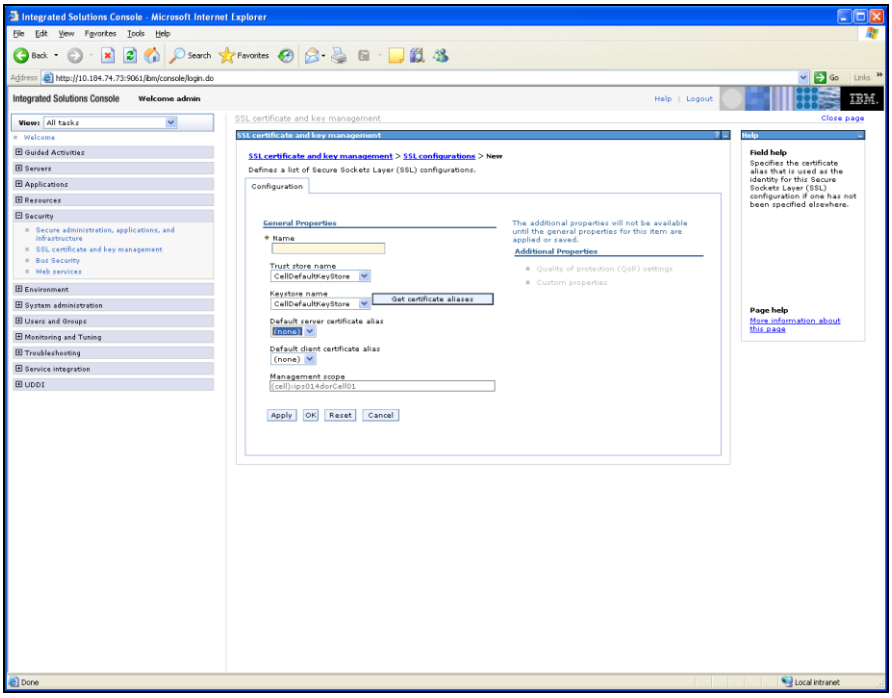


1. Under the section ‘Related items’, click ‘SSL configurations’.

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.

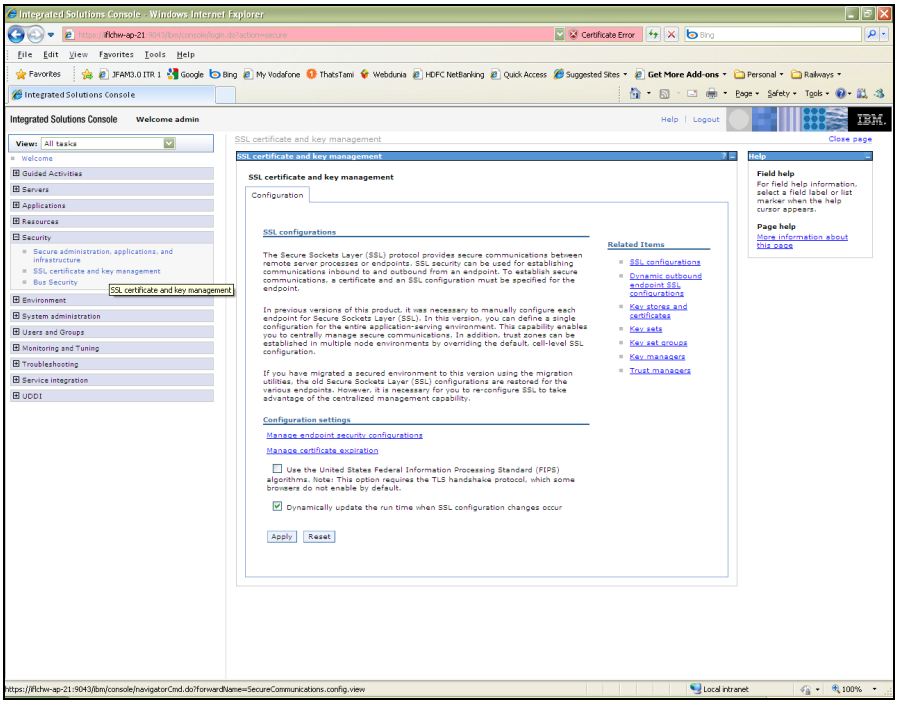
Key Store Name

Select the added key store.

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

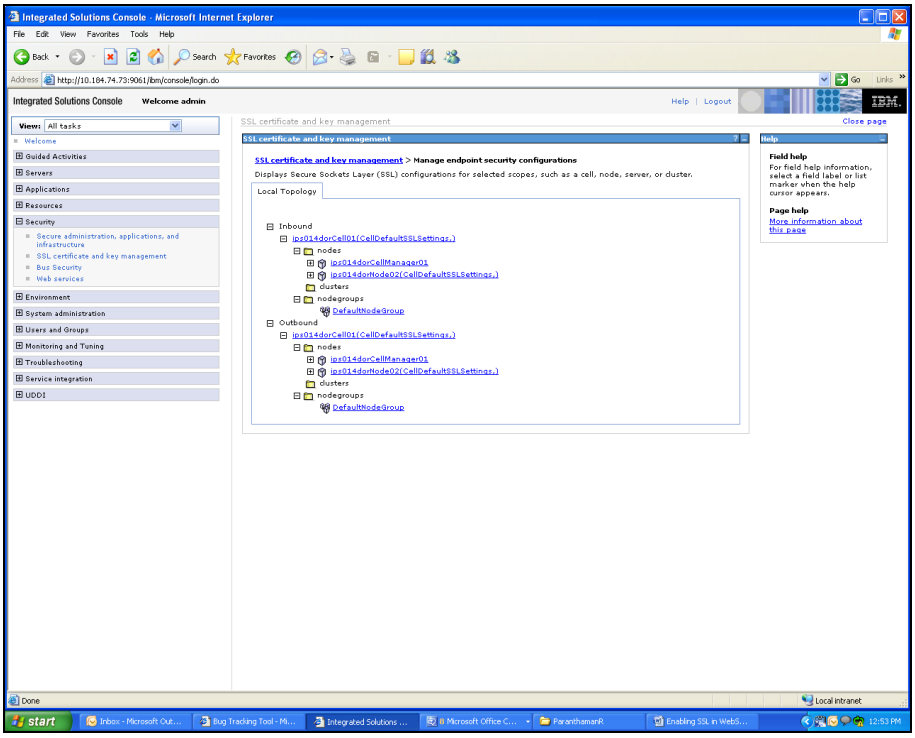
1.5 Managing Endpoint Security Configurations

This section explains the process of managing endpoint security configurations.

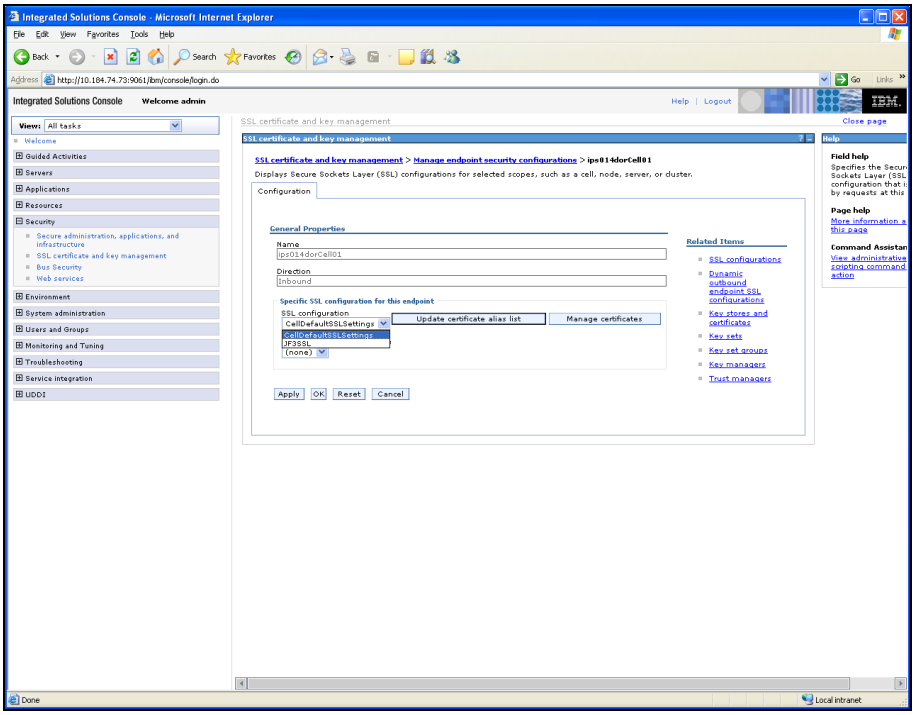


5. On the left pane, expand ‘Security’ and click ‘SSL certificate and key management’. Under ‘Configuration settings’, click ‘Manage endpoint security configurations’.

The following screen is displayed:



6. Click the first link under ‘Inbound tree’. The following screen is displayed:

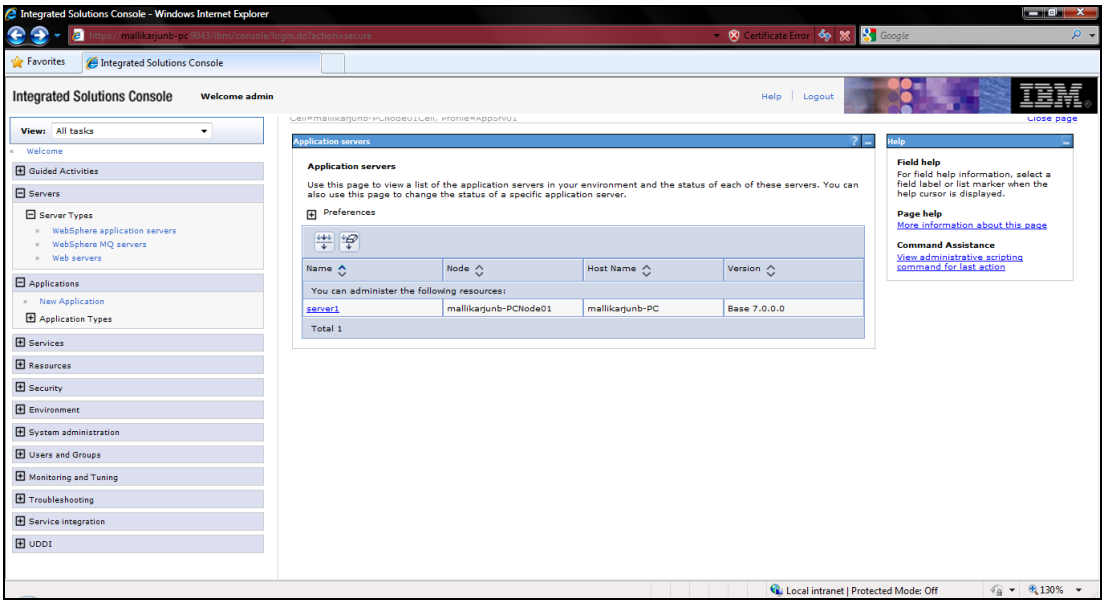


Under SSL configurations, select the configured SSL from the drop-down list.

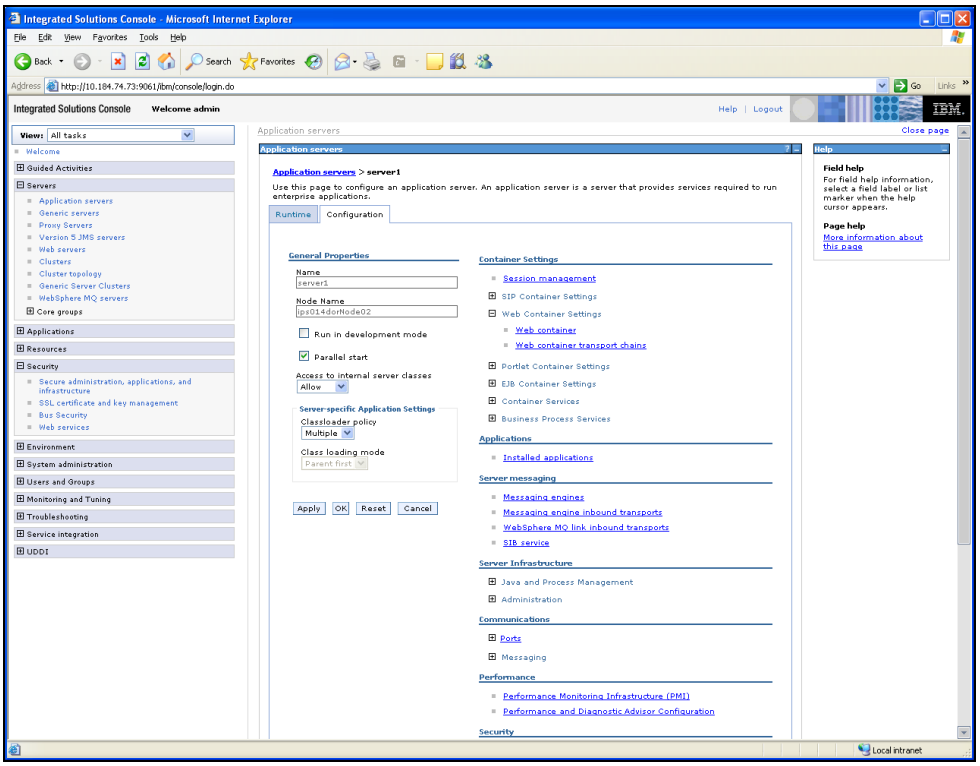
7. Click the button ‘Update certificate alias list’. Click ‘Apply’ and save the changes.

1.6 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

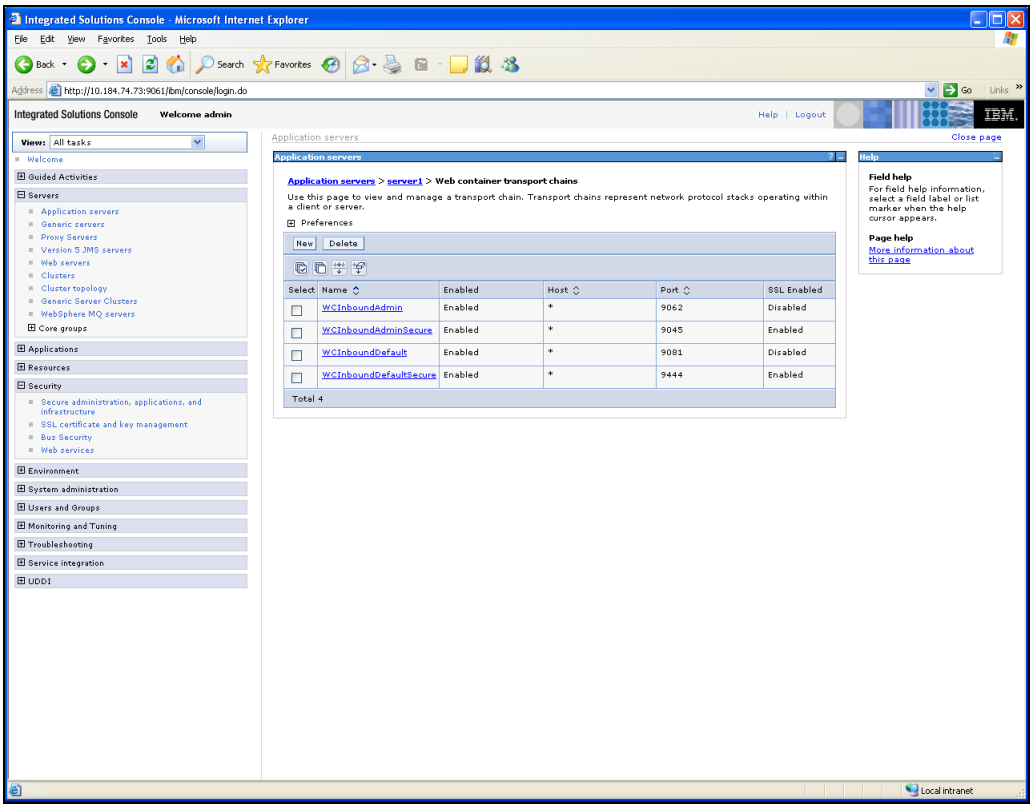


1. Click the server to which SSL configuration has to be applied. The following screen is displayed.



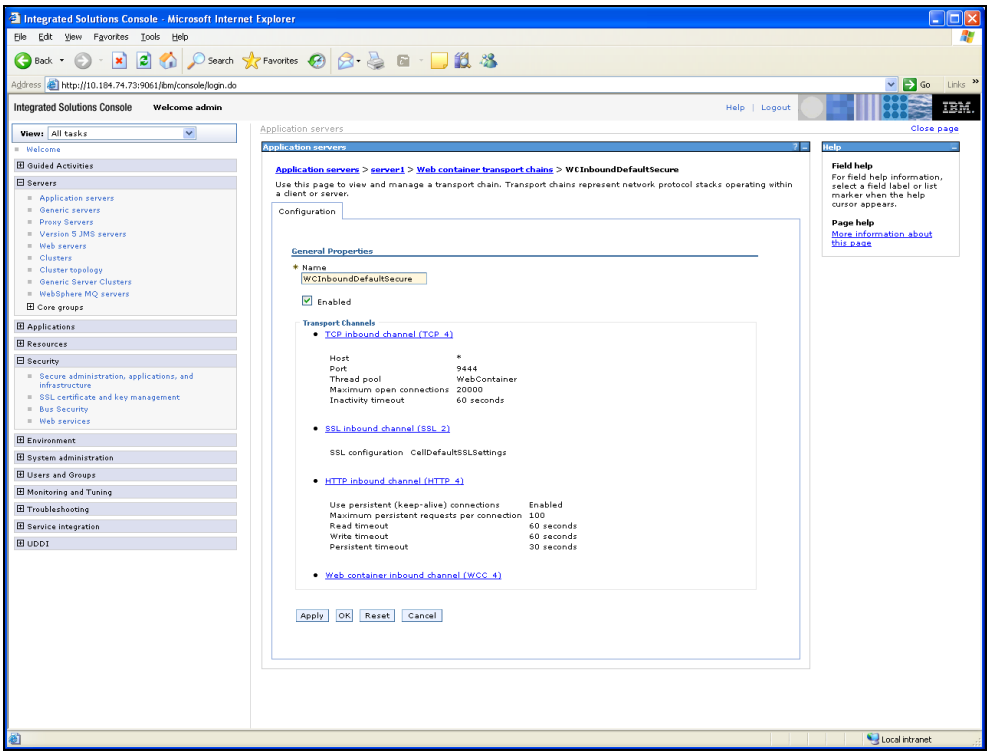
2. Go to Configuration tab and click ‘Web container transport chains’ under ‘Container settings’.

The following screen is displayed.

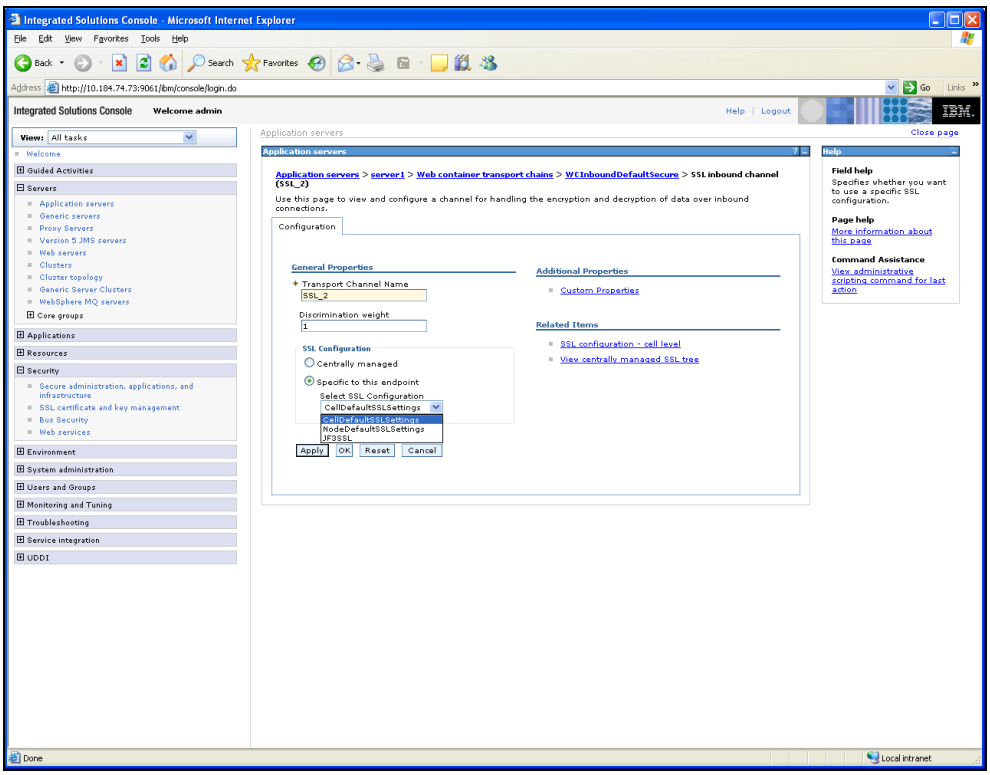


3. Against their respective names, the secured connection is available under the column ‘SSL Enabled’. Click ‘WCInboundDefaultSecure’.

The following screen is displayed:



4. Click ‘SSL Inbound channel (SSL 2).



5. Select the configured SSL from the list of SSL configurations. Click ‘Apply’ and save the changes.

1.7 Running Application with SSL

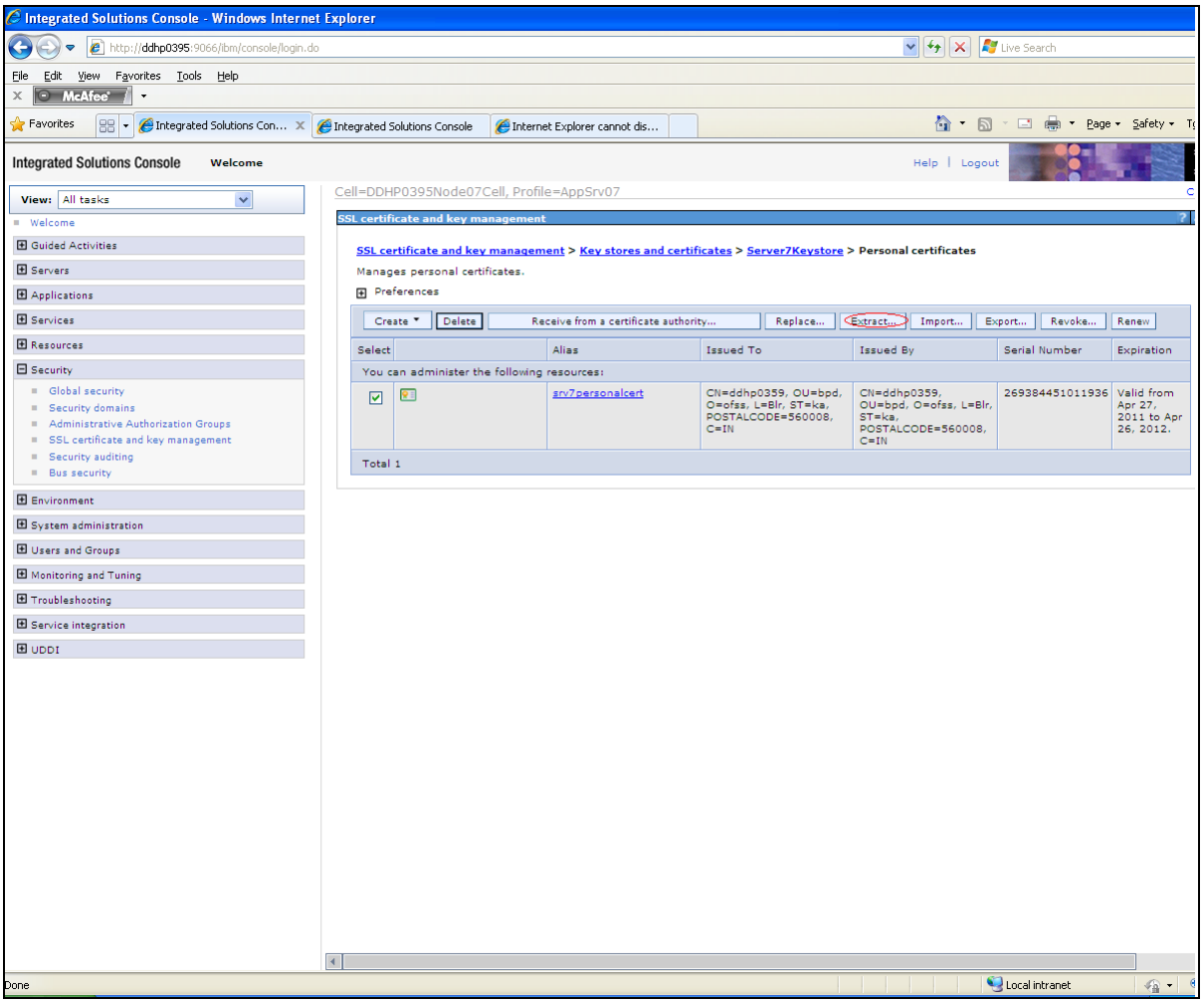
To run the application with SSL, use the following syntax:

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

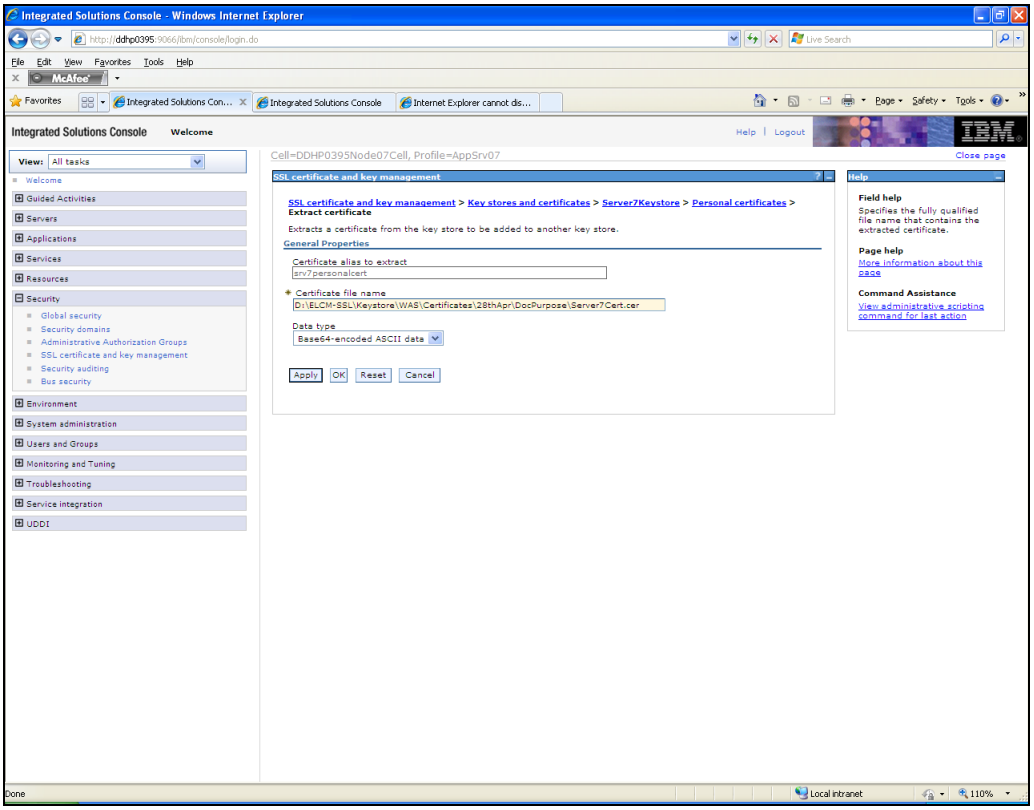
1.8 Certificate Exchange for Two Ways SSL

1.8.1 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 > ELCMKeyStore > 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.

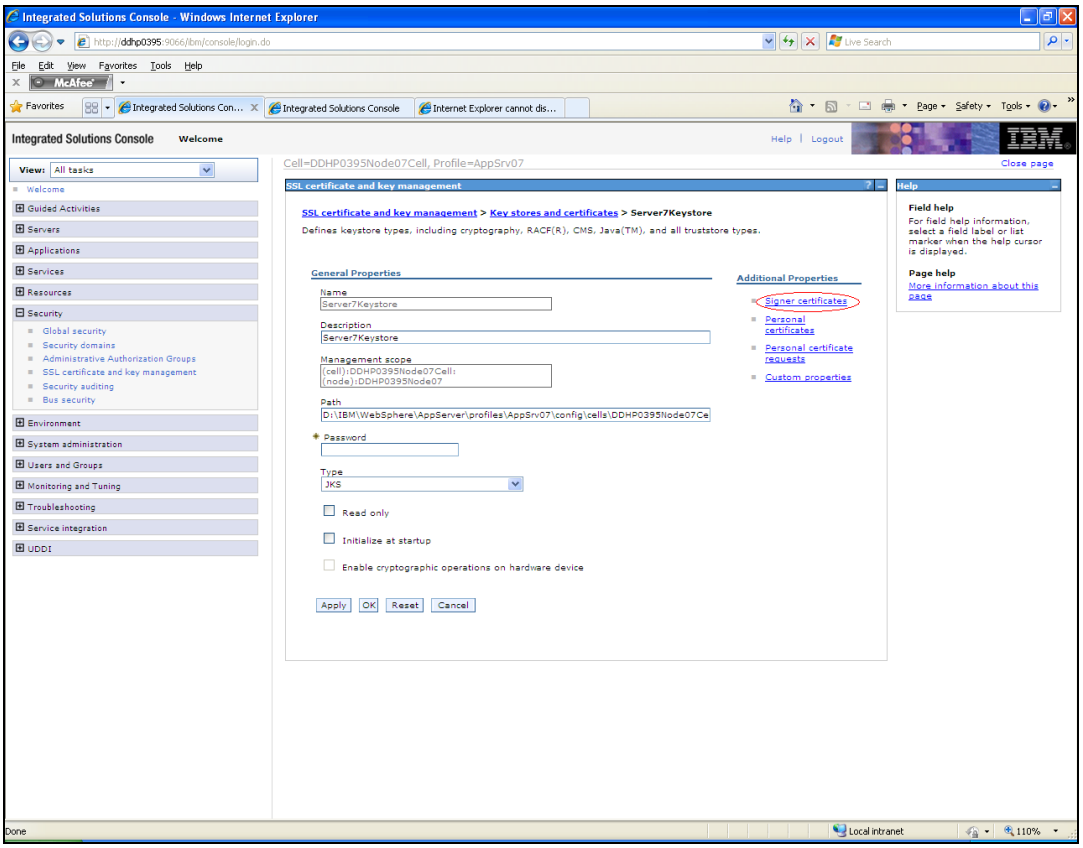
Eg: \<localfolder>\<server2.cer>

1.8.2 Extracting Certificate for Server2

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

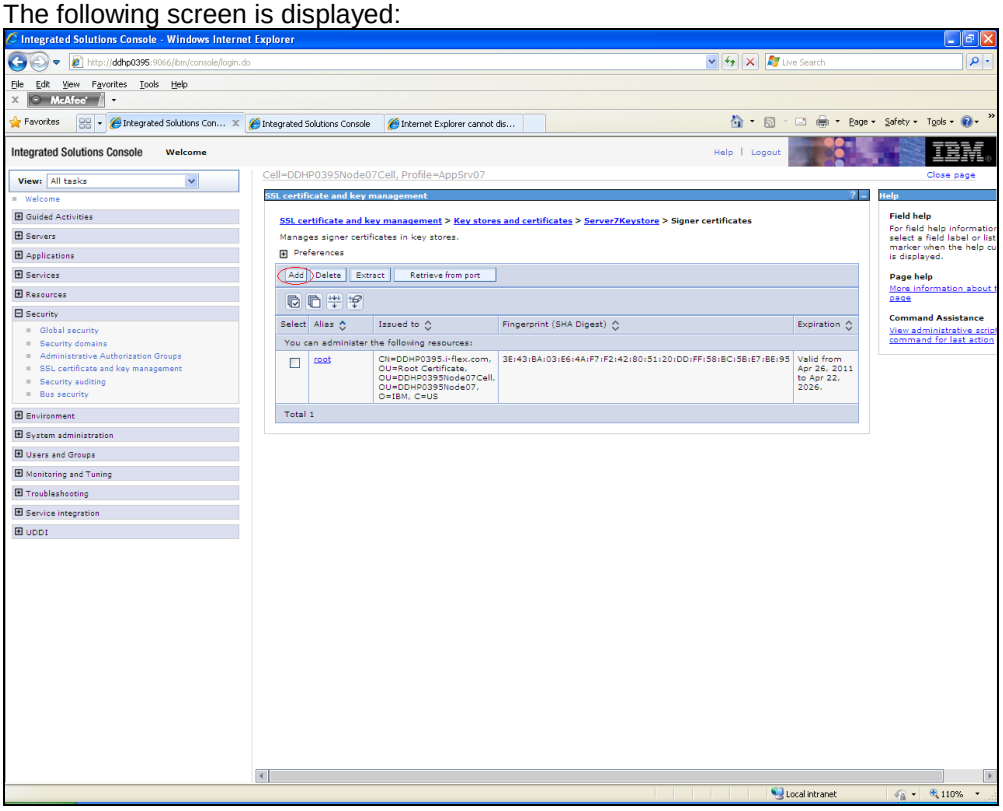
1.8.3 Importing Certificate into Keystore for Server1

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



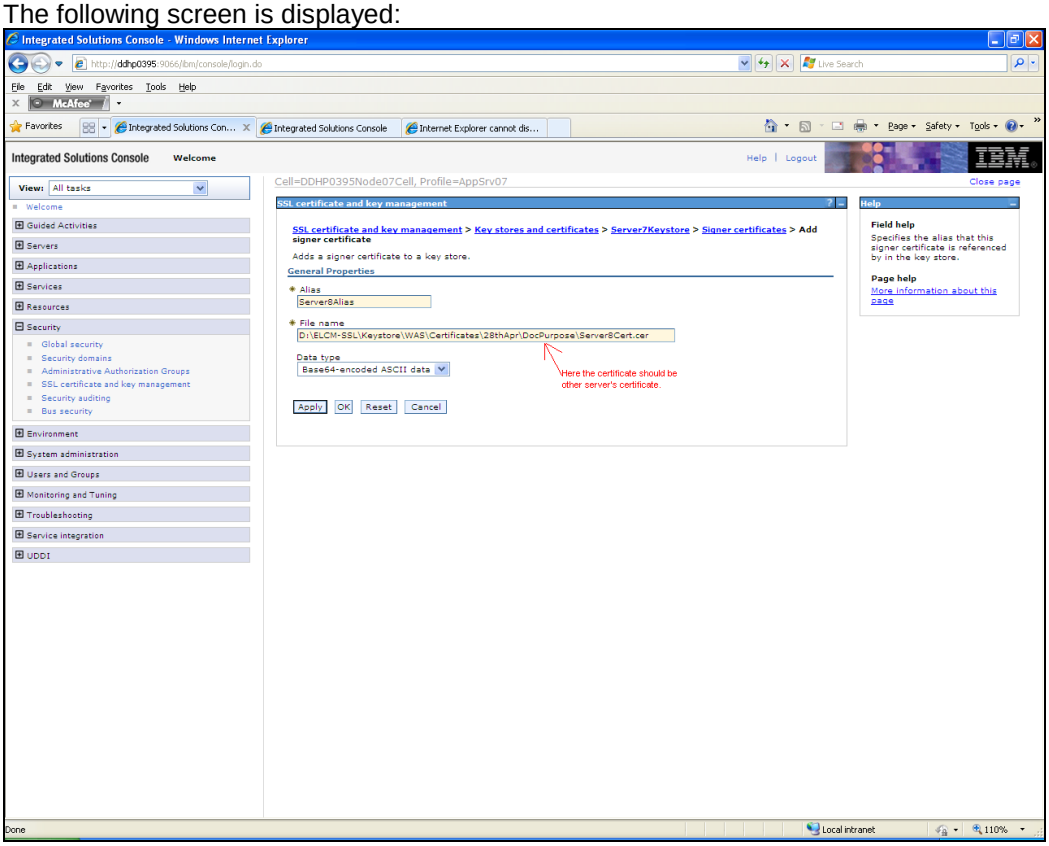
1. Click ‘Signer Certificates’.

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.

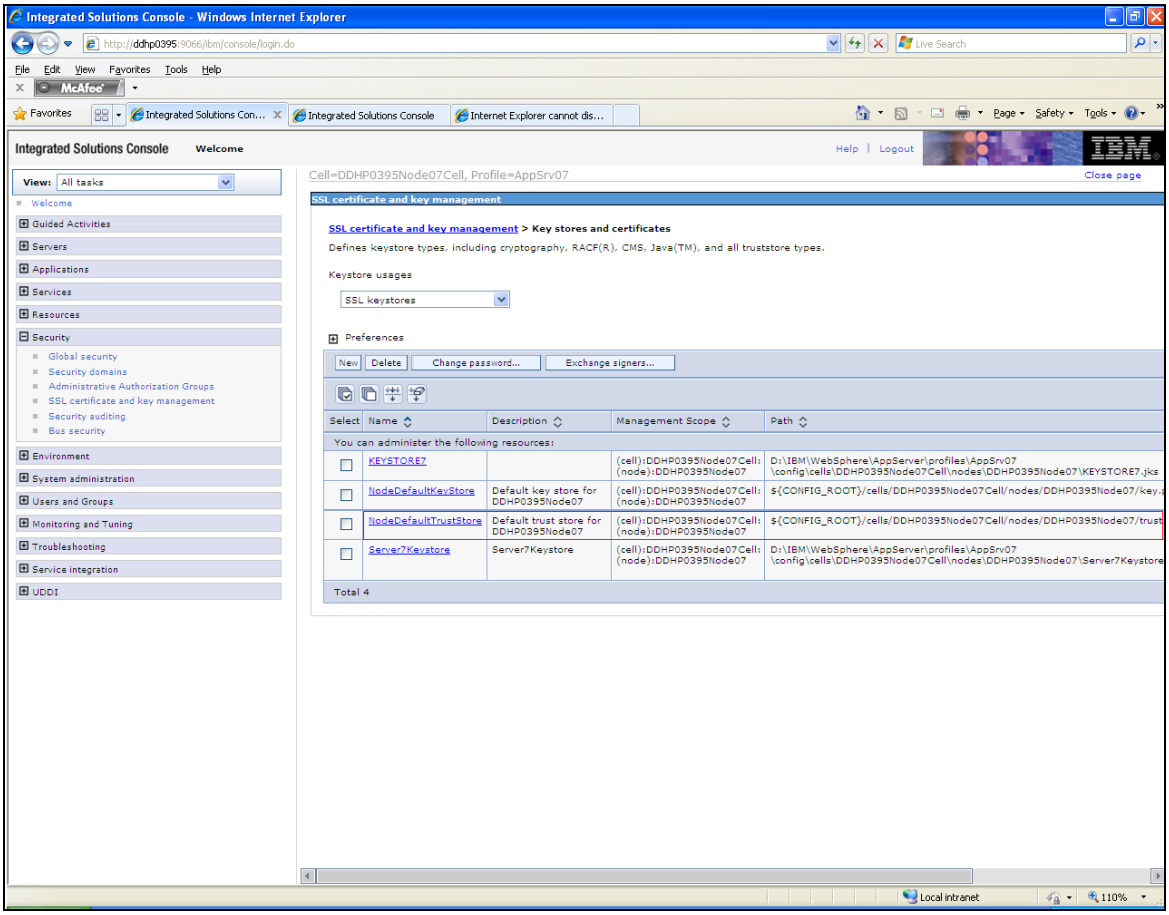
Eg: \<localfolder>\<server1.cer>

1.8.4 Importing Certificate into Keystore for Server2

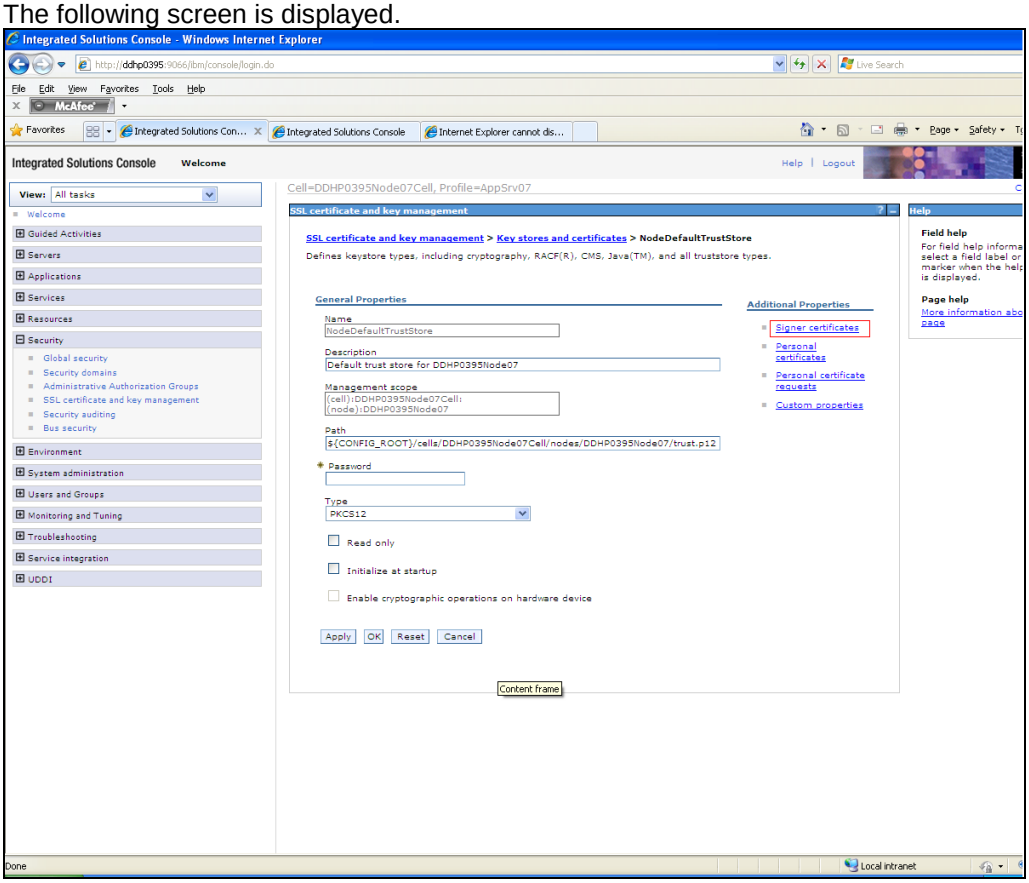
You can follow the steps for server 1 described under ‘Importing Certificate into Keystore for Server1’ to import the certificate into keystore for Server2.

1.8.5 Importing Certificate into Truststore for Server1

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

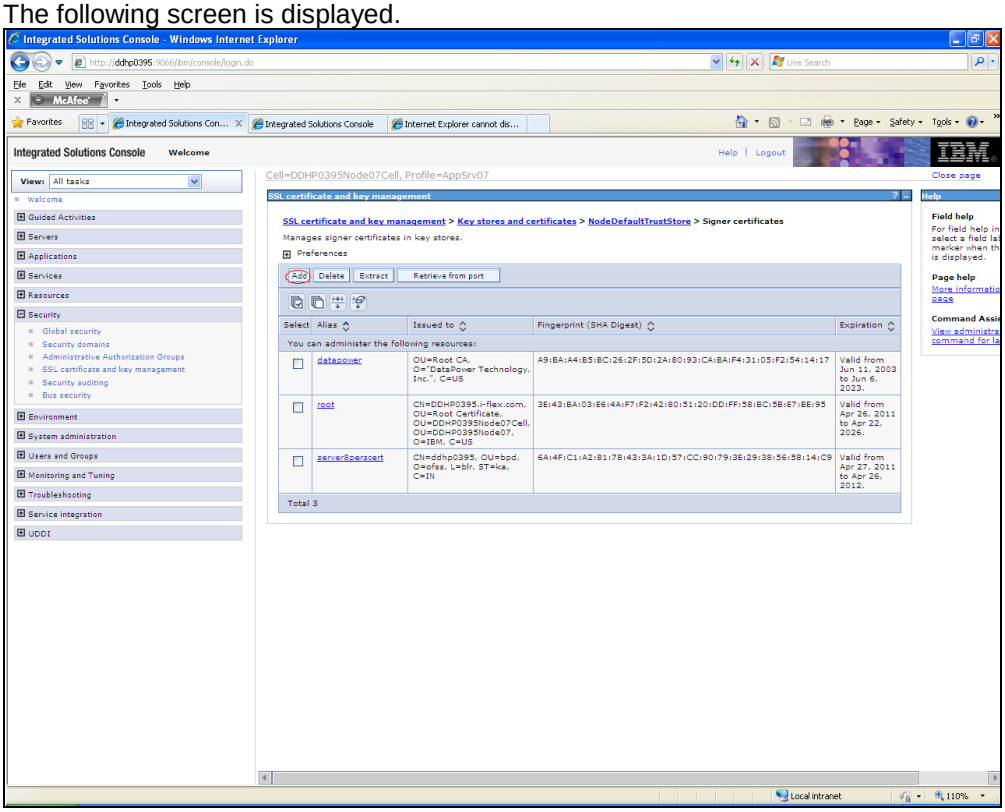


The following screen is displayed.



