

Application Installation Guide

Oracle Financial Services Lending and Leasing

Release 14.2.0.0.0

Part No. E59770-01

December 2014

Application Installation Guide
December 2014
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, 2014, Oracle and/or its affiliates. All rights reserved.

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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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.

Table of Contents

| | |
|---|-------------|
| 1. Preface | 1-1 |
| 1.1 Prerequisites | 1-1 |
| 1.2 Audience | 1-2 |
| 1.3 Conventions Used | 1-2 |
| 2. Installing Software | 2-1 |
| 2.1 Installing Oracle WebLogic Server 11g | 2-1 |
| 2.2 Installing Oracle ADF Runtime | 2-7 |
| 3. Creating Domains, Repositories, Data Sources | 3-1 |
| 3.1 Creating Domain and Servers | 3-1 |
| 3.2 Applying the JRF Template | 3-8 |
| 3.3 Creating Schemas using Repository Creation Utility | 3-9 |
| 3.4 Creating Metadata Repository | 3-15 |
| 3.5 Creating Data Source | 3-18 |
| 3.6 Creating SQL Authentication Provider | 3-24 |
| 3.7 Creating User Groups and Users | 3-29 |
| 3.7.1 <i>Creating Users</i> | 3-29 |
| 3.7.2 <i>Creating User Groups</i> | 3-31 |
| 3.7.3 <i>Assigning Users to Groups</i> | 3-32 |
| 3.7.4 <i>Resetting password via weblogic console</i> | 3-32 |
| 3.8 Implementing JMX Policy for Change Password | 3-33 |
| 3.9 Migrating Policy from File to Database | 3-38 |
| 4. Configuring Policies | 4-1 |
| 4.1 Configuring Password Policy for SQL Authenticator | 4-1 |
| 4.2 Configuring User Lockout Policy | 4-3 |
| 5. Deploying Application | 5-1 |
| 5.1 Deploying Application | 5-1 |
| 6. Enabling SSL | 6-1 |
| 7. Launching Application | 7-1 |
| 8. Mapping Enterprise Group with Application Role | 8-1 |
| 9. Configuring Oracle BI Publisher for Application | 9-1 |
| 10. Configuring JNDI name for HTTP Listener | 10-1 |
| 11. Appendix | A-1 |
| 11.1 XManager Usage | A-1 |

1. Preface

This document contains notes and installation steps needed to install and setup Oracle Financial Services Lending and Leasing. Oracle Financial Services Lending and Leasing relies on several pieces of Oracle software in order to run and this document is in no way meant to replace Oracle documentation supplied with these Oracle products or available via Oracle technical support. The purpose of this document is only meant to supplement the Oracle documentation and to provide Oracle Financial Services Lending and Leasing specific installation instructions.

For recommendations on security configuration, refer Security Configuration Guide.

It is assumed that anyone installing Oracle Financial Services Lending and Leasing will have a thorough knowledge and understanding of Oracle Weblogic Server 10.3.6, Oracle BI Publisher 11.1.1.7.

Application installation is a nine step process.

1. [Installing Software](#)
2. [Creating Domains, Repositories, Data Sources](#)
3. [Configuring Policies](#)
4. [Deploying Application](#)
5. [Enabling SSL](#)
6. [Launching Application](#)
7. [Mapping Enterprise Group with Application Role](#)
8. [Configuring Oracle BI Publisher for Application](#)
9. [Configuring JNDI name for HTTP Listener](#)

1.1 Prerequisites

The following software are required to install Oracle Financial Services Lending and Leasing application and they are available from the following sources:

- Oracle Software Delivery Cloud (<http://edelivery.oracle.com/>)
 - Oracle Technology Network (OTN)
1. Sun JDK Version 1.7.0_55 or above <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
 2. Oracle Repository Creation Utility (RCU) Version 11.1.1.7.0. Download RCU for the respective platform from the "Required Additional Software" section of <http://www.oracle.com/technetwork/middleware/bi-publisher/downloads/index.html>. RCU is available only on Linux and Windows operating systems. Either the Linux RCU or Windows RCU may be used to create schemas in a supported database.
 3. Oracle Repository Creation Utility (RCU) Version 11.1.1.7.0. Download RCU for the respective platform from the "Required Additional Software" section of <http://www.oracle.com/technetwork/middleware/bi-publisher/downloads/index.html>
 4. Oracle WebLogic Server 11gR1 Version 10.3.6 (<http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html>)

Navigate to Oracle WebLogic Server 11gR1 (10.3.6) + Coherence - Package Installer and download the file for respective OS.

To use WebLogic Server with 64-bit JVM's on Linux and Solaris or to use WLS on other supported platforms, use the WebLogic Server generic installer listed under "Additional Platforms". The generic installers do not include a JVM/JDK. These are to be downloaded and installed prior to installing the Weblogic Server.

5. Oracle ADF 11g
<http://www.oracle.com/technetwork/developer-tools/adf/downloads/index.html>

Note

Please use all 64-bit software's for machine hosted with 64-bit O/S.

Note

Use XManager for remote UNIX/LINUX machine. Please refer [XManager Usage](#).

1.2 **Audience**

This document is intended for system administrators or application developers who are installing Oracle Financial Services Lending and Leasing Application.

1.3 **Conventions Used**

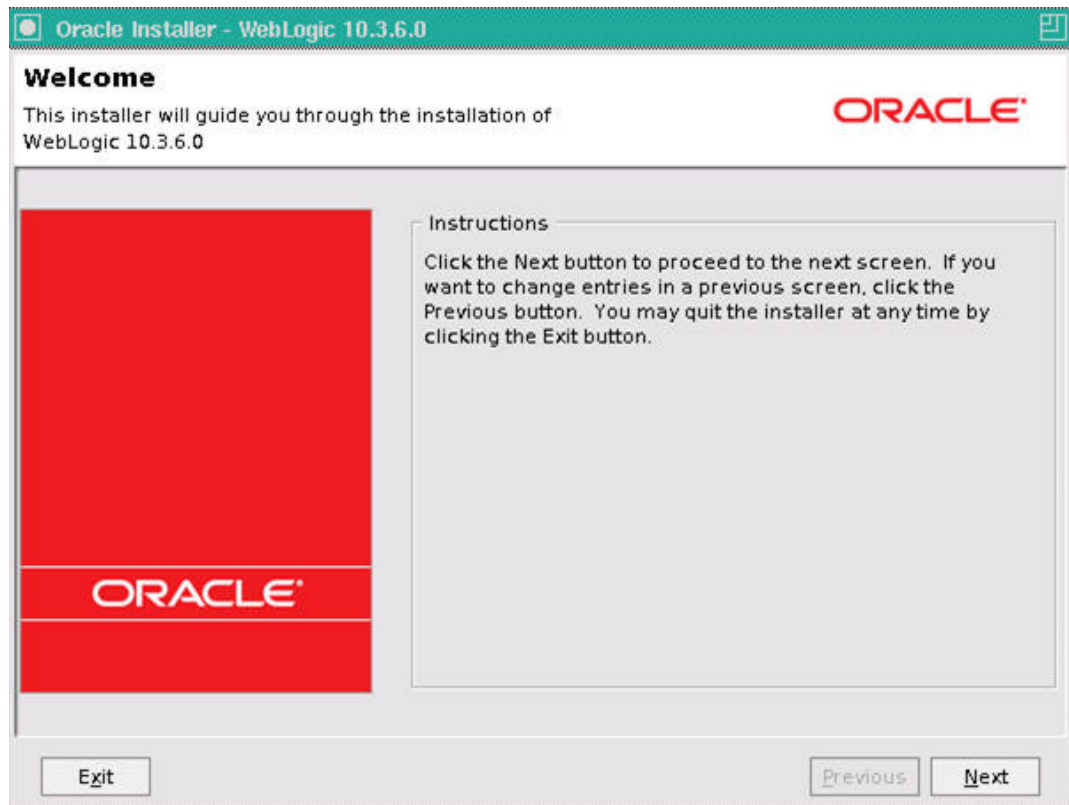
| Term | Refers to |
|-------------|---|
| Application | Oracle Financial Services Lending and Leasing |

2. Installing Software

2.1 Installing Oracle WebLogic Server 11g

To install using generic Weblogic installer -

1. Run the command → `java -jar wls1036_generic.jar`
2. Welcome screen is displayed as shown below.



3. Click **Next** to continue.



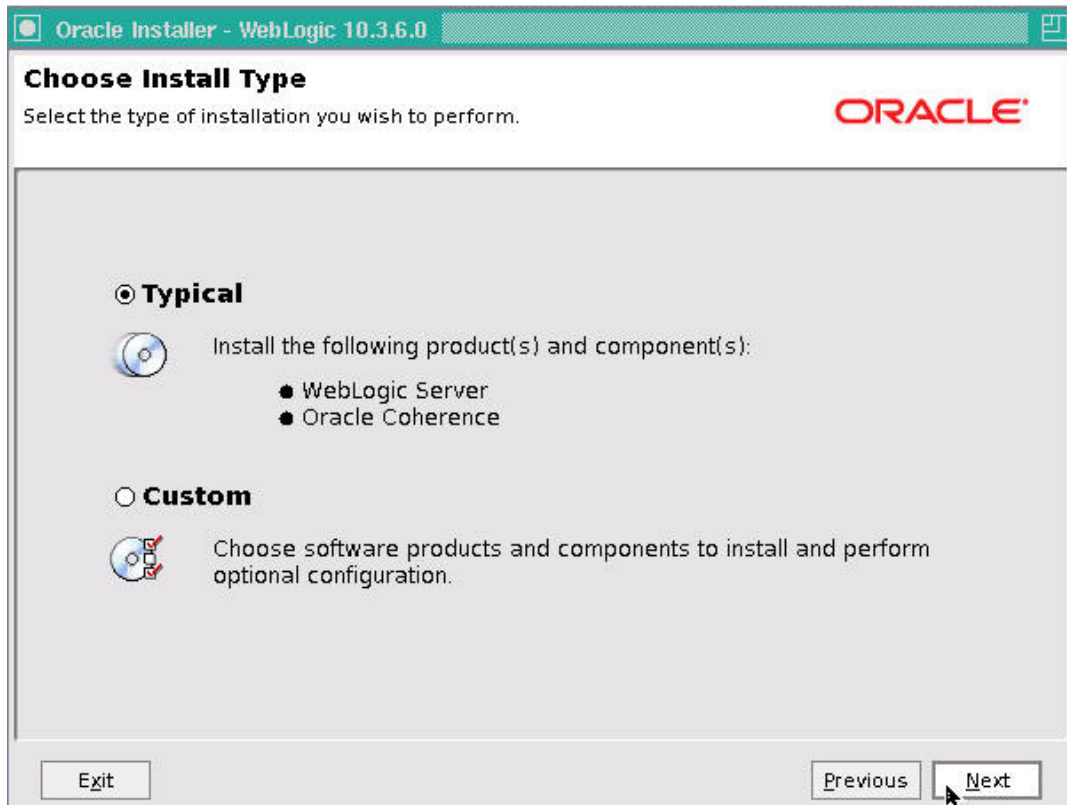
4. Select **Create a new Middleware Home** as **Middleware Home Type**
5. Specify the path for **Middleware Home Directory**, and then click **Next**.
6. The following window is displayed.

7. . Uncheck the check box as in the above screen and click Next. Confirmation window is

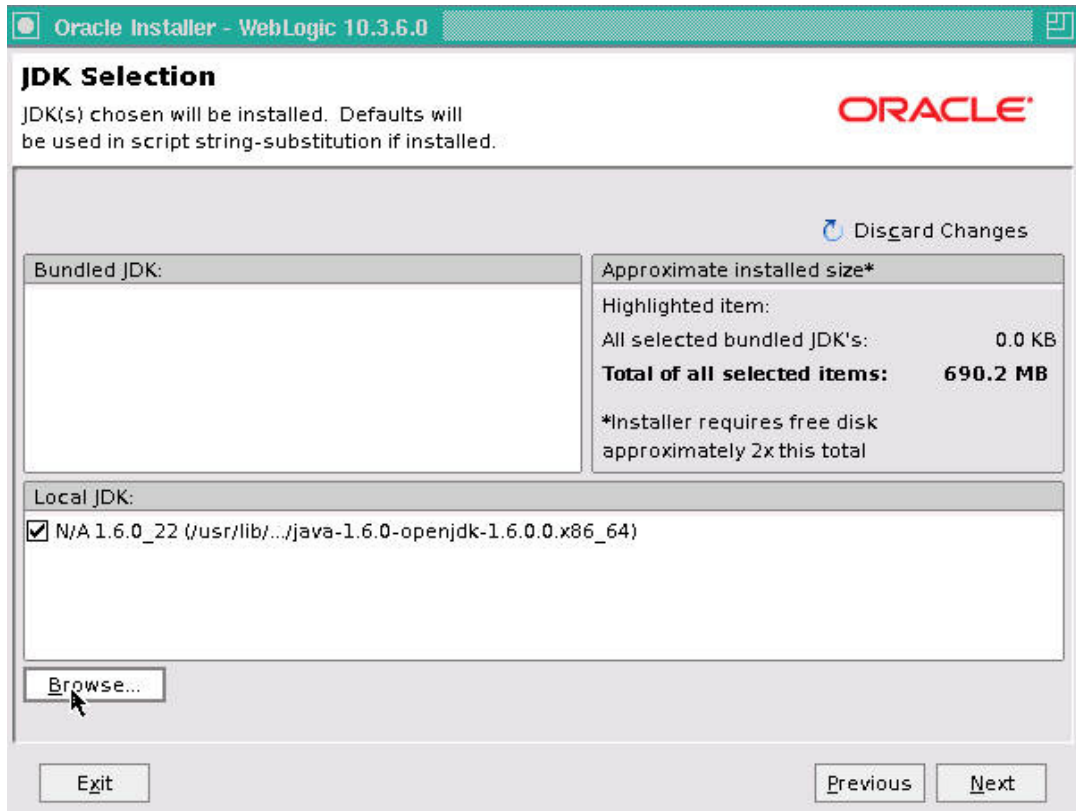


displayed . Click on Yes

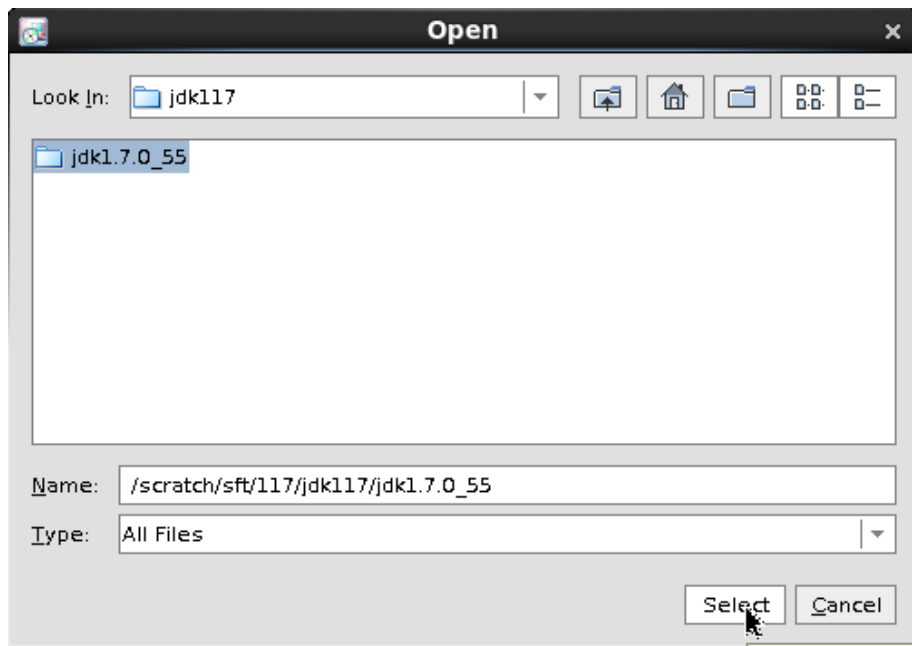
8. Click on **Next** The following window is displayed.



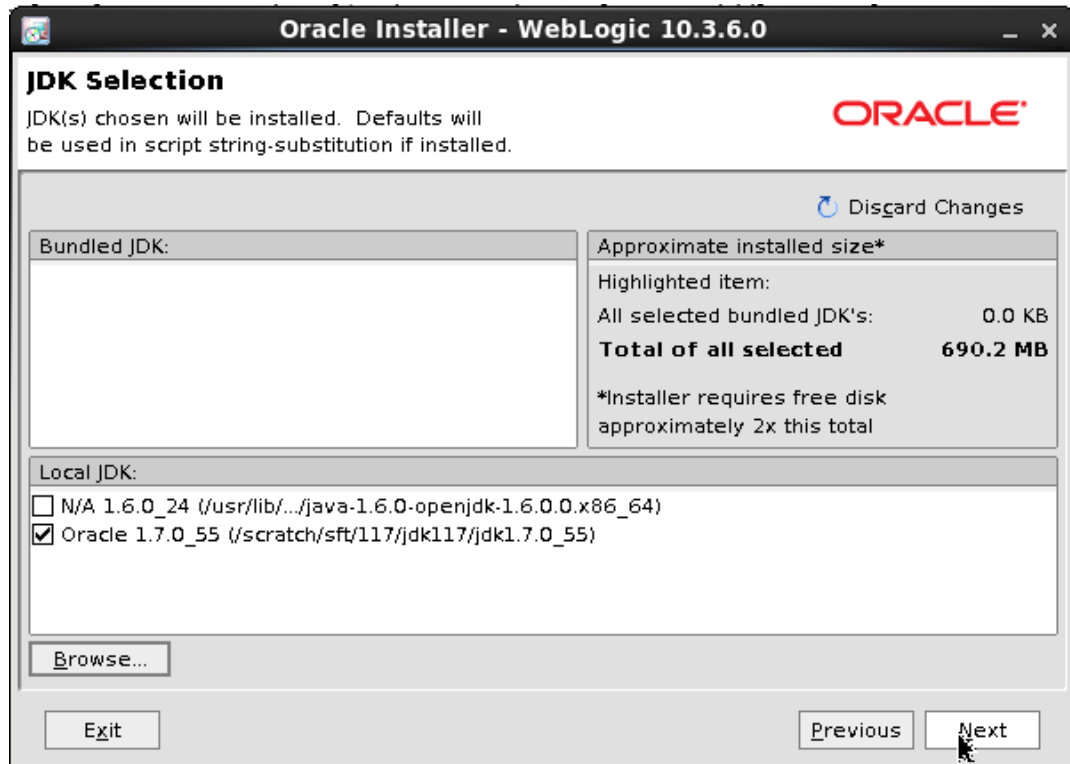
9. Select 'Typical' as the 'Install Type' and click **Next**. The following window is displayed.



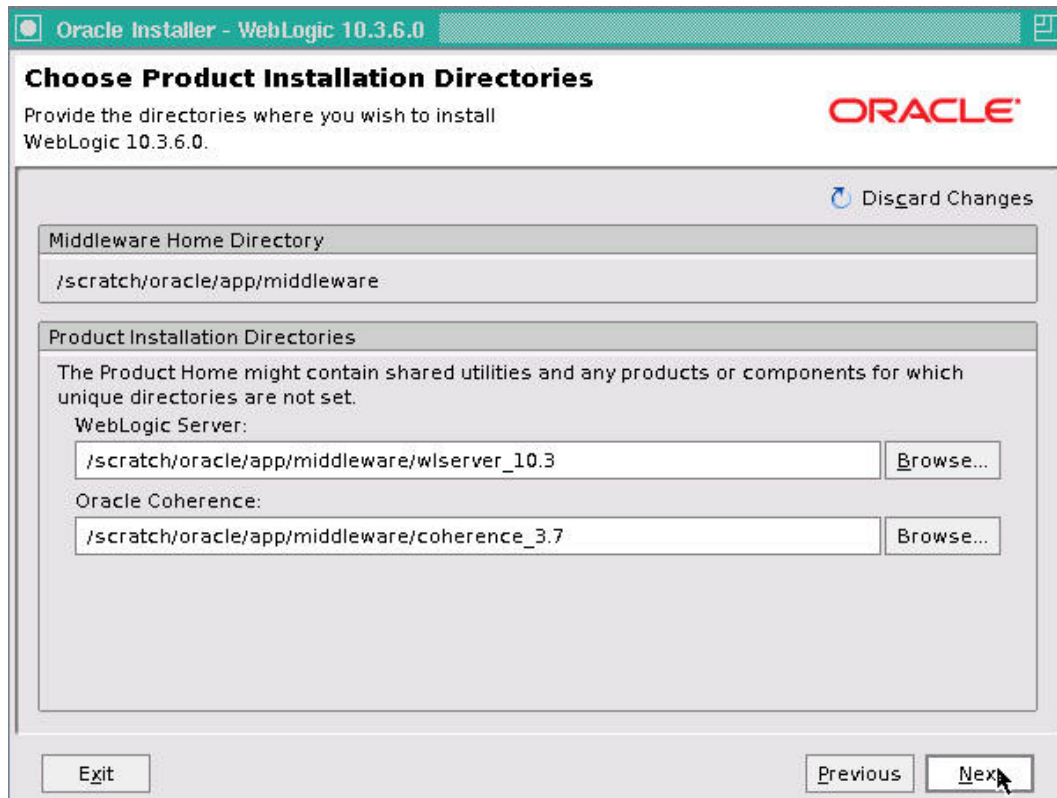
10. Click Browse button and select existing JDK Home Path as shown below.



11. The selected Java Home is displayed as shown below.



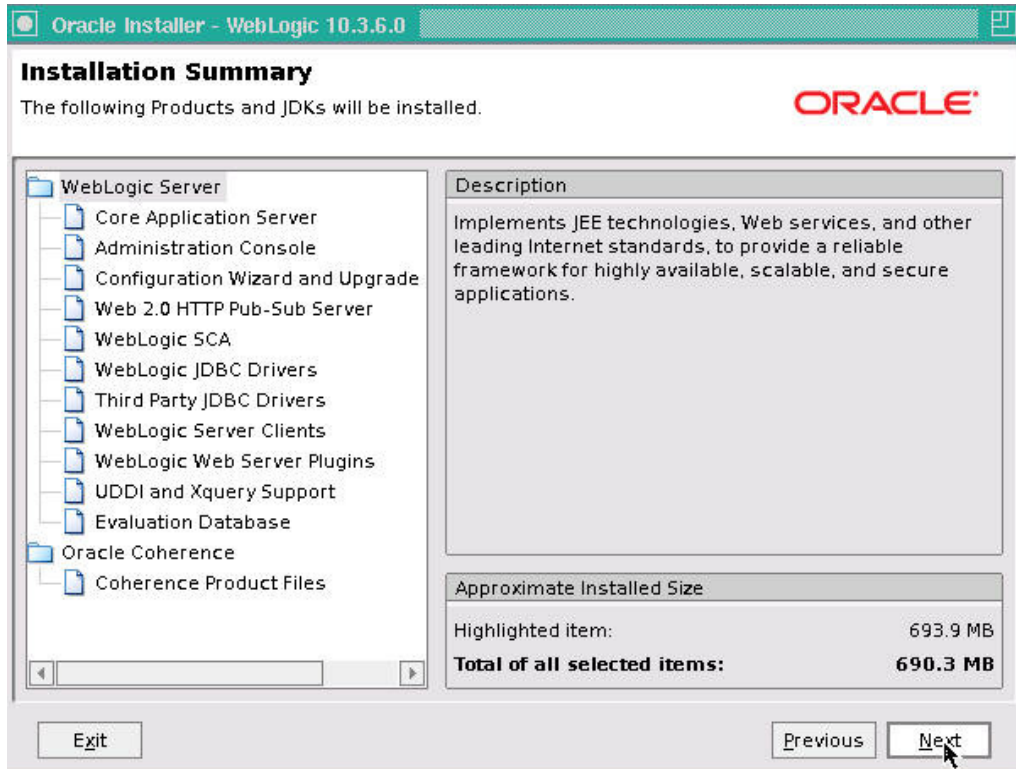
12. Click **Next**. The following window is displayed.



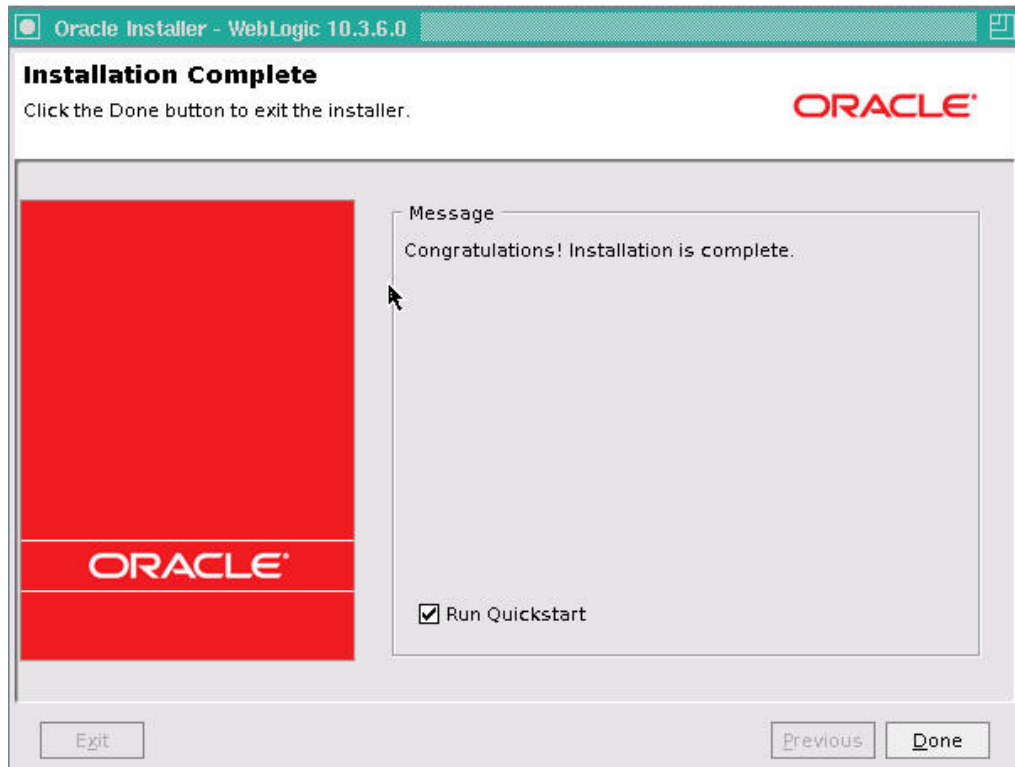
13. Click **Next**. The following window is displayed.

Note

You can change the Oracle WebLogic Server and Oracle Coherence paths, if required. ...



14. Click **Next**. The weblogic installation starts. After its done the following window is displayed.



15. Click **Done** to close the window.

2.2 Installing Oracle ADF Runtime

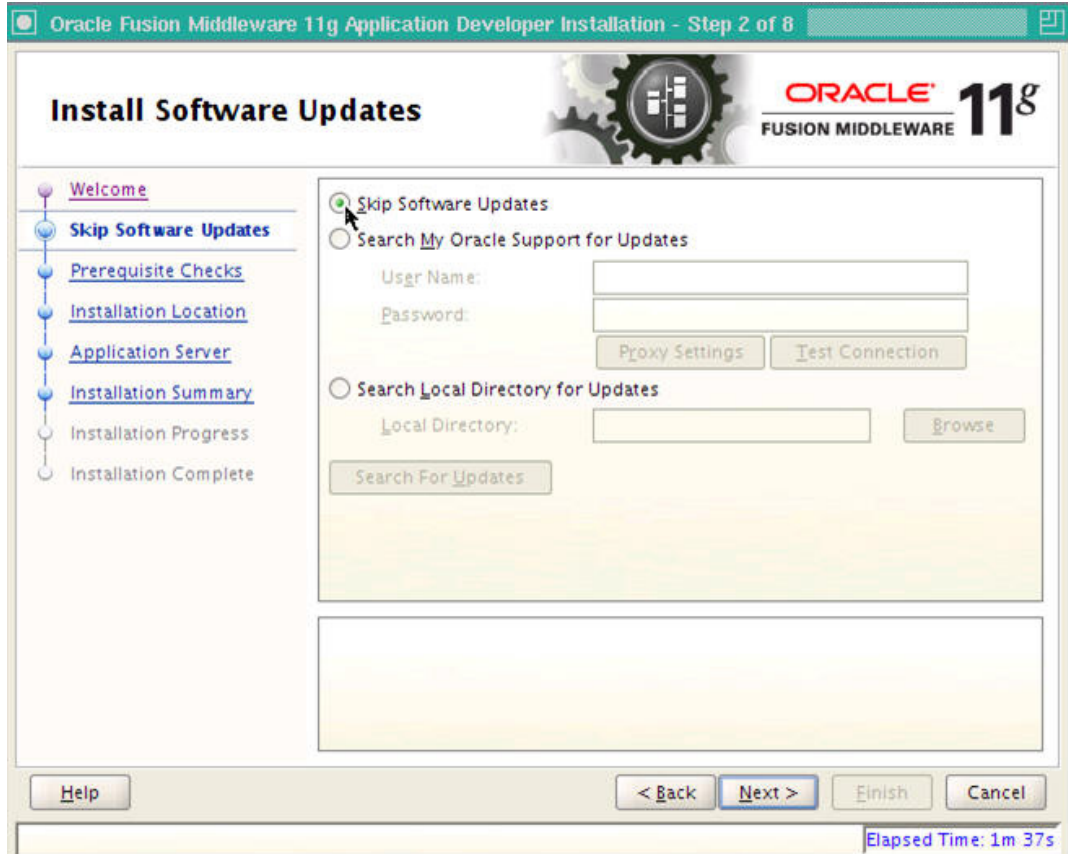
1. Extract the zipped file ofm_appdev_generic_11.1.1.7.0_disk1_1of1.zip.
2. Go to Disk1 folder of the above unzipped file. Run the following command

In **Unix/Linux**:./runInstaller

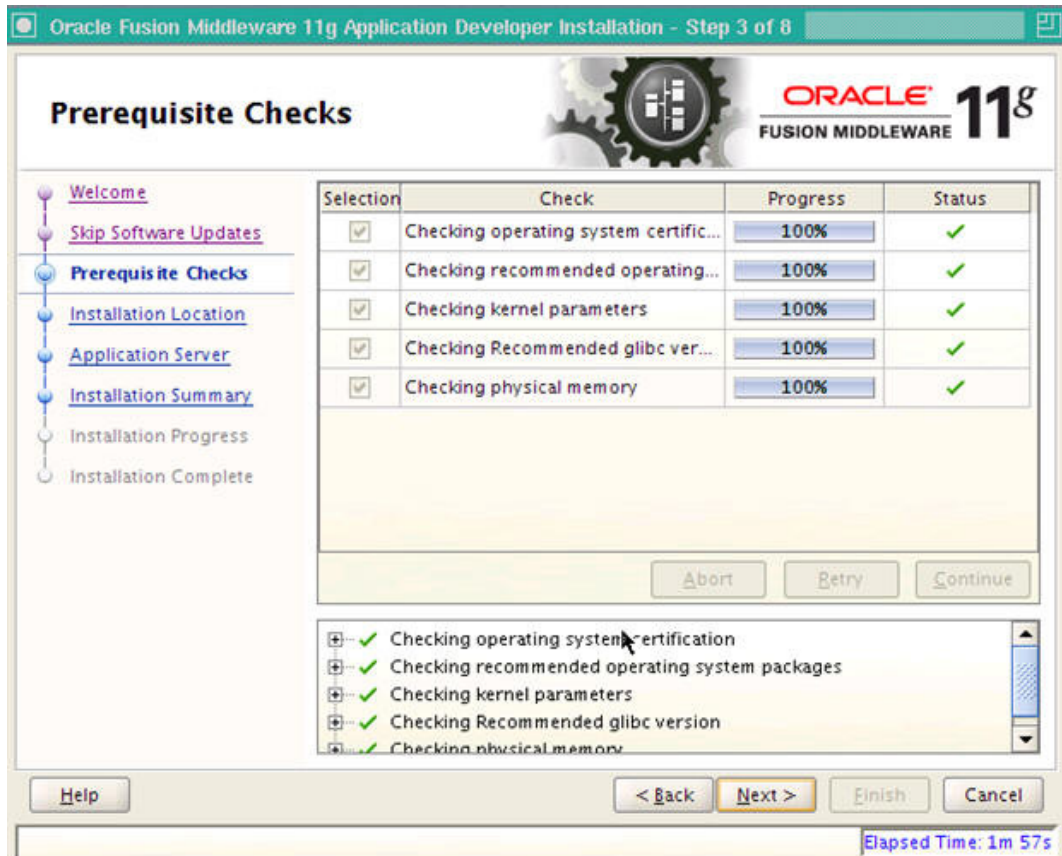
3. Enter JDK/JRE Home Path, when prompted.
4. Welcome window is displayed.



