Oracle® Retail Store Inventory Management

Installation Guide
Release 14.0.2
E60693-02

February 2015

ORACLE

Oracle® Retail Store Inventory Management Installation Guide, Release 14.0.2

Contributors: Nathan Young

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via™** licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex™** licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Send Us Your Comments

Oracle Retail Store Inventory Management, Installation Guide, Release 14.0.2

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

> **Note:** Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at www.oracle.com.

Preface

Oracle Retail Installation Guides contain the requirements and procedures that are necessary for the retailer to install Oracle Retail products.

Audience

This Installation Guide is written for the following audiences:

- Database administrators (DBA)
- System analysts and designers
- Integrators and implementation staff

Related Documents

For more information, see the following documents in the Oracle Retail Store Inventory Management Release 14.0.2 documentation set:

- *Oracle Retail Store Inventory Management Release Notes*

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

https://support.oracle.com

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Review Patch Documentation

When you install the application for the first time, you install either a base release (for example, 14.0) or a later patch release (for example, 14.0.2). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times **not** be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-**02** is an updated version of a document with part number E123456-**01**.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Documentation is packaged with each Oracle Retail product release. Oracle Retail product documentation is also available on the following Web site:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

(Data Model documents are not available through Oracle Technology Network. These documents are packaged with released code, or you can obtain them through My Oracle Support.)

Documentation should be available on this Web site within a month after a product release.

Conventions

Navigate: This is a navigate statement. It tells you how to get to the start of the procedure and ends with a screen shot of the starting point and the statement "the Window Name window opens."

```
This is a code sample
    It is used to display examples of code
```

1

Preinstallation Tasks

This chapter discusses the tasks to complete before installation.

Implementation Capacity Planning

There is significant complexity involved in the deployment of Oracle Retail applications, and capacity planning is site specific. Oracle Retail strongly suggests that before installation or implementation you engage your integrator (such as the Oracle Retail Consulting team) and hardware vendor to request a disk sizing and capacity planning effort.

Sizing estimates are based on a number of factors, including the following:

- Workload and peak concurrent users and batch transactions
- Hardware configuration and parameters
- Data scarcity
- Application features utilized
- Length of time history is retained

Additional considerations during this process include your high availability needs as well as your backup and recovery methods.

Upgrading SIM

SIM 14.0.2 is a patch installation. It is possible to upgrade SIM 14.0.1 installation to version SIM 14.0.2.

Requesting Infrastructure Software

If you are unable to find the necessary version of the required Oracle infrastructure software (database server, application server, WebLogic, etc.) on the Oracle Software Delivery Cloud, you should file a non-technical 'Contact Us' Service Request (SR) and request access to the media. For instructions on filing a non-technical SR, see My Oracle Support Note 1071023.1 – *Requesting Physical Shipment or Download URL for Software Media*.

Check Supported Database Server Requirements

General Requirements for a database server running SIM include:

Supported On	Versions Supported
Database Server OS	OS certified with Oracle Database 11gR2 Enterprise Edition. Options are: ▪ Oracle Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 7.1 (Actual hardware or LPARs) ▪ Solaris 11 SPARC (Actual hardware or logical domains) ▪ HP-UX 11.31 Integrity (Actual hardware, HPVM, or vPars)
Database Server	Oracle Database Enterprise Edition 11gR2 (11.2.0.4) with the following specifications: **Components:** ▪ Oracle Partitioning ▪ Examples CD **Oneoff Patches:** ▪ 18465025: MERGE REQUEST ON TOP OF 11.2.0.4.0 FOR BUGS 18016963 18302329. **Other components:** ▪ Perl interpreter 5.0 or later ▪ X-Windows interface

Check Supported Application Server Requirements

The SIM application must be deployed on Oracle WebLogic 10.3.6

> **Note:** SIM is certified to work with only Oracle Internet Directory LDAP server (OID), as specified in the Application Server Requirements section of the SIM Installation Guide. The sample, unsupported .ldif files that SIM includes are provided only as reference.

General requirements for an Oracle WebLogic Server capable of running the SIM application include the following.