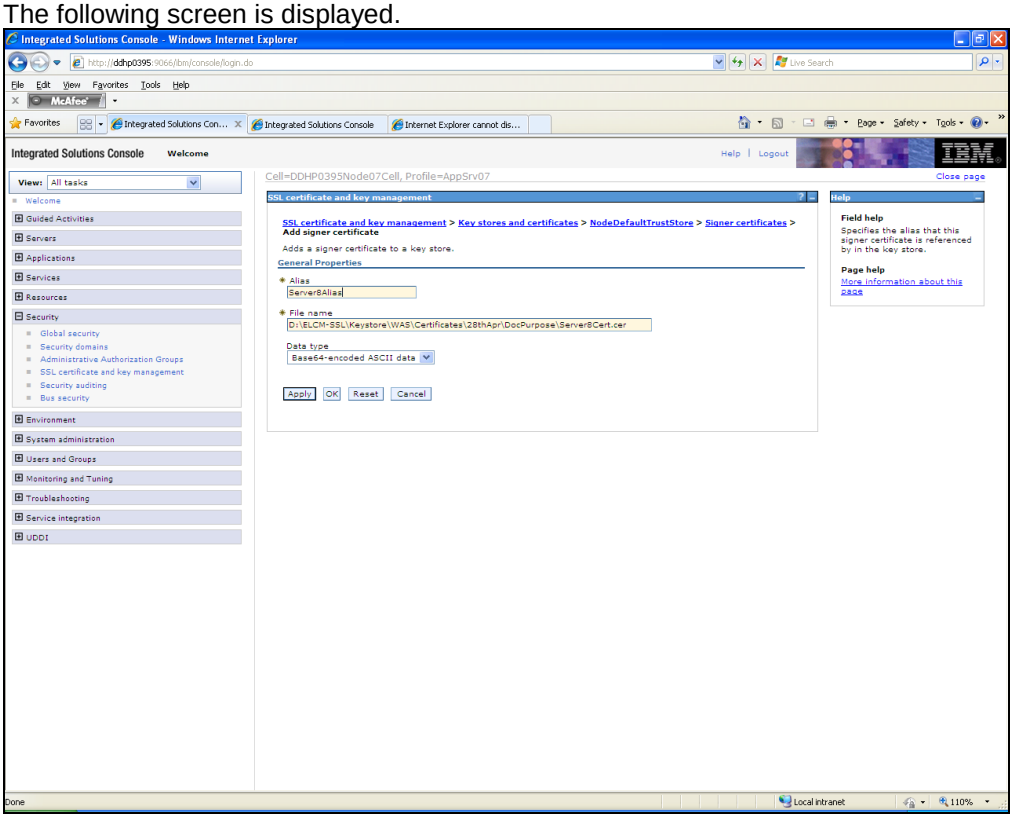
4. Click ‘Signer Certificates’.

The following screen is displayed.



5. Click ‘Add’ button to add the extracted certificate of the second server.

The following screen is displayed.



6. Specify the ‘alias’ name to identify the other server.

Eg: For server1, you can give the alias name ‘*server2Alias*’.

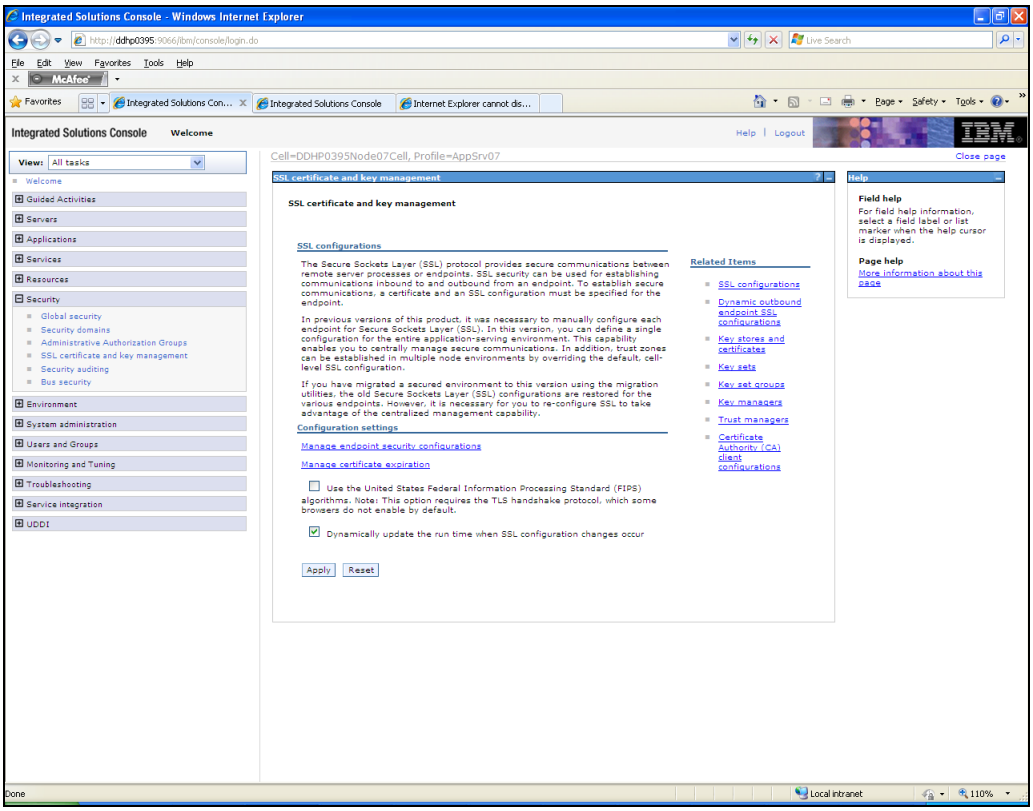
7. Further, specify the location of the extracted certificate.

1.8.6 Importing Certificate into Truststore for Server2

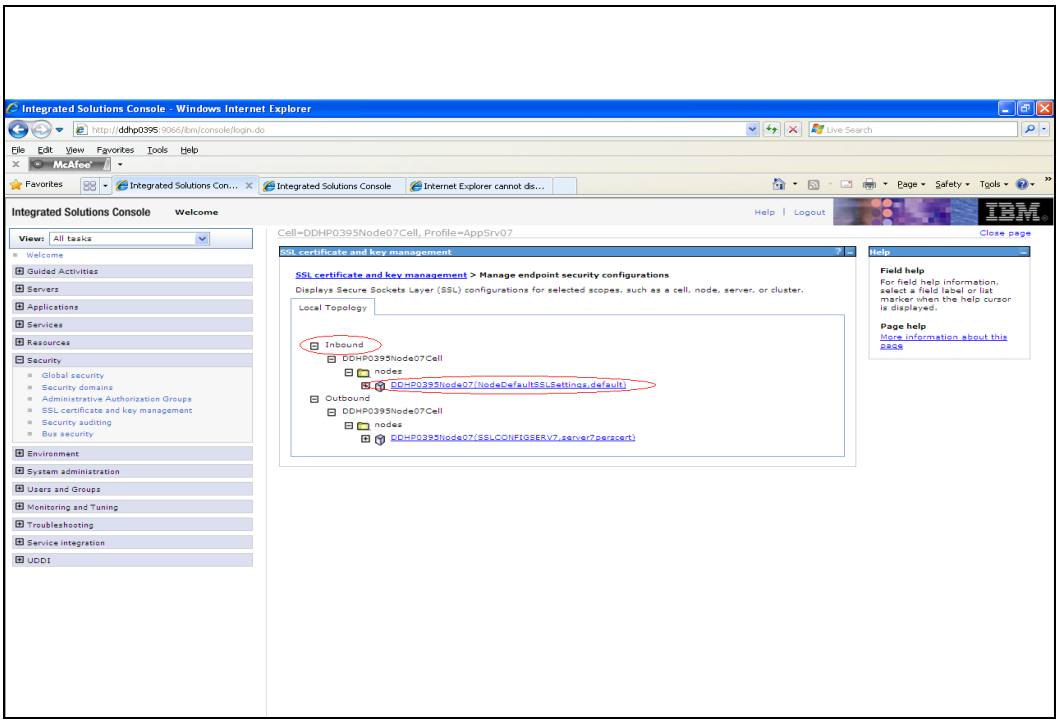
You can follow the steps for server 1 described under ‘Importing Certificate into Truststore for Server2’ to import the certificate into Truststore for Server2.

1.9 Managing Endpoint Security Configurations

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

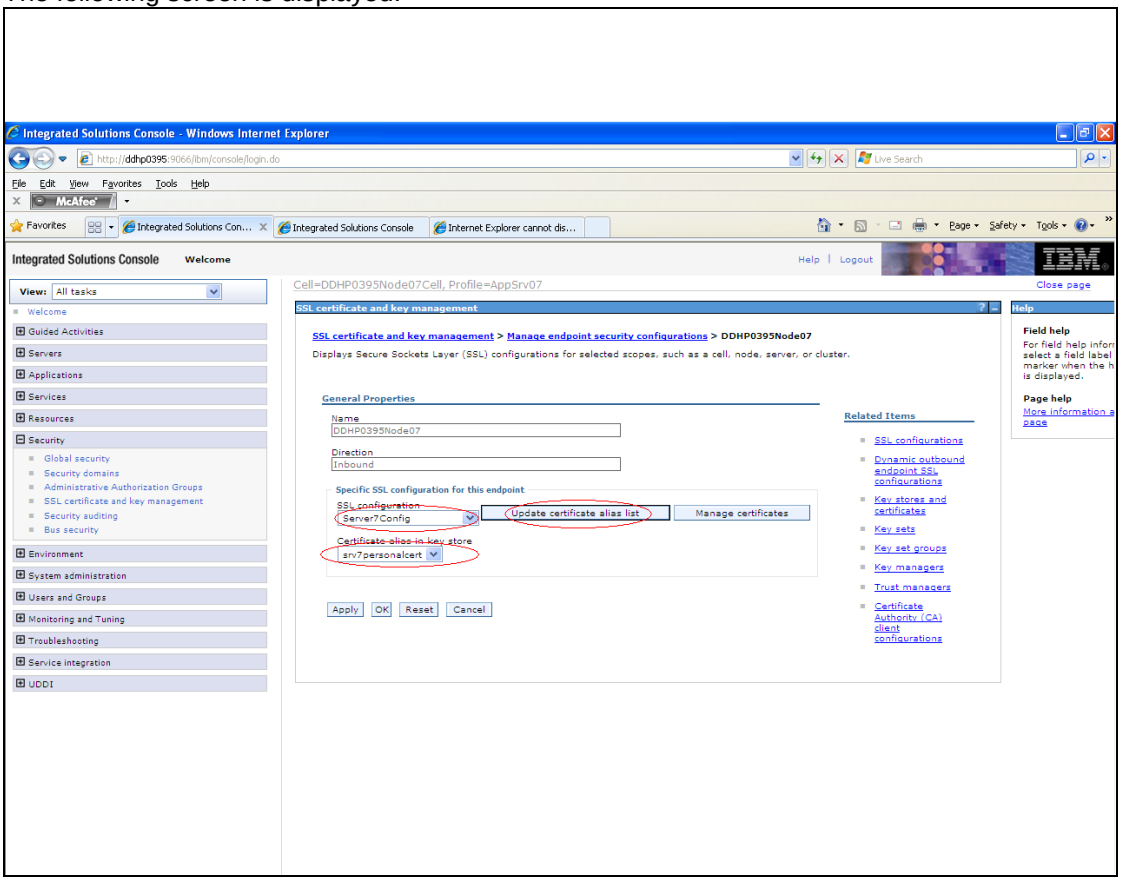


1. Expand ‘Security > SSL certificate and key management’ and click ‘Manage endpoint security configurations’.



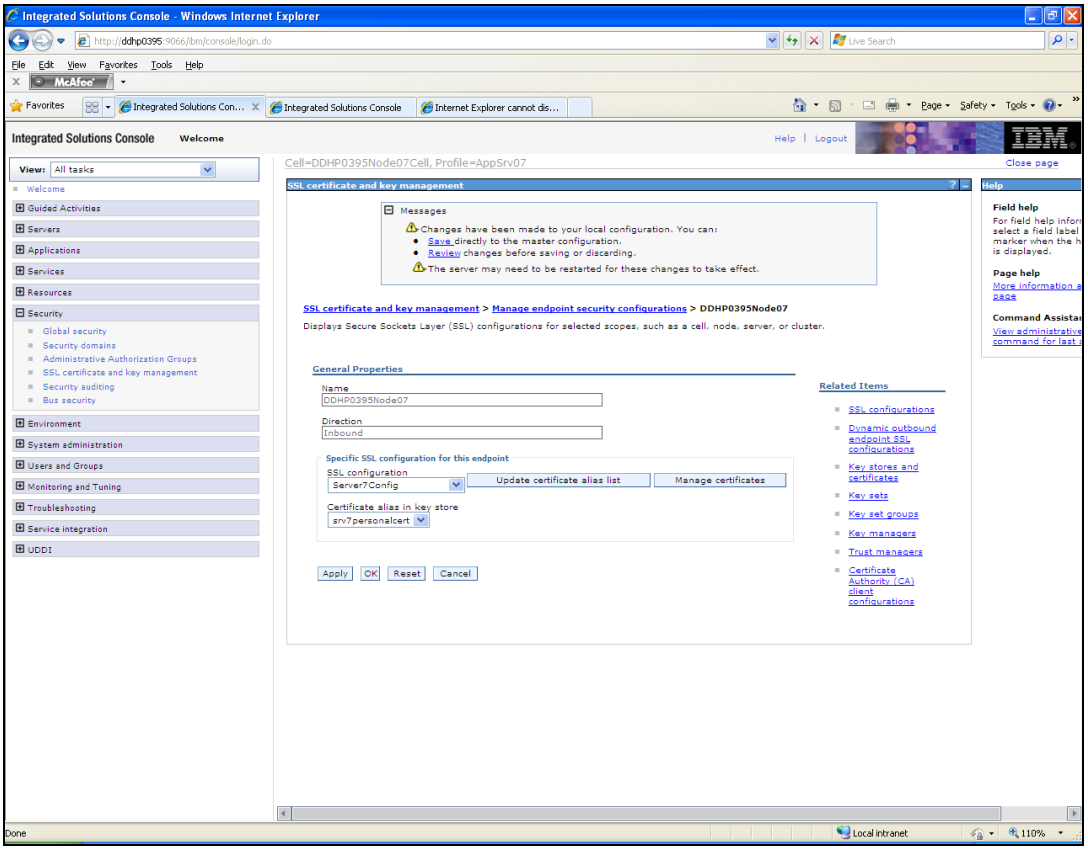
2. Change the inbound node settings. Expand ‘Inbound’ and click ‘DDHP0395Node07(NodeDefaultSSLSettings,default)’.

The following screen is displayed.

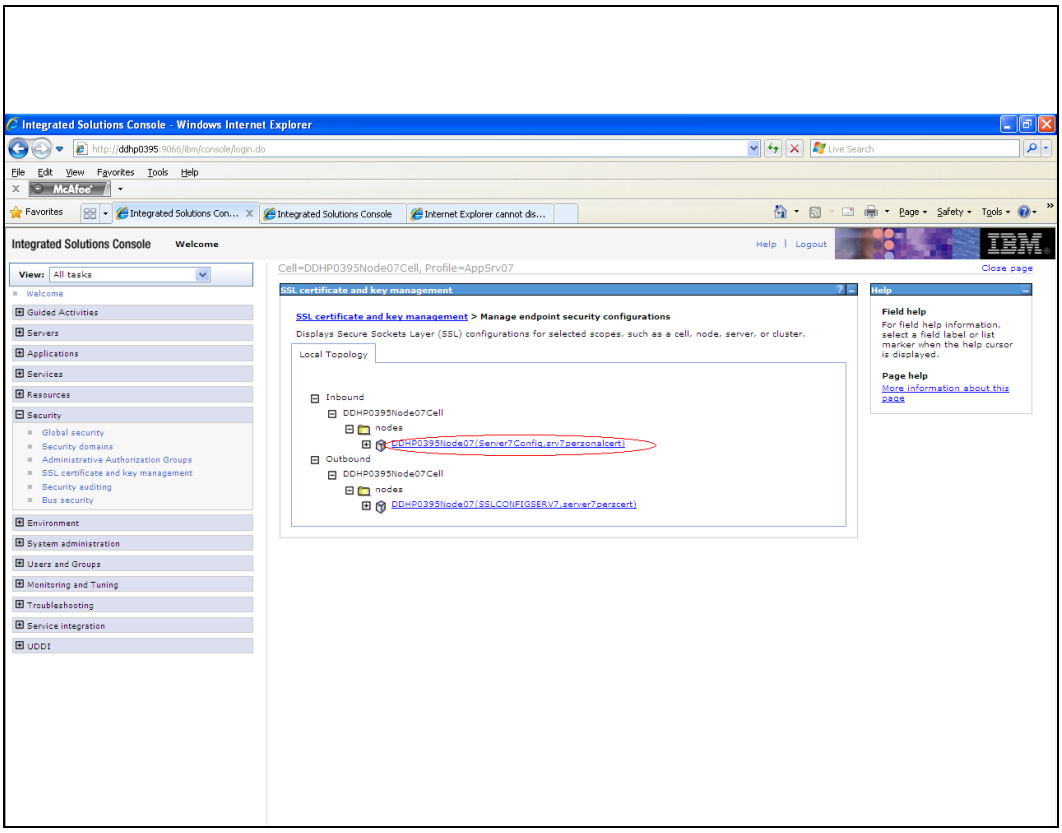


3. Select the ‘SSL Configuration’ created which you just created. Click ‘Update certificate alias list ‘ button.

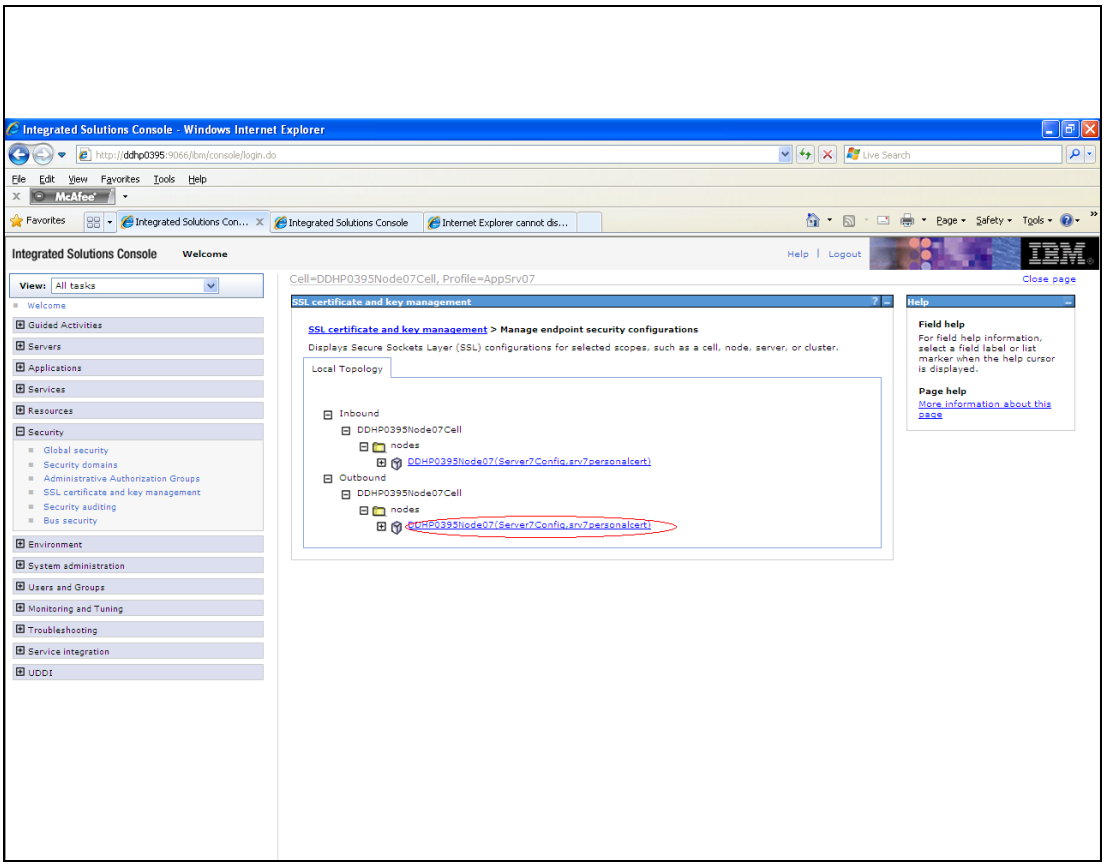
4. Ensure that the proper certificate and SSL configuration are selected. Further, click ‘Apply’ and save the settings.



You can view the settings under ‘Inbound’.



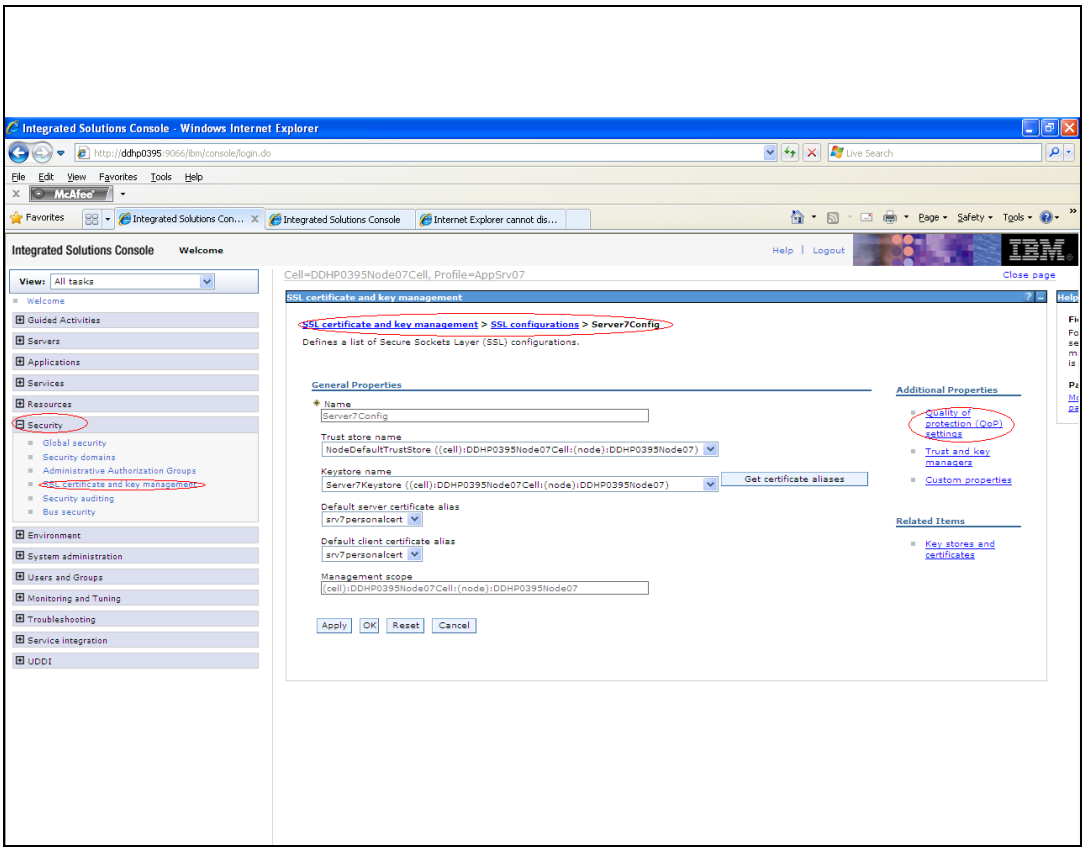
5. Repeat the above steps for ‘Outbound’ as well.



6. You need to repeat the above steps for server2 also.

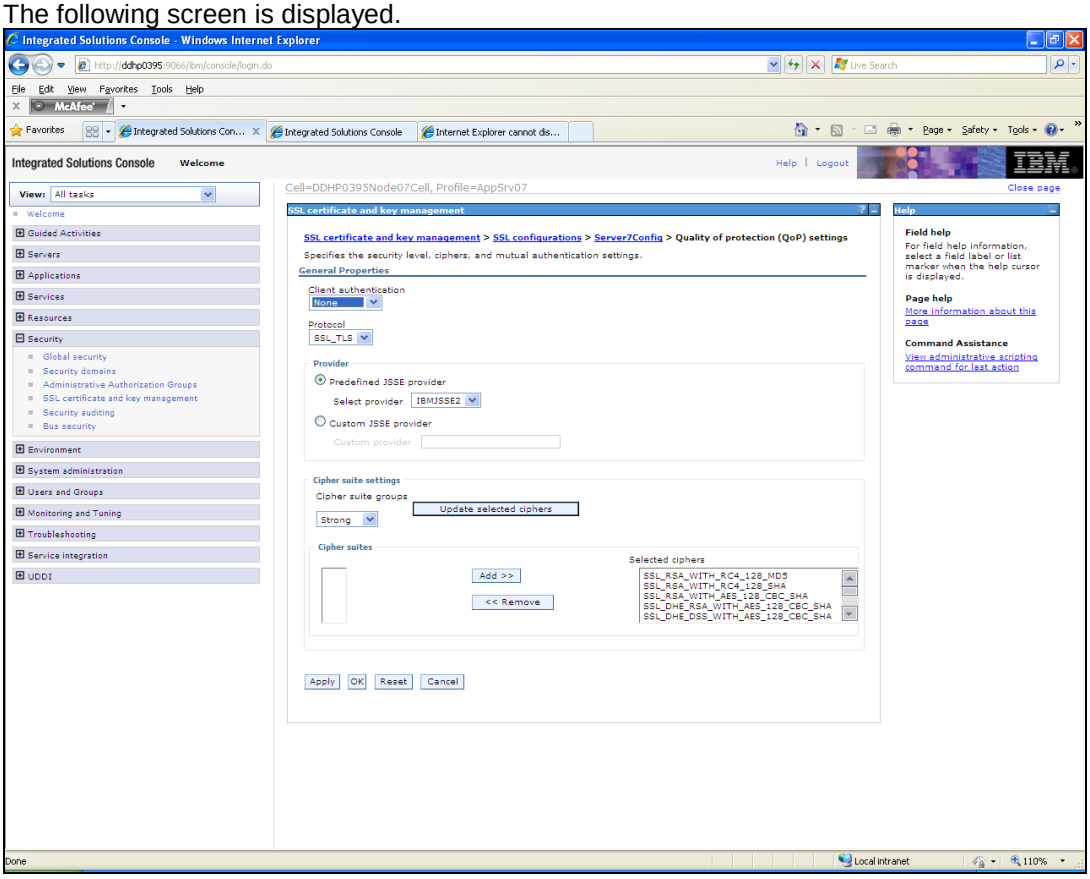
1.10 Protection Quality

1. Expand ‘SSL certificate and key management > SSL configurations > Server7Config’.



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.

// New Changes

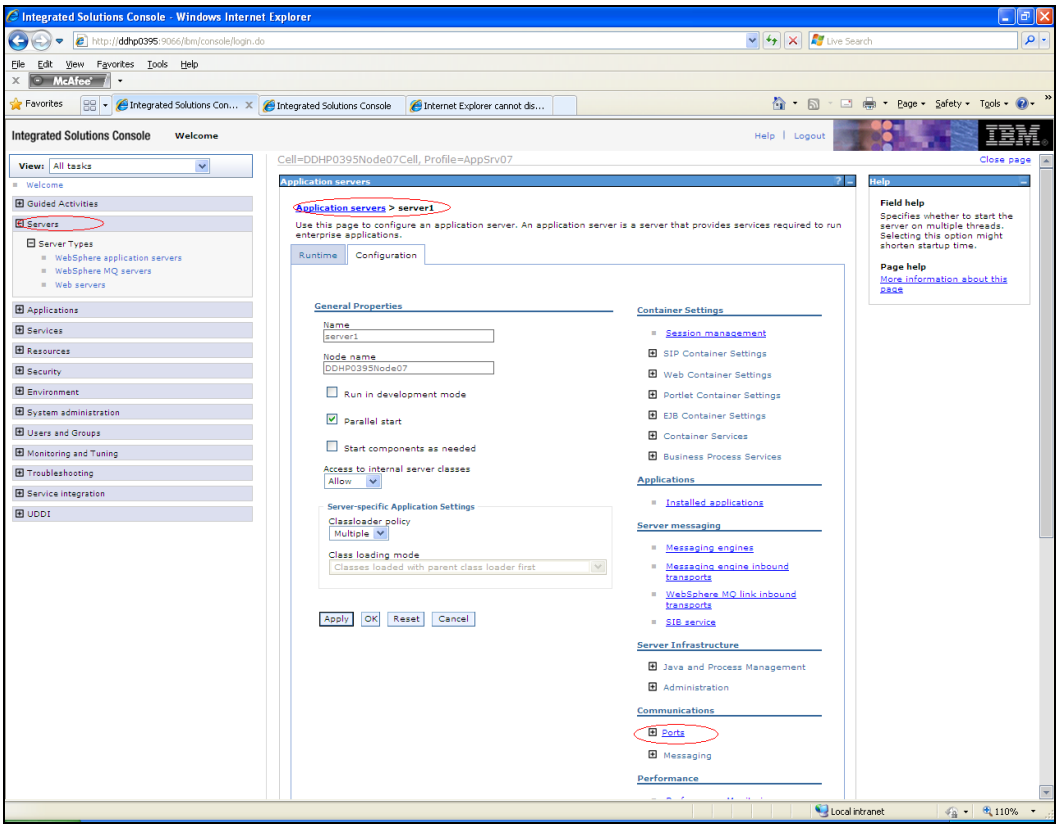
1.11 Importing or Adding Server Certificates using Batch

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

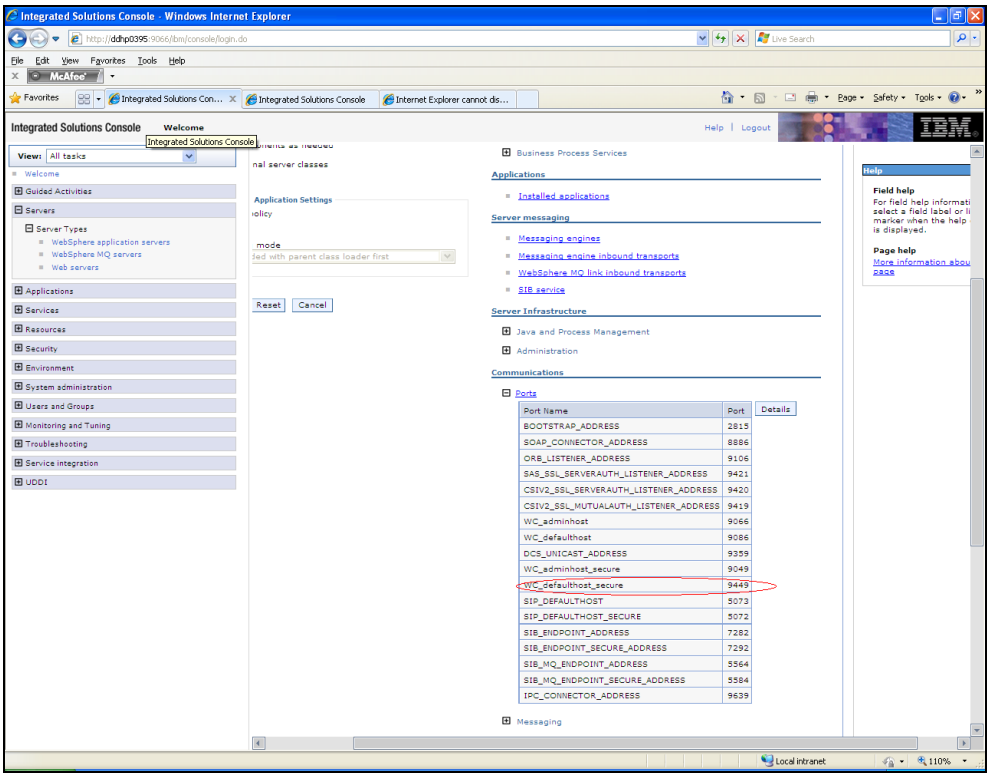
<InstalledLocatio>\IBM\Websphere\AppServer\bin

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

SSL port information is available in the following screens.



1. Click ‘Ports’.
2. The details are displayed as follows.


Integrated Solutions Console - Windows Internet Explorer
Integrated Solutions Console
Welcome
Help | Logout
Business Process Services
Applications
Installed applications
Server messaging
Messaging engines
Messaging engine inbound transports
WebSphere MQ link inbound transports
SIB service
Server Infrastructure
Java and Process Management
Administration
Communications
Ports
Port Name | Port | Details
BOOTSTRAP_ADDRESS | 2815
SOAP_CONNECTOR_ADDRESS | 8886
ORB_LISTENER_ADDRESS | 9106
SAS_SSL_SERVERAUTH_LISTENER_ADDRESS | 9421
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS | 9420
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS | 9419
WC_adminhost | 9066
WC_defaulthost | 9086
DCS_UNICAST_ADDRESS | 9359
WC_adminhost_secure | 9049
WC_defaulthost_secure | 9449
SIP_DEFAULTHOST | 5073
SIP_DEFAULTHOST_SECURE | 5072
SIB_ENDPOINT_ADDRESS | 7282
SIB_ENDPOINT_SECURE_ADDRESS | 7292
SIB_MQ_ENDPOINT_ADDRESS | 5564
SIB_MQ_ENDPOINT_SECURE_ADDRESS | 5584
IPC_CONNECTOR_ADDRESS | 9639
Messaging

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.

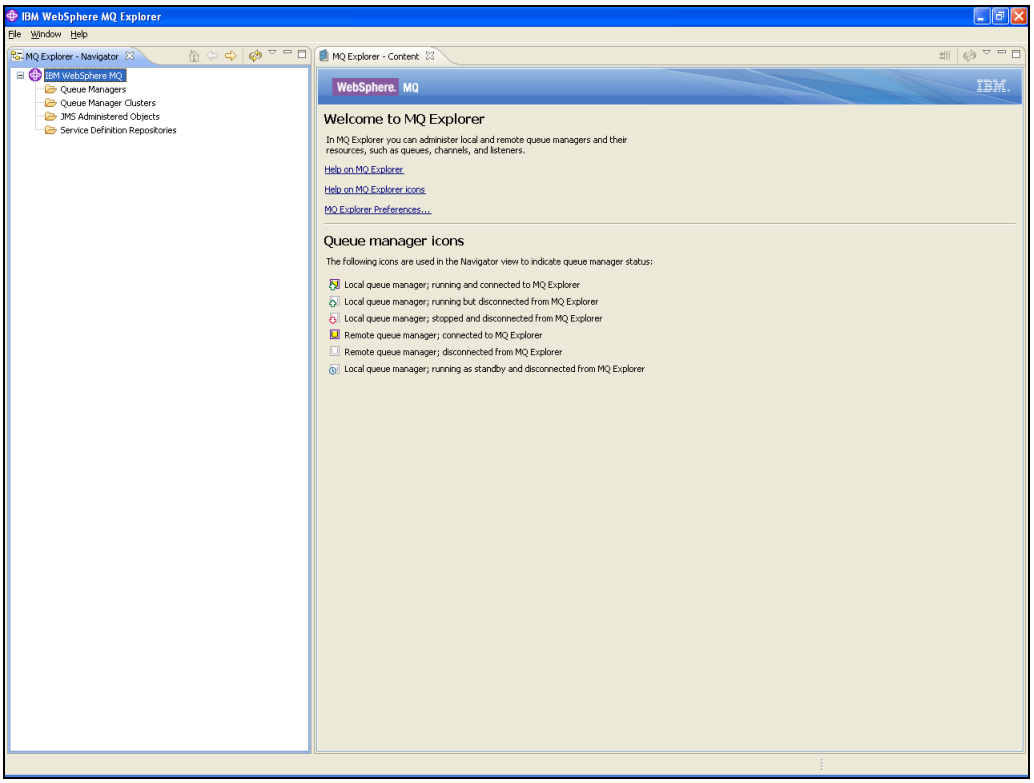
2.2 Creating Queues on Websphere MQ Server

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

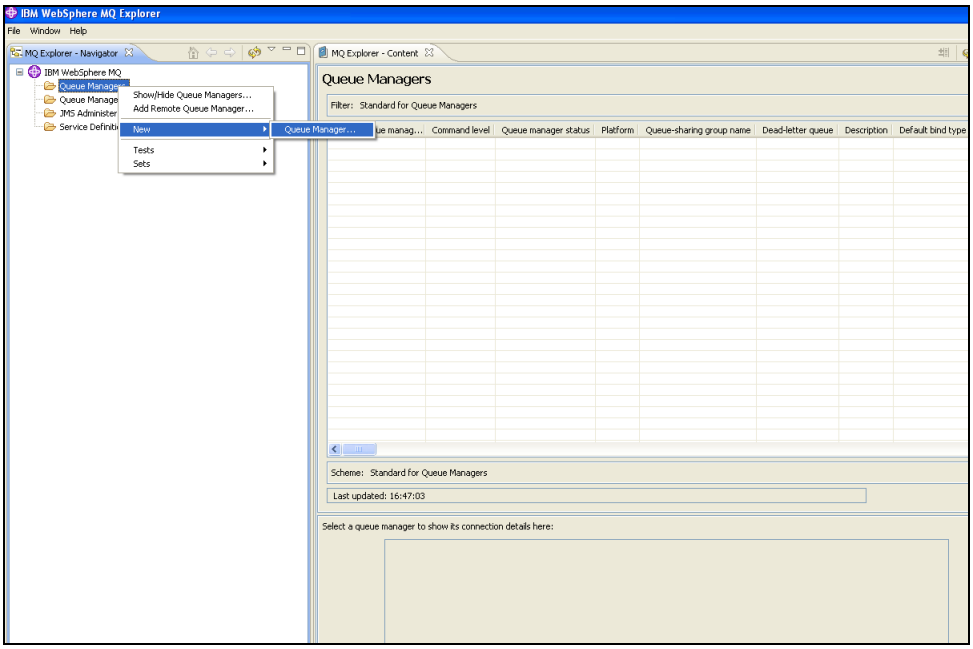
2.2.1 Creating Queue Manager through Console

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

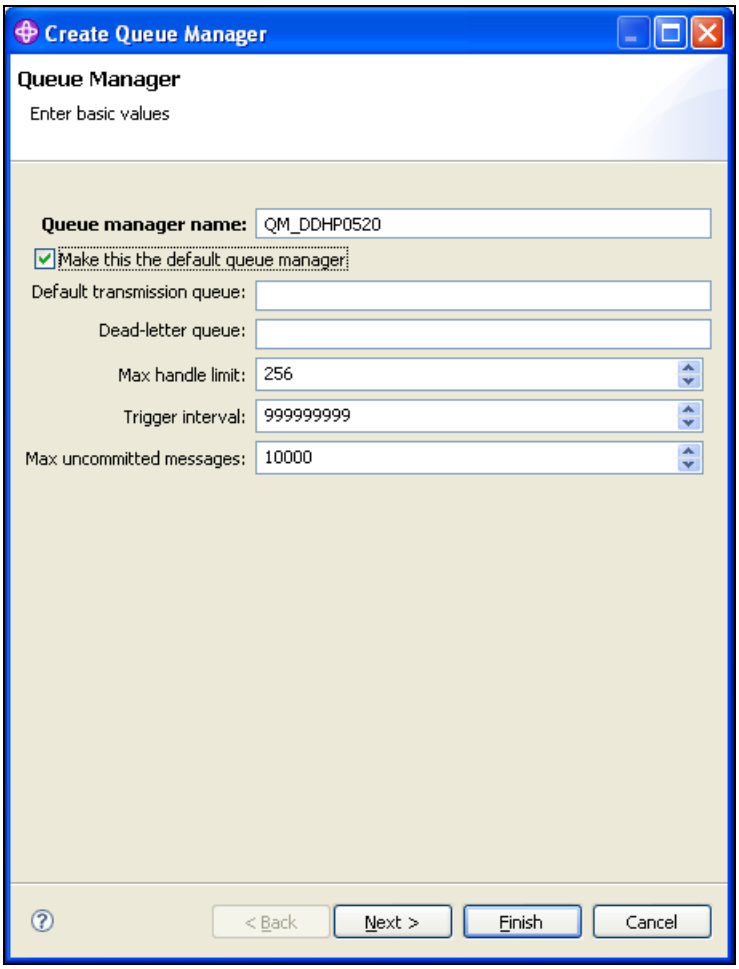
1. Start MQ server console.