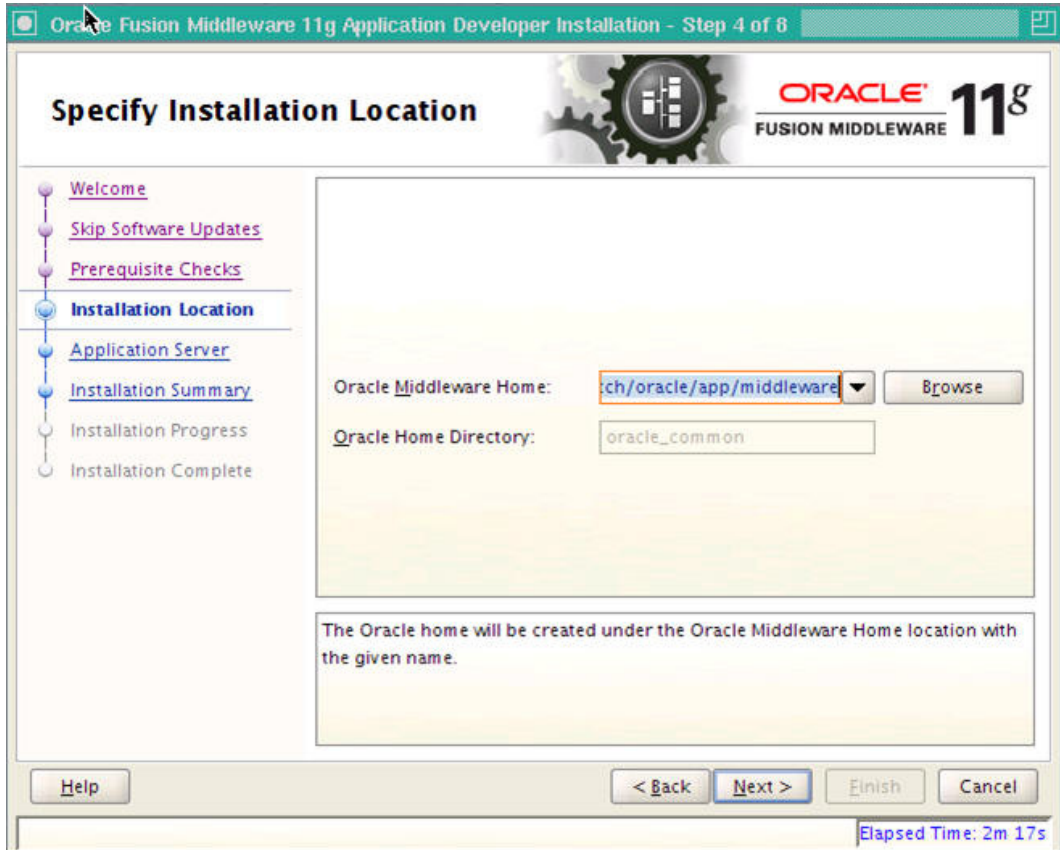
5. Click **Next**. The following window is displayed.



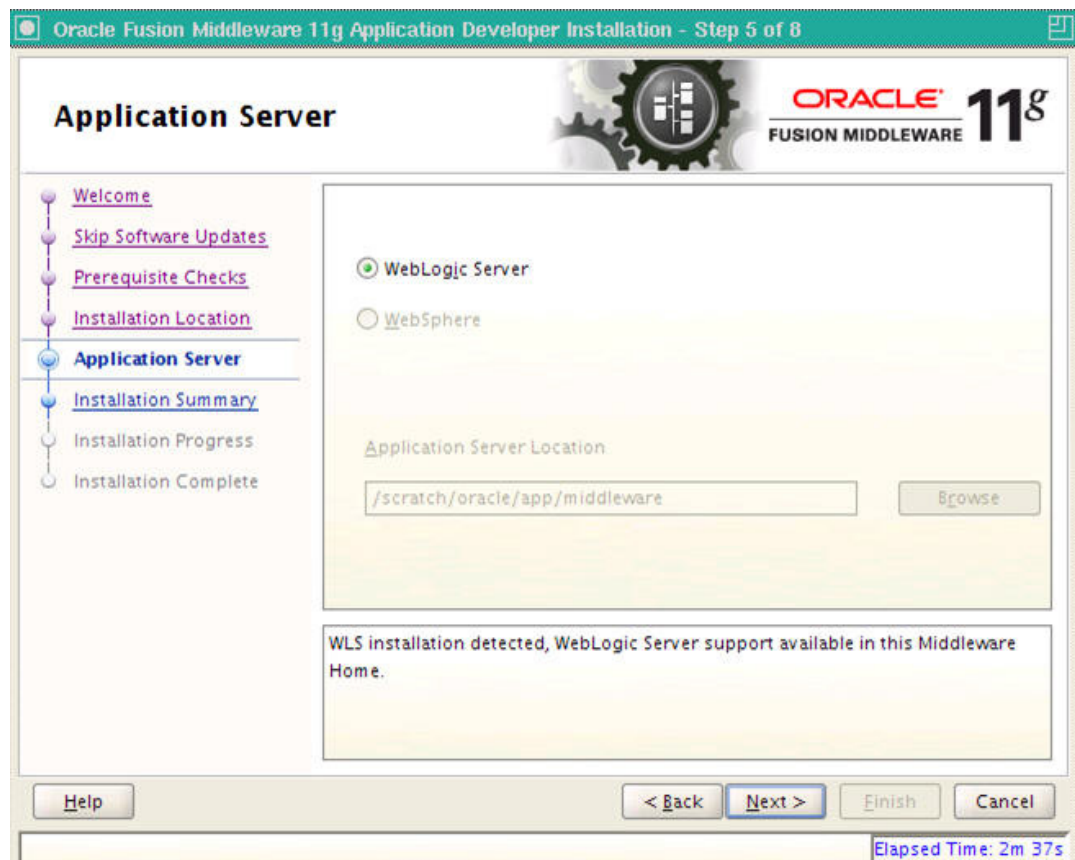
6. Select **Skip Software Updates** and click **Next**. The following window is displayed.



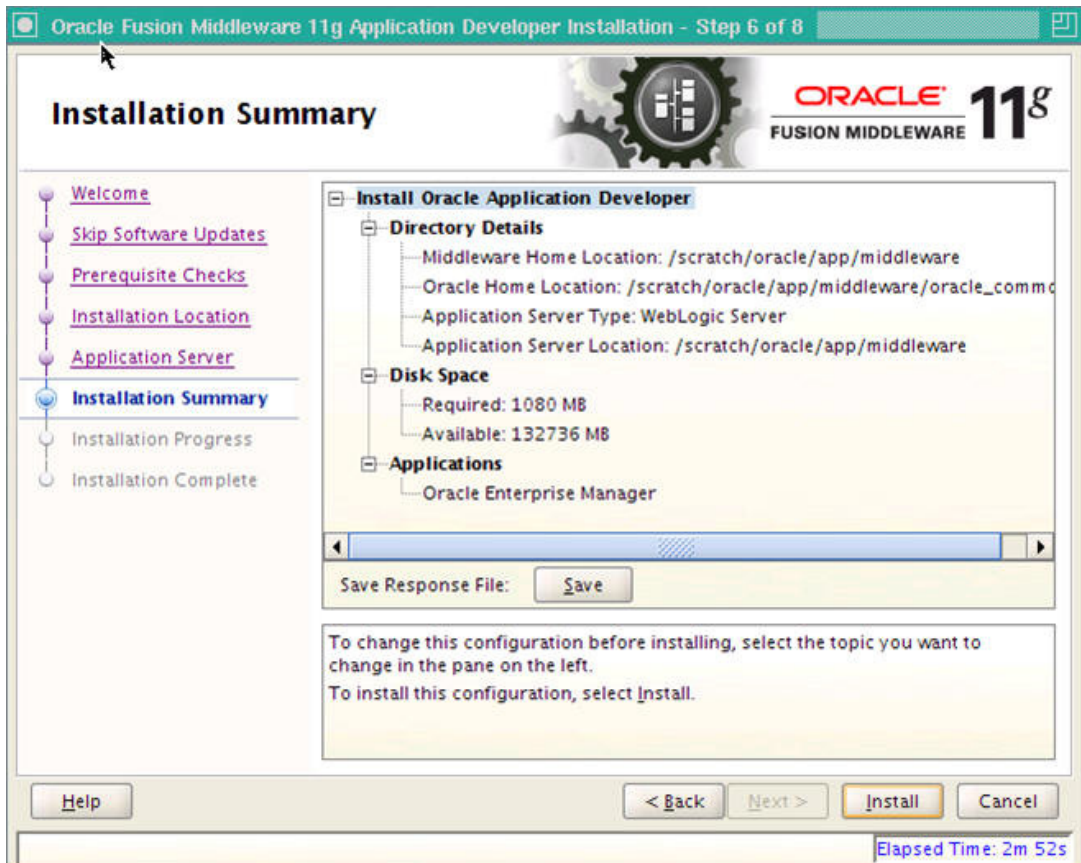
7. Click Next. The following window is displayed.



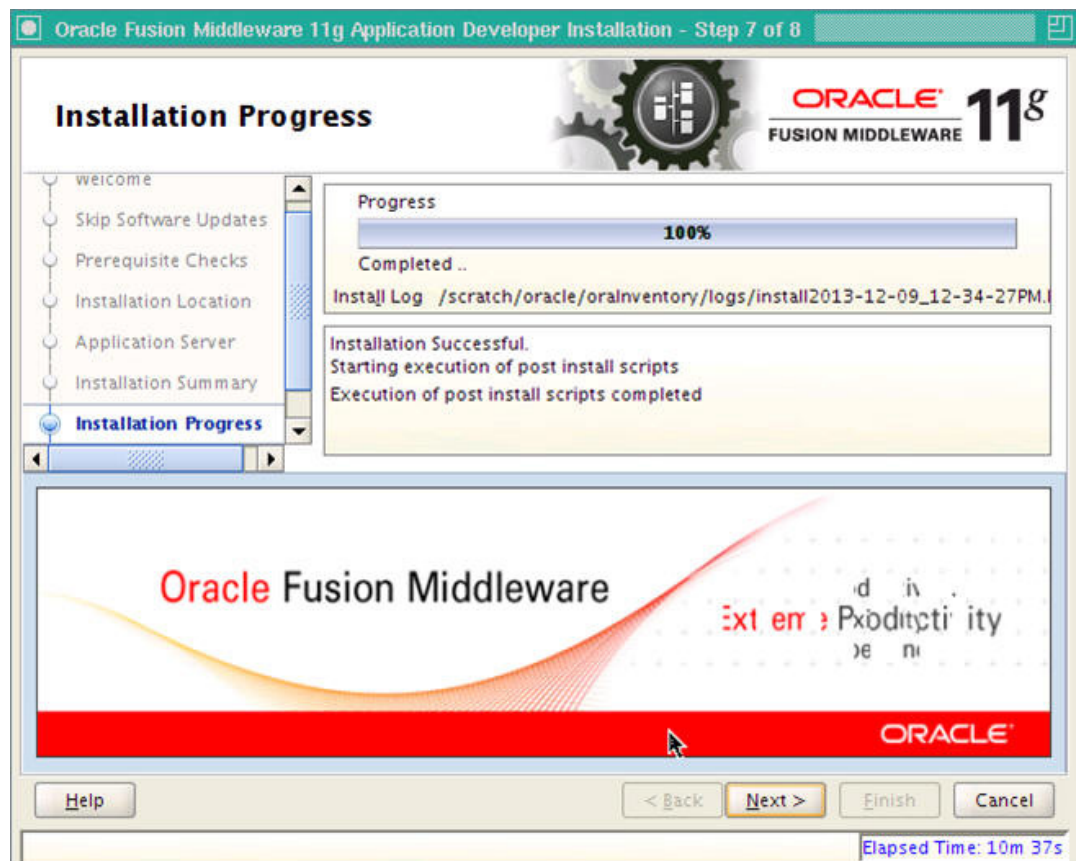
8. Select Oracle **Middleware Home Path** as highlighted and click **Next**. The following window is displayed.



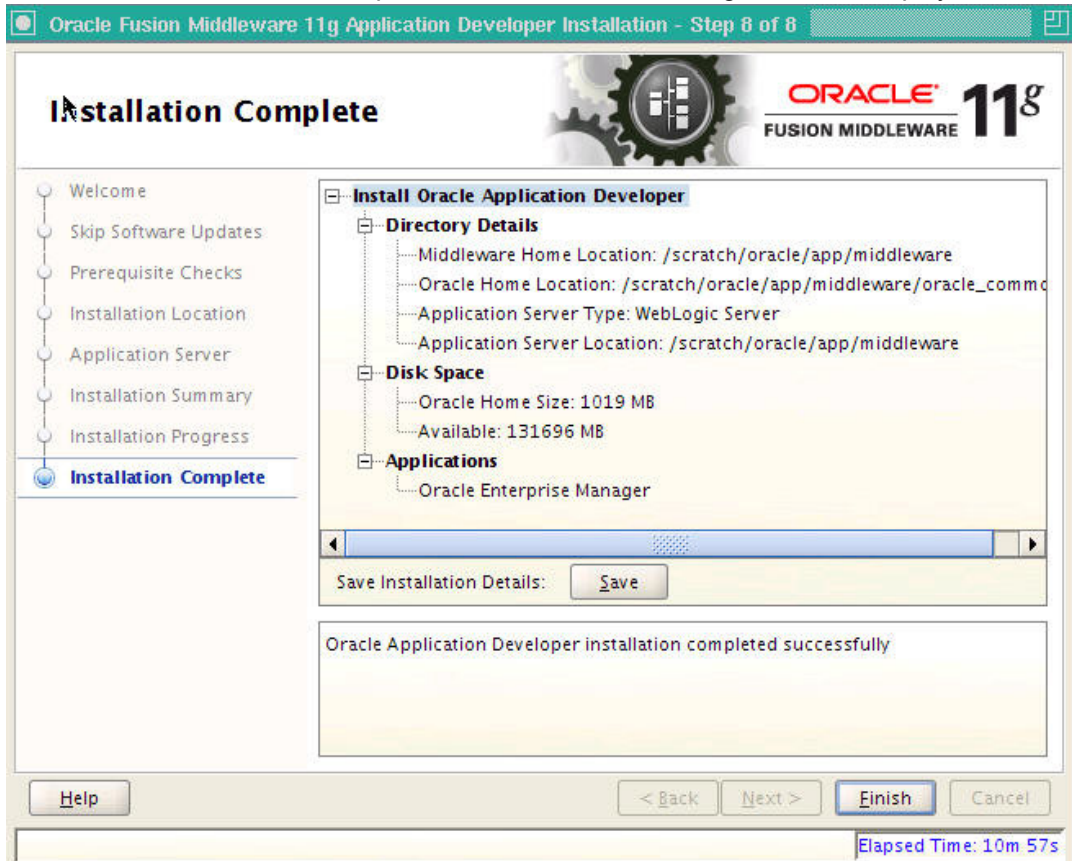
9. Select **WebLogic Server** and click **Next**. The following window is displayed.



10. Click **Install**. The following window is displayed.



11. Once the installation is complete, click **Next**. The following window is displayed.



12. Click **Finish** to close the window.

3. Creating Domains, Repositories, Data Sources

3.1 Creating Domain and Servers

1. In Unix/Linux machine, once the Oracle WebLogic Server is installed, navigate to the following path.

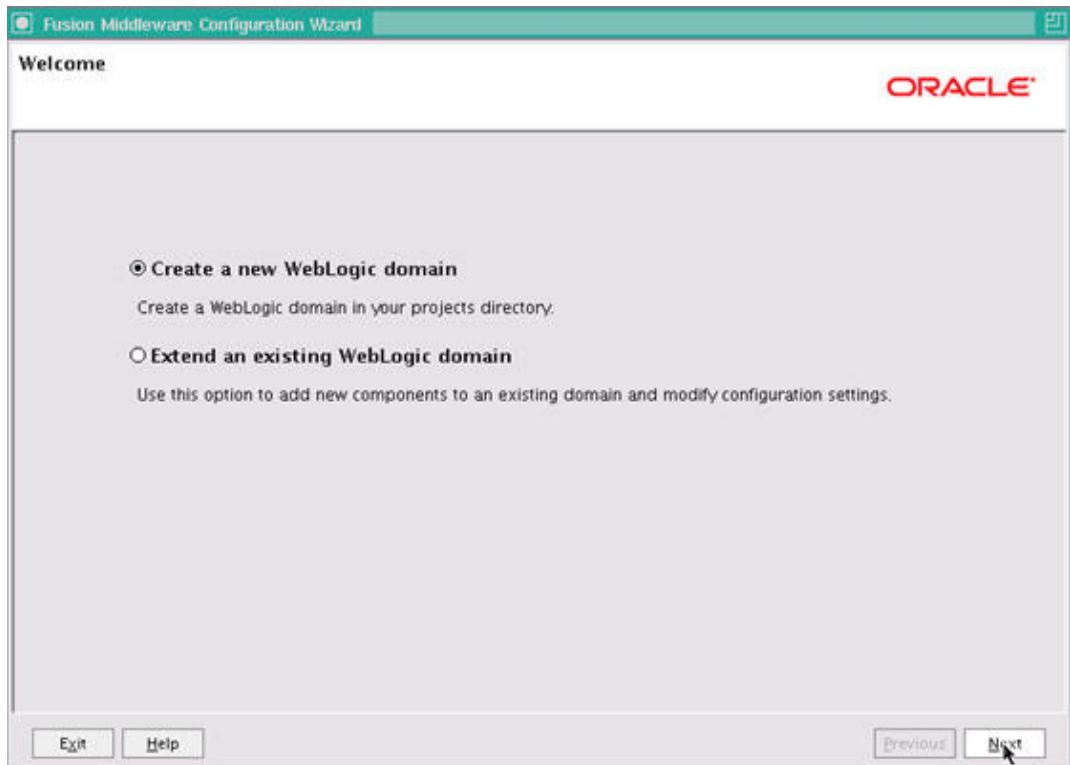
<WL_HOME>/wlserver_10.3/common/bin

Note

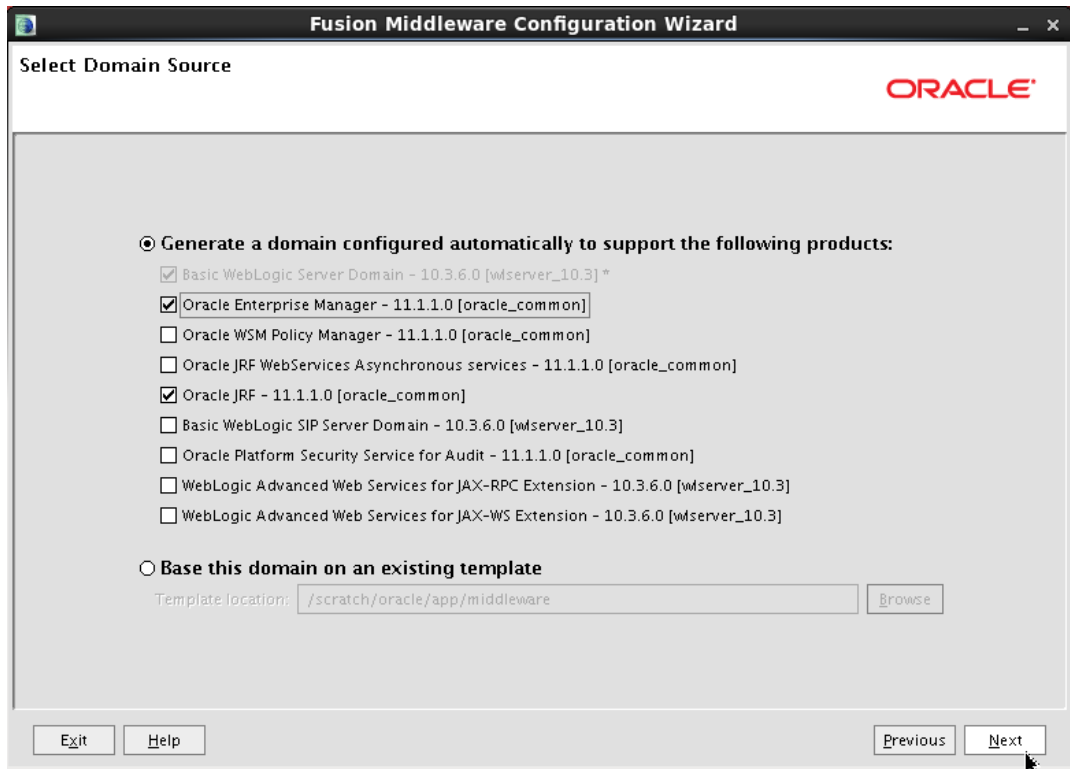
Use XManager for remote UNIX/LINUX machine. Refer [XManager Usage](#).

Here, WL_HOME is **/home/Oracle/Middleware**.

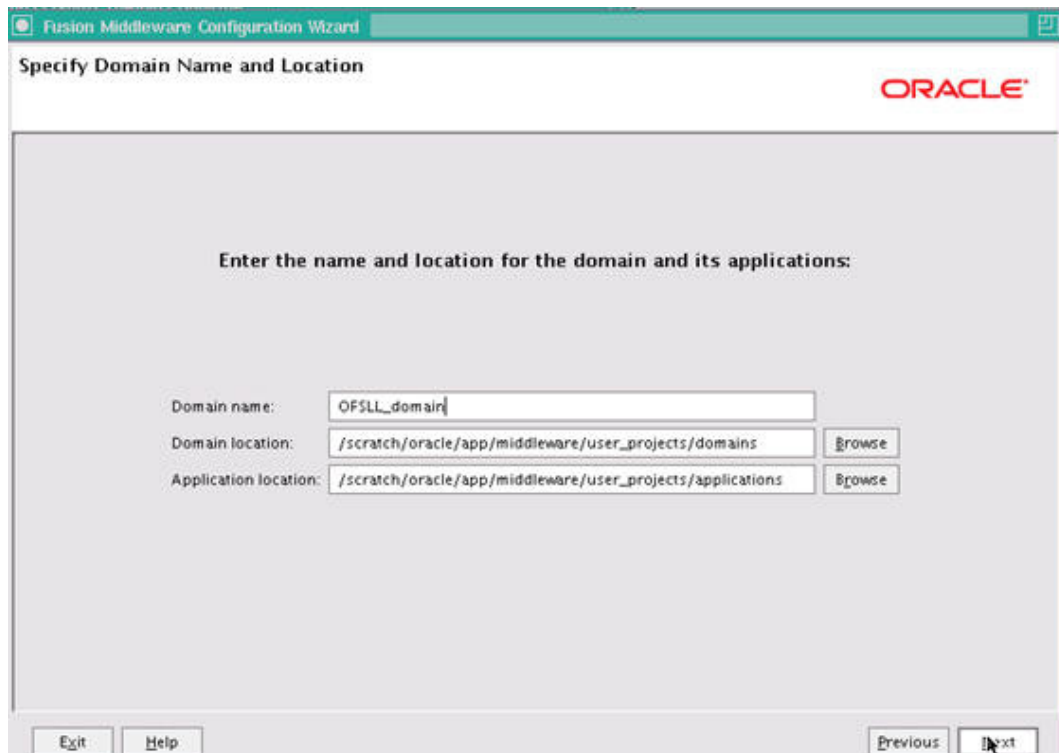
2. In Unix run **config.sh.**,
3. Click Configuration Wizard icon.



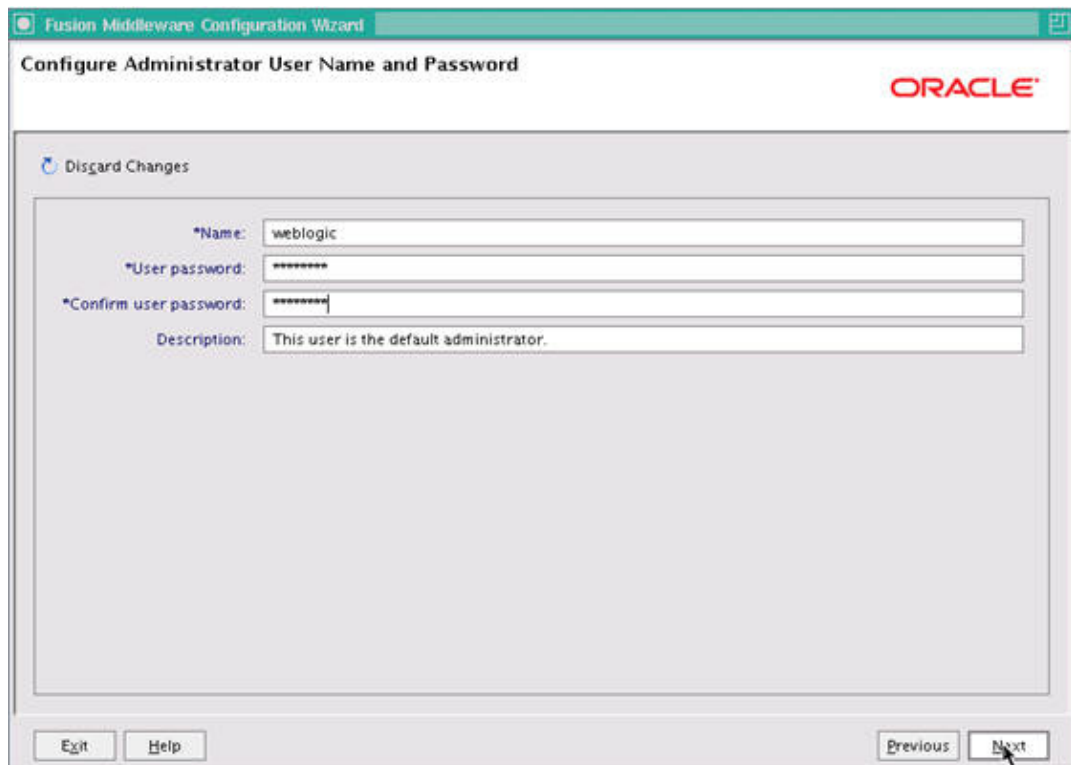
4. Select **Create a new WebLogic domain** and click **Next**. The following window is displayed.



5. Select **Generate a domain configured automatically to support the following products** option.
6. Select **Oracle Enterprise Manager - 11.1.1.0 [oracle_common]** check box.
7. Select **Oracle JRF - 11.1.1.0 [oracle_common]** check box.
8. Click **Next**. The following window is displayed.



9. Enter **Domain** Name and click **Next**. The following window is displayed.
10. Edit Domain Location, if needed.



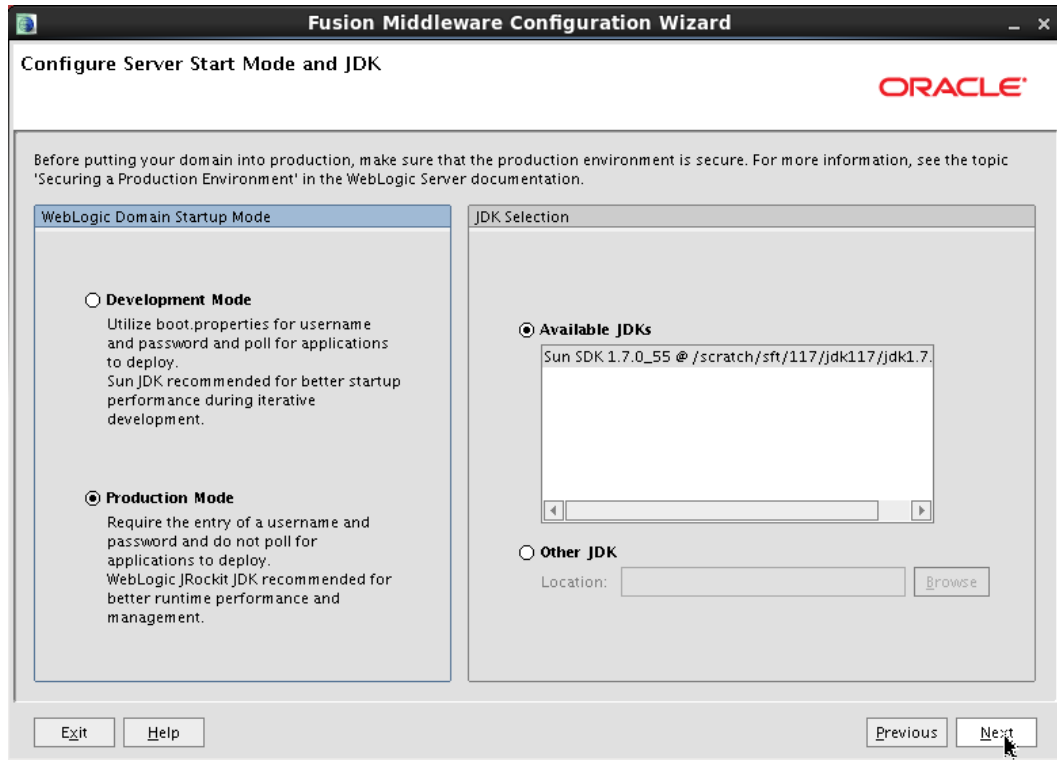
The screenshot shows a window titled "Fusion Middleware Configuration Wizard" with a sub-header "Configure Administrator User Name and Password" and the Oracle logo. A "Disgard Changes" button is visible. The form contains the following fields:

- *Name:
- *User password:
- *Confirm user password:
- Description:

At the bottom, there are buttons for "Exit", "Help", "Previous", and "Next".

11. Enter credentials for the following:
 - Name
 - User password
 - Confirm user password
 - Description

12. Click **Next**. The following window is displayed.

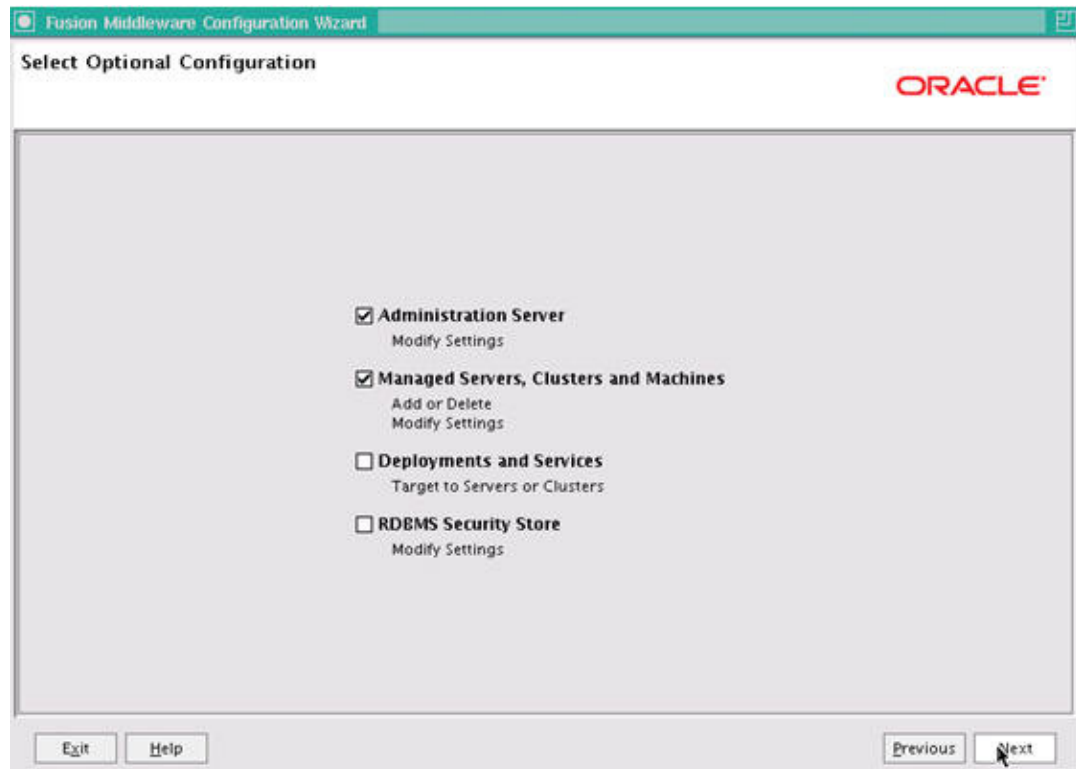


13. Select **Production Mode** and **JDK** from **Available JDKs**

OR

Select **Other JDK** option to select any other JDK.

14. Click **Next**. The following window is displayed.



15. Select **Administration Server** and **Managed Servers, Clusters and Machines** and click **Next**. The following window is displayed.

The screenshot shows the 'Configure the Administration Server' window in the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Configure the Administration Server'. The Oracle logo is in the top right corner. Below the title bar, there is a 'Disgard Changes' button. The main area contains several input fields: '*Name:' with the value 'OFSSL_AdminServer', '*Listen address:' with a dropdown menu set to 'All Local Addresses', 'Listen port:' with the value '7001', 'SSL listen port:' with the value '7002', and 'SSL enabled:' with a checked checkbox. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons. A mouse cursor is pointing at the 'Next' button.

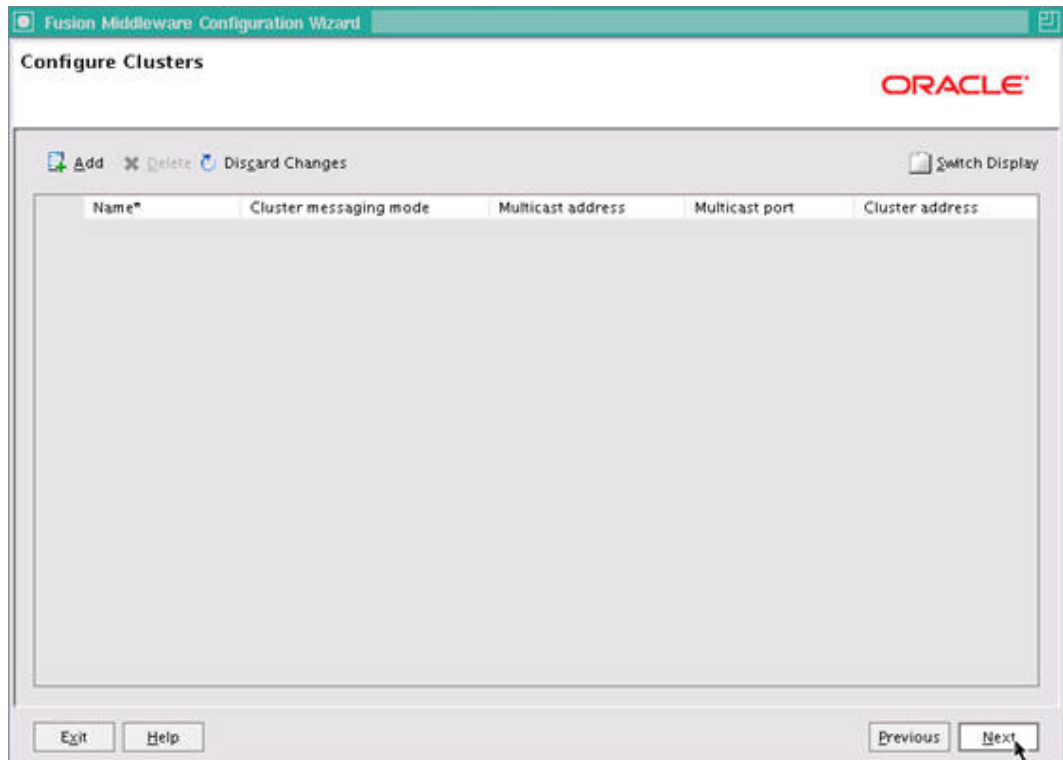
16. Enter Administration Server **Name** and **Listen Port** details. Check the SSL port and click Next. The following window is displayed..

