

Application Installation Guide

Oracle Financial Services Lending and Leasing

Release 14.1.0.0.0

Part No. E51268-01

November 2013

Application Installation Guide
November 2013
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	3-14
3.5 Creating Data Source	3-16
3.6 Creating SQL Authentication Provider	3-20
3.7 Creating User Groups and Users	3-25
3.7.1 Creating Users	3-25
3.7.2 Creating User Groups	3-26
3.7.3 Assigning Users to Groups	3-27
3.7.4 Resetting password via weblogic console	3-27
3.8 Implementing JMX Policy for Change Password	3-29
3.9 Migrating Policy from File to Database	3-33
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
5.2 Verifying Successful Application Deployment	5-4
6. Enabling SSL	6-1
7. Launching Application	7-1
8. Mapping of 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	11-1
11.1 XManager Usage	11-1

1. Preface

For recommendations on security configuration, refer Security Configuration Guide.

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.

It is assumed that anyone installing Oracle Financial Services Lending and Leasing will have a thorough knowledge and understanding of Oracle Weblogic Server 10.3.5/10.3.6, Oracle BI Publisher 11.1.1.6.

Application installation is a seven step process.

1. [Installing Software](#)
2. [Creating Domains, Repositories, Data Sources](#)
3. [Configuring Policies](#)
4. [Configuring Oracle BI Publisher for Application](#)
5. [Deploying Application](#)
6. [Enabling SSL](#)
7. [Launching Application](#)

1.1 Prerequisites

The following software are required to install Oracle Financial Services Lending and Leasing application.

1. Sun JDK Version 1.6 update 31 or above <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
OR
Oracle JRockit JDK Version 1.6 update 22 or above <http://www.oracle.com/technetwork/middleware/jrockit/downloads/index.html>
2. Oracle Repository Creation Utility (RCU) Version 11.1.1.6.0. Download RCU for the respective platform from the "Required Additional Software" section of <http://www.oracle.com/technetwork/middleware/bi-publisher/downloads/index.html>
3. Oracle WebLogic Server 11gR1 Version 10.3.5/10.3.6
<http://www.oracle.com/technetwork/middleware/weblogic/downloads/wls-main-097127.html>
Navigate to Oracle WebLogic Server 11gR1 (10.3.5/10.3.6) + 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.
4. 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**

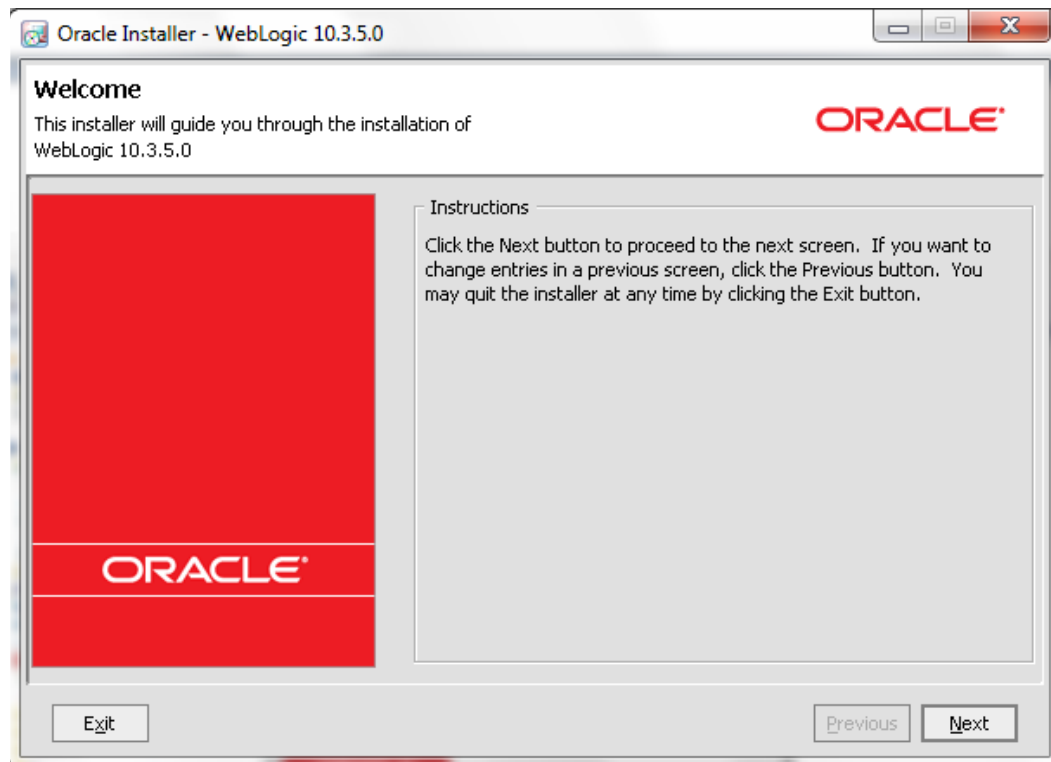
Term	Refers to
Application	Oracle Financial Services Lending and Leasing

2. Installing Software

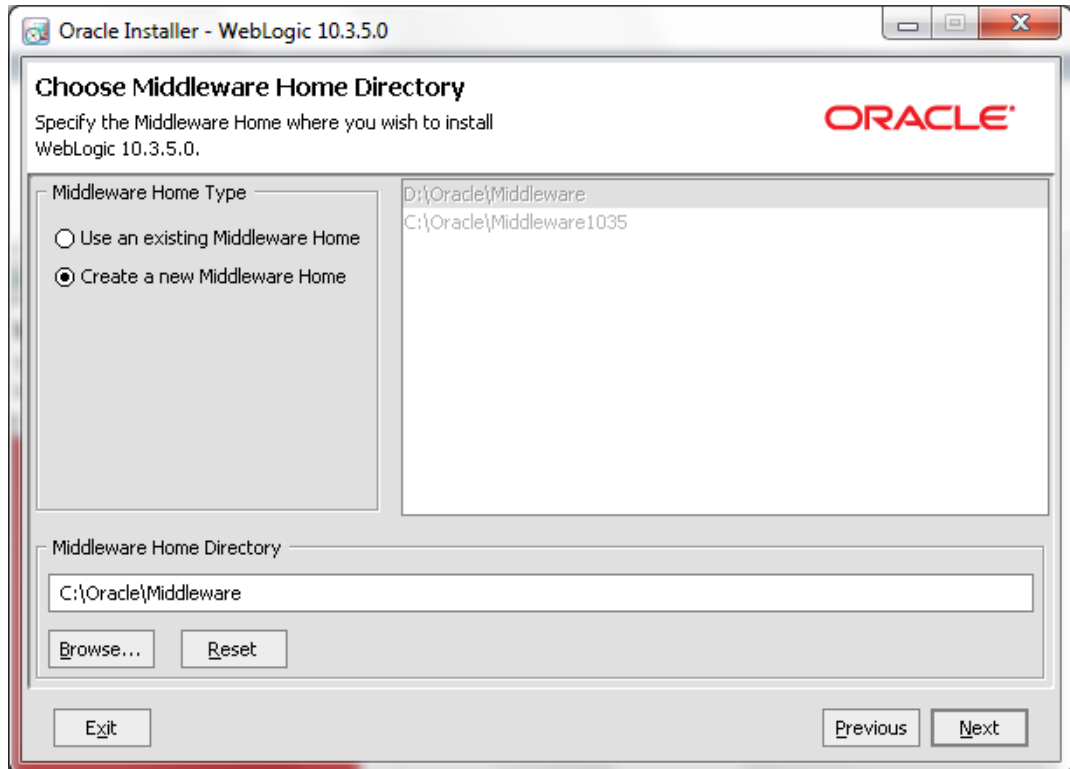
2.1 Installing Oracle WebLogic Server 11g

To install using generic Weblogic installer -

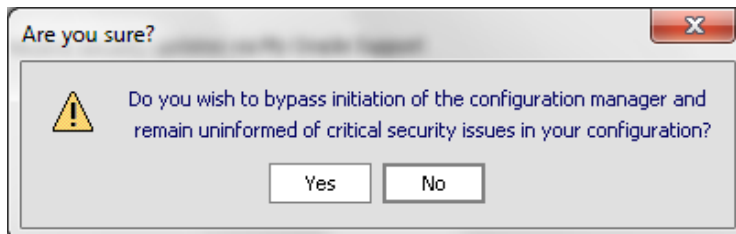
1. Run the command → `java -jar wls1035_generic.jar / java -jar wls1036_generic.jar`
2. Welcome screen is displayed as shown below.



3. Click **Next** to continue.



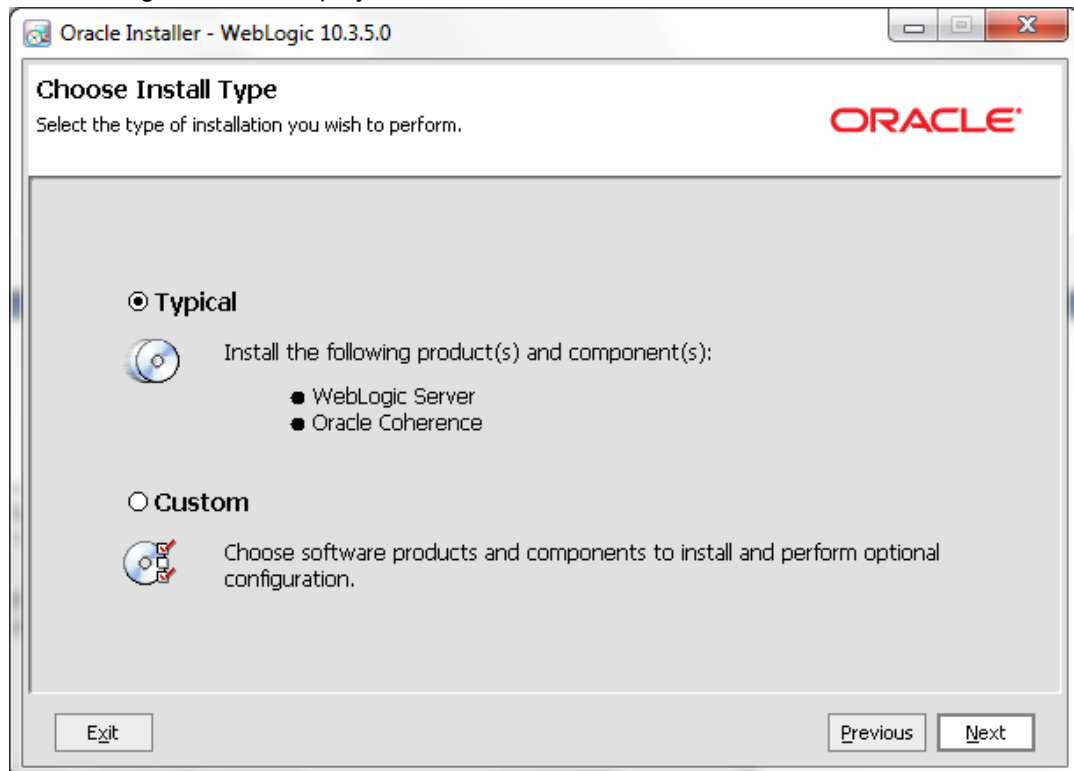
4. Select **Create a new Middleware Home** as **Middleware Home Type**
5. Specify the path for **Middleware Home Directory**, and then click **Next**.
6. Confirmation window is displayed as shown below.



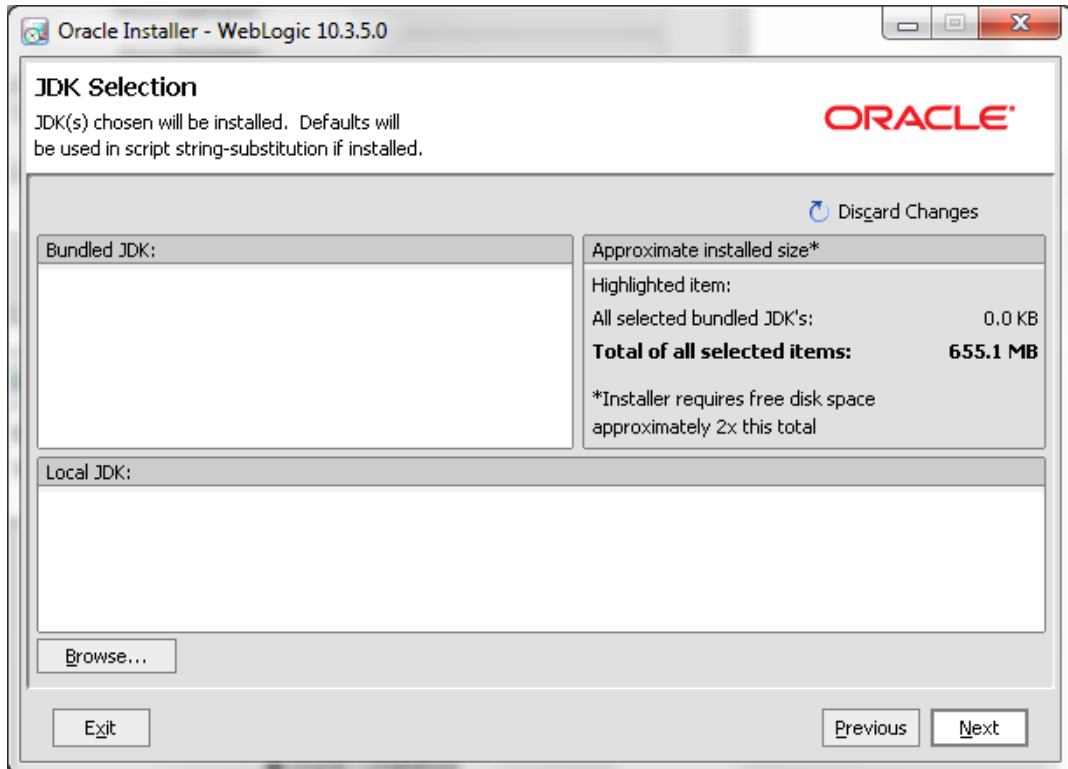
7. Click **Yes** to continue.



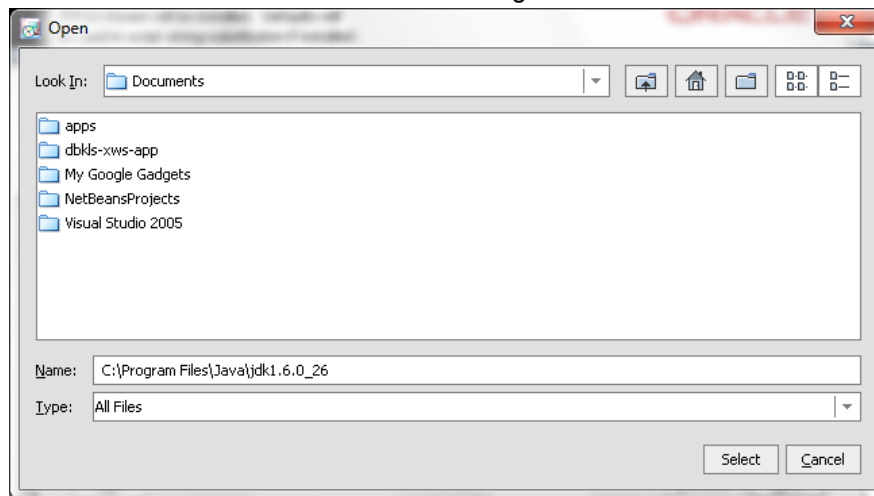
8. Check the check box as shown in the above screen shot and click **Continue**. The following window is displayed.



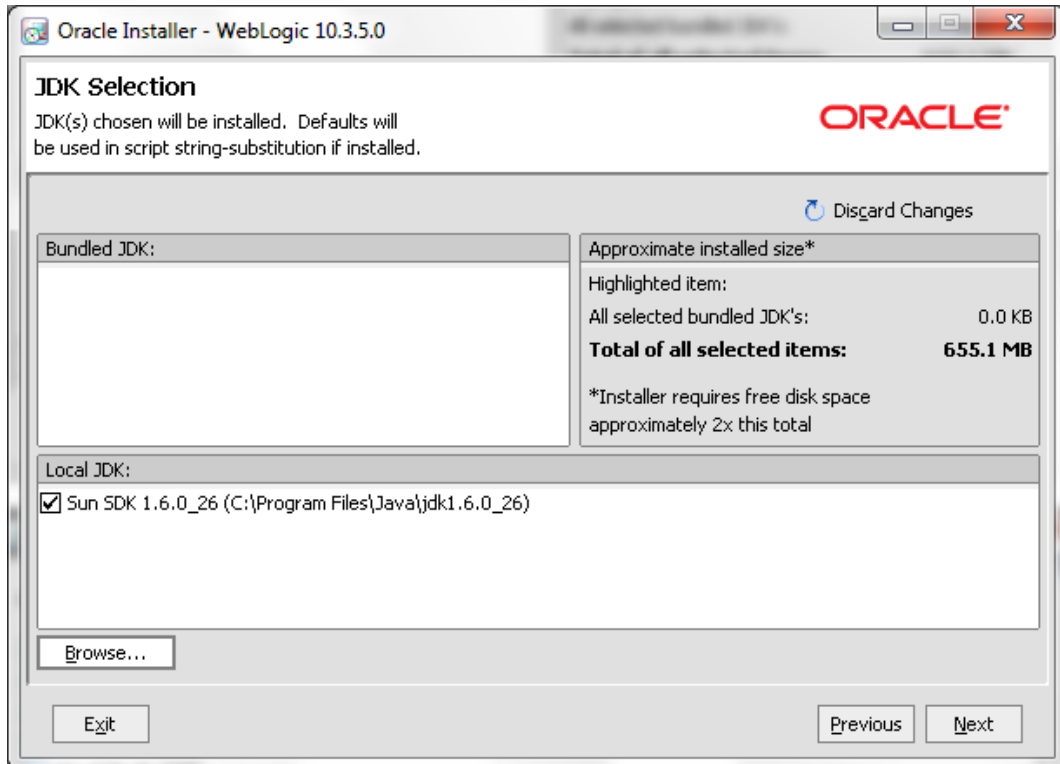
9. Select 'Typical' as the 'Install Type' and click **Next**. The following window is displayed.



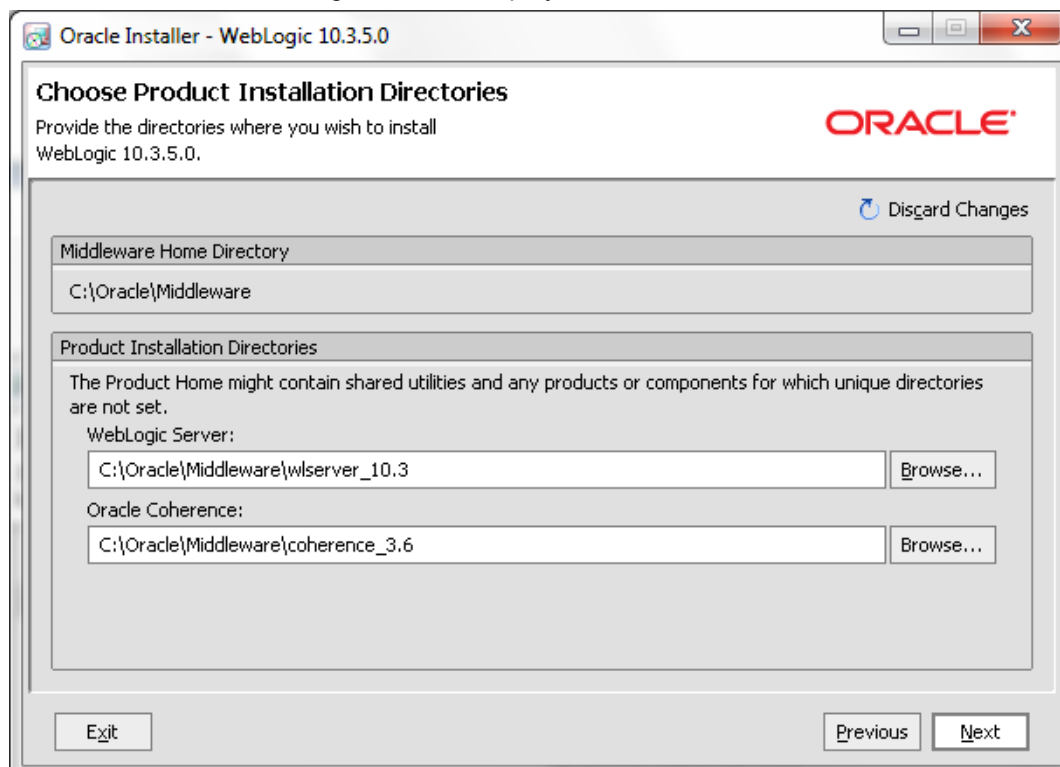
10. Click Browser button and select existing JDK Home Path as shown below.



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



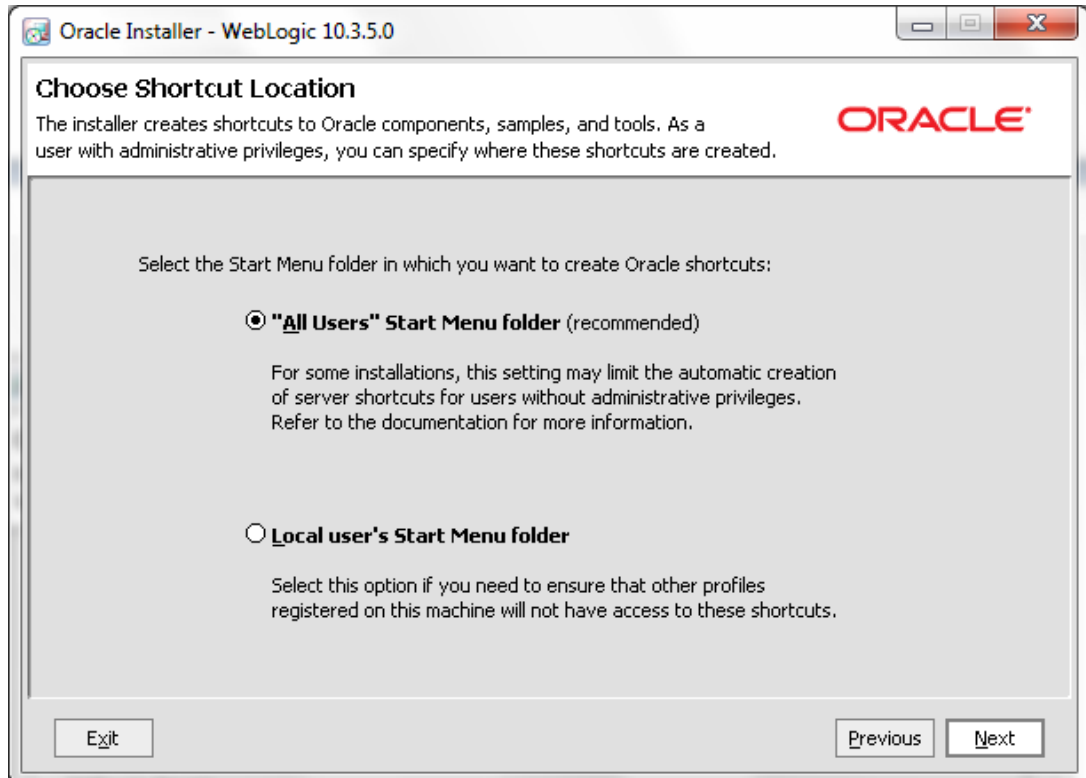
12. Click **Next**. The following window is displayed.



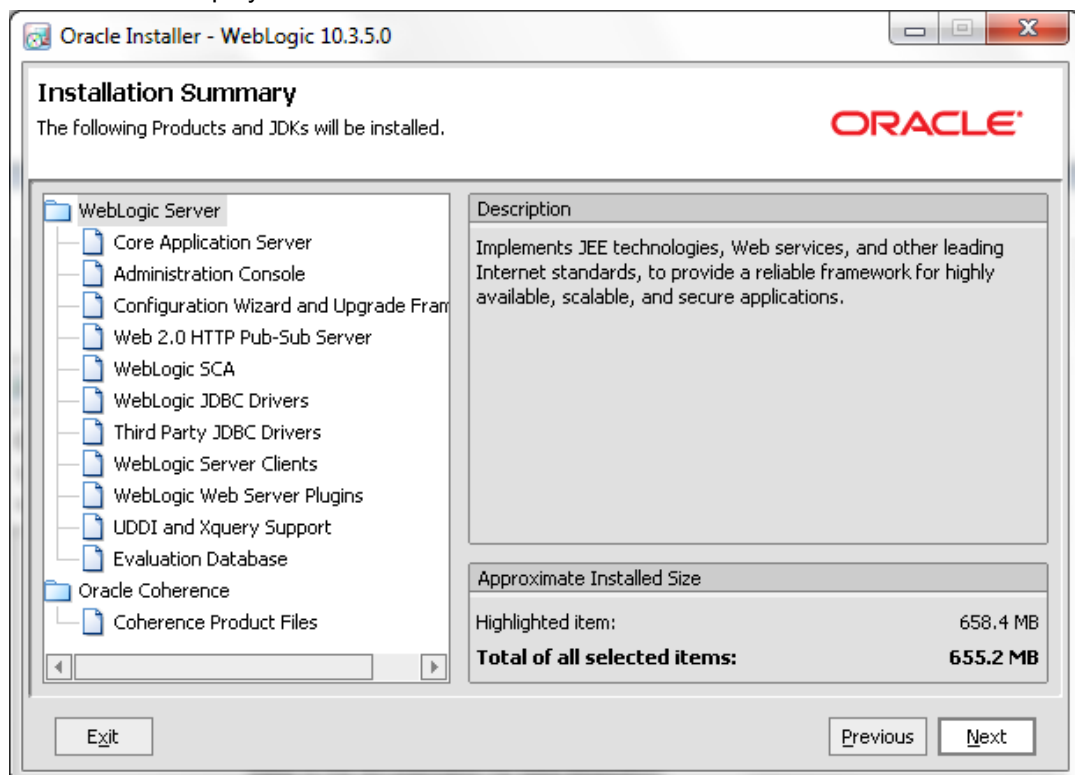
13. Click **Next**. The following window is displayed.

Note

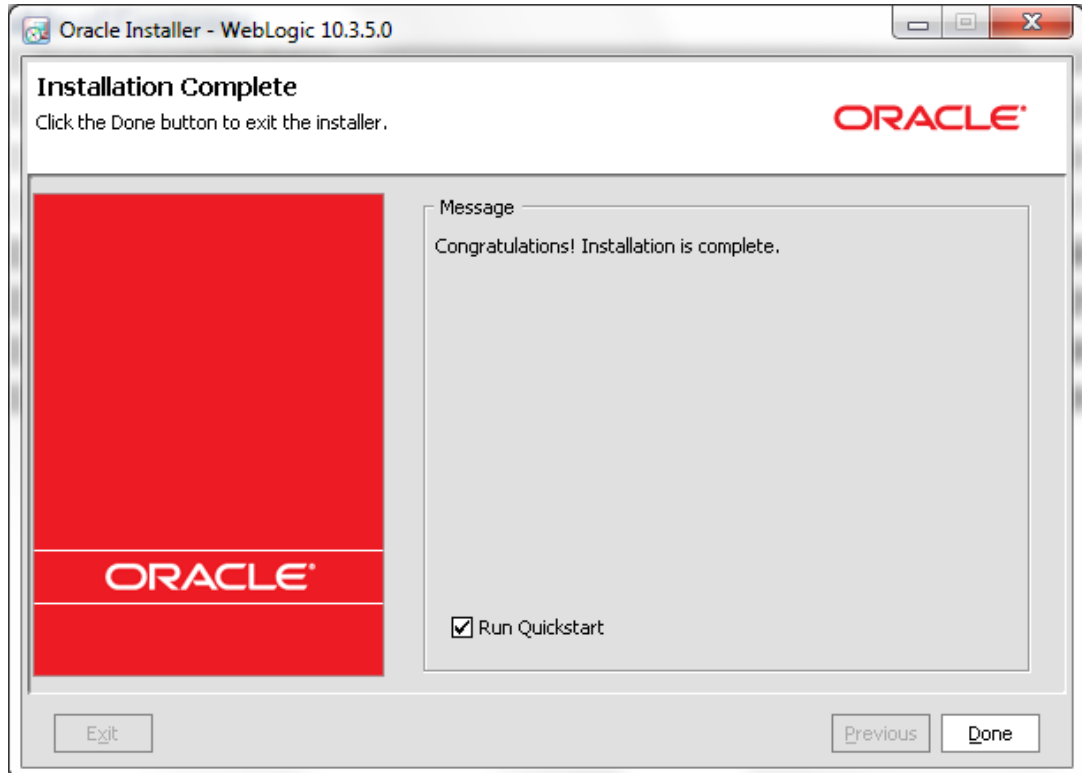
You can change the Oracle WebLogic Server and Oracle Coherence paths, if needed.