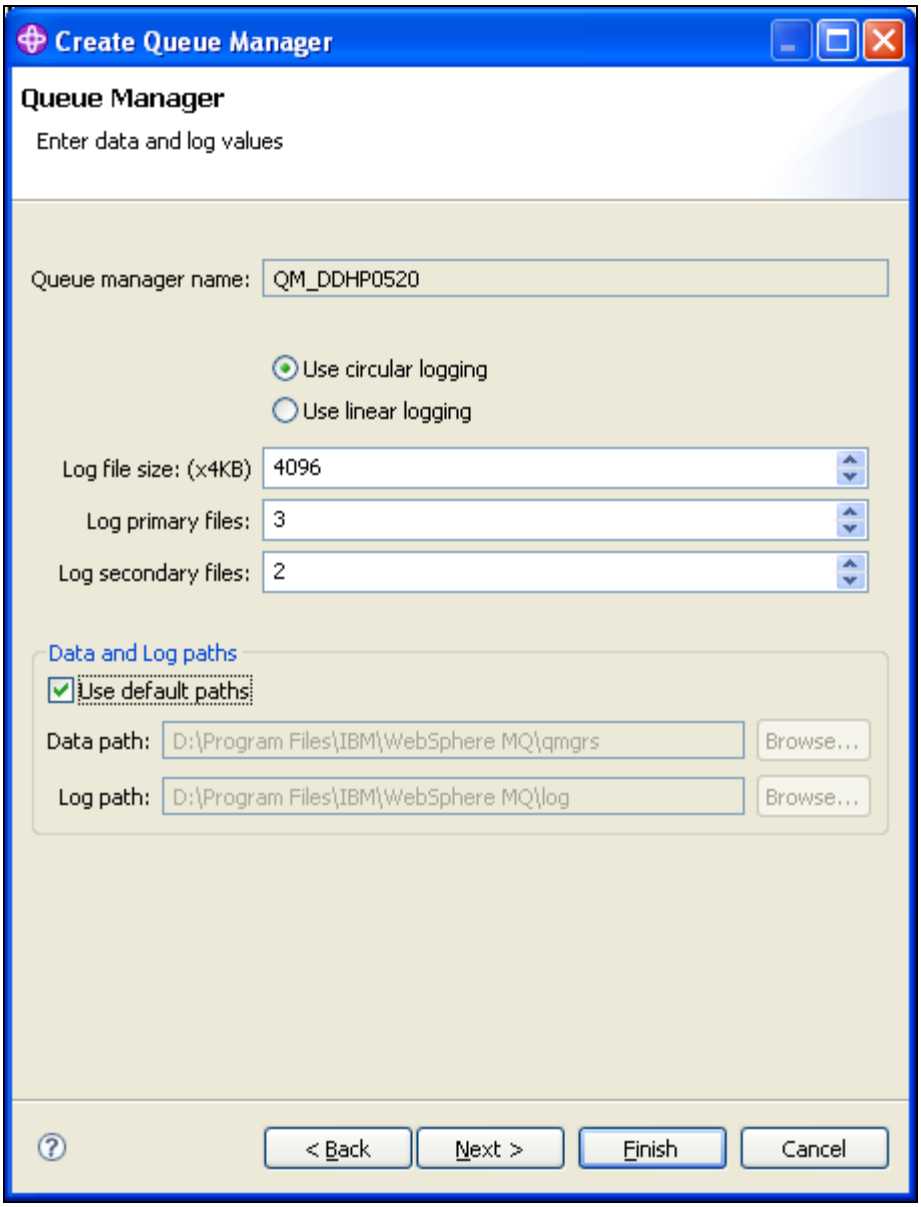
2. On the left pane, go to 'IBM Websphere MQ > Queue Manager > New > Queue Manager' as shown below:



The following screen is displayed:

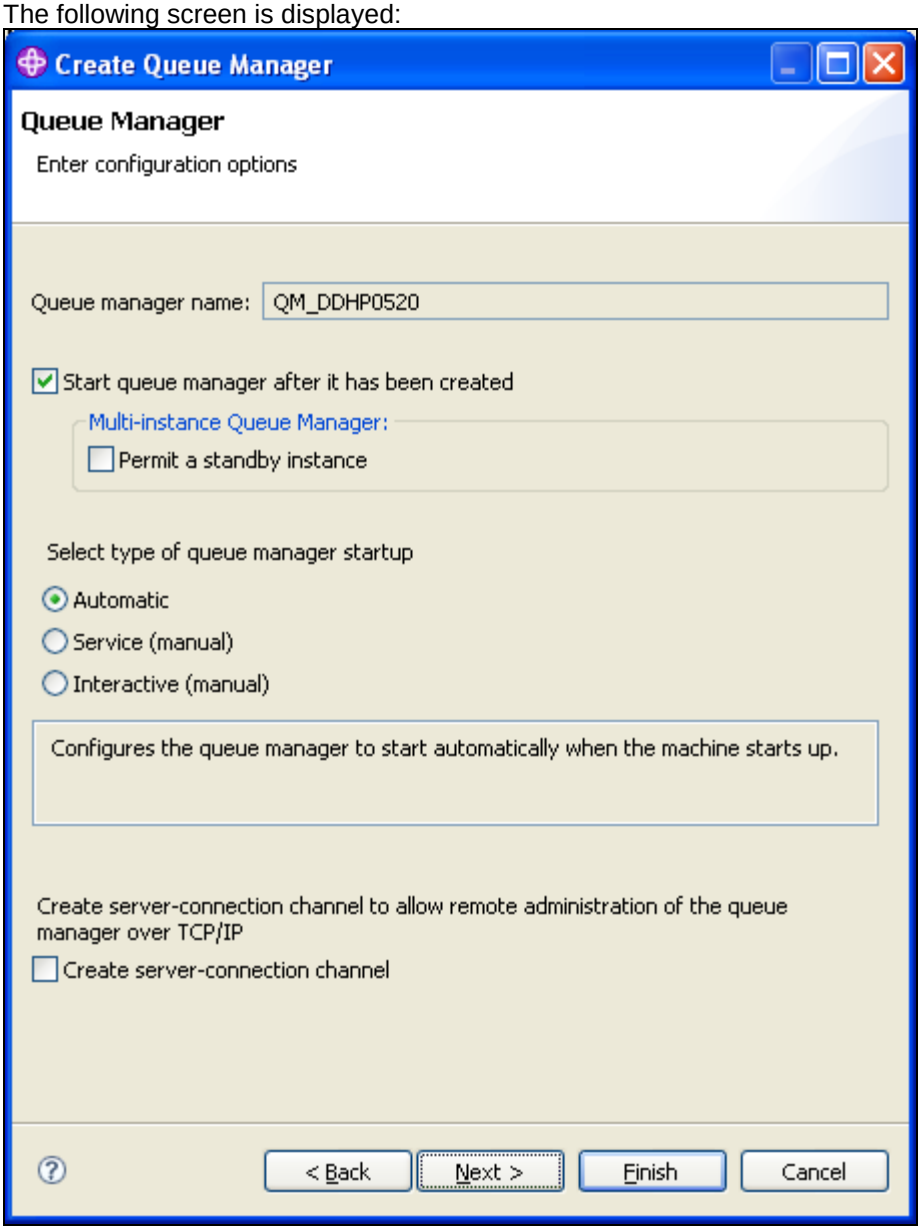


3. Specify the ‘Queue manager name’. Check the box ‘Make this the default queue manager’.
4. Click ‘Next’. The following screen is displayed:


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

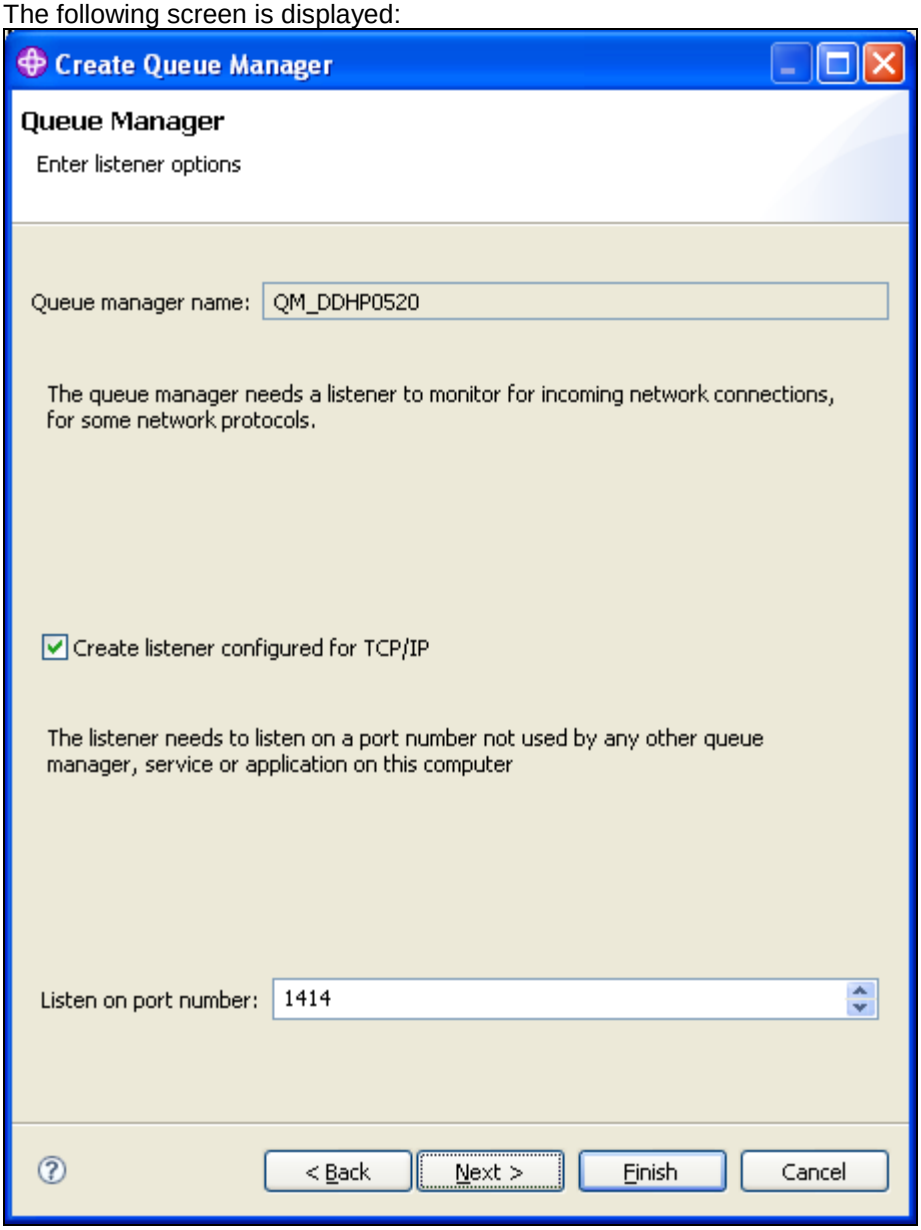
5. Click ‘Next’.

The following screen is displayed:



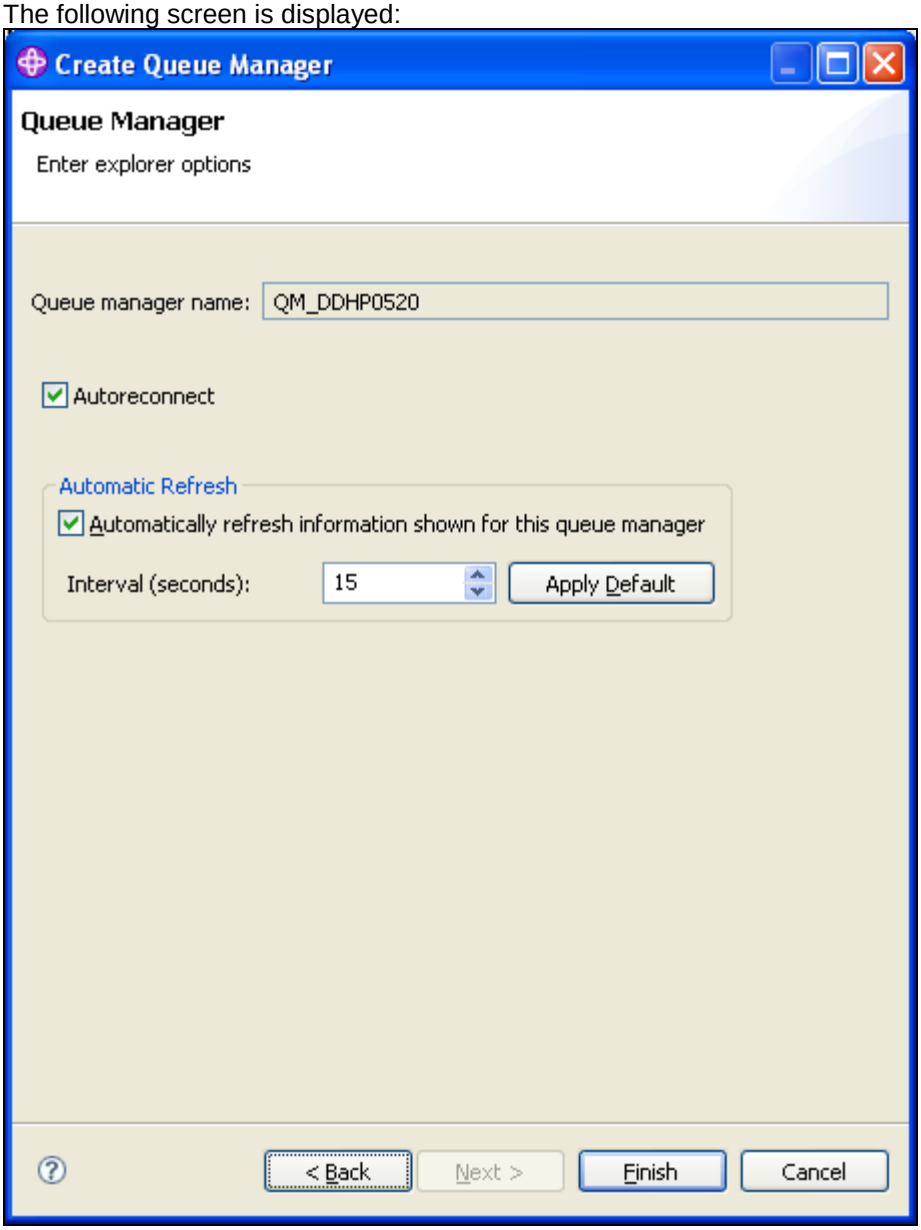
6. Click ‘Next’.

The following screen is displayed:



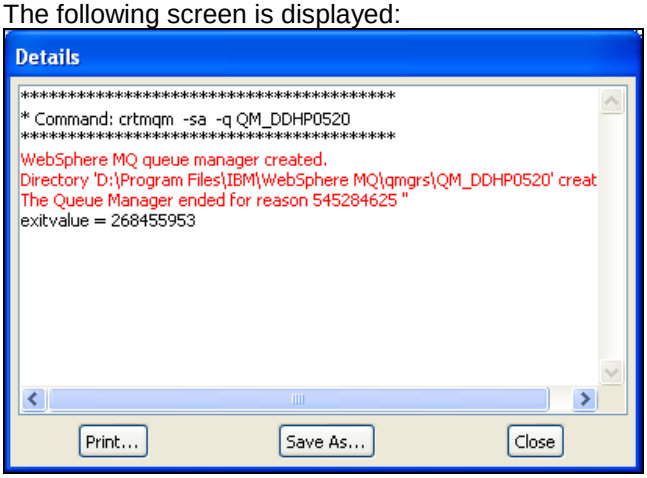
7. Specify the ‘Listen on port number’ as ‘1414’ (default). Click ‘Next’

The following screen is displayed:

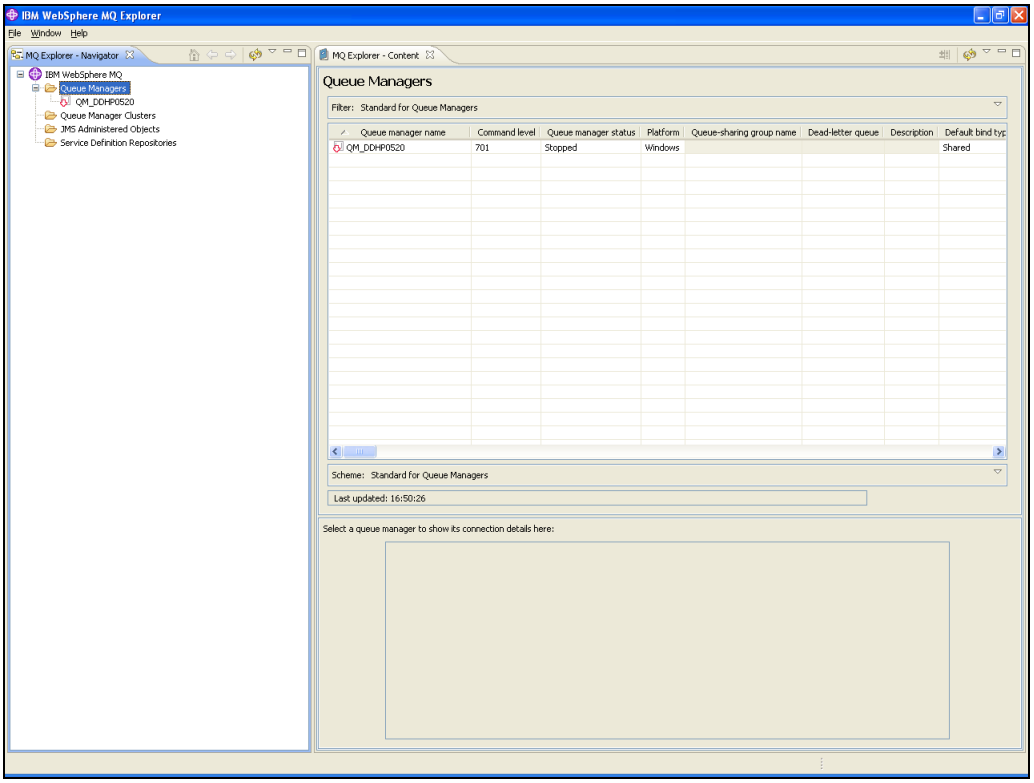


8. Click ‘Finish’.

The following screen is displayed:

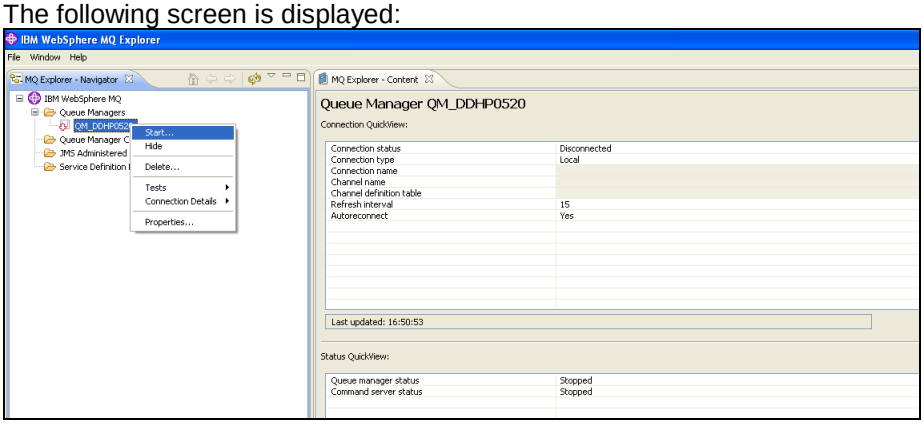


9. Close the message. The following screen is displayed:

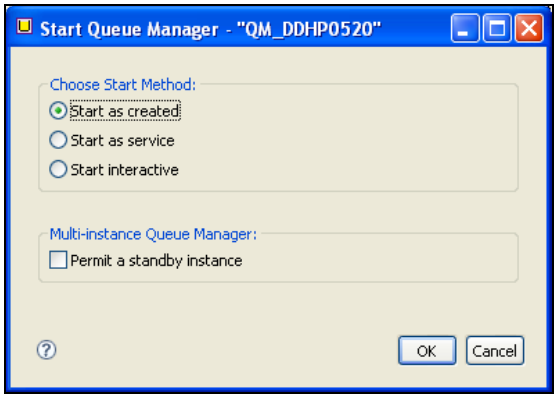


10. Right click ‘Queue Manager’ and select ‘Start’.

The following screen is displayed:

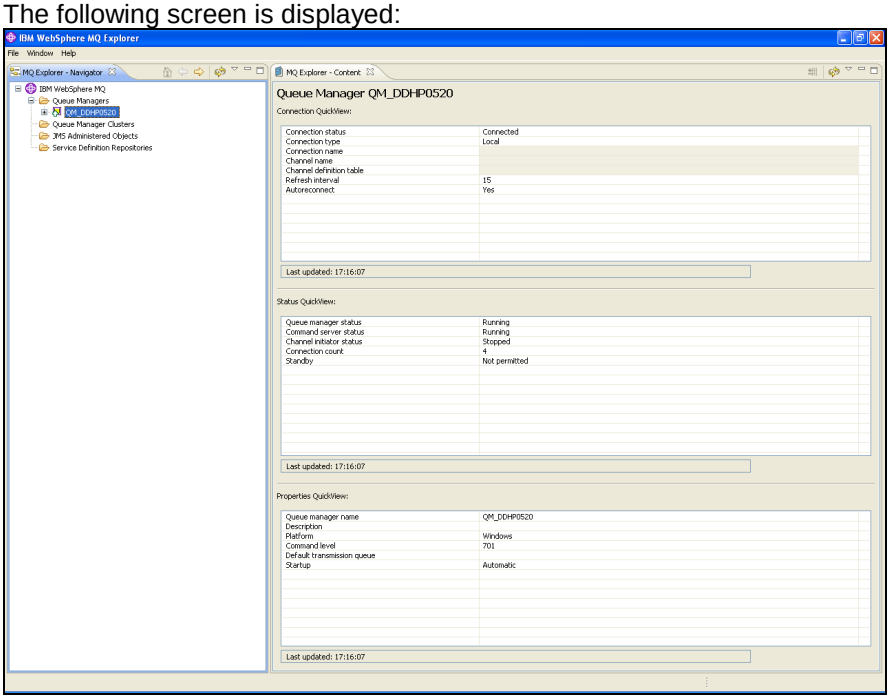


11. Right click ‘Queue Manager QM_DDHP0520’ and select ‘Start’. The following screen is displayed:



12. Click ‘OK’.

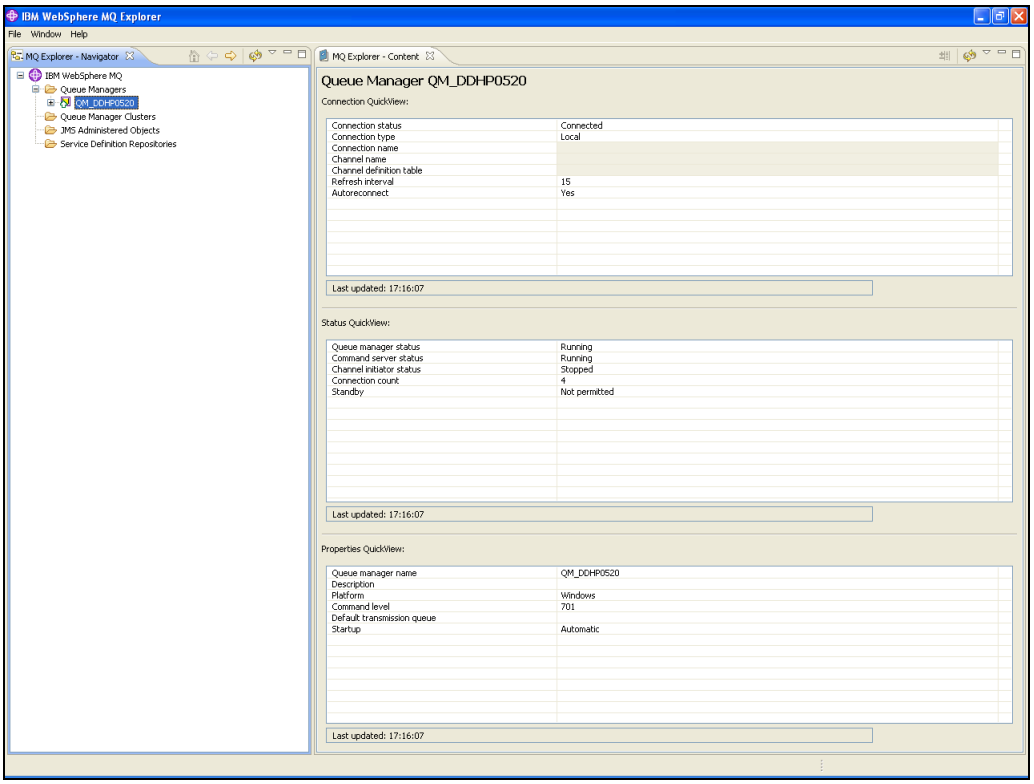
The following screen is displayed:



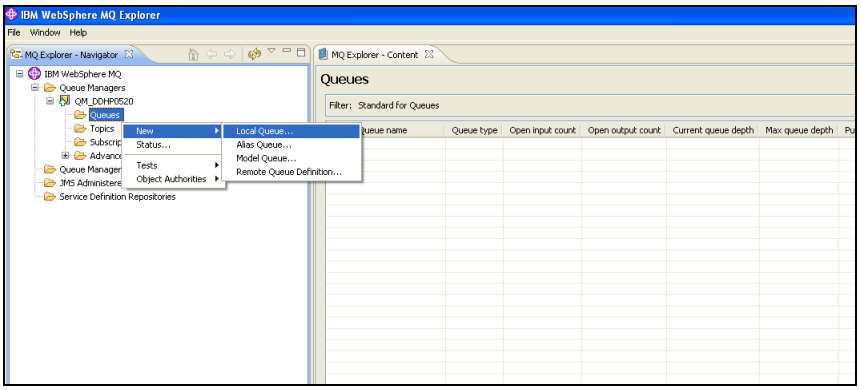
2.2.2 Creating Queues

To create queues, follow the steps given below:

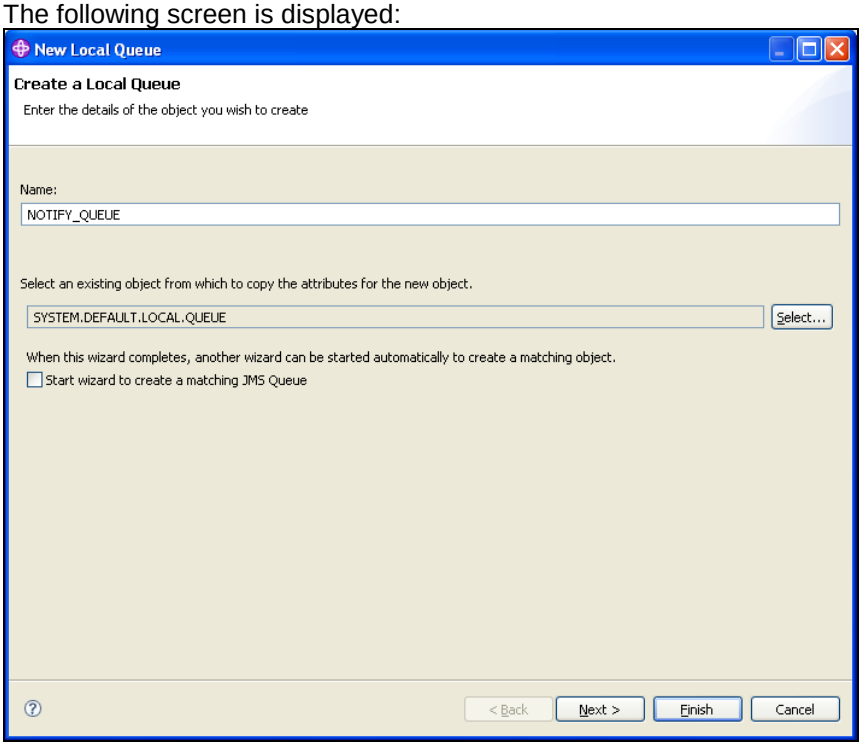
1. Start MQ server console.



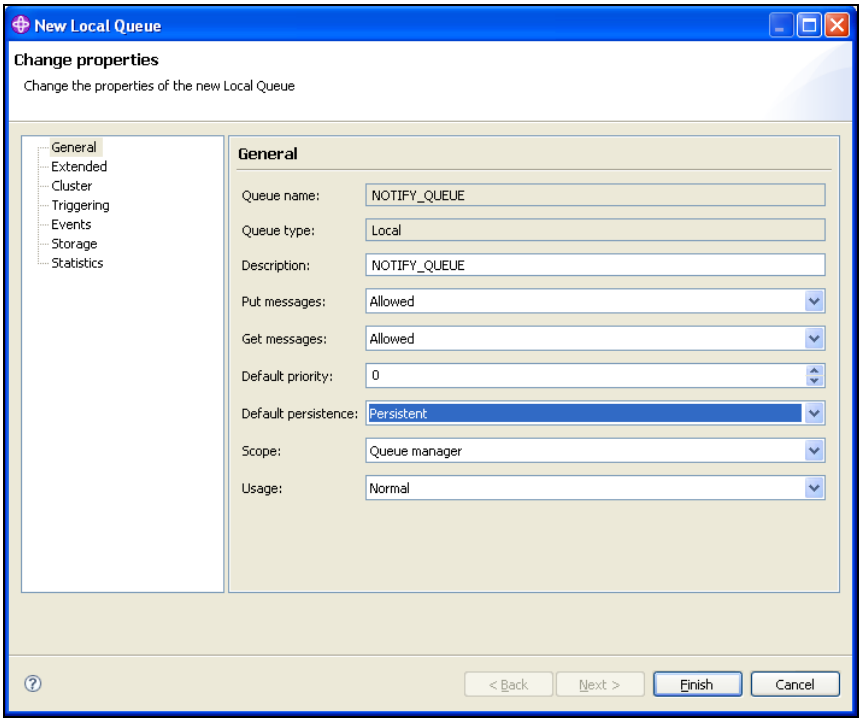
2. On the left pane, go to 'IBM Websphere MQ > Queue Managers > QM_DDHP0520 > Queues > New > Local Queue' as shown below.



The following screen is displayed:

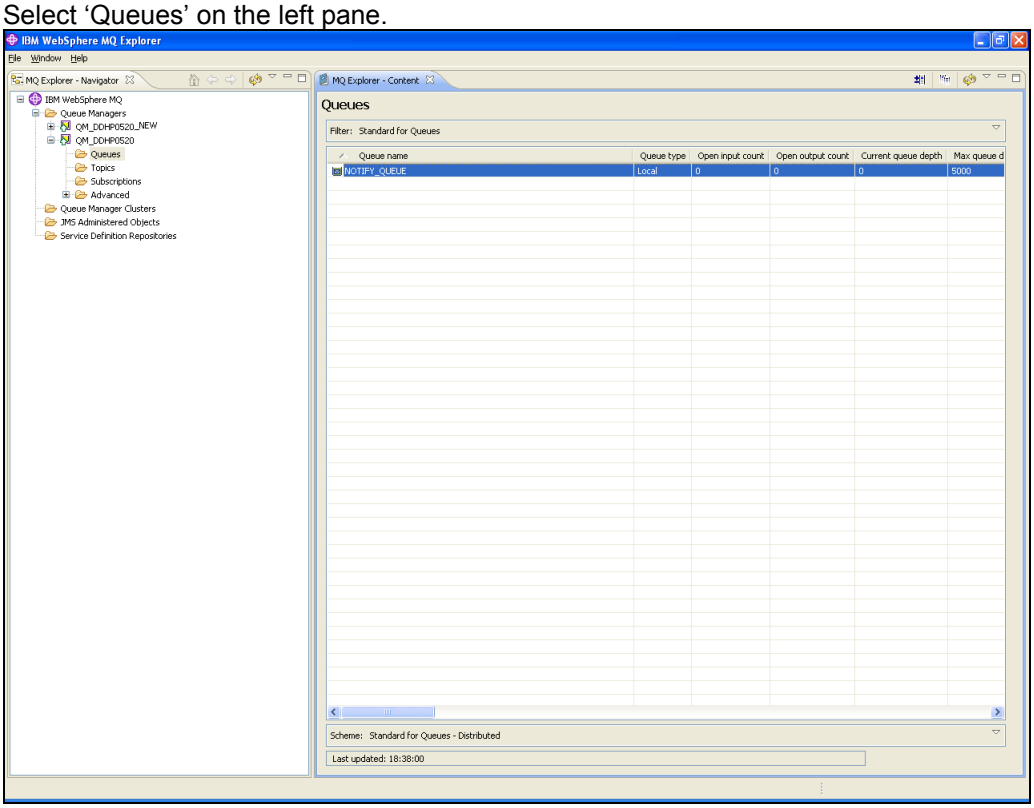


3. Specify the queue name. Click ‘Next’. The following screen is displayed:



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 stating 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

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.

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>'.

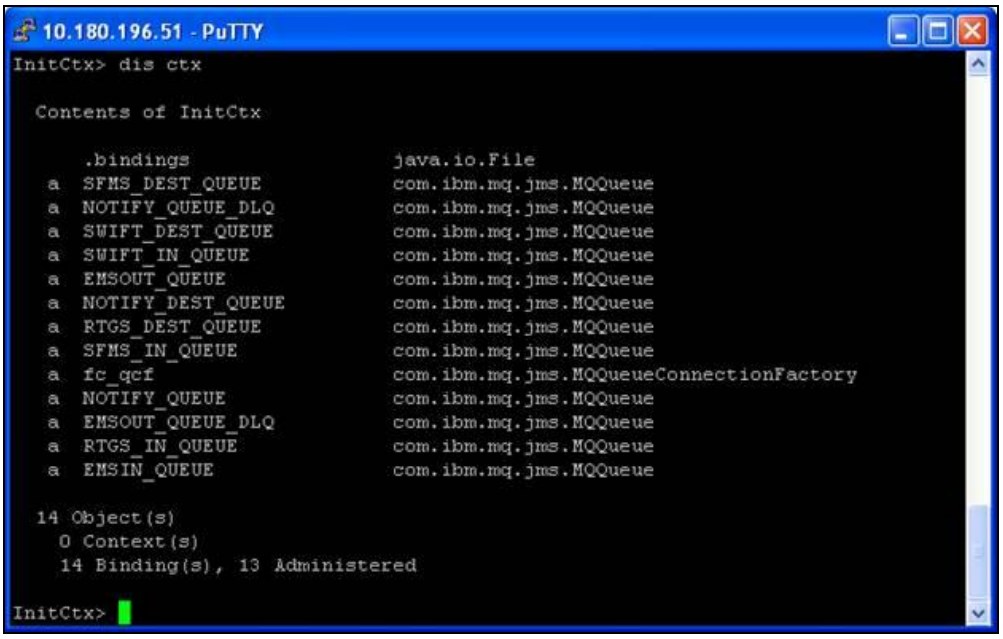
DEFINE Q(EMSOUT_QUEUE) QUEUE(EMSOUT_QUEUE) QMGR(FC_QMGR)

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.



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

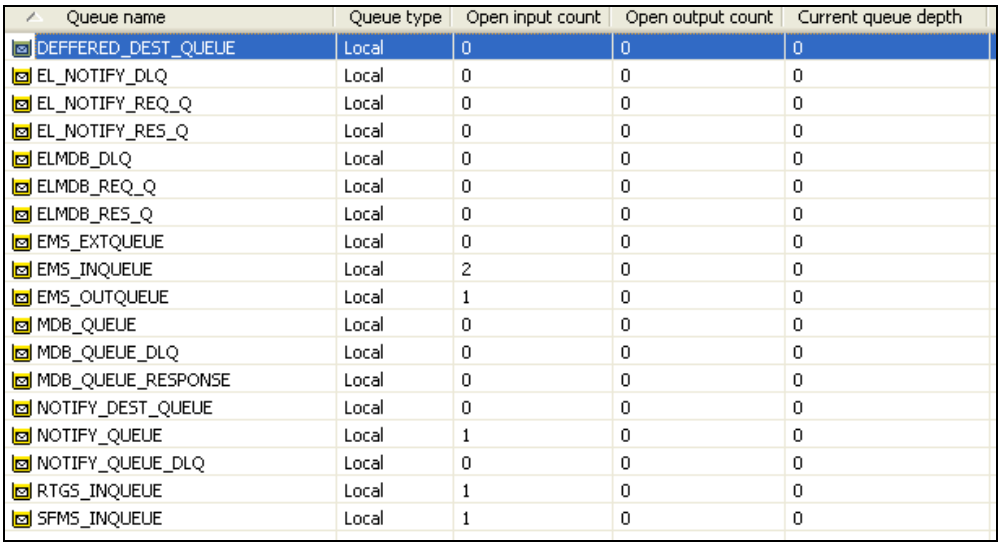
Now, you need to create JMS queues for DIRECT queues to post messages. DIRECT queues require connection to Oracle FLEXCUBE application.

Example

Following are the DIRECT queues:

- NOTIFY_QUEUE
- EMSIN_QUEUE
- EMSOUT_QUEUE
- SFMS_INQUEUE
- SFMSOUT_QUEUE
- RTGS_INQUEUE
- INTERNAL_BIPREPORT_QUEUE
- INTERNAL_BIP_QUEUE_DLQ
- INTERNAL_BIPADVREPORT_QUEUE
- INTERNAL_BIP_ADVICE_QUEUE_DLQ
- INTERNAL_GI_UPLOAD_QUEUE
- INTERNAL_GI_UPLOAD_DLQ
- EMS_QUEUE_DLQ

You need to create JMS queues for the above queues as shown in the figure:



Queue name	Queue type	Open input count	Open output count	Current queue depth
DEFFERED_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)

- b) Allow MQ Privileged Users to access Channel

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

- c) 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.

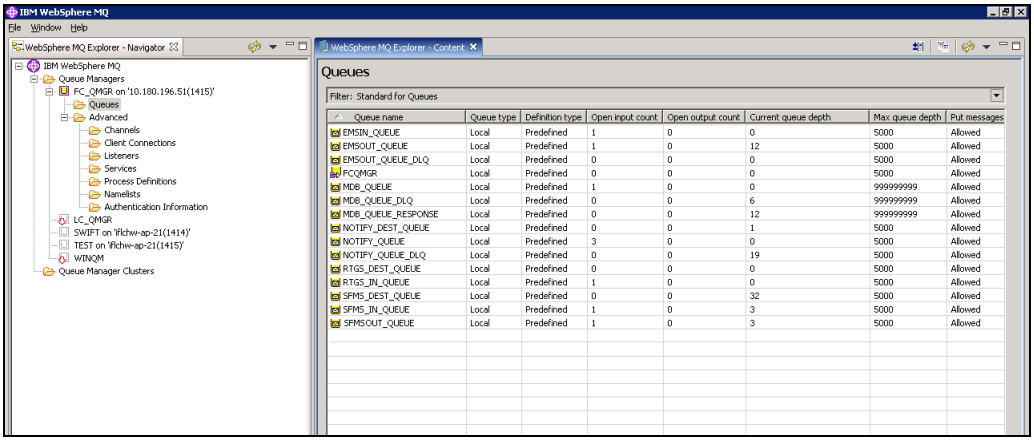
Follows the below steps to view the queues created in server, from an MQ client:

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.

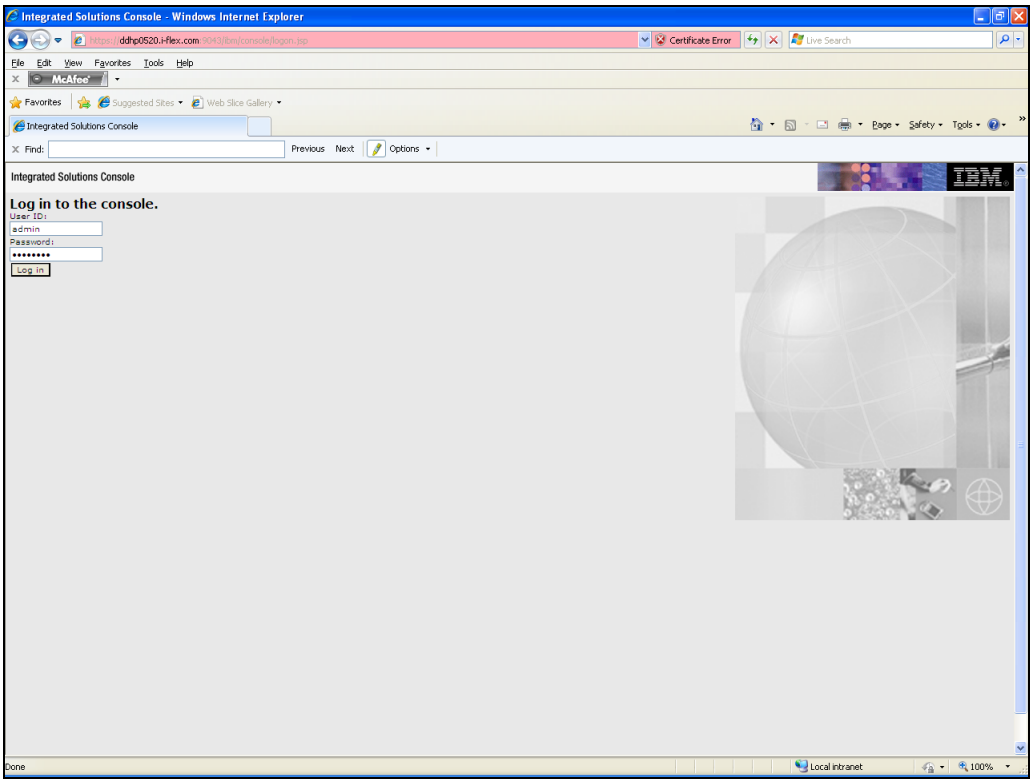


3. Creating JDBC Resources on Web Sphere

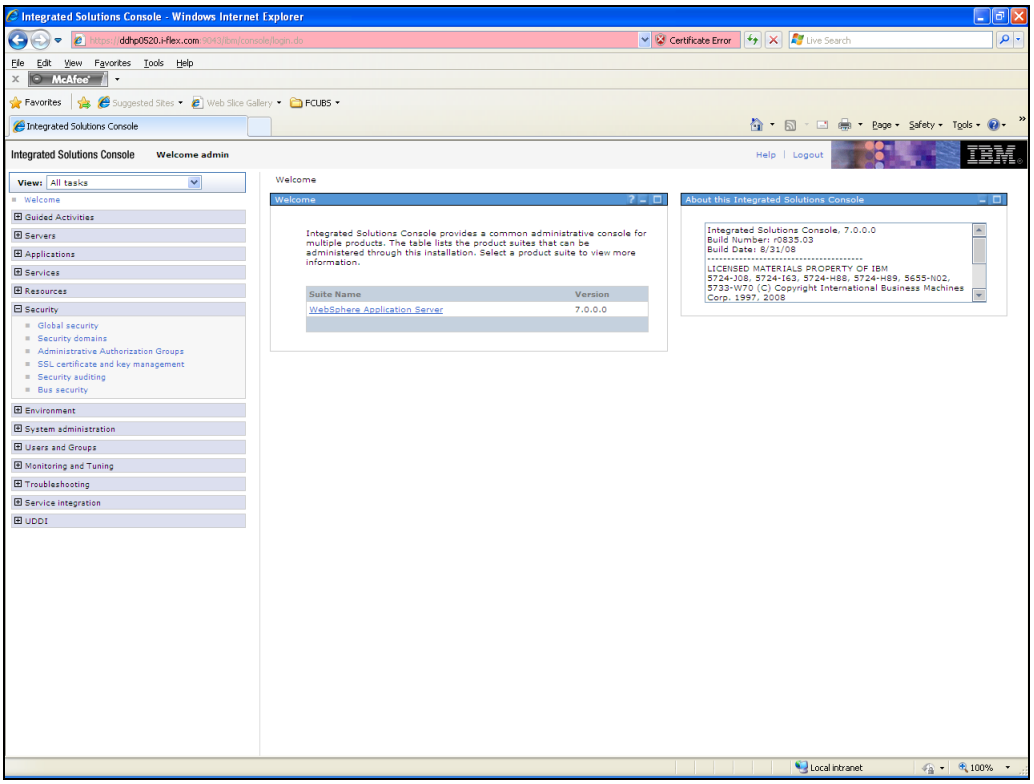
3.1 Introduction

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

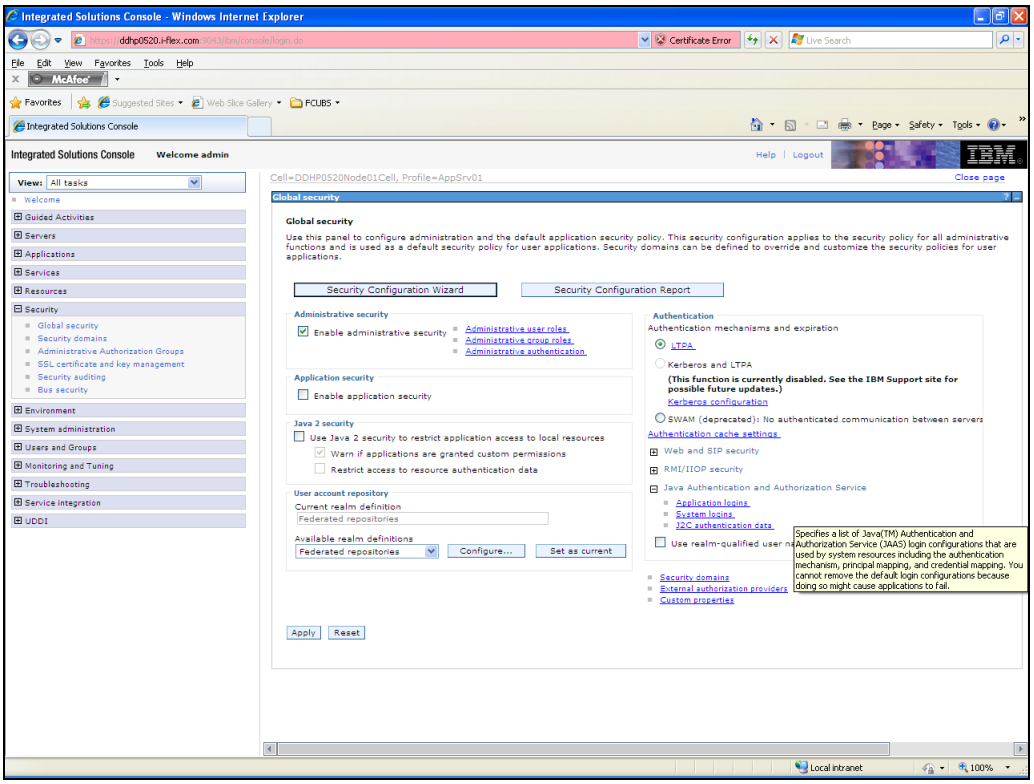
3.2 Creating JDBC Sources



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

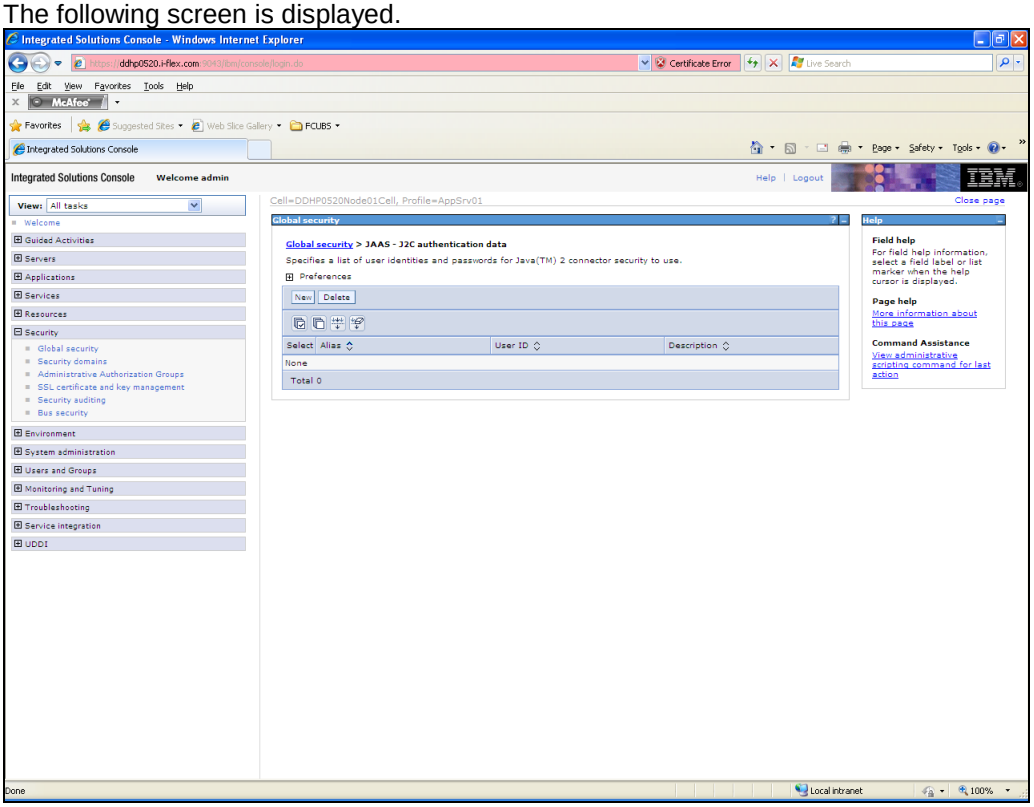


4. Expand ‘Security’ and select ‘Global Security’. The following screen is displayed.



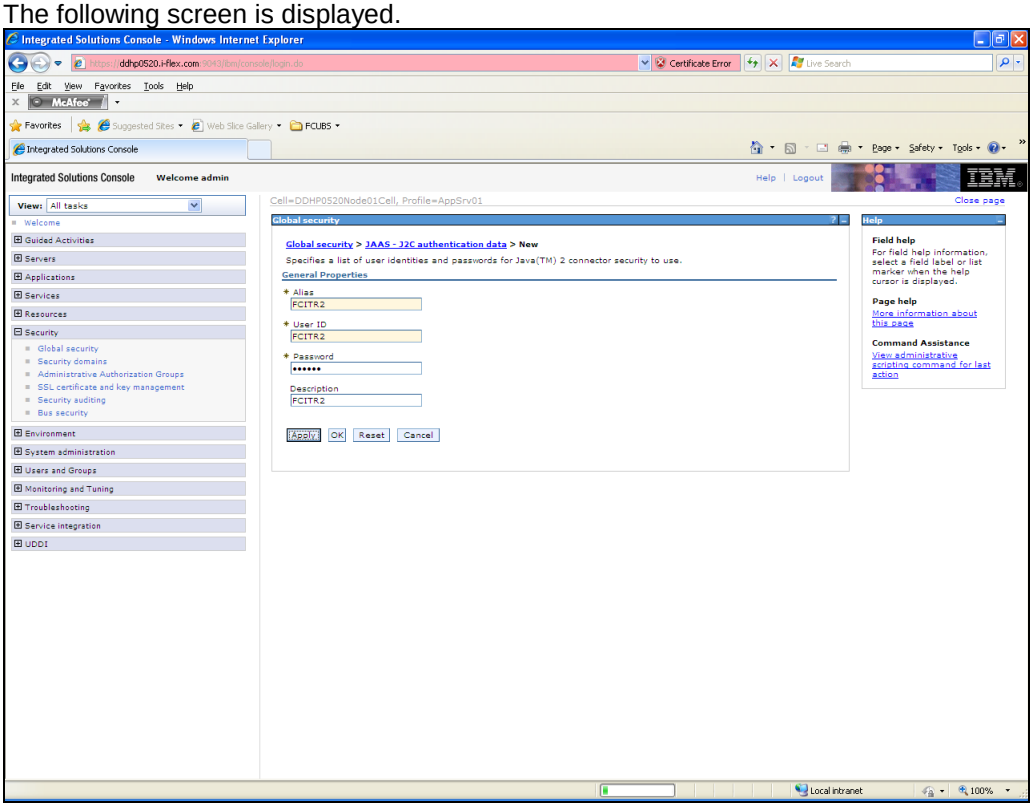
5. Expand ‘Java Authentication’, go to ‘Authorization Service’ and click ‘J2C authentication data’.