The screenshot shows the 'Configure Managed Servers' window in the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Configure Managed Servers'. The Oracle logo is in the top right corner. Below the title bar, there are 'Add', 'Delete', and 'Disgard Changes' buttons, and a 'Switch Display' checkbox. The main area contains a table with the following data:

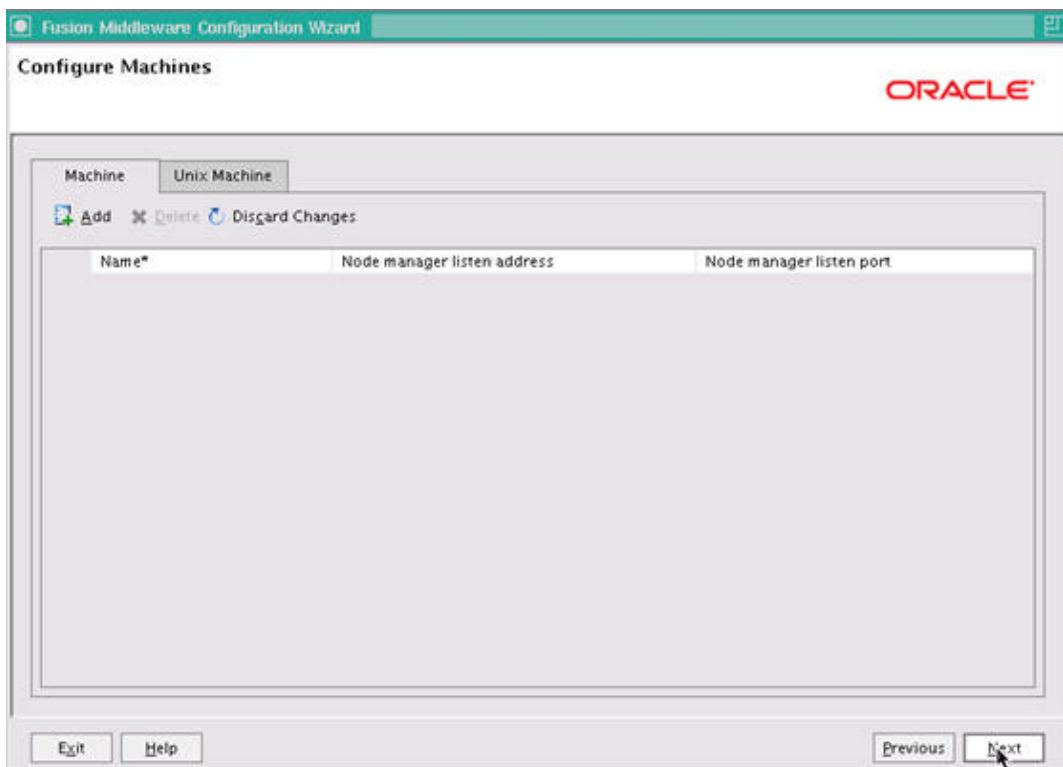
| | Name* | Listen address* | Listen port | SSL listen port | SSL enabled |
|-----|---------------------|---------------------|-------------|-----------------|-------------------------------------|
| → 1 | OFSSL_ManagedServer | All Local Addresses | 7003 | 7503 | <input checked="" type="checkbox"/> |

At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons. A mouse cursor is pointing at the 'Next' button.

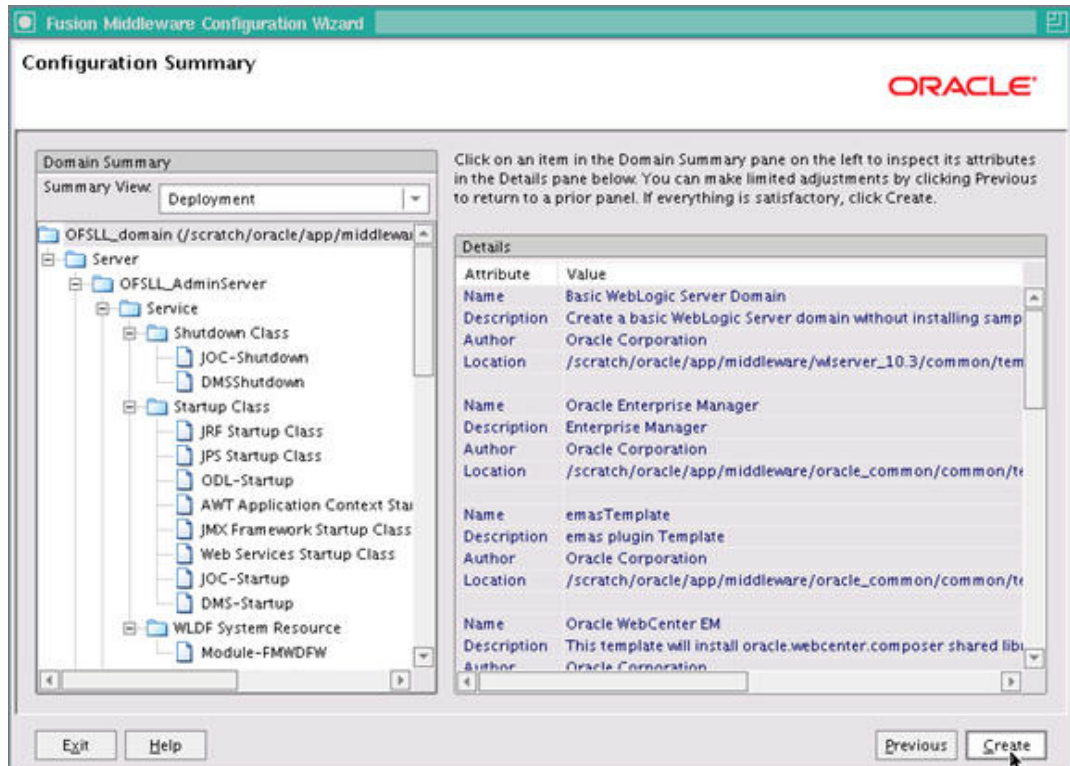
17. Click Add button. Enter **Name** and **Listen Port** details in Configure Managed Servers window. Check the SSL port and click Next. The following window is displayed.



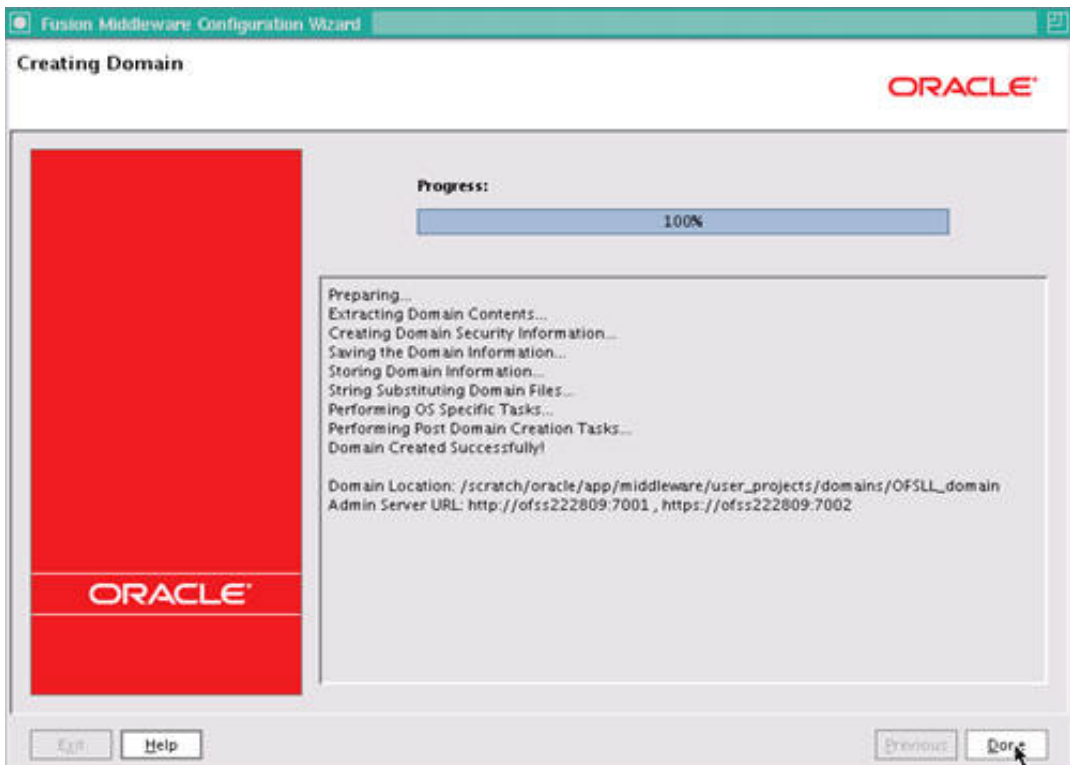
18. Configure as required and click **Next**. The following window is displayed.



19. Configure as required and click **Next**. The following window is displayed.



20. Click **Create**. The following window is displayed.



21. Once the creation of the Domain is complete, click **Done** to close the window.

Note

The default Weblogic installation will be running JVM with 512MB, this has to be increased for the ADF managed server. Say, for a 2 CPU Quad Core with 16 GB it could have the JVM running at 8 GB as:

```
USER_MEM_ARGS="-Xms8192m -Xmx8192m -XX:PermSize=2048m -XX:Max-PermSize=2048m"
```

22. The "\$MW_HOME/user_projects/domains/mydomain" directory contains a script that can be used to start the Admin server.

```
$ cd $MW_HOME/user_projects/domains/mydomain/bin
$ ./startWebLogic.sh
```

If the server is required to be running and access to command line needs to be returned use "nohup" and "&"

```
$ nohup ./startWebLogic.sh &
```

23. To Start Managed Server

```
$ cd $MW_HOME/user_projects/domains/mydomain/bin
$ ./startManagedWebLogic.sh
{ManagedServer_name} {AdminServer URL}
```

If the server is required to be running and access to command line needs to be returned use "nohup" and "&"

```
$ nohup ./startManagedWebLogic.sh {ManagedServer_name} {AdminServer URL} &
```

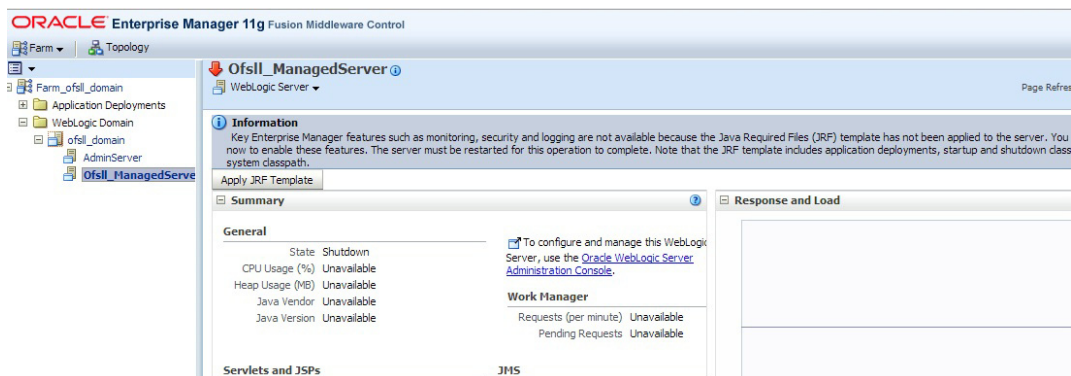
3.2 Applying the JRF Template

1. Start Oracle WebLogic Server
2. Login to Oracle Enterprise Manager 11g Console (<http://hostname:port/em>).

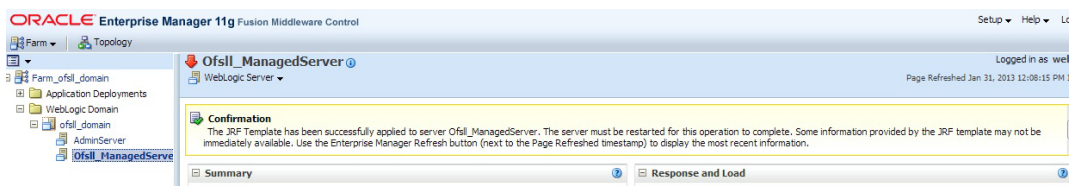
The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The main window shows the 'Farm_ofs1l_domain' with a 'Deployments' section indicating 'Up (4)' and a 'Fusion Middleware' section showing a 'WebLogic Domain' with 'ofs1l_domain' containing 'AdminServer' and 'Ofs1_ManagedServer'. The 'AdminServer' is shown as 'Up (1)' and the 'Ofs1_ManagedServer' as 'Down (1)'. The CPU usage for the 'Ofs1_ManagedServer' is 0.00%.

| Name | Status | Host | CPU Usage (%) |
|--------------------|----------|------------------|---------------|
| WebLogic Domain | | | |
| ofs1l_domain | | | |
| AdminServer | Up (1) | MBQMMVA-2N.in... | 0.00 |
| Ofs1_ManagedServer | Down (1) | | |

- On Left window panel, expand **WebLogic Domain** → **OFSLL_domain** and click **OFSLL_ManagedServer** as shown below.



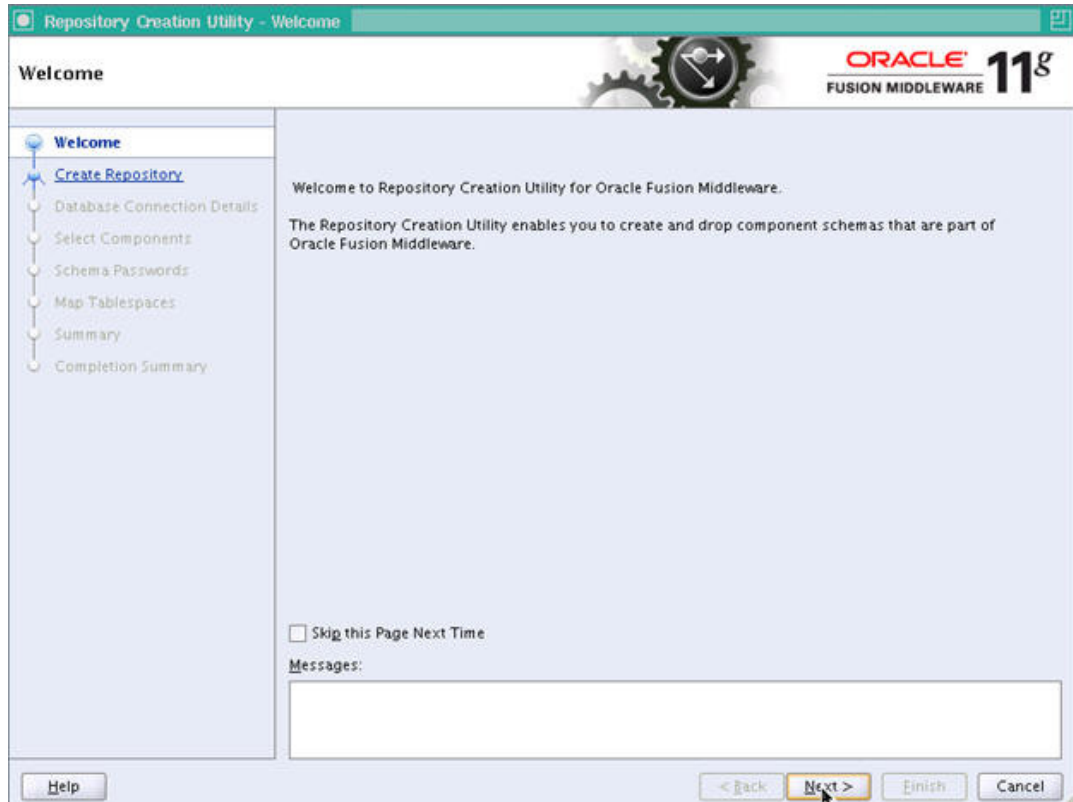
- On right window panel, click **Apply JRF Template** Button. The confirmation message is displayed as shown below.



3.3 Creating Schemas using Repository Creation Utility

- Download Oracle Repository Creation Utility Tool (ofm_rcu_linux_11.1.1.7.0_disk1_1of1.zip) from the link mentioned in prerequisites.
- Unzip the ofm_rcu_linux_11.1.1.7.0_disk1_1of1.zip to your local drive.
- Open command prompt on Unix and browse to \$RCU_HOME/bin and run **./rcu**

4. The following window is displayed.



5. Select **Create** to create new schemas and click **Next**. The following screen is displayed.



6. Provide database details where schemas need to be created, as shown in the above screen. Click on Next. The following window is displayed.

Repository Creation Utility - Step 2 of 7 : Database Connection Details

Database Connection Details

ORACLE 11g
FUSION MIDDLEWARE

Welcome
Create Repository
Database Connection Details
Select Components
Schema Passwords
Map Tablespaces
Summary
Completion Summary

Database Type: Oracle Database

Host Name: ofss222464.in.oracle.com
For RAC database, specify VIP name or one of the Node name as Host name.
For SCAN enabled RAC database, specify SCAN host as Host name.

Port: 1521

Service Name: OFSLDDB

Username: sys
User with DBA or SYSDBA privileges. Example:sys

Password:

Role: SYSDBA
One or more components may require SYSDBA role for the operation to succeed.

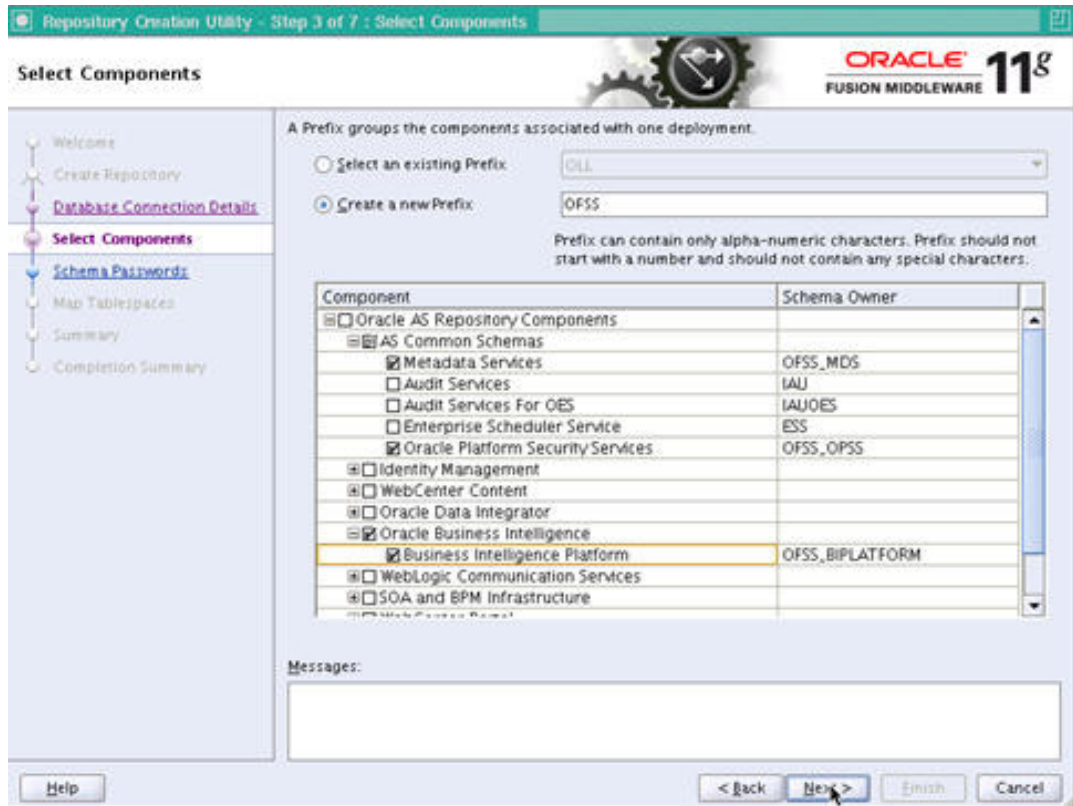
Messages:

Help < Back Next > Finish Cancel

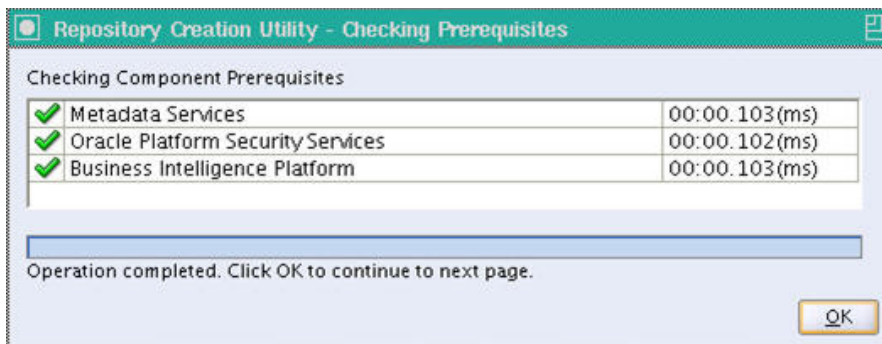
7. Provide database details where you want to create schemas, as shown in the above screen.

Note

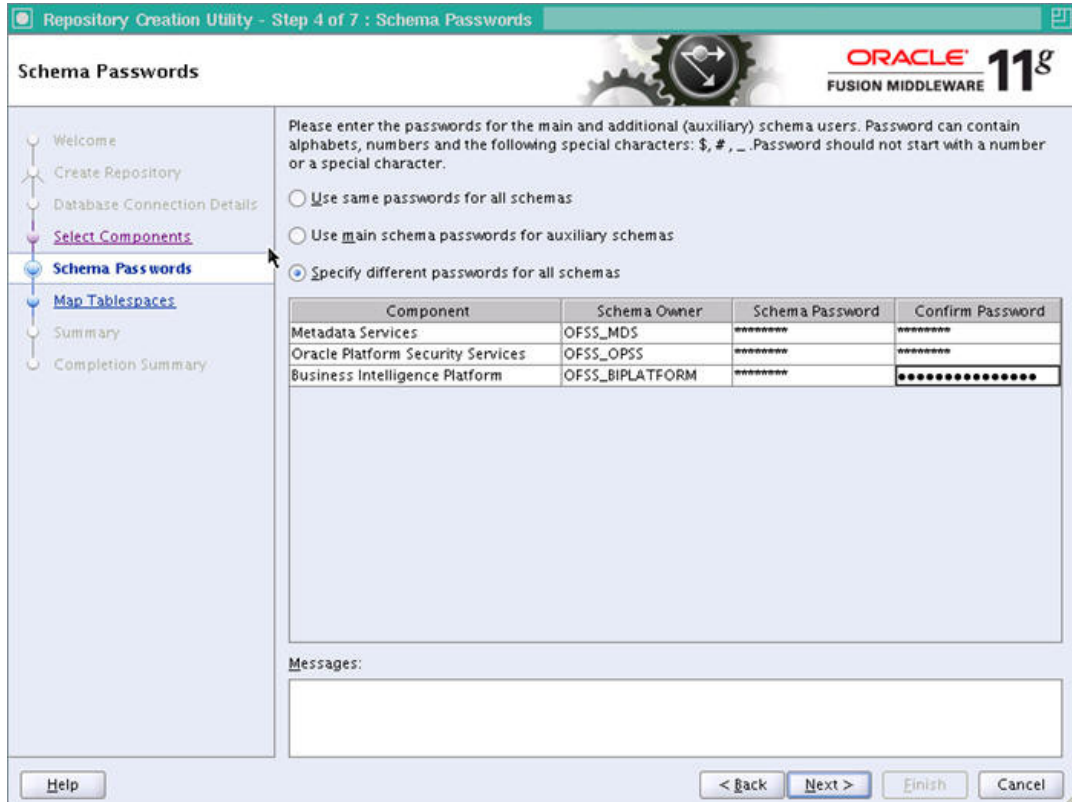
You will require a user with SYSDBA role to create schemas.



8. Select **Create a new Prefix** option and specify value. For example, OFSS. Check **Metadata Services**, **Oracle Platform Security Services** and **Business Intelligence Platform** as shown in the above screen.
9. Click **Next**. The following window is displayed.

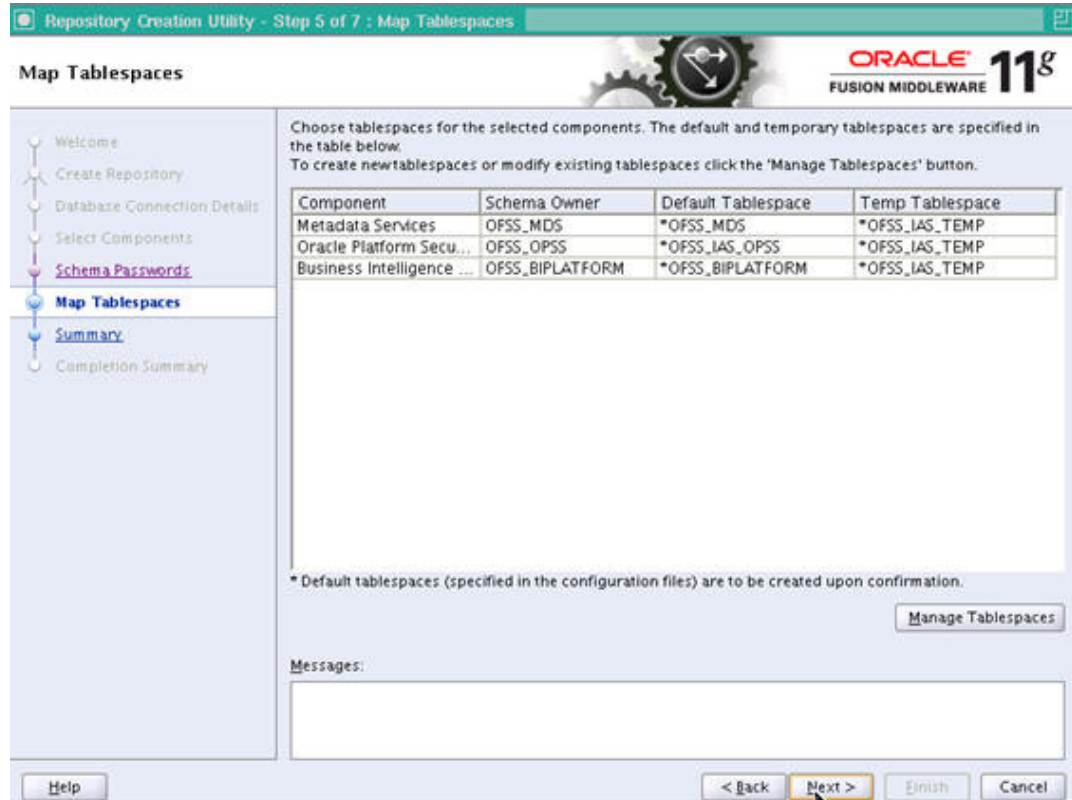


10. Once the operation is complete, click **OK**. The following window is displayed.

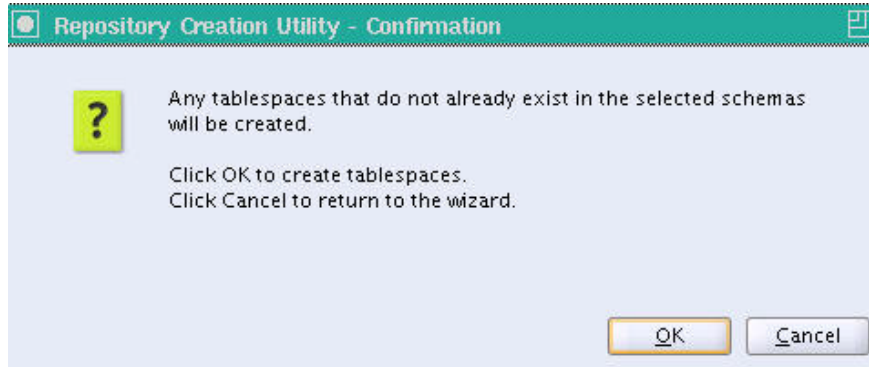


11. Select **Specify different passwords for all schemas** and provide Schema Passwords for each server as shown above.

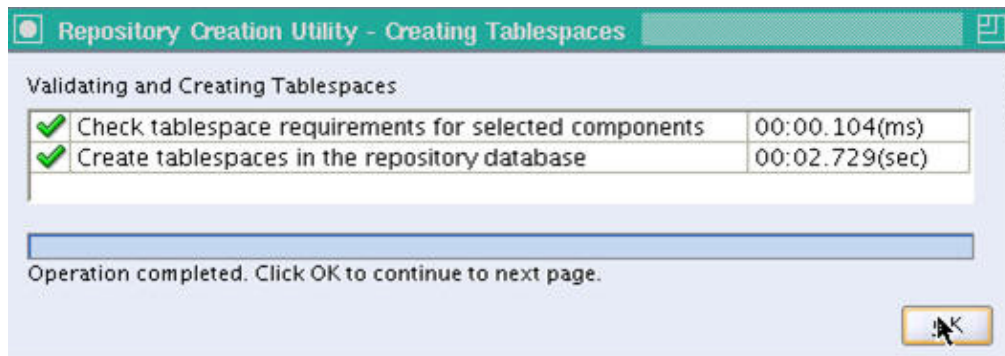
12. Click Next. The following window is displayed.



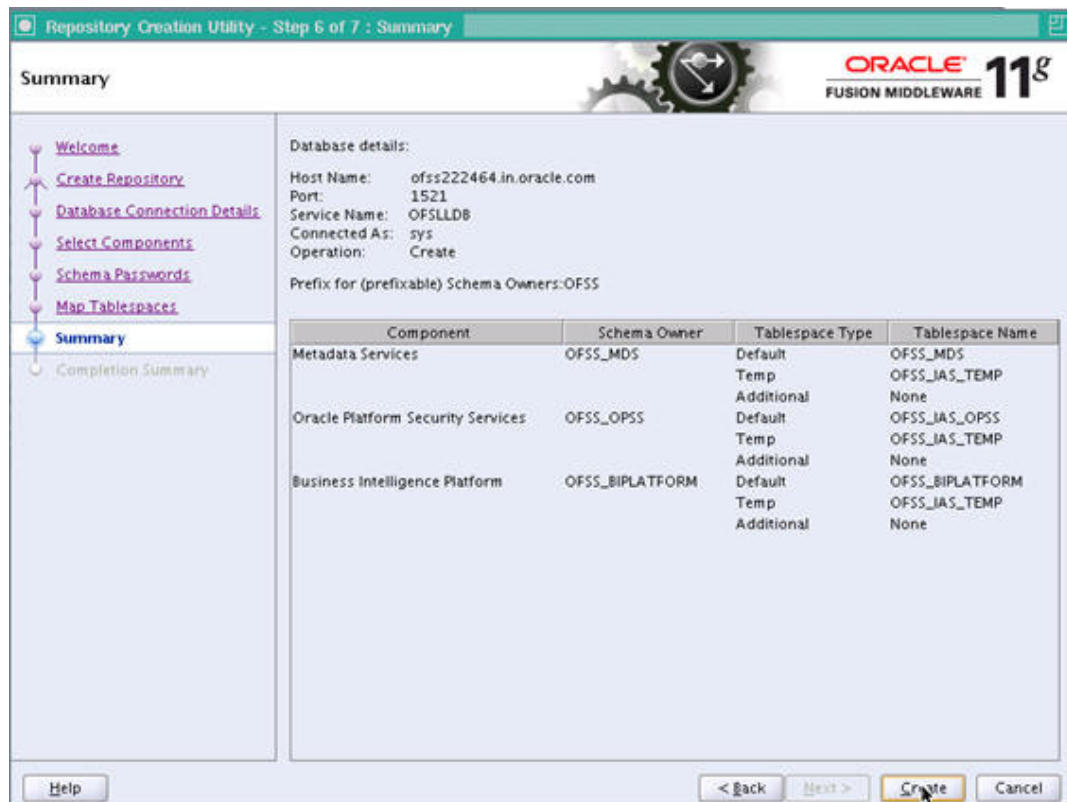
13. Click **Next**. The following window is displayed.



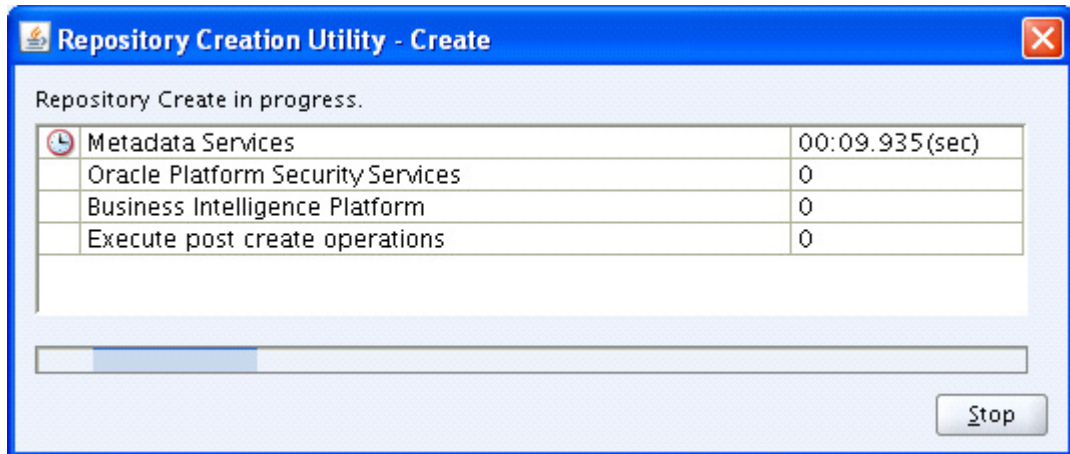
14. Click **OK**. The following window is displayed.