14. Select the recommended option for the Shortcut Location and click **Next**. The following window is displayed.



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



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

2.2 Installing Oracle ADF Runtime

1. Extract the zipped file ofm_appdev_generic_11.1.1.6.0_disk1_1of1.zip.
2. Go to Disk1 folder of the above unzipped file. Run the following command

In Unix/Linux:./runInstaller

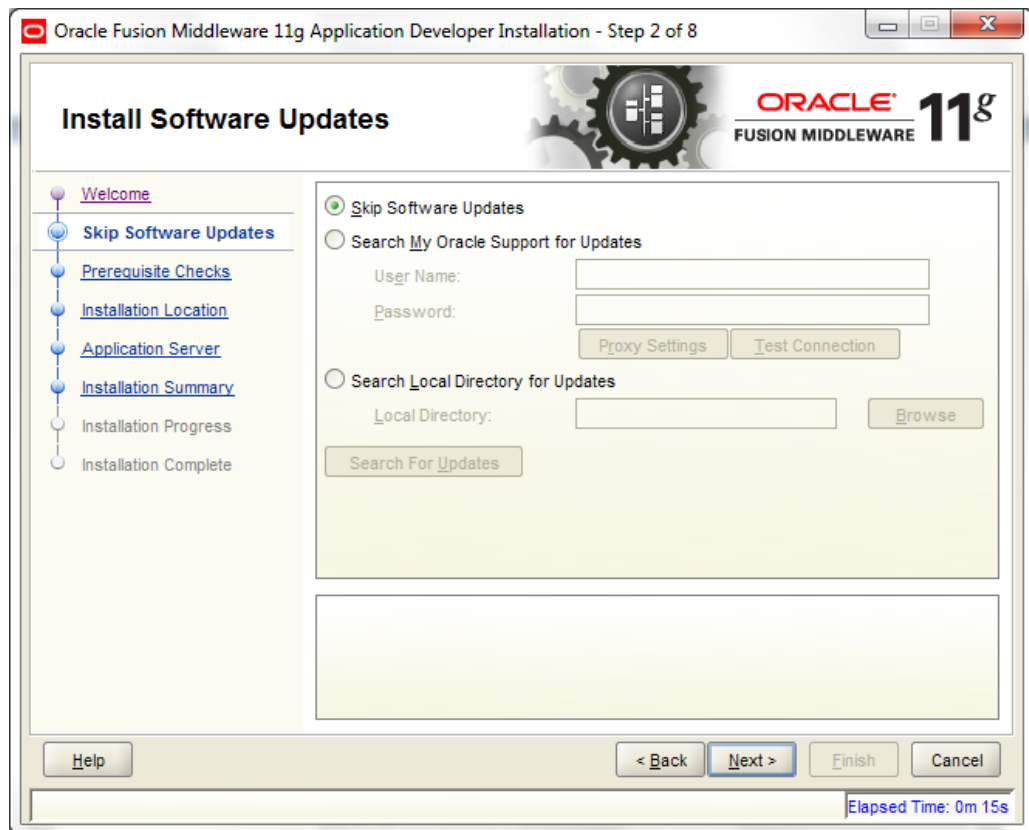
3. Enter JDK/JRE Home Path, when prompted.

In Windows:setup.exe -jreLoc <JDK/JRE Home Path>

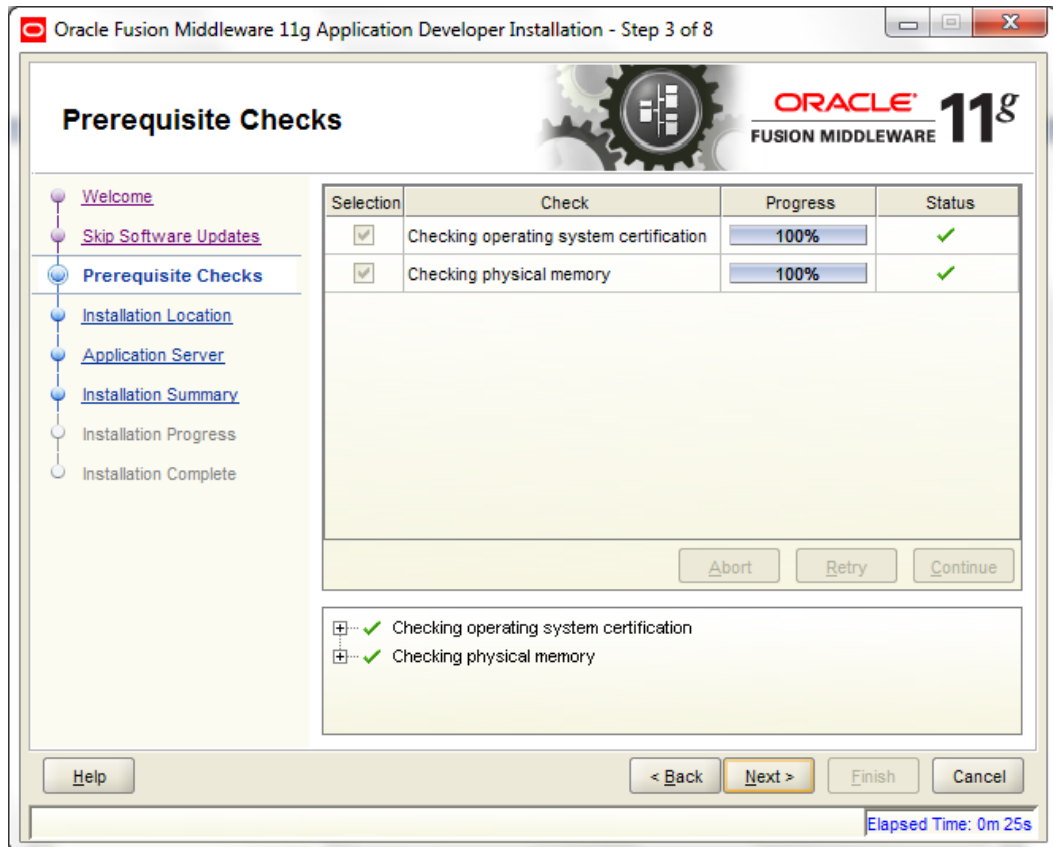
4. Welcome window is displayed.



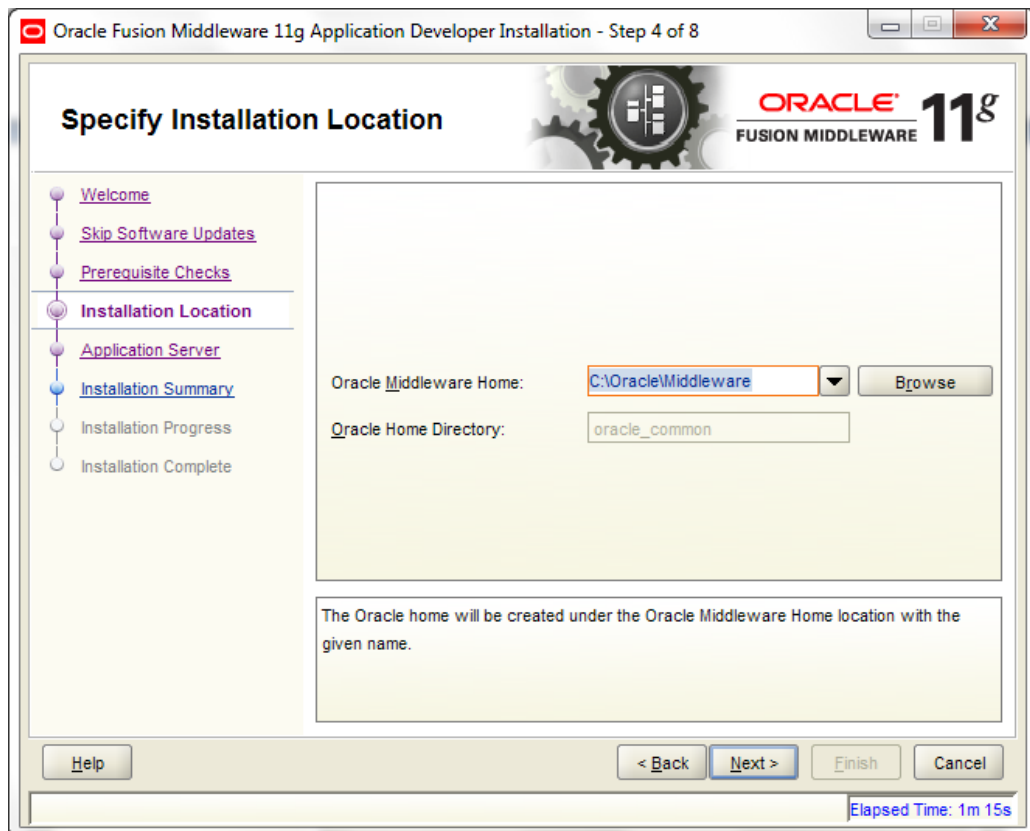
5. Click **Next**. The following window is displayed.



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



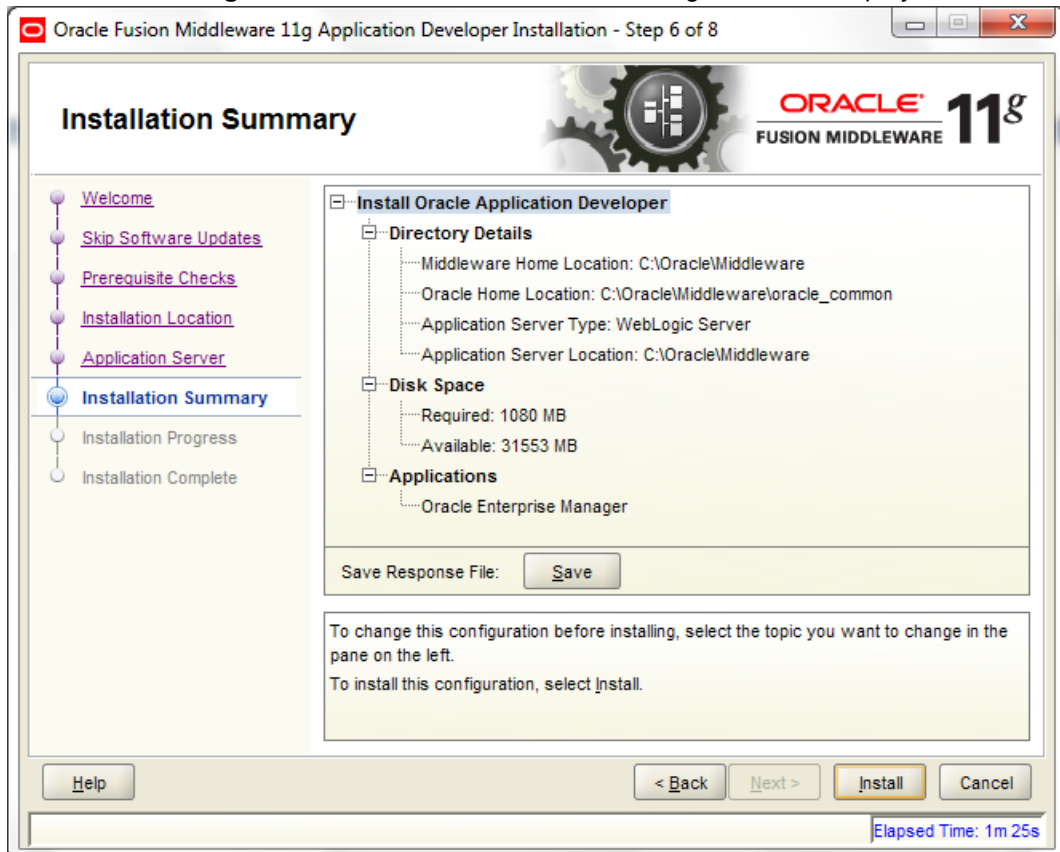
7. Click Next. The following window is displayed.



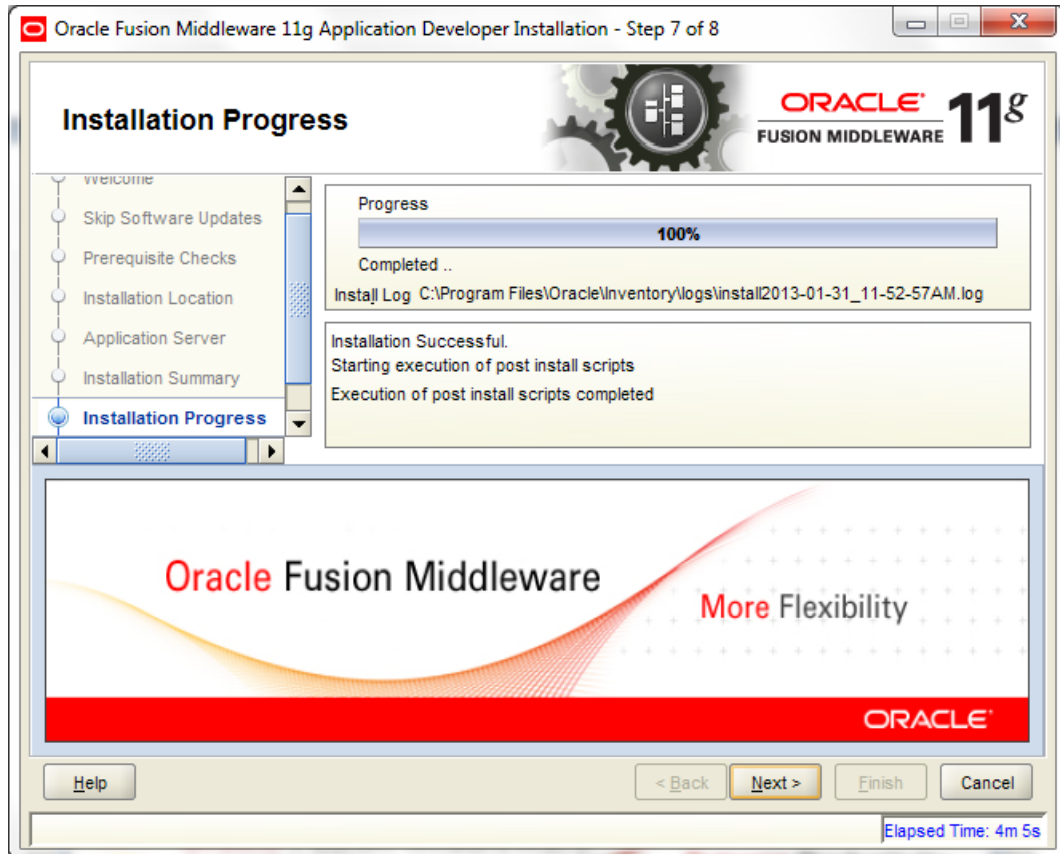
8. Select Oracle **Middleware Home Path** as highlighted and click **Next**. The following window is displayed.



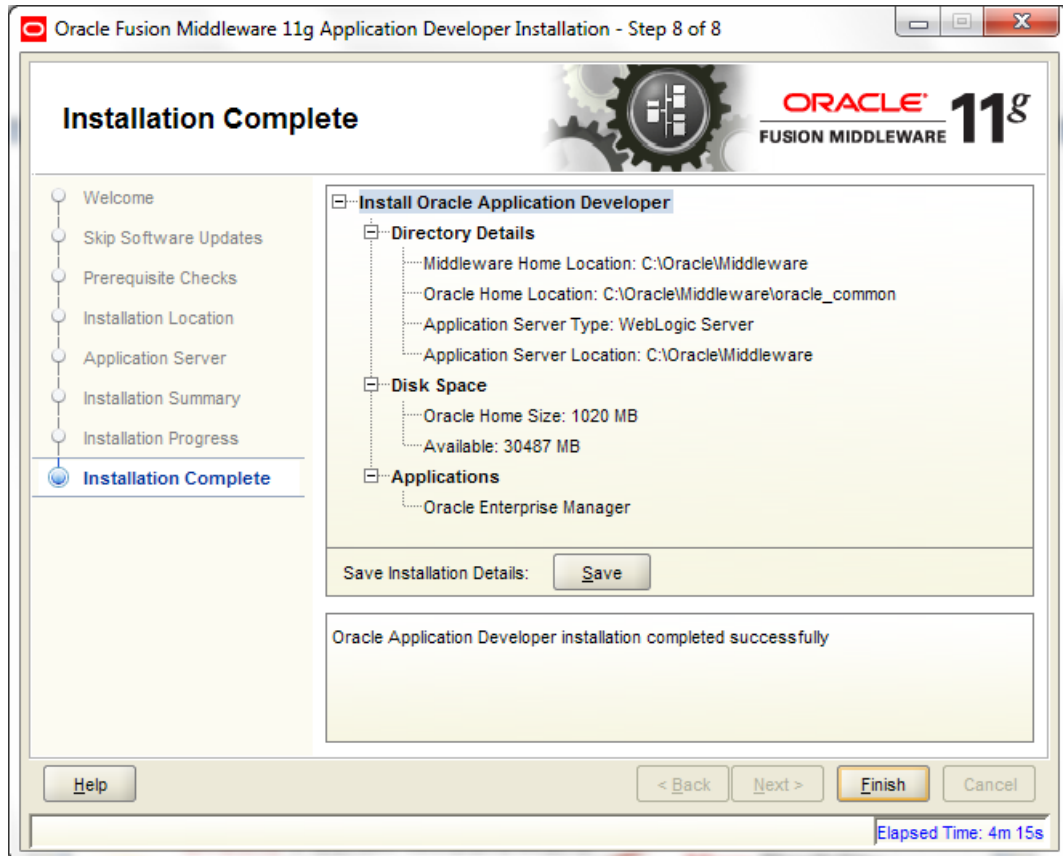
9. Select **WebLogic Server** and click **Next**. The following window is displayed.



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

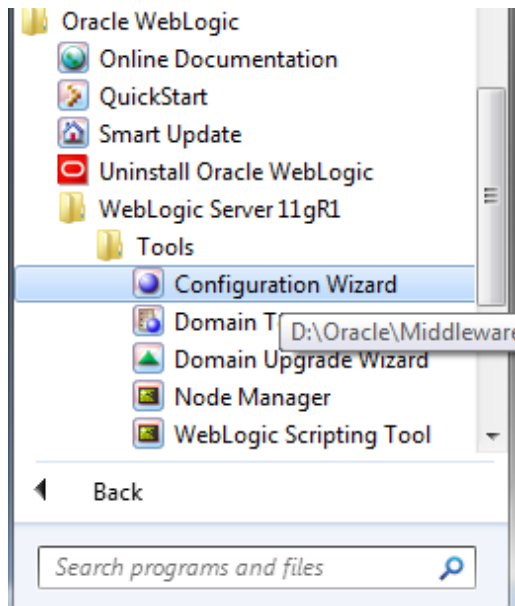
Note

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

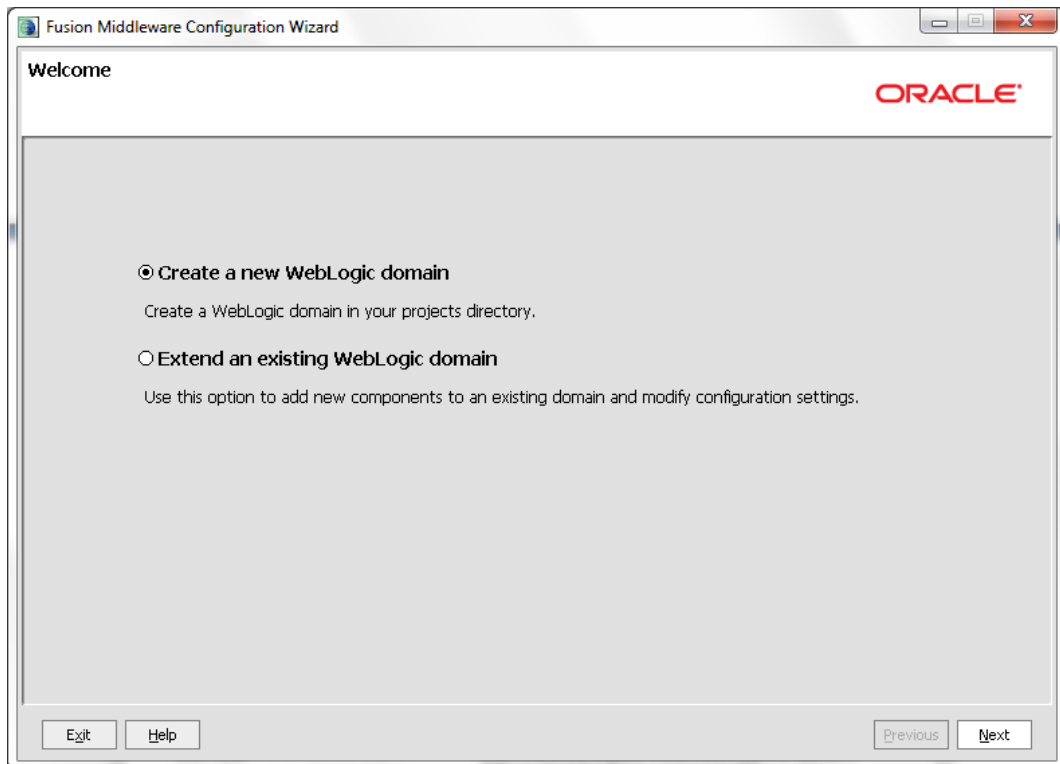
Here, WL_HOME is **/home/Oracle/Middleware**.

2. In Unix run **config.sh**.

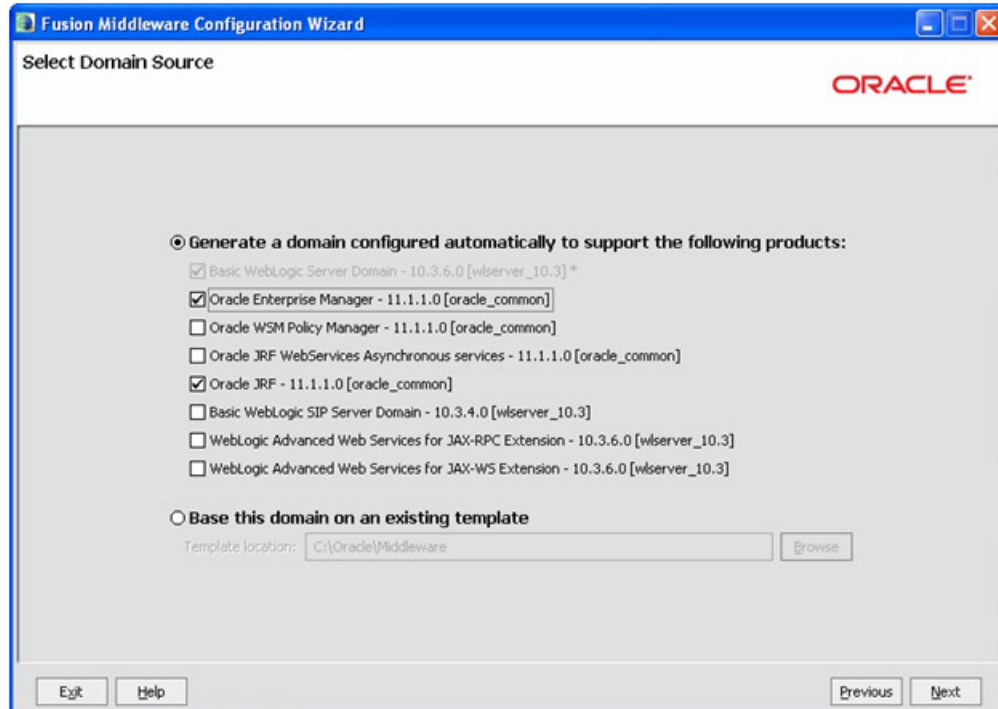
In Windows Go to Start Menu → All Programs → Oracle WebLogic → WebLogic Server 11gR1 → Tools,



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.

The screenshot shows the 'Specify Domain Name and Location' window of the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Specify Domain Name and Location'. The Oracle logo is in the top right corner. The main instruction is 'Enter the name and location for the domain:'. There are two input fields: 'Domain name:' with the value 'ofsil_domain' and 'Domain location:' with the value 'C:\Oracle\Middleware\user_projects\domains'. A 'Browse' button is next to the domain location field. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons.

9. Enter **Domain** Name and click **Next**. The following window is displayed.

10. Edit Domain Location, if needed.

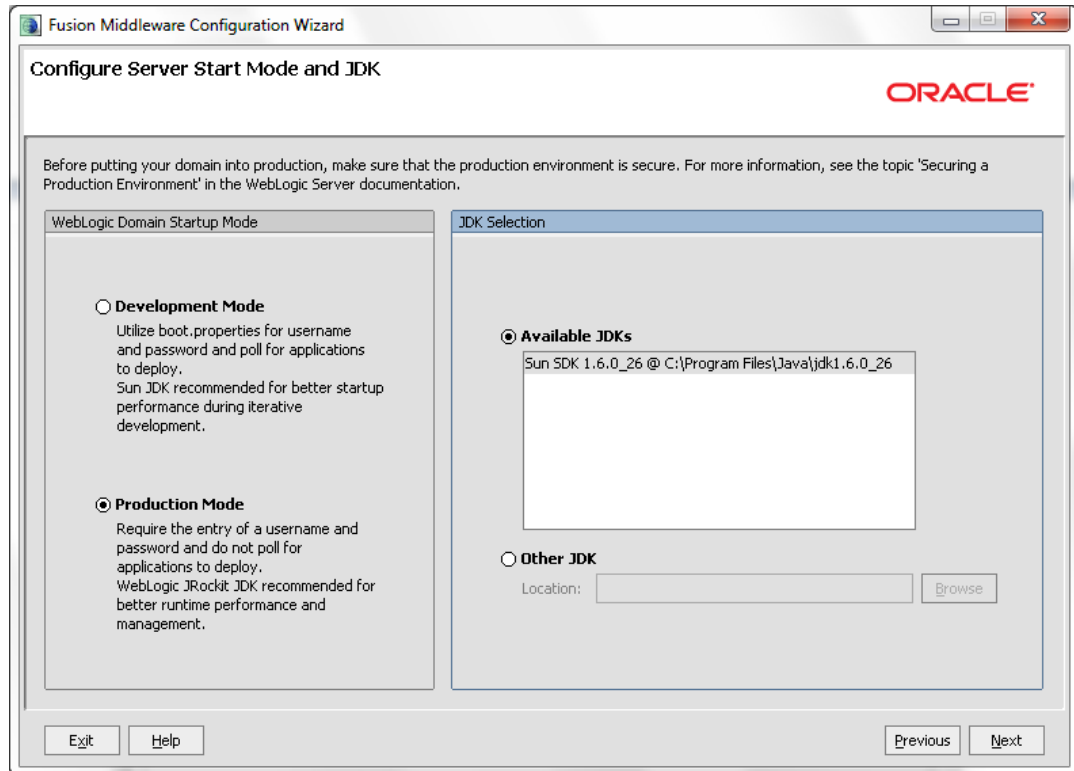
The screenshot shows the 'Configure Administrator User Name and Password' window of the Fusion Middleware Configuration Wizard. The window title is 'Fusion Middleware Configuration Wizard' and the subtitle is 'Configure Administrator User Name and Password'. The Oracle logo is in the top right corner. There is a 'Discard Changes' button with a circular arrow icon. The main form has four fields: '*Name:' with the value 'weblogic', '*User password:' with '*****', '*Confirm user password:' with '*****', and 'Description:' with the text 'This user is the default administrator.'. At the bottom, there are 'Exit', 'Help', 'Previous', and 'Next' buttons.