The following screen is displayed.



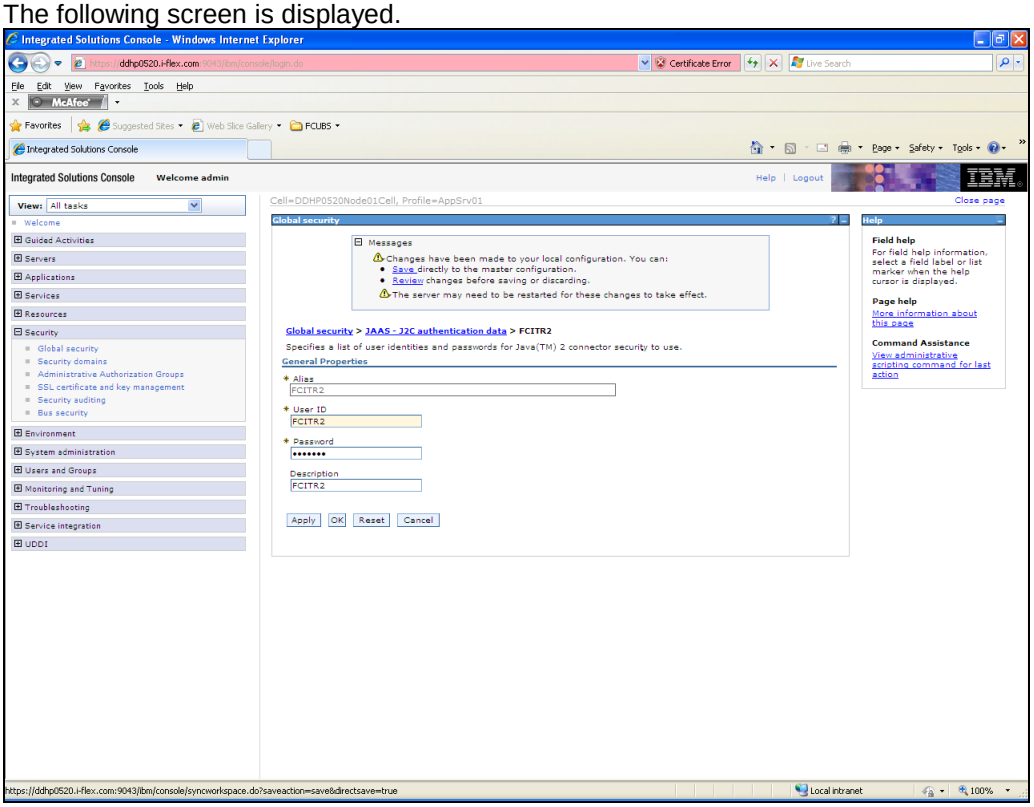
6. Click ‘New’.

The following screen is displayed.



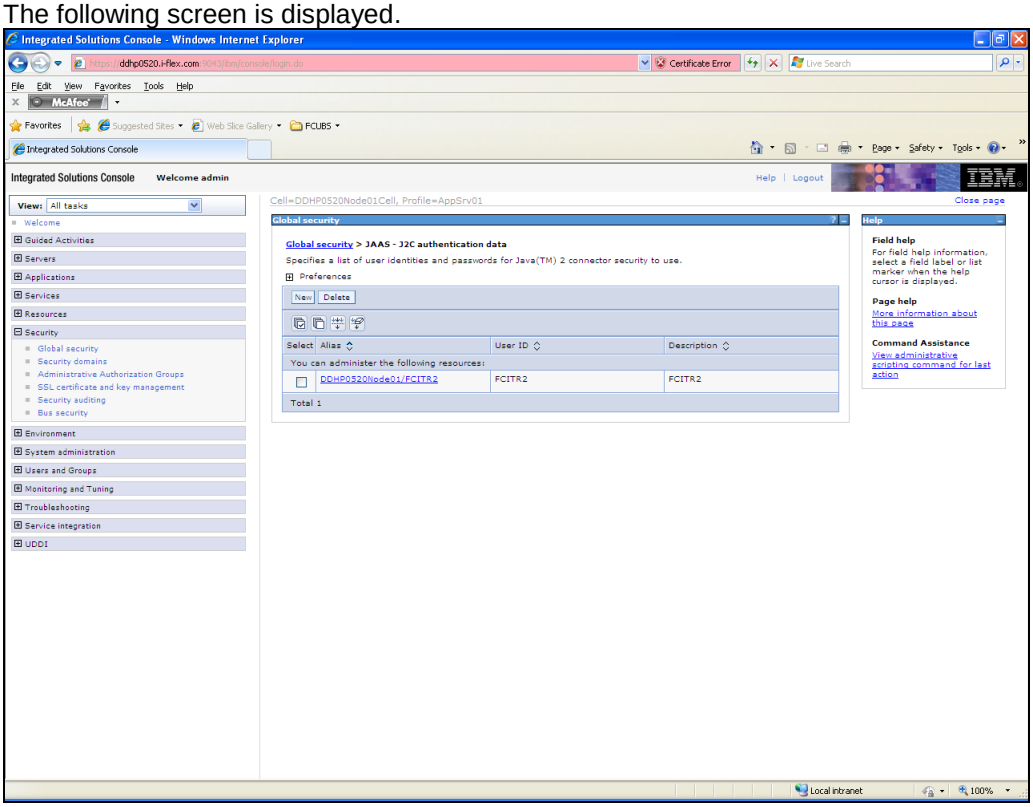
7. You need to define the connection properties. Specify the following details.
   - Alias
   - User ID of the Database
   - Password of the Database
   - Description
8. Once you have specified the above details, click ‘Apply’.

The following screen is displayed.



9. Click ‘Save’.

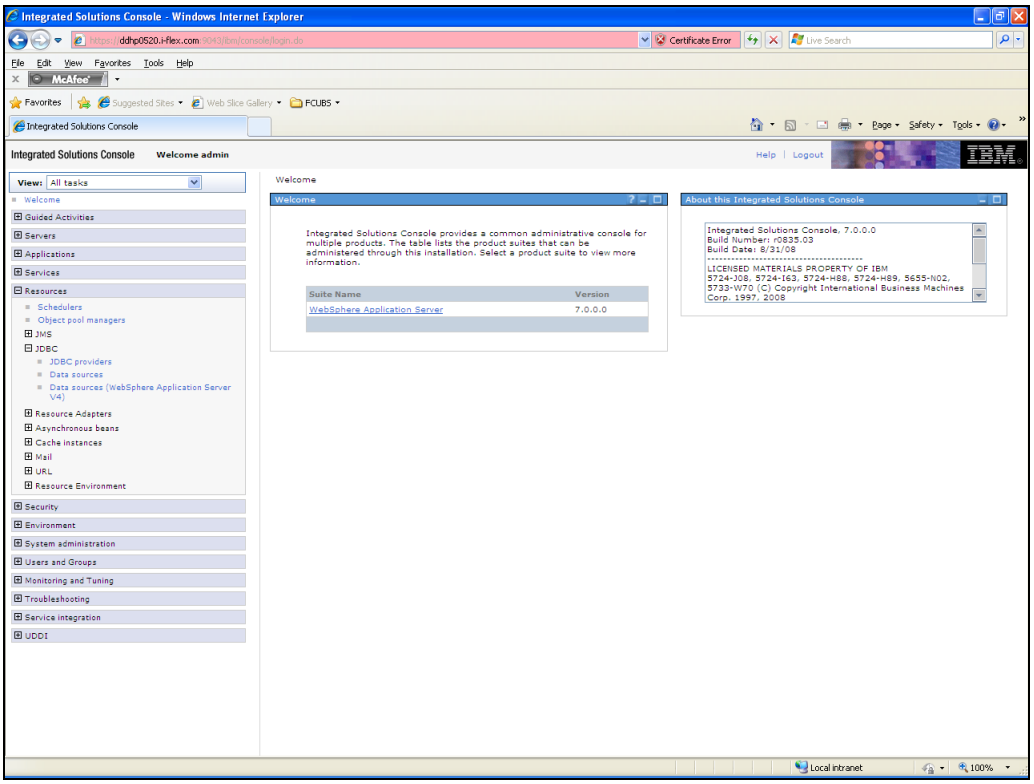
The following screen is displayed.



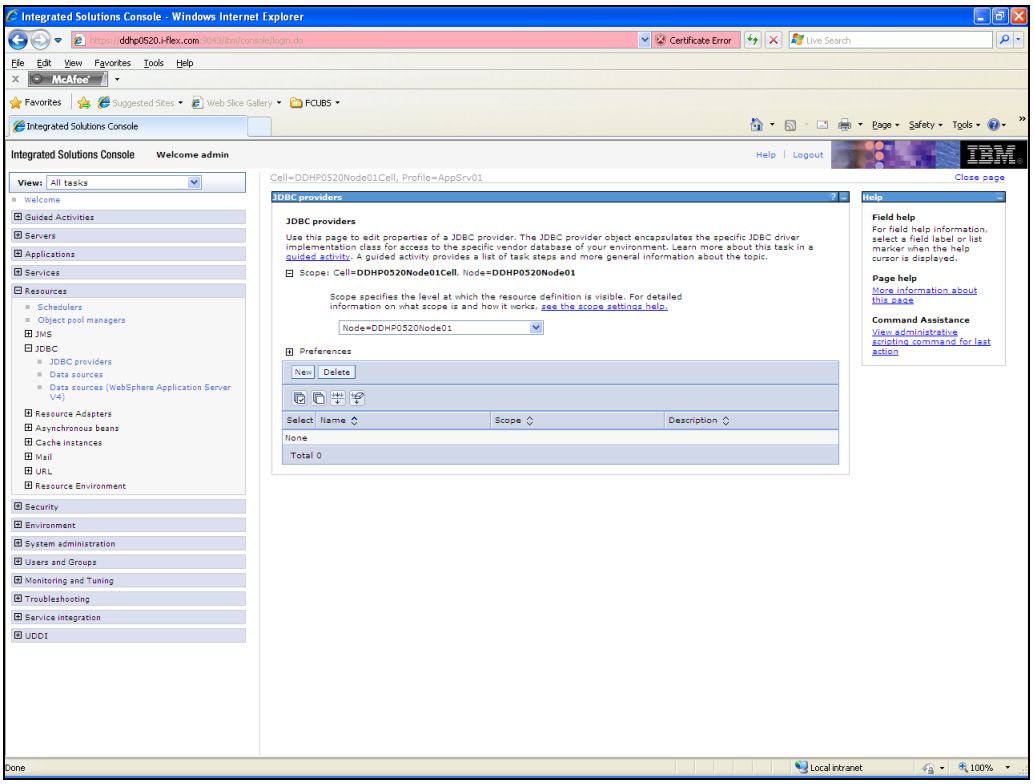
3.2.1 JDBC Provider for Non XA Data Source

Follow the steps given below:

10. Login to the application server administration console.
11. Expand ‘Resources > JDBC’ and select ‘JDBC Providers’.

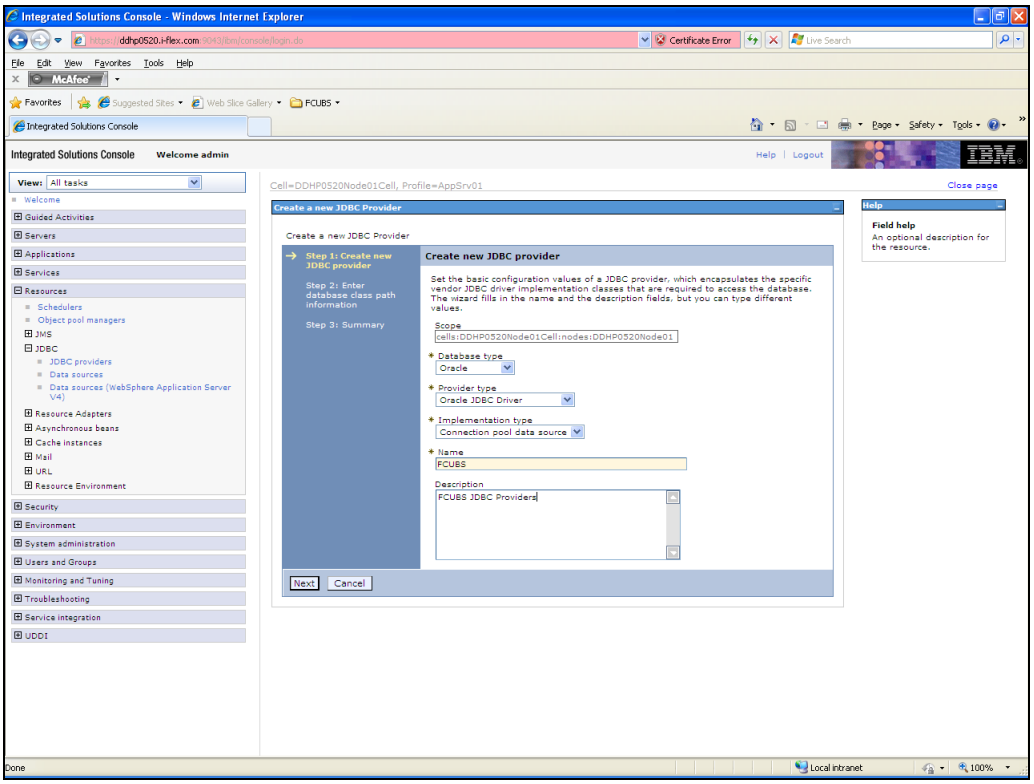


12. The following screen is displayed:



13. Select ‘Node’ from the dropdown list.

14. The following screen is displayed:

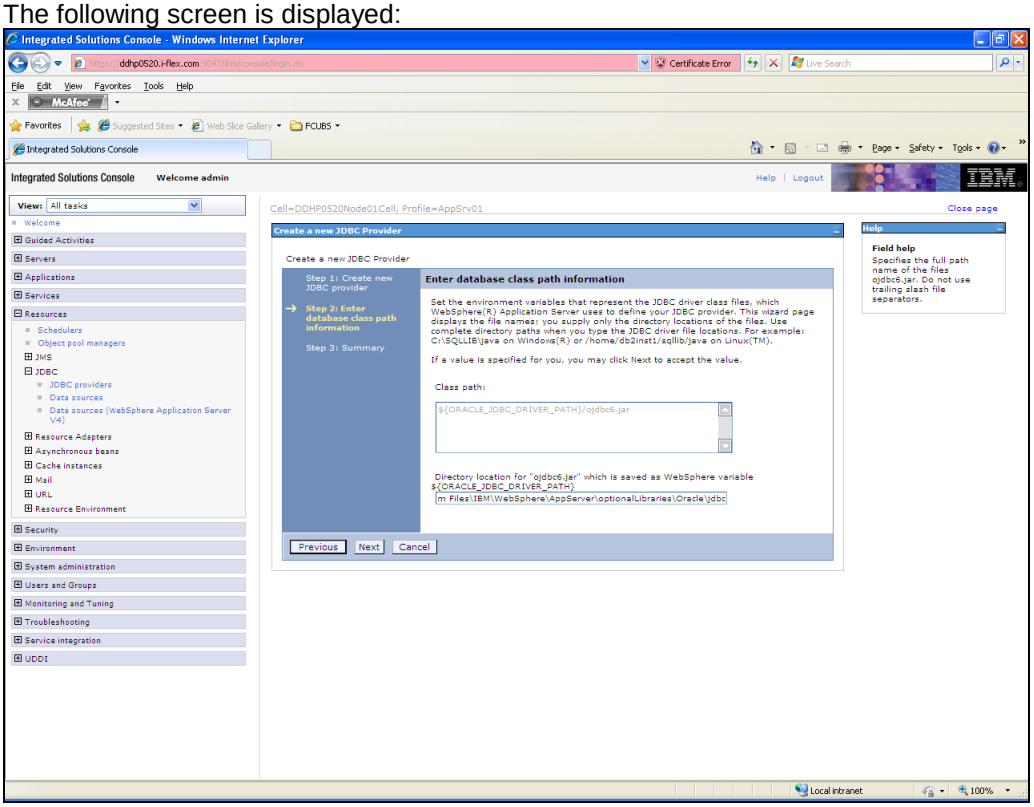


15. Specify the following details:

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

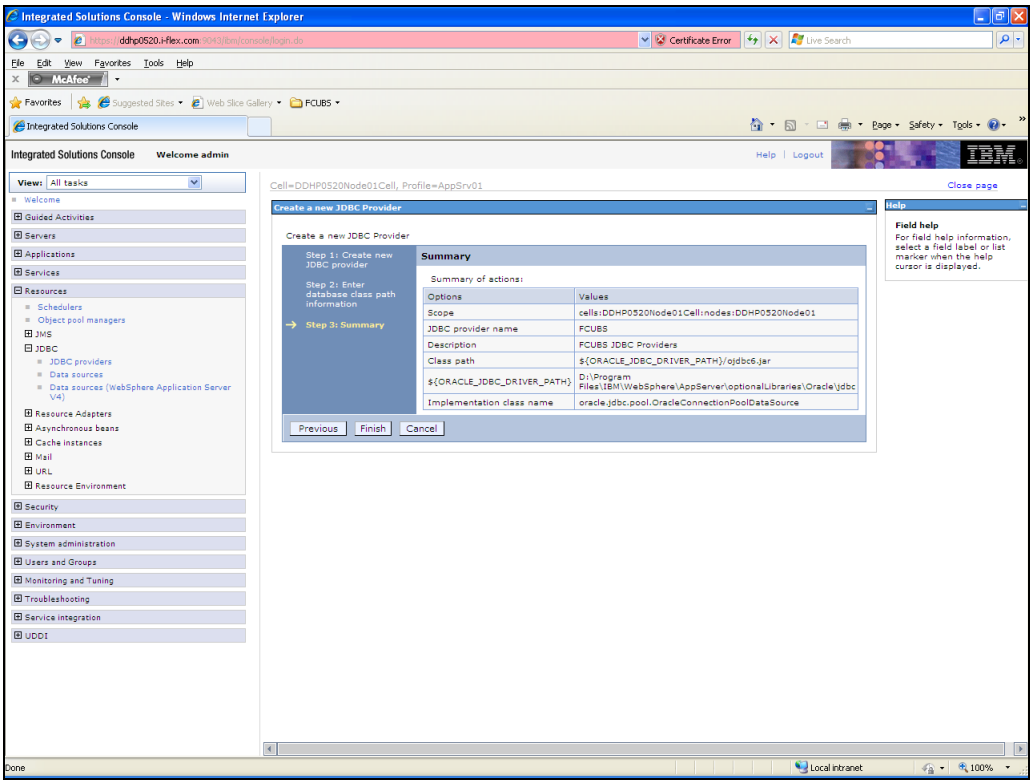
16. Click ‘Next’.

The following screen is displayed:



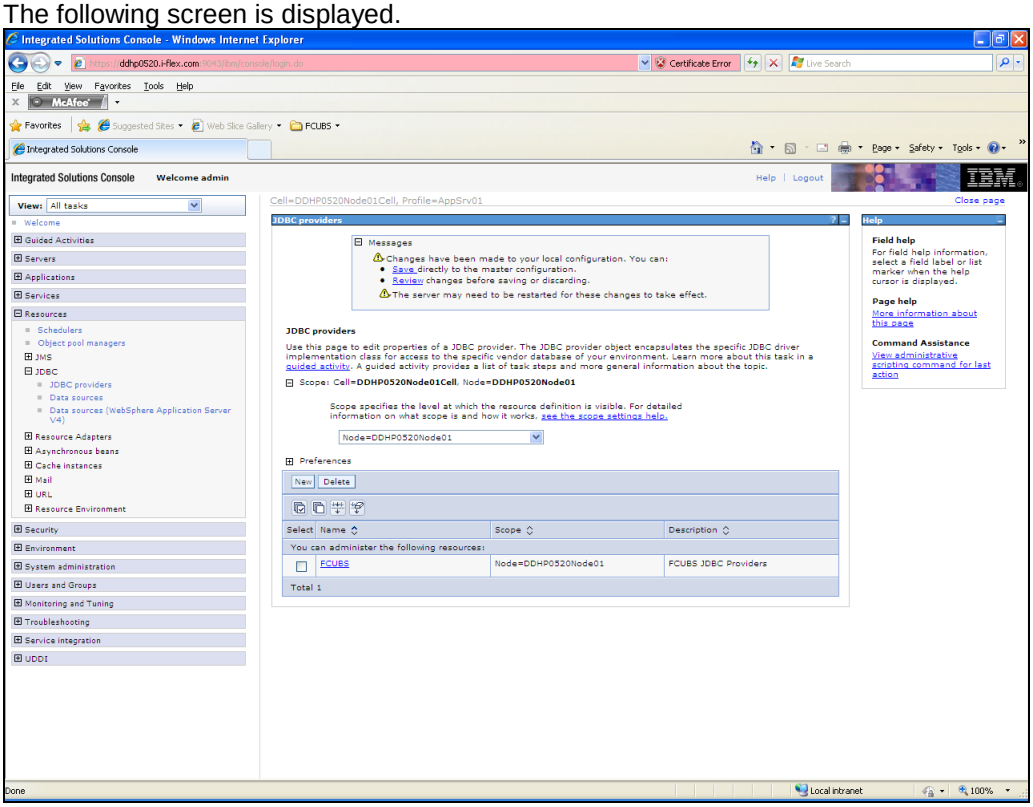
17. Provide the location of ojbc6.jar. Click ‘Next’.

The following screen is displayed.



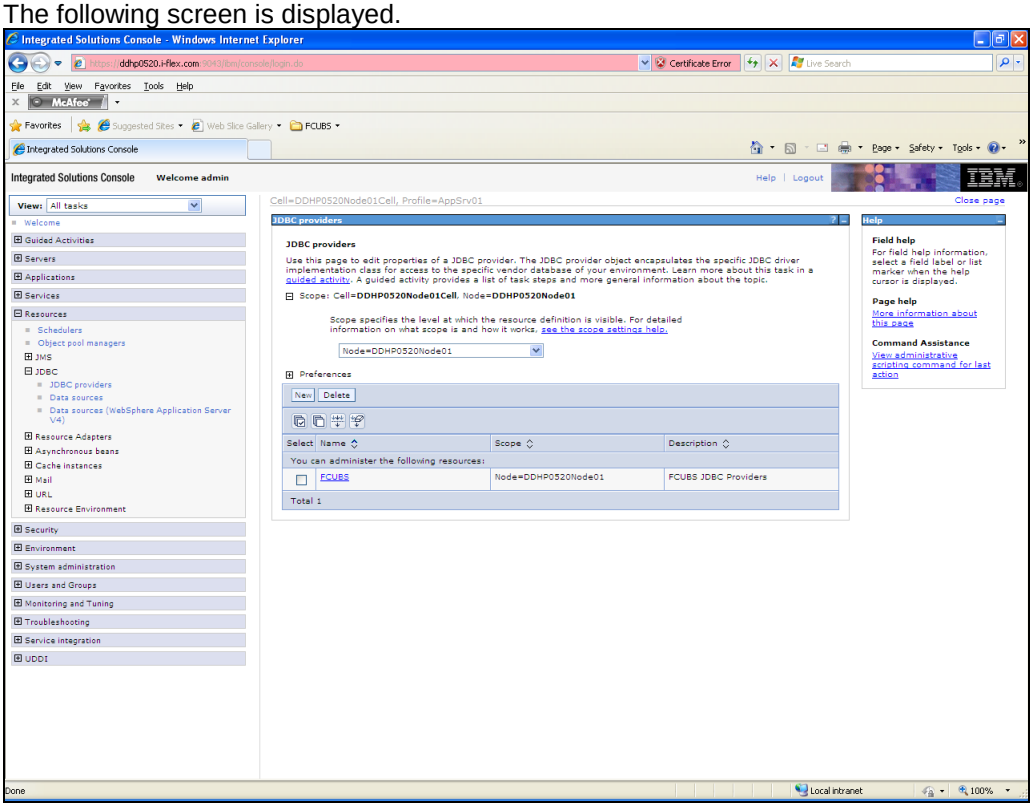
18. Click ‘Finish’.

The following screen is displayed.



19. Click ‘Save’.

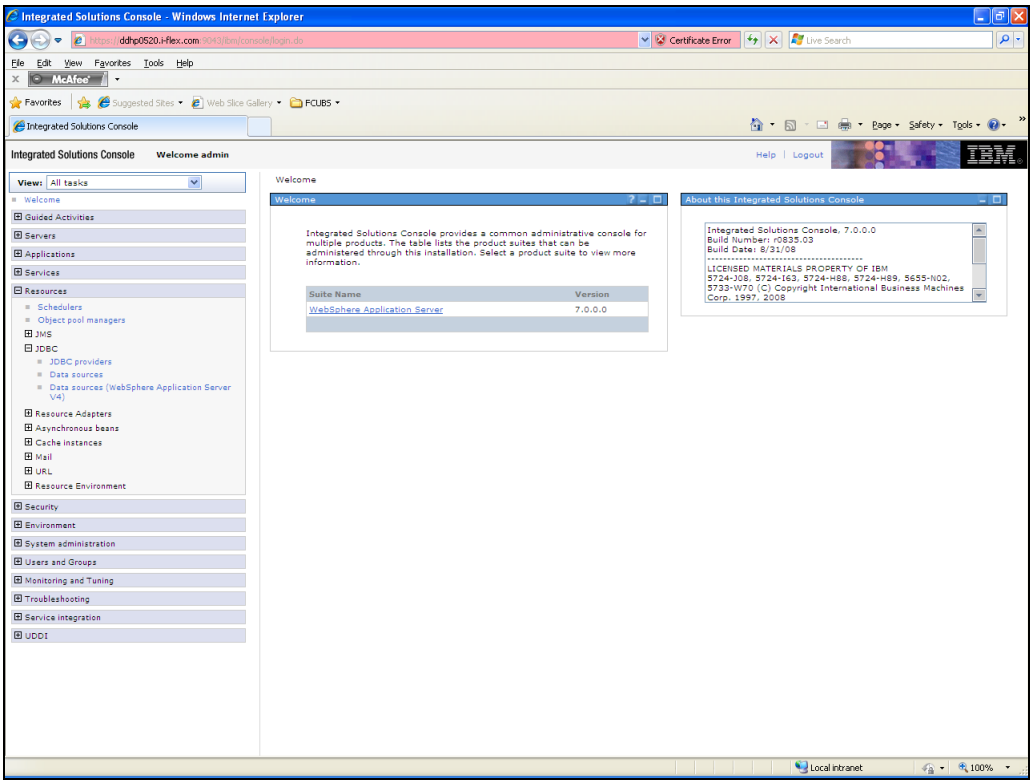
The following screen is displayed.



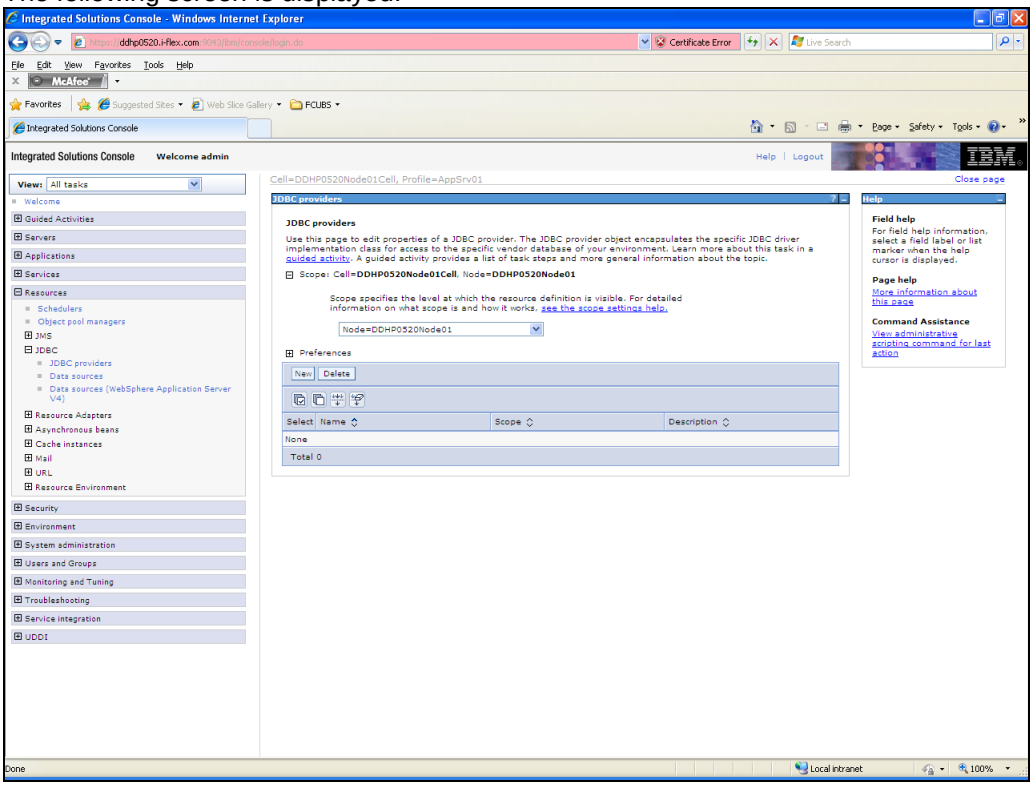
3.2.2 Creating Non XA Data Source

Follow the steps given below:

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

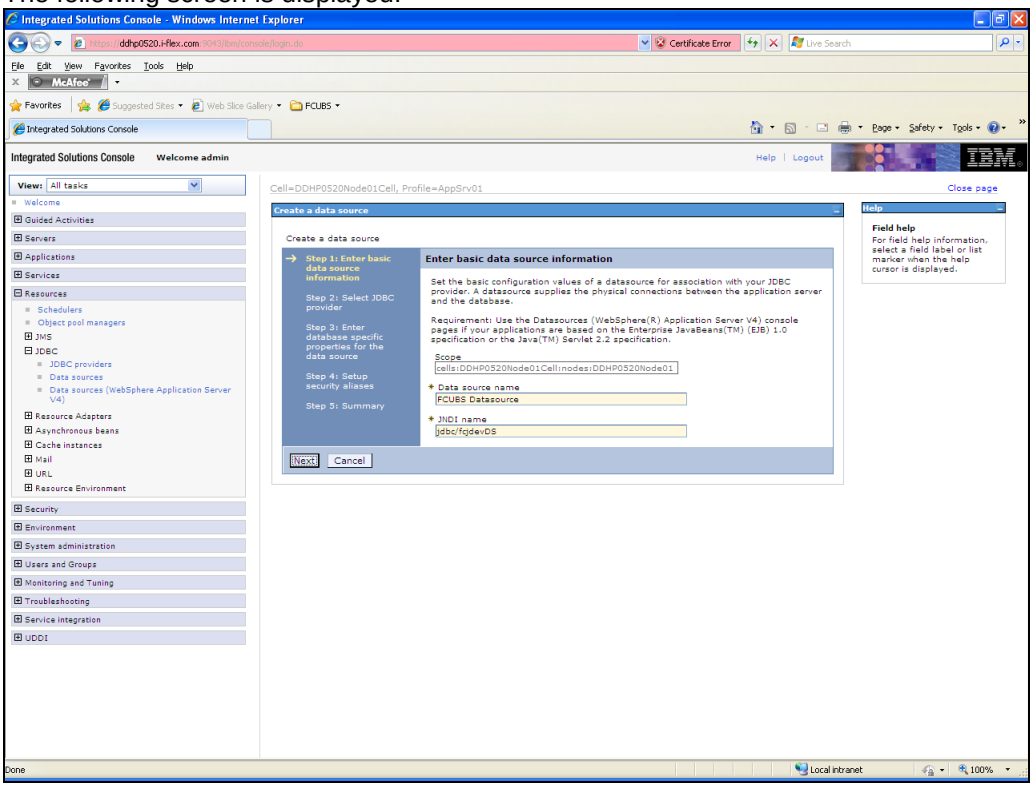


The following screen is displayed.



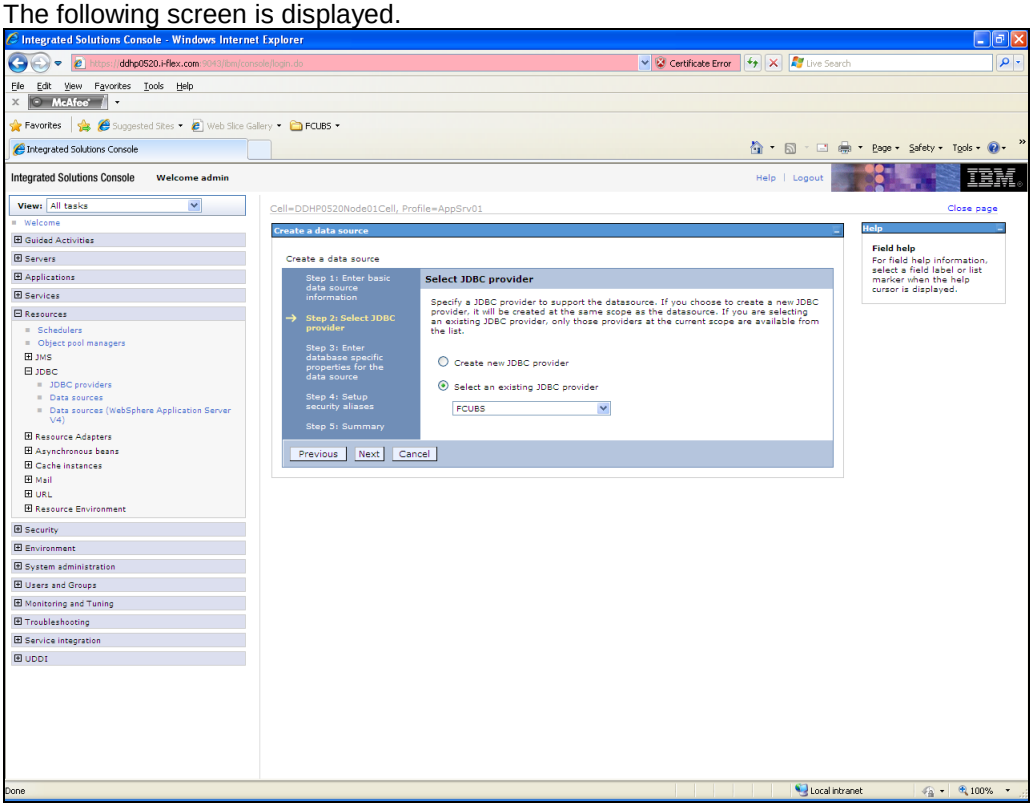
3. Select ‘Node’ from the drop-down list.

The following screen is displayed.



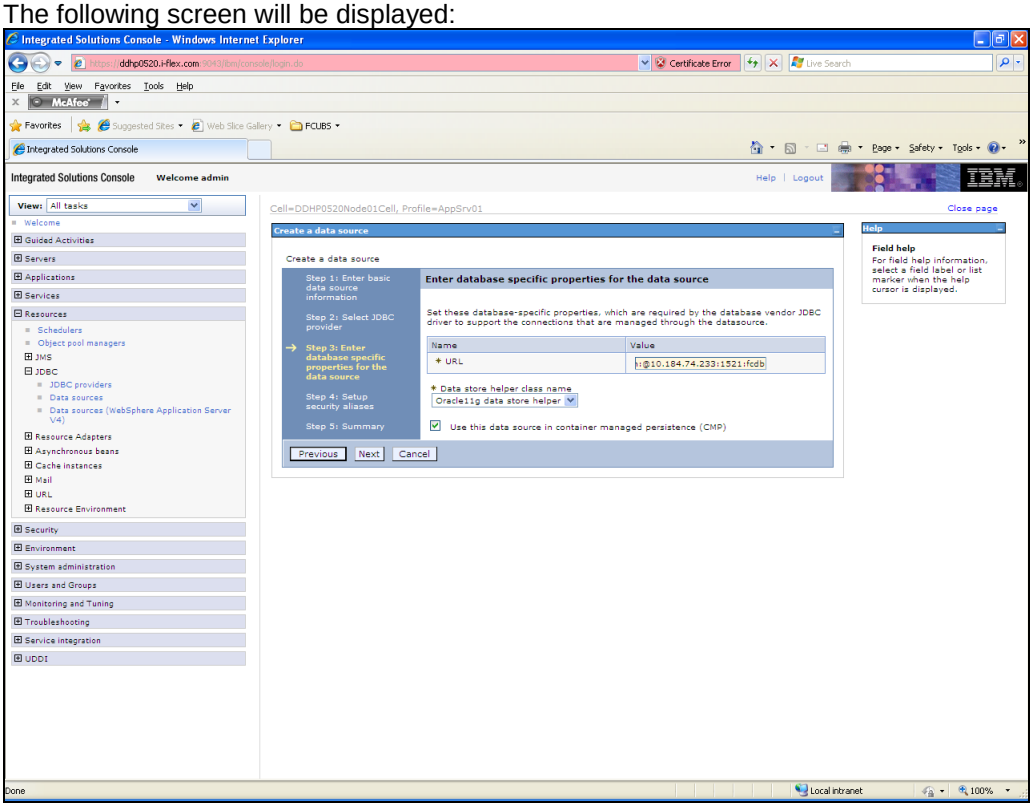
4. Specify the data source name as ‘FCUBS Data source’.
5. Specify the JNDI name as ‘jdbc/fcjdevDS’.
6. Click ‘Next’.

The following screen is displayed.



7. Select the option ‘Select an existing JDBC provider’. From the drop-down list, choose ‘FCUBS’.

The following screen will be displayed:



8. Specify the URL of the Database

Example

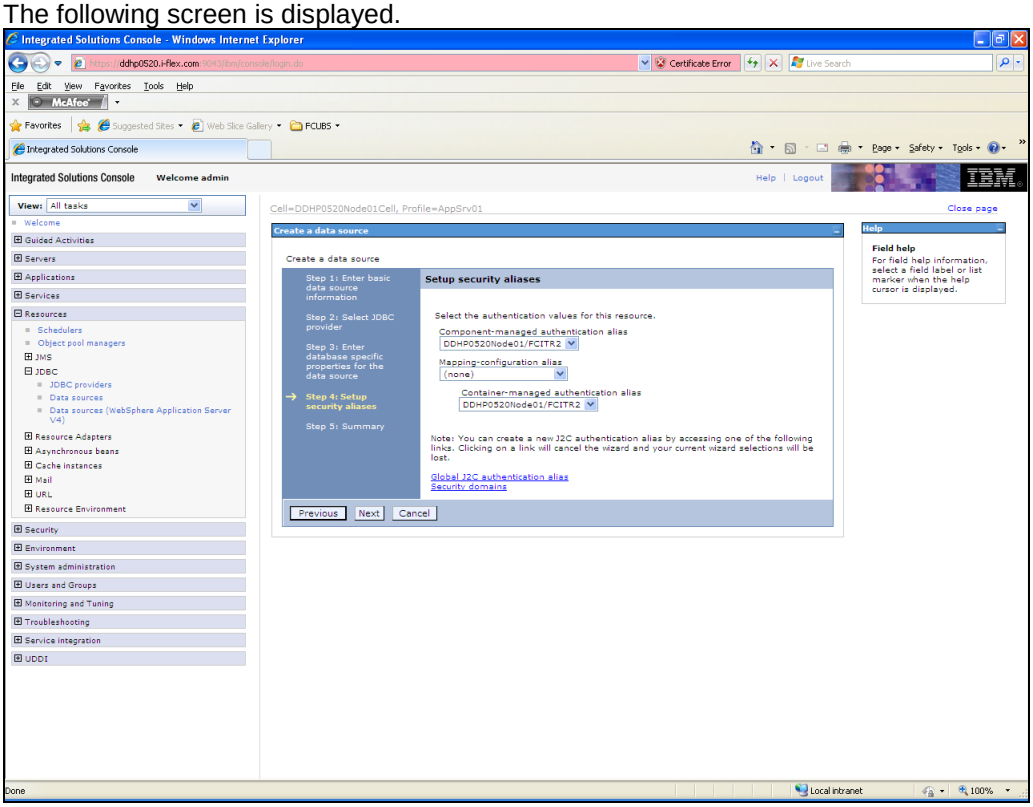
jdbc:oracle:oci:@10.10.10.10:1010:KERDEV2

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

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

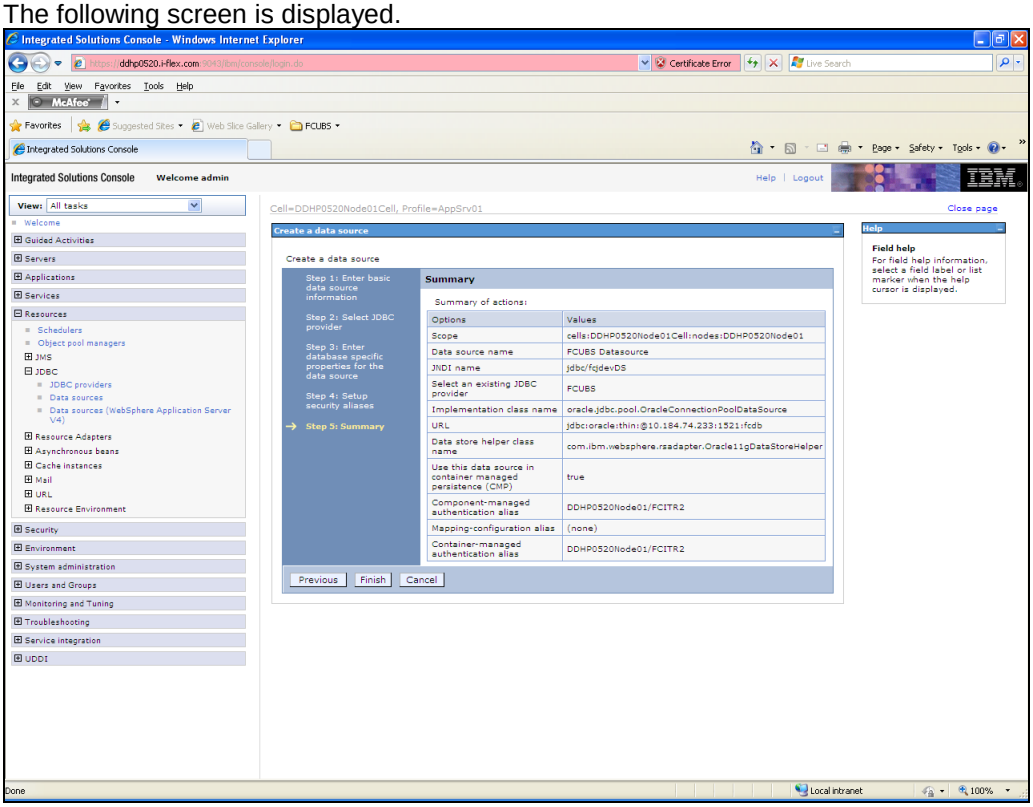
10. Click ‘Next’.