15. Click **OK** to continue to the next page. The following window is displayed.



16. Click **Create**. The following windows are displayed.

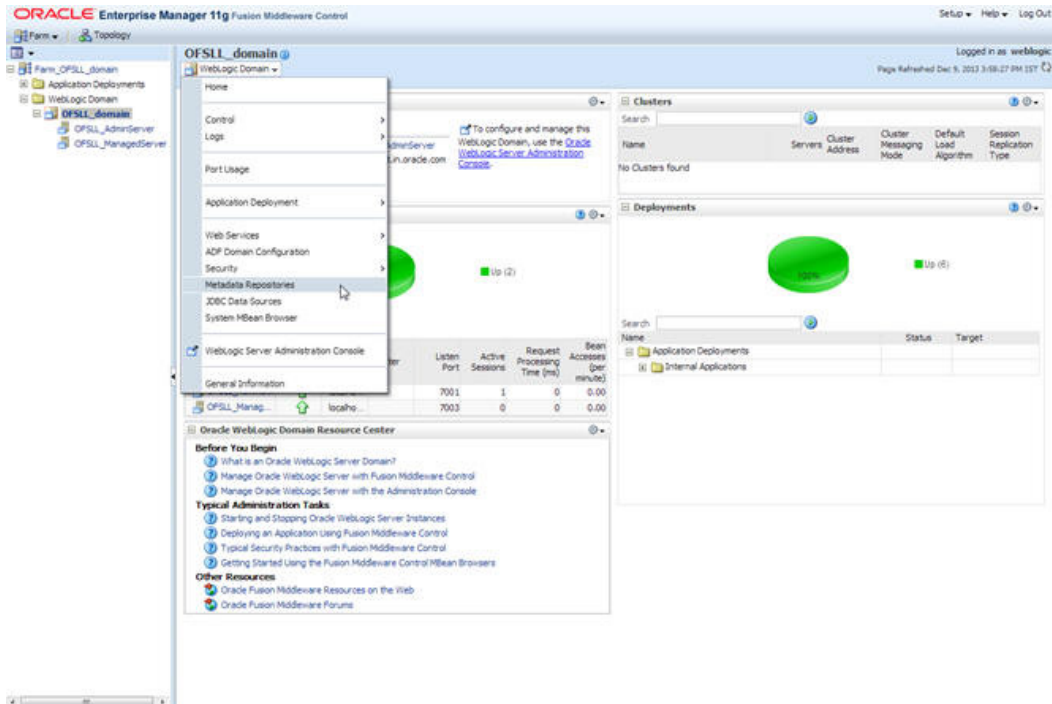


17. Click **Close** to close the window.

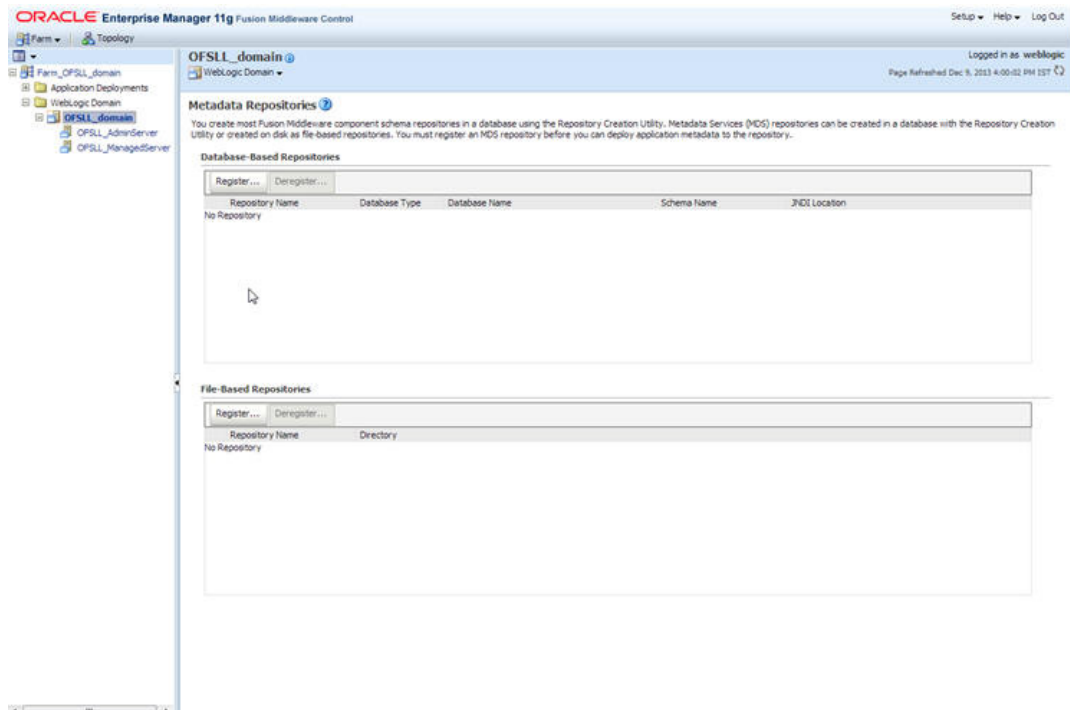
3.4 Creating Metadata Repository

Assuming that **OFSS_MDS** schema is created using Oracle Repository Creation Utility (RCU) as mentioned in [Creating Schemas using Repository Creation Utility](#) section, follow the below steps to create the repository.

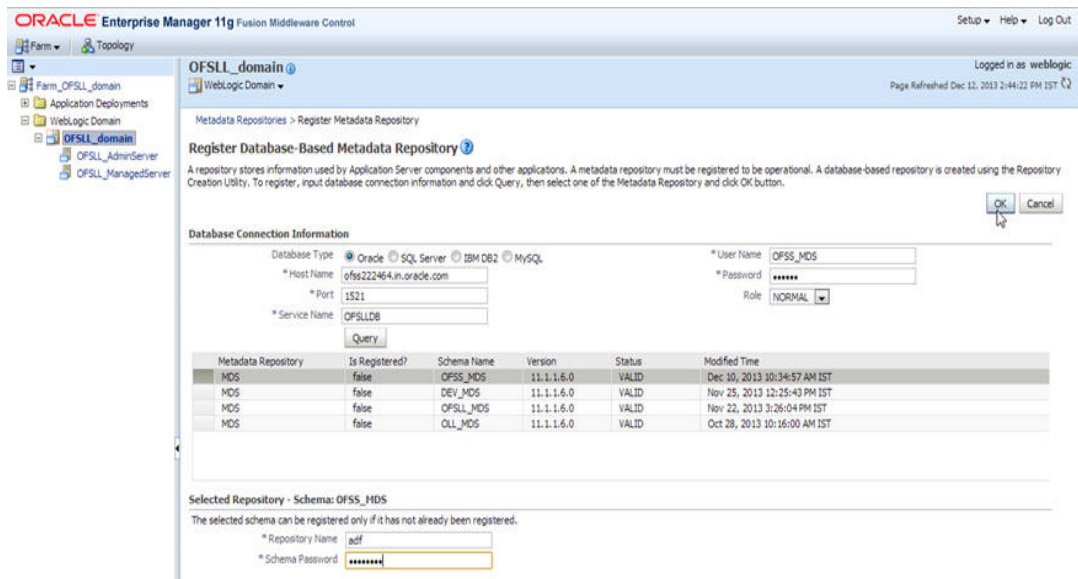
1. Login to Oracle Enterprise Manager 11g console (<http://hostname:port/em>).



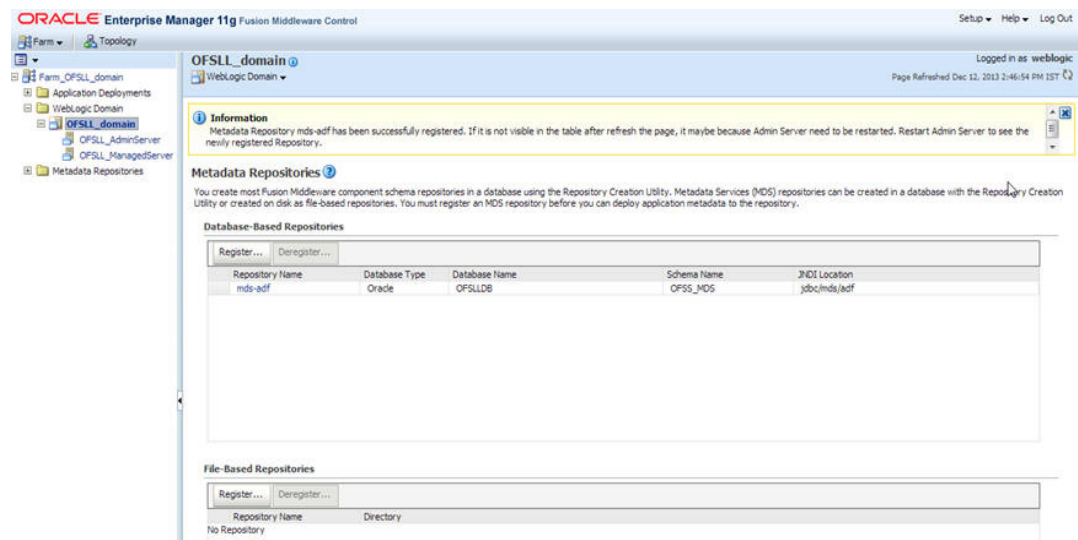
2. Click on domain name OFSLL_domain on the left side panel.
3. Expand Weblogic domain OFSLL_domain and click Metadata Repositories on right side panel, as shown above screen.
4. The following window is displayed.



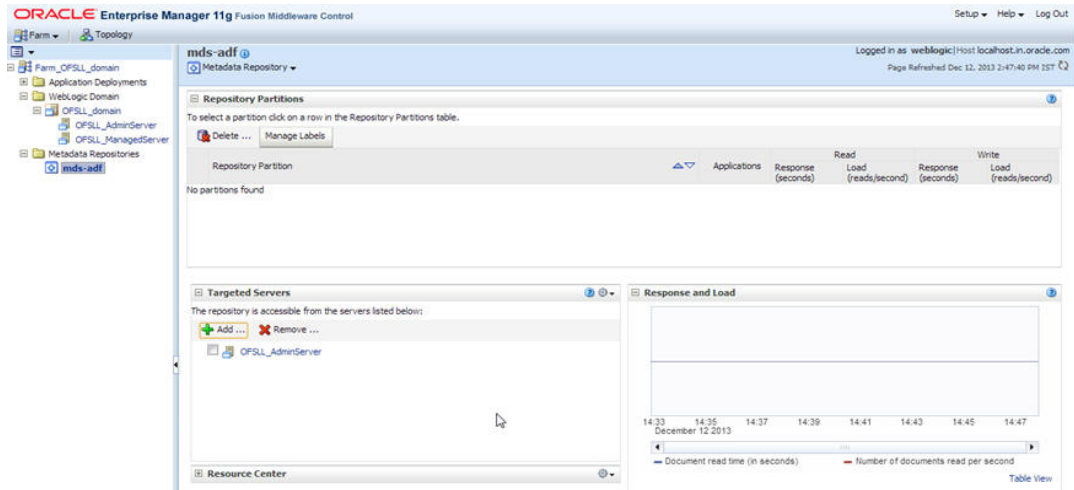
- Click Register button. The following window is displayed.



- Enter database instance details under Database Connection Information section and click **Query**.
- All available schemas in the given database instance are listed.
- Select the schema you require and enter **Repository Name (adf)** and the password under Selected Repository – Schema **OFSS_MDS** section.
- Click OK. The following window is displayed.



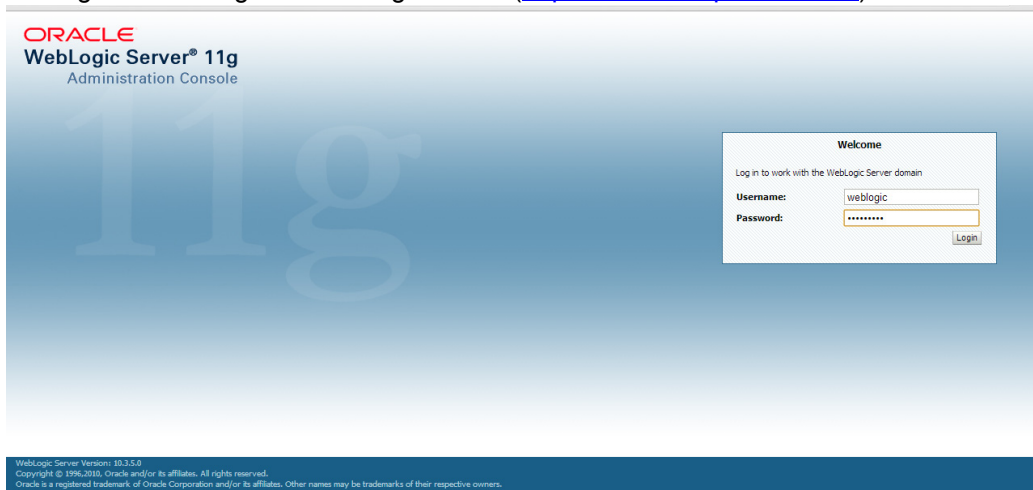
10. Click Repository name **mds-adf** on left panel. You can even select it from right panel.



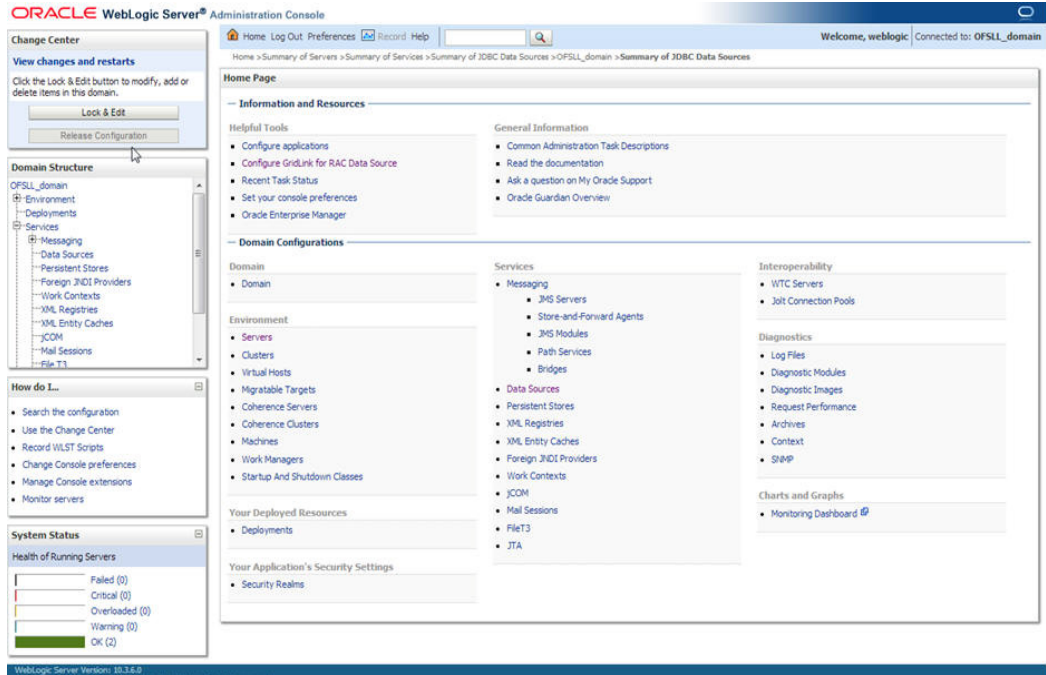
11. Click Add and target to OFSSL_AdminServer and OFSSL_ManagedServer as on right panel.

3.5 Creating Data Source

1. Login to WebLogic Server 11g console (<http://hostname:port/console>).

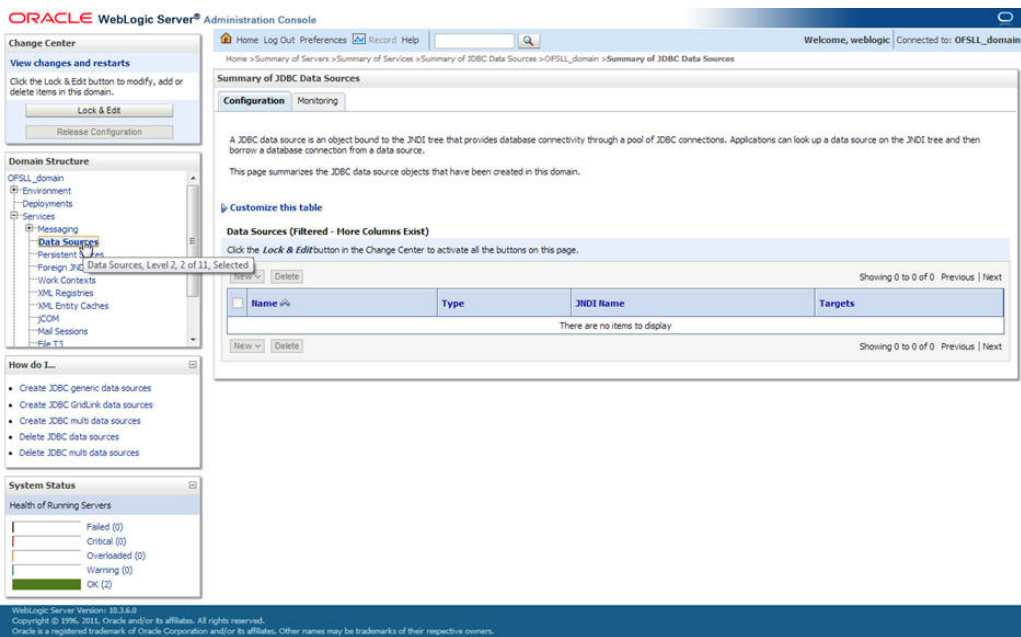


2. The following window is displayed.

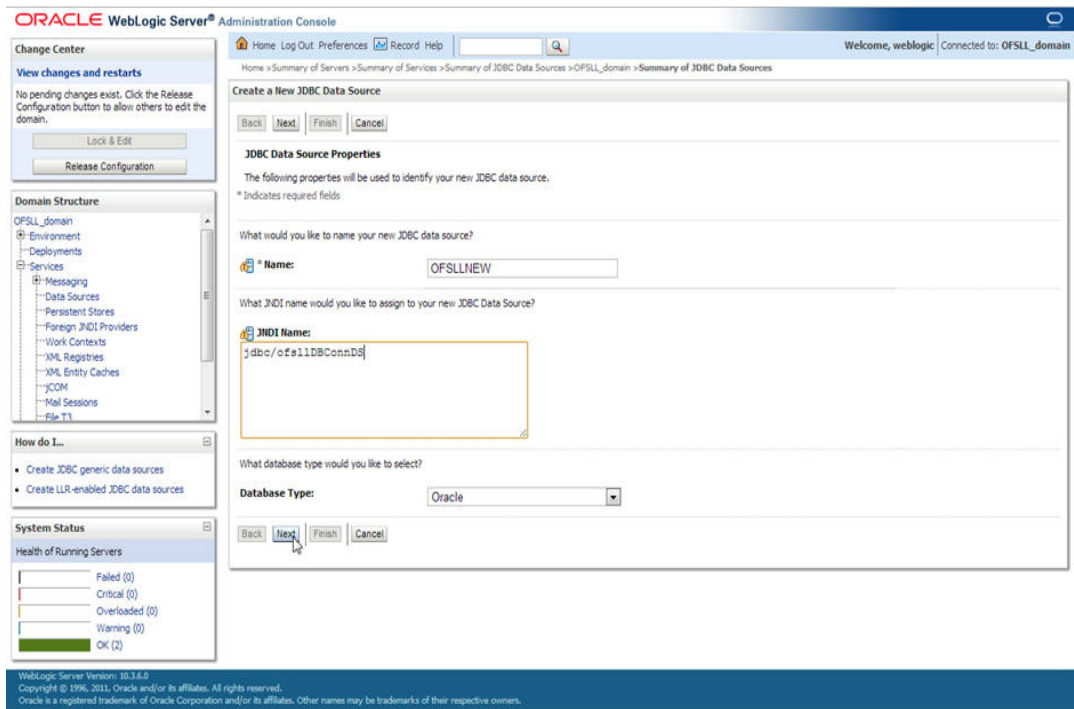


3. Click Domain Name → Services → Data Sources.

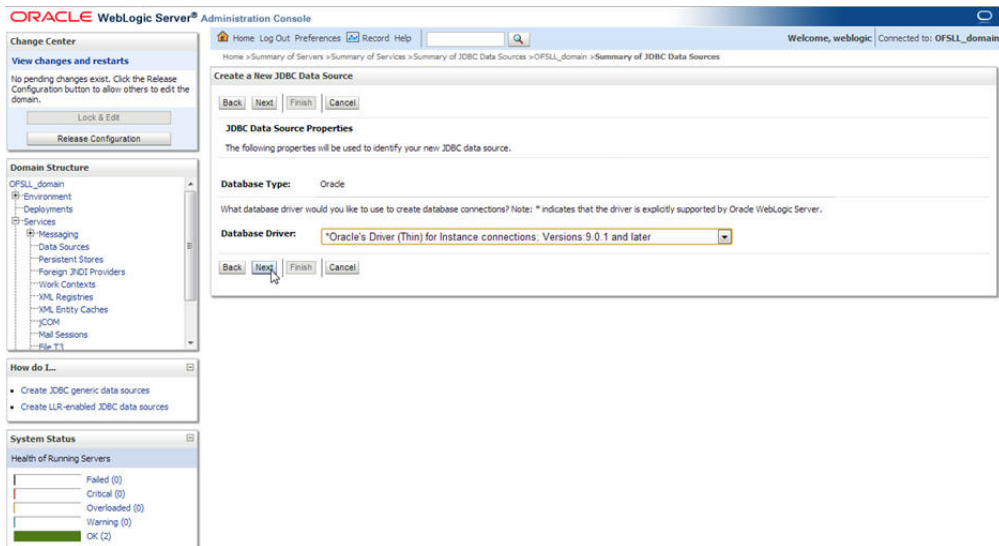
4. The following window is displayed.



- Click **Lock & Edit** button on the left panel. Click **New** on right panel and select **Generic Data Source**.

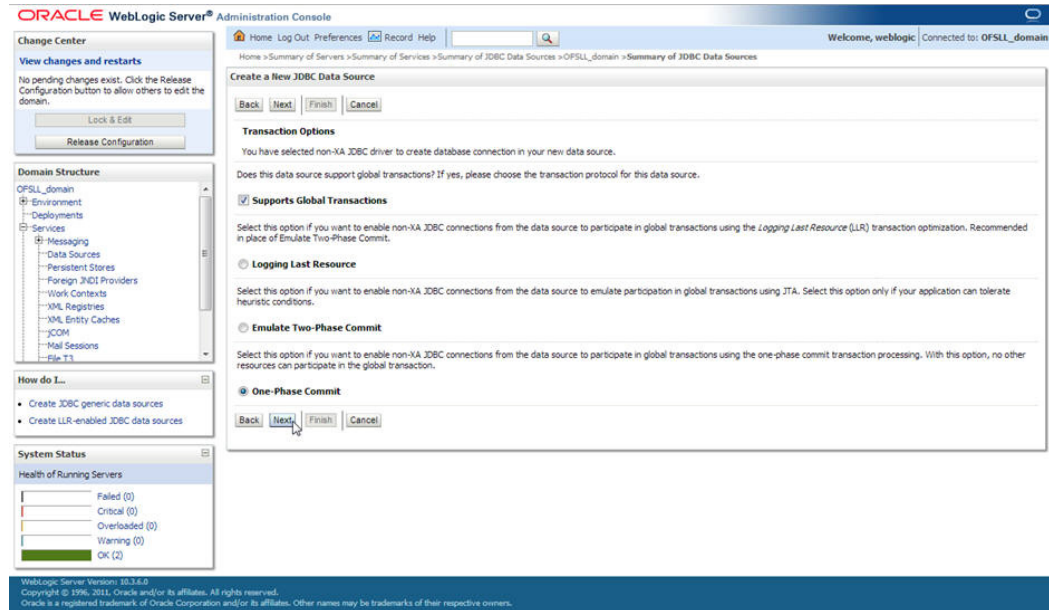


- Enter Data source **Name**
- Enter **JNDI Name** as **jdbc/ofs11DBConnDS**.
- Select **Oracle** as **Database Type** and click **Next**. The following window is displayed.

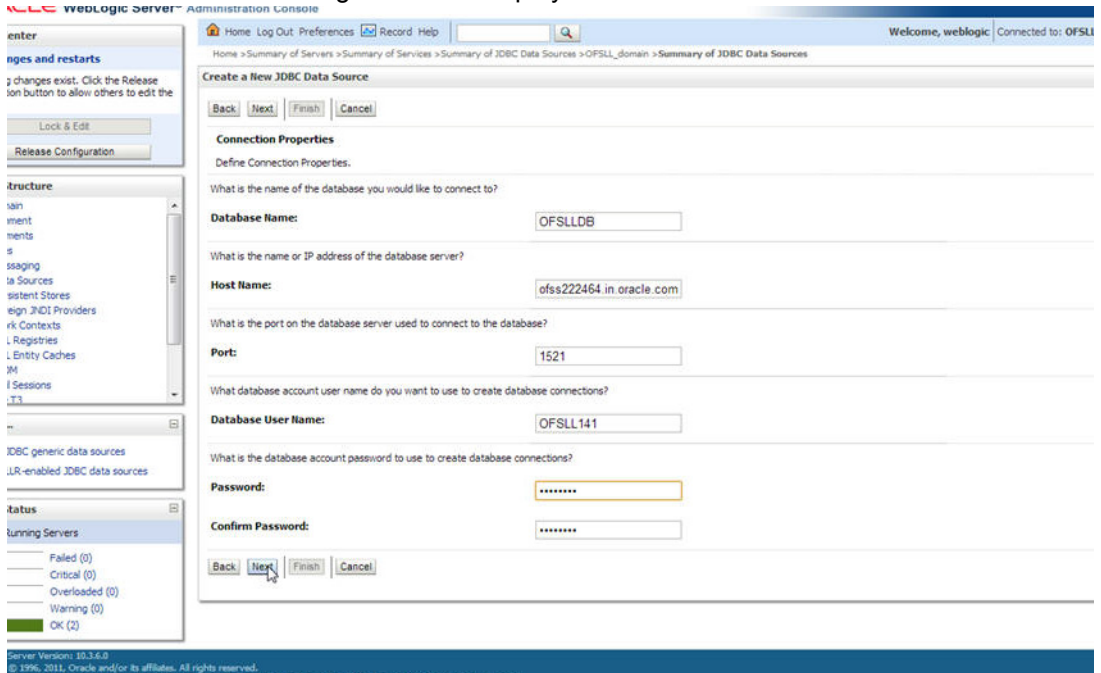


- Select the Database Driver "Oracle's Driver(Thin) for Instance connections; Versions:9.0.1 and later" as shown above.

10. Click **Next**. The following window is displayed.



11. Click **Next**. The following window is displayed.



12. Enter Database details click **Next**. The following window is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console. The main window is titled "Create a New JDBC Data Source". The "Test Database Connection" step is active, and the "Next" button is highlighted. The form contains the following fields and text:

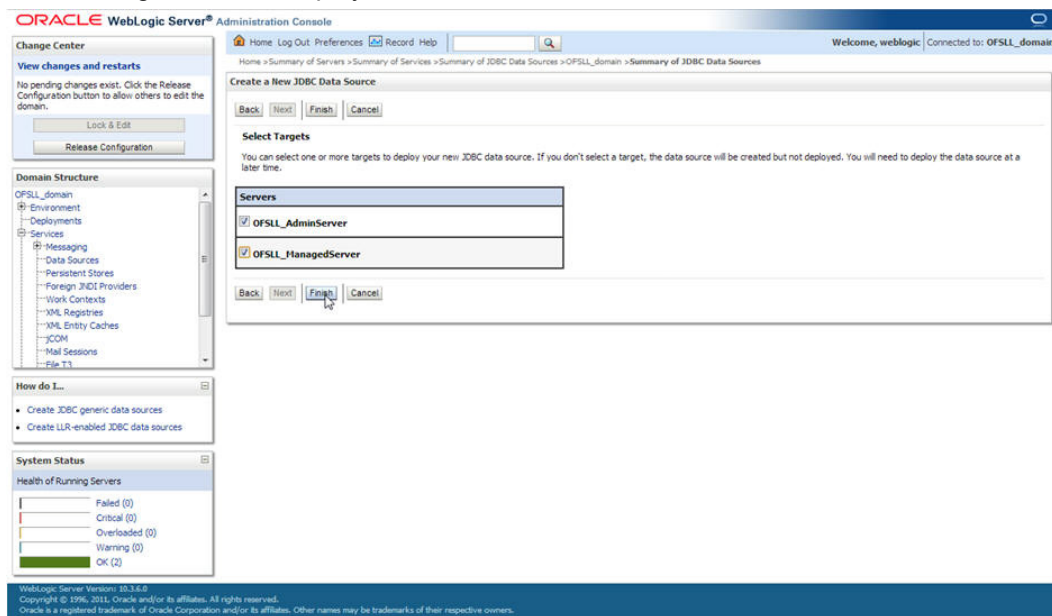
- Test Configuration:** Back, Next, Finish, Cancel
- Test Database Connection:** Test the database availability and the connection properties you provided.
- Driver Class Name:** oracle.jdbc.OracleDriver
- URL:** jdbc:oracle:thin:@ofss222
- Database User Name:** OFSLL141
- Password:** [Redacted]
- Confirm Password:** [Redacted]
- Properties:** user=OFSLL141

13. Click **Test Configuration**. The following window is displayed.

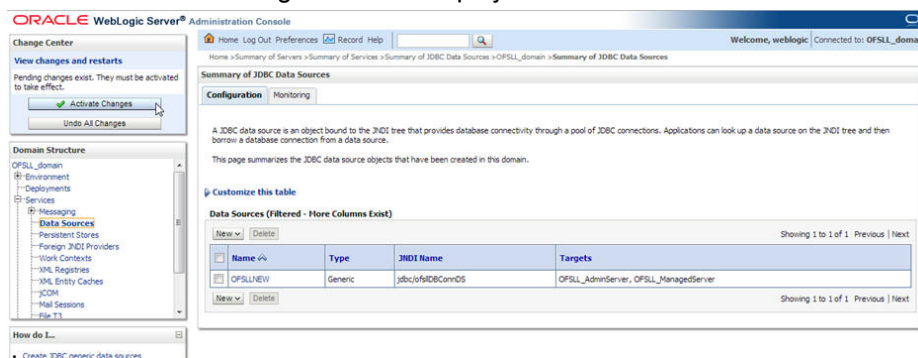
The screenshot shows the Oracle WebLogic Server Administration Console. The main window is titled "Create a New JDBC Data Source". The "Test Configuration" button is highlighted, and a message indicates "Connection test succeeded". The form contains the following fields and text:

- Test Configuration:** Back, Next, Finish, Cancel
- Test Database Connection:** Test the database availability and the connection properties you provided.
- Driver Class Name:** oracle.jdbc.OracleDriver
- URL:** jdbc:oracle:thin:@ofss222
- Database User Name:** OFSLL141
- Password:** [Redacted]
- Confirm Password:** [Redacted]
- Properties:** user=OFSLL141

14. Displays confirmation message as “Connection test succeeded”. Click **Next**. The following window is displayed.



15. Select target Servers **OFSSL_AdminServer** and **OFSSL_ManagedServer** and click **Finish**. The following window is displayed.



16. Click **Activate Changes** on the left panel.

Update the following parameters in JDBC data source connection pool:

1. Select **Services** → **Data Sources** → select the **OFSSL** data source → **Connection Pool**.
2. Initial capacity and Maximum capacity is defaulted to 15, if the number of concurrent users are more this needs to be increased.
3. Click **Advanced** button and update the following:
 - Inactive Connection Timeout=900
 - Uncheck the "Wrap Data Types" parameter for better performance.
4. Click **Save**.

3.6 Creating SQL Authentication Provider

1. Login to WebLogic server administration console and click Security Realms in left panel. The following window is displayed.