11. Enter credentials for the following:

- Name
- User password

- Confirm user password
- Description

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

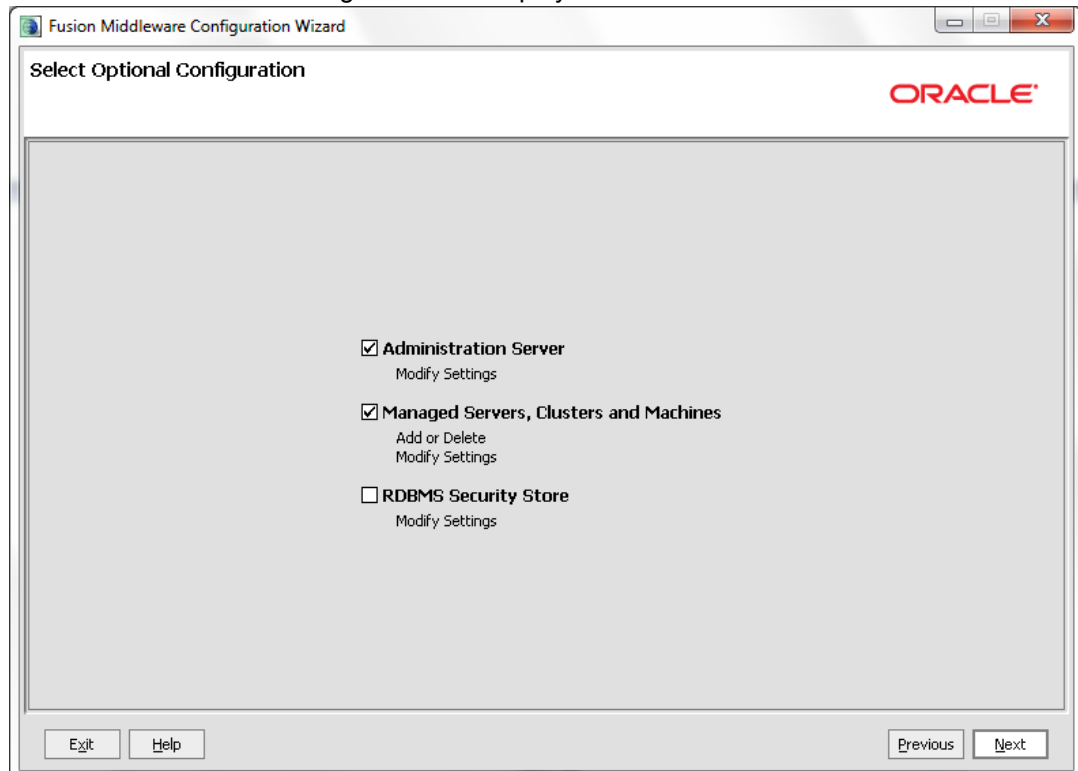


13. Select **Production Mode** and **JDK/JRockit** from **Available JDKs**

OR

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

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 the following fields:

- *Name: AdminServer
- *Listen address: All Local Addresses
- Listen port: 7001
- SSL listen port: N/A
- SSL enabled:

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

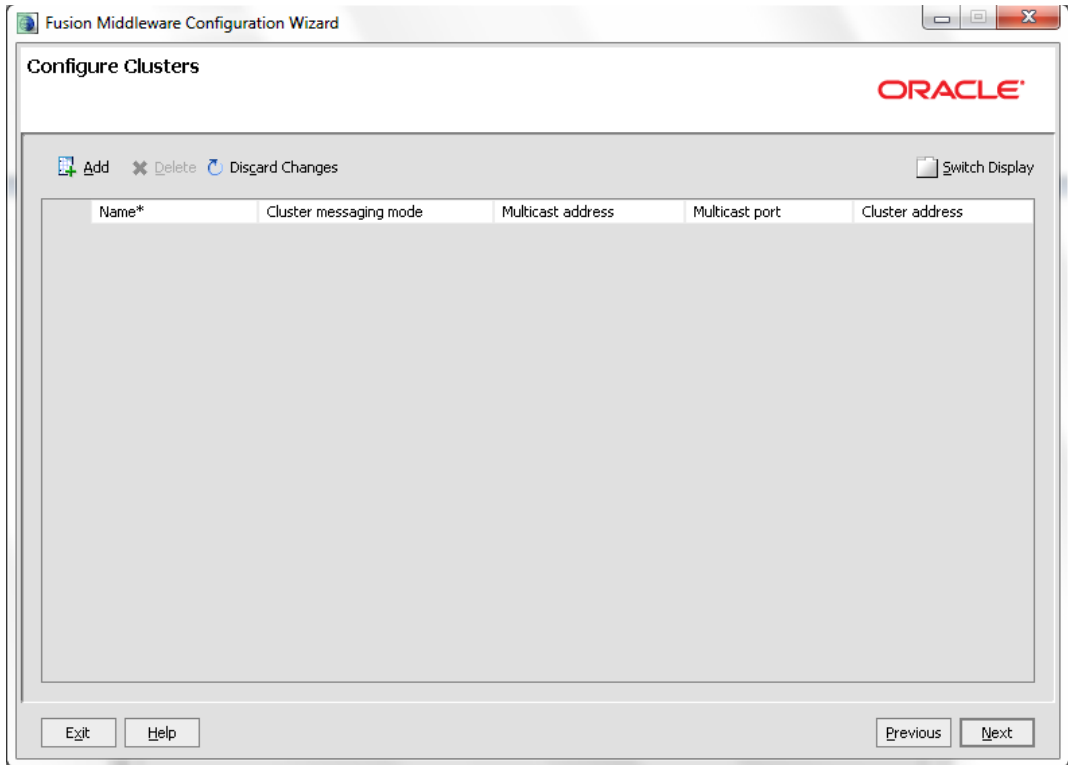
16. Enter Administration Server **Name** and **Listen Port** details and click **Next**. The following window is displayed.

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 buttons for '+ Add', 'x Delete', and 'Disgard Changes', along with a 'Switch Display' checkbox. The main area contains a table with the following data:

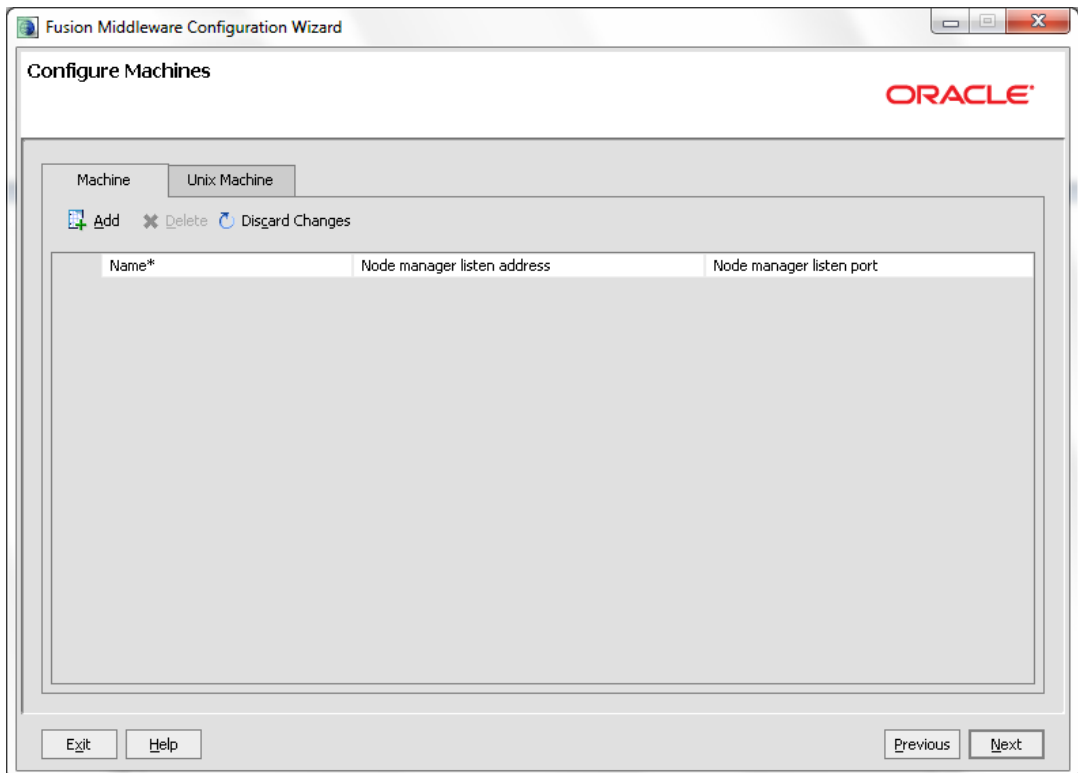
	Name*	Listen address*	Listen port	SSL listen port	SSL enabled
→ 1	Ofssl_ManagedServer	All Local Addresses	7003	N/A	<input type="checkbox"/>

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

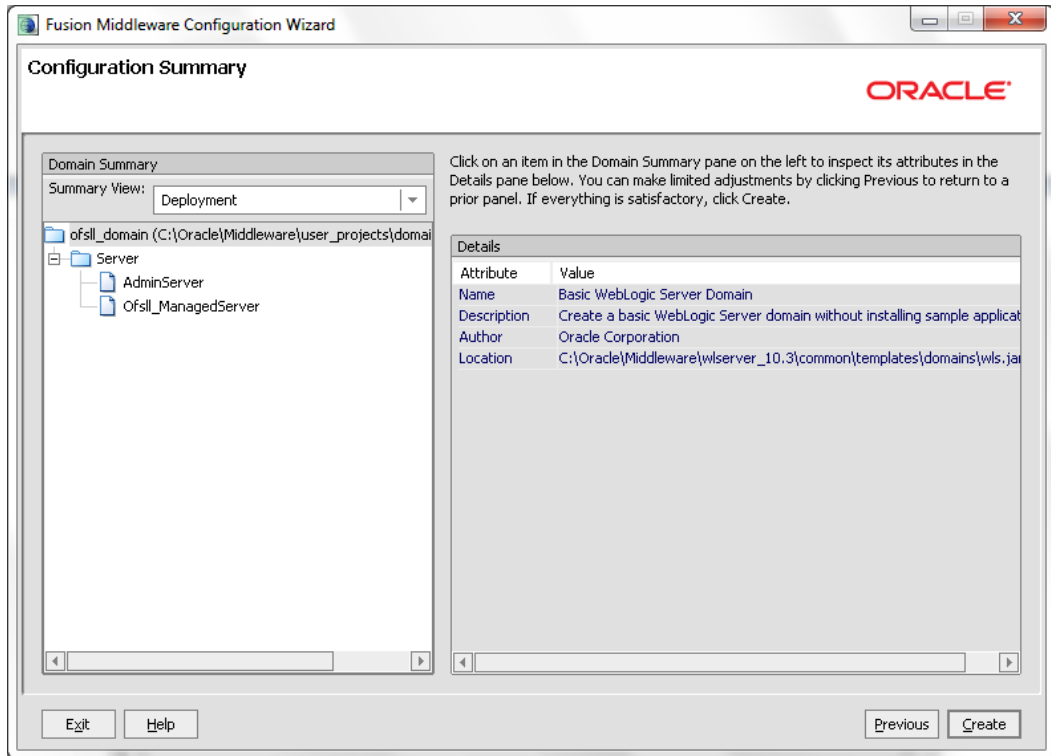
17. Enter **Name** and **Listen Port** details in Configure Managed Servers window and click **Next**. The following window is displayed.



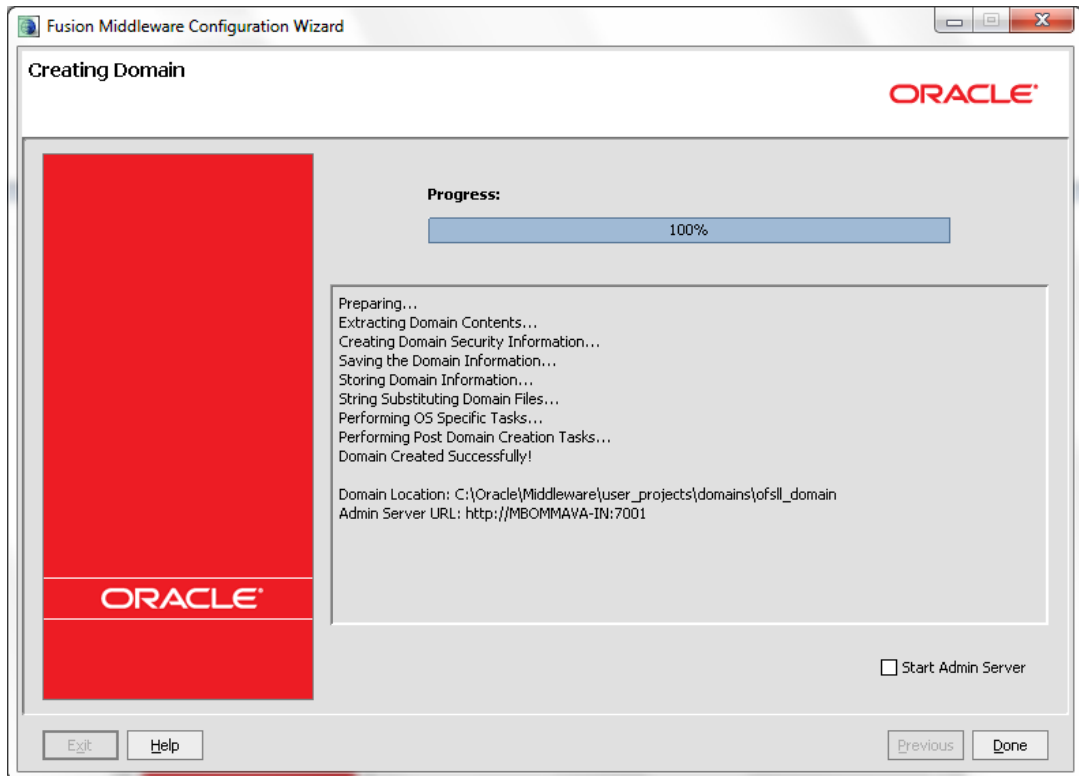
18. Configure as required and click **Next**. The following window is displayed.



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.

22. 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"
```

- The "\$MW_HOME/user_projects/domains/mydomain" directory contains a script that can be used to start the Admin server. Use the "&" if you want access to the command line to be returned.

```
$ cd $MW_HOME/user_projects/domains/mydomain
```

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

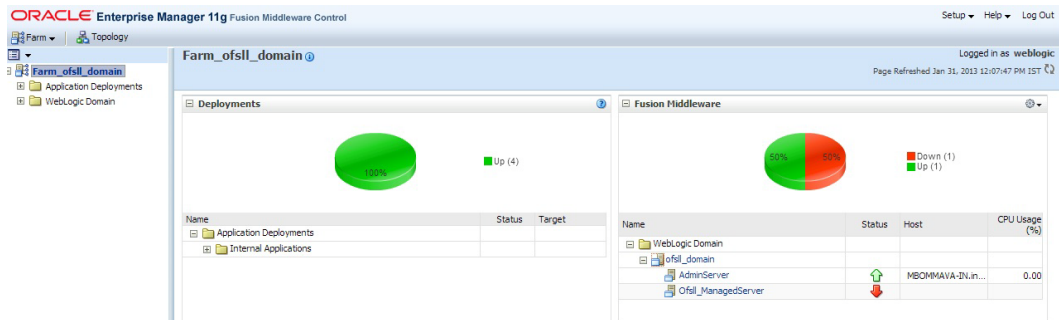
- To Start Managed Server