The following screen is displayed.



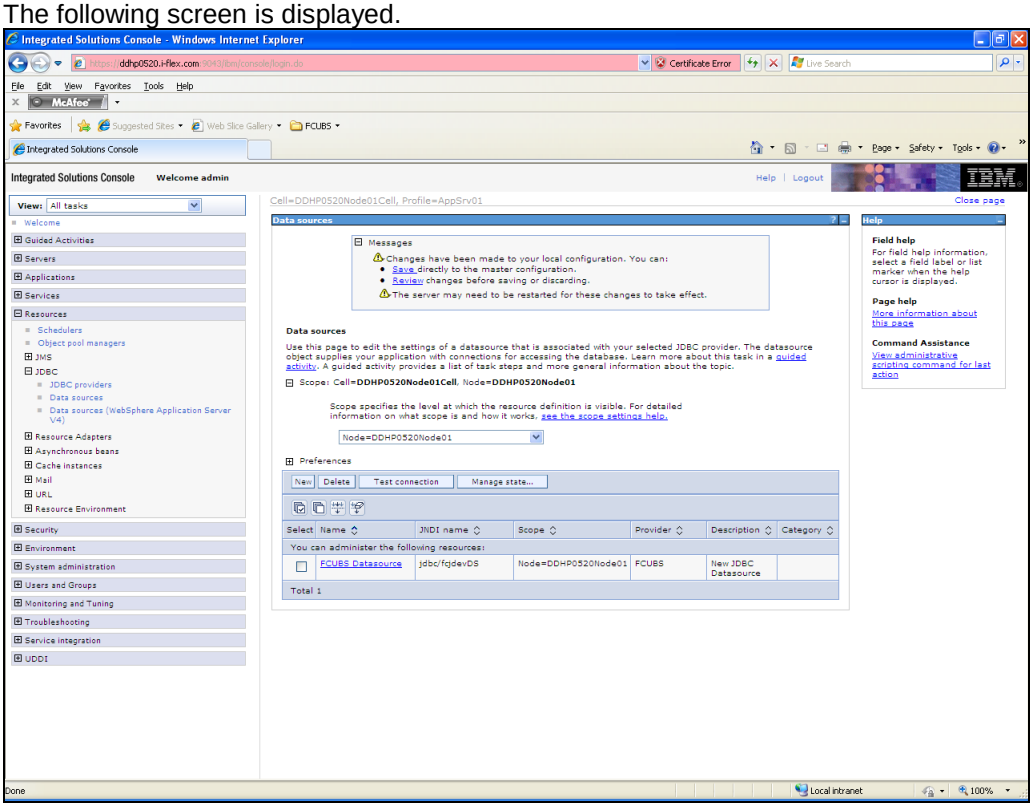
11. Click ‘Next’.

The following screen is displayed.



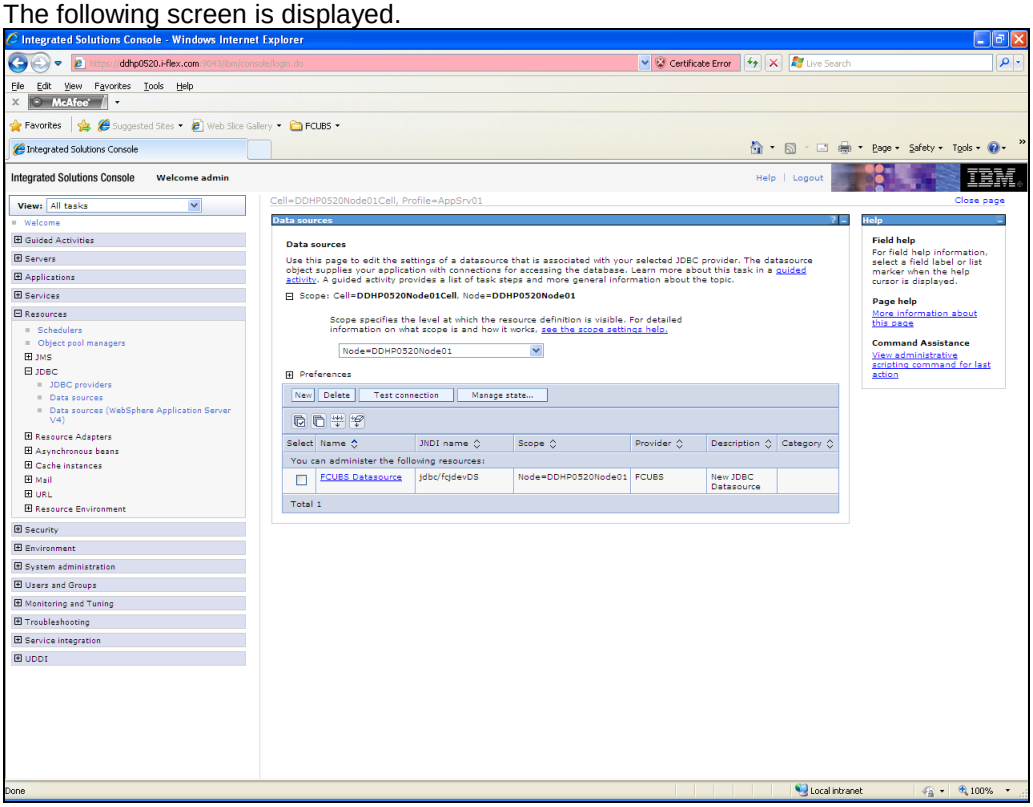
12. Click ‘Finish’.

The following screen is displayed.



13. Click ‘Save’.

The following screen is displayed.



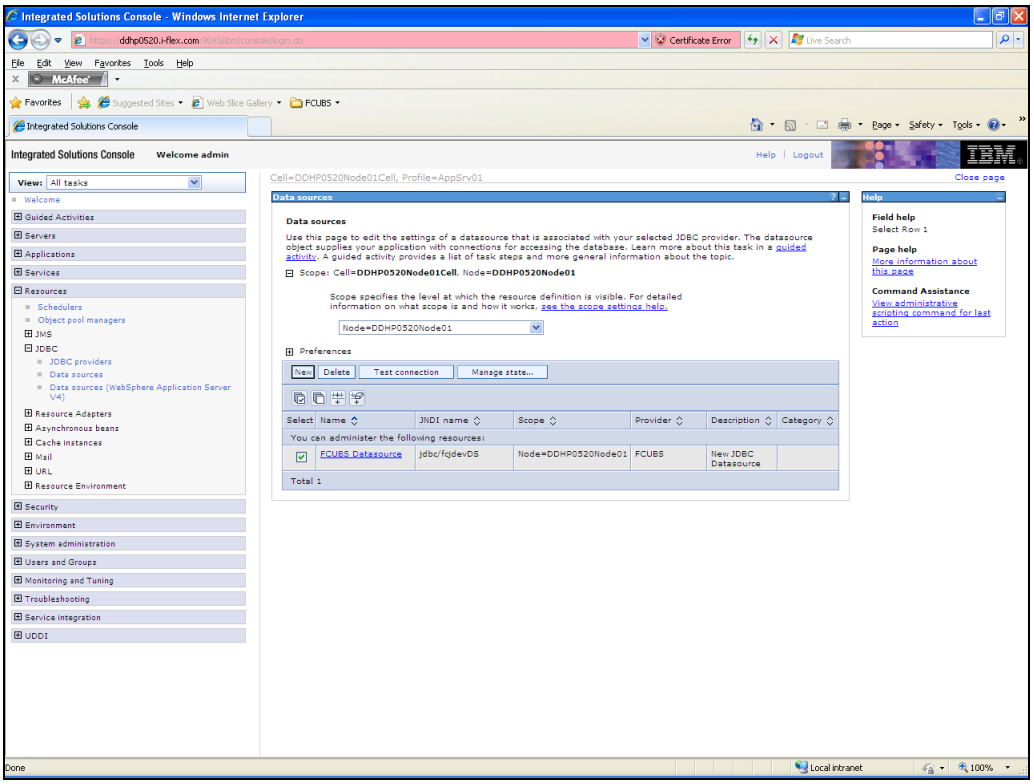
Note the following

- 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'.

3.2.3 Testing Data Source

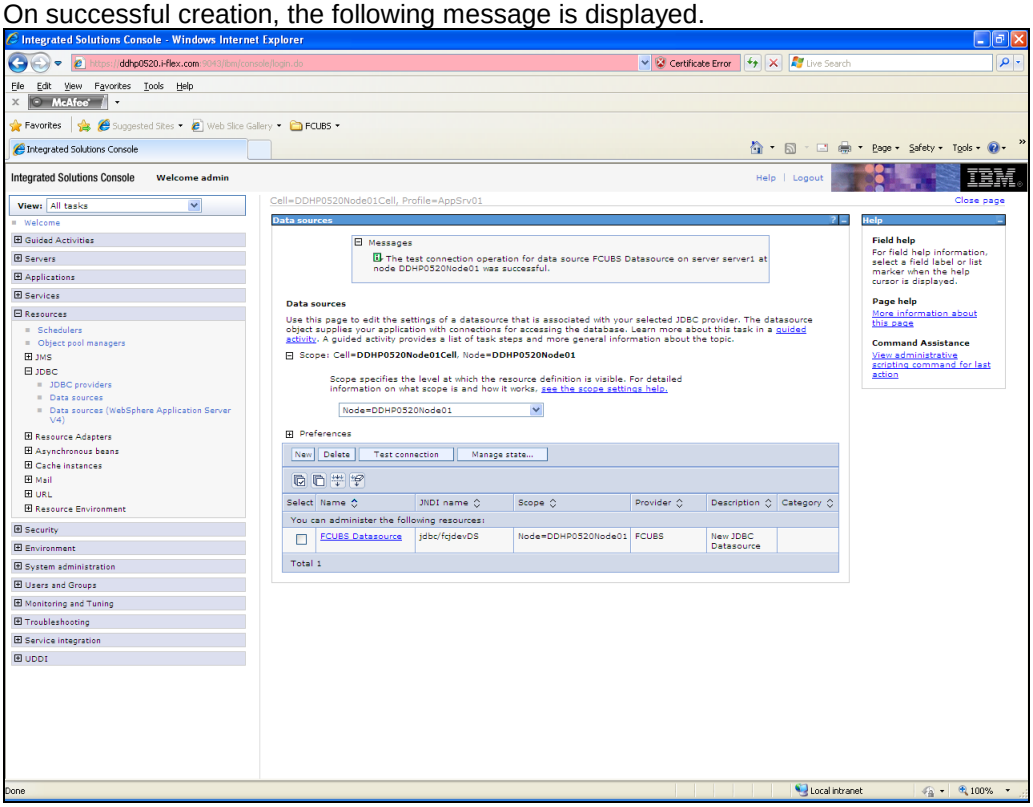
Follow the steps given below:

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



2. Click ‘Test connection’ button.

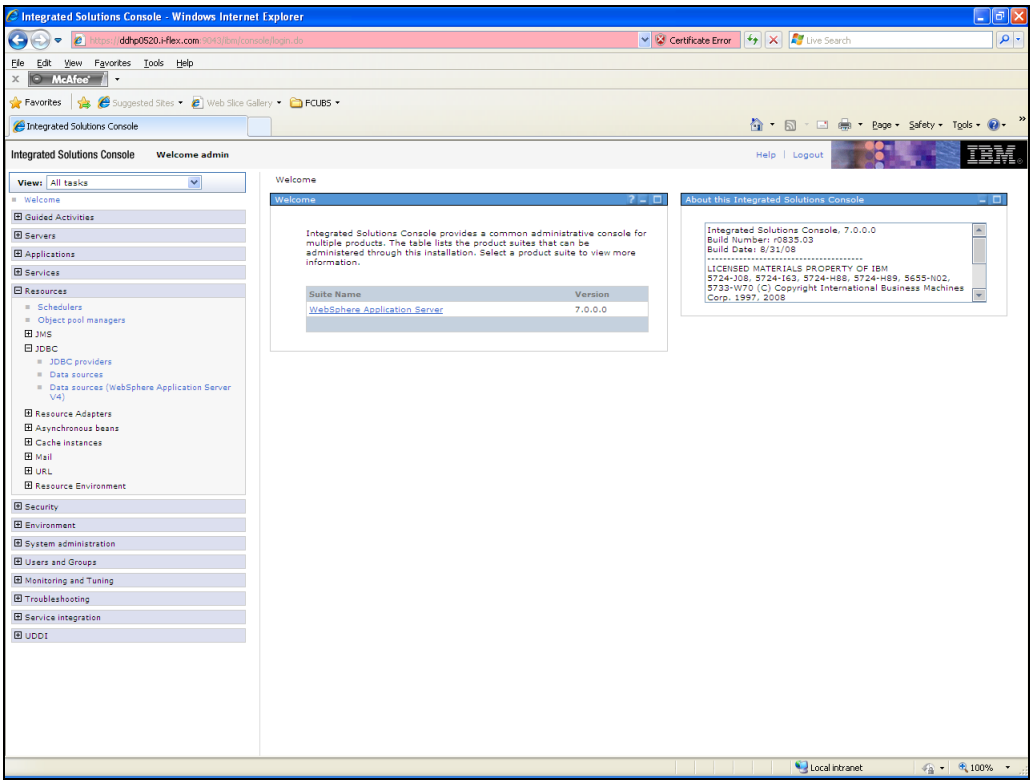
On successful creation, the following message is displayed.



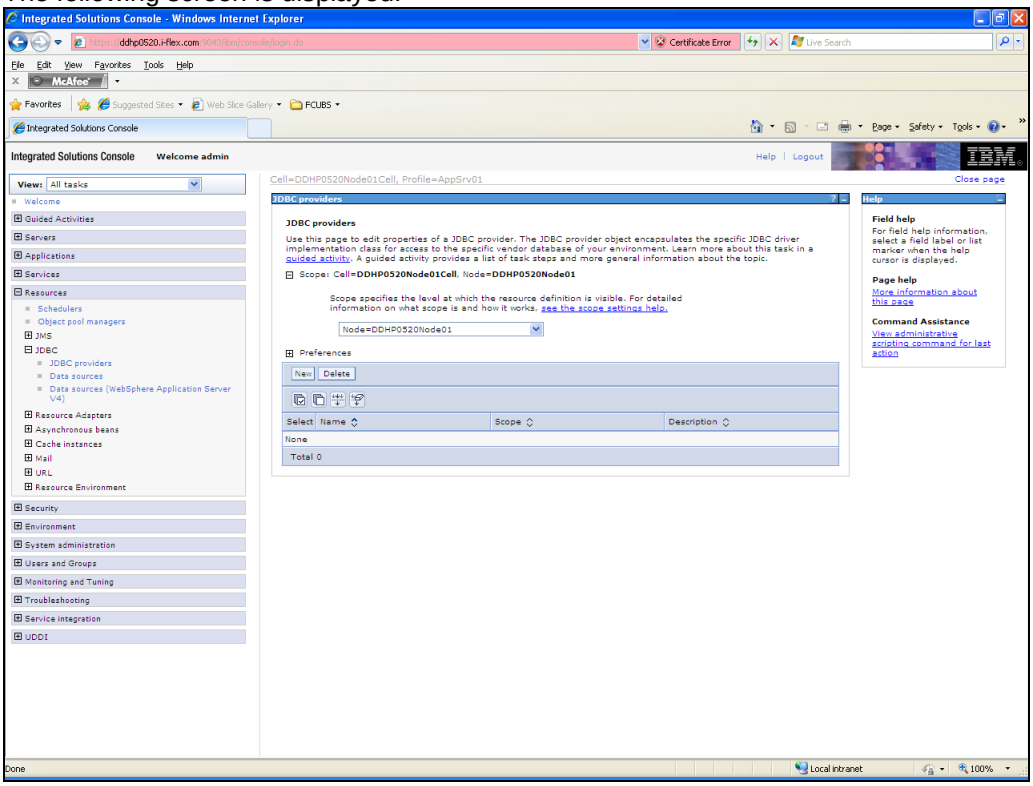
3.2.4 JDBC Provider for XA Data Source

Follow the steps given below:

1. Login to the application server administration console.
2. Expand ‘Resources > JDBC’ and click ‘JDBC Providers’.

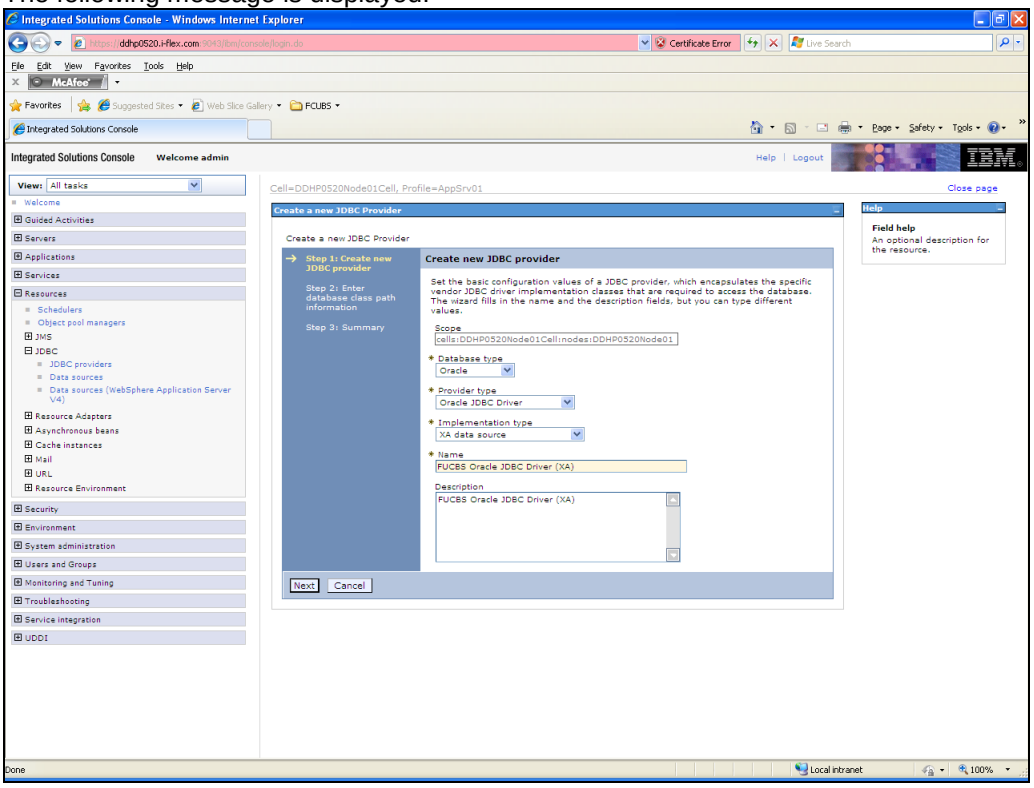


The following screen is displayed.



3. Select ‘Node’ from the drop-down list.

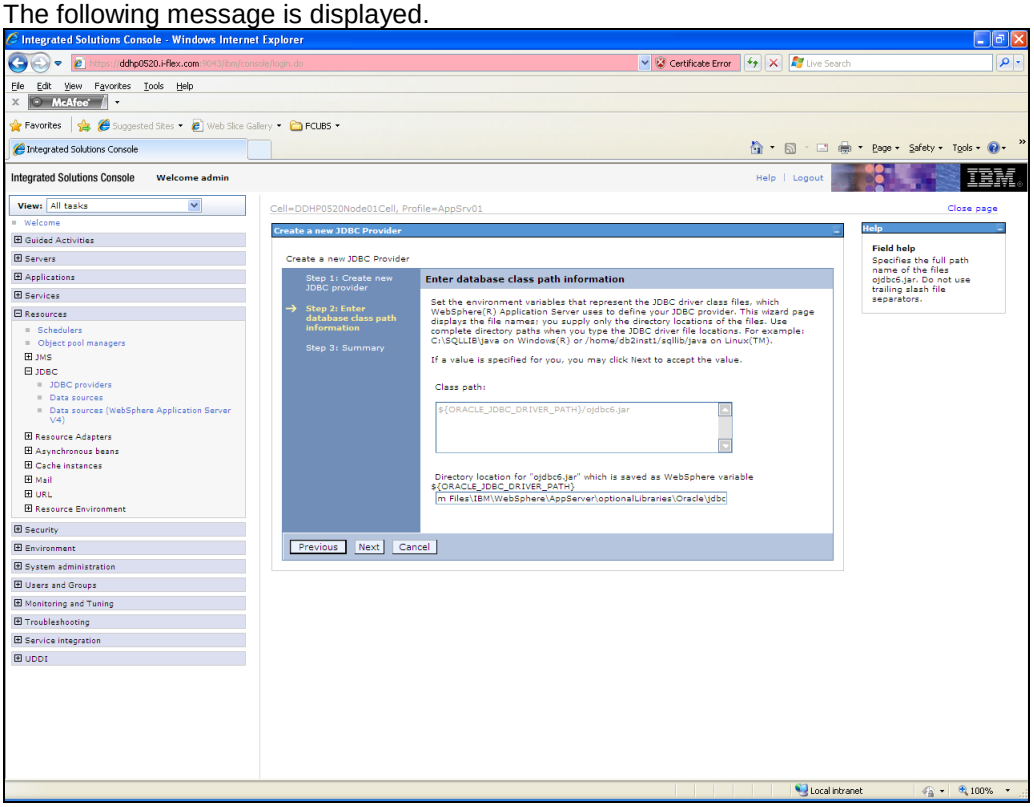
The following message is displayed.



4. Specify the following details:

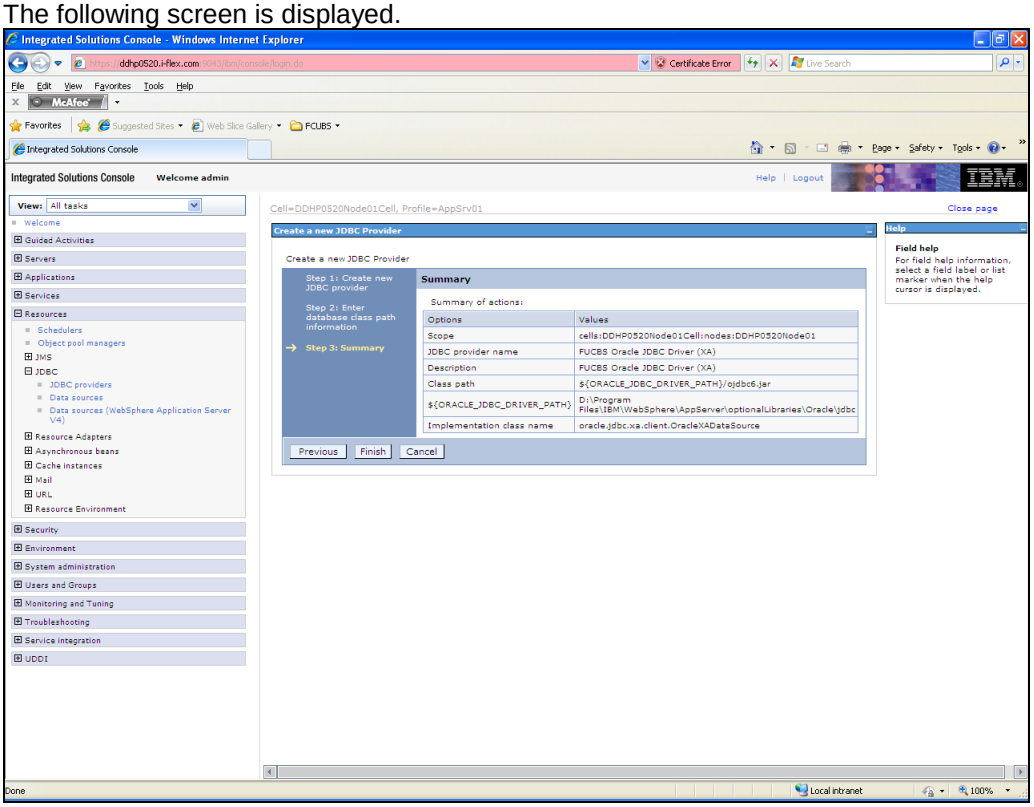
Database Type	Oracle
Provider Type	Oracle JDBC Driver
Implementation Type	XA data source
Name	FCUBS Oracle JDBC Driver (XA)
Description	FCUBS Oracle JDBC Driver (XA)

The following message is displayed.



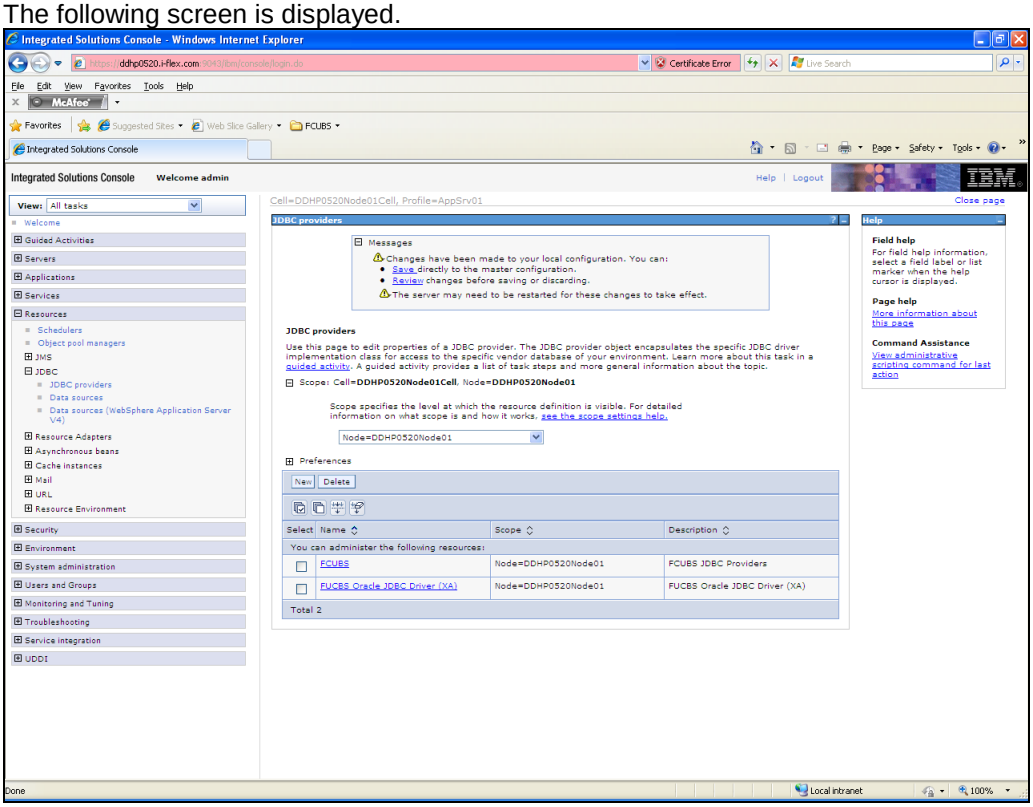
5. Specify the location of ojbc6.jar.

The following screen is displayed.



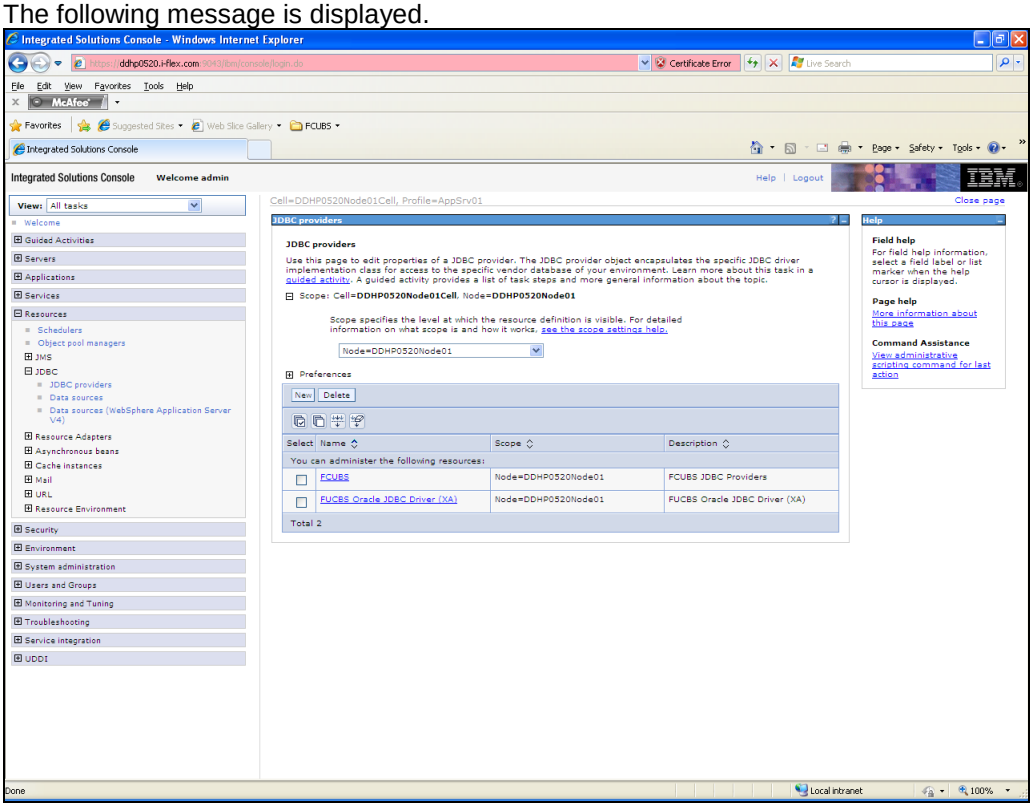
6. Click ‘Finish’.

The following screen is displayed.



7. Click ‘Save’.

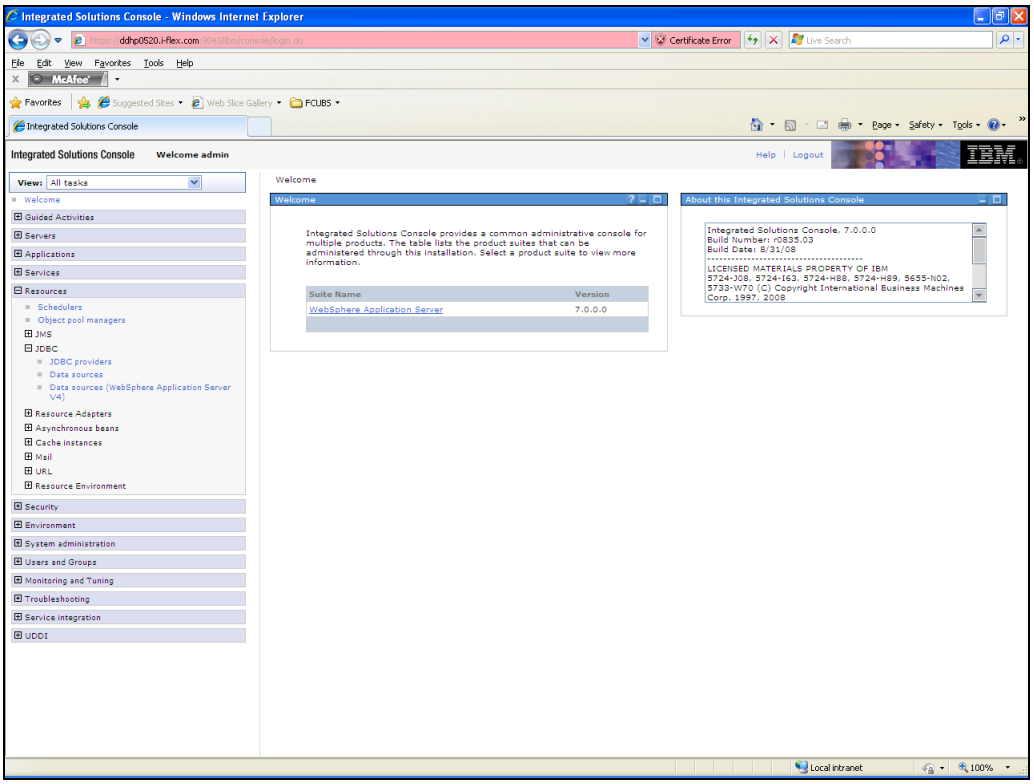
The following message is displayed.



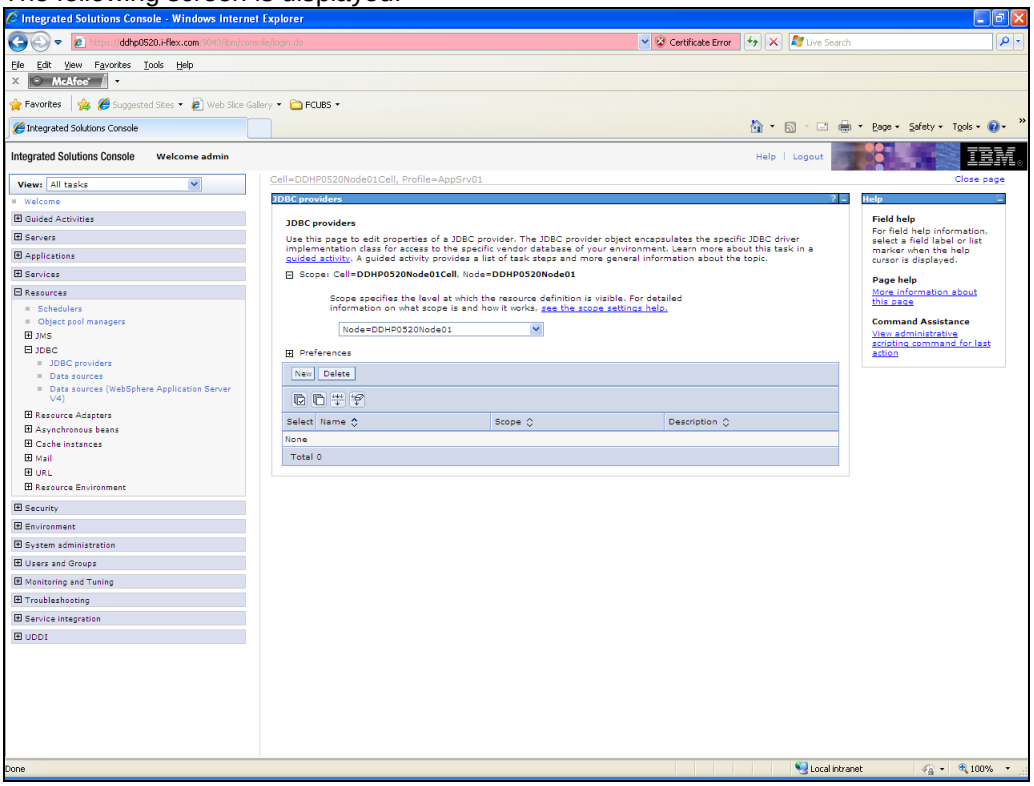
3.2.5 Creating XA Data Source

Follow the steps given below:

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

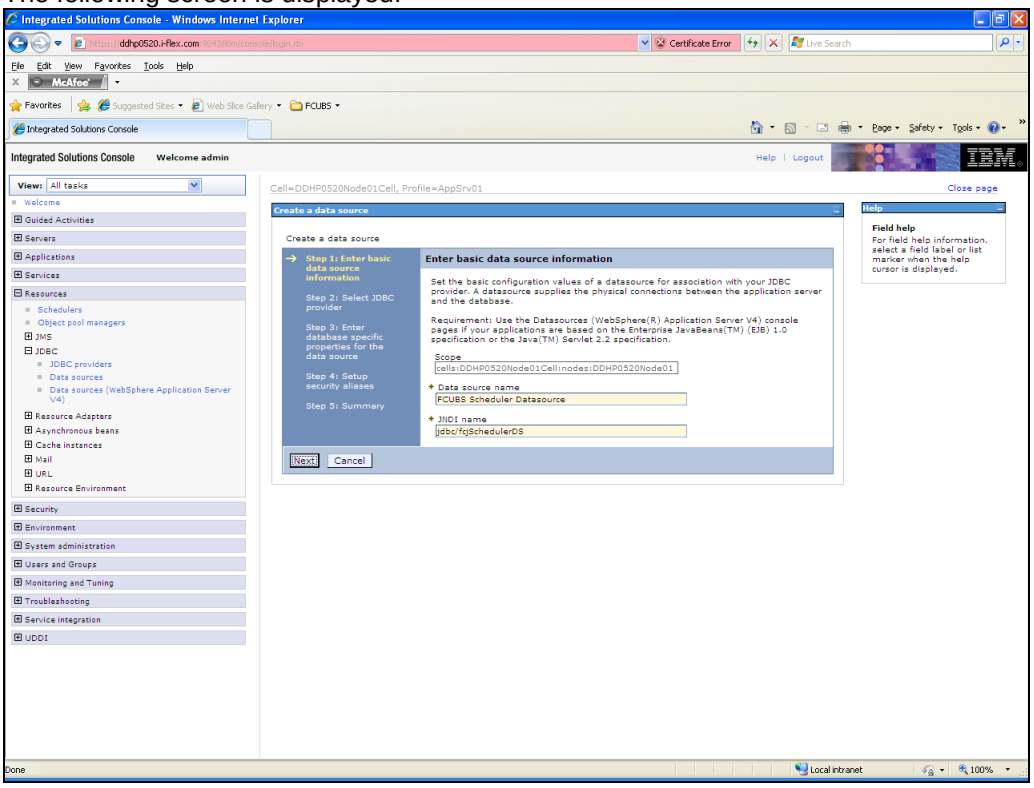


The following screen is displayed.



3. Select ‘Node’ from the dropdown list.

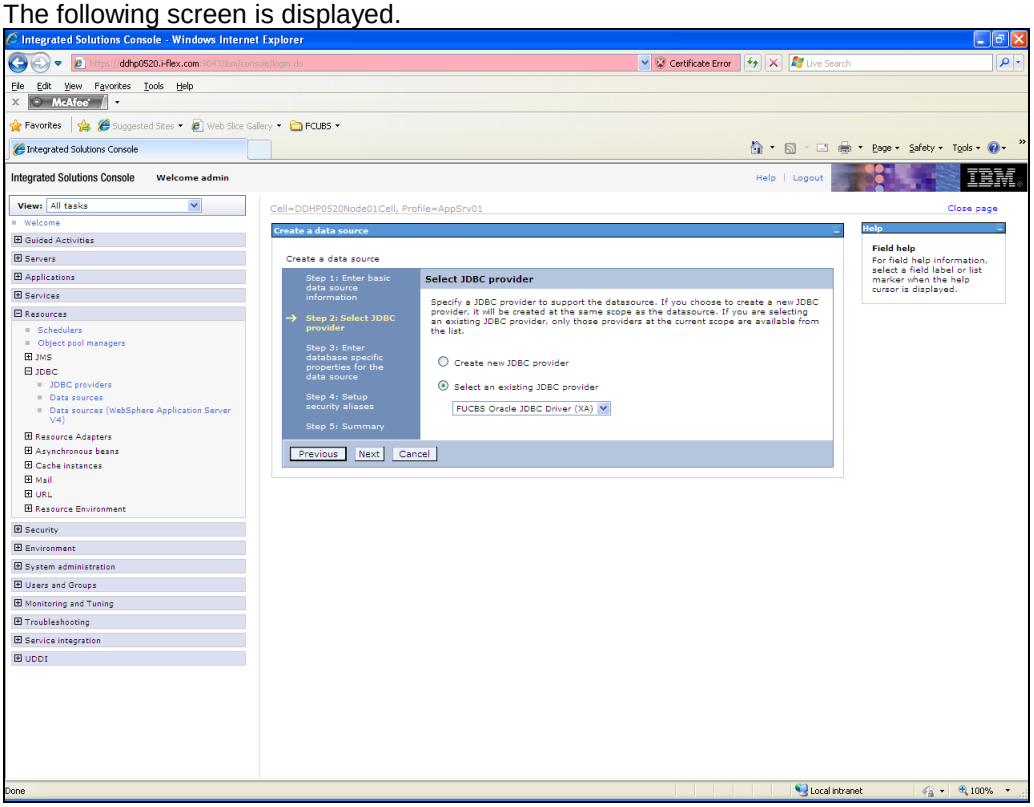
The following screen is displayed.



4. Specify the following details:

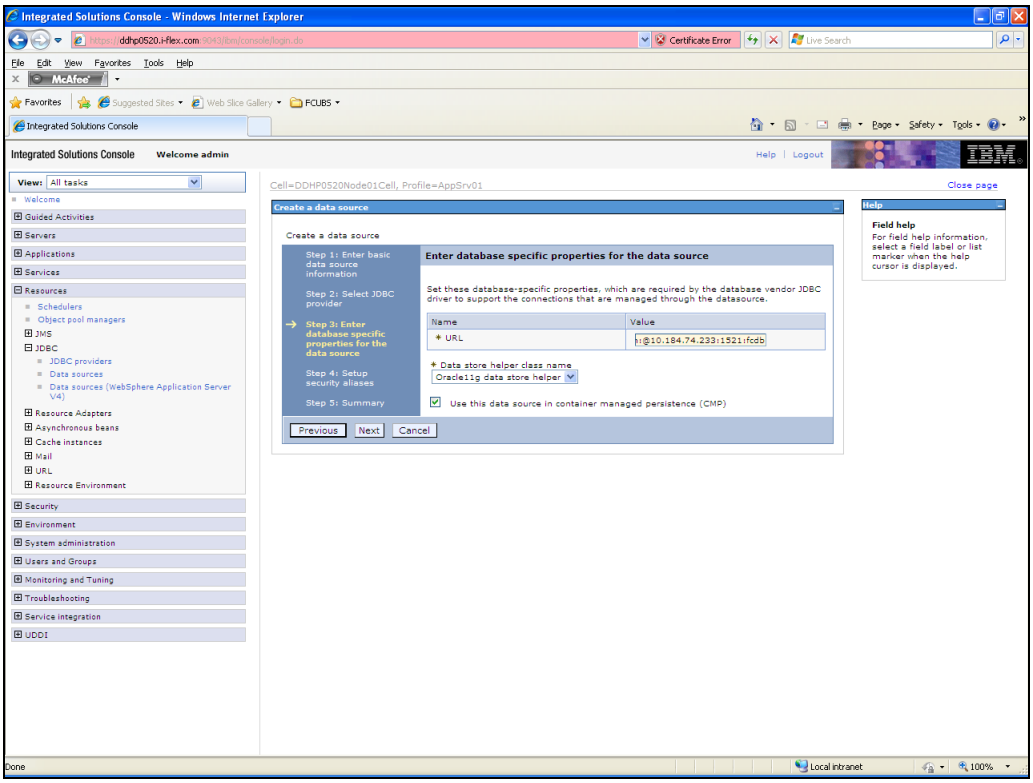
Data source name	FCUBS Scheduler Data source
JNDI Name	jdbc/fcjSchedulerDS

The following screen is displayed.



5. Select the option ‘Select an existing JDBC provider’ and choose ‘FCUBS Oracle JDBC Deriver (XA)’ from the drop-down list.

The following screen is displayed.