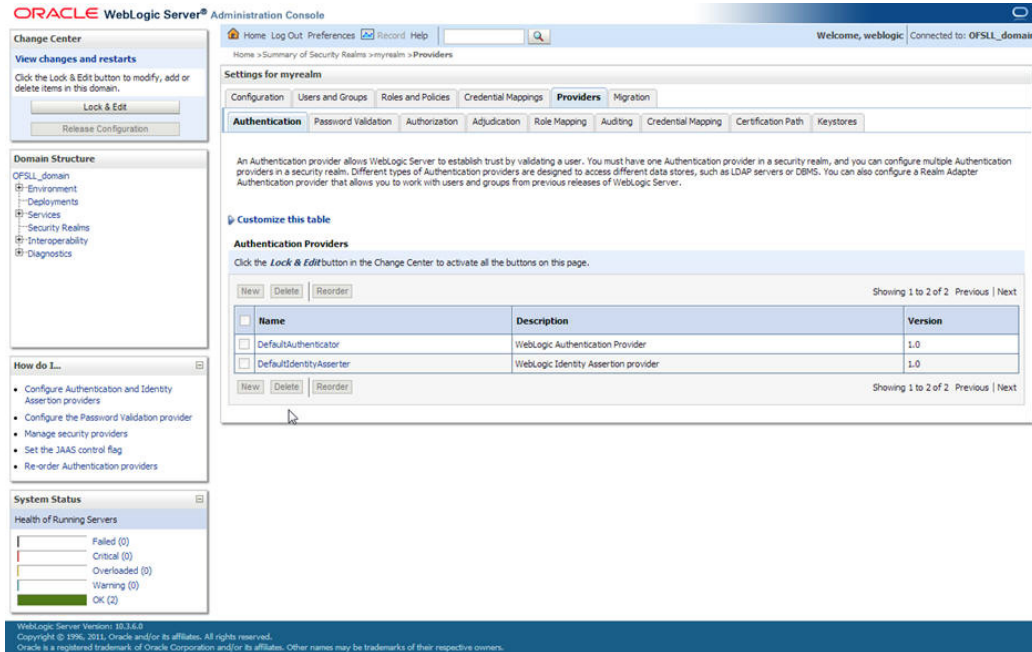
The screenshot shows the Oracle WebLogic Server Administration Console. The left-hand navigation pane is expanded to 'Security Realms'. The main content area displays the 'Summary of Security Realms' page. It includes a 'Change Center' on the left with 'Lock & Edit' and 'Release Configuration' buttons. Below that is the 'Domain Structure' tree showing 'OFSLL_domain' > 'Security Realms'. The 'How do I...' section lists tasks like 'Configure new security realms'. The 'System Status' section shows 'Health of Running Servers' with a bar chart indicating 'OK (2)'. The main panel shows a 'Summary of Security Realms' section with a table of realms. The table has columns for 'Name' and 'Default Realm'. One realm, 'myrealm', is listed with 'true' as its default realm. A 'Customize this Table' section is also visible.

| Name | Default Realm |
|---------|---------------|
| myrealm | true |

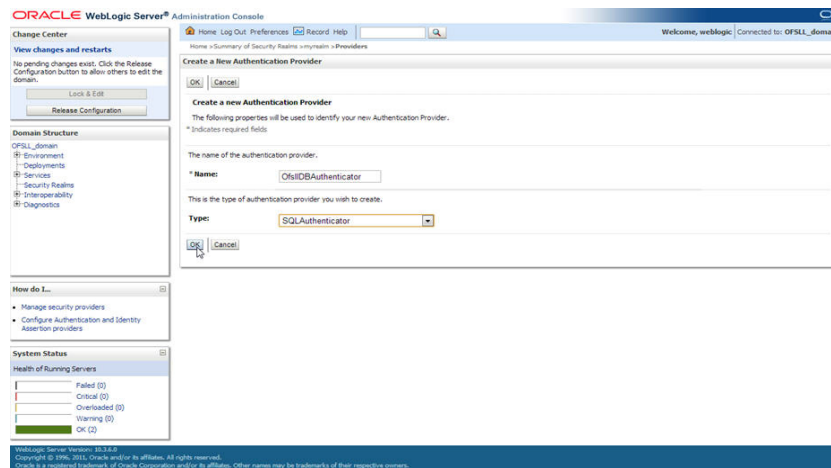
2. Click **myrealm** on right panel. The following window is displayed.

The screenshot shows the 'Settings for myrealm' page in the Oracle WebLogic Server Administration Console. The left-hand navigation pane is expanded to 'myrealm'. The main content area displays the 'Settings for myrealm' page. It includes a 'Change Center' on the left with 'Lock & Edit' and 'Release Configuration' buttons. Below that is the 'Domain Structure' tree showing 'OFSLL_domain' > 'Security Realms' > 'myrealm'. The 'How do I...' section lists tasks like 'Manage security for Web applications and EJBs'. The 'System Status' section shows 'Health of Running Servers' with a bar chart indicating 'OK (2)'. The main panel shows the 'Settings for myrealm' page with tabs for 'Configuration', 'Users and Groups', 'Roles and Policies', 'Credential Mappings', 'Providers', and 'Migration'. The 'Configuration' tab is active, showing a 'General' sub-tab. It includes a 'Save' button and a 'Note' section. The 'Name' field is set to 'myrealm'. The 'Security Model Default' is set to 'DD Only'. The 'Combined Role Mapping Enabled' checkbox is checked. The 'Use Authorization Providers to Protect JMX Access' checkbox is unchecked. The 'Advanced' section is collapsed.

3. Click on Providers tab. The following window is displayed.



4. Click **Lock & Edit** to unlock the screen and click **New** button in Authentication Providers sub tab. The following window is displayed.

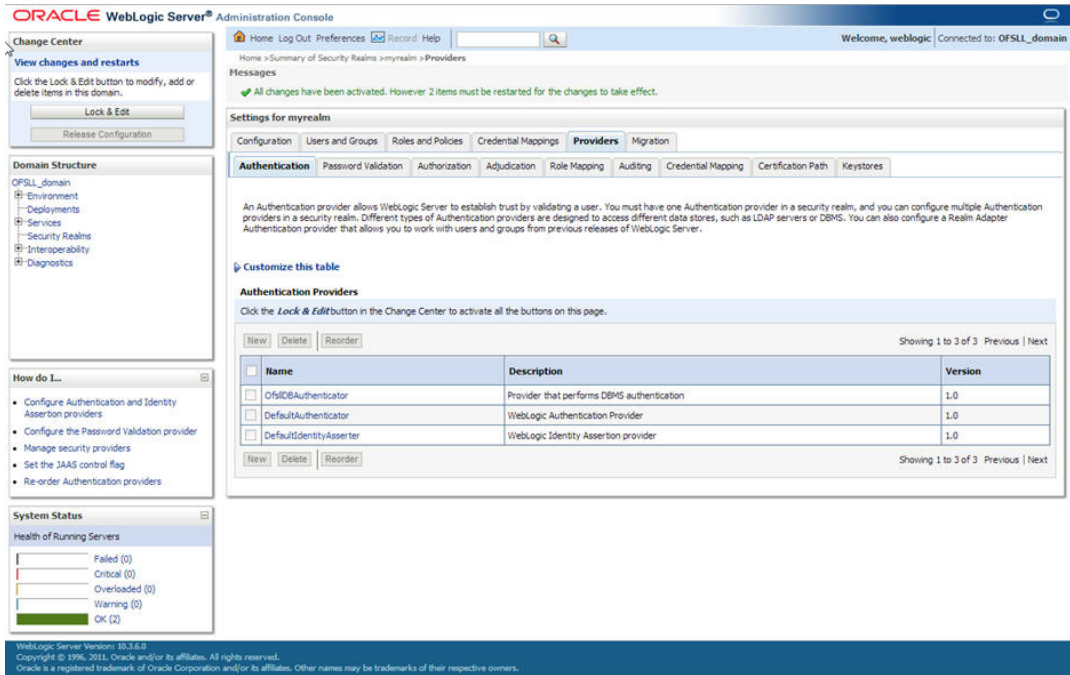


5. Create Authentication provider with following values.

Name: **OFSLLDBAuthenticator**

Type: **SQLAuthenticator**

6. Click OK button. The following window is displayed.

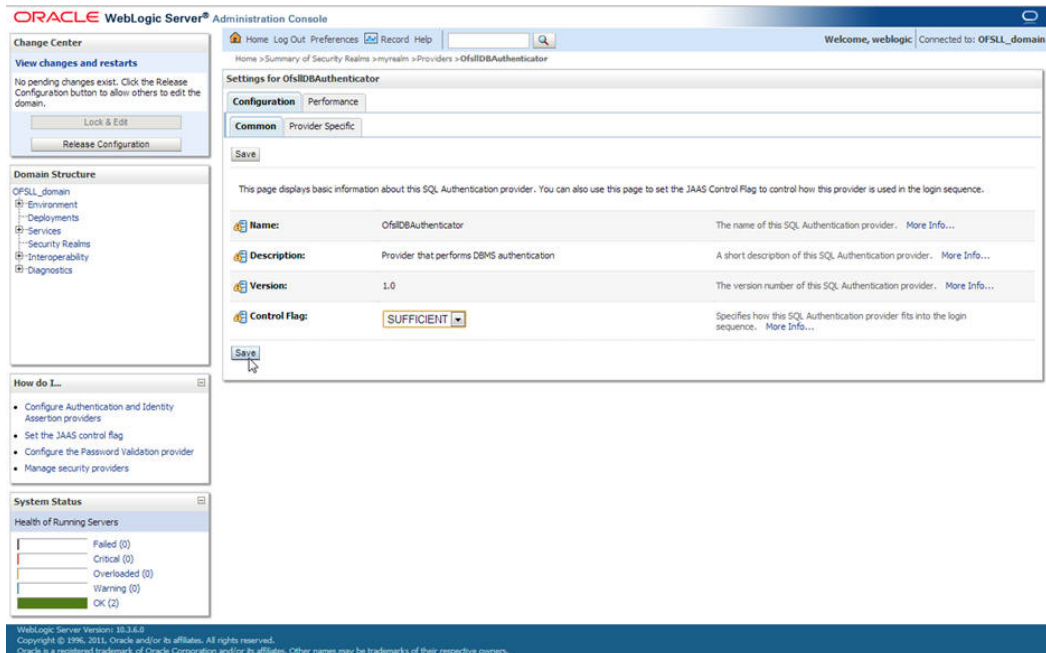


Authentication order should be maintained as mentioned in the above screen.

7. **OFSLDBAuthenticator** will be displayed as above.

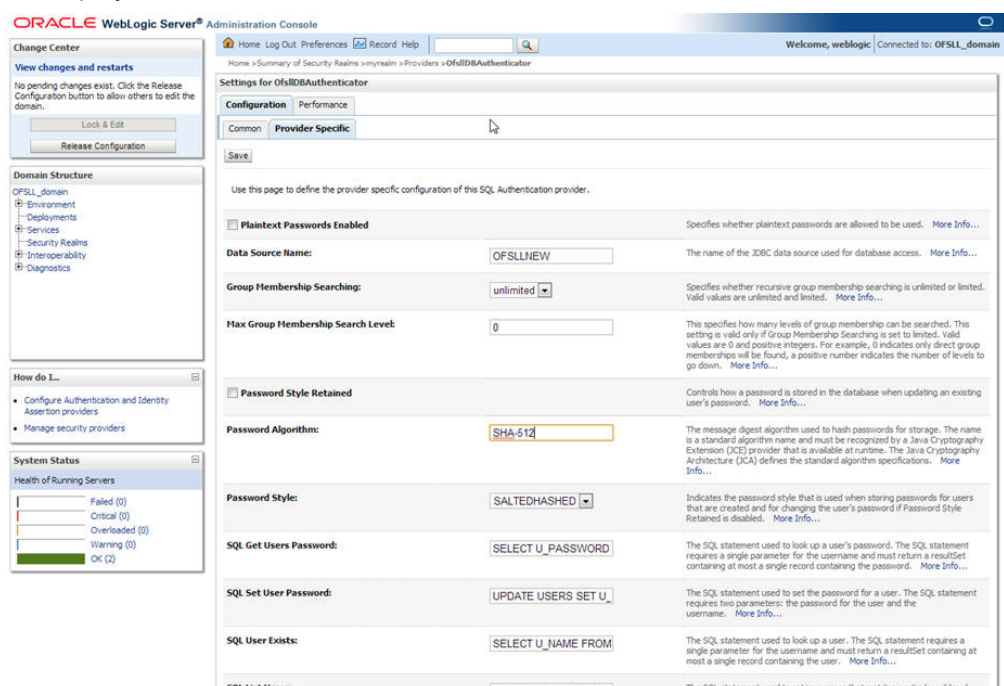
8. Click on **OFSLDBAuthenticator**.

9. The following window is displayed.



10. Select SUFFICIENT as the **Control Flag** and click Save.

11. Click Provider Specific sub tab under Configuration tab. The following window is displayed.



12. Provide the following values in corresponding fields.

Data Source Name: **OFSLLNEW**

Password Style Retained: **Uncheck**

Password Algorithm: **SHA-512**

Password Style: **SALTEDHASHED**

Provide the SQL Queries from the column **Corresponding SQL Queries as per OFSLL Tables** as given below.

| Operation | Default SQL Query from Weblogic | Corresponding SQL Queries as per our Tables |
|-------------------------|--|--|
| SQL Get Users Password: | SELECT U_PASSWORD FROM USERS WHERE U_NAME = ? | SELECT UAU_USR_PASSWORD FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ? |
| SQL Set User Password: | UPDATE USERS SET U_PASSWORD = ? WHERE U_NAME = ? | UPDATE USER_AUTHORISATIONS SET UAU_USR_PASSWORD = ? WHERE UAU_USR_CODE = ? |
| SQL User Exists: | SELECT U_NAME FROM USERS WHERE U_NAME = ? | SELECT UAU_USR_CODE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ? |
| SQL List Users: | SELECT U_NAME FROM USERS WHERE U_NAME LIKE ? | SELECT UAU_USR_CODE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE LIKE ? |

| Operation | Default SQL Query from Weblogic | Corresponding SQL Queries as per our Tables |
|-------------------------------|--|--|
| SQL Create User: | INSERT INTO USERS VALUES (?, ?, ?) | INSERT INTO USER_AUTHORISATIONS(UAU_USR_CODE, UAU_USR_PASSWORD,UAU_DESC) VALUES(?,?,?) |
| SQL Remove User: | DELETE FROM USERS WHERE U_NAME = ? | DELETE FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE= ? |
| SQL List Groups: | SELECT G_NAME FROM GROUPS WHERE G_NAME LIKE ? | SELECT UGR_GROUP_CODE FROM USER_GROUPS WHERE UGR_GROUP_CODE LIKE ? |
| SQL Group Exists: | SELECT G_NAME FROM GROUPS WHERE G_NAME = ? | SELECT UGR_GROUP_CODE FROM USER_GROUPS WHERE UGR_GROUP_CODE = ? |
| SQL Create Group: | INSERT INTO GROUPS VALUES (?, ?) | INSERT INTO USER_GROUPS(UGR_GROUP_CODE,UGR_GROUP_DESC) VALUES(?,?) |
| SQL Remove Group: | DELETE FROM GROUPS WHERE G_NAME = ? | DELETE FROM USER_GROUPS WHERE UGR_GROUP_CODE = ? |
| SQL Is Member: | SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER = ? | SELECT UGM_MEMBER_USR_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE = ? |
| SQL List Member Groups: | SELECT G_NAME FROM GROUPMEMBERS WHERE G_MEMBER = ? | SELECT UGM_MEMBER_GROUP_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_USR_CODE= ? |
| SQL List Group Members: | SELECT G_MEMBER FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER LIKE ? | SELECT UGM_MEMBER_USR_CODE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE LIKE ? |
| SQL Remove Group Memberships: | DELETE FROM GROUPMEMBERS WHERE G_MEMBER = ? OR G_NAME = ? | DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_USR_CODE= ? OR UGM_MEMBER_GROUP_CODE= ? |
| SQL Add Member To Group: | INSERT INTO GROUPMEMBERS VALUES(?, ?) | INSERT INTO USER_GROUP_MEMBERS (UGM_MEMBER_GROUP_CODE,UGM_MEMBER_USR_CODE) VALUES(?,?) |

| Operation | Default SQL Query from Weblogic | Corresponding SQL Queries as per our Tables |
|-------------------------------|--|--|
| SQL Remove Member From Group: | DELETE FROM GROUPMEMBERS WHERE G_NAME = ? AND G_MEMBER = ? | DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? AND UGM_MEMBER_USR_CODE= ? |
| SQL Remove Group Member: | DELETE FROM GROUPMEMBERS WHERE G_NAME = ? | DELETE FROM USER_GROUP_MEMBERS WHERE UGM_MEMBER_GROUP_CODE= ? |
| SQL Get User Description: | SELECT U_DESCRIPTION FROM USERS WHERE U_NAME = ? | SELECT UAU_DESC FROM USER_AUTHORISATIONS WHERE UAU_USR_CODE = ? |
| SQL Set User Description: | UPDATE USERS SET U_DESCRIPTION = ? WHERE U_NAME = ? | UPDATE USER_AUTHORISATIONS SET UAU_DESC= ? WHERE UAU_USR_CODE= ? |
| SQL Get Group Description: | SELECT G_DESCRIPTION FROM GROUPS WHERE G_NAME = ? | SELECT UGR_GROUP_DESC FROM USER_GROUPS WHERE UGR_GROUP_CODE= ? |
| SQL Set Group Description: | UPDATE GROUPS SET G_DESCRIPTION = ? WHERE G_NAME = ? | UPDATE USER_GROUPS SET UGR_GROUP_DESC= ? WHERE UGR_GROUP_CODE= ? |
| Provider Name | OFSLLDBAuthenticator | |

13. Click Save.

Note

Application server needs to be restarted for these changes to take effect.

3.7 Creating User Groups and Users

3.7.1 Creating Users

Create an OFSLL application super user to login to the application.

A script is provided in the distribution media in the dba_utils folder to create an user.

Note

By default there are no users created to login to OFSLL application.

Run the script "crt_app_user.sql script" as a OFSLL application owner user.

```
$ sqlplus
SQL*Plus: Release 11.2.0.3.0 Production on Wed Nov 27 15:06:06 2013
Copyright (c) 1982, 2011, Oracle. All rights reserved.

Enter user-name: OFSLL141
Enter password:

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> @/tmp/dba_utils/crt_app_user.sql
Enter the name of the OFSLL App user Id you
Want to create user: OLLUSER
Enter the First Name for this user: OLL
Enter the Last Name for this user: USER
Enter the Phone Number for this user: 9090900990
Enter the Fax Number for this user: 8976986798

1 row created.

1 row created.

1 row created.

SQL> █
```

1. Login into WebLogic server console.
2. Click **Security Realms** on the left panel.
3. Click **myrealm** on the right panel..

The screenshot displays the Oracle WebLogic Server Administration Console. The main content area is titled "Summary of Security Realms" and contains a table of configured realms. The table has two columns: "Name" and "Default Realm". One realm, "myrealm", is listed with its "Default Realm" set to "true". The interface includes a left-hand navigation pane with "Security Realms" selected, and a top navigation bar with "Home", "Log Out", "Preferences", "Record", and "Help".

| Name | Default Realm |
|---------|---------------|
| myrealm | true |

1. Select **Users** tab under **Users and Groups**.

- If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Users are automatically created in weblogic when created through an application.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area displays the 'Users' tab under 'Users and Groups'. A table lists the following users:

| Name | Description | Provider |
|------------------|--|----------------------|
| BATCH | BATCH USER | OsfIDBAuthenticator |
| DEMOCOLL | DEMO COLLECTOR | OsfIDBAuthenticator |
| DEMOSALES | DEMO SALES AGENT | OsfIDBAuthenticator |
| DEMOSUPR | DEMO SUPERUSER | OsfIDBAuthenticator |
| DEMOUNDRW | DEMO UNDERWRITER | OsfIDBAuthenticator |
| EVENT | BATCH USER | OsfIDBAuthenticator |
| OLLUSER | OLL USER | OsfIDBAuthenticator |
| OracleSystemUser | Oracle application software system user. | DefaultAuthenticator |
| USER1 | USER1 | OsfIDBAuthenticator |
| weblogic | This user is the default administrator. | DefaultAuthenticator |

3.7.2 Creating User Groups

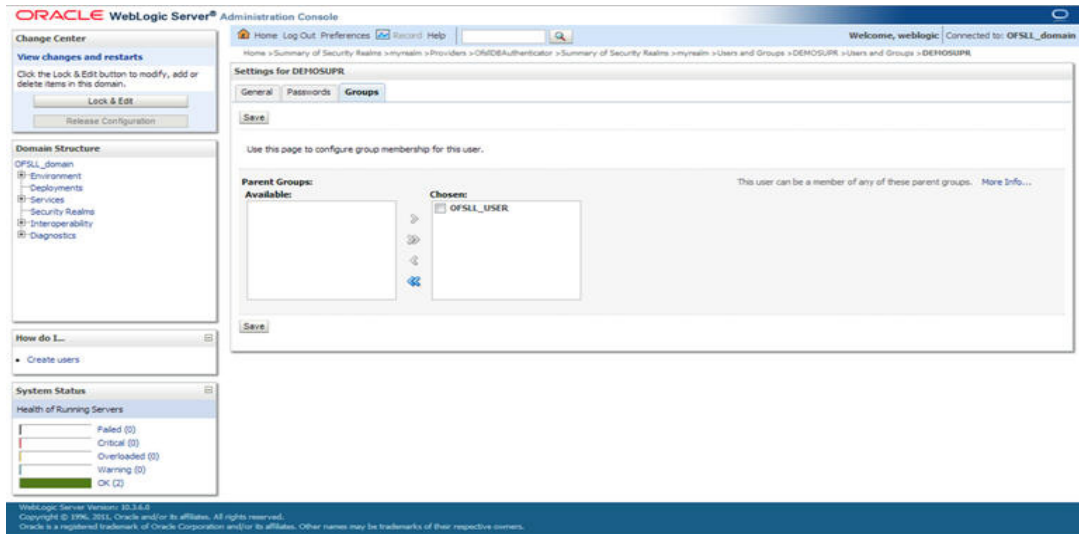
- Select **Groups** tab under **Users and Groups**.
- If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Groups are automatically created in weblogic when created through an application.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area displays the 'Groups' tab under 'Users and Groups'. A table lists the following groups:

| Name | Description | Provider |
|-----------------------|--|----------------------|
| AdminChannelUsers | AdminChannelUsers can access the admin channel. | DefaultAuthenticator |
| Administrators | Administrators can view and modify all resource attributes and start and stop servers. | DefaultAuthenticator |
| AppTesters | AppTesters group. | DefaultAuthenticator |
| CrossDomainConnectors | CrossDomainConnectors can make inter-domain calls from foreign domains. | DefaultAuthenticator |
| Deployers | Deployers can view all resource attributes and deploy applications. | DefaultAuthenticator |
| Monitors | Monitors can view and modify all resource attributes and perform operations not restricted by roles. | DefaultAuthenticator |
| OFSLL_USER | OFSLL USER GROUP | OsfIDBAuthenticator |
| Operators | Operators can view and modify all resource attributes and perform server lifecycle operators. | DefaultAuthenticator |
| OracleSystemGroup | Oracle application software system group. | DefaultAuthenticator |

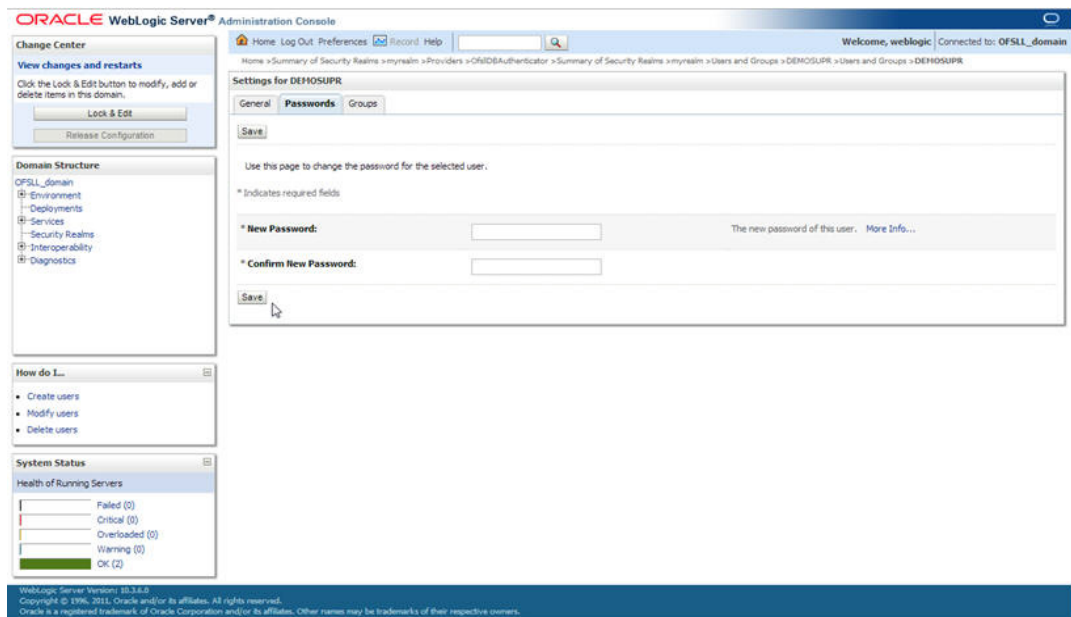
3.7.3 Assigning Users to Groups

The USERS are automatically mapped to default application group - OFSSL_USER.

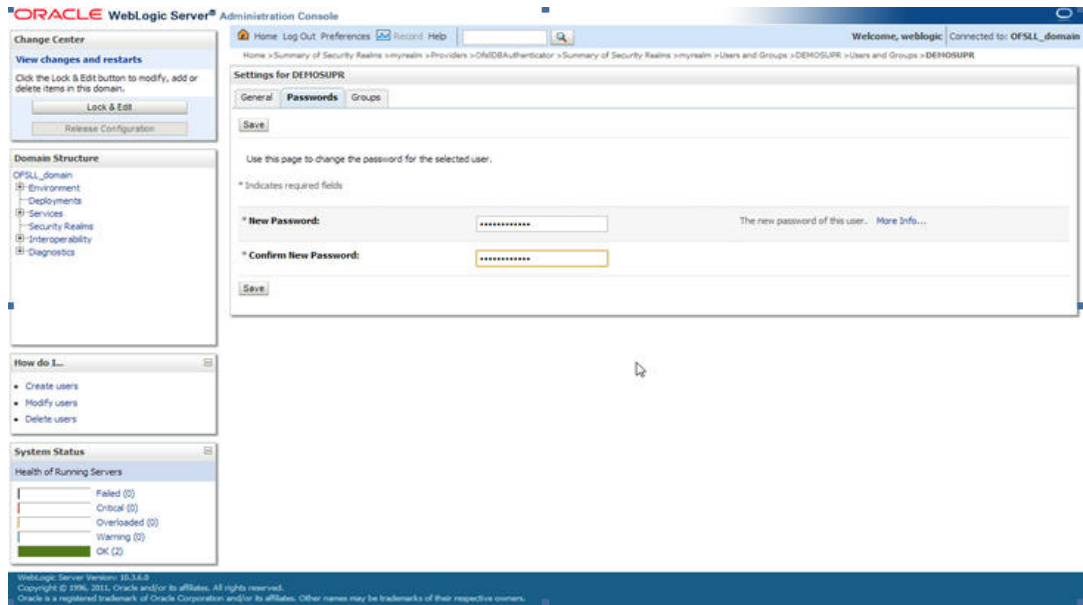


3.7.4 Resetting password via weblogic console

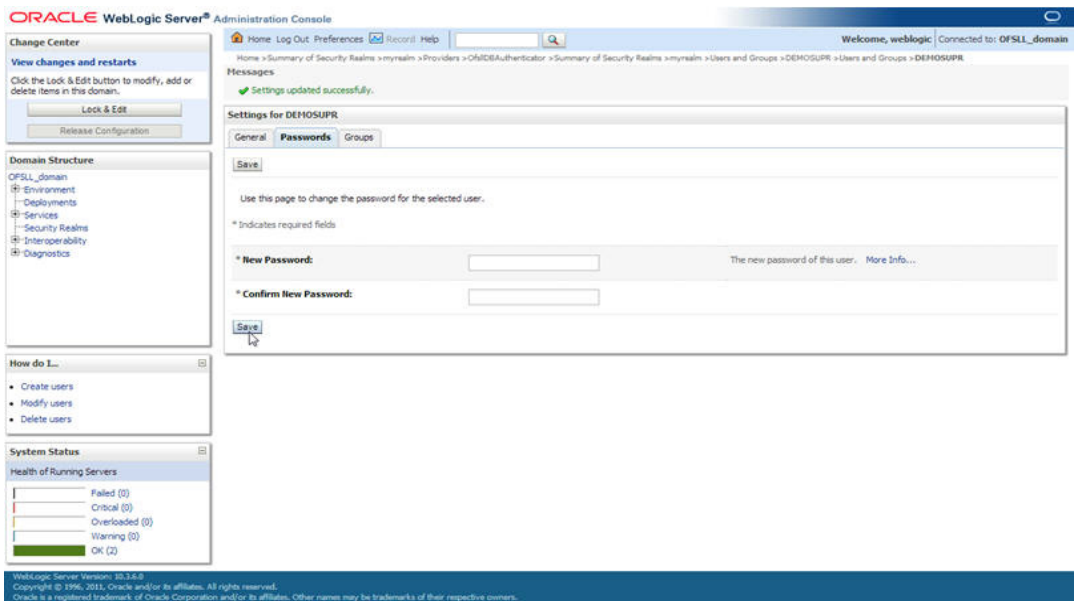
1. Click on **User**. Select **Passwords** tab. The following window is displayed.



2. Enter the new password and confirm password.



3. Click on **Save**. The following window displayed.



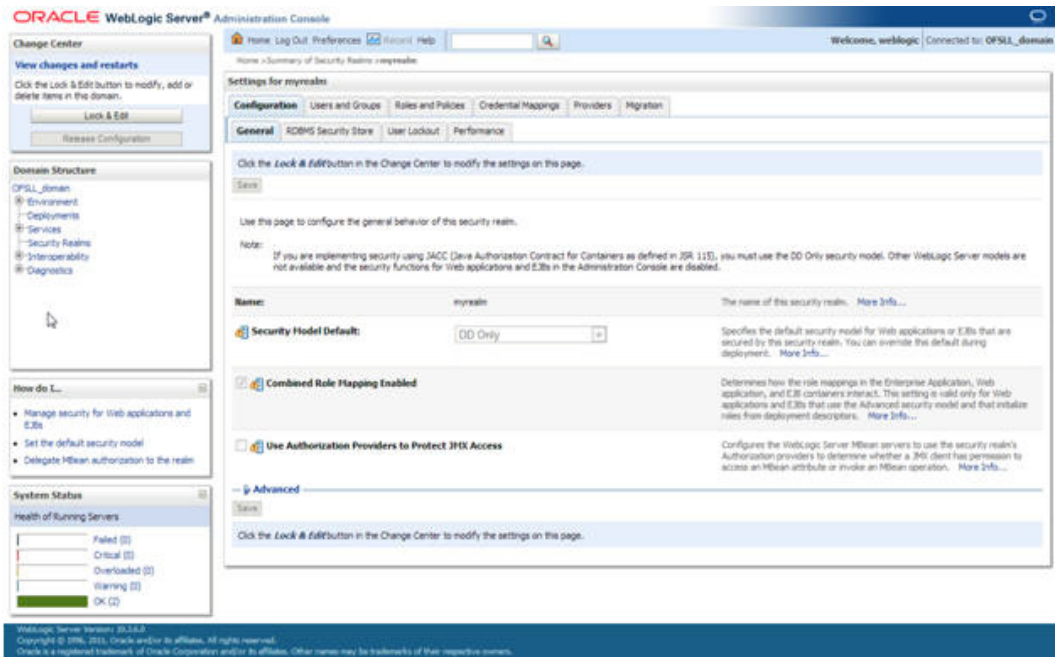
3.8 Implementing JMX Policy for Change Password

1. Login to Oracle WebLogic Server 11g console (<http://hostname:port/console>)

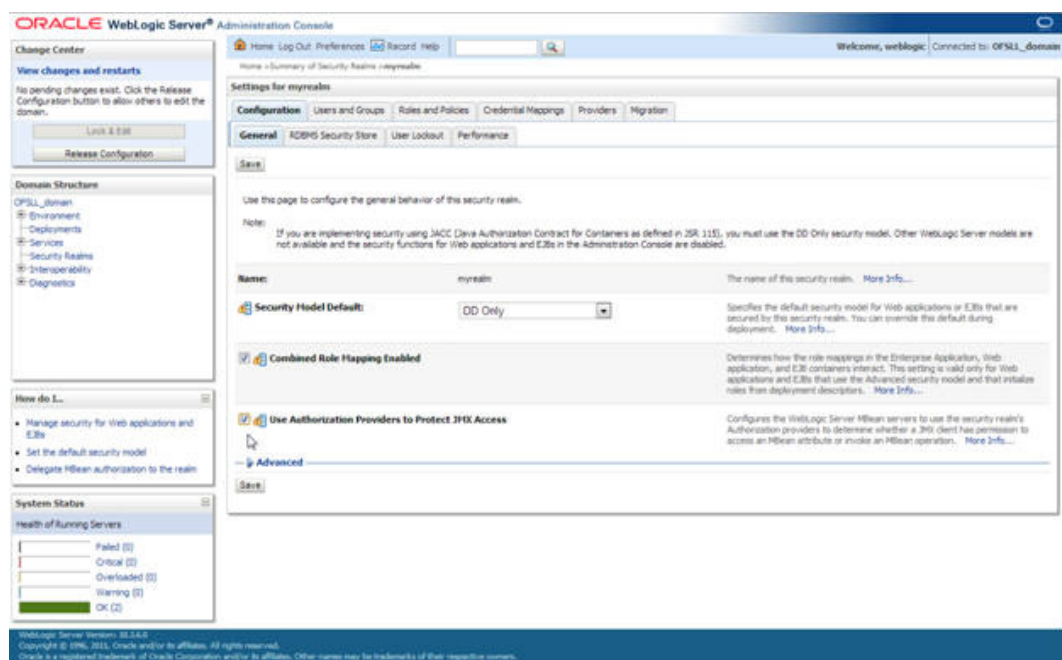
Note

The Change Password feature uses the JMX Policy configured on the domain. Hence, the AdminServer is required to be up and running to enable this.