```
$ cd $MW_HOME/user_projects/domains/mydomain/bin
```

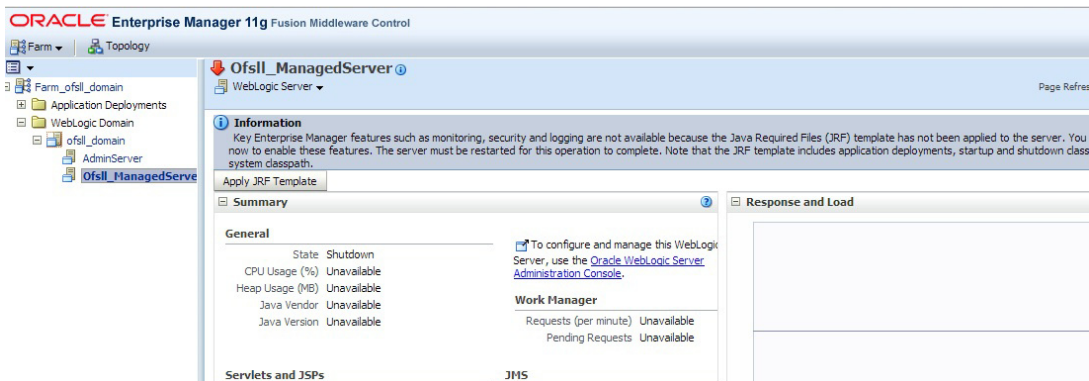
```
$ $MW_HOME/user_projects/domains/mydomain/bin/startManagedWebLogic.sh {ManagedServer_name} {AdminServer URL} &
```

3.2 Applying the JRF Template

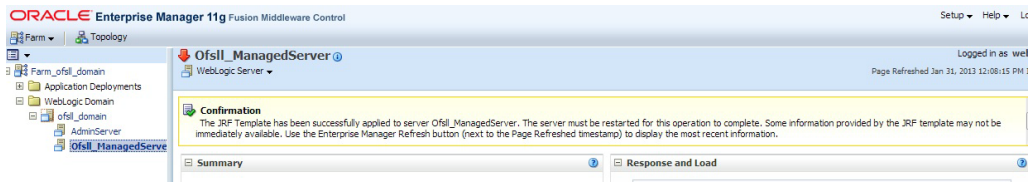
- Start Oracle WebLogic Server
- Login to Oracle Enterprise Manager 11g Console (<http://hostname:port/em>).



- 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_11.1.1.6.0_disk1_1of1.zip) from the link mentioned in prerequisites.
- Unzip the ofm_rcu_linux_11.1.1.6.0_disk1_1of1.zip to your local drive.
- On windows, assume that it is unzipped to C:/oracle/rcuHome and set the value as RCU_HOME.

i.e. export RCU_HOME=C:/oracle/rcuHome

- Open command prompt and browse to \$RCU_HOME/bin and run **./rcu**
- On Unix, /home/oracle/rcuHome/bin and run **./rcu**
- The following window is displayed.



- Click Next. The following window is displayed.



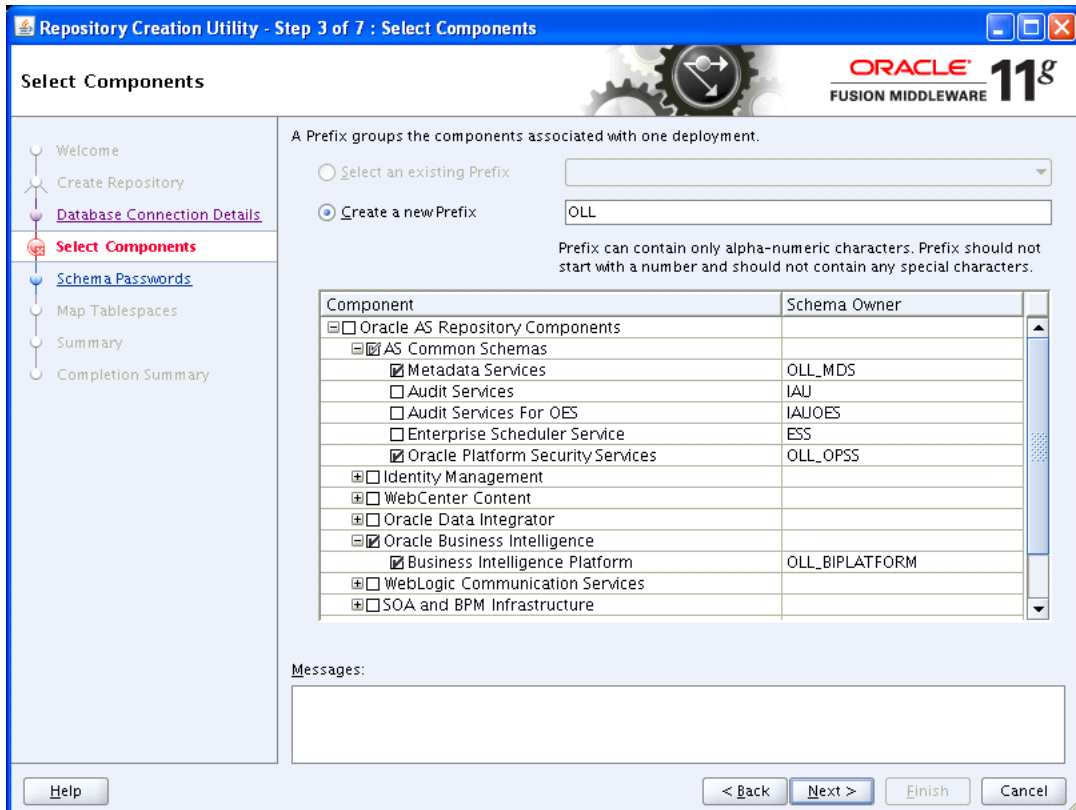
8. Select **Create** to create new schemas and click **Next**. The following window is displayed.



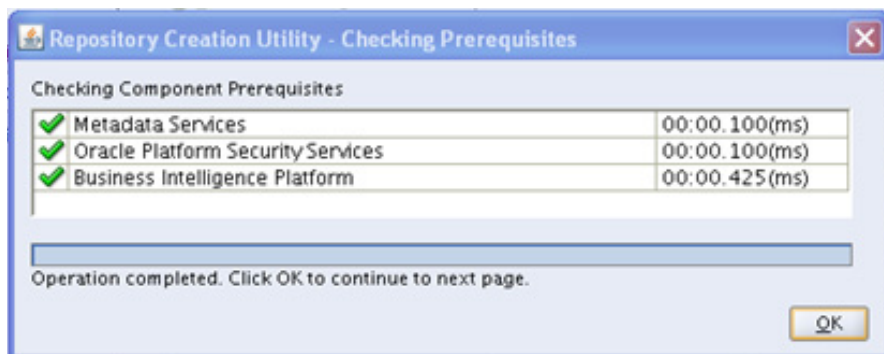
9. Provide database details where you want to create schemas, as shown in the above screen.

Note

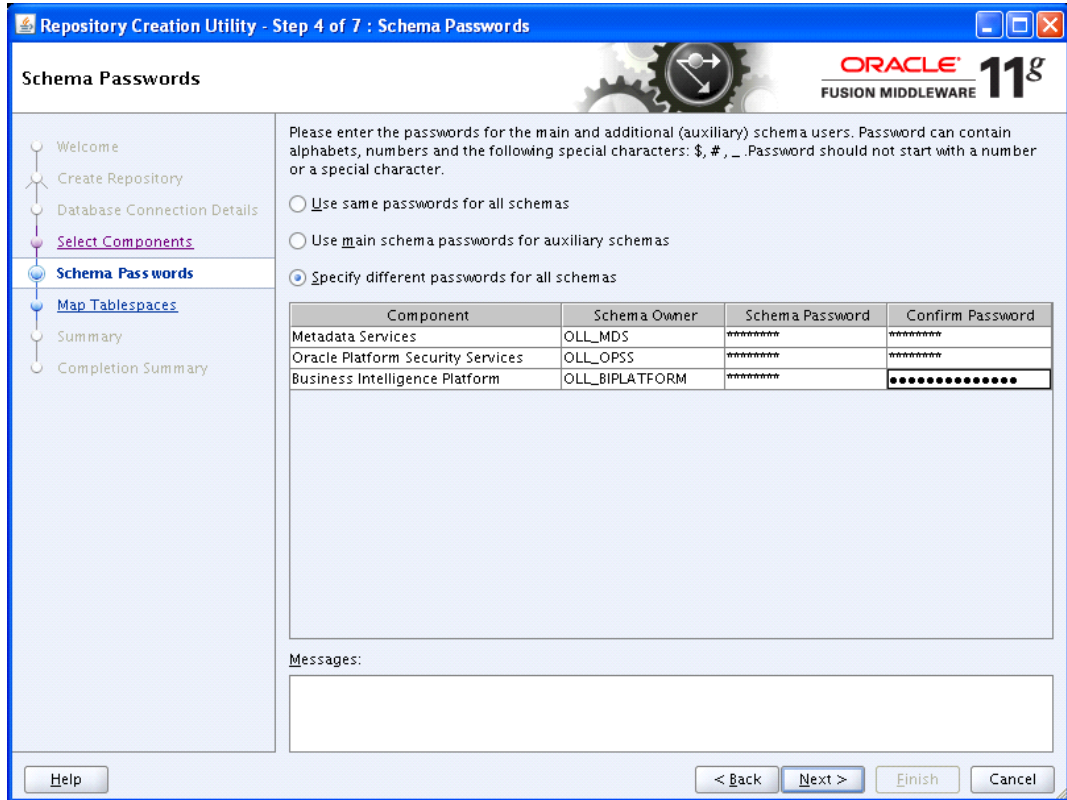
You will require a user with SYSDBA role to create schemas.



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

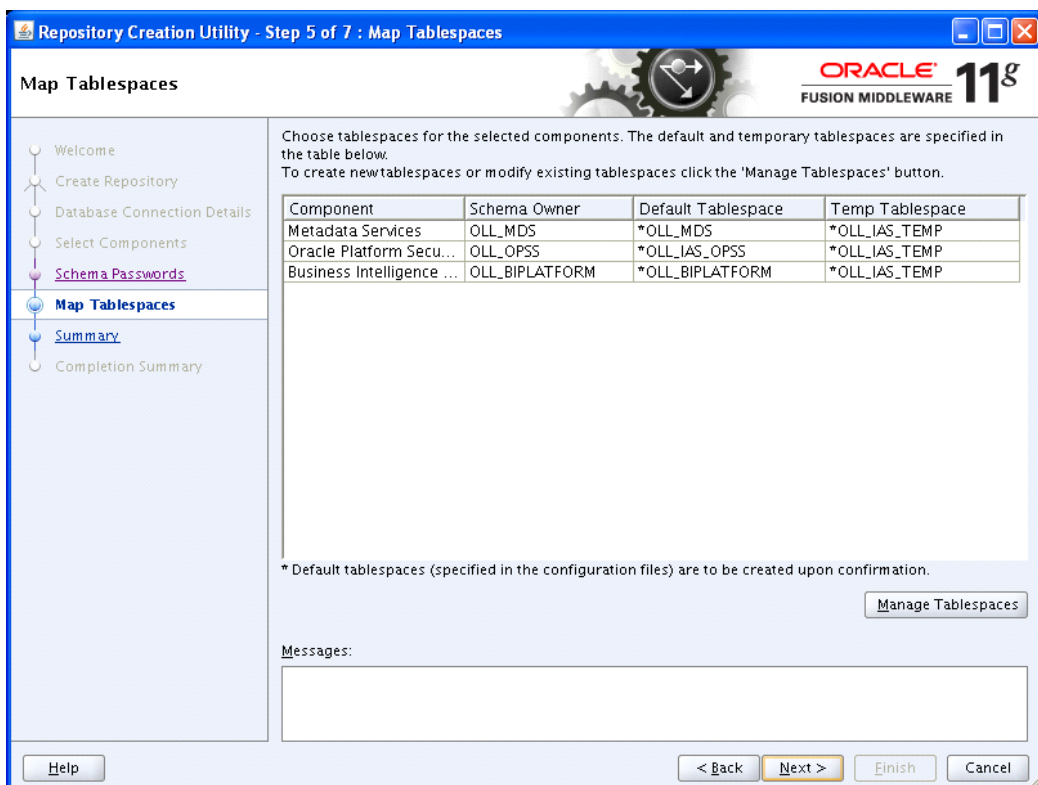


13. Once the operation is complete, click **OK**. The following window is displayed.

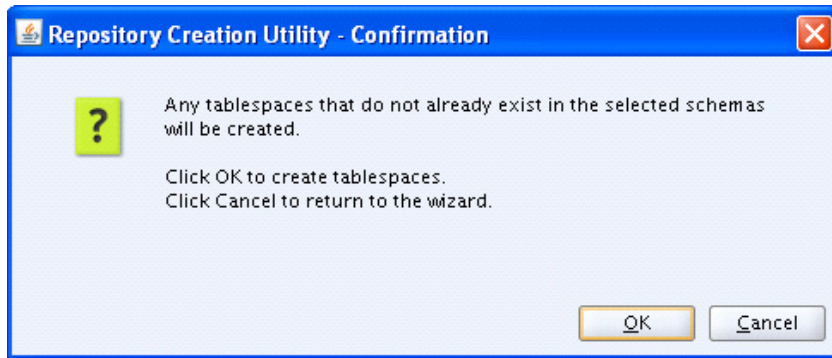


14. Select **Specify different passwords for all schemas** and provide Schema Passwords for each server as shown above.

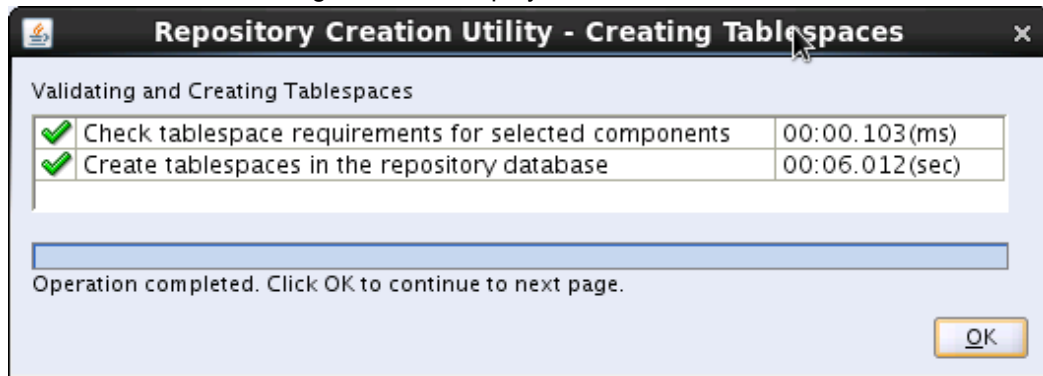
15. Click Next., The following window is displayed.



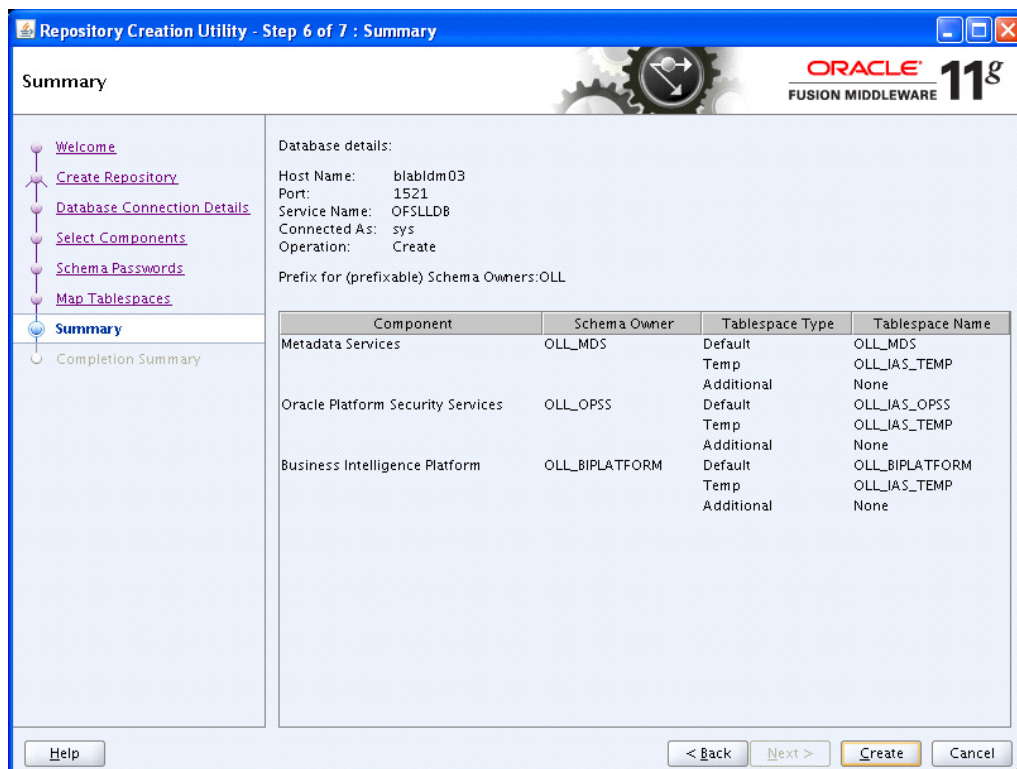
16. Click **Next**. The following window is displayed.



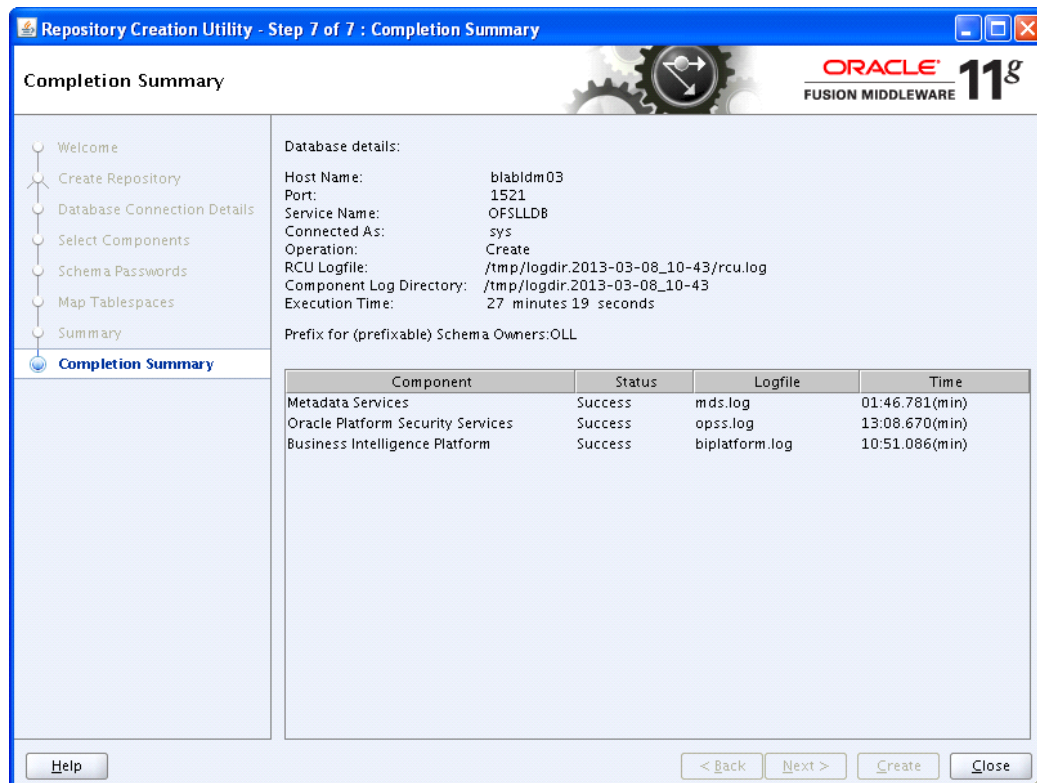
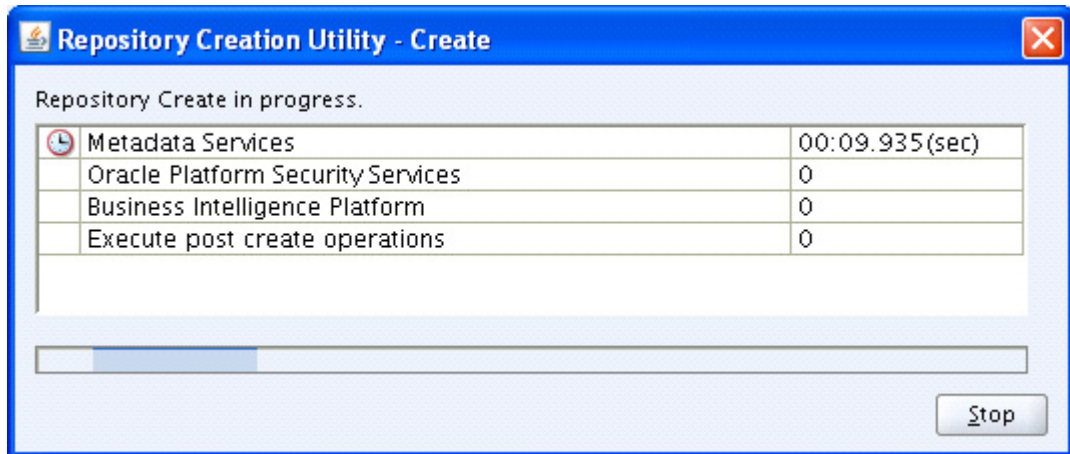
17. Click **OK**. The following window is displayed.



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



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

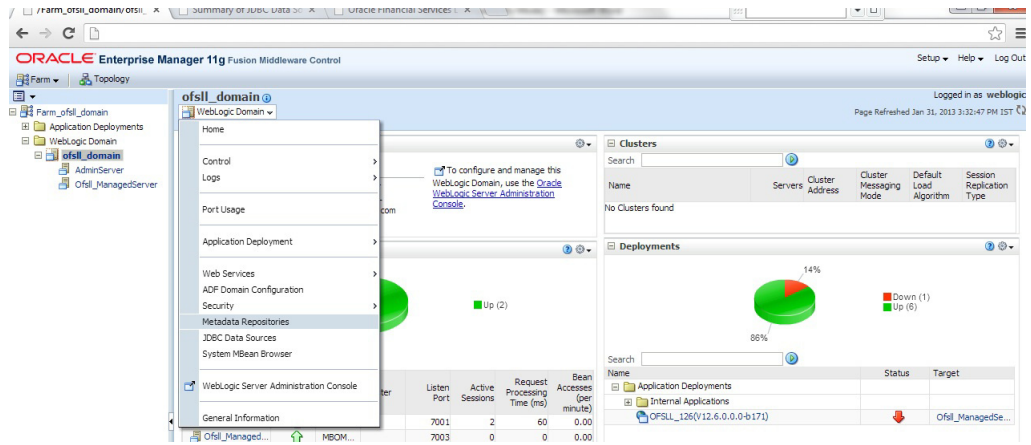


20. Click **Close** to close the window.

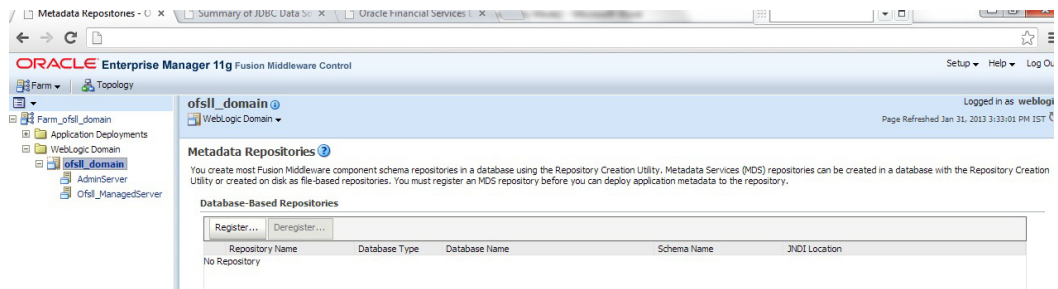
3.4 Creating Metadata Repository

Assuming that **DEV_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.

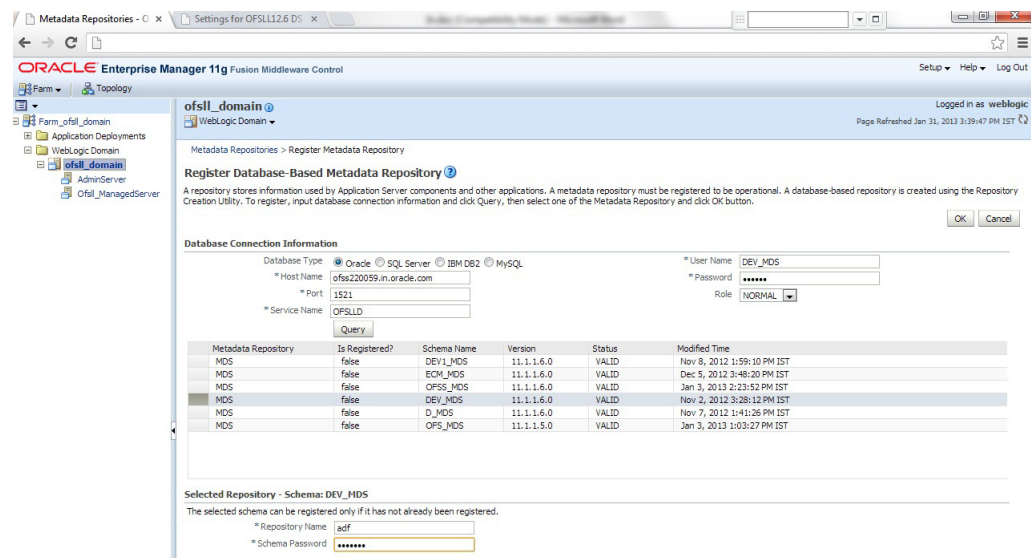
1. Login to Oracle Enterprise Manager 11g console (<http://hostname:port/em>).



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

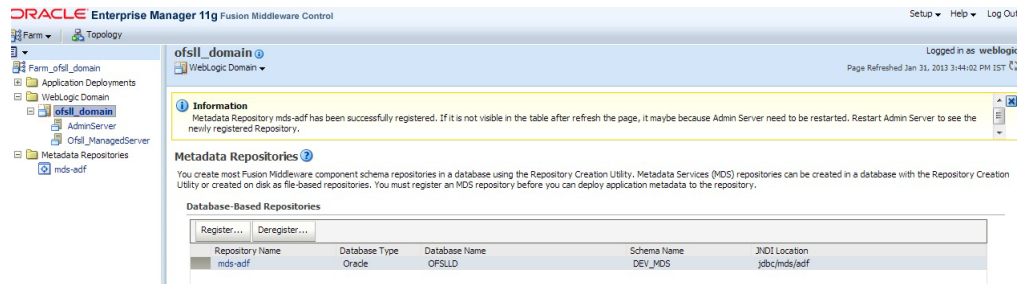


5. Click Register button. The following window is displayed.

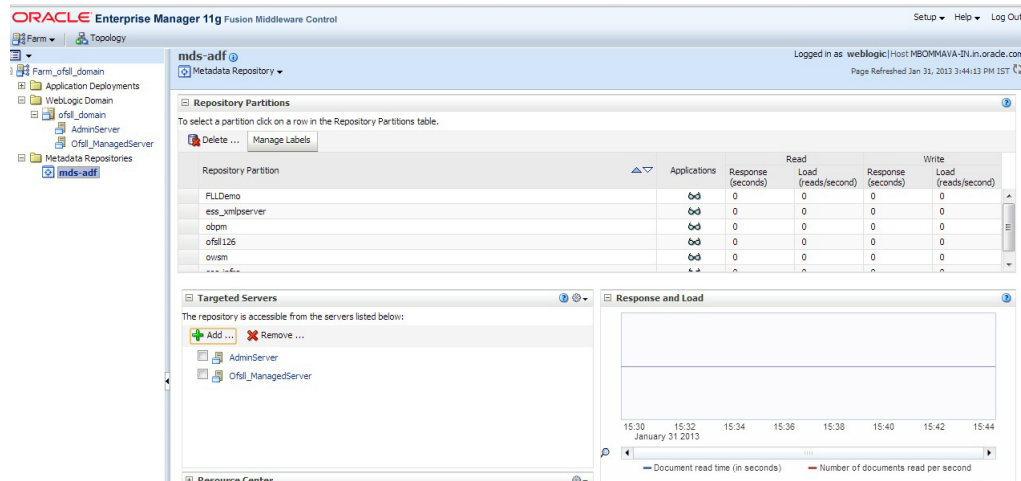


6. Enter database instance details under Database Connection Information section and click **Query**.
7. All available schemas in the given database instance are listed.
8. Select the schema you require and enter **Repository Name (adf)** and the password under Selected Repository – Schema **DEV_MDS** section.

9. Click OK. The following window is displayed.



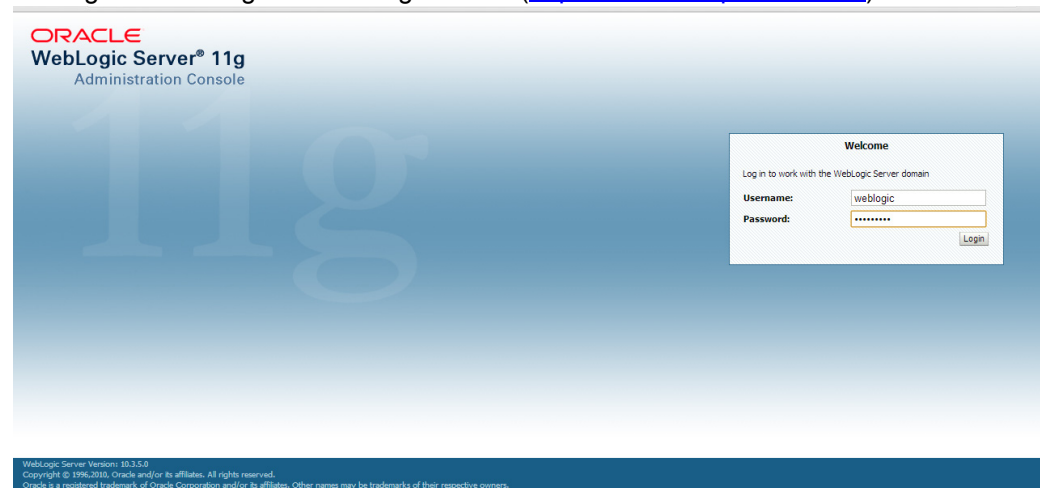
10. Click Repository name **mds-adf** on left panel. You can even select it from right panel.



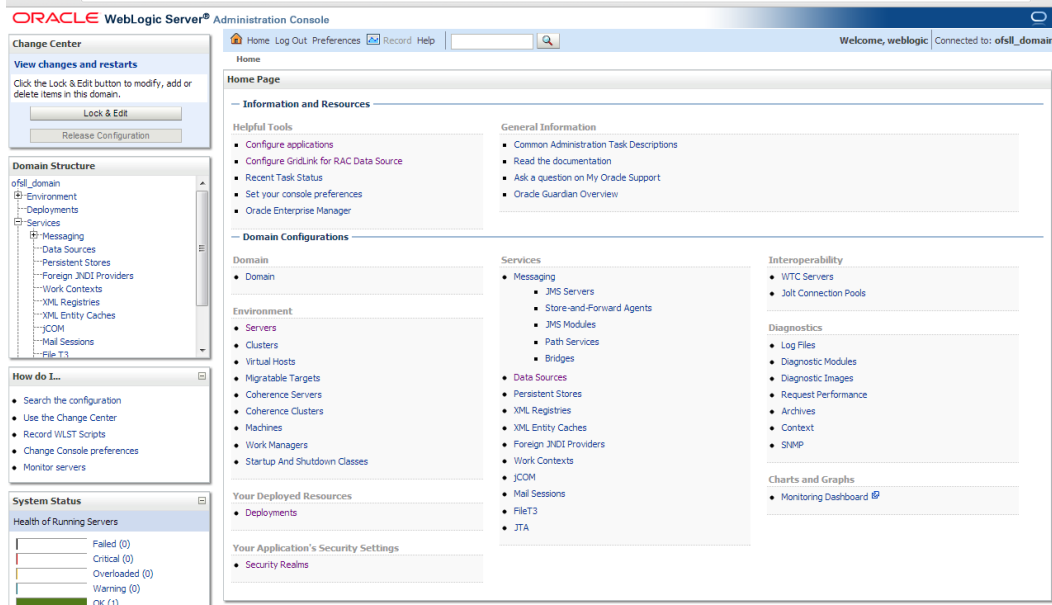
11. And target to AdminSever and Ofsl_ManagedServer as on right panel.

3.5 Creating Data Source

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

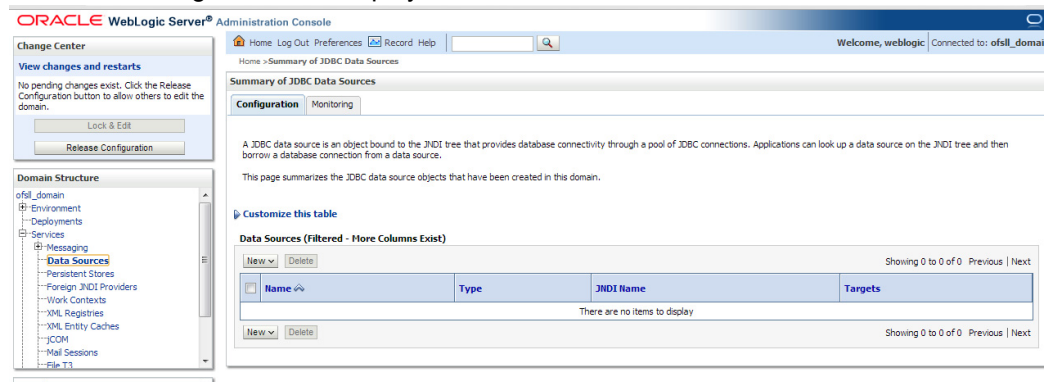


2. The following window is displayed.

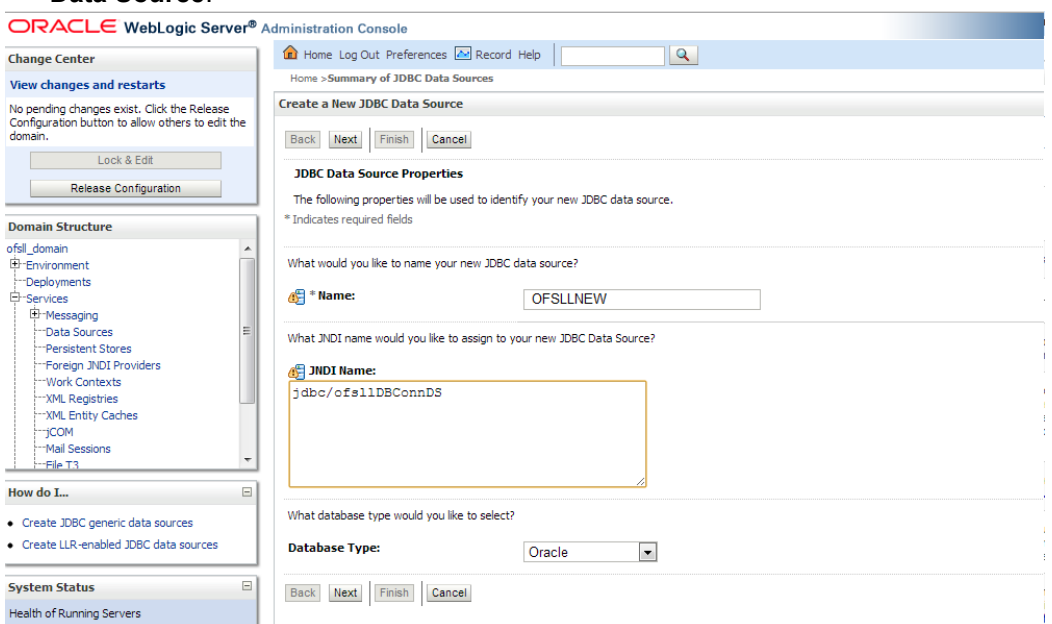


3. Click Domain Name → Services → Data Sources.

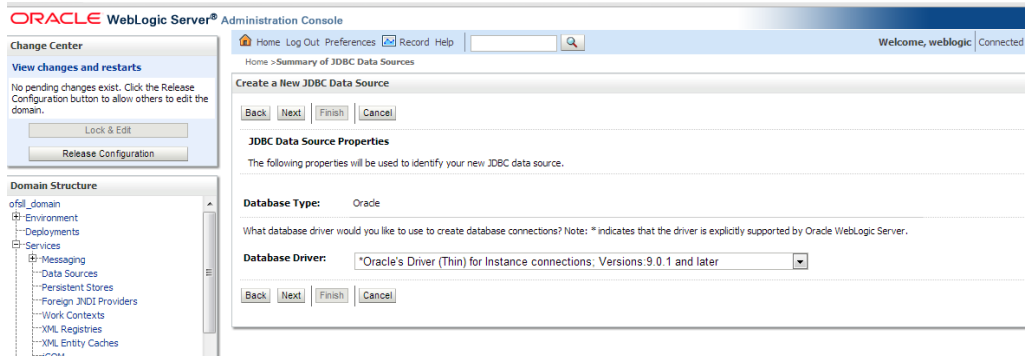
4. The following window is displayed.



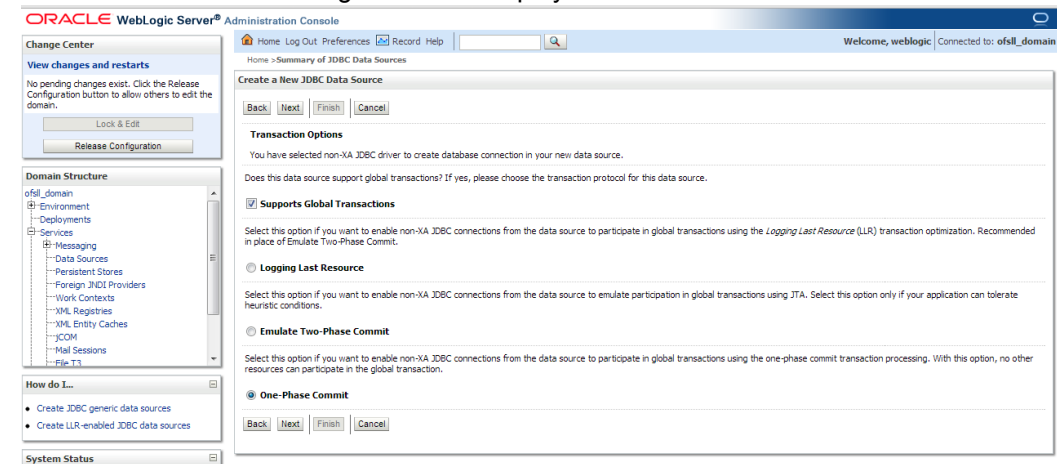
5. Click **Lock & Edit** button on the left panel. Click **New** on right panel and select **Generic Data Source**.



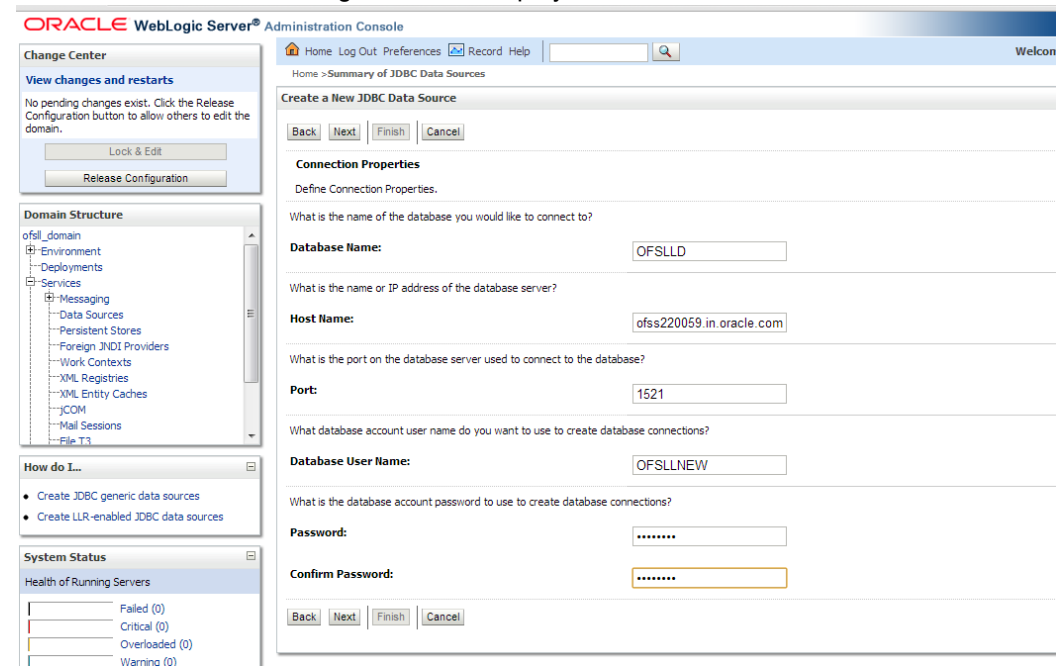
6. Enter Data source **Name**
7. Enter **JNDI Name** as **jdbc/ofsIIDBCConnDS**.
8. Select **Oracle** as **Database Type** and click **Next**. The following window is displayed.



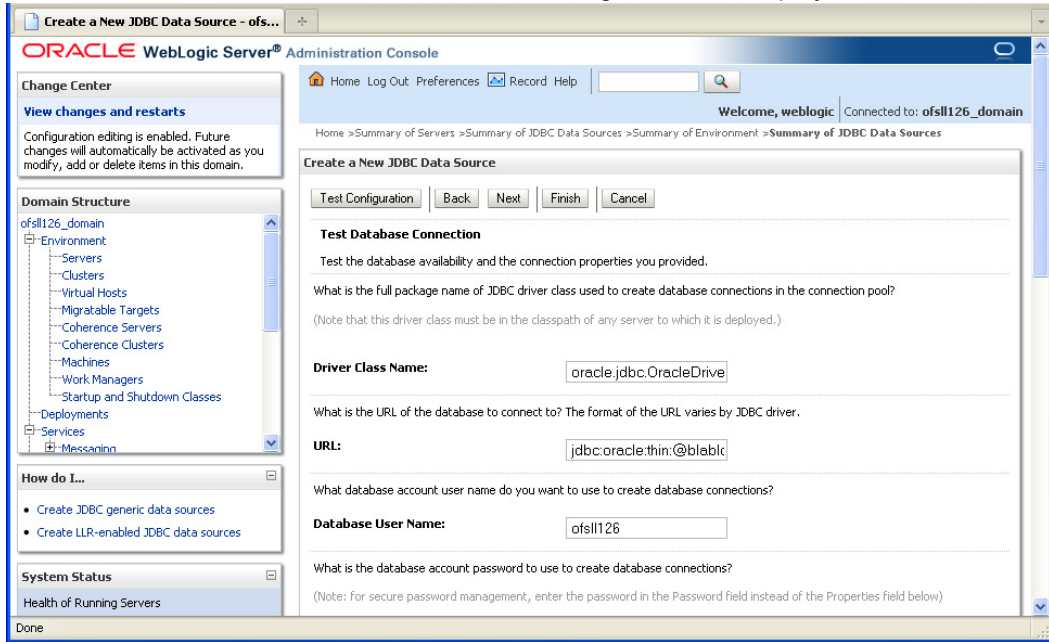
9. Select the Database Driver "Oracle's Driver(Thin) for Instance connections; Versions:9.0.1 and later" as shown above.
10. Click **Next**. The following window is displayed.



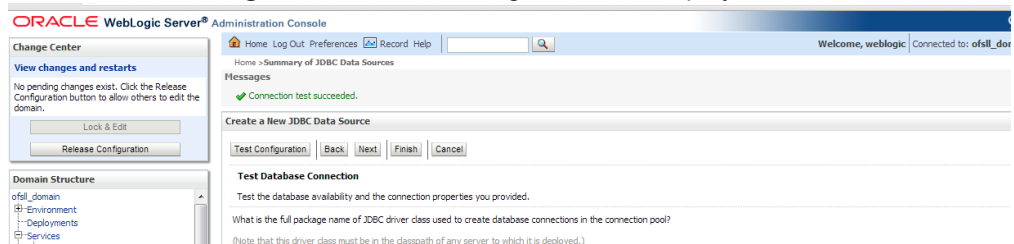
11. Click **Next**. The following window is displayed.



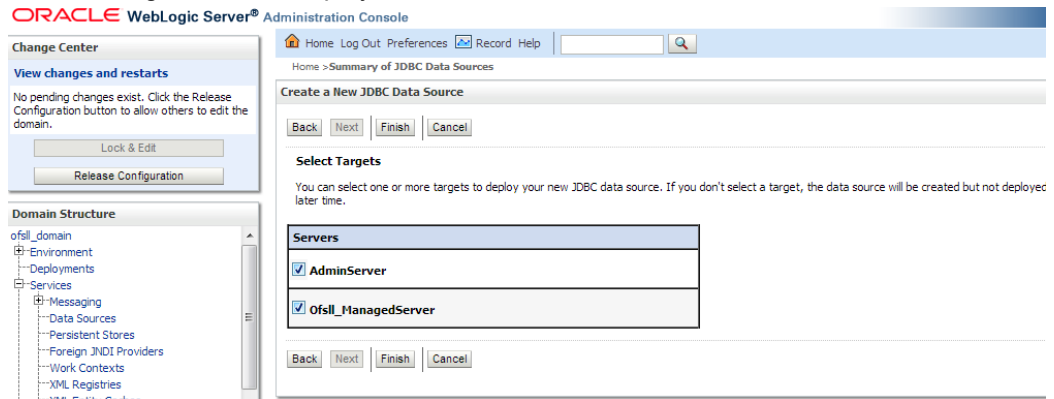
12. Enter Database details click **Next**. The following window is displayed.



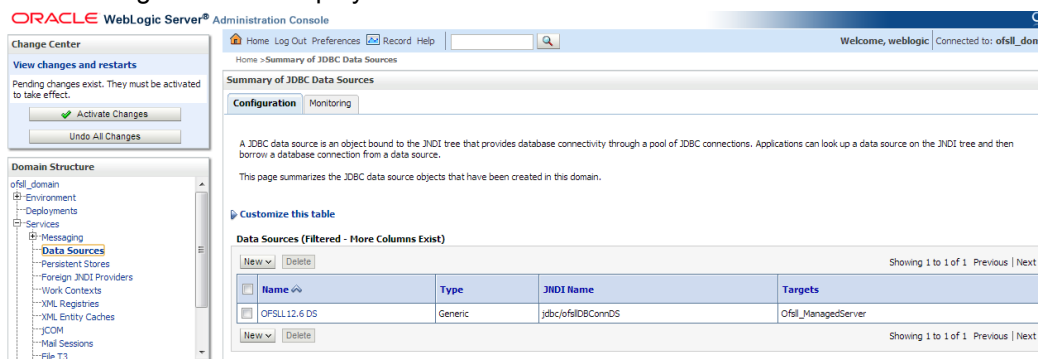
13. Click **Test Configuration**. The following window is displayed.



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



15. Select target Servers **AdminServer** and **Ofsll_ManagedServer** and click **Finish**. The following window is displayed.



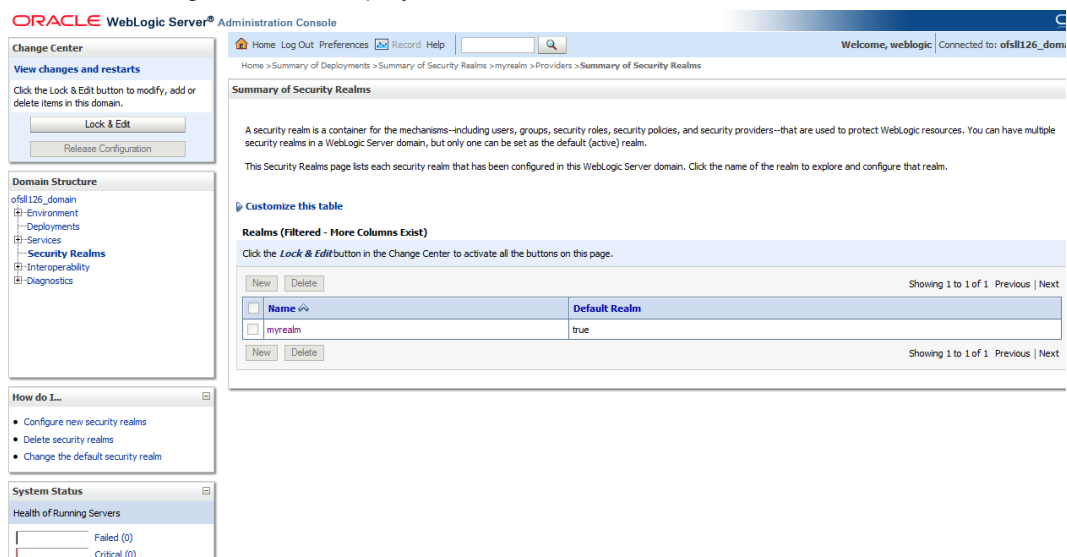
16. Click **Activate Changes**.

Update the following parameters in JDBC data source connection pool:

1. Select **Services** → **Data Sources** → select the **OFSLL** 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..



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

Home > Summary of Deployments > Summary of Security Realms > myrealm > Providers > Summary of Security Realms > myrealm

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

General RDBMS Security Store User Lockout Performance

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

Save

Use this page to configure the general behavior of this security realm.

Note:
If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled.

Name: myrealm The name of this security realm. [More Info...](#)

Security Model Default: DD Only Specifies the default security model for Web applications or EJBs that are secured by this security realm. You can override this default during deployment. [More Info...](#)

Combined Role Mapping Enabled Determines how the role mappings in the Enterprise Application, Web application, and EJB containers interact. This setting is valid only for Web applications and EJBs that use the Advanced security model and that initialize roles from deployment descriptors. [More Info...](#)

Use Authorization Providers to Protect JMX Access Configures the WebLogic Server MBean servers to use the security realm's Authorization providers to determine whether a JMX client has permission to access an MBean attribute or invoke an MBean operation. [More Info...](#)

Advanced

Save

Click the **Lock & Edit** button in the Change Center to modify the settings on this page.

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

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: ofsl126_doma

Home > Summary of Deployments > Summary of Security Realms > myrealm > Providers > Summary of Security Realms > myrealm > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings Providers Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping Certification Path Keystores

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure multiple Authentication providers in a security realm. Different types of Authentication providers are designed to access different data stores, such as LDAP servers or DBMS. You can also configure a Realm Adapter Authentication provider that allows you to work with users and groups from previous releases of WebLogic Server.

Customize this table

Authentication Providers

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

Name	Description	Version
<input type="checkbox"/> DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/> DefaultIdentityAsserter	WebLogic Identity Asserter provider	1.0

New Delete Reorder Showing 1 to 2 of 2 Previous | Next

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

ORACLE WebLogic Server® Administration Console

Home Log Out Preferences Record Help Welcome, weblogic Connected to: ofsl126_doma

Home > Summary of Deployments > Summary of Security Realms > myrealm > Providers > Summary of Security Realms > myrealm > Providers

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

The following properties will be used to identify your new Authentication Provider.

* Indicates required fields

The name of the authentication provider.

* **Name:** OfsIDBAuthenticator

This is the type of authentication provider you wish to create.

Type: SQLAuthenticator

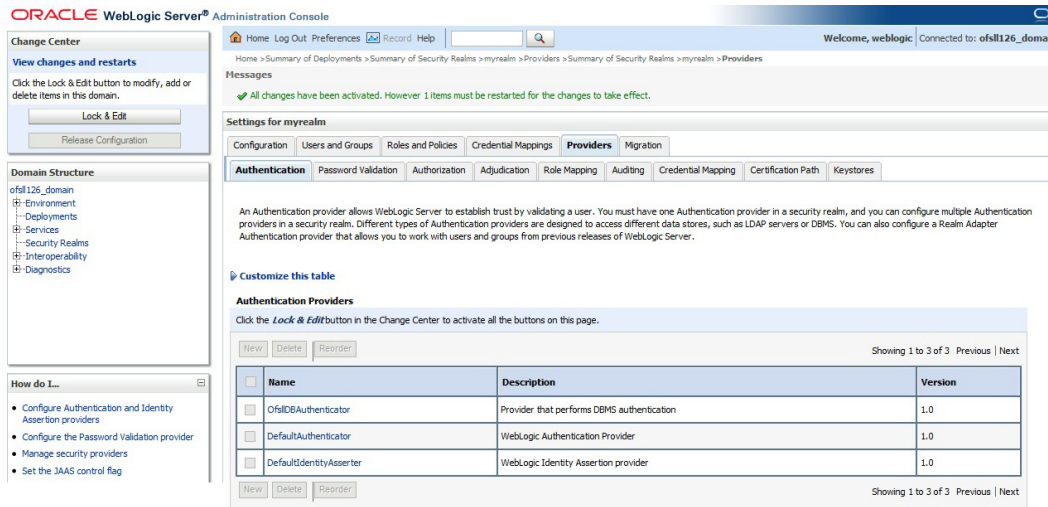
OK Cancel

5. Create Authentication provider with following values.

Name: **OfsIIDBAuthenticator**

Type: **SQLAuthenticator**

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

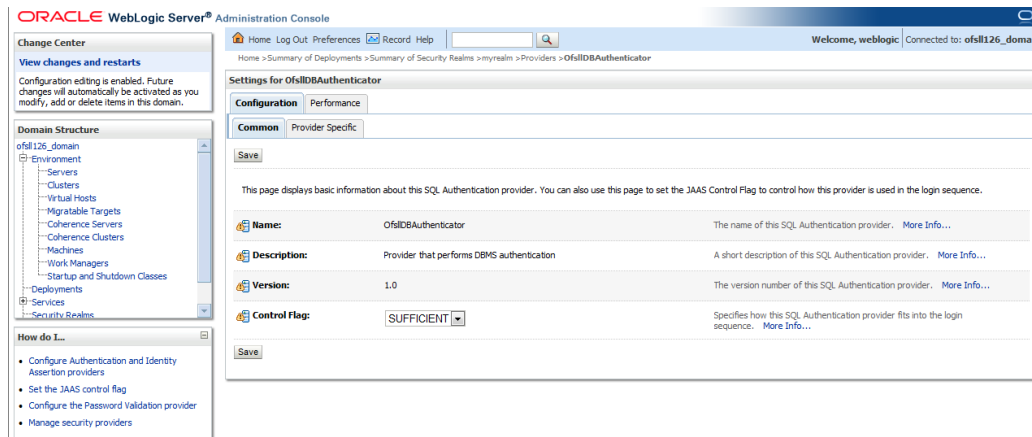


Authentication order should be maintained as mentioned in the above screen.

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

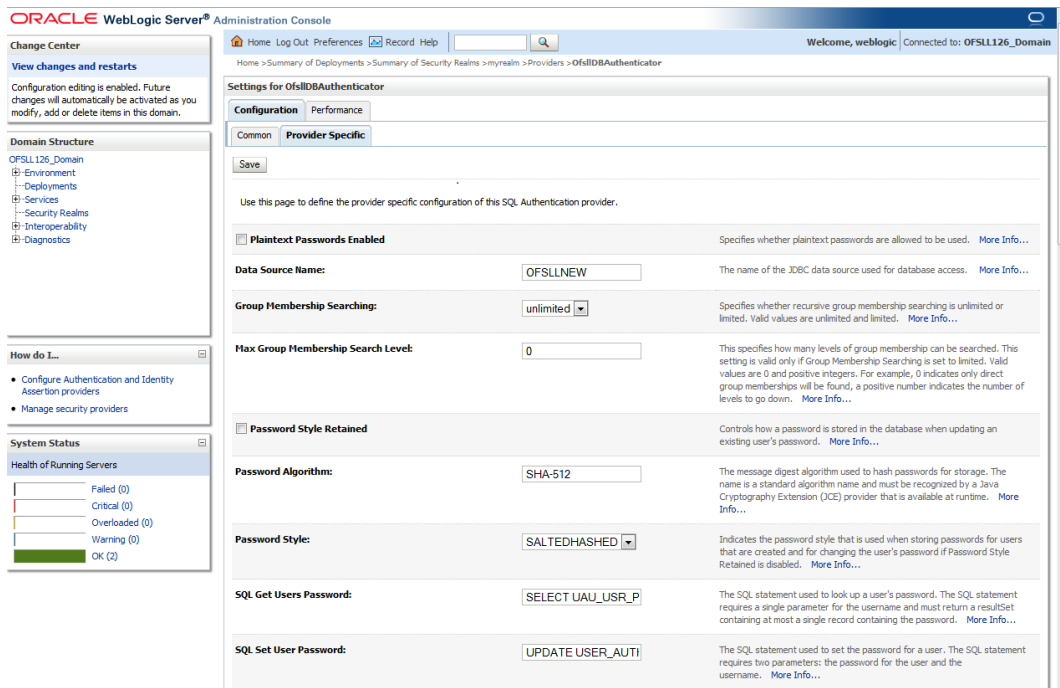
8. Click on **OfsIIDBAuthenticator**.

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 Webllogic	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,U GR_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	OfsIIDBAAuthenticator	

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.

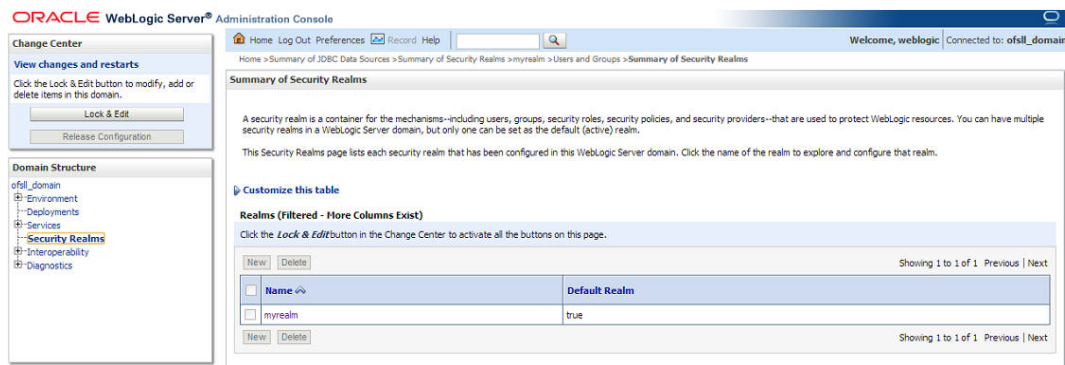
1 row created.

1 row created.

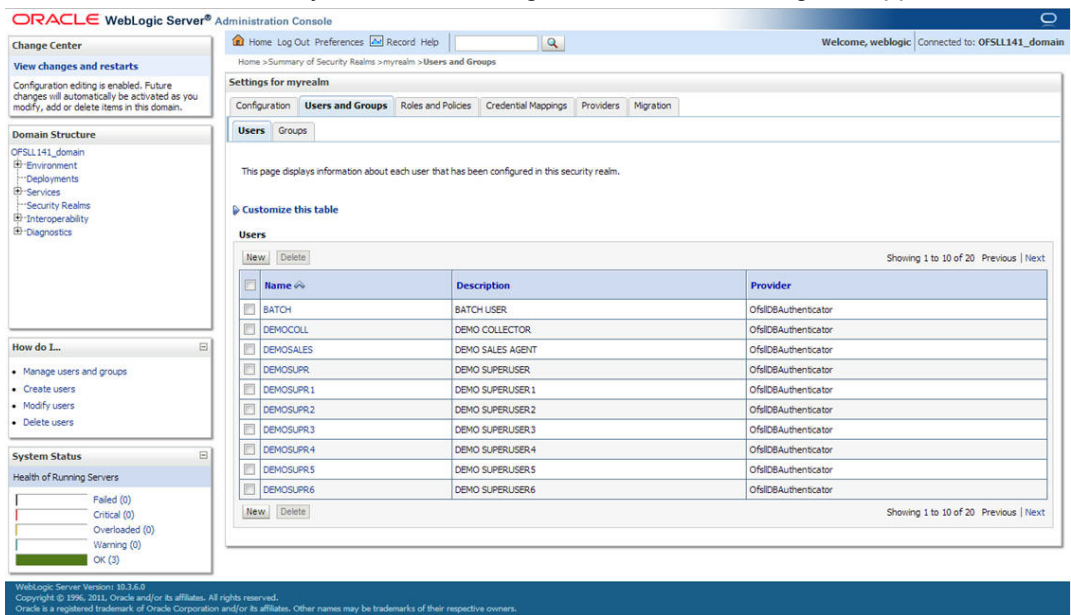
SQL>