6. Specify the URL.

Example

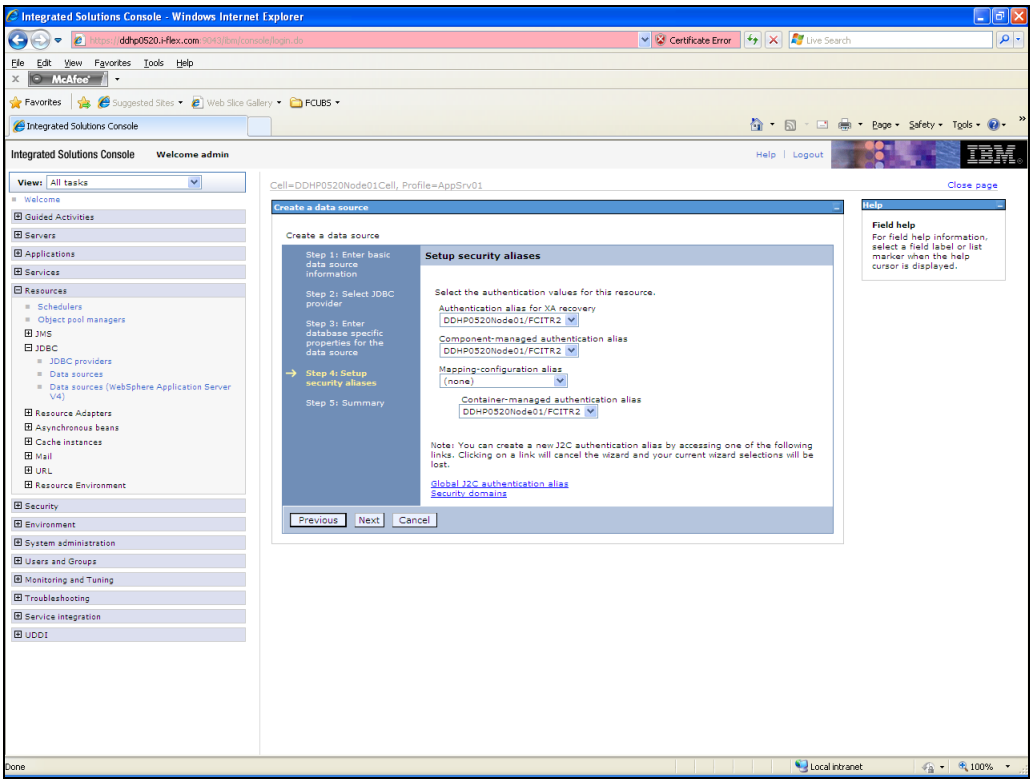
jdbc:oracle:oci:@10.10.10.10:1010:KERDEV2

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’.

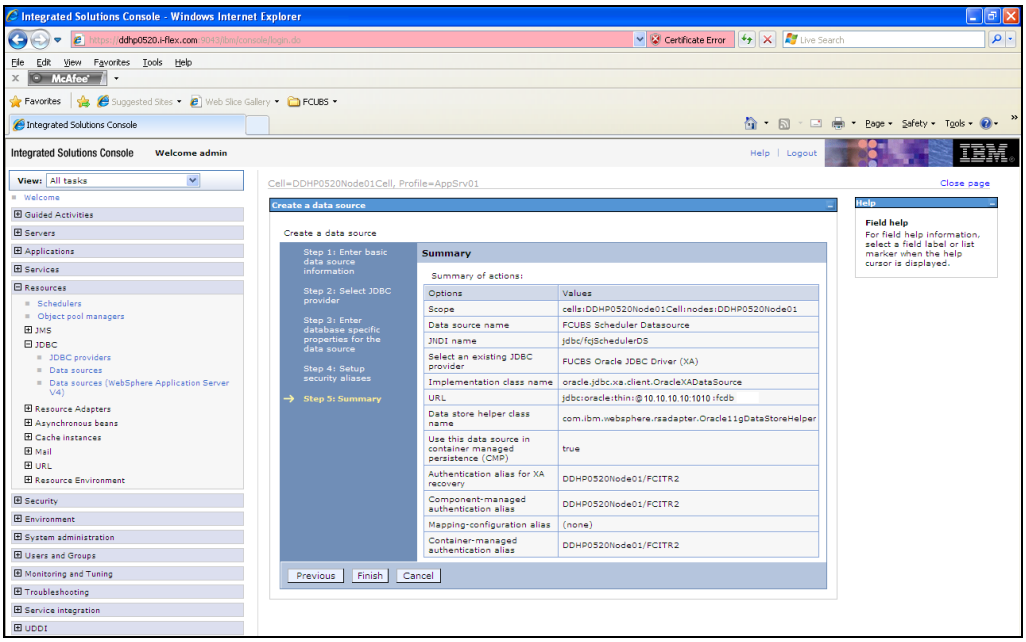
8. Click ‘Next’.

The following screen is displayed.

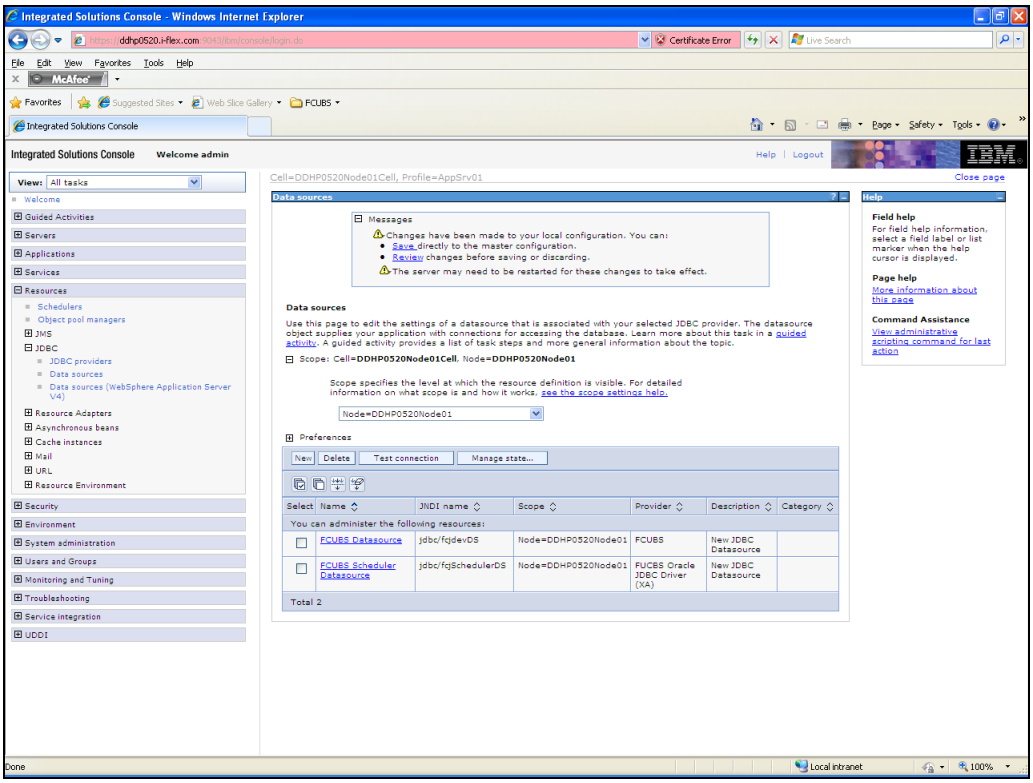


9. Click ‘Next’.

The following screen is displayed.

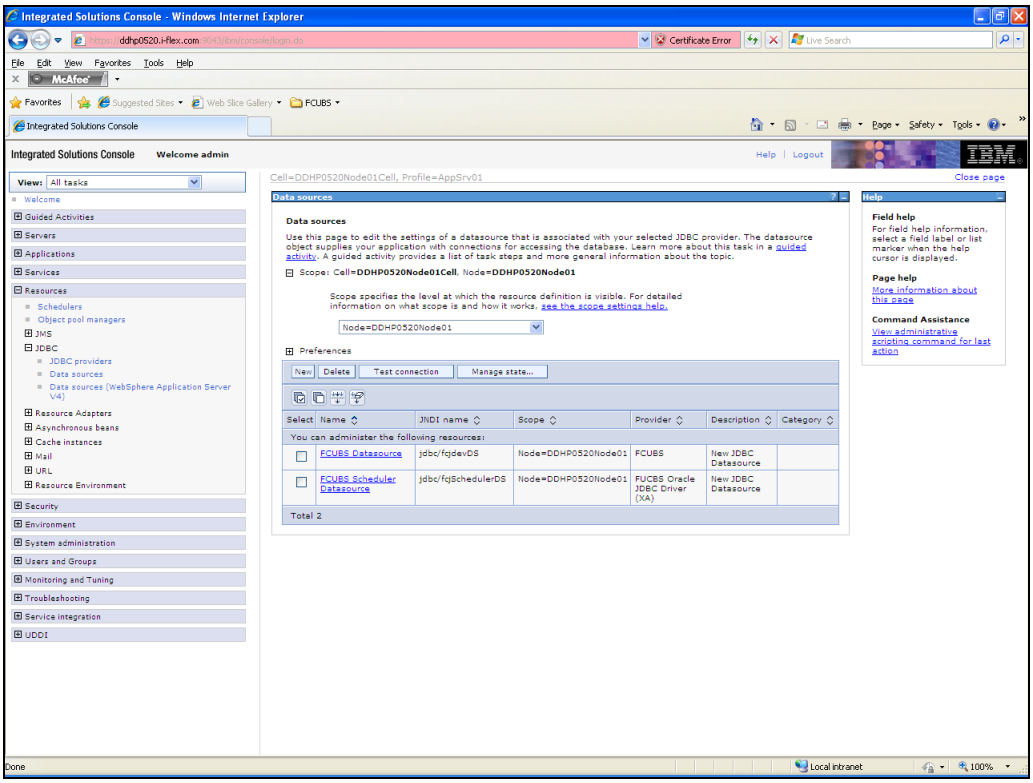


The following screen is displayed.



10. Click ‘Save’.

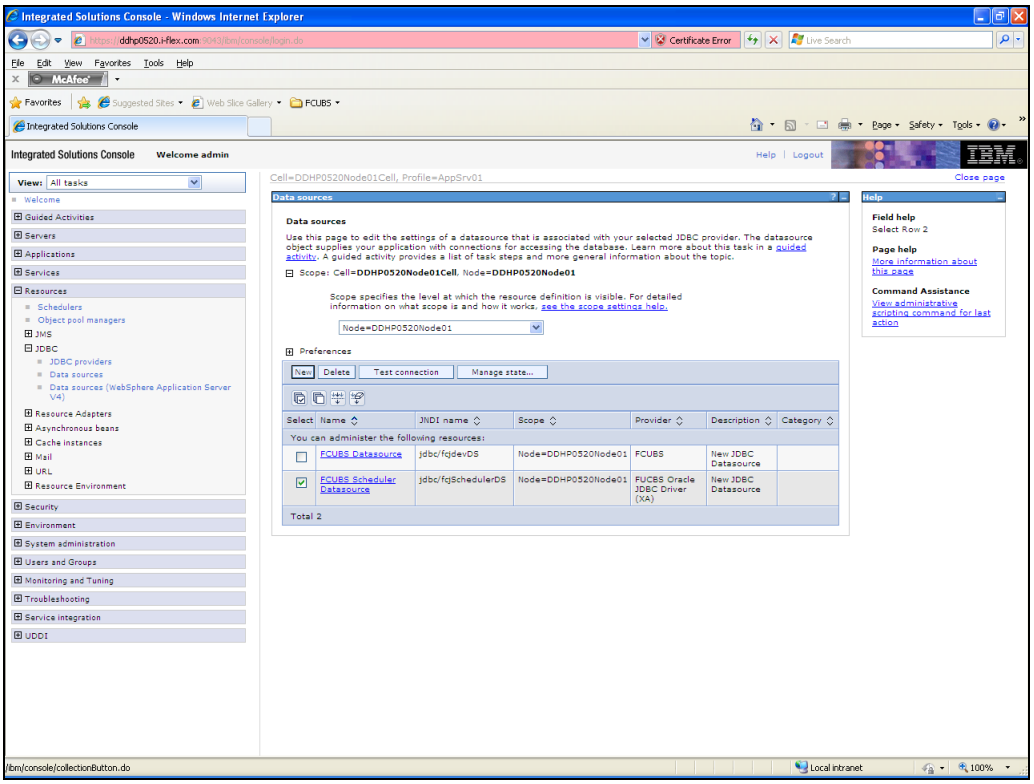
The following screen is displayed.



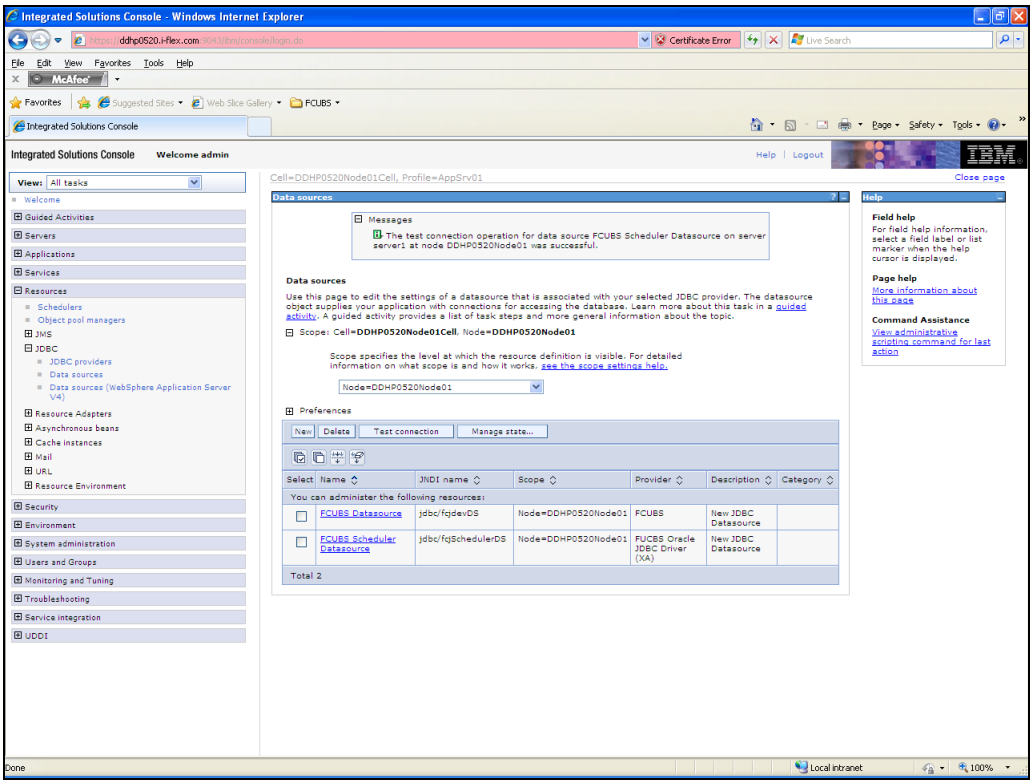
3.2.6 Testing Data Source

Follow the steps given below:

1. Select data source as given below.



11. Click ‘Test connection’ button. The following screen is displayed on successful creation.



3.3 Creating JMS Resources

3.3.1 Creating Queue Connection Factory

Follow the steps given below:

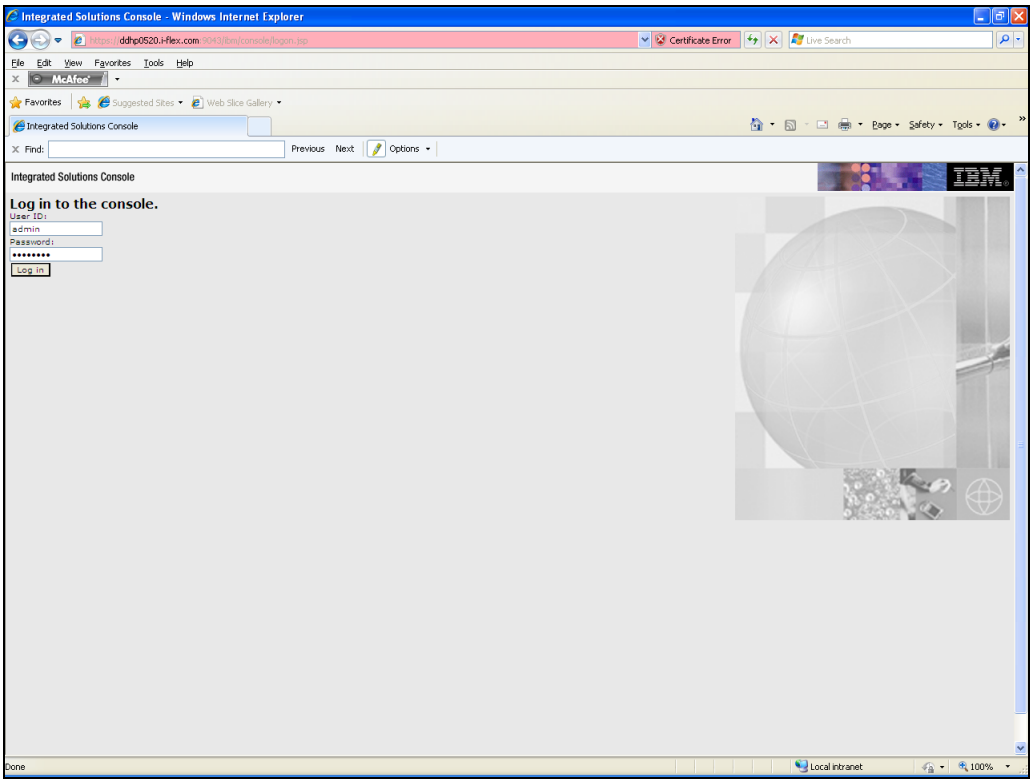
1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

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

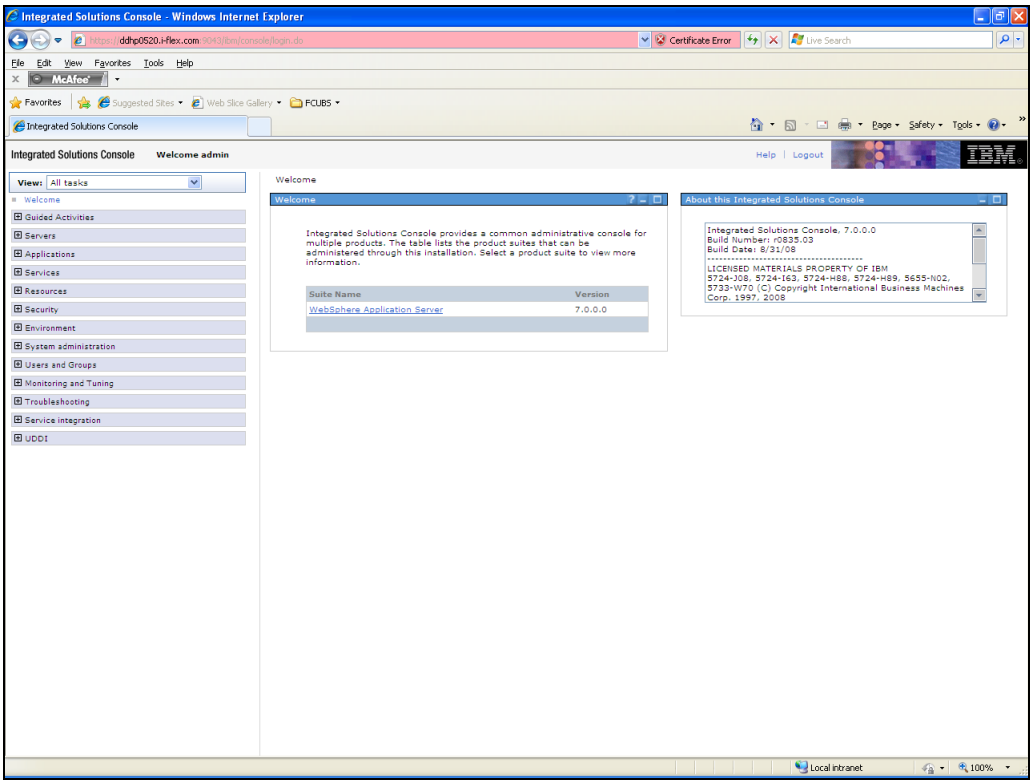
Eg: https://10.10.10.10:1010/console

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

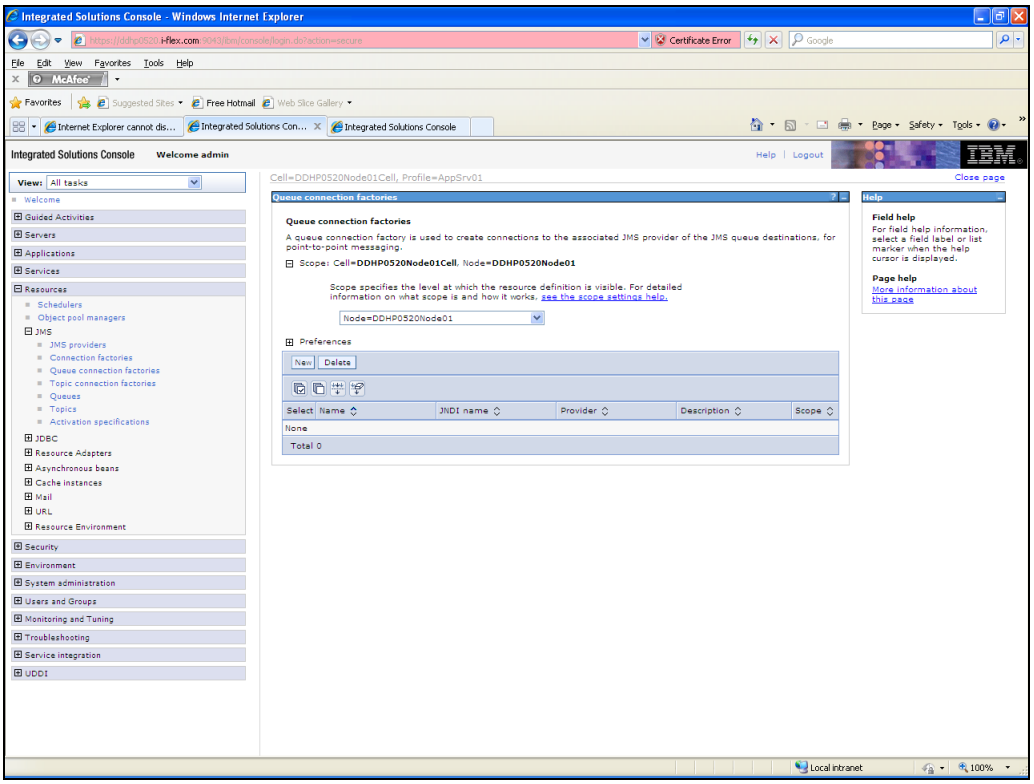
The following screen is displayed:



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

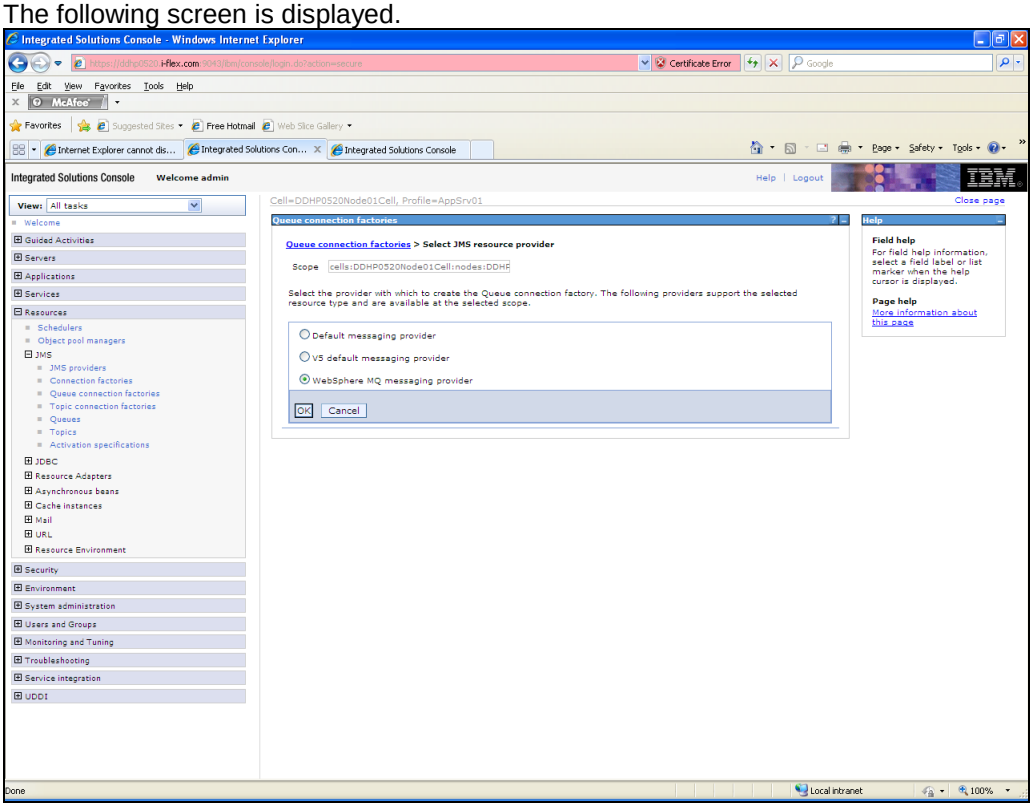


5. Expand ‘Resources’ and select ‘JMS’. Click ‘Queue Connection Factories. ‘The following screen is displayed.



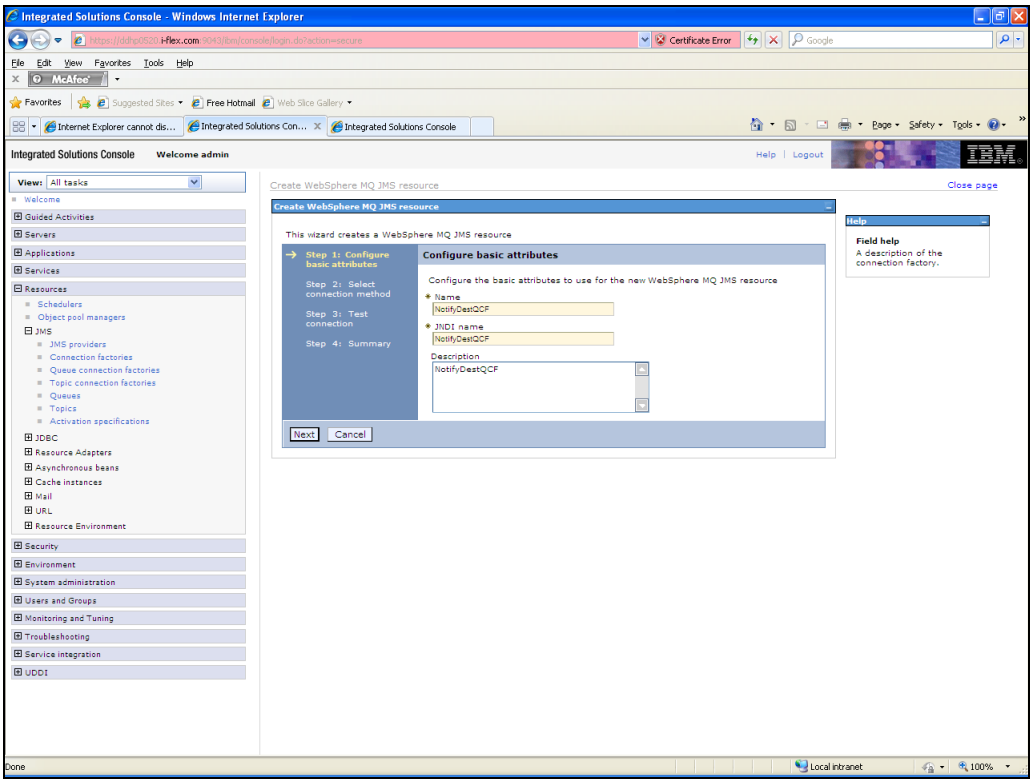
6. Select ‘Node’ from the drop down list.

The following screen is displayed.



7. Select ‘Websphere MQ messaging provider’ and click ‘OK’.

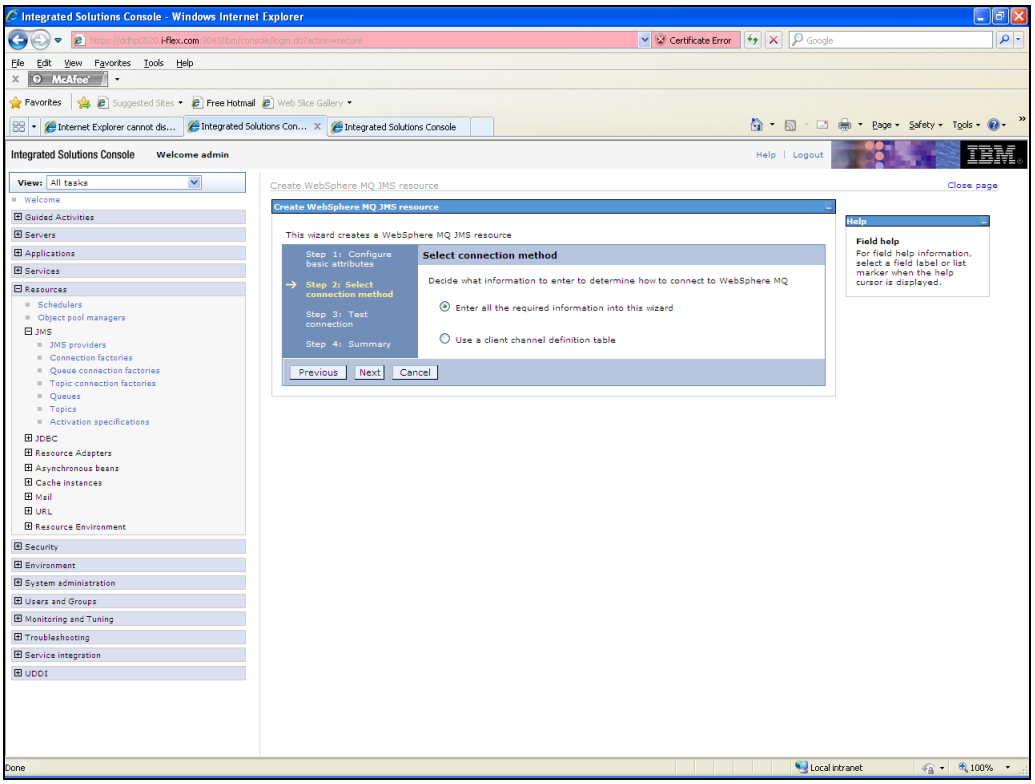
The following screen is displayed.



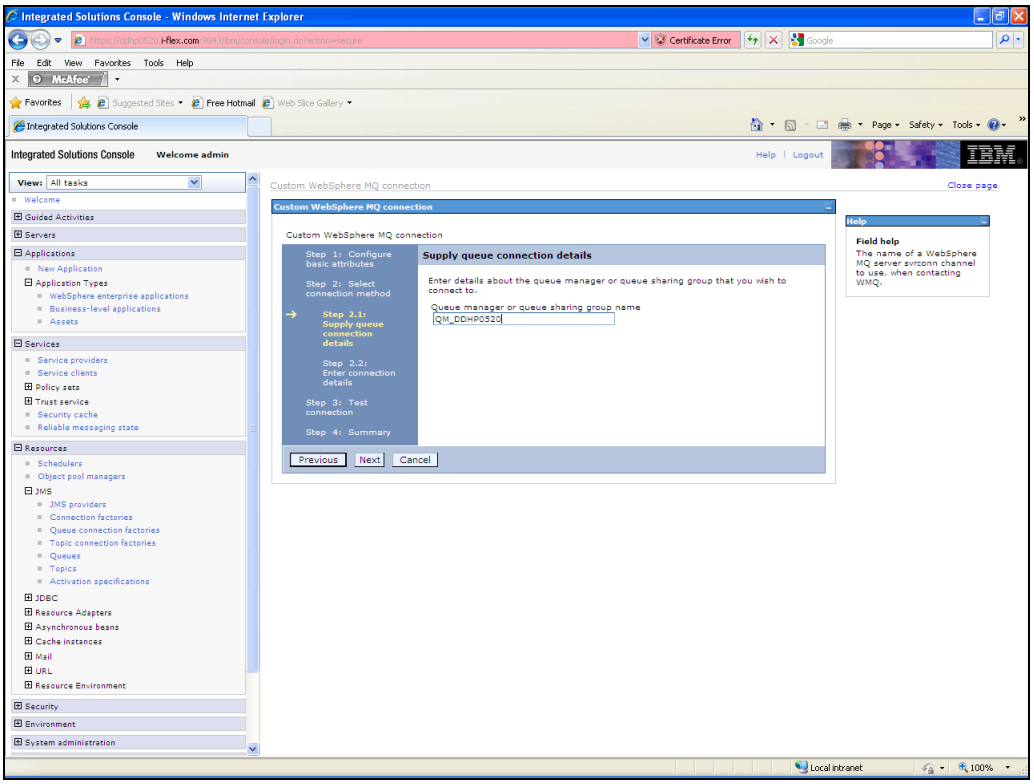
8. Specify the following details:

Name	NotifyDestQCF
JNDI Name	NotifyDestQCF
Description	NotifyDestQCF

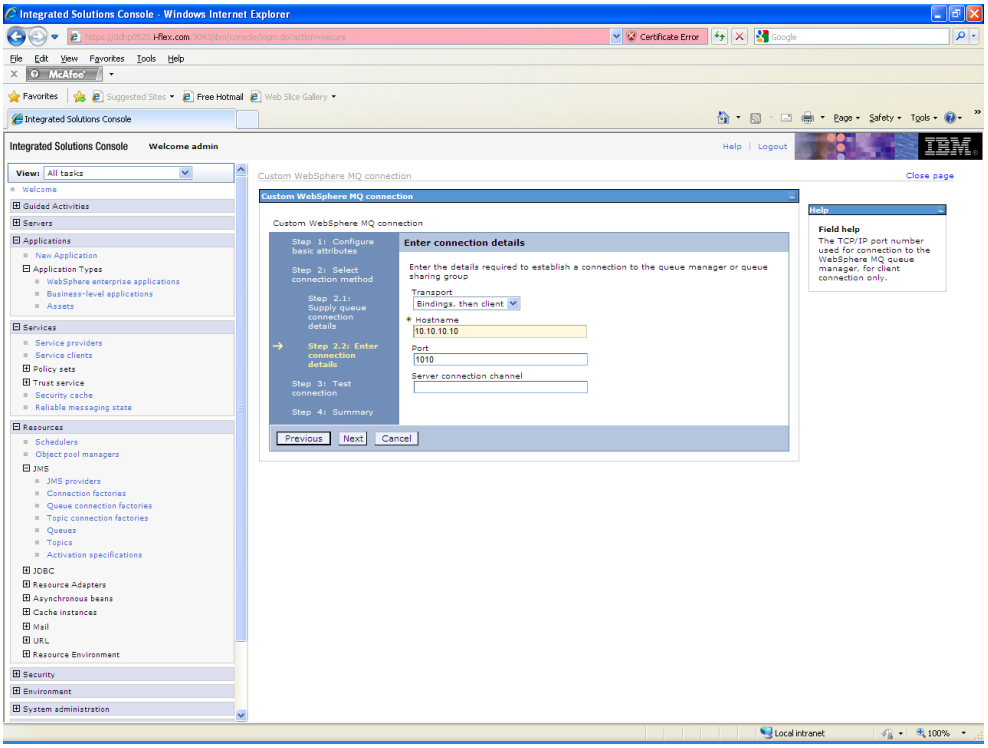
9. Click ‘Next’. The following screen is displayed.



10. Set the options as shown in the figure. Click ‘Next’.
11. The following screen is displayed.



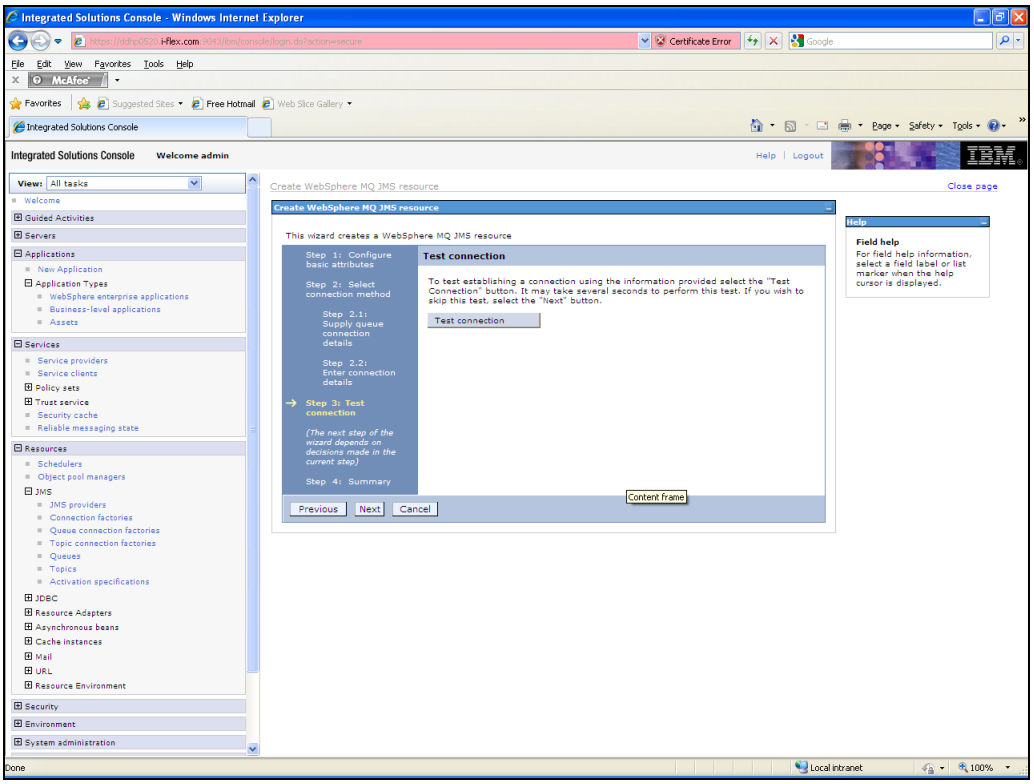
12. Specify the queue manager name ‘QM_DDHP0520’. Click ‘Next’.



13. Specify the following details:

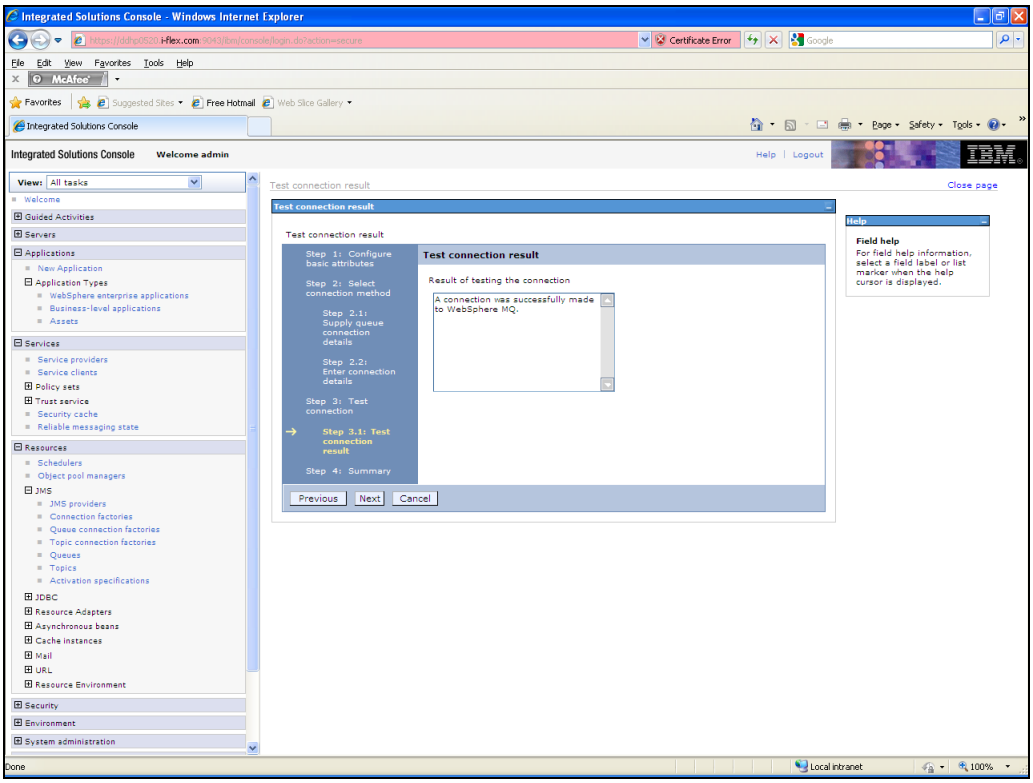
Host Name	10.10.10.10 (Host where Websphere MQ is installed)
Port	1010 (Web sphere MQ port)
Server Connection Channel	SYSTEM.DEF.SVRCONN

14. Click ‘OK’. The following screen is displayed.

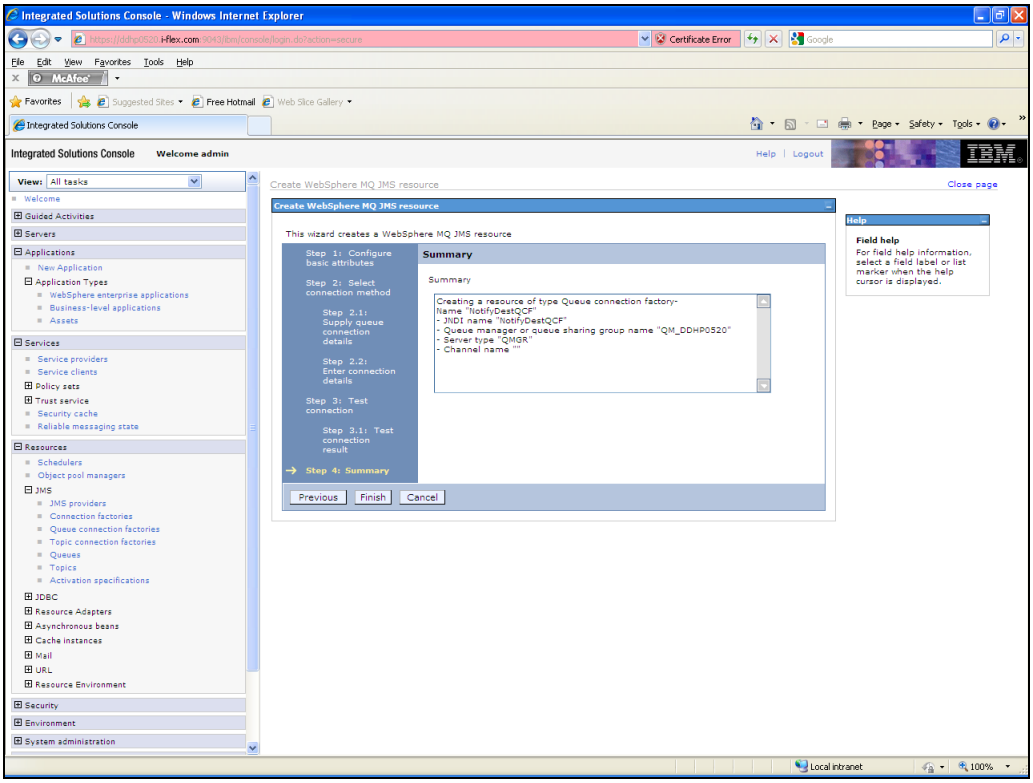


15. Click ‘Test Connection’ button.

The following screen is displayed:

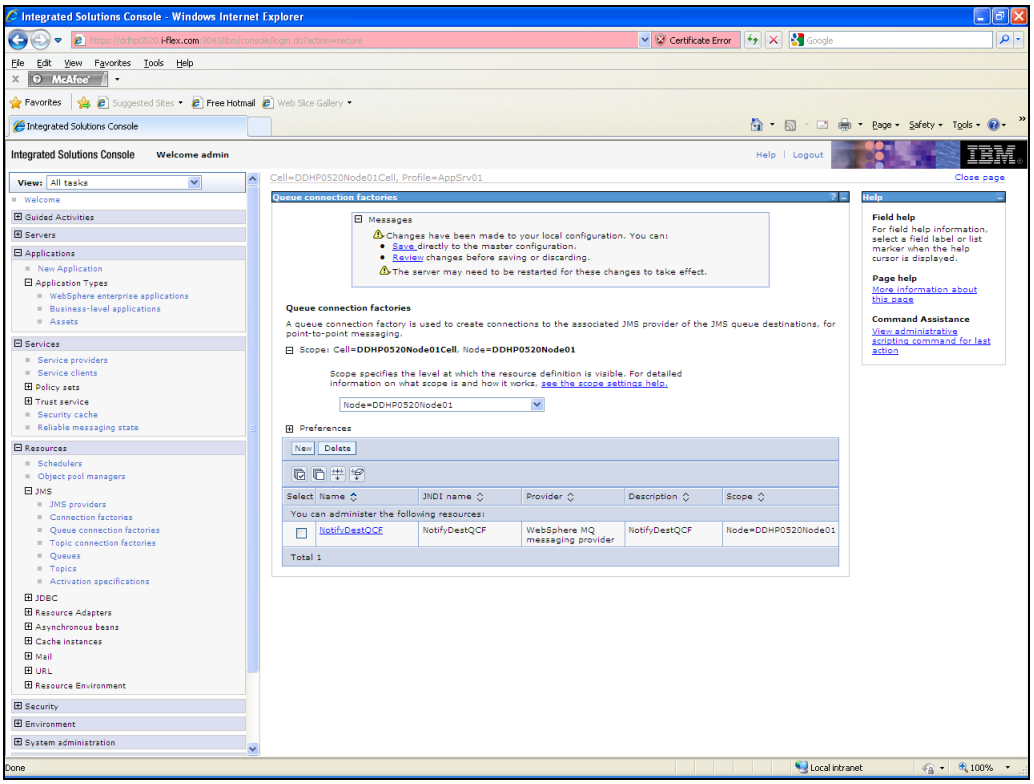


16. Click ‘Next’. The following screen is displayed with a message in the summary field.



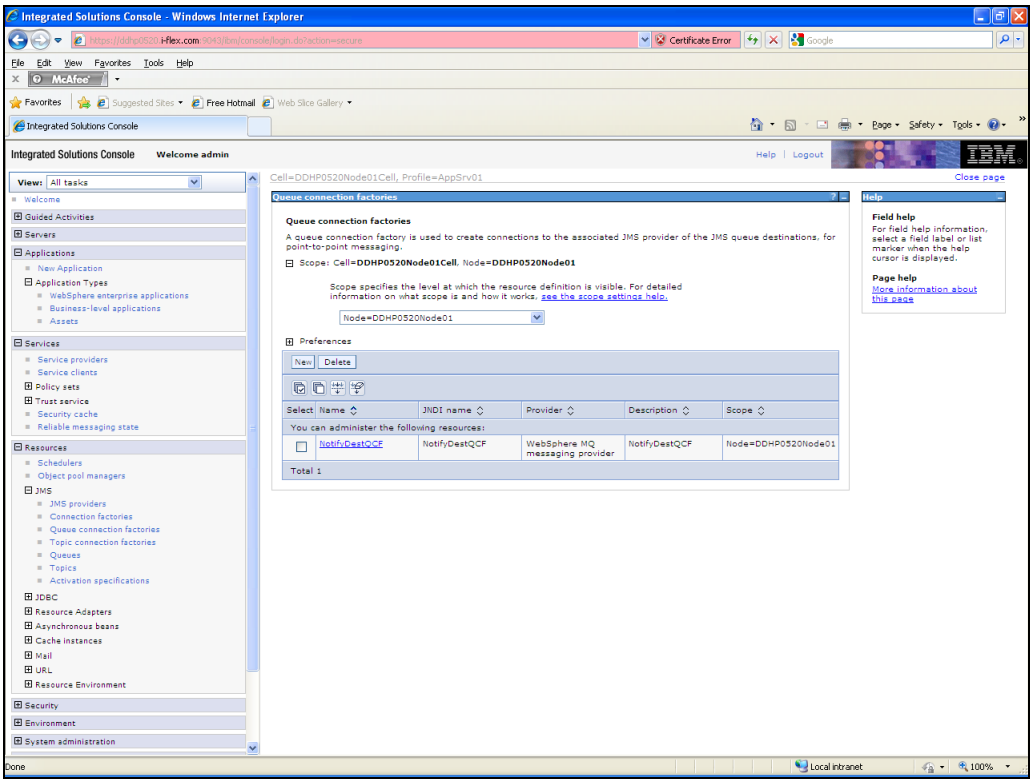
17. Click ‘Finish’.