2. Click **Domain** → **Security** → **myrealm** → **Configuration**



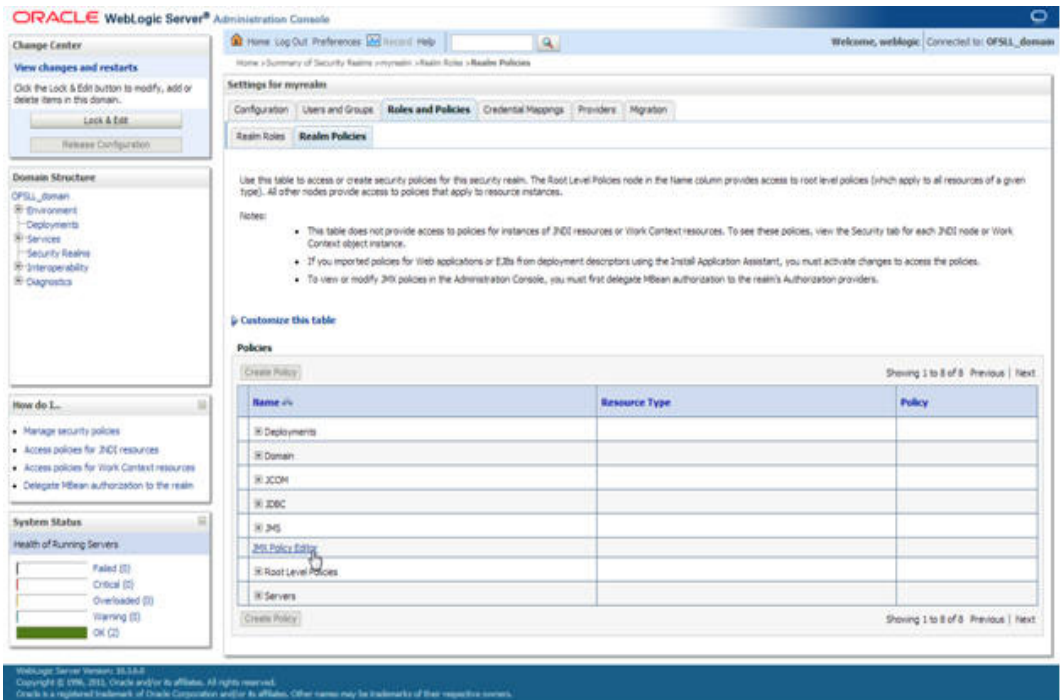
3. To enable JMX policy select the "Use Authorization Providers to Protect JMX Access" check box on the right panel



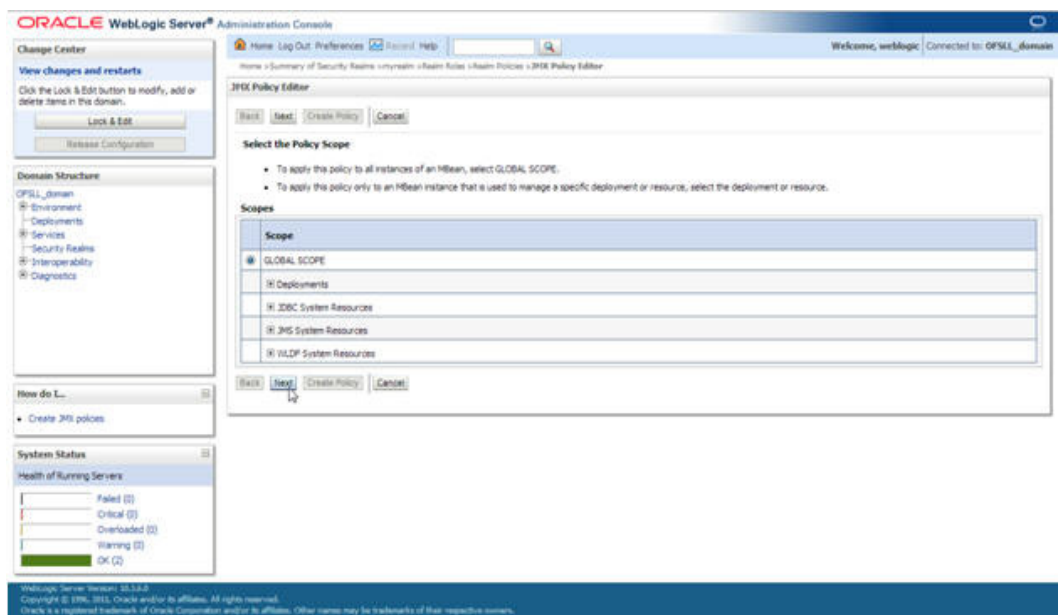
4. Click **Save** and restart the server.
5. Re-login to console.
6. Click **Domain** → **Security** → **myrealm** → **Roles and Policies** → **Realm Policies**

Note

If server is not restarted, JMX Policy Editor option will not appear



7. Click on JMX Policy Editor to configure



8. Select GLOBAL SCOPE

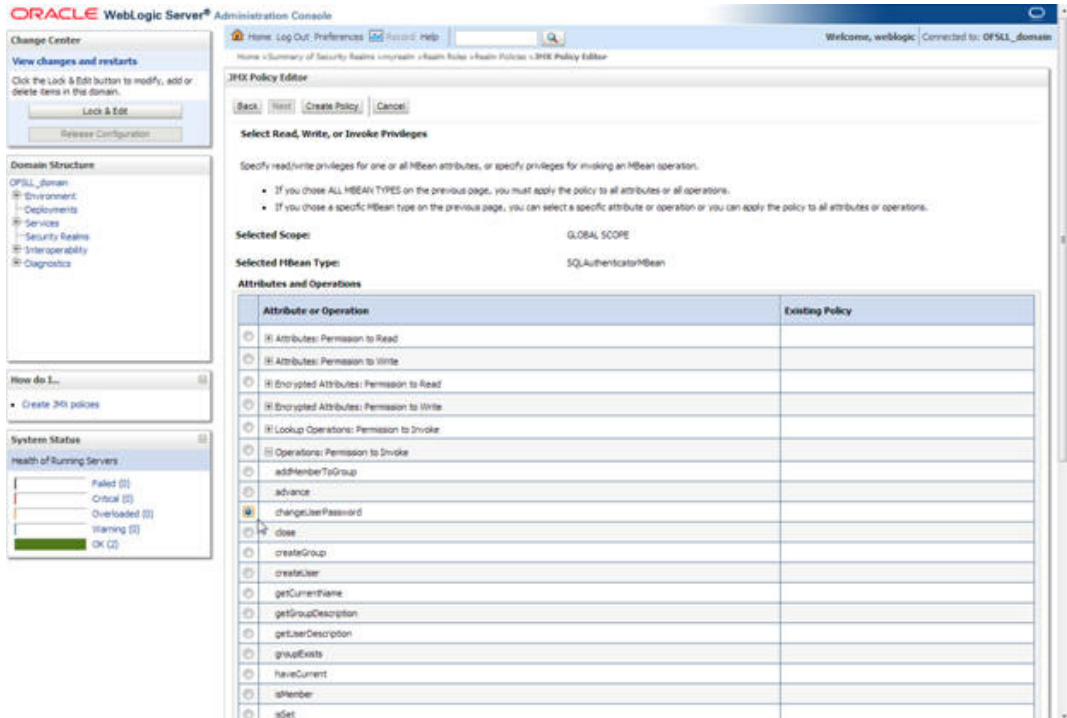
9. Click Next



WebLogic Server Version: 10.3.6.0
Copyright © 1996, 2011, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

10. Select weblogic.security.providers.authentication.

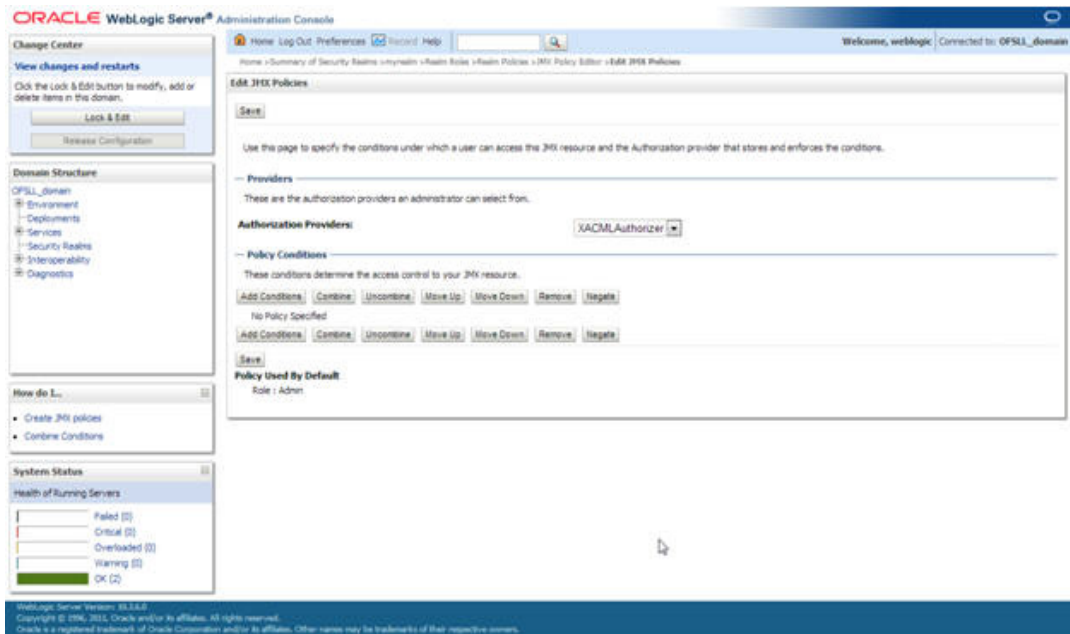
11. Select "SQLAuthenticatorMBean". Click Next.



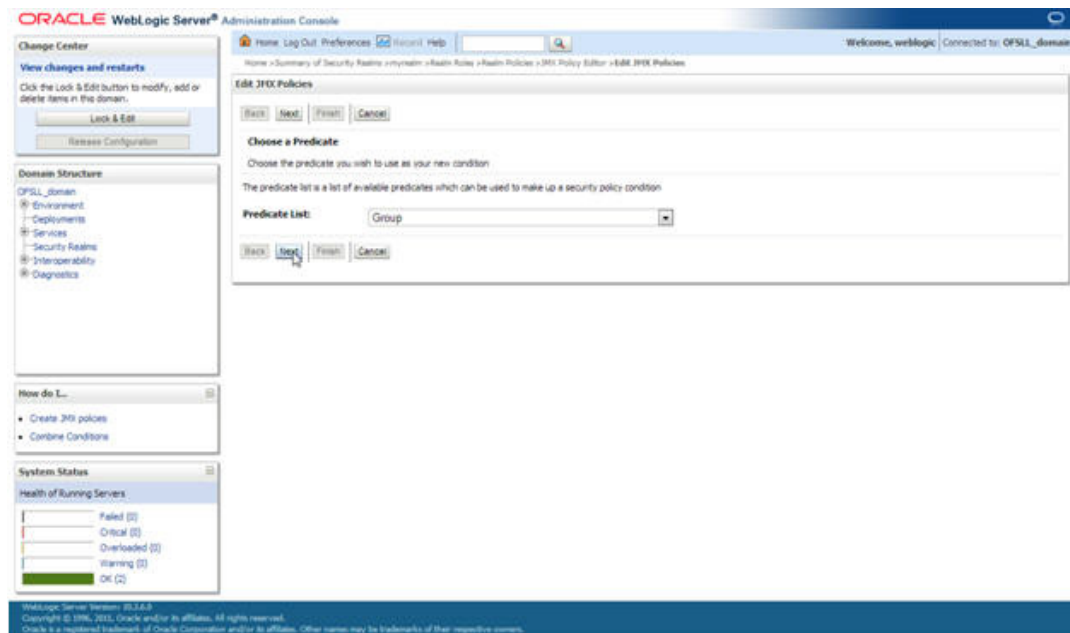
12. Expand "Operations: Permissions to Invoke" and select "ChangePassword"

13. Click "Create Policy"

- It opens the below screen for Authorization providers where you can add conditions to setup the policy.

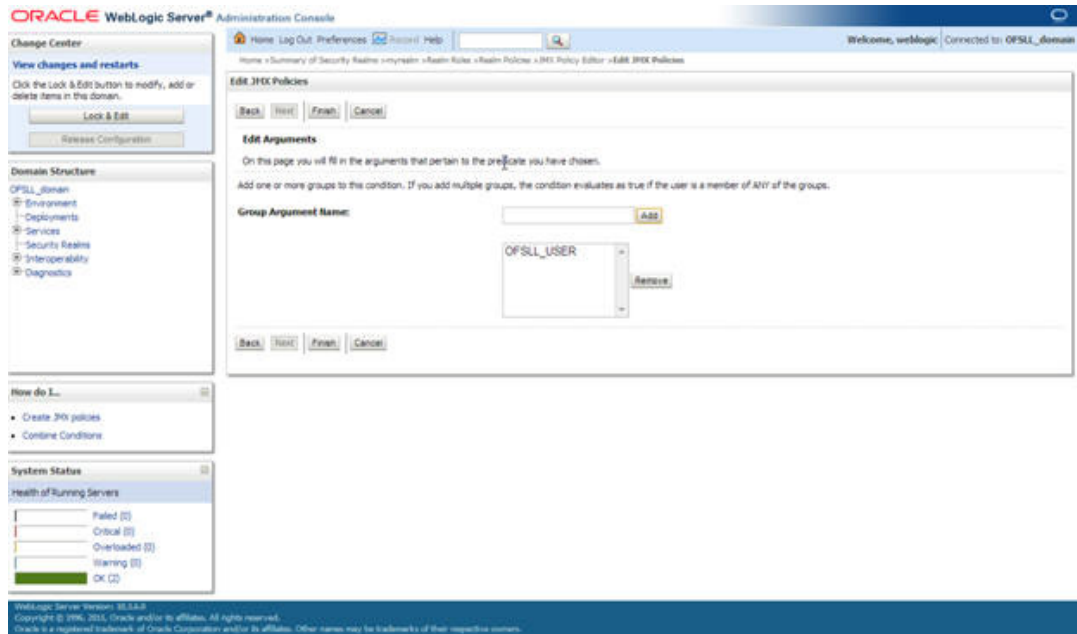


- Click **Add Condition**. The below screen will be displayed.



- For **Predicate List**, select **Group** for configuration.

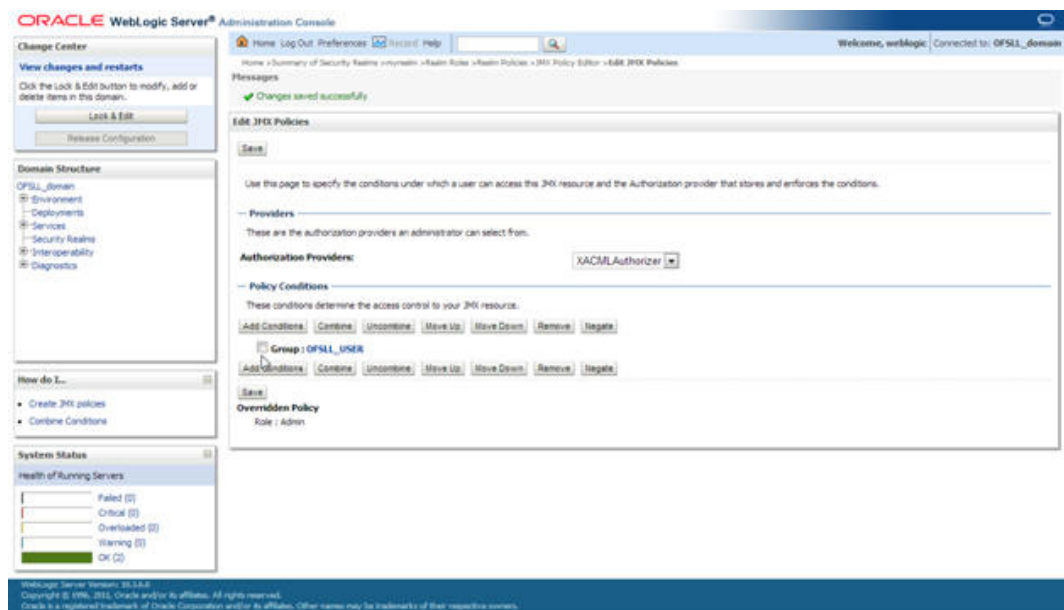
17. Click Next.



18. Select user roles for application.

19. Click Finish. Click on Save to complete the configuration. The following window will be displayed.

3.9 Migrating Policy from File to Database



For the scalability and manageability of the policy, you must migrate them from a file to database.

To migrate policy from File to Database:

1. Create a data source for OPSS schema with non XA and non global transaction.

| Name | Type | JNDI Name | Targets |
|--------------|---------|--------------------|------------------------------------|
| jdbc/devopss | Generic | jdbc/devopss | 126_AdminServer, 126_ManagedServer |
| mids-126 | Generic | jdbc/mids/126 | 126_AdminServer, 126_ManagedServer |
| OFSLLNEW | Generic | jdbc/ofslIDBConnDS | 126_AdminServer, 126_ManagedServer |

For data source creation refer [Creating Data Source](#) section of this chapter.

2. Go to \$MW_Home/oracle_common/common/bin.
3. Run /setWlstEnv.sh
4. Run /wlst.sh.
5. When prompted, enter **connect()**
6. Enter Username, Password and Server URL
7. Run the below command:

```
reassociateSecurityStore(domain="OFSLL_domain",servertime="DB_ORACLE",datasourcename="jdbc/devopss",jpsroot="cn=opssNode",join="false")
```

datasourcename is the data source created in Step 1.

```
wls:/OFSLL_domain/serverConfig> reassociateSecurityStore(domain="OFSLL_domain",servertime="DB_ORACLE",datasourcename="jdbc/devopss",jpsroot="cn=opssNode",join="false")
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean as the root.
For more help, use help(domainRuntime)

Starting policy store reassociation.
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Policy store reassociation done.
Starting credential store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Credential store reassociation done
Starting Keystore reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Keystore reassociation done
Starting audit store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Audit store reassociation done
Jps Configuration has been changed. Please restart the application server.
```

8. The policy gets migrated from file to Database.
9. Restart the server for the changes to take effect.

4. Configuring Policies

4.1 Configuring Password Policy for SQL Authenticator

1. Login to the WebLogic server administration console with user login credentials.
2. Browse to **Security Realms** → **myrealm** → **Providers** as shown below. The following window is displayed

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for myrealm" and has tabs for Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers, and Migration. The "Providers" tab is active, and the "Authentication" sub-tab is selected. A table titled "Authentication Providers" lists three providers: OfidDBAuthenticator, DefaultAuthenticator, and DefaultIdentityAsserter. The "OfidDBAuthenticator" provider is highlighted.

| Name | Description | Version |
|--|--|---------|
| <input type="checkbox"/> OfidDBAuthenticator | Provider that performs DBMS authentication | 1.0 |
| <input type="checkbox"/> DefaultAuthenticator | WebLogic Authentication Provider | 1.0 |
| <input type="checkbox"/> DefaultIdentityAsserter | WebLogic Identity Assertion provider | 1.0 |

3. Click **Password Validation** tab. The following window is displayed

The screenshot shows the Oracle WebLogic Server Administration Console with the "Password Validation" sub-tab selected. A table titled "Password Validation Providers" lists one provider: SystemPasswordValidator. The "SystemPasswordValidator" provider is highlighted.

| Name | Description | Version |
|--|-----------------------------|---------|
| <input type="checkbox"/> SystemPasswordValidator | Password composition checks | 1.0 |

4. Click **SystemPasswordValidator** link. The following window is displayed

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for SystemPasswordValidator" and has two tabs: "Common" (selected) and "Provider Specific". The "Common" tab displays the following information:

| | | |
|---------------------|-----------------------------|---|
| Name: | SystemPasswordValidator | The name of this System Password Validation provider. More Info... |
| Description: | Password composition checks | A short description of the System Password Validator provider. More Info... |
| Version: | 1.0 | The version number of the System Password Validator provider. More Info... |

On the left side, there are several panels: "Change Center" with "Lock & Edit" and "Release Configuration" buttons; "Domain Structure" showing a tree view; "How do I..."; and "System Status" showing "Health of Running Servers" with a bar chart indicating 2 OK servers.

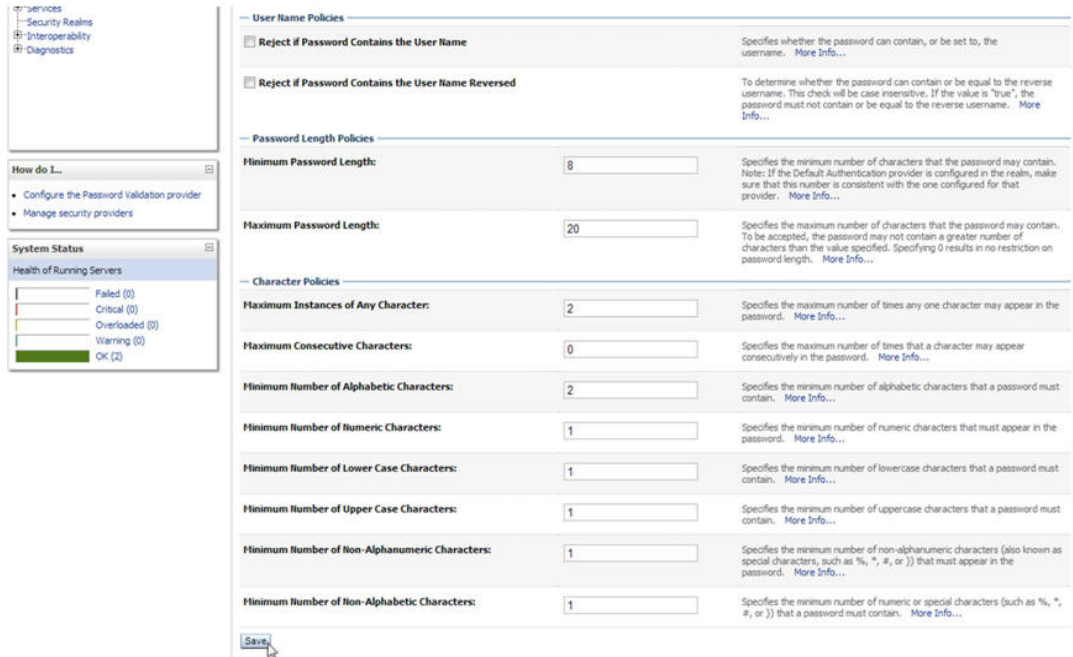
5. Click **Provider Specific** Tab. The following window is displayed.

The screenshot shows the "Provider Specific" configuration page for SystemPasswordValidator. It contains several sections with configuration options and their descriptions:

- User Name Policies:**
 - Reject if Password Contains the User Name**: Specifies whether the password can contain, or be set to, the username. [More Info...](#)
 - Reject if Password Contains the User Name Reversed**: To determine whether the password can contain or be equal to the reverse username. This check will be case insensitive. If the value is "true", the password must not contain or be equal to the reverse username. [More Info...](#)
- Password Length Policies:**
 - Minimum Password Length:** Specifies the minimum number of characters that the password may contain. Note: If the Default Authentication provider is configured in the realm, make sure that this number is consistent with the one configured for that provider. [More Info...](#)
 - Maximum Password Length:** Specifies the maximum number of characters that the password may contain. To be accepted, the password may not contain a greater number of characters than the value specified. Specifying 0 results in no restriction on password length. [More Info...](#)
- Character Policies:**
 - Maximum Instances of Any Character:** Specifies the maximum number of times any one character may appear in the password. [More Info...](#)
 - Maximum Consecutive Characters:** Specifies the maximum number of times that a character may appear consecutively in the password. [More Info...](#)
 - Minimum Number of Alphabetic Characters:** Specifies the minimum number of alphabetic characters that a password must contain. [More Info...](#)
 - Minimum Number of Numeric Characters:** Specifies the minimum number of numeric characters that must appear in the password. [More Info...](#)
 - Minimum Number of Lower Case Characters:** Specifies the minimum number of lowercase characters that a password must contain. [More Info...](#)
 - Minimum Number of Upper Case Characters:** Specifies the minimum number of uppercase characters that a password must contain. [More Info...](#)
 - Minimum Number of Non-Alphanumeric Characters:** Specifies the minimum number of non-alphanumeric characters (also known as special characters, such as %, *, #, or ;) that must appear in the password. [More Info...](#)
 - Minimum Number of Non-Alphabetic Characters:** Specifies the minimum number of numeric or special characters (such as %, *, #, or ;) that a password must contain. [More Info...](#)

A "Save" button is located at the bottom left of the configuration area.

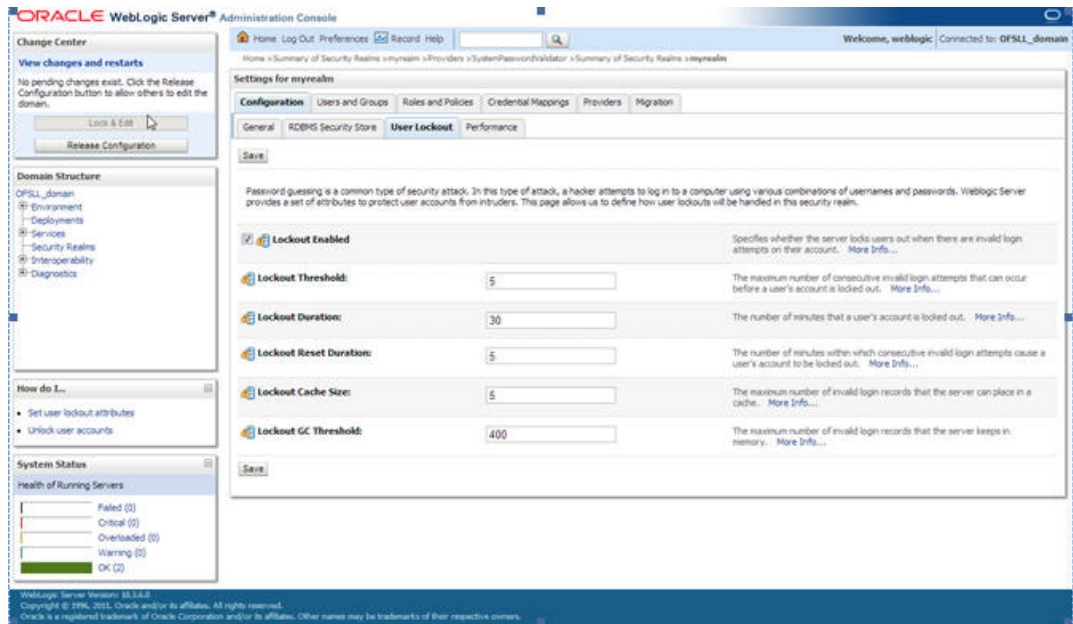
6. Configure the password policy as per the requirement. An example is provided below.



7. Click Save.

4.2 Configuring User Lockout Policy

1. To Change User lockout policy, browse to **Security Realms** → **myrealm** → **Configuration Tab** → **User Lockout Tab**. The following window is displayed

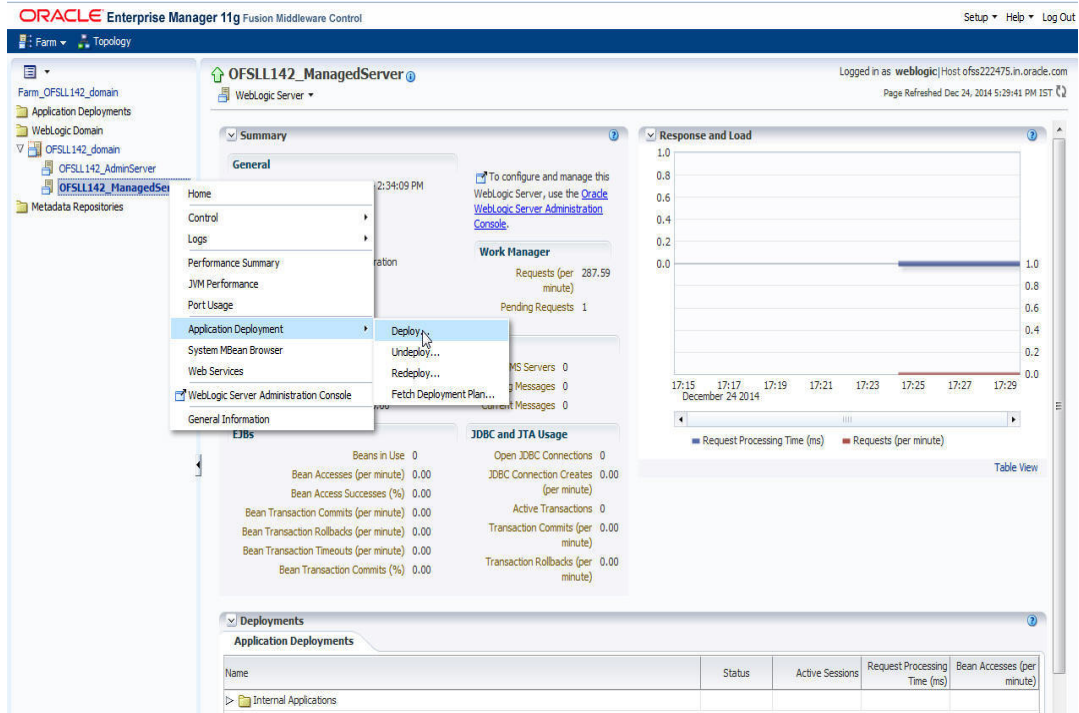


2. Configure the User Lockout details as per the requirement. An example is provided above.

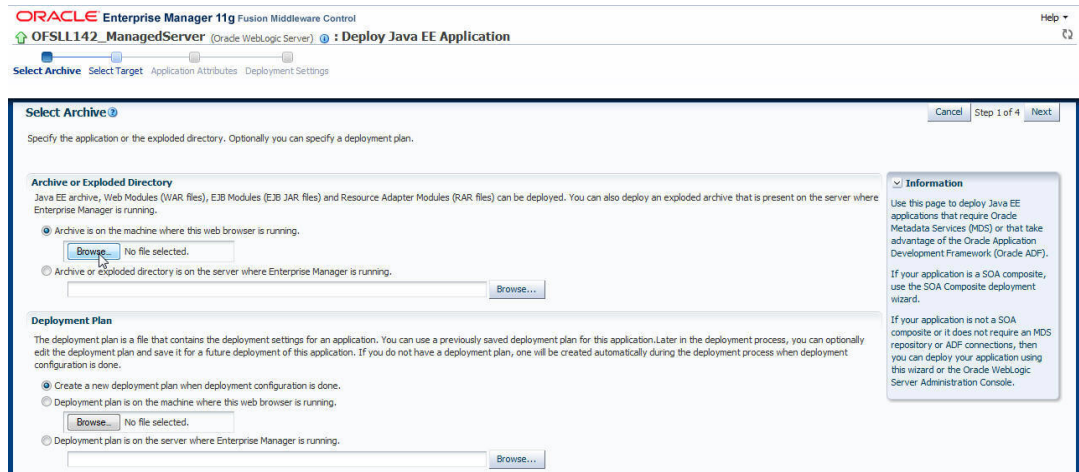
5. Deploying Application

5.1 Deploying Application

1. Login to the Oracle Enterprise Manager 11g console . (i.e. <http://hostname:port/em>)

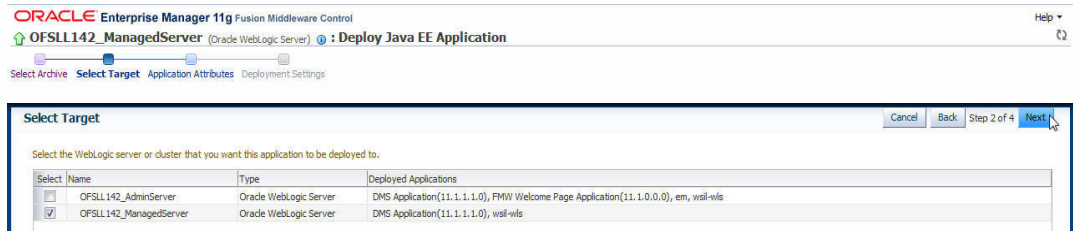


2. Right click on **OFSLL_ManagedServer** in left panel, select **Application Deployment** → **Deploy**. The following window is displayed.



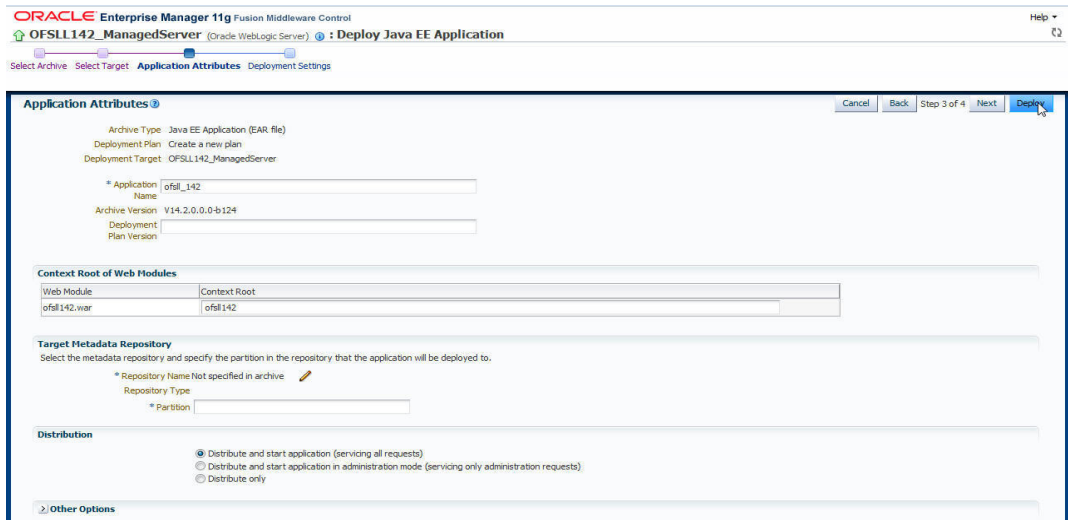
3. Click Choose File button and select OFSLL application archive file i.e. ofssl_142.ear.