```

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



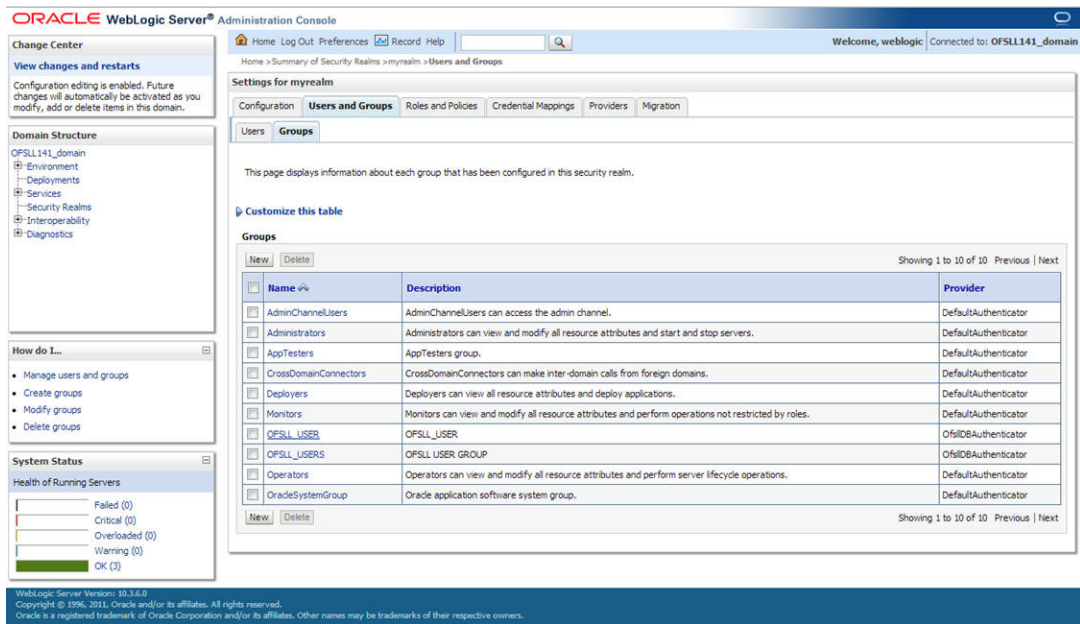
1. Select **Users** tab under **Users and Groups**.
2. If SQLAuthenticator is configured as a Security Provider for the OFSLL application, the Users are automatically created in weblogic when created through an application.



3.7.2 Creating User Groups

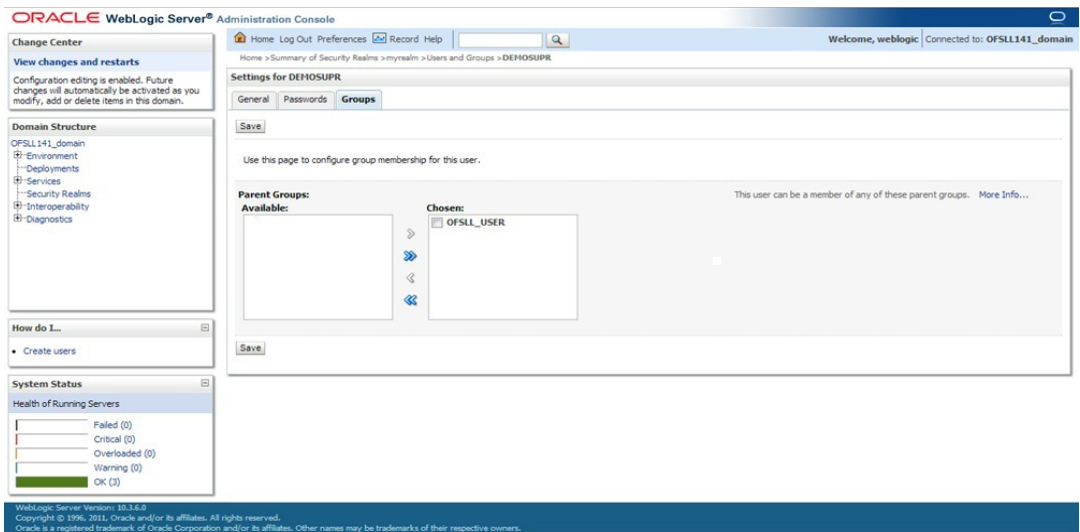
1. Select **Groups** tab under **Users and Groups**.

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



3.7.3 Assigning Users to Groups

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

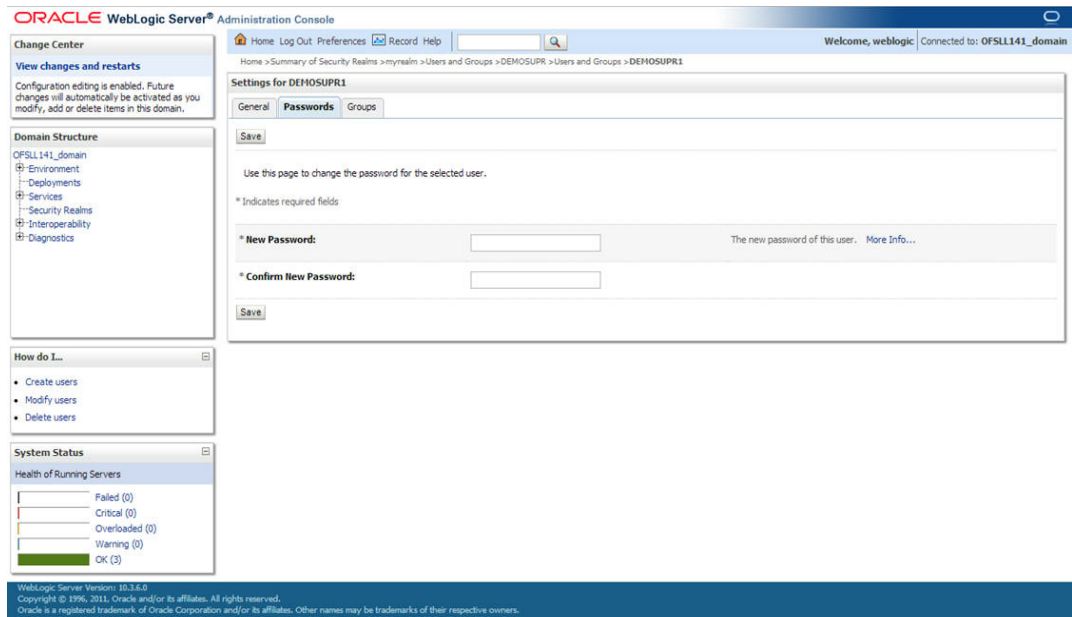


3.7.4 Resetting password

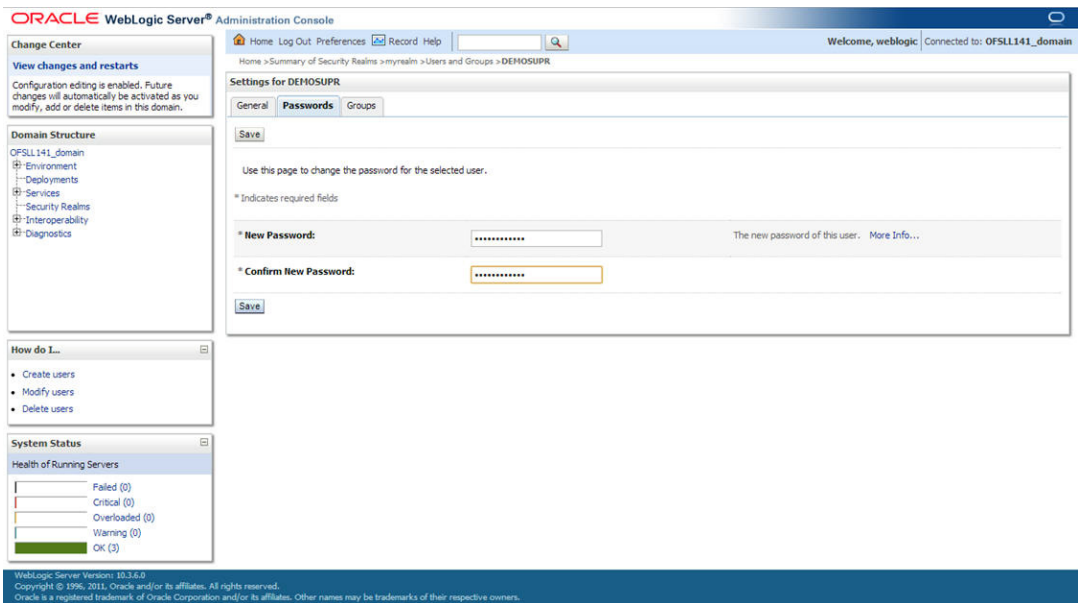
The password for the USER can be reset in weblogic using console or through a sample python script provided with the distribution Media. The script is available in the utils directory of the media with the instructions. The script resets the password of OFSLL users defined within Weblogic Application Server in bulk.

3.7.5 Resetting password via weblogic console

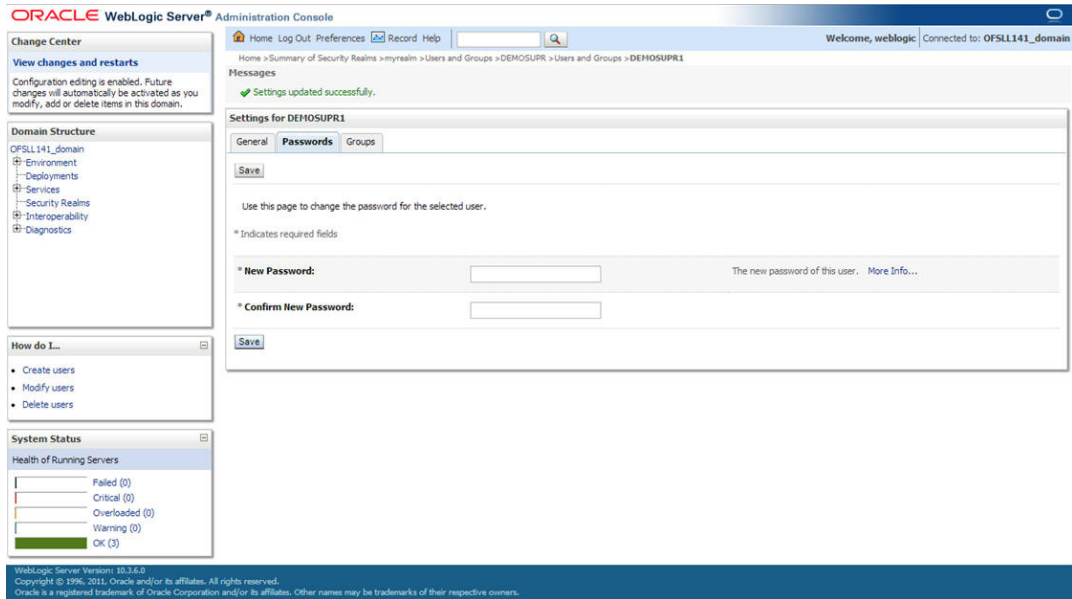
1. Click on **User**. Select **Passwords** tab. The following window is displayed.