The following screen is displayed.



18. Click ‘Save’.

The following screen is displayed.



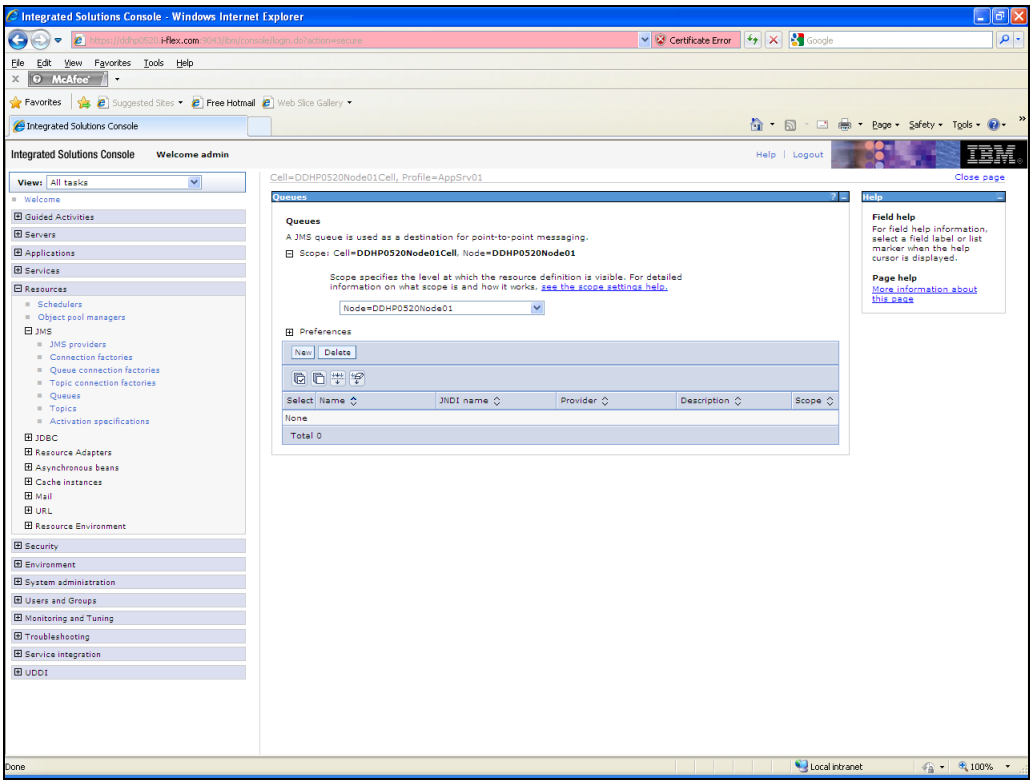
19. Similarly, you need to create the following queue connection factories:

MDBQCF
NOTIFY_MDB_QCF
NotifyDestQCF
DefferedDestQCF
RTGSQCF
SFMSQCF
ELMDBQCF
EL_NOTIFY_QCF
EmsQcf
BIPQCF
GI_UPLOAD_QCF

3.3.2 Creating Queues

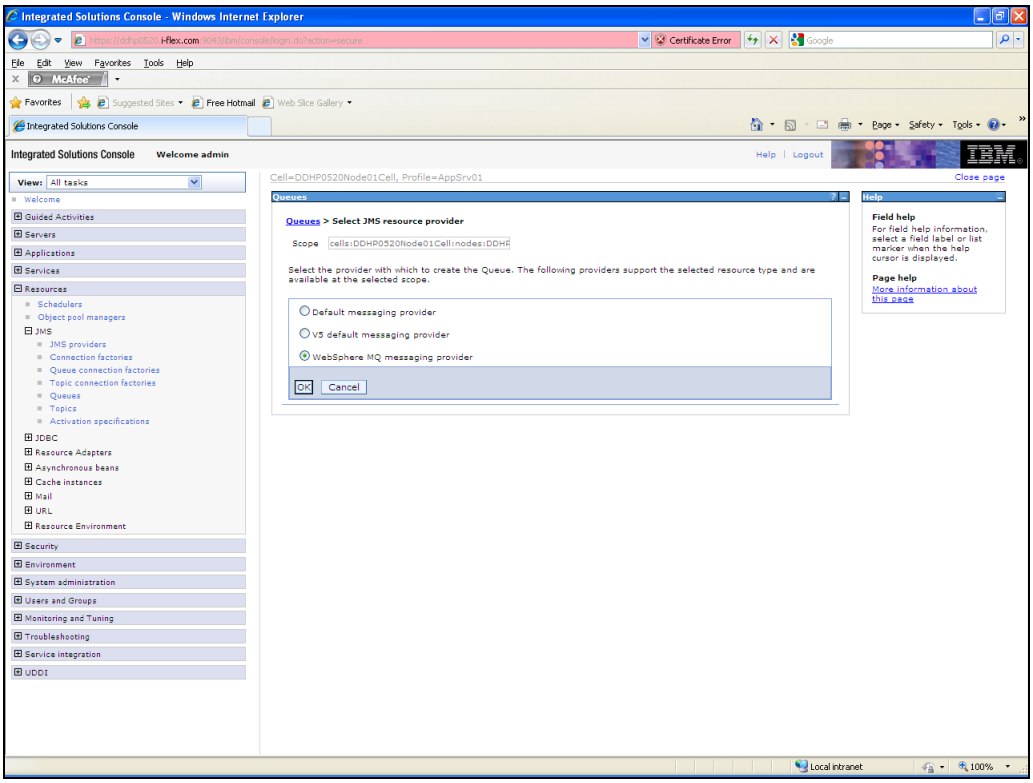
Follow the steps given below:

1. Expand ‘Resources > JMS’ and click Queues.



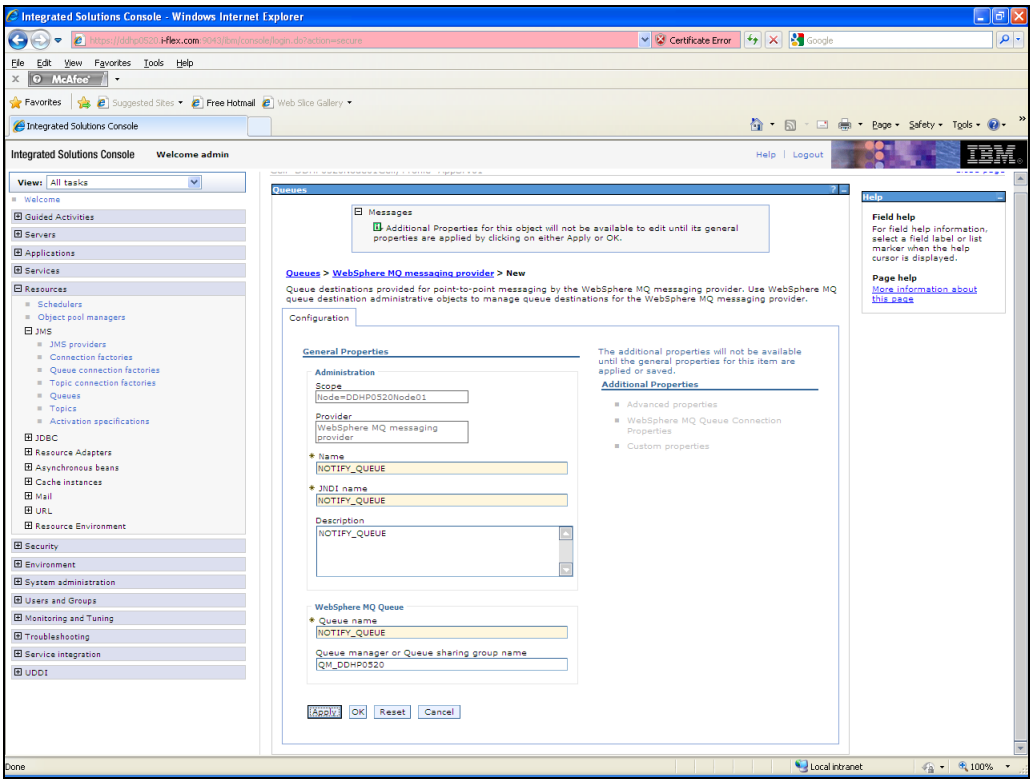
2. Select ‘Node’ from the drop down list. Click ‘New’.

The following screen is displayed:



3. Select ‘Websphere MQ messaging provider’. Click ‘OK’.

The following screen is displayed.

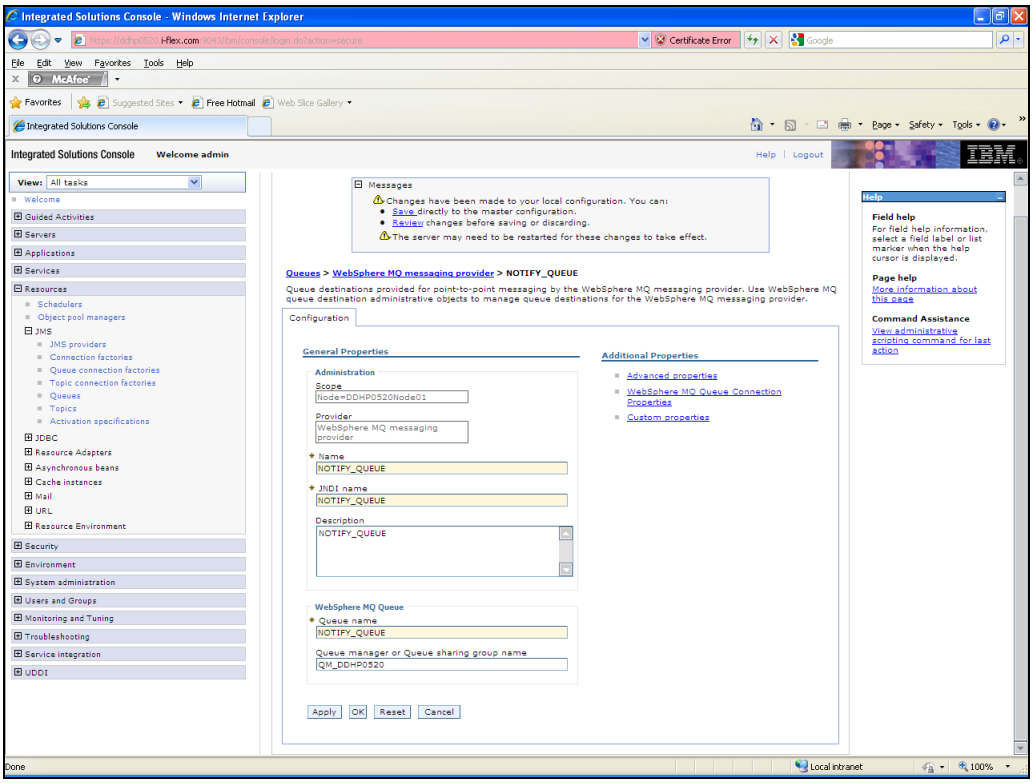


Specify the following details:

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

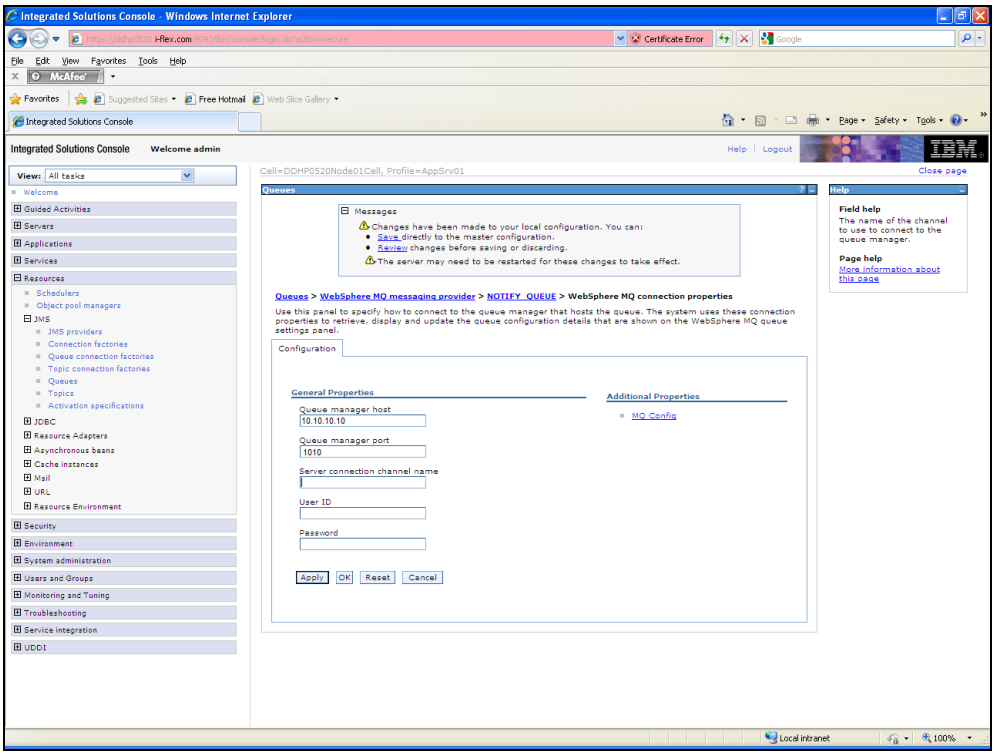
4. Click ‘Apply’.

The following screen is displayed.



5. Click ‘Websphere MQ Queue Connection Properties’.

The following screen is displayed.

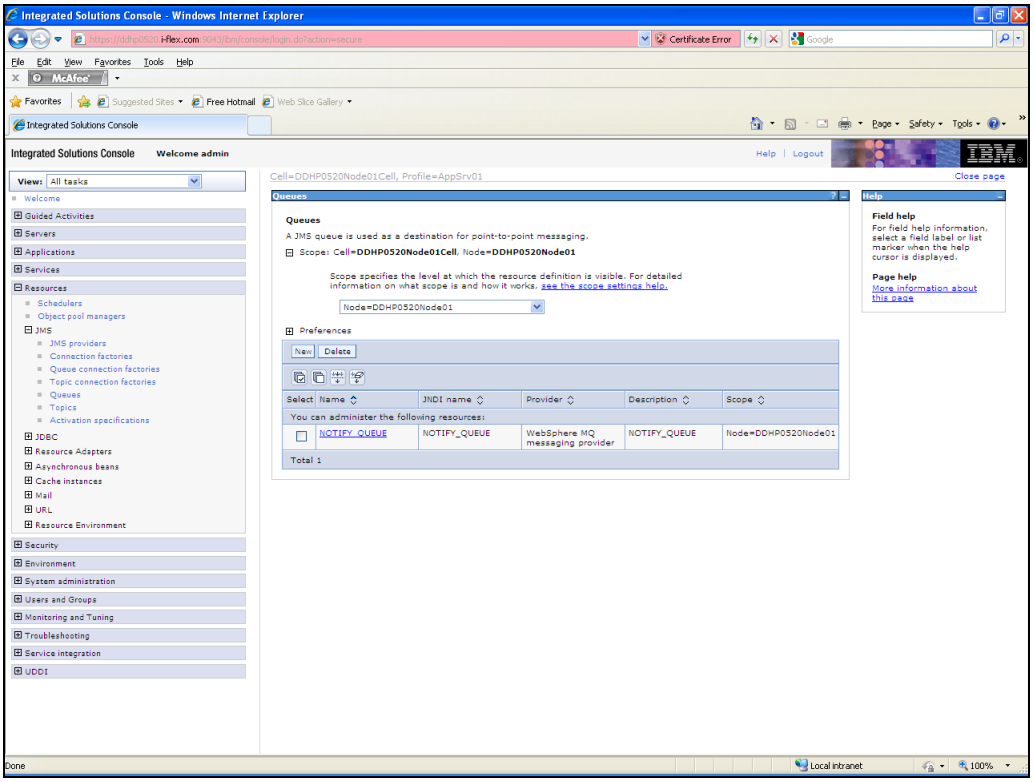


6. Specify the following details:

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 the following queues.

MDB_QUEUE
MDB_QUEUE_DLQ
MDB_QUEUE_RESPONSE
NOTIFY_QUEUE
NOTIFY_DEST_QUEUE
NOTIFY_QUEUE_DLQ
DEFFERED_DEST_QUEUE

RTGS_INQUEUE
SFMS_INQUEUE
ELMDB_REQ_Q
ELMDB_RES_Q
ELMDB_DLQ
EL_NOTIFY_REQ_Q
EL_NOTIFY_RES_Q
EL_NOTIFY_DLQ
EMS_INQUEUE
EMS_OUTQUEUE
EMS_EXTQUEUE
INTERNAL_BIPREPORT_QUEUE
INTERNAL_BIPADVREPORT_QUEUE
INTERNAL_GI_UPLOAD_QUEUE
EMS_QUEUE_DLQ

3.4 Creating Message Listener

Follow the steps given below:

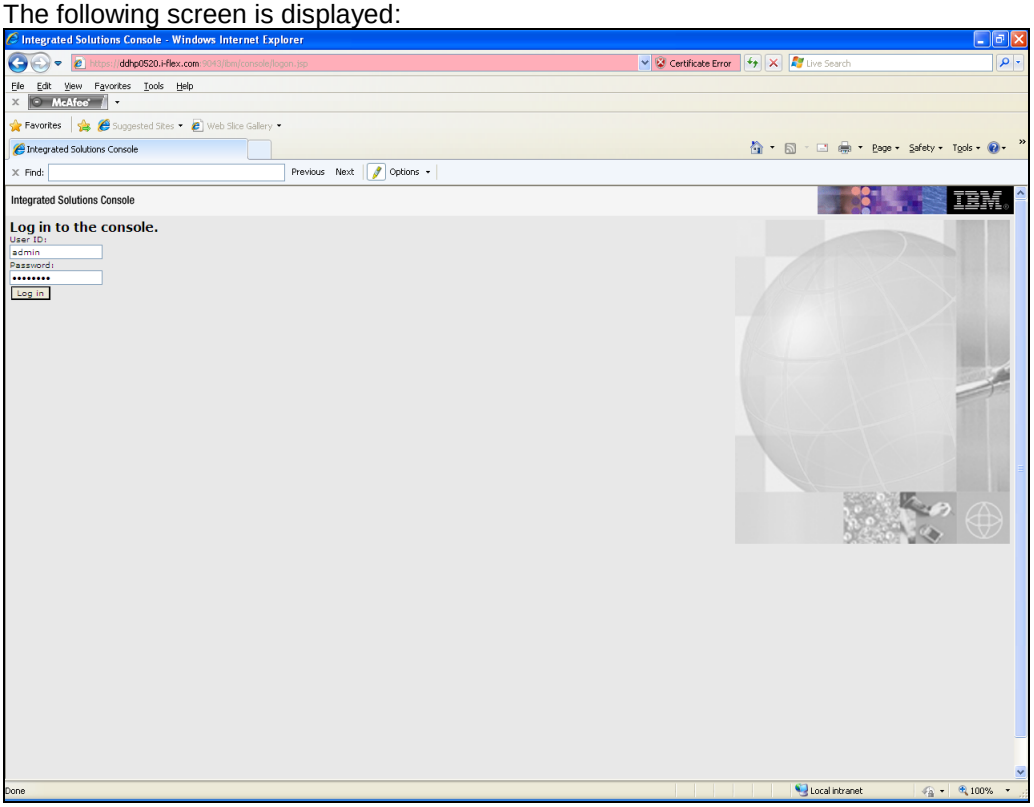
1. Start the administrative console of Websphere application server. Open an internet browser and enter the Websphere admin console URL.

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

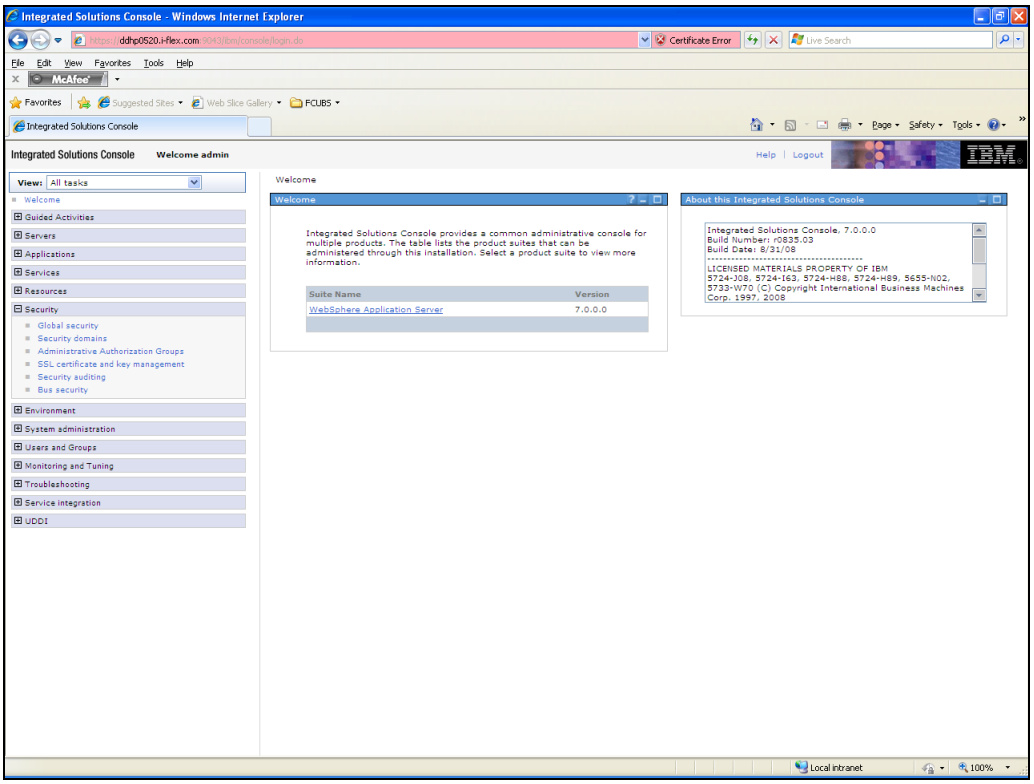
Eg: https://10.10.10.10:1010/console

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

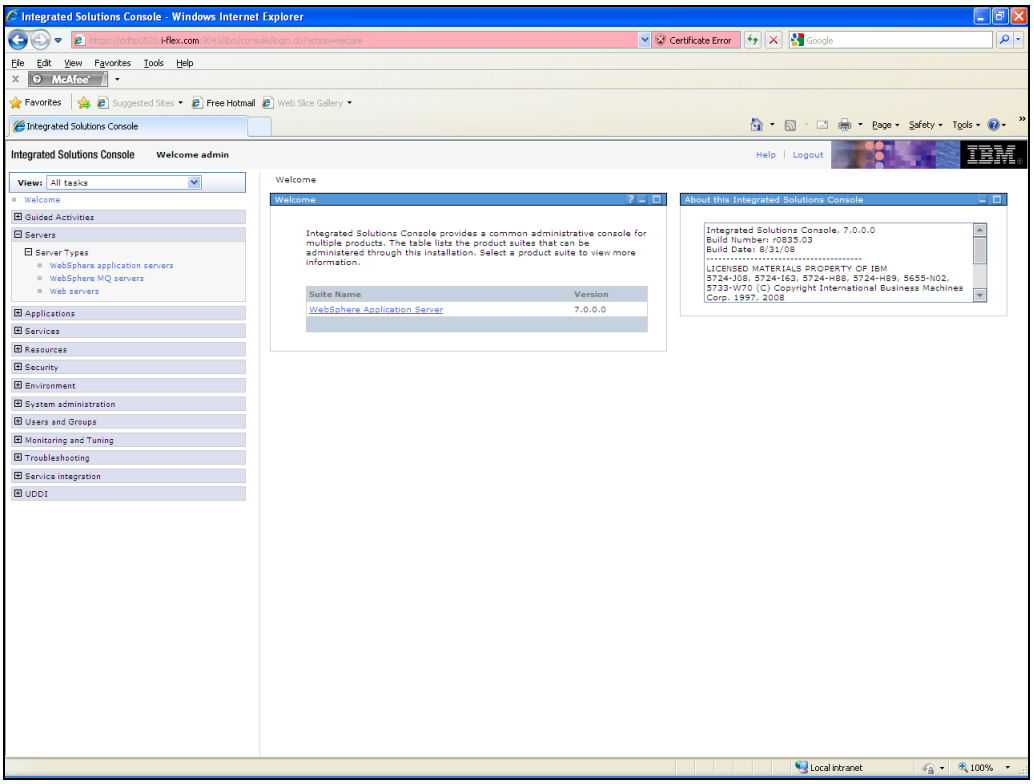
The following screen is displayed:



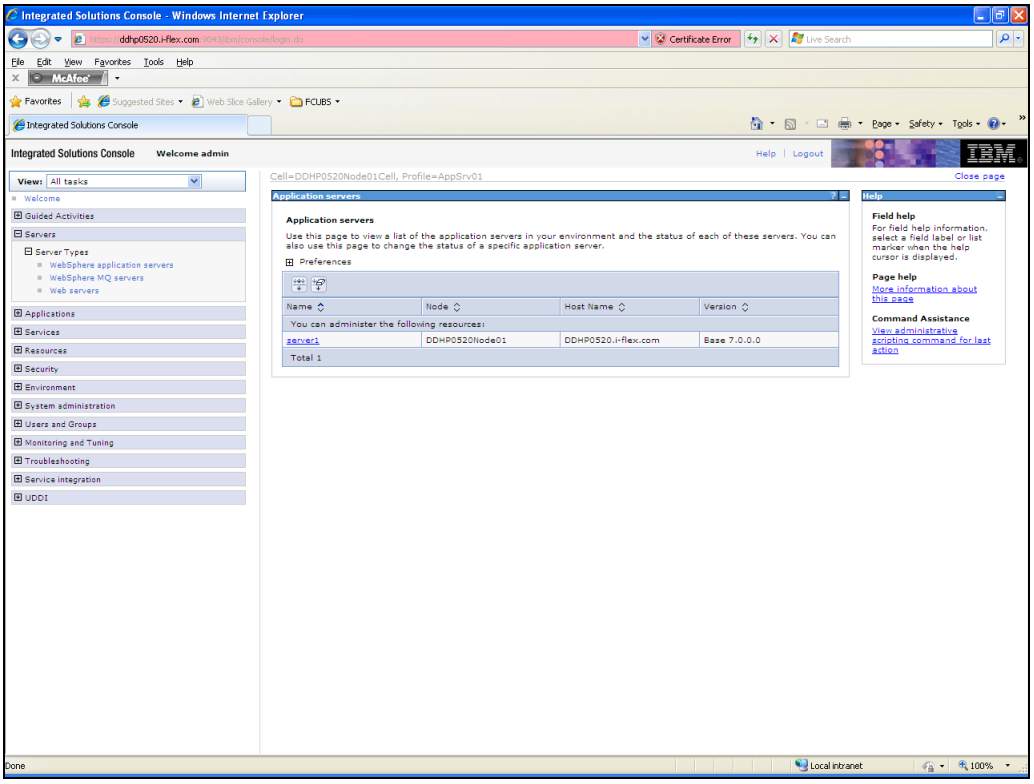
2. Specify the Websphere administrator username and password.
3. Click ‘Log In’.
4. Navigate to Websphere home page.



5. Expand ‘Servers > Server Types’ and click ‘Websphere application servers’.

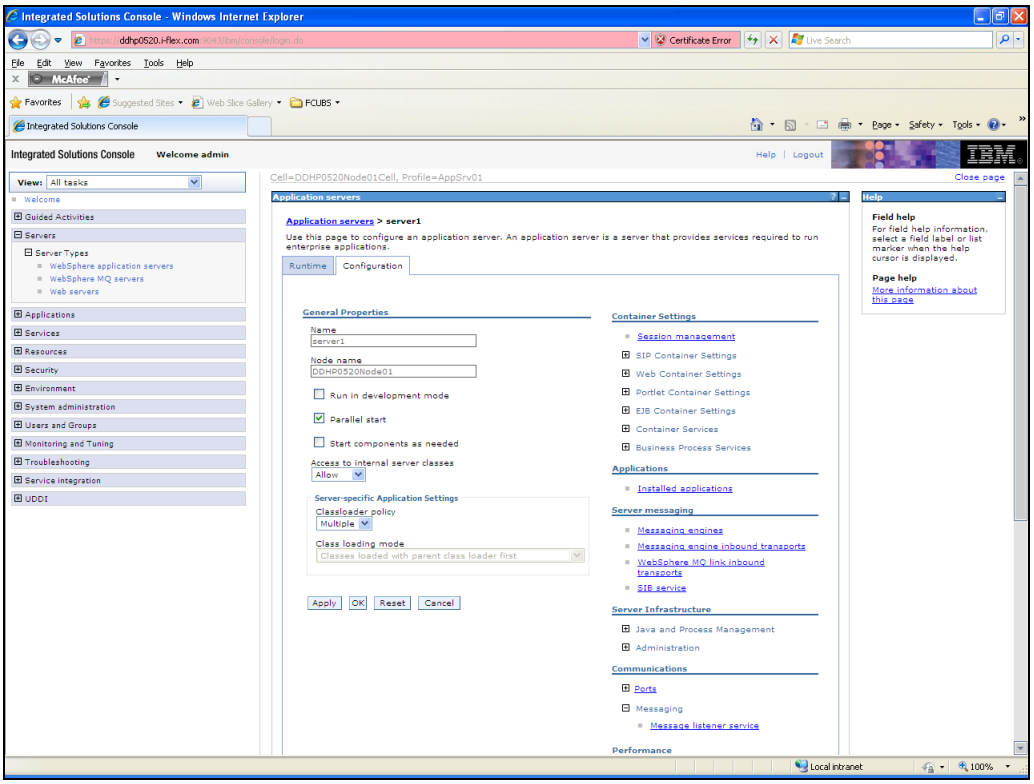


The following screen is displayed.



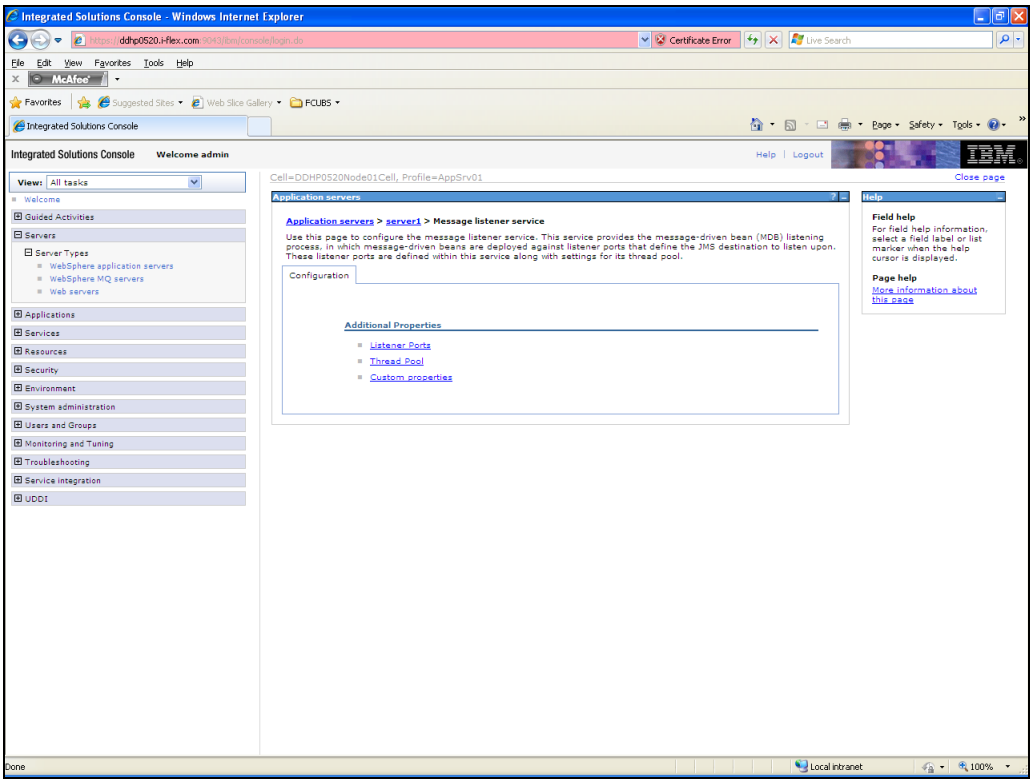
6. Click ‘server1’.

The following screen is displayed.



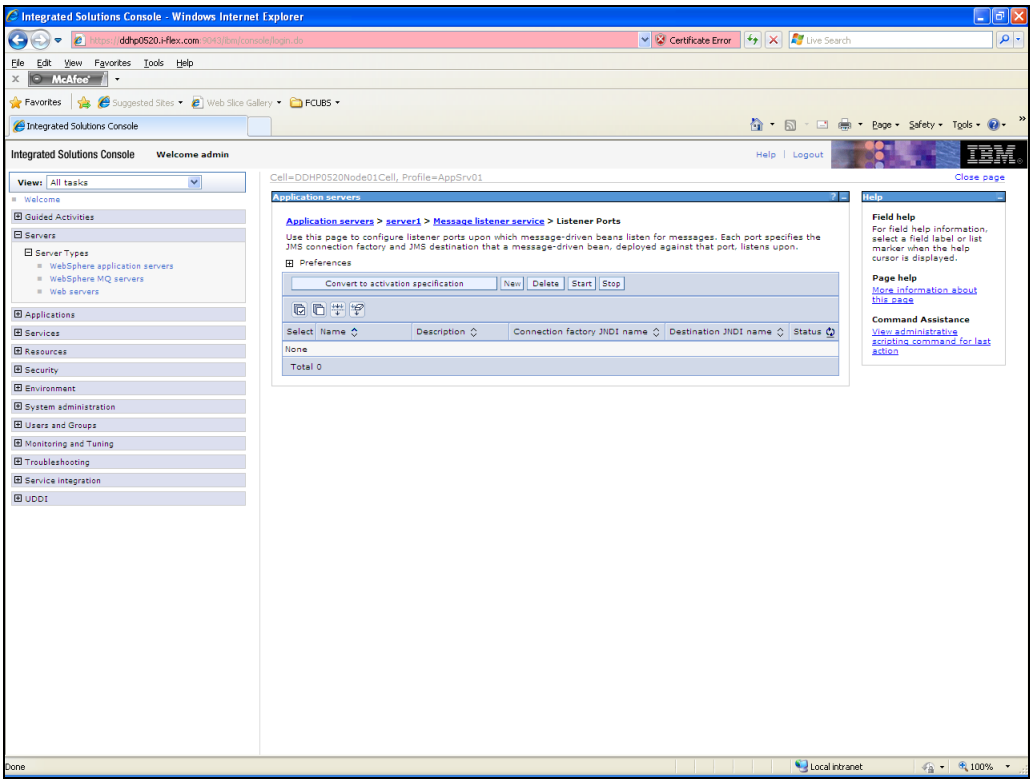
7. Expand ‘Messaging’ and select ‘Message listener service’.

The following screen is displayed.



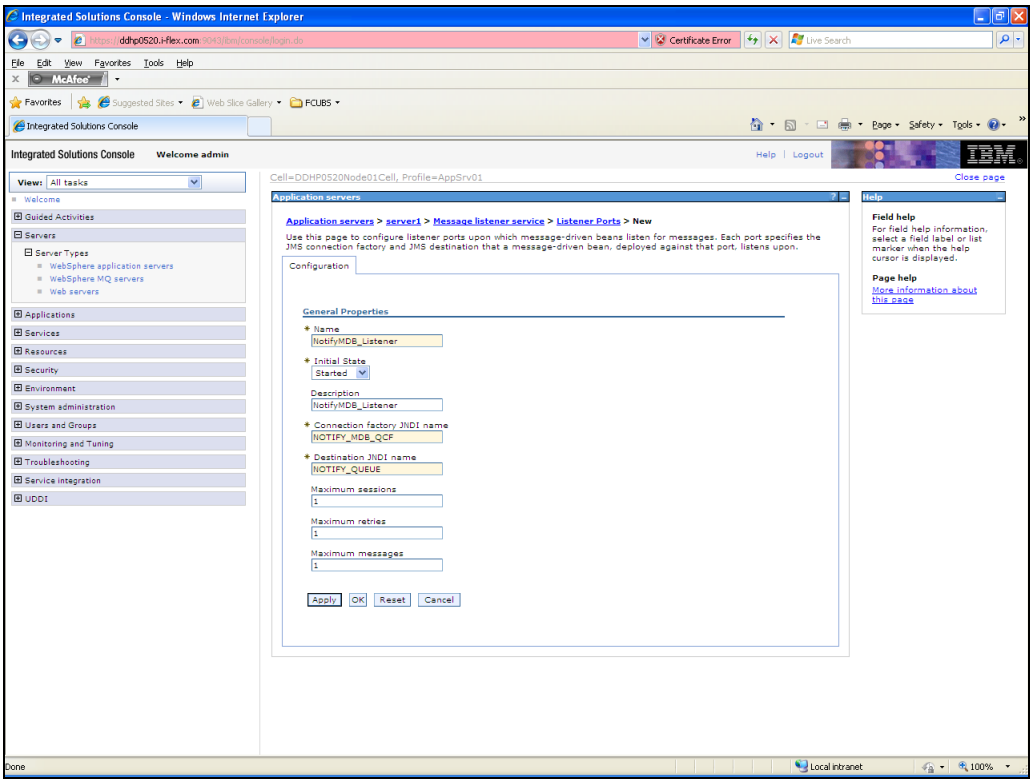
8. Click ‘Listener Ports’.

The following screen is displayed.



9. Click ‘New’.

The following screen is displayed.

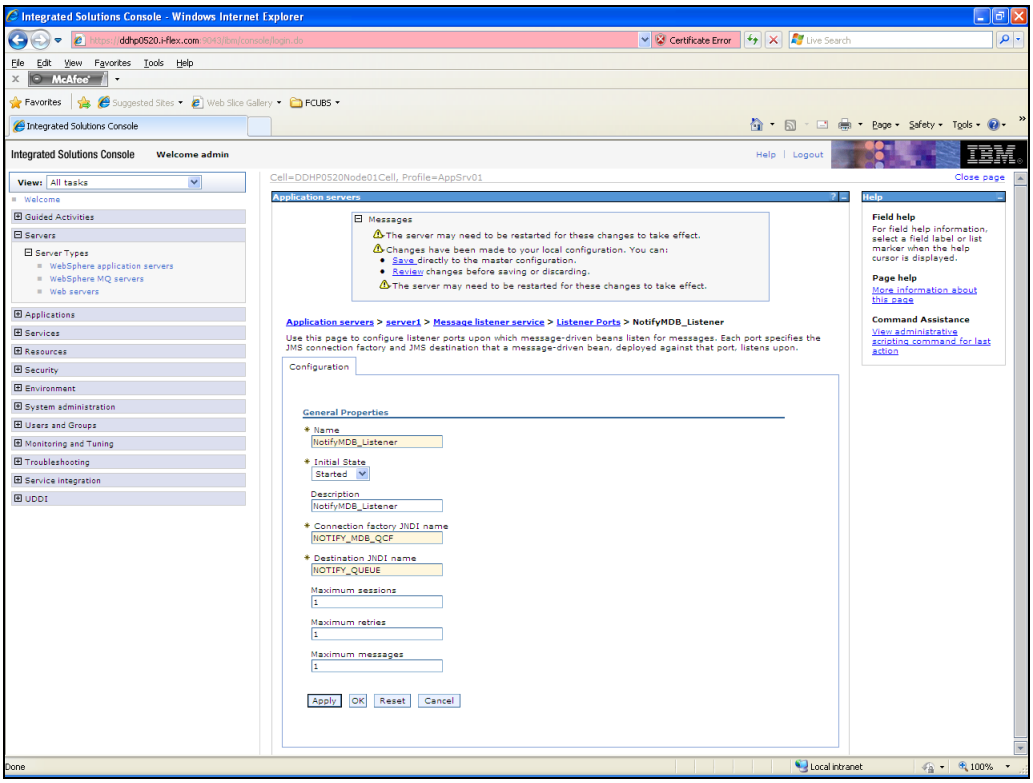


10. Specify the following details:

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

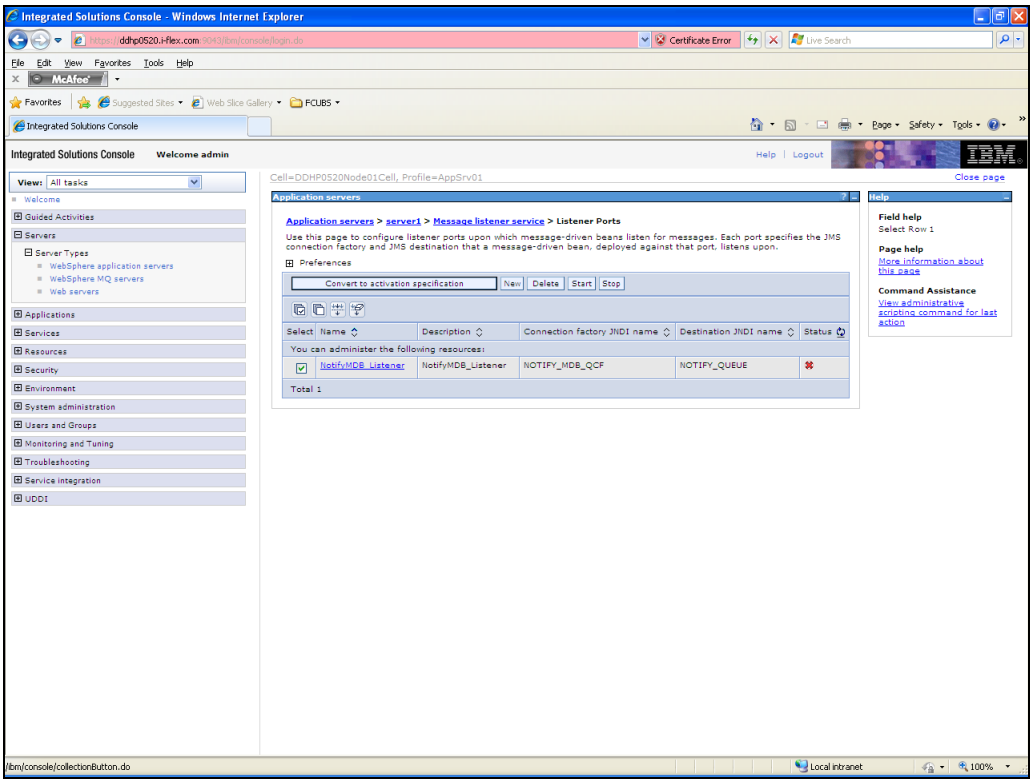
11. Click ‘Apply’.