4. Click **Next**. The following window is displayed

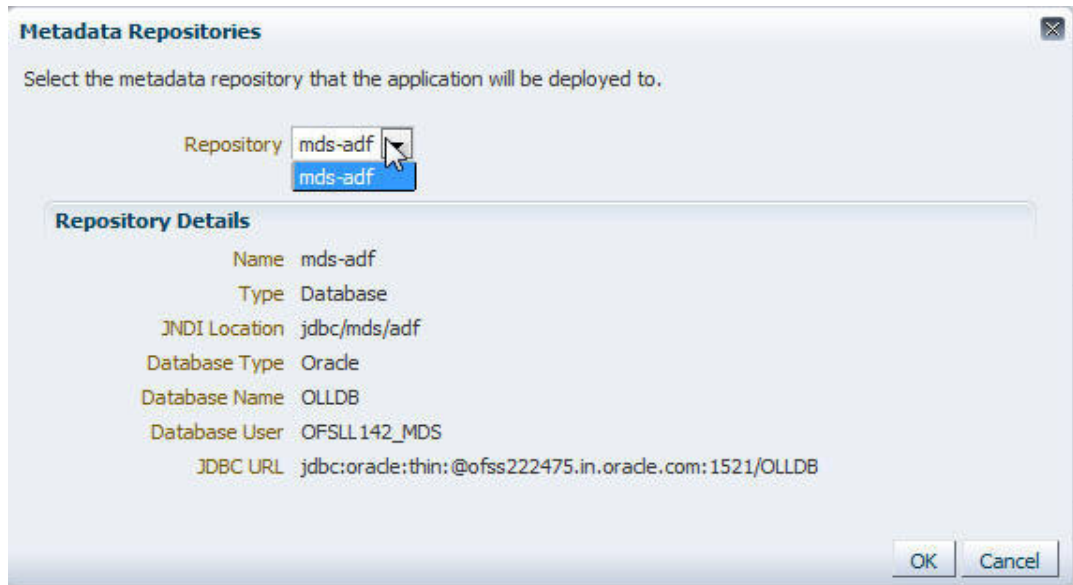


5. Check target server as per the requirement **OFSLL_ManagedServer** and click **Next**.

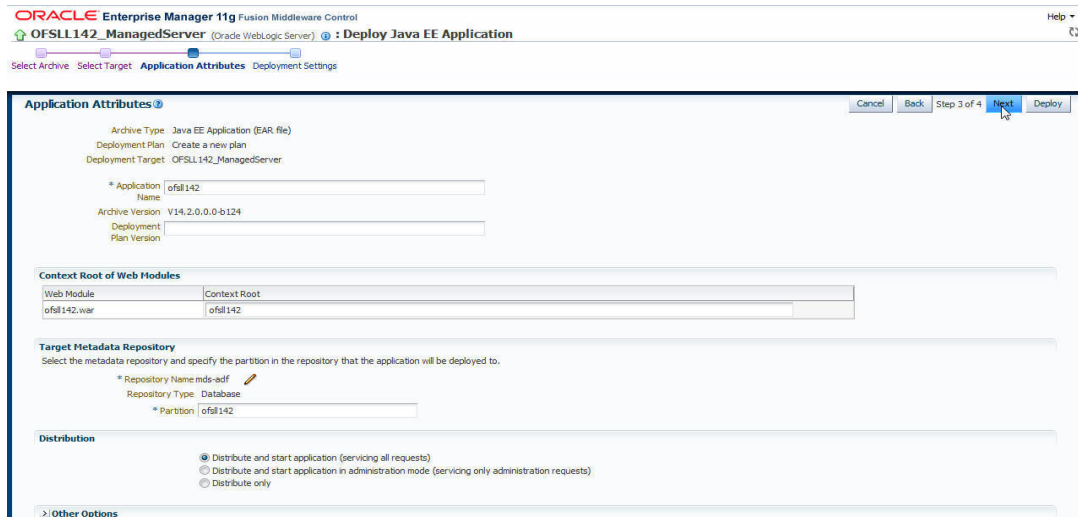
6. The following window is displayed.



7. Click  button to select Repository Name. The following window is displayed.



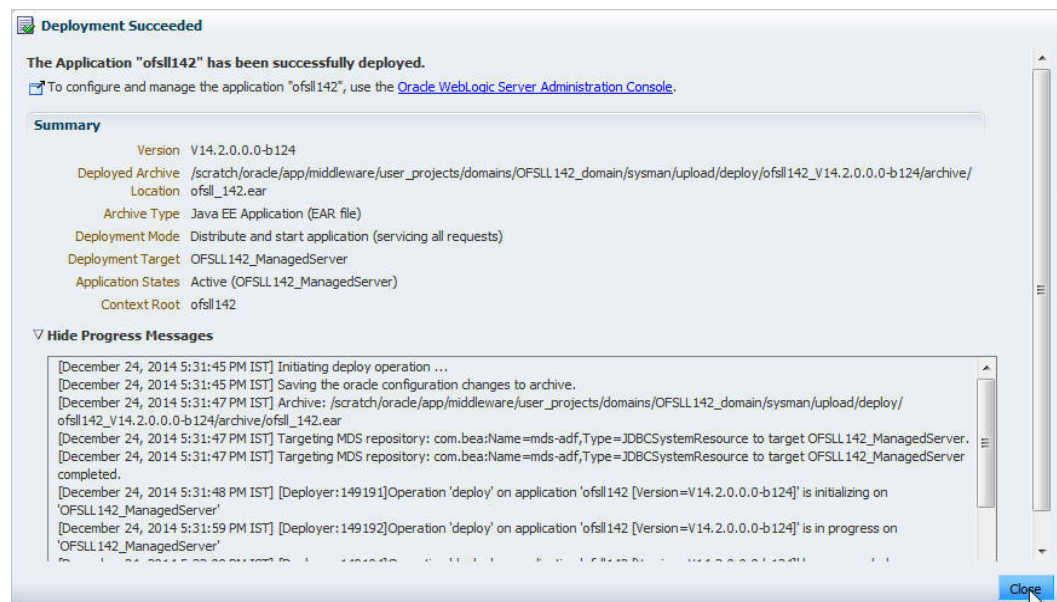
8. Select Repository as per requirement and click **OK**.



9. Enter Partition name as per the requirement and click **Next**.



10. Click **Deploy**. The following window is displayed



- Click Close once the message “Deploy operation completed” is displayed. The following window is displayed with Application deployment status

The screenshot displays the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The main window shows the 'Ofsll_ManagedServer' status, which is 'Running'. The 'Summary' tab provides detailed performance metrics across various categories:

- General:** Up Since: Feb 1, 2013 5:20:32 PM; State: Running; Health: OK; CPU Usage (%): 7.56; Heap Usage (MB): 242.85; Java Vendor: Sun Microsystems Inc.; Java Version: 1.6_0_26.
- Work Manager:** Requests (per minute): 167.48; Pending Requests: 1.
- Servlets and JSPs:** Active Sessions: 0; Request Processing Time (ms): 0; Requests (per minute): 0.00.
- JMS:** JMS Servers: 1; Pending Messages: 0; Current Messages: 0.
- EJBS and JDBC and JTA Usage:** Beans in Use: 0; Bean Accesses (per minute): 0.00; Bean Access Successes (%): 0.00; Bean Transaction Commits (per minute): 0.00; Bean Transaction Rollbacks (per minute): 0.00; Bean Transaction Timeouts (per minute): 0.00; Bean Transaction Commits (%): 0.00.

The 'Response and Load' graph shows a flat line at 0.0 on the y-axis (0.0 to 1.0) over time (17:39 to 17:51). The legend indicates 'Request Processing Time (ms)' and 'Requests (per minute)'. Below the graph is a 'Table View' button.

The 'Deployments' section shows a table of application deployments:

| Name | Status | Active Sessions | Request Processing Time (ms) | Bean Accesses (per minute) |
|---------------------------|--------|-----------------|------------------------------|----------------------------|
| Internal Applications | | | | |
| Ofsll_141(14.2.0.0.0-017) | 📈 | 0 | 0 | 0.00 |

6. Enabling SSL

The application is accessible only via https protocol; hence, after the deployment of the application, you need to enable SSL.

To enable SSL:

1. Login to console.
2. **\$Domain_Home** → **Servers** → **Manage Servers** → **Configuration** → **General**. The below screen is displayed.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled 'Settings for OFSLL_ManagedServer' and is under the 'Configuration' tab. The 'SSL' sub-tab is selected. The 'SSL Listen Port Enabled' checkbox is checked, and the 'SSL Listen Port' is set to 7503. Other settings include 'Listen Address', 'Listen Port' (7003), 'Client Cert Proxy Enabled' (unchecked), 'Java Compiler' (javac), and 'Diagnostic Volume' (Low). The left sidebar shows the 'Domain Structure' tree with 'OFSLL_domain' expanded to 'Services'.

3. Check the 'SSL Listen Port Enabled' check box.
4. Specify the port for 'SSL Listen Port'.

Note

It is recommended to disable http protocol.

7. Launching Application

Verifying Successful Application Deployment and Launching Application

Successful Application deployment can be verified by following:

- Making sure that the state is ACTIVE and health in OK in the Weblogic.
- Access and log into the application.

After you enable SSL you can launch the application via https:\\ protocol.

To launch application

1. Verify if the deployed OFSLL application is **Active**.

The screenshot shows the Oracle WebLogic Server Administration Console. The main area is titled "Summary of Deployments" and contains a table of installed applications. The table has columns for Name, State, Health, Type, and Deployment Order. The application "Ofsll_142" is listed with a state of "Active" and a health of "OK".

| Name | State | Health | Type | Deployment Order |
|--|--------|--------|------------------------|------------------|
| ofsl(1.1.1.2.0.0) | Active | | Library | 100 |
| Ofsll_142 (114.1.0.0.2-932) | Active | OK | Enterprise Application | 100 |
| ofsl-vof(1.5.0) | Active | | Library | 100 |
| ofsl-vuf(1.5.0) | Active | | Library | 100 |
| oracle.adf.configbeans(1.0.11.1.1.2.0) | Active | | Library | 100 |
| oracle.adf.desktopintegration(1.0.11.1.1.2.0) | Active | | Library | 100 |
| oracle.adf.desktopintegration.mode(1.0.11.1.1.2.0) | Active | | Library | 100 |
| oracle.adf.management(1.0.11.1.1.2.0) | Active | | Library | 100 |
| oracle.bi.adf.model.sbc(1.0.11.1.1.2.0) | Active | | Library | 100 |
| oracle.bi.adf.view.sbc(1.0.11.1.1.2.0) | Active | | Library | 100 |

2. The URL of the OFSLL application will be

`https://<hostname>:<Port>/<ContextName>/faces/pages/OfsllSignIn.jspx`

(Example: `https://localhost:7003/ofsl142/faces/pages/OfsllSignIn.jspx`)

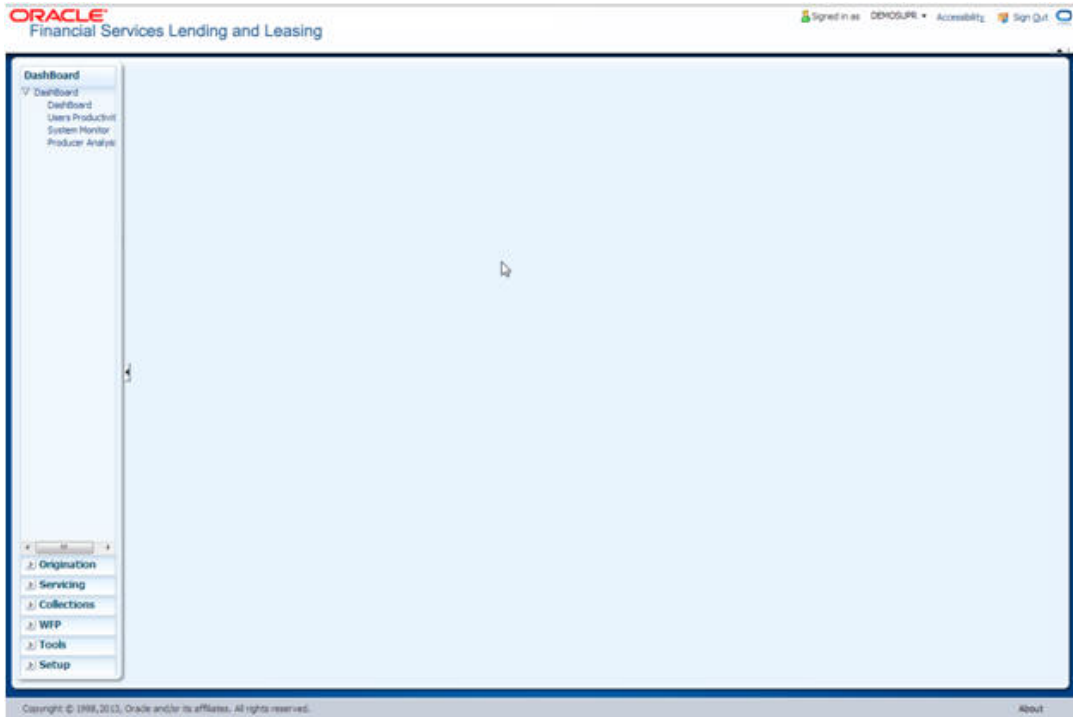
The screenshot shows the Oracle Financial Services Lending and Leasing application's Sign In page. The page has a blue header with the Oracle logo and the text "Financial Services Lending and Leasing". The main content area is white and contains a sign-in form with the following fields:

- Sign In to Oracle Financial Services Lending and Leasing.
- * User ID
- * Password
- Sign In button

3. Login with the user credentials that was created in Users Creation.



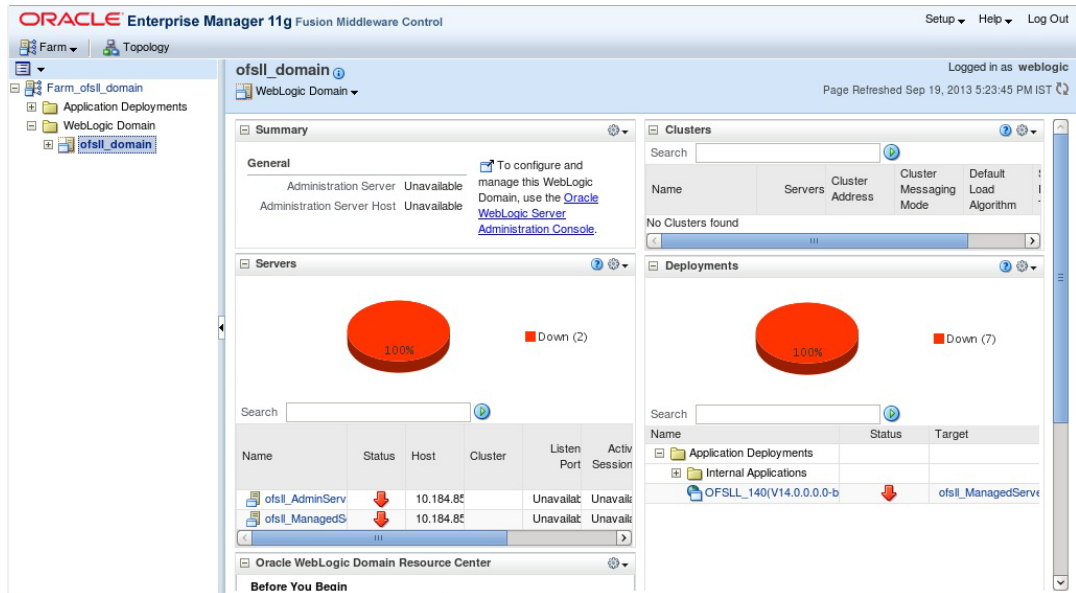
4. After successful login, the following screen is displayed



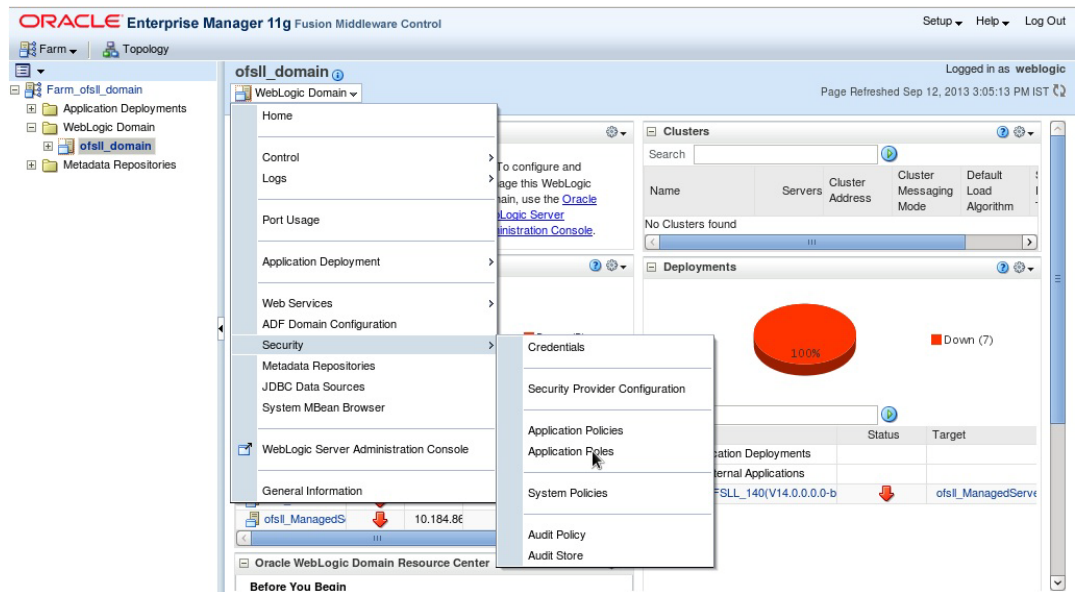
8. Mapping Enterprise Group with Application Role

Follow the below steps to add an user to the group

1. Login to Oracle Enterprise Manager 11g console (<http://hostname:port/em>).
2. Click **WebLogic Domain** → **Security** → **Application Roles** on the right panel.



3. On clicking **Application Roles**, The following screen is displayed:



4. Select **Application Roles** from the drop-down menu.
5. Click the arrow head button. Details of the existing Roles are displayed below.

- Select the **Role Name**. Membership details of the selected Role Name are displayed under **Membership for "role_name"**.

Application Roles

Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.

To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Search

Select an application and enter search keyword for role name to search for roles defined by this application. Use application stripe to search if application uses a stripe that is different from application name.

Application Stripe: OFSLL_140#V14.0.0.0-b265

Role Name: Starts With

Create... Create Like... Edit... Delete...

| Role Name | Display Name | Description |
|------------|--------------|-------------|
| OFSLL_USER | OFSLL USER | |

Membership for OFSLL_USER

| Principal | Display Name | Type | Description |
|-----------|--------------|-------|-------------|
| DEMOSUPR | | User | |
| FLL_USER | | Group | |

- Click **Edit**. The following window is displayed.

Edit Application Grant [OK] [Cancel]

Application Policies > Edit Application Grant

Application Stripe: OFSLL_140#V14.0.0.0-b265

Grantee

Select the grantees (user, group or application role) you want to add to the policy.

+ Add - Delete...

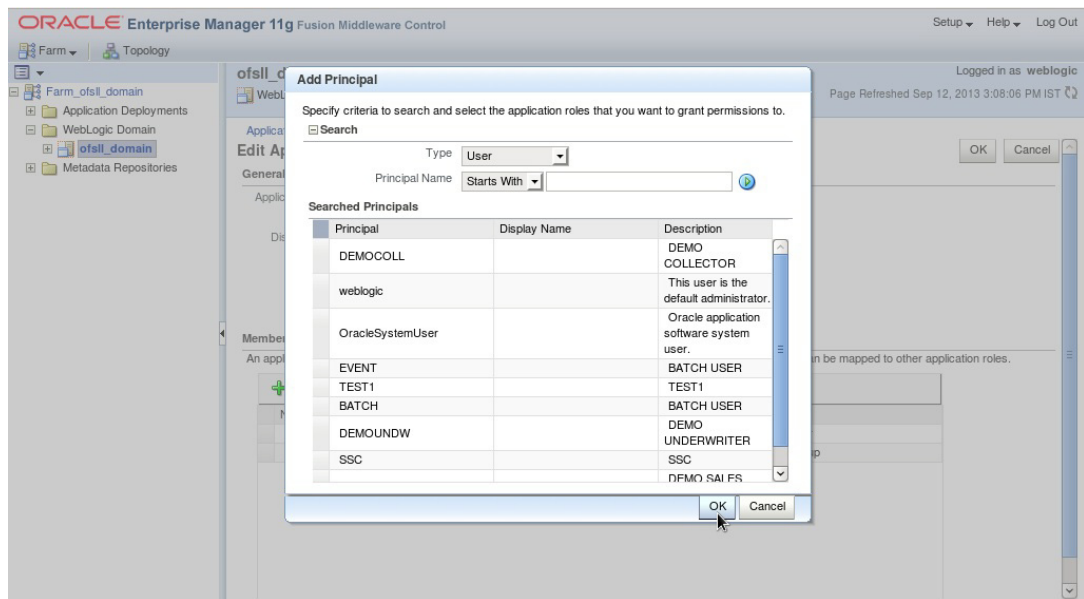
| Name | Display Name | Type | Description |
|----------------|----------------|----------------|-------------|
| anonymous-role | Anonymous Role | Anonymous Role | |

Permissions

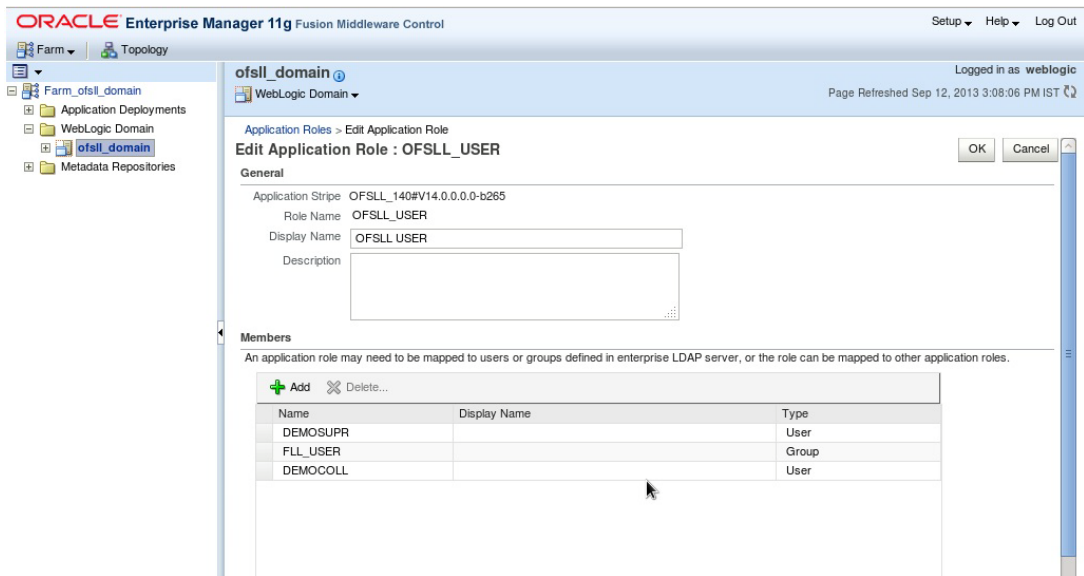
+ Add Edit... Delete...

| Permission Class | Resource Name | Resource Type | Permission Actions |
|---|----------------------------------|---------------|--------------------|
| oracle.adf.share.security.authorization.RegionPermissions | oracle.ofssl.view.pagedefs.pages | | view |
| oracle.adf.share.security.authorization.RegionPermissions | oracle.ofssl.view.pagedefs.pages | | view |
| oracle.adf.share.security.authorization.RegionPermissions | oracle.ofssl.view.pagedefs.templ | | view |
| oracle.adf.share.security.authorization.RegionPermissions | oracle.ofssl.view.pagedefs.pages | | view |

8. Click **Add**. Select type as **Group**. Click on the arrow head button.



9. Select the Principal "OFSLL_USER" to add and click **OK**. The following window is displayed.



10. The selected Principal is listed under **Members**.

Click OK. The following window is displayed with the confirmation message as “The Application role of ‘group_name’ has been updated”.

ORACLE Enterprise Manager 11g Fusion Middleware Control

Setup Help Log Out

Farm Topology

ofssl_domain
WebLogic Domain

Logged in as weblogic
Page Refreshed Sep 12, 2013 3:10:55 PM IST

Information
An application role OFSSL_USER has been updated.

Application Roles
Application roles are the roles used by security aware applications that are specific to the application. These roles are seeded by applications in single global policy store when the applications are registered. These are also application roles that are created in the context of end users accessing the application.
To manage users and groups in the WebLogic Domain, use the [Oracle WebLogic Server Security Provider](#).

Policy Store Provider

Search
Select an application and enter search keyword for role name to search for roles defined by this application. Use application stripe to search if application uses a stripe that is different from application name.

Application Stripe: OFSSL_140#V14.0.0.0-b265
Role Name: Starts With

Create... Create Like... Edit... Delete...

| Role Name | Display Name | Description |
|------------|--------------|-------------|
| OFSSL_USER | OFSSL USER | |

9. Configuring Oracle BI Publisher for Application

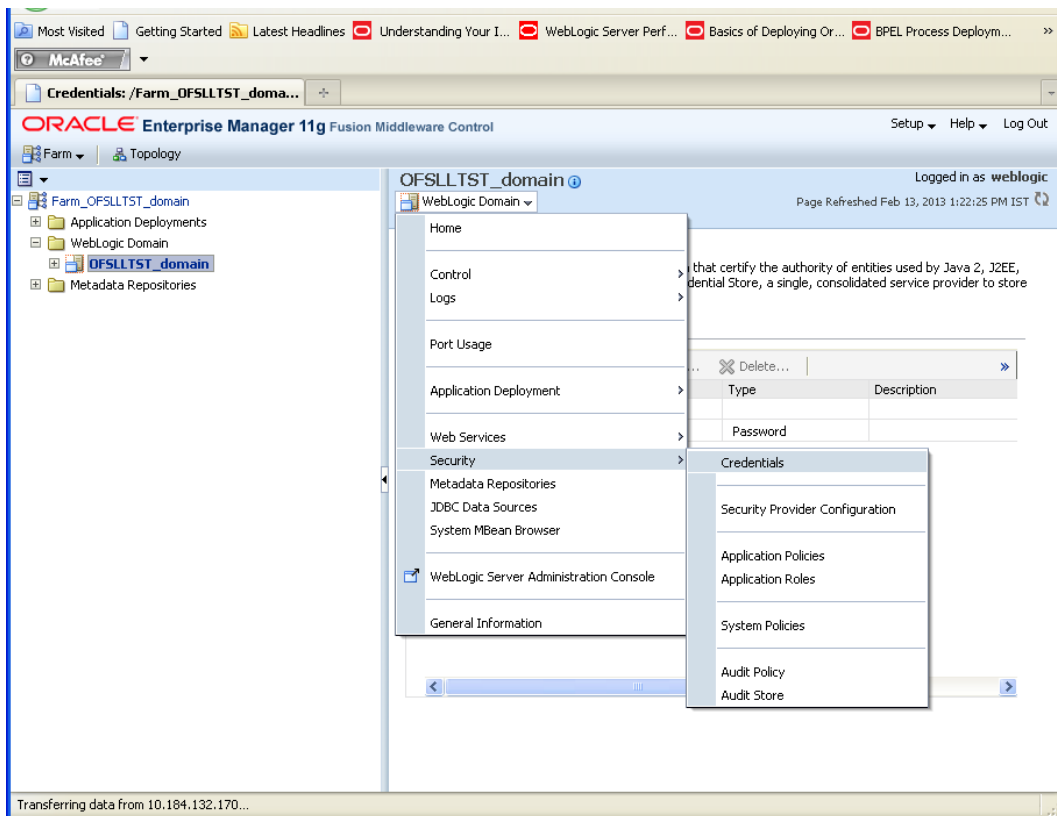
1. Copy the OfsslCommonCSF.jar from /WEB-INF/lib available in the staging area to \$DOMAIN_HOME/lib
2. Update the setDomainEnv.sh file (\$MW_HOME/user_projects/domains/mydomain/bin directory) by appending the above jar file path –

```
EXTRA_JAVA_PROPERTIES="..... ${EXTRA_JAVA_PROPERTIES}  
-Dofssl.csf.path=${DOMAIN_HOME}"
```

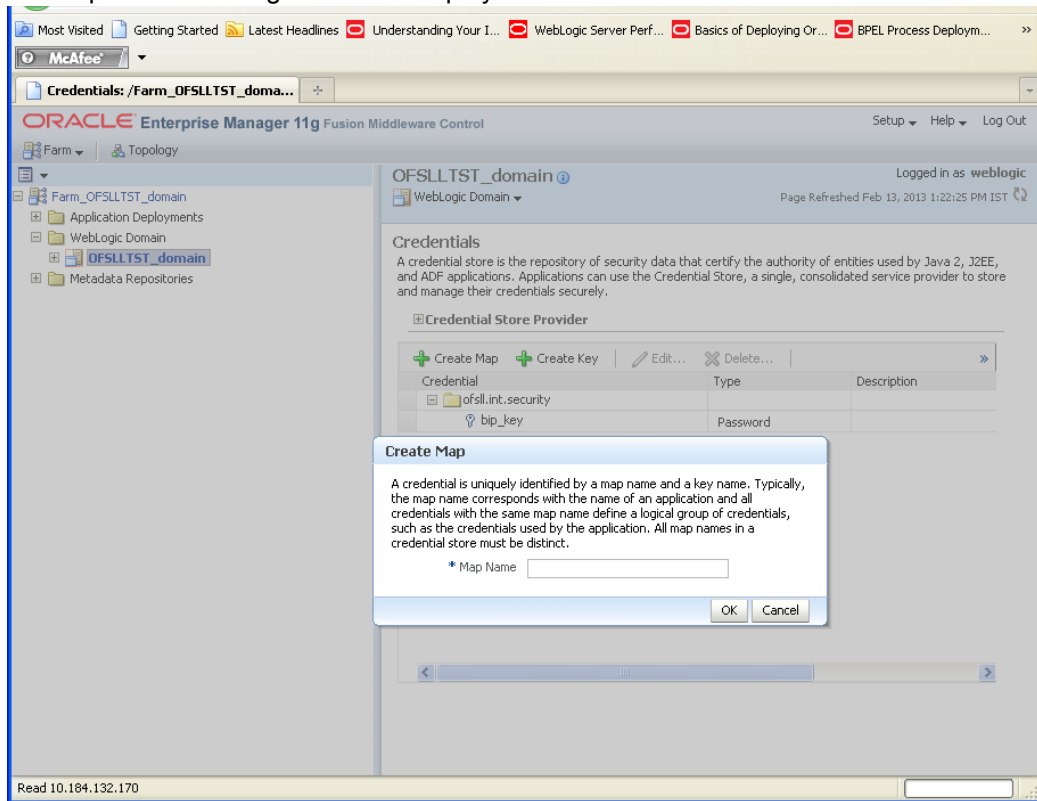
3. Configure Security via EMconsole

Note

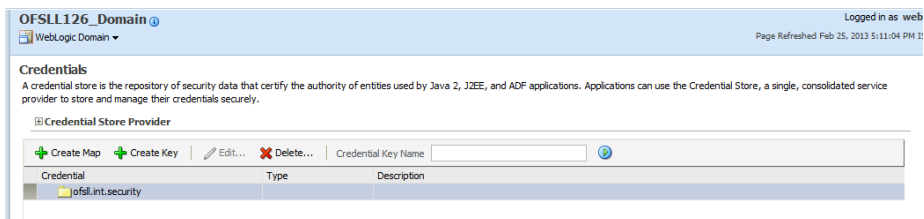
It is assumed that BI Publisher is installed and configured. Refer BI Publisher Guide for further details.



- Click WebLogic Domain on the right panel. Select Security -> Credentials. Click 'Create Map'. The following window is displayed.

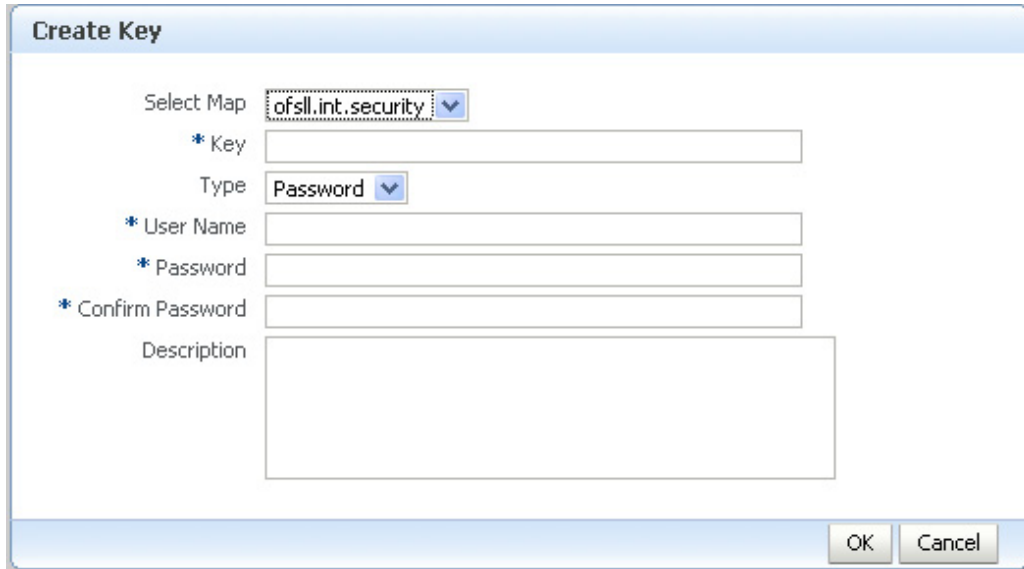


- Enter the Map Name: ofssl.int.security
- Click OK. The following window is displayed.



- Click **Create Key** Button.

The following window is displayed.