2. Enter the new password and confirm password.



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



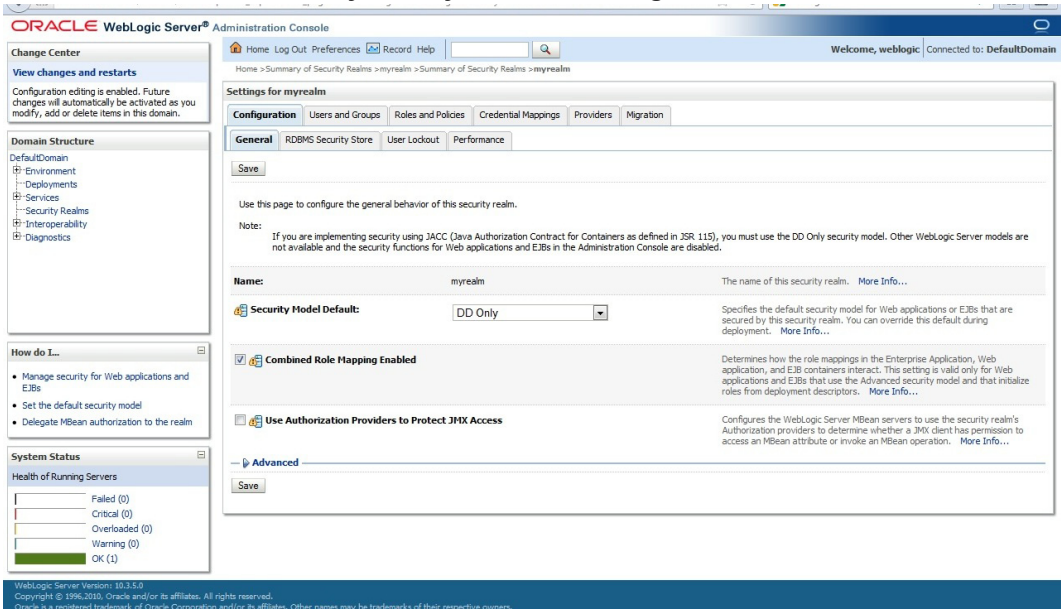
3.8 Implementing JMX Policy for Change Password

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**



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

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for myrealm" and has several tabs: Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers, and Migration. The "Configuration" tab is active, and the "General" sub-tab is selected. A "Save" button is at the top left. Below the "Save" button, there is a note: "Use this page to configure the general behavior of this security realm." Another note states: "If you are implementing security using JACC (Java Authorization Contract for Containers as defined in JSR 115), you must use the DD Only security model. Other WebLogic Server models are not available and the security functions for Web applications and EJBs in the Administration Console are disabled." 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 also checked. There are "Advanced" and "Save" buttons at the bottom.

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

Note

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

The screenshot shows the Oracle WebLogic Server Administration Console. The main content area is titled "Settings for myrealm" and has several tabs: Configuration, Users and Groups, Roles and Policies, Credential Mappings, Providers, and Migration. The "Roles and Policies" tab is active, and the "Realm Policies" sub-tab is selected. Below the "Realm Roles" and "Realm Policies" tabs, there is a note: "Use this table to access or create security policies for this security realm. The Root Level Policies node in the Name column provides access to root level policies (which apply to all resources of a given type). All other nodes provide access to policies that apply to resource instances." Another note states: "This table does not provide access to policies for instances of JNDI resources or Work Context resources. To see these policies, view the Security tab for each JNDI node or Work Context object instance." Below the notes, there is a "Customize this table" button. The "Policies" section contains a table with columns "Name", "Resource Type", and "Policy". The table shows 8 rows: "Deployments", "Domain", "JCOM", "JDBC", "JMS", "JMX Policy Editor", "Root Level Policies", and "Servers". The "JMX Policy Editor" row is highlighted. There are "Create Policy" buttons at the top and bottom of the table. The table shows "Showing 1 to 8 of 8" and "Previous | Next" links.

7. Click on JMX Policy Editor to configure

The screenshot shows the Oracle WebLogic Server Administration Console. The main window is titled "JMX Policy Editor" and contains the following elements:

- Change Center:** A sidebar on the left with sections for "View changes and restarts", "Domain Structure", "How do I...", and "System Status".
- Navigation:** "Home", "Log Out", "Preferences", "Record", "Help" buttons at the top.
- Breadcrumbs:** "Home > Summary of Security Realms > myrealm > Realm Roles > Realm Policies > JMX Policy Editor".
- Buttons:** "Back", "Next", "Create Policy", and "Cancel" buttons.
- Select the Policy Scope:** A section with two bullet points: "To apply this policy to all instances of an MBean, select GLOBAL SCOPE." and "To apply this policy only to an MBean instance that is used to manage a specific deployment or resource, select the deployment or resource."
- Scopes:** A list of scopes with radio buttons: "GLOBAL SCOPE" (selected), "Deployments", "JDBC System Resources", "JMS System Resources", and "WLDJF System Resources".

At the bottom of the console, the version information is displayed: "WebLogic Server Version: 10.3.5.0. Copyright © 1996, 2010, 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."

8. Select GLOBAL SCOPE

9. Click Next

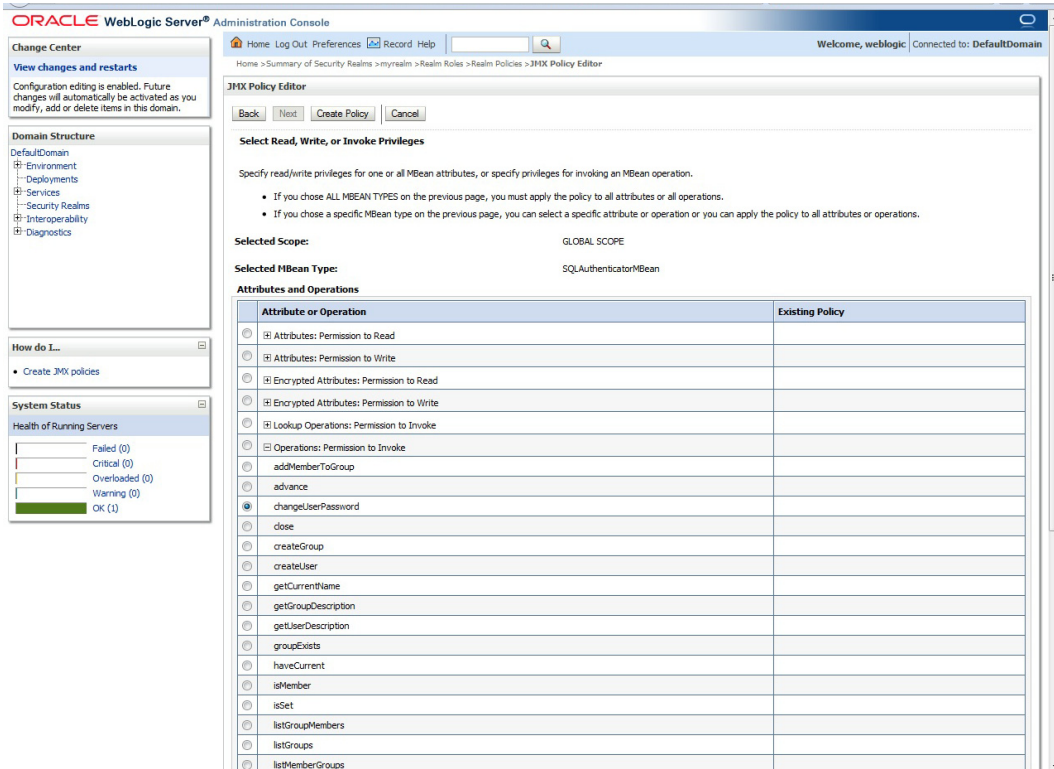
The screenshot shows the "JMX Policy Editor" window with a list of MBeans. The "Next" button is highlighted, indicating the user has moved to the next step. The list of MBeans includes:

- weblogic.management.mbeanservers
- weblogic.management.mbeanservers.domainruntime
- DomainRuntimeServiceMBean
- MBeanServerConnectorManagerMBean
- weblogic.management.mbeanservers.edit
- weblogic.management.mbeanservers.runtime
- weblogic.management.runtime
- weblogic.management.security
- weblogic.management.security.authentication
- weblogic.security.providers.audit
- weblogic.security.providers.authentication
- ActiveDirectoryAuthenticatorMBean
- CustomDBMSAuthenticatorMBean
- DefaultAuthenticatorMBean
- DefaultIdentityAsserterMBean
- IPPlanetAuthenticatorMBean
- LDAPAuthenticatorMBean
- LDAPX509IdentityAsserterMBean
- NegotiateIdentityAsserterMBean
- NovellAuthenticatorMBean
- OpenLDAPAuthenticatorMBean
- OracleInternetDirectoryAuthenticatorMBean
- OracleVirtualDirectoryAuthenticatorMBean
- ReadOnlySQLAuthenticatorMBean
- SQLAuthenticatorMBean
- WindowsNTAuthenticatorMBean
- weblogic.security.providers.authorization
- weblogic.security.providers.credentials
- weblogic.security.providers.pk
- weblogic.security.providers.realmadapter
- weblogic.security.providers.saml
- weblogic.security.providers.xml.authorization

At the bottom of the console, the version information is displayed: "WebLogic Server Version: 10.3.5.0. Copyright © 1996, 2010, 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

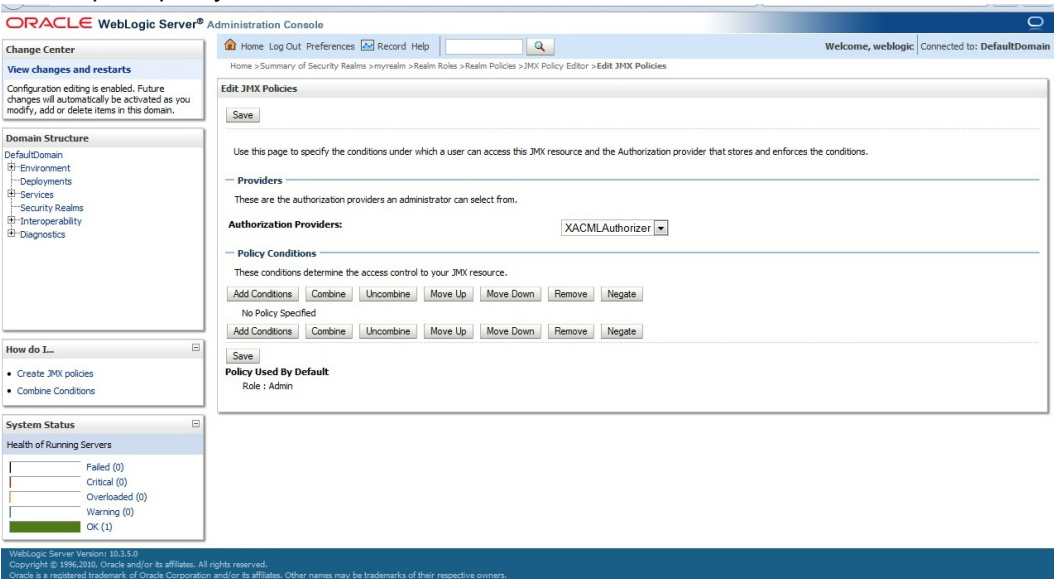
11. Select "SQLAuthenticatorMBean". Click **Next**.



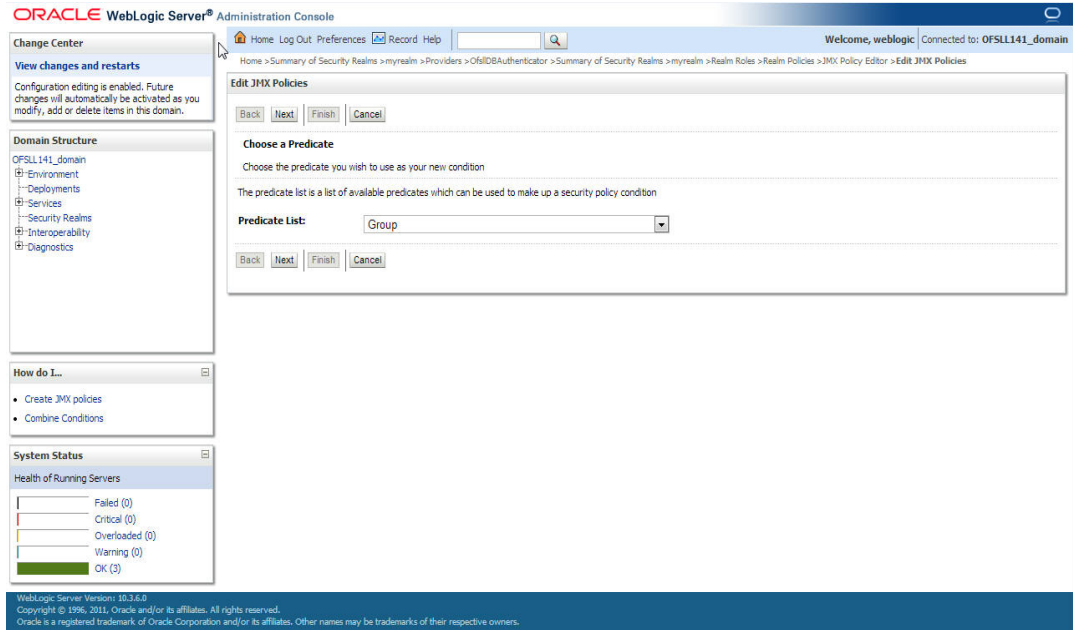
12. Expand "Operations: Permissions to Invoke" and select "ChangePassword"

13. Click "Create Policy"

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

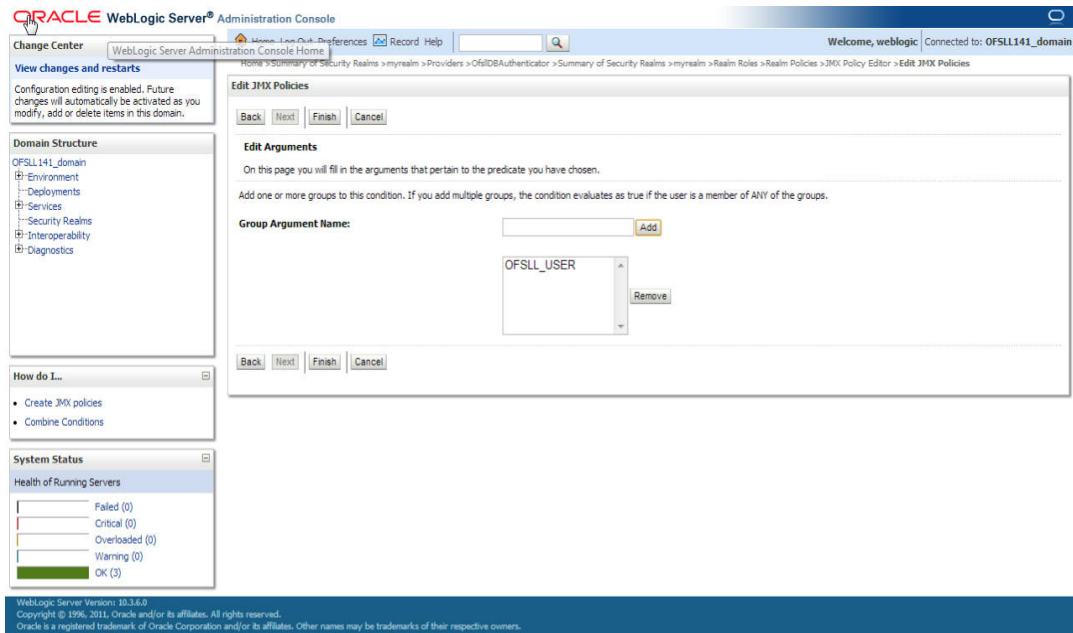


15. Click **Add Condition**. The below screen will be displayed.



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

17. Click **Next**.



18. Select user roles for application.

19. Click **Finish** to complete the configuration.

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
mds-126	Generic	jdbc/mds/126	126_AdminServer, 126_ManagedServer
OFSSLNEW	Generic	jdbc/ofsslDBConnDS	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="ofssl_domain",servertime="DB_ORACLE",datasourcename="jdbc/devopss",jpsroot="cn=opssNode",join="false")
```

datasourcename is the data source created in Step 1.

```
wls:/OFSSL_domain/serverConfig> reassociateSecurityStore(domain="OFSSL_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 breadcrumb trail is: Home > myrealm > Users and Groups > Summary of Security Realms > myrealm > Summary of Security Realms > myrealm > Users and Groups > Realm Roles > Credential Mappings > Providers. The page title is "Settings for myrealm". The "Providers" tab is selected. A table lists the authentication providers:

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
OfsIDBAuthenticator	Provider that performs DBMS authentication	1.0

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

The screenshot shows the Oracle WebLogic Server Administration Console. The breadcrumb trail is: Home > Summary of Security Realms > myrealm > Summary of Security Realms > myrealm > Users and Groups > Realm Roles > Credential Mappings > Providers > OfsIDBAuthenticator > Providers. The page title is "Settings for myrealm". The "Password Validation" tab is selected. A table lists the password validation providers:

Name	Description	Version
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 breadcrumb trail is: Home > myrealm > Summary of Security Realms > myrealm > Users and Groups > Realm Roles > Credential Mappings > Providers > OfsIDBAuthenticator > Providers > SystemPasswordValidator. The page title is "Settings for SystemPasswordValidator". The "Configuration" tab is selected. The "Common" sub-tab is active. The page displays basic information about the System Password Validation provider:

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...

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

<div style="border: 1px solid gray; padding: 5px;"> <p>How do I...</p> <ul style="list-style-type: none"> Configure the Password Validation provider Manage security providers </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;"> <p>System Status</p> <p>Health of Running Servers</p> <p>Failed (0)</p> <p>Critical (0)</p> <p>Overloaded (0)</p> <p>Warning (0)</p> <p>OK (1)</p> </div>	<p>— User Name Policies</p> <p><input type="checkbox"/> Reject if Password Contains the User Name Specifies whether the password can contain, or be set to, the username. More Info...</p> <p><input type="checkbox"/> 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...</p>	
	<p>— Password Length Policies</p> <p>Minimum Password Length: <input type="text" value="8"/> 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...</p> <p>Maximum Password Length: <input type="text" value="0"/> 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...</p>	
	<p>— Character Policies</p> <p>Maximum Instances of Any Character: <input type="text" value="0"/> Specifies the maximum number of times any one character may appear in the password. More Info...</p> <p>Maximum Consecutive Characters: <input type="text" value="0"/> Specifies the maximum number of times that a character may appear consecutively in the password. More Info...</p> <p>Minimum Number of Alphabetic Characters: <input type="text" value="0"/> Specifies the minimum number of alphabetic characters that a password must contain. More Info...</p> <p>Minimum Number of Numeric Characters: <input type="text" value="0"/> Specifies the minimum number of numeric characters that must appear in the password. More Info...</p> <p>Minimum Number of Lower Case Characters: <input type="text" value="0"/> Specifies the minimum number of lowercase characters that a password must contain. More Info...</p> <p>Minimum Number of Upper Case Characters: <input type="text" value="0"/> Specifies the minimum number of uppercase characters that a password must contain. More Info...</p> <p>Minimum Number of Non-Alphanumeric Characters: <input type="text" value="0"/> Specifies the minimum number of non-alphanumeric characters (also known as special characters, such as %, *, #, or ;) that must appear in the password. More Info...</p> <p>Minimum Number of Non-Alphabetic Characters: <input type="text" value="1"/> Specifies the minimum number of numeric or special characters (such as %, *, #, or ;) that a password must contain. More Info...</p> <p style="text-align: right;"><input type="button" value="Save"/></p>	

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

<div style="border: 1px solid gray; padding: 5px;"> <p>How do I...</p> <ul style="list-style-type: none"> Configure the Password Validation provider Manage security providers </div> <div style="border: 1px solid gray; padding: 5px; margin-top: 5px;"> <p>System Status</p> <p>Health of Running Servers</p> <p>Failed (0)</p> <p>Critical (0)</p> <p>Overloaded (0)</p> <p>Warning (0)</p> <p>OK (1)</p> </div>	<p>Note: If the Default Authentication provider is configured in the realm, make sure that the setting for the minimum password length is consistent with the setting configured for that provider.</p> <p>— User Name Policies</p> <p><input type="checkbox"/> Reject if Password Contains the User Name Specifies whether the password can contain, or be set to, the username. More Info...</p> <p><input type="checkbox"/> 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...</p>	
	<p>— Password Length Policies</p> <p>Minimum Password Length: <input type="text" value="8"/> 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...</p> <p>Maximum Password Length: <input type="text" value="20"/> 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...</p>	
	<p>— Character Policies</p> <p>Maximum Instances of Any Character: <input type="text" value="2"/> Specifies the maximum number of times any one character may appear in the password. More Info...</p> <p>Maximum Consecutive Characters: <input type="text" value="0"/> Specifies the maximum number of times that a character may appear consecutively in the password. More Info...</p> <p>Minimum Number of Alphabetic Characters: <input type="text" value="2"/> Specifies the minimum number of alphabetic characters that a password must contain. More Info...</p> <p>Minimum Number of Numeric Characters: <input type="text" value="1"/> Specifies the minimum number of numeric characters that must appear in the password. More Info...</p> <p>Minimum Number of Lower Case Characters: <input type="text" value="1"/> Specifies the minimum number of lowercase characters that a password must contain. More Info...</p> <p>Minimum Number of Upper Case Characters: <input type="text" value="1"/> Specifies the minimum number of uppercase characters that a password must contain. More Info...</p> <p>Minimum Number of Non-Alphanumeric Characters: <input type="text" value="1"/> Specifies the minimum number of non-alphanumeric characters (also known as special characters, such as %, *, #, or ;) that must appear in the password. More Info...</p> <p>Minimum Number of Non-Alphabetic Characters: <input type="text" value="1"/> Specifies the minimum number of numeric or special characters (such as %, *, #, or ;) that a password must contain. More Info...</p> <p style="text-align: right;"><input type="button" value="Save"/></p>	

7. Click Save.

4.2 Configuring User Lockout Policy

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

The screenshot displays the Oracle WebLogic Server Administration Console interface. The main content area is titled "Settings for myrealm" and has several tabs: "Configuration", "Users and Groups", "Roles and Policies", "Credential Mappings", "Providers", and "Migration". The "Configuration" tab is active, and within it, the "User Lockout" sub-tab is selected. The "Lockout Enabled" checkbox is checked. Below this, several configuration parameters are shown with input fields and descriptions:

Parameter	Value	Description
Lockout Threshold	5	The maximum number of consecutive invalid login attempts that can occur before a user's account is locked out.
Lockout Duration	30	The number of minutes that a user's account is locked out.
Lockout Reset Duration	5	The number of minutes within which consecutive invalid login attempts cause a user's account to be locked out.
Lockout Cache Size	5	The maximum number of invalid login records that the server can place in a cache.
Lockout GC Threshold	400	The maximum number of invalid login records that the server keeps in memory.

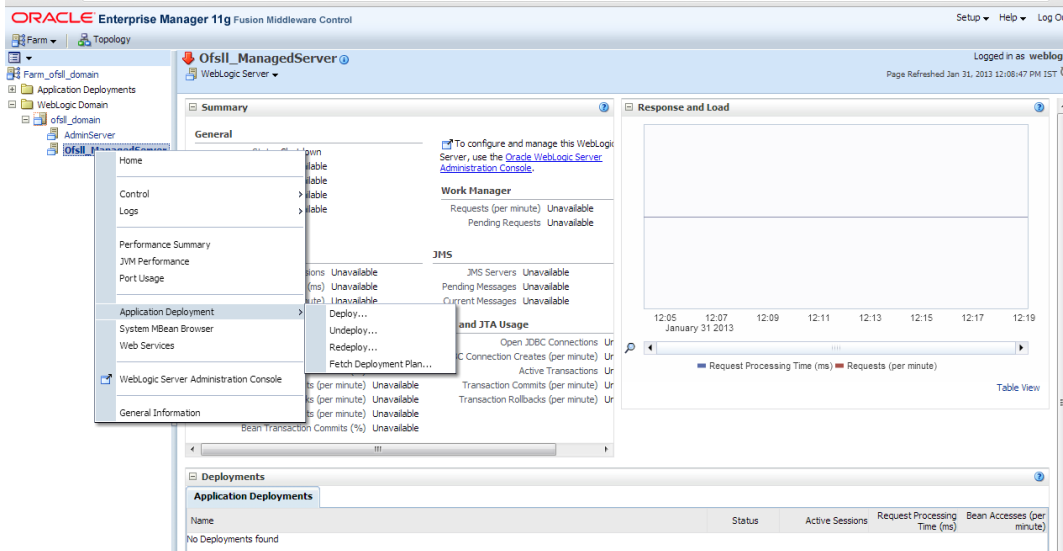
Each parameter has a "More Info..." link next to its description. There are "Save" buttons at the top and bottom of the configuration area.

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

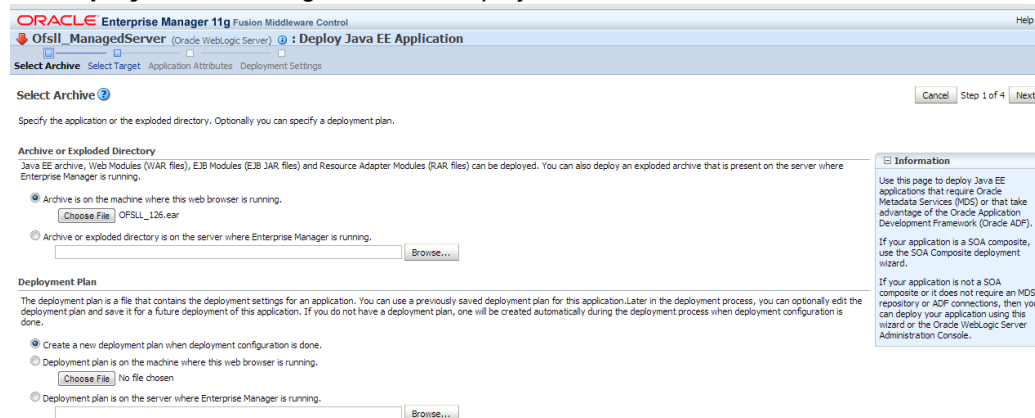
5. Deploying Application

5.1 Deploying Application

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

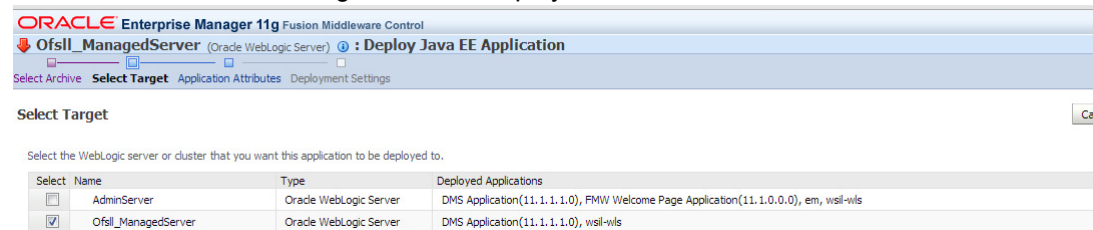


2. Right click on **Ofsll_ManagedServer** in left panel, select **Application Deployment** → **Deploy**. The following window is displayed.



3. Click Choose File button and select OFSSL application archive file i.e. OFSSL_141.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.

The screenshot shows the 'Application Attributes' window in Oracle Enterprise Manager 11g. The window title is 'Ofsll_ManagedServer (Oracle WebLogic Server) : Deploy Java EE Application'. The main content area is titled 'Application Attributes' and includes the following sections:

- Archive Information:** Archive Type: Java EE Application (EAR file); Deployment Plan: Create a new plan; Deployment Target: Ofsll_ManagedServer.
- Application Name and Version:** Application Name: OFSLL_126; Archive Version: V12.6.0.0-0-0171; Deployment Plan Version: (empty).
- Context Root of Web Modules:** A table with two columns: Web Module and Context Root. The row shows 'ofsll126.war' and 'ofsll126'.
- Target Metadata Repository:** A section with the instruction 'Select the metadata repository and specify the partition in the repository that the application will be deployed to.' It includes fields for Repository Name (Not specified in archive), Repository Type, and Partition.
- Distribution:** Radio buttons for 'Distribute and start application (servicing all requests)', 'Distribute and start application in administration mode (servicing only administration requests)', and 'Distribute only'.
- Other Options:** A section for 'Source Accessibility' with radio buttons for 'Use the defaults defined by the deployment's targets. Recommended selection.' and 'Copy this application onto every target. During deployment, the files will be copied automatically to the managed servers to which the application is targeted.'