The following screen is displayed.



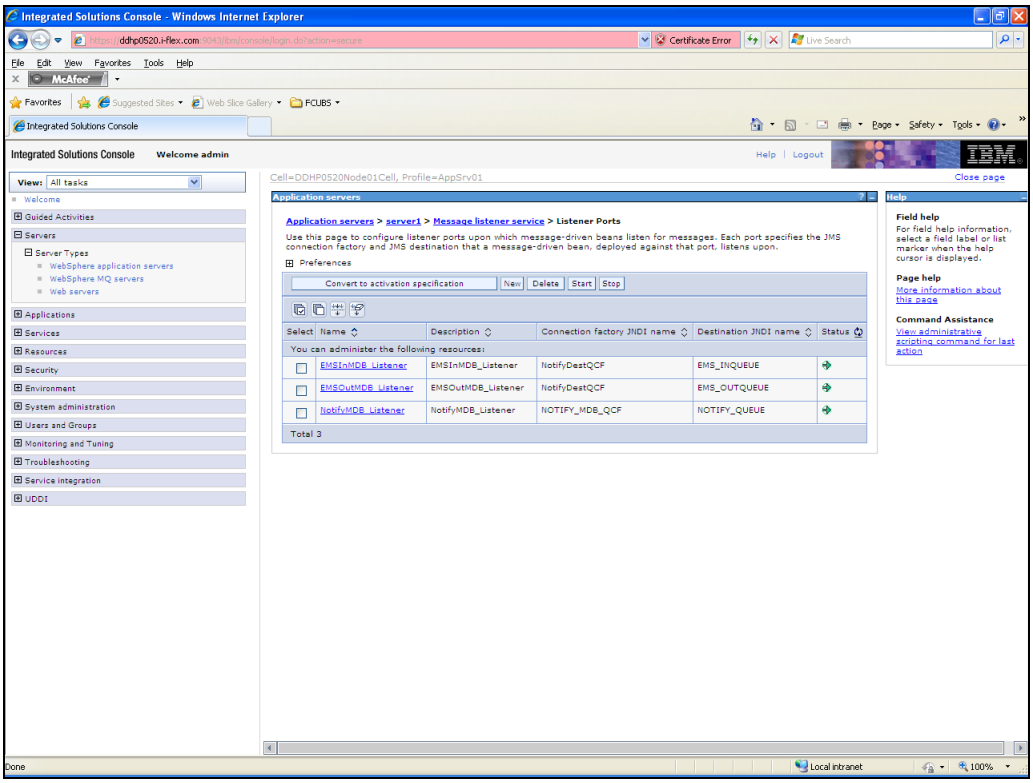
12. Click ‘Save’.

The following screen is displayed.



13. Select ‘NotifyMDB_Listener’. Click ‘Start’.

The following screen is dosplayed.



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

MDB_Listener
NotifyMDB_Listener
RTGS_Listener
SFMS_Listener
ELMDB_Listener
ELNotifyMDB_Listener
EmsIn_Listener
EmsOut_Listener
BipReport_Listener
BipAdvReport_Listener
Gi_Upload_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
GWMDB	MDB_Listener	MDBQCF	MDB_QUEUE
GWNotifyMDBBean	NotifyMDB_Listener	NOTIFY_MDB_QCF	NOTIFY_QUEUE
RTGSInMDB	RTGS_Listener	RTGSQCF	RTGS_INQUEUE
SFMSInMDB	SFMS_Listener	SFMSQCF	SFMS_INQUEUE
ELGWMDBBean	ELMDB_Listener	ELMDBQCF	ELMDB_REQ_Q
ELNotifyMDBBean	ELNotifyMDB_Listener	EL_NOTIFY_QCF	EL_NOTIFY_REQ_Q
EMSInMDB	EmsIn_Listener	EmsQcf	EMS_INQUEUE
EMSOutMDB	EmsOut_Listener	EmsQcf	EMS_OUTQUEUE
BipReportMDB	BipReport_Listener	BIPQCF	INTERNAL_BIPREPORT_QUEUE
BipAdviceMDB	BipAdvReport_Listener	BIPQCF	INTERNAL_BIPADVREPORT_QUEUE
GIUploadMDB	Gi_Upload_Listener	GI_UPLOAD_QCF	INTERNAL_GI_UPLOAD_QUEUE

Here,

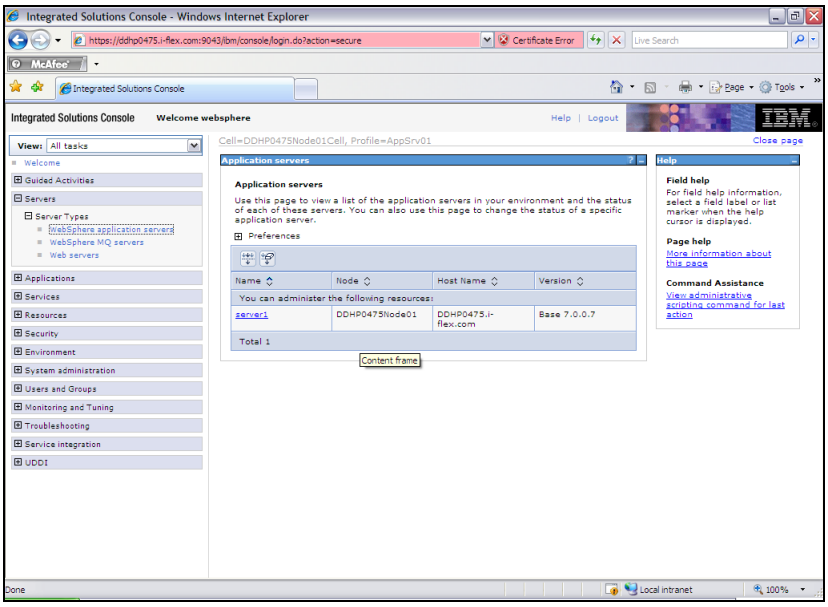
- MDB_Listener is mandatory for Gateway MDB applications
- All others are required for FCJ Applications embedded with Scheduler and ELCM

4. Default Settings for Web Sphere

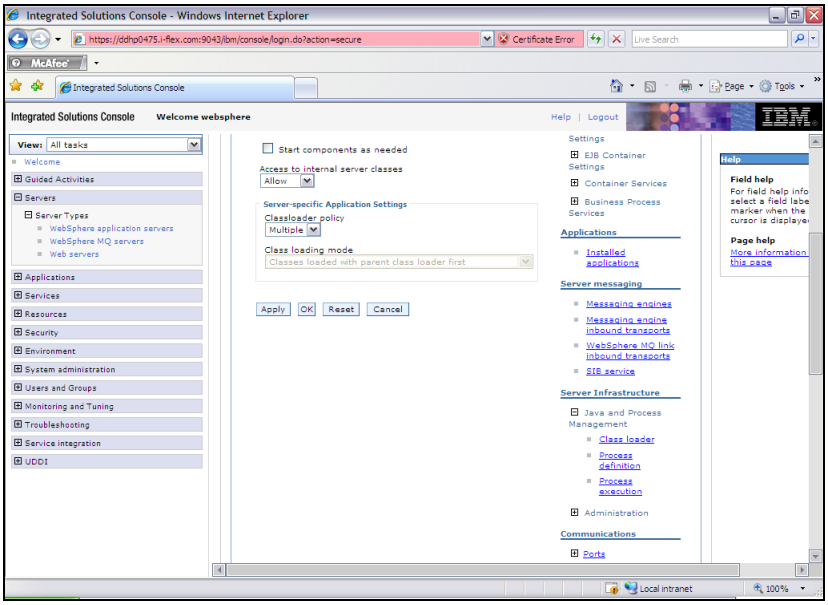
4.1 JVM Custom Toplink Property

To set the JVM toplink properties, follow the steps below:

1. Navigate to ‘Application servers > {Configured Server} > Java and Process Management>) Process Definition > Java Virtual Machine > Custom Properties >’.

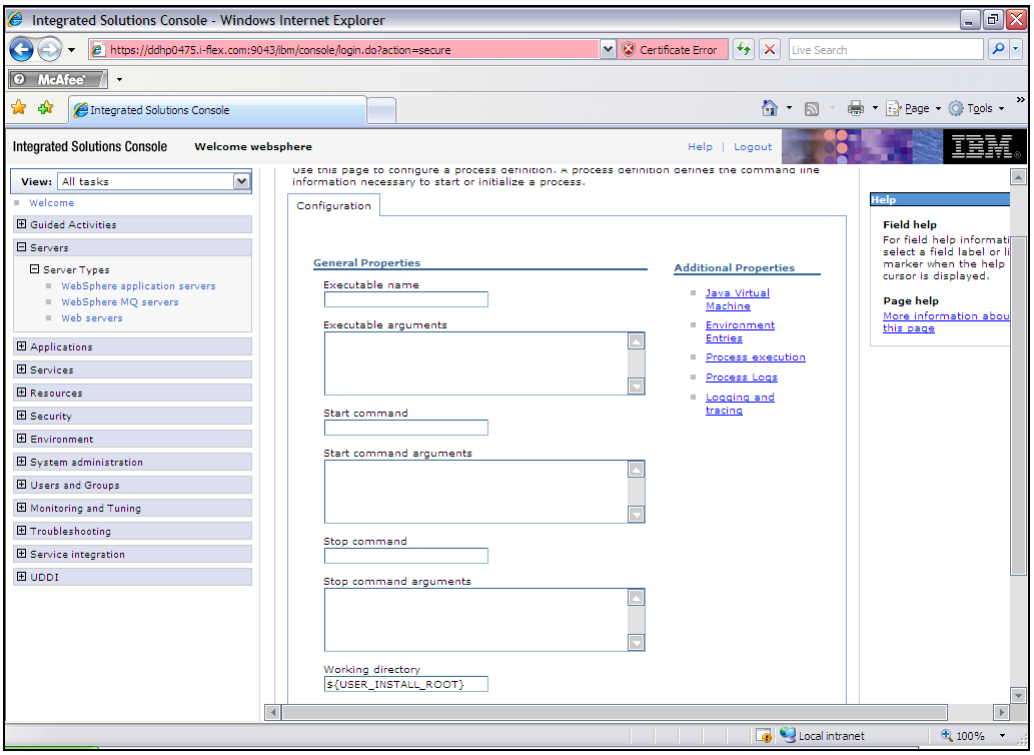


2. Expand ‘Java and Process Management’.

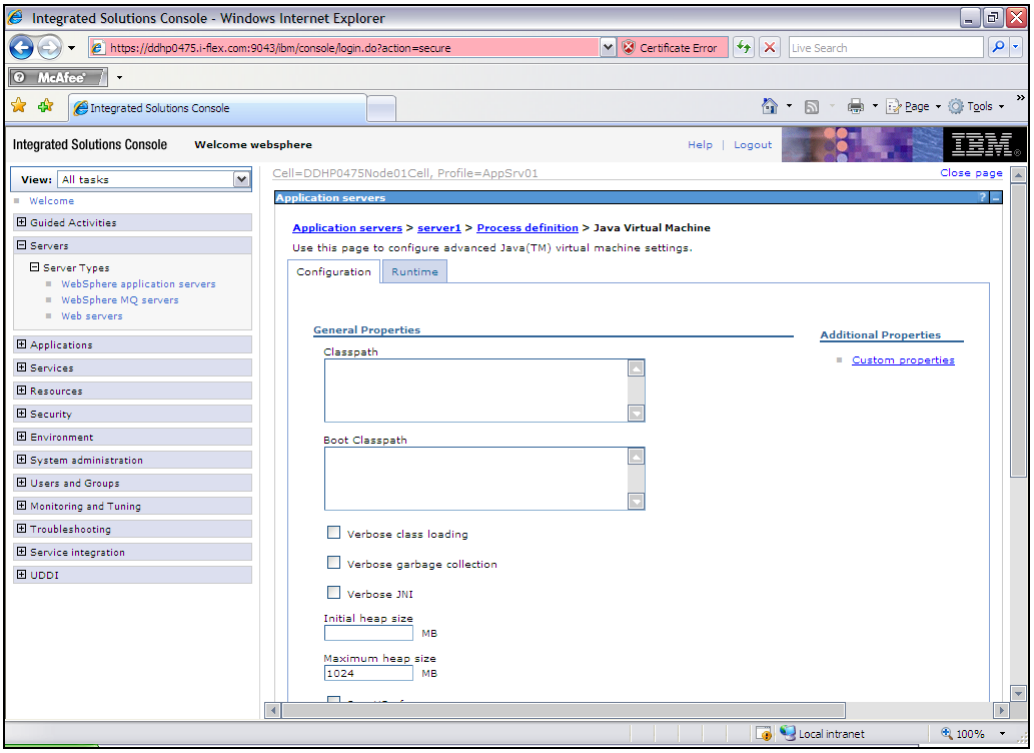


3. Click on ‘Process definition’.

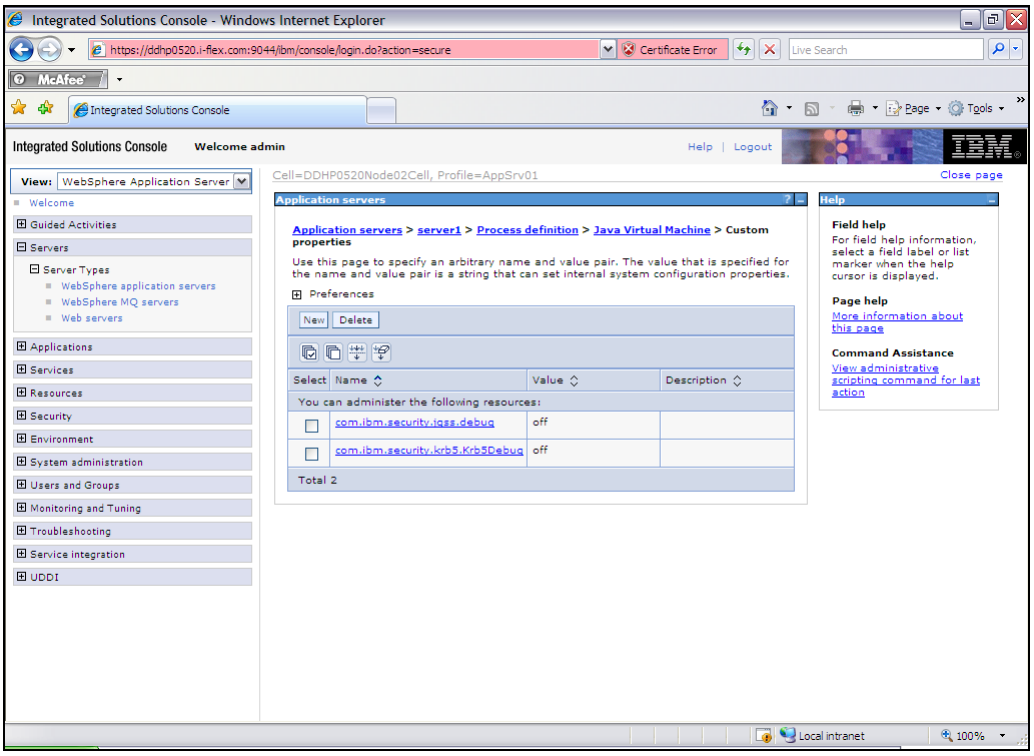
The following screen is displayed:



4. Click ‘Custom Properties’.

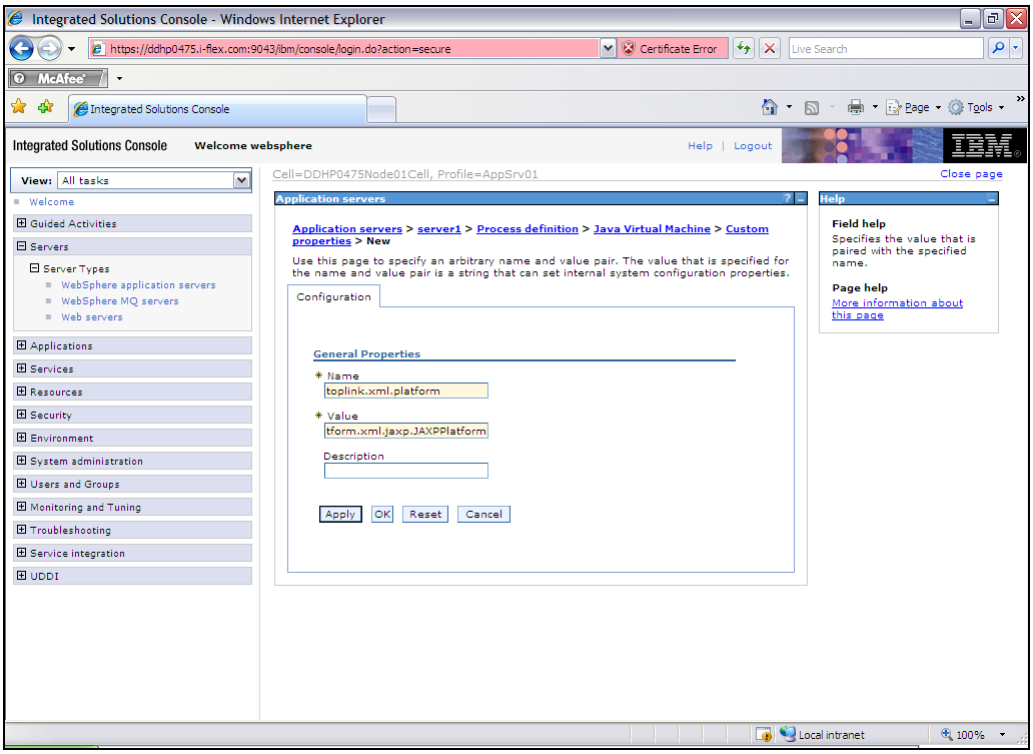


The following screen is displayed:



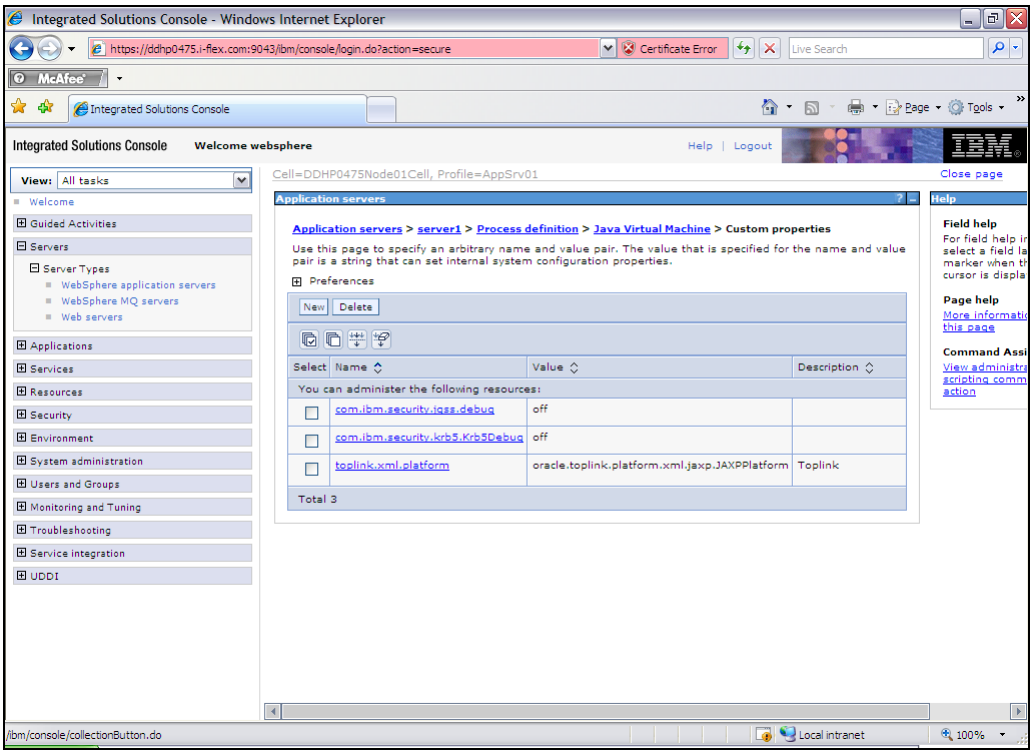
5. Click ‘New’.

The following screen is displayed:



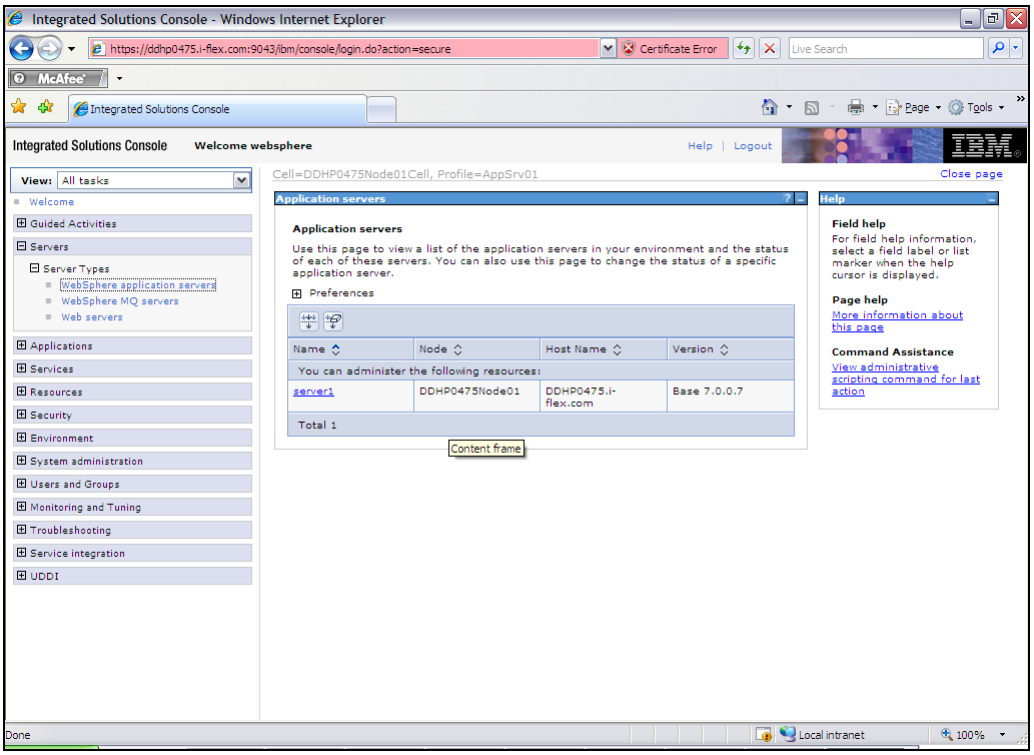
6. Specify the Name ‘toplink.xml.platform’.
7. Specify the value ‘tform.xml.jaxp.JAXPPlatform’.
8. Click ‘Apply’.

The following screen is displayed:



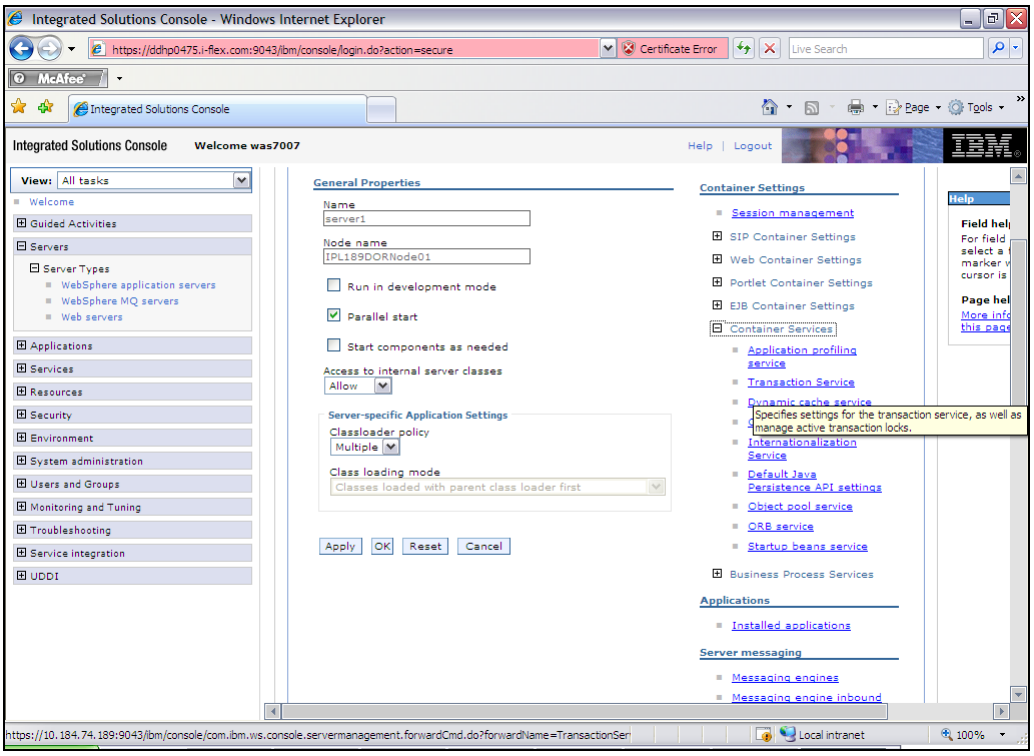
Transaction Services Changes

9. Navigate to Application servers > {Configured Server}.



10. On the right, expand ‘Container services’ and click on ‘Transaction service’.

The following screen is displayed:

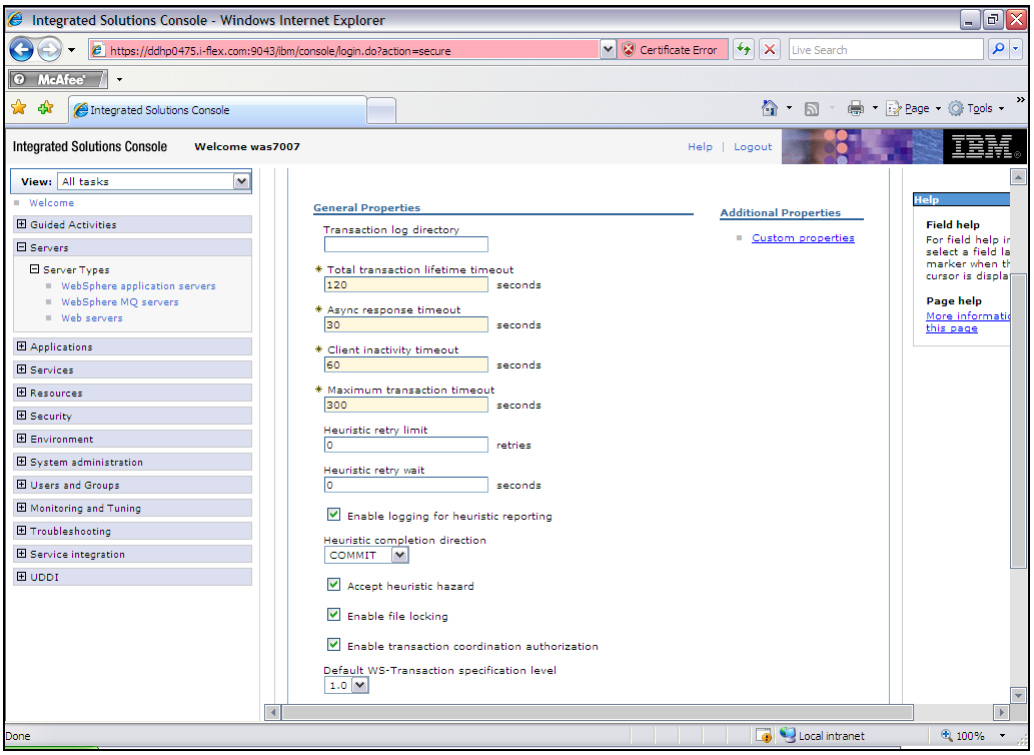


11. Specify the following details.

Against ‘Heuristic completion direction’, select COMMIT from the drop down list.

Check the option ‘Accept heuristic hazard’.

12. It is optional to check ‘Enable logging for heuristic reporting’. This will enable logging of heuristic reporting.


Integrated Solutions Console - Windows Internet Explorer
https://ddhp0475.i-flex.com:9043/ibm/console/login.do?action=secure
Certificate Error
Live Search
Integrated Solutions Console
Page
Tools
Integrated Solutions Console
Welcome was7007
Help | Logout
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
General Properties
Transaction log directory
Total transaction lifetime timeout
120
seconds
Async response timeout
30
seconds
Client inactivity timeout
60
seconds
Maximum transaction timeout
300
seconds
Heuristic retry limit
0
retries
Heuristic retry wait
0
seconds
Enable logging for heuristic reporting
Heuristic completion direction
COMMIT
Accept heuristic hazard
Enable file locking
Enable transaction coordination authorization
Default WS-Transaction specification level
1.0
Additional Properties
Custom properties
Help
Field help
Page help
Done
Local intranet
100%

5. Configuring Mail Session on Websphere

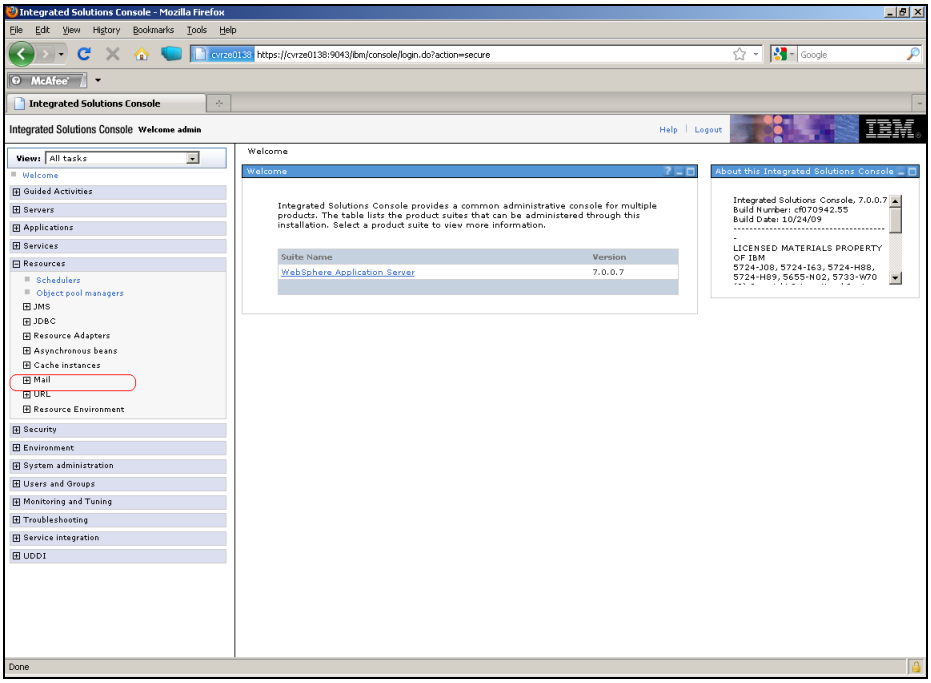
5.1 Introduction

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

5.2 Creating Java Mail Session

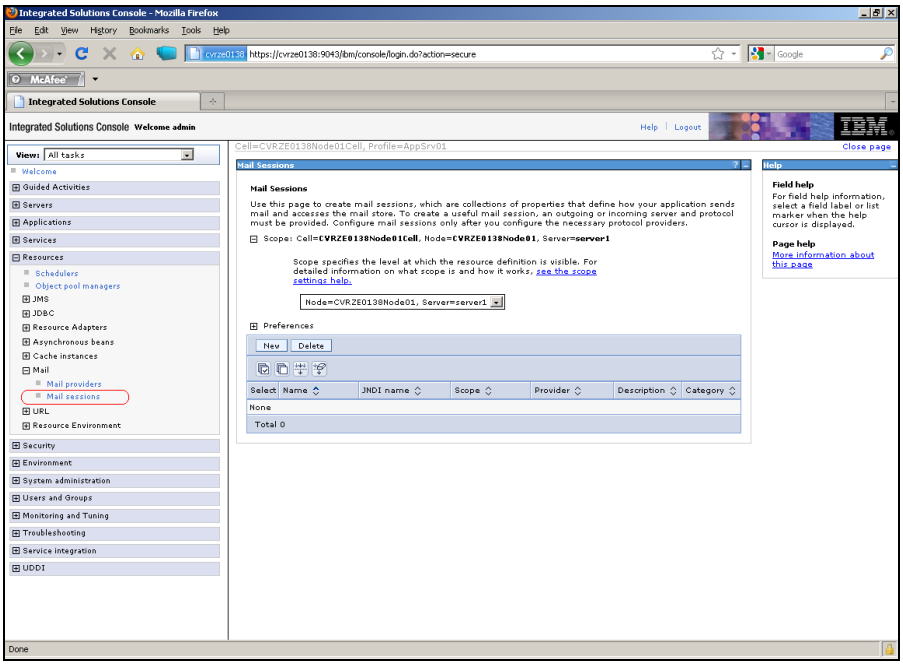
To create Java mail session, follow the steps given below:

13. On the left pane, expand ‘Resources’ and select ‘Mail’.



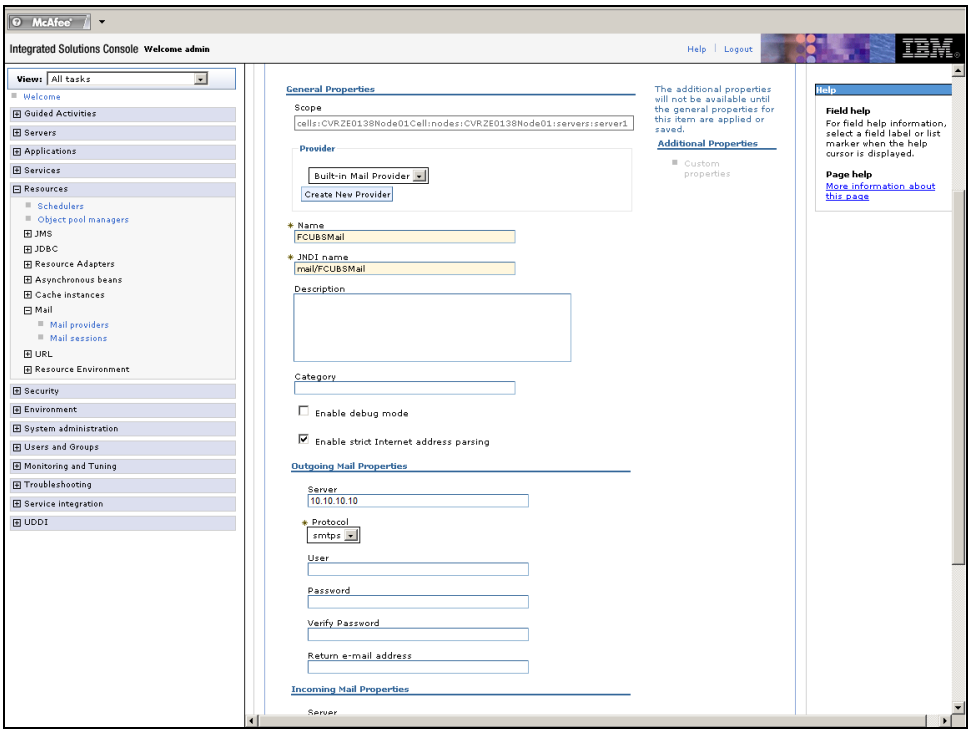
14. Click ‘Mail Sessions’ to invoke the ‘Mail sessions’ screen.

The following screen is displayed:



15. Click ‘New’ button to create a new mail session.

The following screen is displayed:

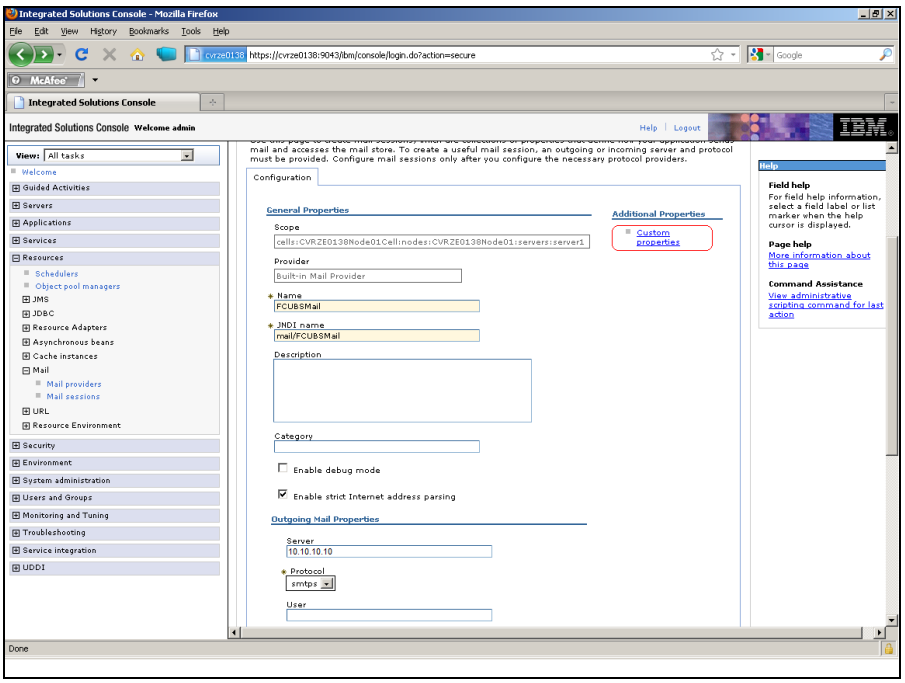


16. Provide the required information. Sample details are given below for your reference.

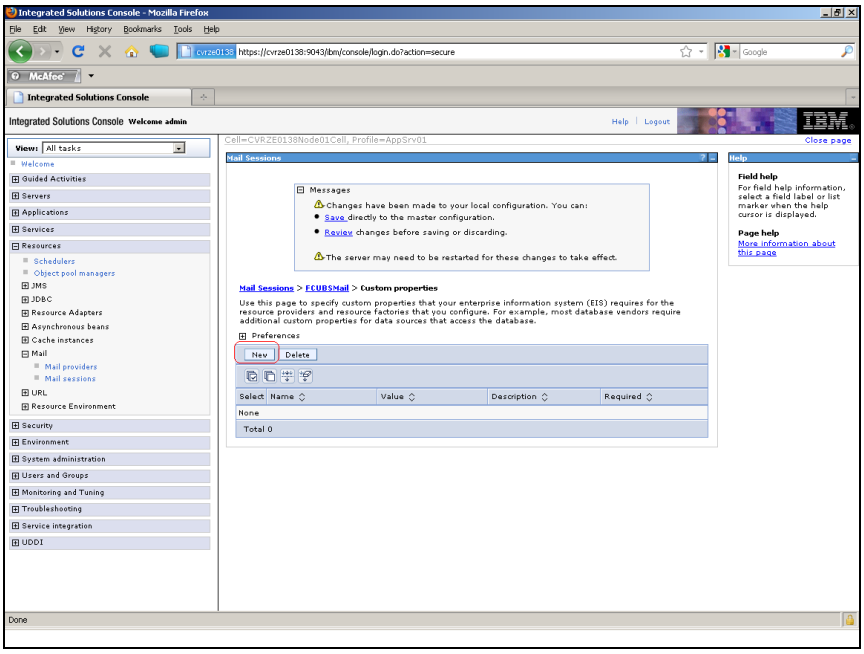
General Properties

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

17. Click ‘Custom Properties’ link to configure the custom properties.

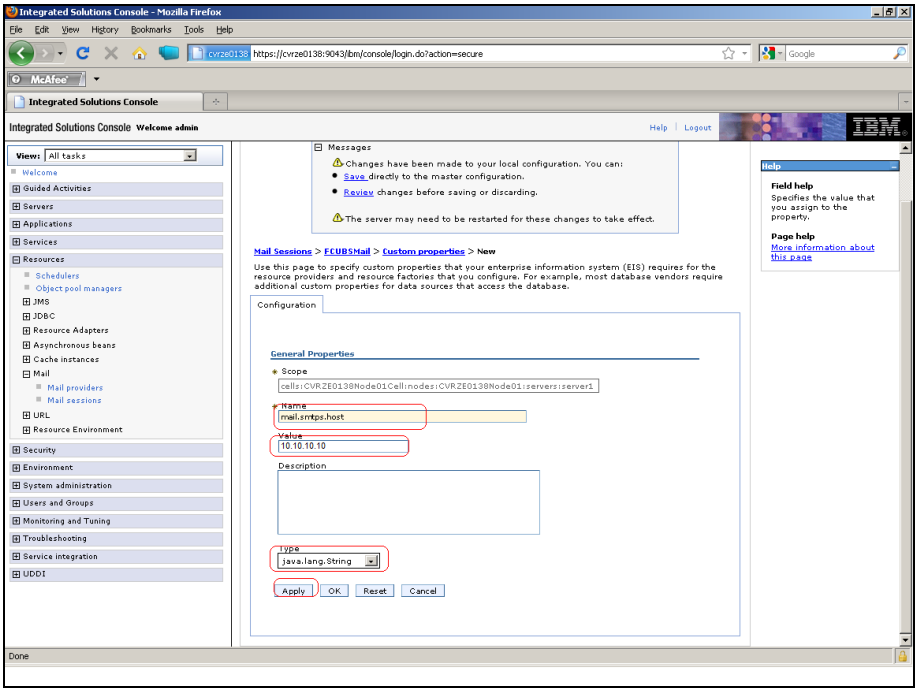


The following screen is displayed.



18. Click ‘New’ button to create new custom properties.

The following screen is displayed.



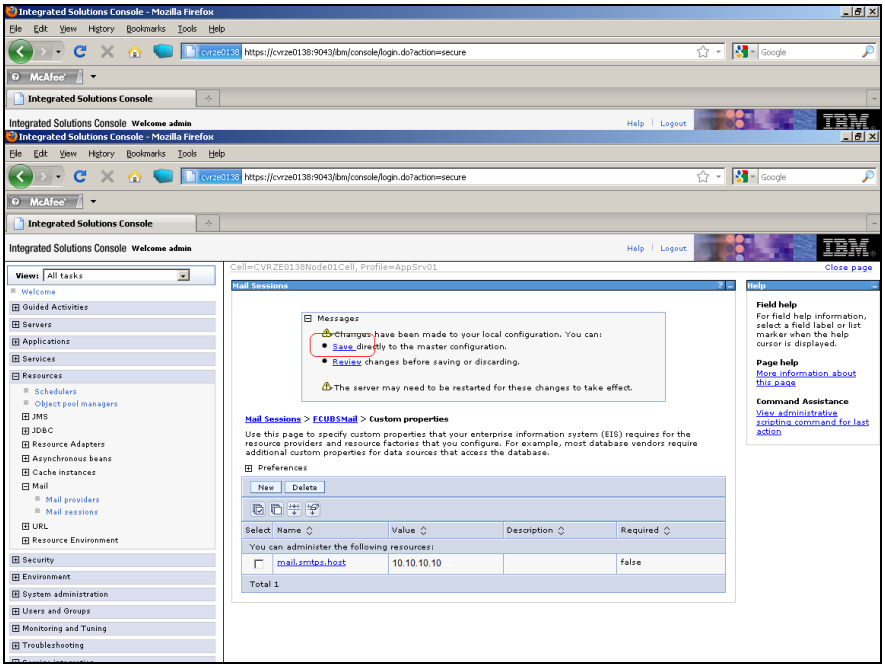
19. Specify the information required for creating custom properties. Sample details are given below:

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.

SSL Configuration on Websphere
[April] [2014]
Version 12.0.3.0.0

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/