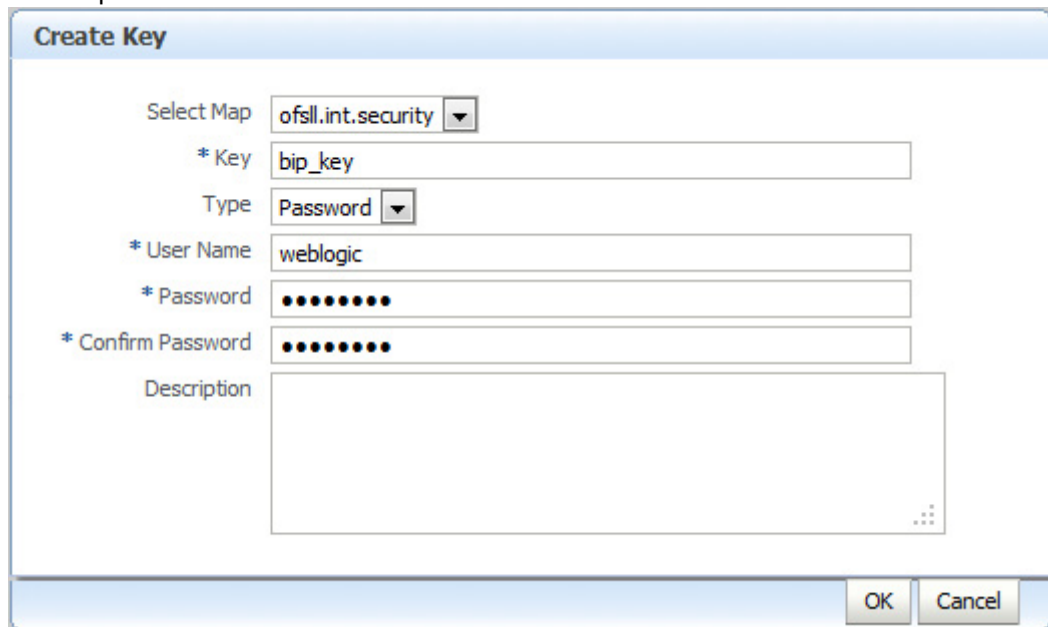
The 'Create Key' dialog box is shown with the following fields:

- Select Map: ofssl.int.security
- * Key: (empty text box)
- Type: Password
- * User Name: (empty text box)
- * Password: (empty text box)
- * Confirm Password: (empty text box)
- Description: (empty text area)

Buttons: OK, Cancel

8. Enter the details as per your requirement.

9. And provide User Name and Password of BI Publisher console.

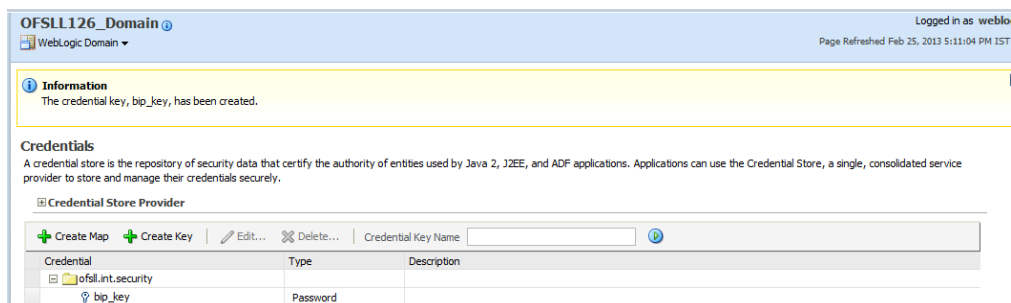


The 'Create Key' dialog box is shown with the following filled details:

- Select Map: ofssl.int.security
- * Key: bip_key
- Type: Password
- * User Name: weblogic
- * Password: (masked with dots)
- * Confirm Password: (masked with dots)
- Description: (empty text area)

Buttons: OK, Cancel

10. Click **OK**. The following window is displayed.

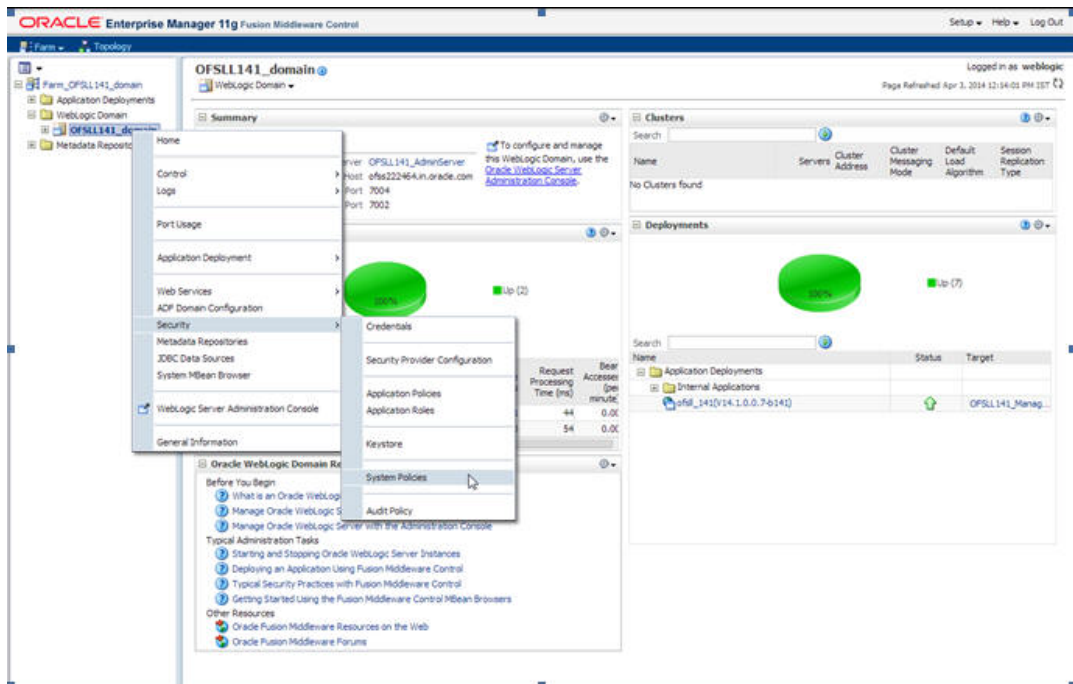


The screenshot shows the WebLogic console interface with the following elements:

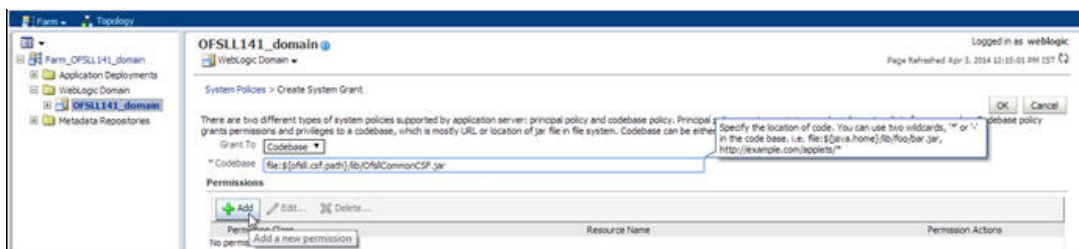
- Page Title: OFSSL126_Domain
- Page Subtitle: WebLogic Domain
- Page Info: Logged in as weblo, Page Refreshed Feb 25, 2013 5:11:04 PM IST
- Information Message: The credential key, bip_key, has been created.
- Section: Credentials
- Text: A credential store is the repository of security data that certify the authority of entities used by Java 2, J2EE, and ADF applications. Applications can use the Credential Store, a single, consolidated service provider to store and manage their credentials securely.
- Section: Credential Store Provider
- Buttons: Create Map, Create Key, Edit..., Delete..., Credential Key Name
- Table:

| Credential | Type | Description |
|--------------------|----------|-------------|
| ofssl.int.security | | |
| bip_key | Password | |

11. On the left panel, right click on the domain OFSLL141_domain > Security > System Policies. The following window is displayed. Click Create.



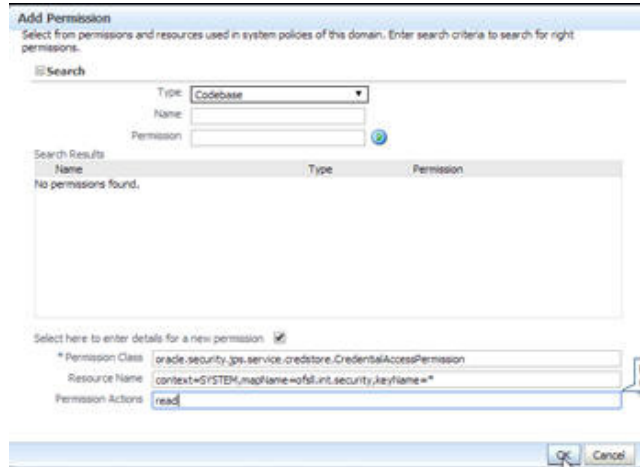
12. The following window is displayed. Enter the codebase as "file:\${ofssl.csf.path}/lib/OFSllCommonCSF.jar" and click Add.



13. The following window is displayed. Select the checkbox 'Select here to enter details for a new permission' and enter the following details as the first permission class.

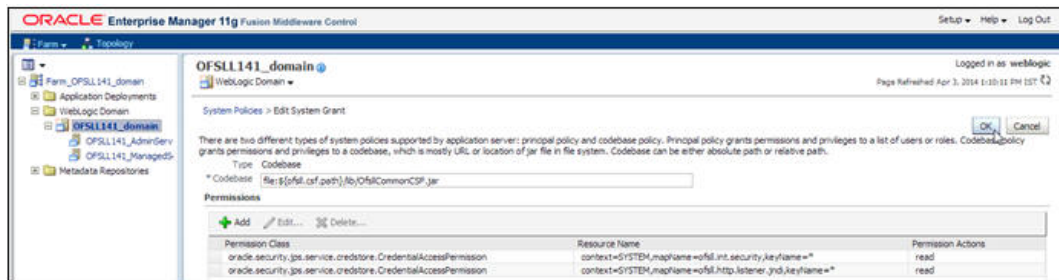
- Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
- Resource Name: context=SYSTEM,mapName=ofssl.int.security,keyName=*

- Permission Actions: read

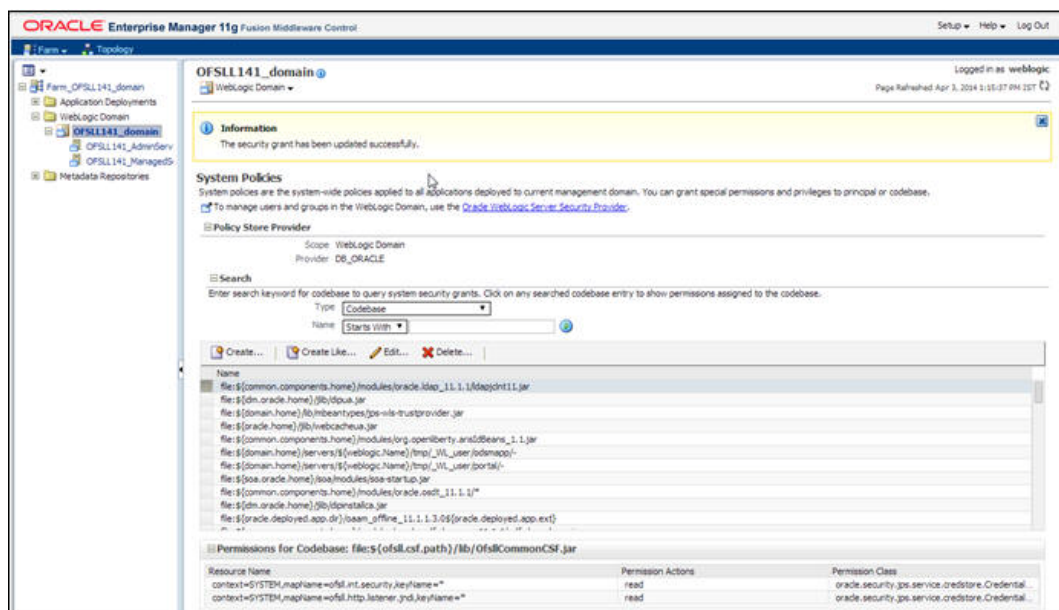


Configuring JNDI Name for http Listener

1. Similarly, click Add to add the second permission class. Select the check box 'Select here to enter details for a new permission' and enter the following details as the second permission class.
 - Permission Class: oracle.security.jps.service.credstore.CredentialAccessPermission
 - Resource Name: context=SYSTEM,mapName=ofssl.http.listener.jndi,keyName=*
 - Permission Actions: read
2. Click OK. The following window is displayed.

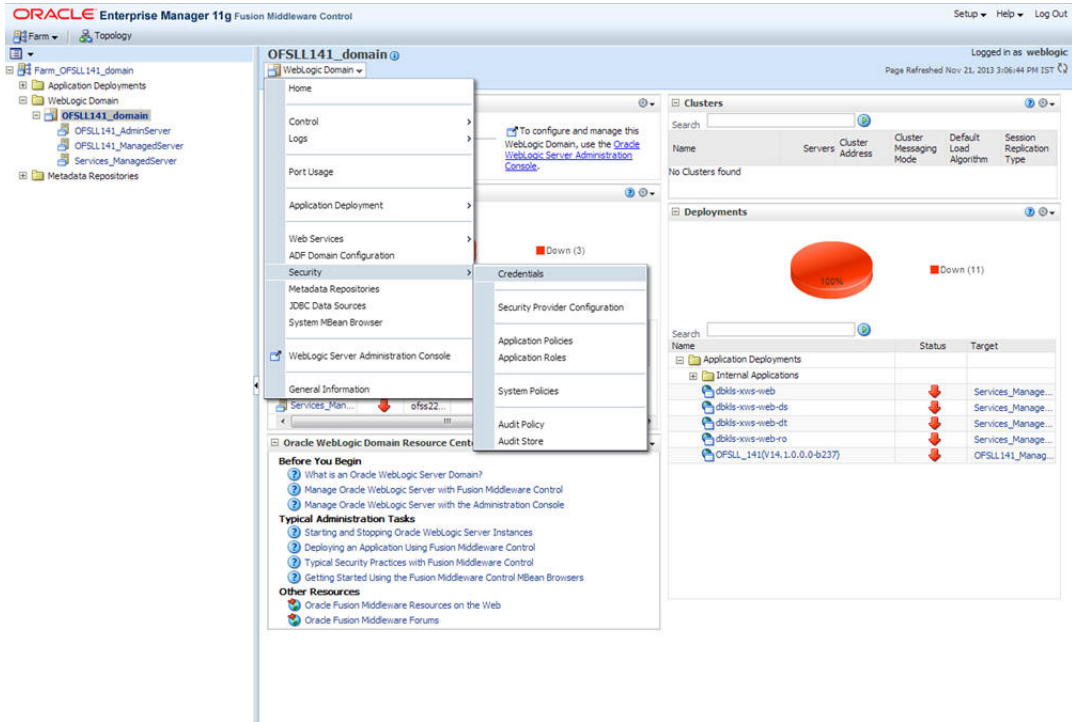


3. Click OK. The following window is displayed.

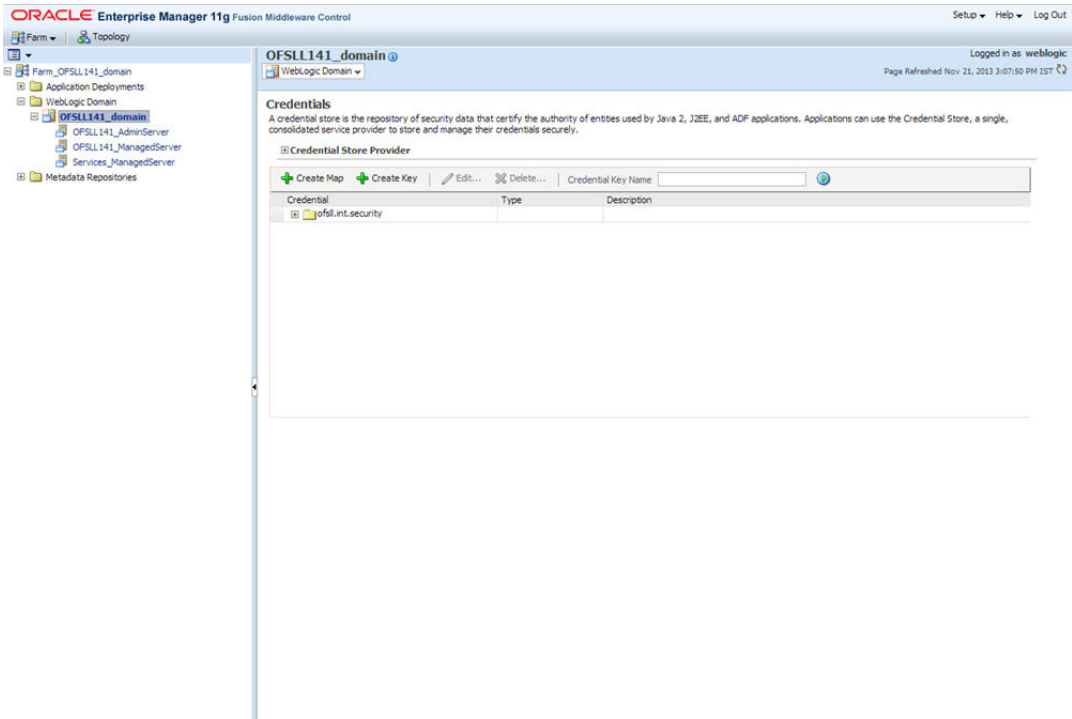


10. Configuring JNDI name for HTTP Listener

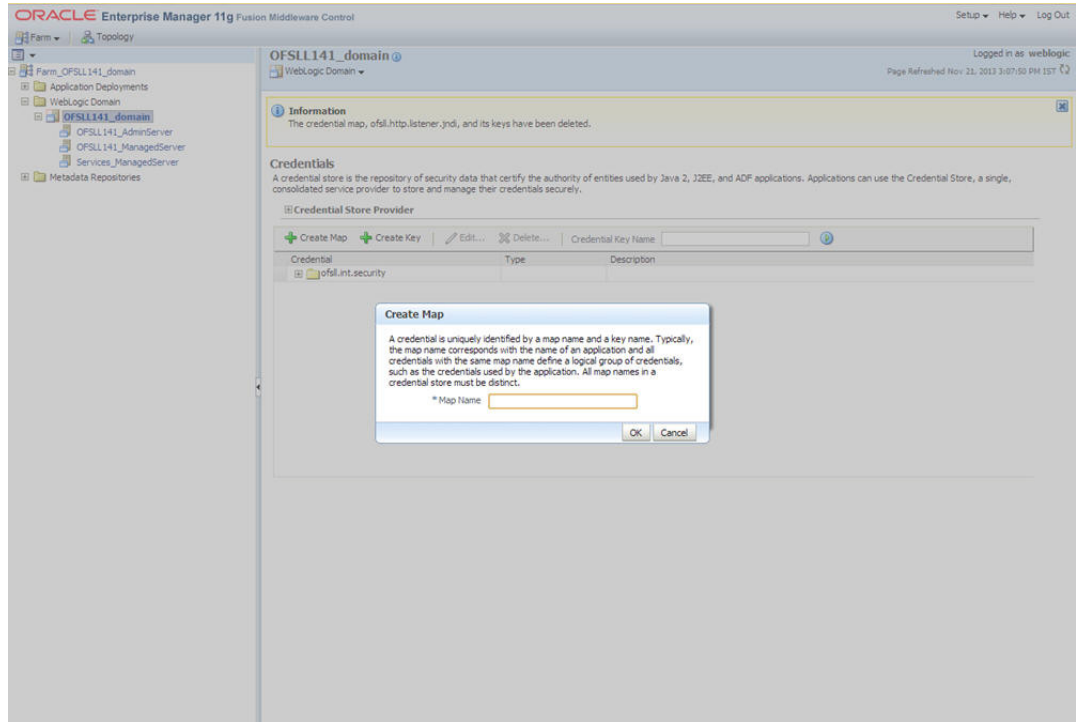
1. Click **WebLogic Domain** on the right panel. Select **Security** → **Credentials**.



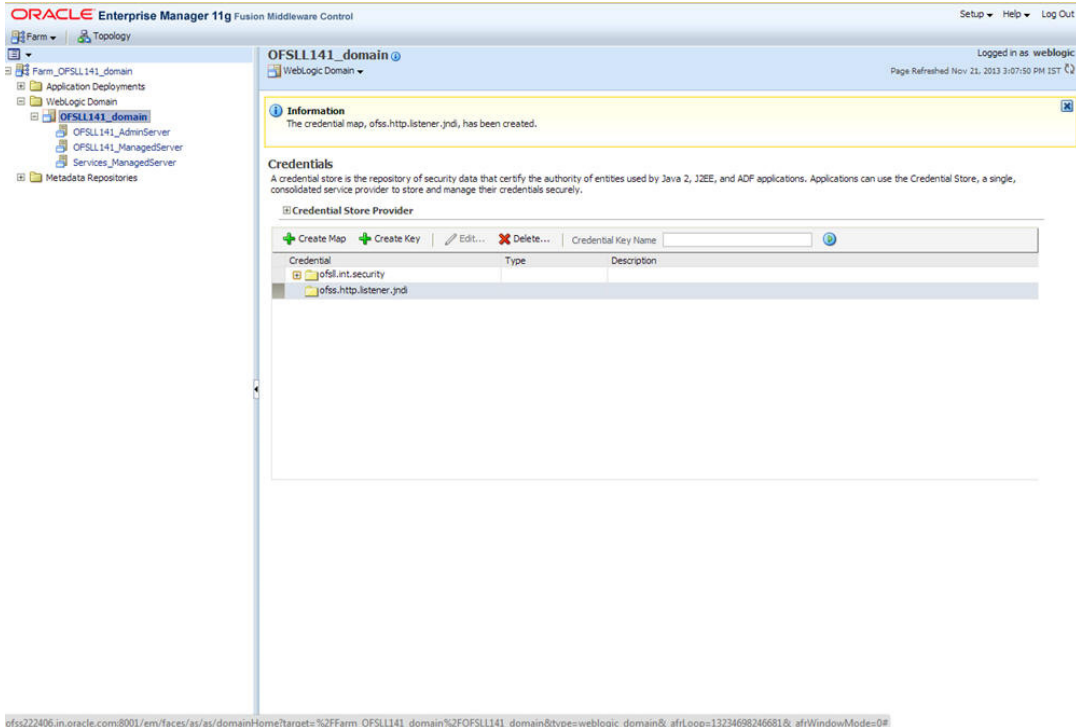
2. On clicking **Credentials** the following window is displayed.



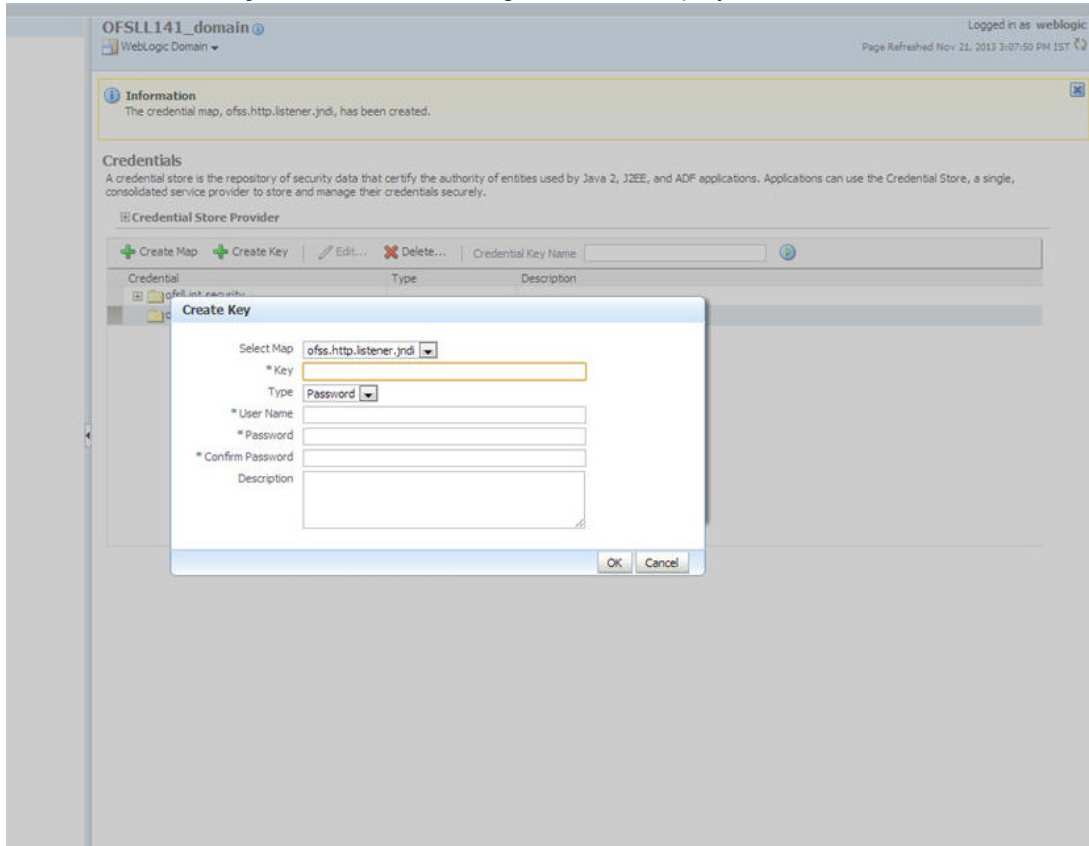
3. Click on **Create Map**. The following window is displayed.



4. Enter Map name as '**ofssl.http.listener.jndi**'.
5. Click **OK**. The following window is displayed.



6. Click **Create Key** Button. The following window is displayed.

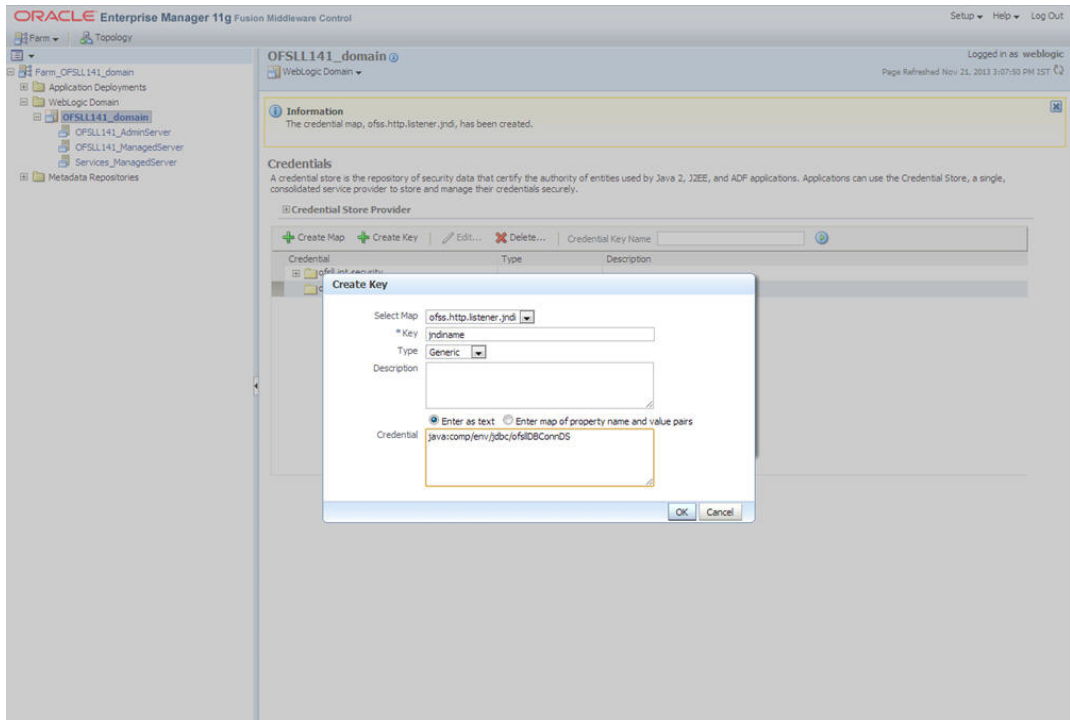


7. Enter the details as per your requirement.

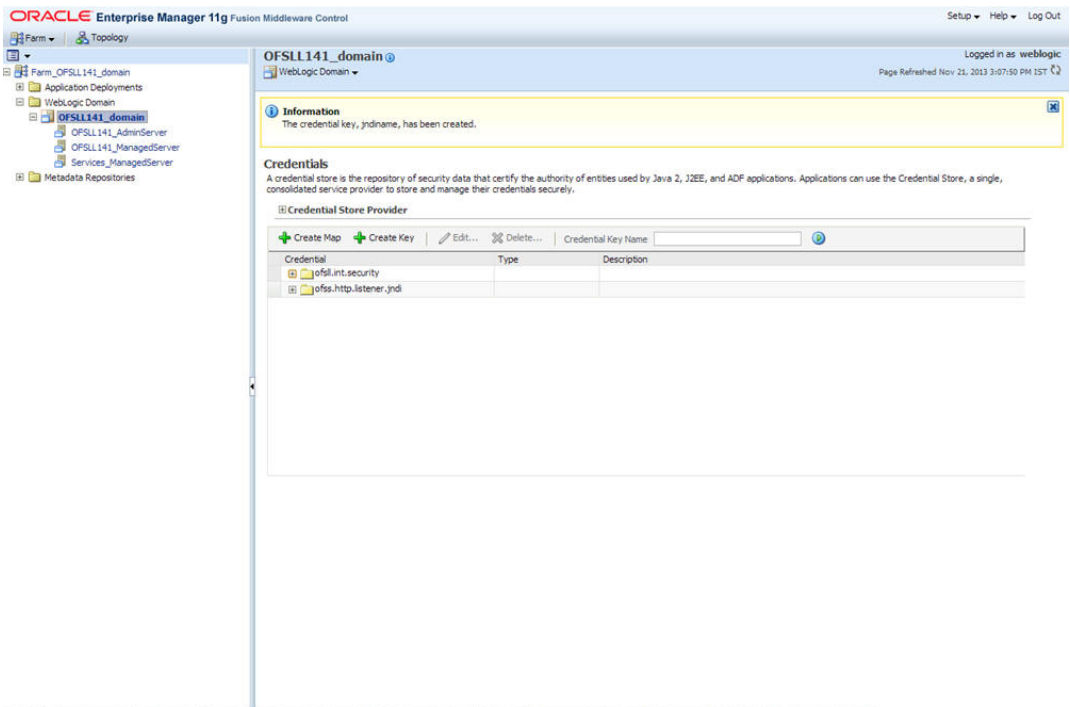
Key: jndiname

Credential: java:comp/env/jdbc/ofslIDBConnDS

Type:Generic



8. Click **OK**. The following window is displayed.

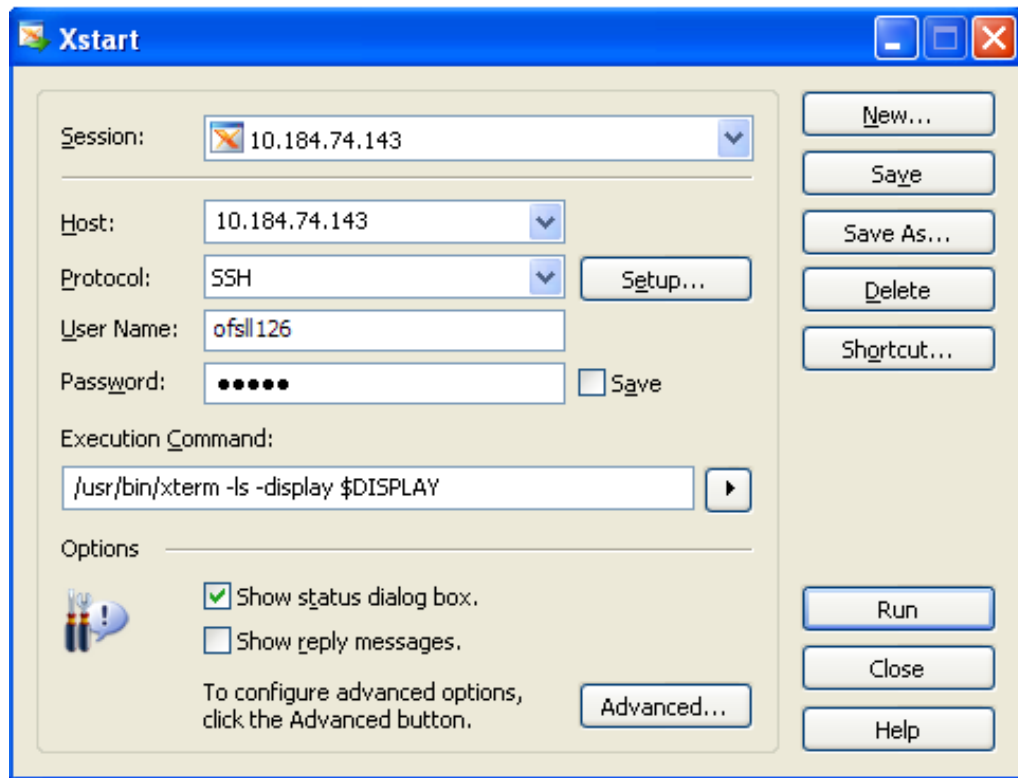


ofss222406.in.oracle.com:8001/em/faces/as/as/domainHome?target=%2Ffarm_OFSSL141_domain%2Fofssl141_domain&type=weblogic.domain&_afLoop=13234698246681&_afWindowMode=0#

A. Appendix

A.1 XManager Usage

To run any installer on remote non window machine user should have XManager software.



Give the following details

Session name:Give session name.

Host name:Give the UNIX machine address.

Protocol:This value depends on the operating system.

For Example E.g.:

Oracle Enterprise Linux: SSH

IBM AIX: TELNET

Solaris: SSH

UNIX: SSH

User Name:Give the UNIX user name.

Password:Give the password.

Execution Command: This value depends on the operating system.

E.g.:

Oracle Enterprise Linux: /usr/bin/xterm -ls -display \$DISPLAY

IBM AIX: /usr/dt/bin/dtterm -ls -display \$DISPLAY

Solaris: /usr/openwin/bin/xterm -ls -display \$DISPLAY

UNIX: /usr/bin/X11/xterm -ls -display \$DISPLAY