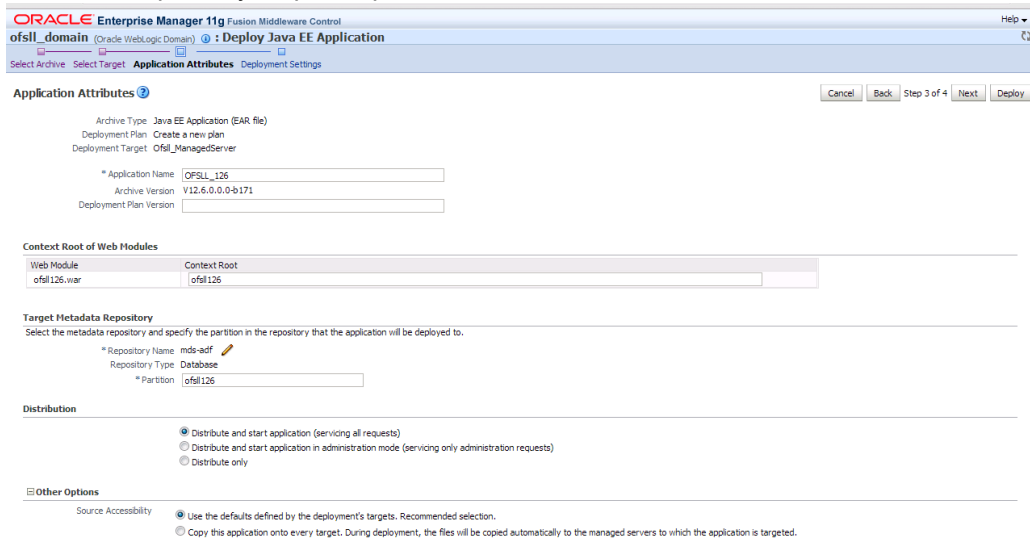
7. Click button to select Repository Name. The following window is displayed.

The screenshot shows the 'Metadata Repositories' dialog box. The title bar reads 'Metadata Repositories'. The main text says 'Select the metadata repository that the application will be deployed to.' Below this is a 'Repository' dropdown menu with 'mds-adf' selected. Underneath is a 'Repository Details' section with the following information:

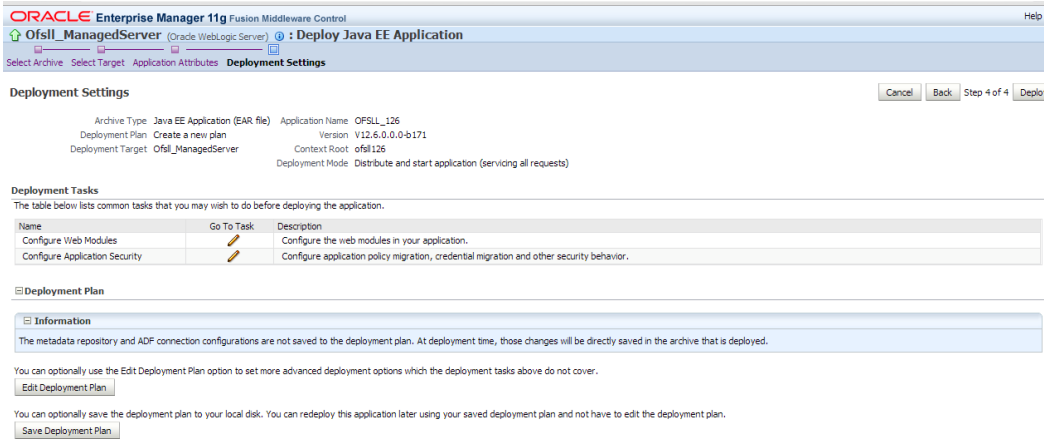
Name	mds-adf
Type	Database
JNDI Location	jdbc/mds/adf
Database Type	Oracle
Database Name	OFSLLD
Database User	DEV_MDS
JDBC URL	jdbc:oracle:thin:@ofss220059.in.oracle.com:1521/OFSLLD

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

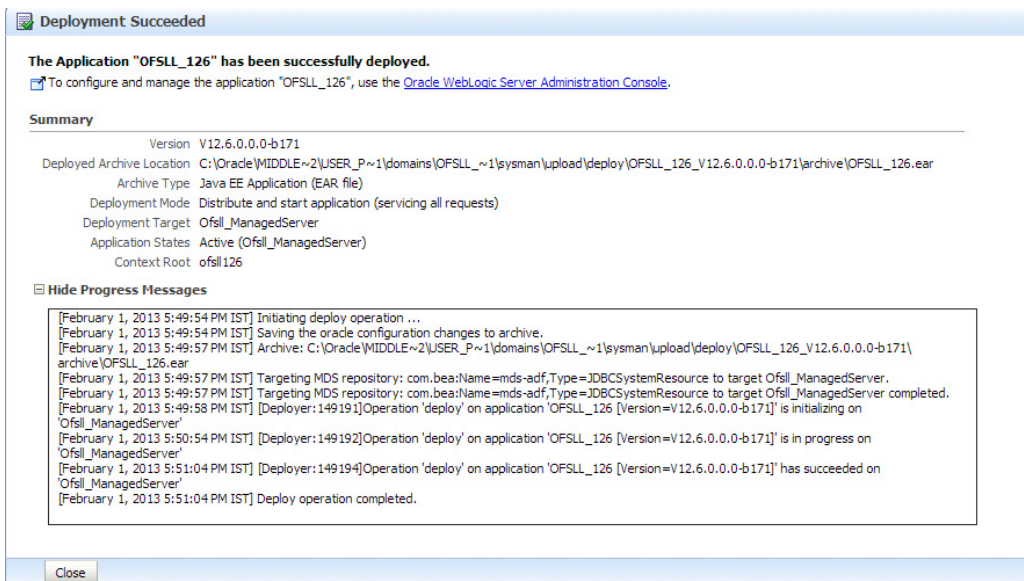
8. Select Repository as per requirement and click **OK**.



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 content area shows the 'Summary' tab for the 'Ofssl_ManagedServer'.

General Information:

- 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:

- 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

JDBC and JTA Usage:

- Open JDBC Connections: 0
- JDBC Connection Creates (per minute): 0.00
- Active Transactions: 0
- Transaction Commits (per minute): 0.00
- Transaction Rollbacks (per minute): 0.00

Response and Load Graph:

The graph shows 'Request Processing Time (ms)' and 'Requests (per minute)' over time. The Y-axis ranges from 0.0 to 1.0. The X-axis shows time points from 17:39 to 17:51. The 'Requests (per minute)' series is a flat line at 0.0. The 'Request Processing Time (ms)' series is a flat line at approximately 0.05.

Deployments Table:

Name	Status	Active Sessions	Request Processing Time (ms)	Bean Accesses (per minute)
Internal Applications				
OfSSL_126(V12.6.0.0.0-b171)	↑	0	0	0.00

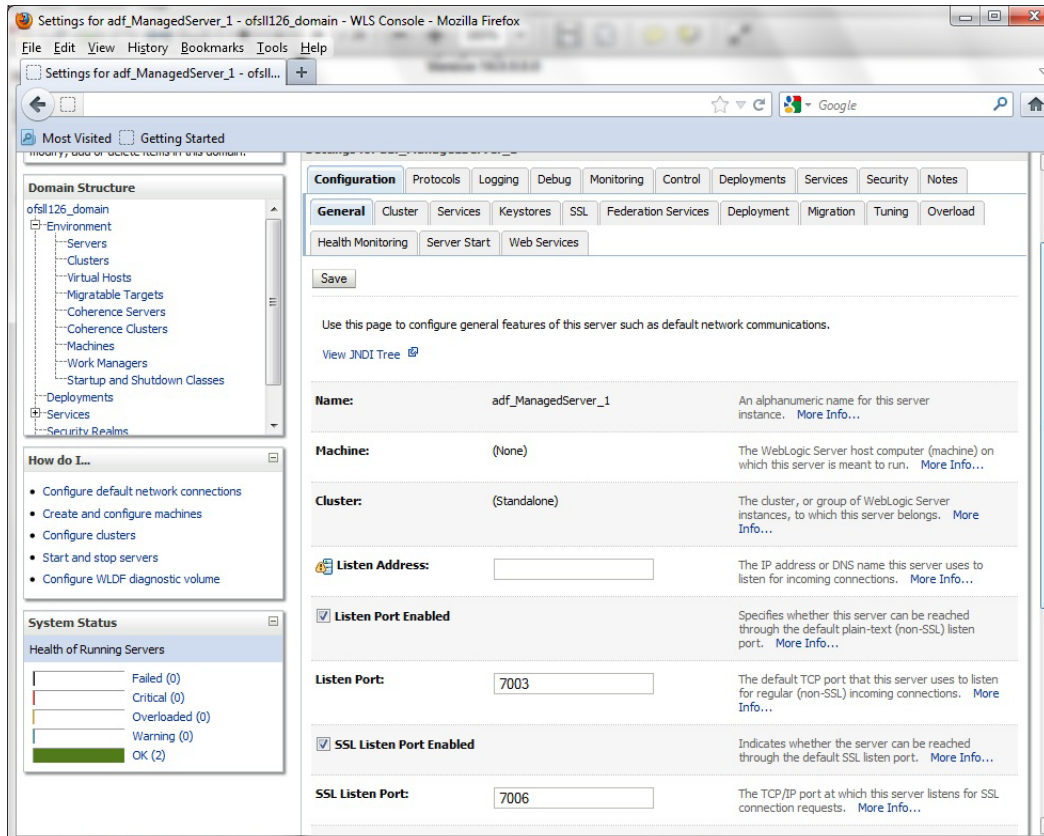
5.2

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.



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.

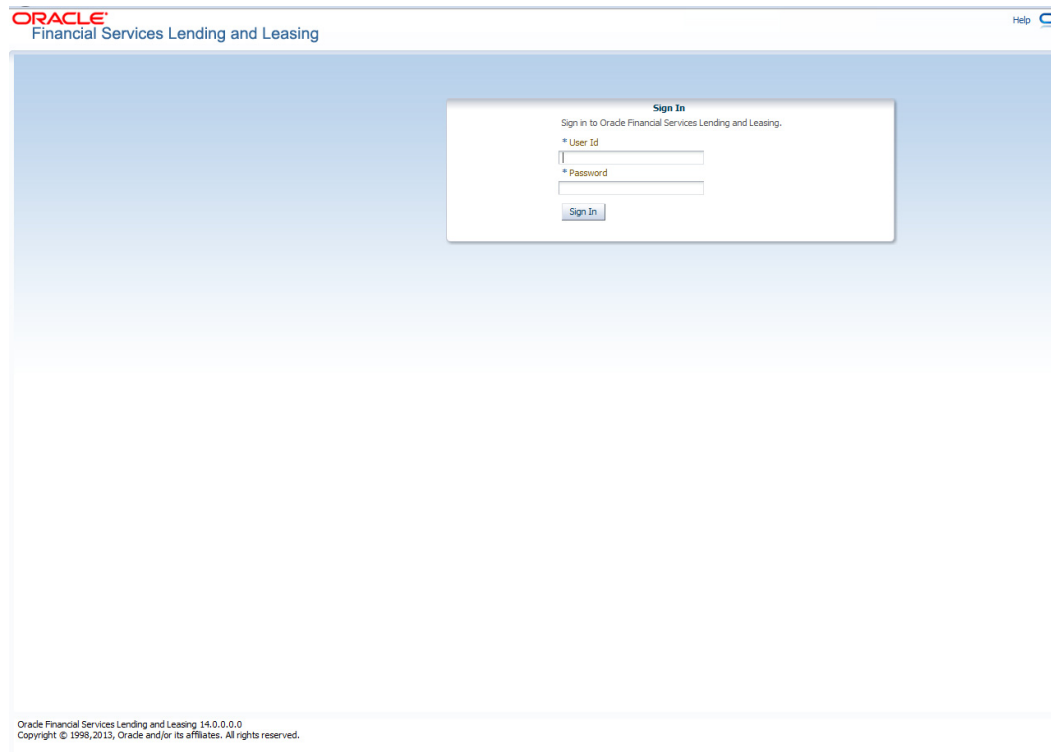
The screenshot shows the Oracle WebLogic Server Administration Console interface. The main content area is titled "Summary of Deployments" and includes a "Control" tab. Below this, there is a table of deployed applications. The table has columns for Name, State, Health, Type, and Deployment Order. The OFSLL application is listed with a state of "Active" and a health status of "OK".

Name	State	Health	Type	Deployment Order
DMS Application (11.1.1.1.0)	Active	OK	Web Application	5
em	Active	OK	Enterprise Application	400
FMW Welcome Page Application (11.1.0.0.0)	Active	OK	Enterprise Application	5
OFSLL126 (V12.6.0.0.0-b171)	Active	OK	Enterprise Application	150
wsl-ils	Active	OK	Enterprise Application	5

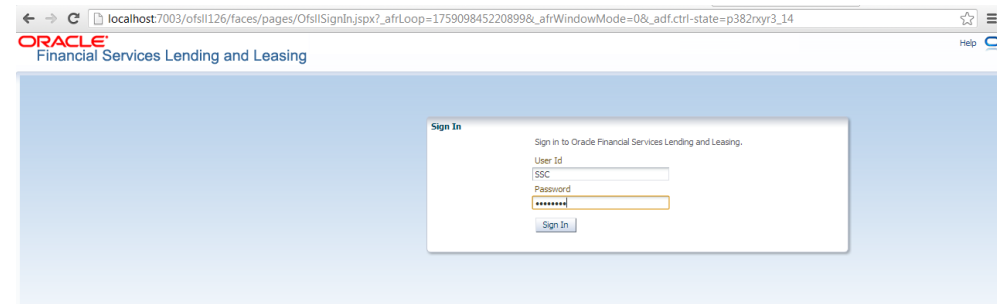
2. The URL of the OFSLL application will be

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

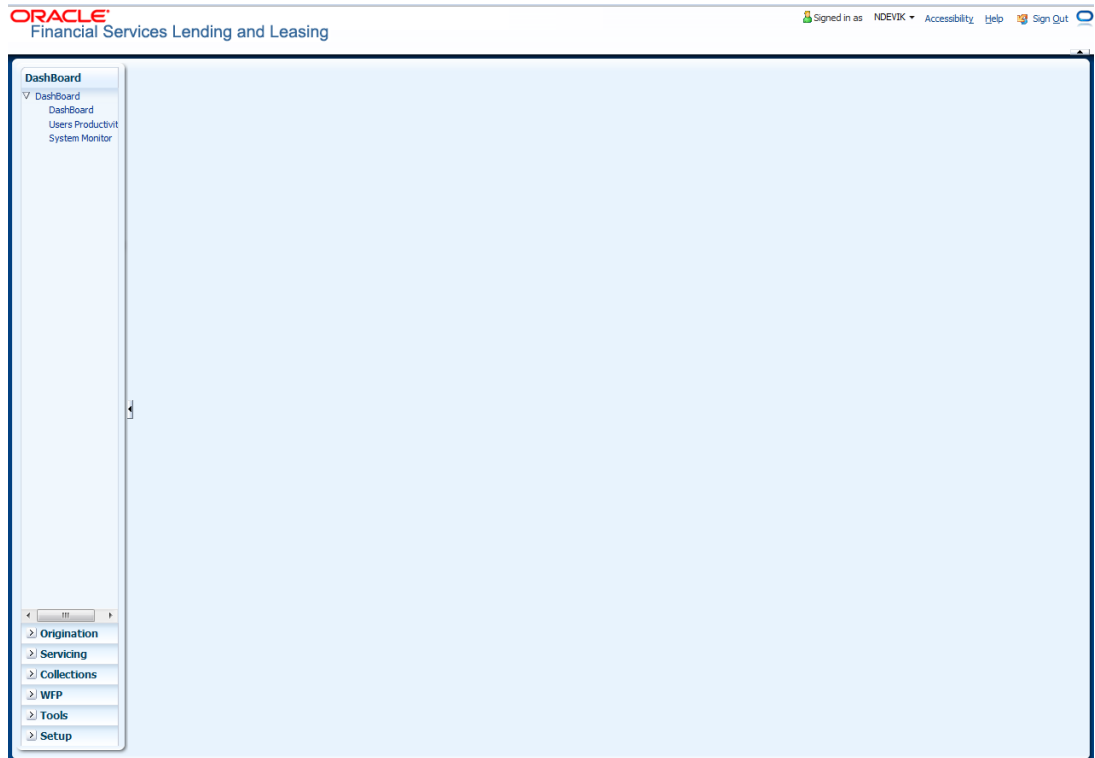
(eg. <https://localhost:7003/ofsl140/faces/pages/OfslSignIn.jspx>)



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



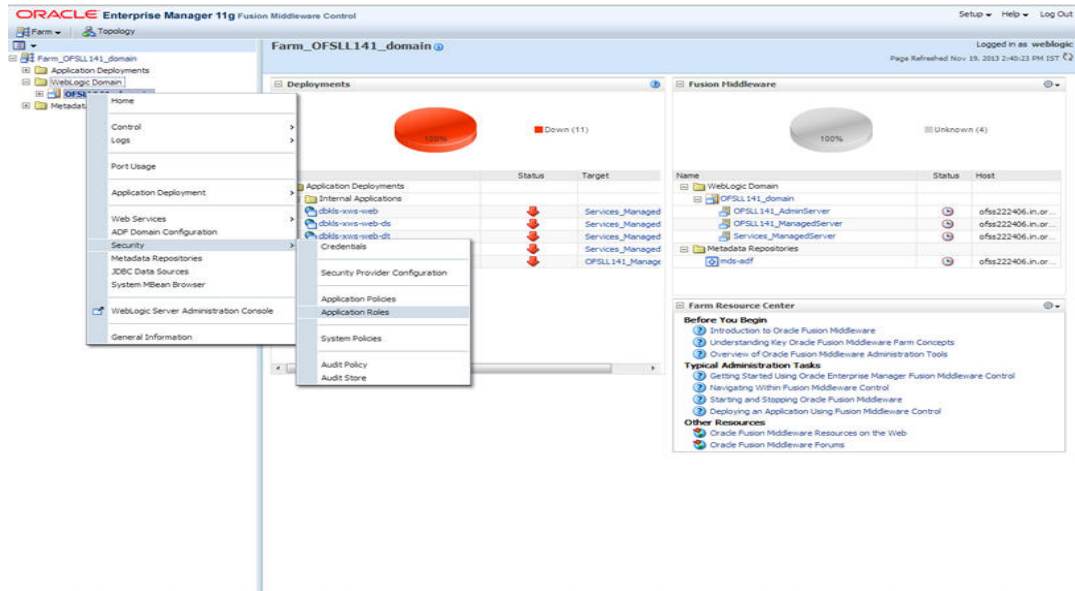
4. After successful login, the following screen is displayed



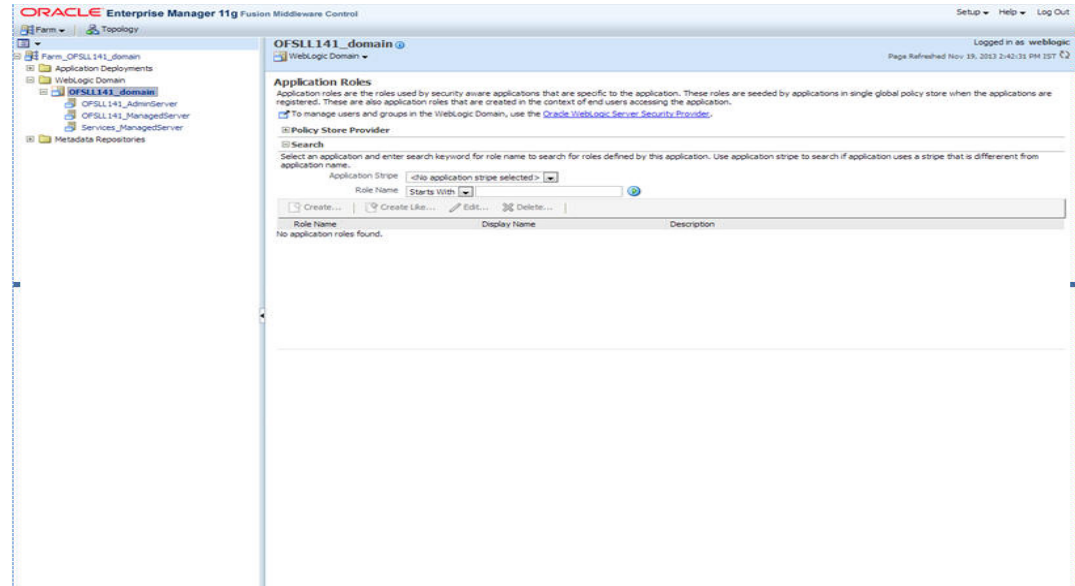
8. Mapping of Enterprise Group with Application Role

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..

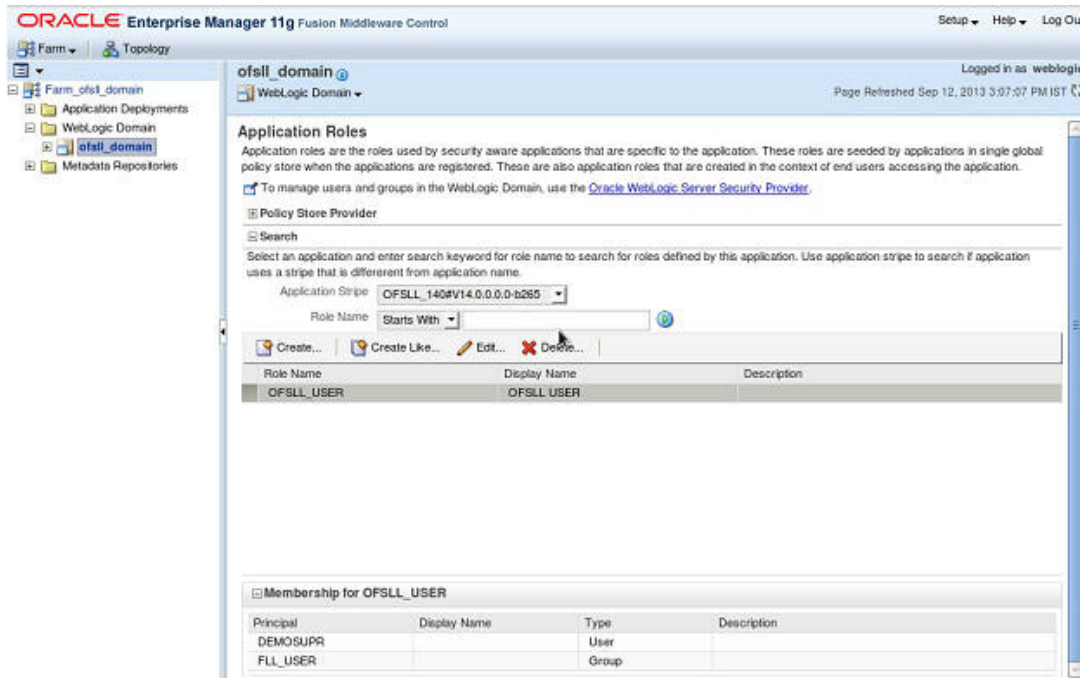


3. On clicking **Application Roles**, the following screen is displayed:

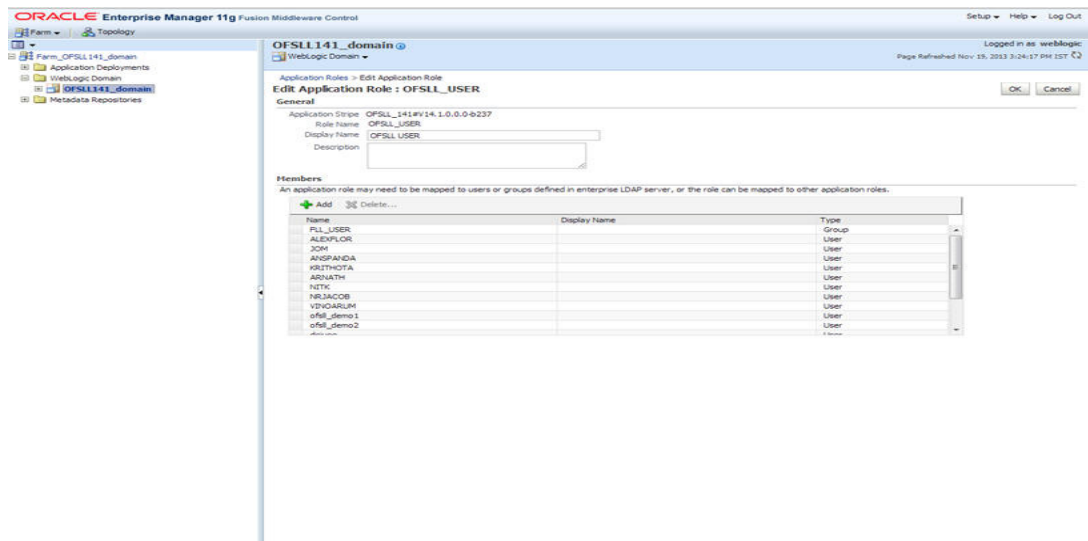


4. Select **Application Stripe** from the drop-down menu.
5. Click the arrow head button. Details of the existing Roles are displayed below.

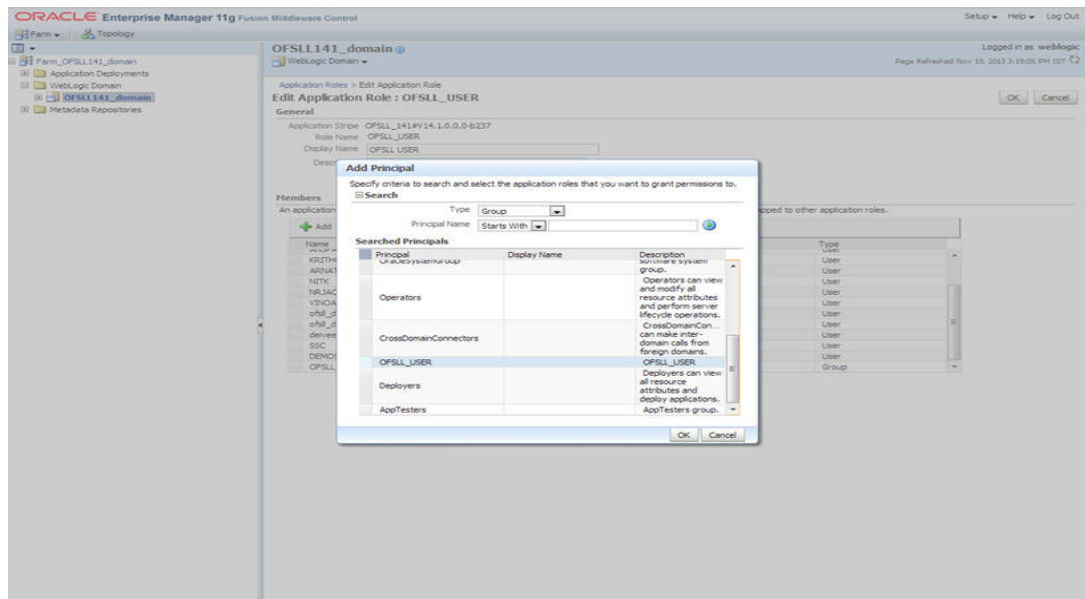
- Select the **Role Name**. Membership details of the selected Role Name are displayed under **Membership for "role_name"...**



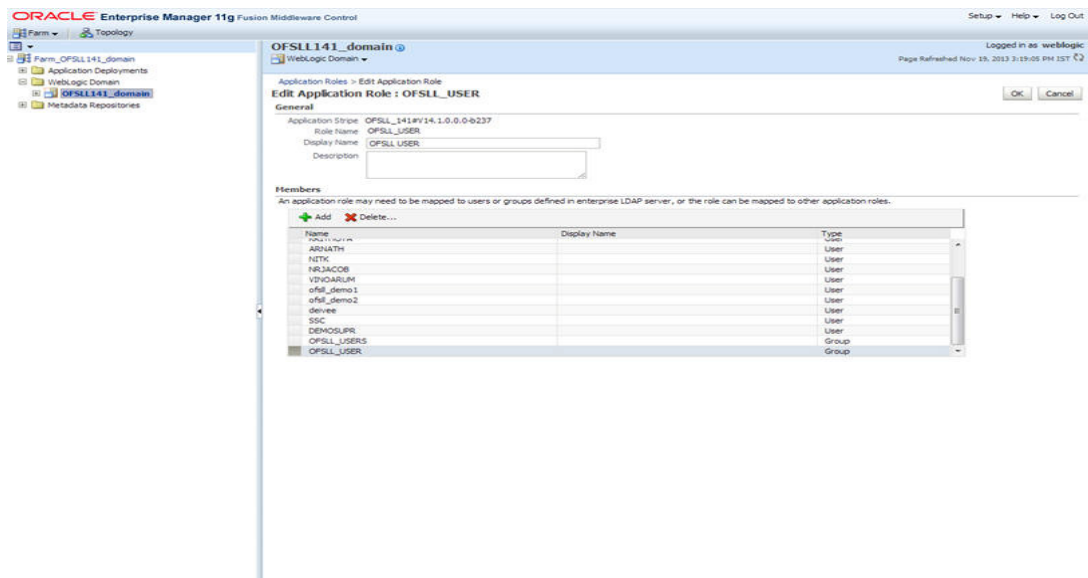
- Click **Edit**. The following window is displayed.



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



9. Select the Principal "OFSSL_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”.

The screenshot shows the Oracle Enterprise Manager 11g Fusion Middleware Control interface. The left-hand navigation pane shows the tree structure: Farm -> Topology -> Farm_OFSLL141_domain -> Application Deployments -> WebLogic Domain -> OFSLL141_domain. The main content area is titled "OFSLL141_domain" and "WebLogic Domain". At the top right, it says "Logged in as weblogic" and "Page Refreshed Nov 19, 2013 3:31:35 PM EST".

An information message at the top states: "An application role OFSLL_USER has been updated." Below this is the "Application Roles" section, which includes a description and a link to the Oracle WebLogic Server Security Provider. The "Policy Store Provider" section has a search field with the application stripe "OFSLL_141ev14.1.0.0.0-6237". Below the search field are buttons for "Create...", "Create Like...", "Edit...", and "Delete...".

A table below the search section shows the application roles:

Role Name	Display Name	Description
OFSLL_USER	OFSLL_USER	

At the bottom, the "Membership for OFSLL_USER" section shows a table of principals:

Principal	Display Name	Type	Description
FL_USER		Group	
ALEXFLOR		User	
XOM		User	
ANSPANDA		User	

9. Configuring Oracle BI Publisher for Application

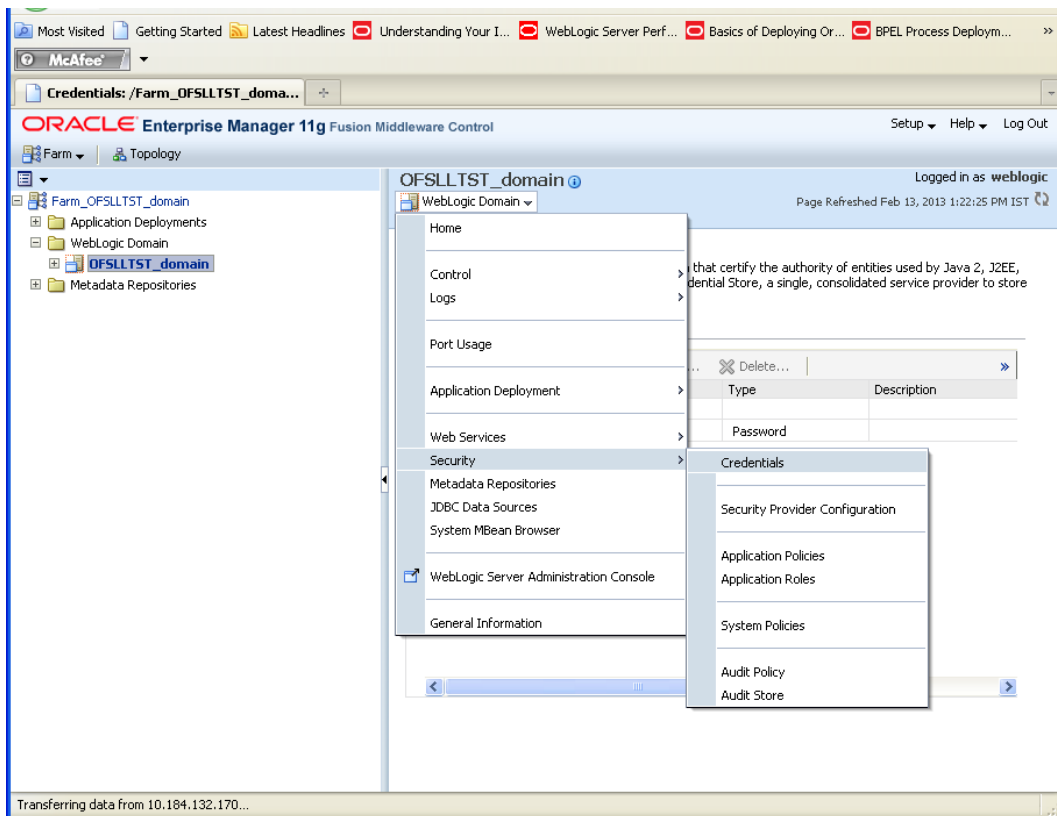
1. Copy the OfsslCommonCSF.jar from /WEB-INF/lib available in the staging area to \$DOMAIN_HOME/lib
2. Update the setDomainEnv.sh file (\$MW_HOME/user_projects/domains/mydomain/bin directory) by appending the above jar file path –

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

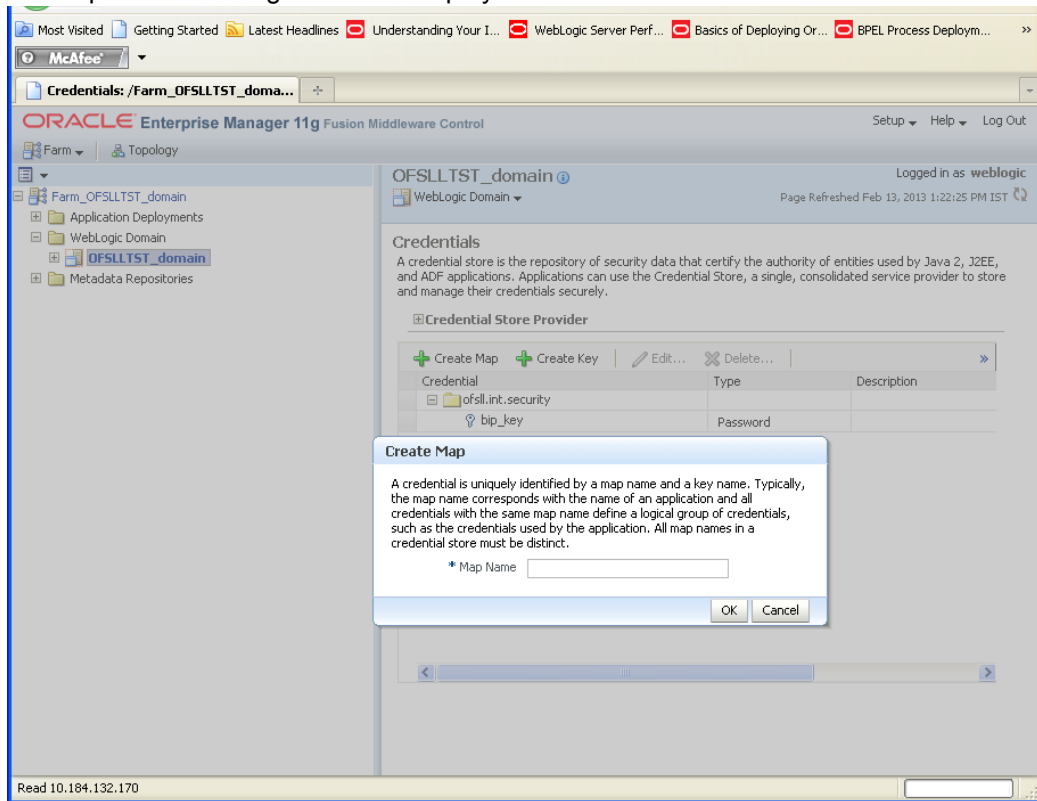
3. Configure Security via EMconsole

Note

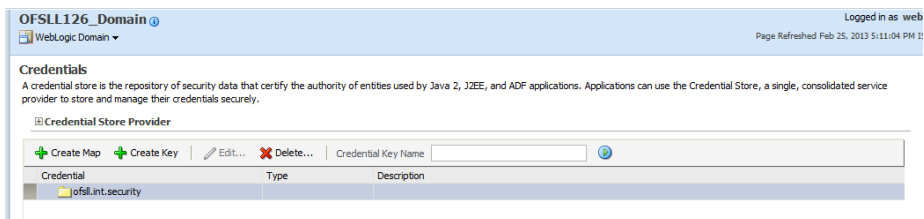
It is assumed that BI Publisher is installed and configured. Refer BI Publisher Guide for further details.



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



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



7. Click **Create Key** Button.

The following window is displayed.

Create Key

Select Map: ofssl.int.security

* Key:

Type: Password

* User Name:

* Password:

* Confirm Password:

Description:

OK Cancel

8. Enter the details as per your requirement.

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

Create Key

Select Map: ofssl.int.security

* Key: bip_key

Type: Password

* User Name: weblogic

* Password: ●●●●●●

* Confirm Password: ●●●●●●

Description:

OK Cancel

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

OFSLL126_Domain | WebLogic Domain | Logged in as weblo | Page Refreshed Feb 25, 2013 5:11:04 PM IST

Information
The credential key, bip_key, has been created.

Credentials
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.

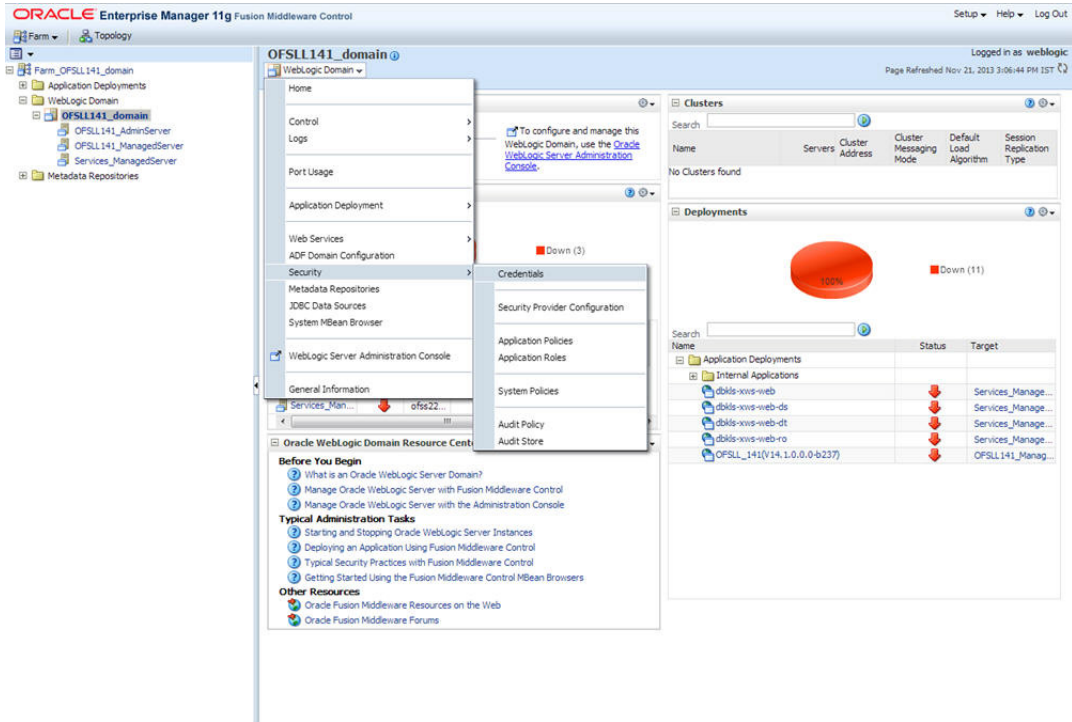
Credential Store Provider

Create Map | Create Key | Edit... | Delete... | Credential Key Name:

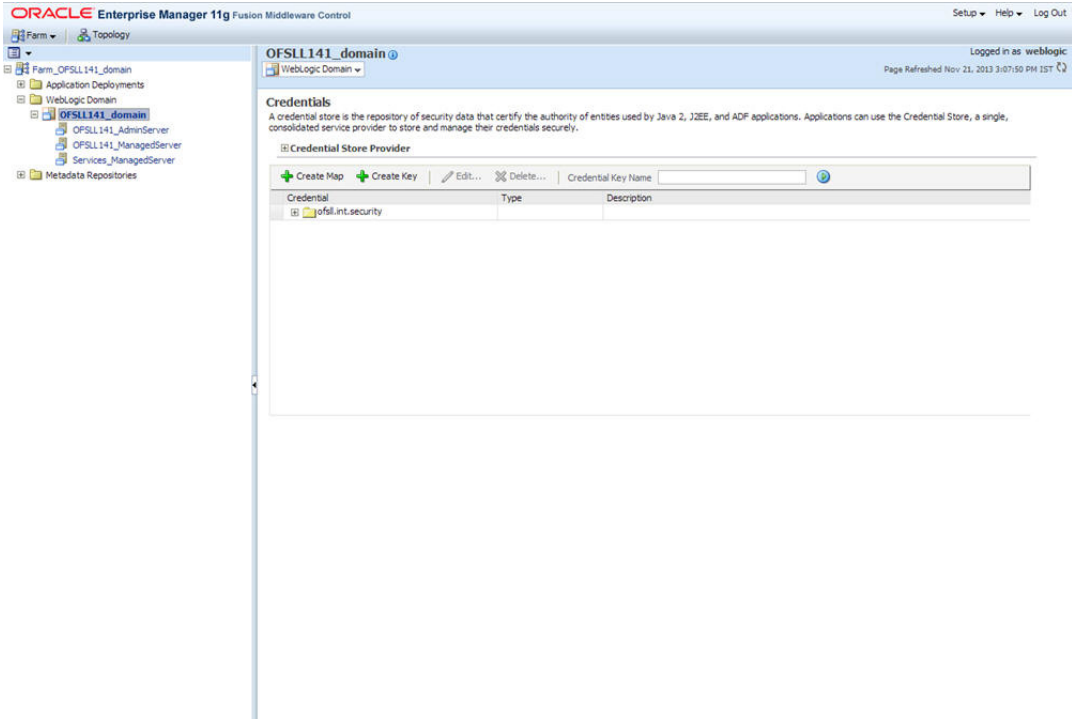
Credential	Type	Description
ofssl.int.security		
bip_key	Password	

10. Configuring JNDI name for HTTP Listener

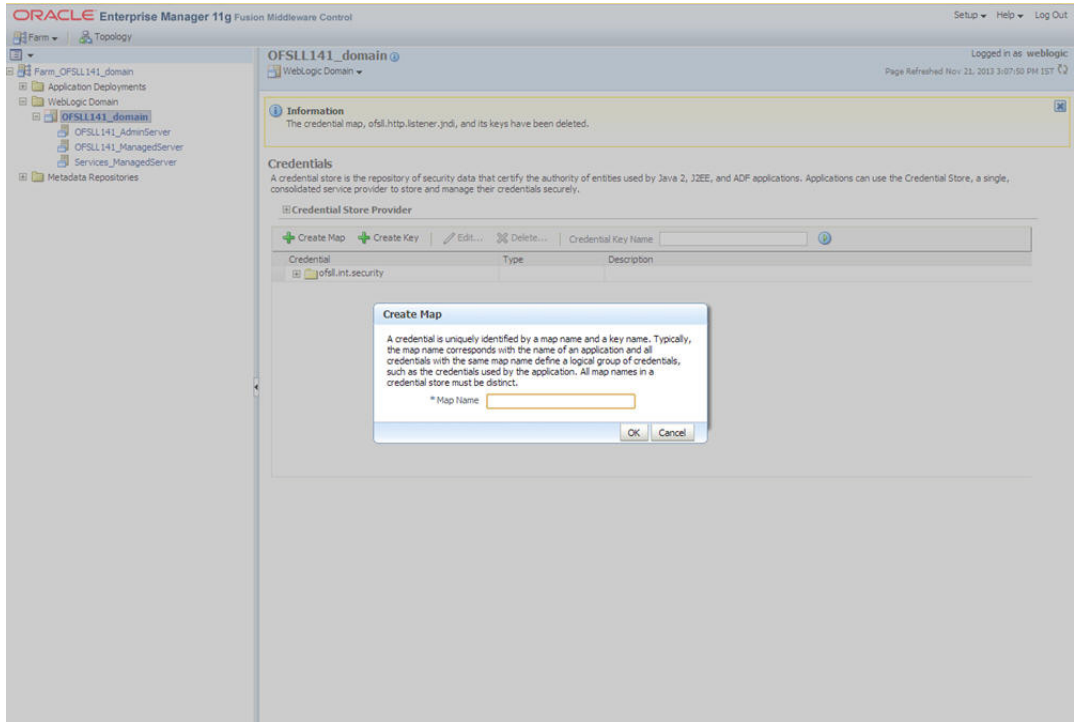
1. Click **WebLogic Domain** on the right panel. Select **Security** → **Credentials**.



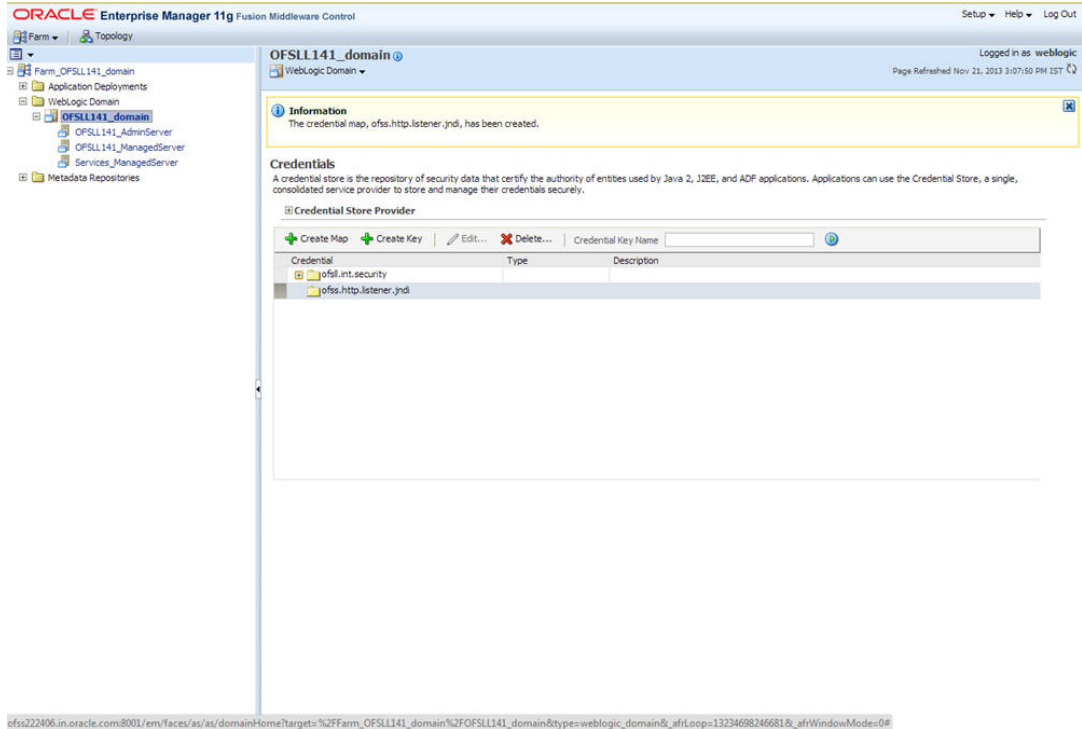
2. On clicking **Credentials** the following window is displayed.



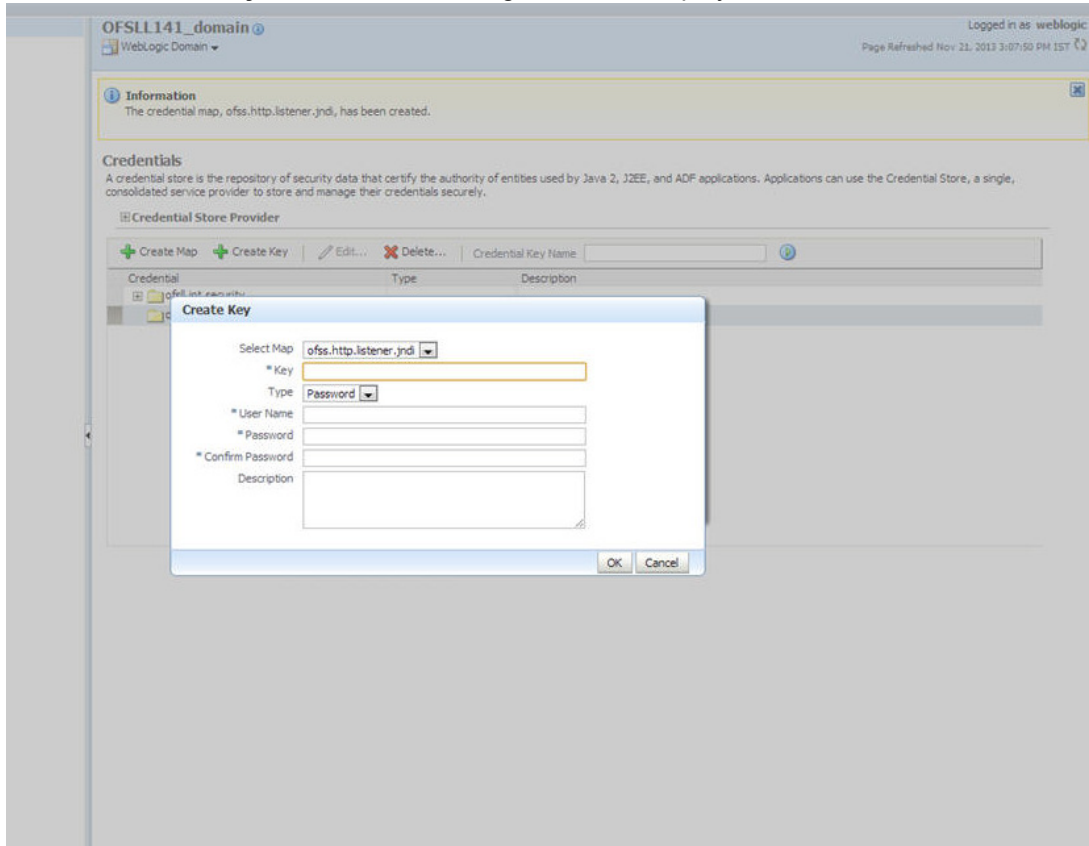
3. Click on **Create Map**. The following window is displayed.



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.

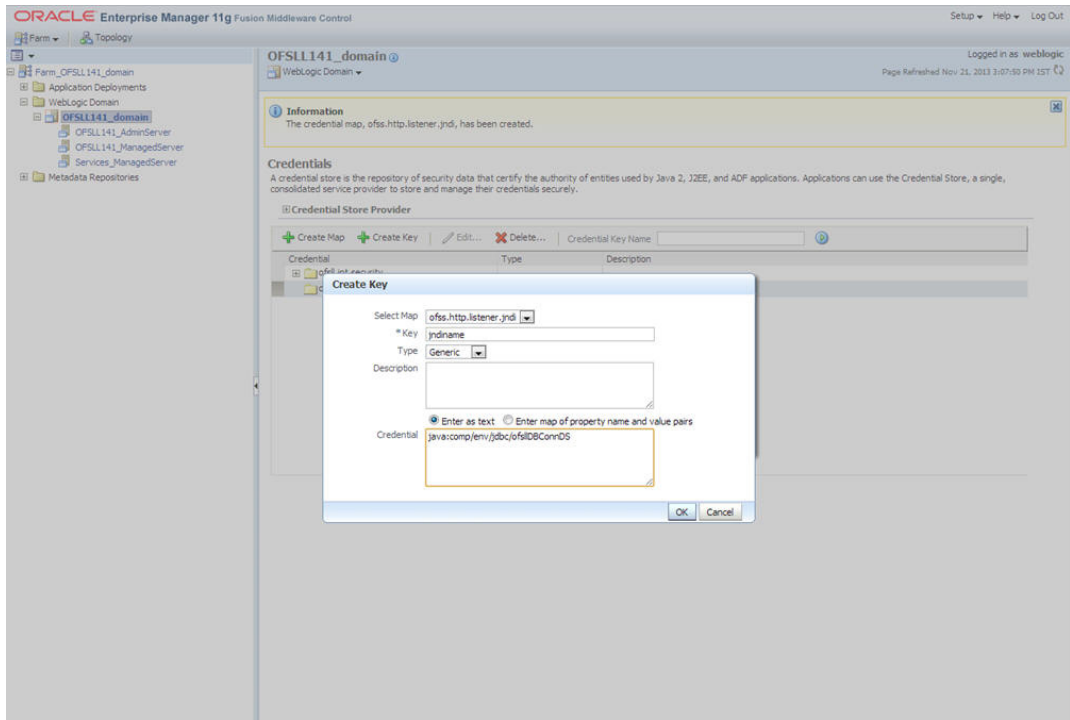


7. Enter the details as per your requirement.

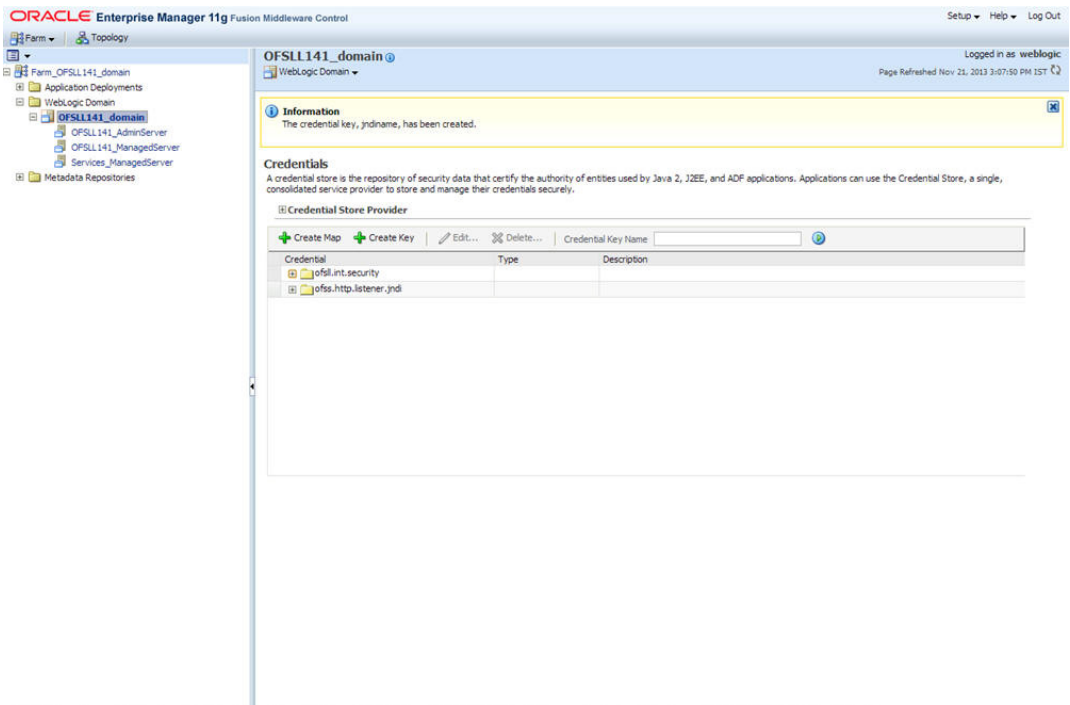
Key: jndiname

Credential: java:comp/env/jdbc/ofslIDBConnDS

Type:Generic



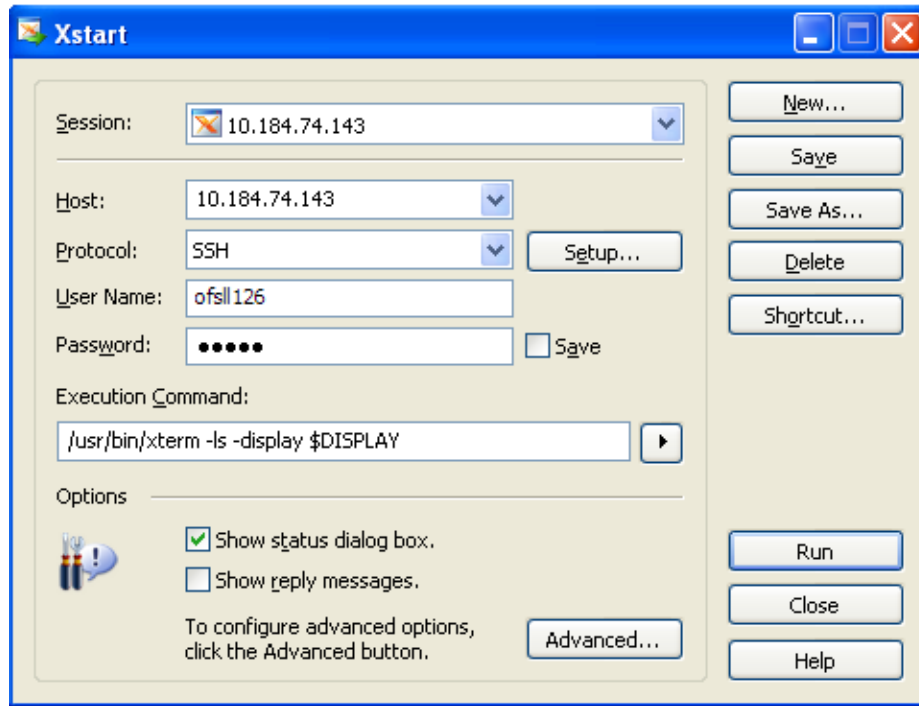
8. Click **OK**. The following window is displayed.



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

11.1 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