Supported on:	Versions Supported:
Application Server OS	OS certified with Oracle Fusion Middleware 11g Release 1 (11.1.1.7). Options are: ▪ Oracle Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 6 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 7.1 (Actual hardware or LPARs) ▪ Solaris 11 SPARC (Actual hardware or logical domains) ▪ HP-UX 11.31 Integrity (Actual hardware, HPVM, or vPars)
Application Server	Oracle Fusion Middleware 11g Release 1 (11.1.1.7) **Components:** ▪ Oracle WebLogic Server 11g Release 1 (10.3.6) ▪ Oracle Identity Management 11g Release 1 (11.1.1.7) ▪ ADF 11.1.1.7 ▪ Oracle Enterprise Manager **Note:** Oracle Internet Directory (OID) is the supported LDAP directory for Oracle Retail products. For alternate LDAP directories, refer to Oracle WebLogic documentation set. **Java:** ▪ JDK 1.7+ 64 bit **IMPORTANT**: If there is an existing WebLogic installation on the server, you must upgrade it to WebLogic 10.3.6. All middleware components associated with WebLogic server should be upgraded to 11.1.1.7. **Optional (required for SSO**) ▪ Oracle WebTier 11g (11.1.1.7) Oracle Access Manager 11g Release 1 (11.1.1.7) Note: A separate WebLogic 10.3.5 installation is required for Oracle Access Manager 11g. ▪ Oracle Access Manager Agent (WebGate) 11g Release 1 (11.1.1.7)

Check Single Sign-On Requirements

If SIM is not being deployed in a Single Sign-On environment, skip this section.

If Single Sign-On is to be used, verify the Oracle Identity Management 11gR1 version 11.1.1.7 has been installed along with the components listed in the above Application Server requirements section. Verify the Oracle WebTier Server is registered with the Oracle Access Manager 11gR1 as a partner application.

Check Directory Server Requirements

SIM uses directory server based user authentication and searching. For LDAP, SIM is supported with the following directory servers:

- Oracle Identity Management 11gR1 version 11.1.1.7

Check Third-Party Software Dependencies

- Oracle Retail Wireless Foundation Server, provided by Wavelink 5.x.

Check Client PC and Web Browser Requirements

Requirement	Versions
Operating system	Windows 7
Display resolution	1024x768 or higher
Processor	1GHz or higher
Memory	512MBytes or higher
Oracle (Sun) Java Runtime Environment (JRE)	Java 1.7+
Browser	Microsoft Internet Explorer 11 (Upgraded from 9) Mozilla Firefox 24(upgraded from 17) The browser is used to launch the Java WebStart client.

Note: Oracle Retail does not recommend or support installations with less than 128 kb bandwidth available between the PC client and the data center. Limiting the client to less than 128 kb total available bandwidth causes unpredictable network utilization spikes, and performance of the client degrades below requirements established for the product. The 128 kb requirement provides reasonable, predictable performance and network utilization.

Supported Oracle Retail Products

The following Oracle Retail products can be integrated with SIM. Next to each product is an indication of whether it is required or optional for SIM to function properly:

- Retail Integration Bus (RIB) 14.0 and all subsequent patches and hot fixes – Required

  Although typically used to integrate SIM with RMS, RIB can also be used to integrate SIM with other merchandising systems.

  > **Note:** RIB requires custom modifications to use a merchandising system other than RMS.

- Retail Merchandising System (RMS) 14.0.2 – Optional
- Oracle Retail Price Management 14.0.2 – Optional
- Oracle Retail POS Suite 14.0.2 – Optional

The above products can be installed before or after SIM. However, it is helpful to know the connection details for the other products ahead of time so that you can provide them to the SIM application installer, which will configure the connection points for you.

> **Note:** If integrating SIM with RSL, having SIM and RSL servers configured in the same domain is recommended. If the RSL server is installed in a different domain, you must set up a "trusted relationship" between the two WebLogic domains for RMI calls.

UNIX User Account Privileges to Install the Software

A UNIX user account is needed to install the software. The UNIX user that is used to install the software should have write access to the WebLogic server installation files.

For example, "oretail."

> **Note:** Installation steps will fail when trying to modify files under the WebLogic installation unless the user has write access.

SIM Installation Overview

The following basic steps are required to install and set up SIM for the first time.

1. Install the database (with or without RAC).
2. Install application server (WebLogic) if it has not been installed
3. Install the SIM database schema
4. Set role-based access control. See Chapter 3 of the *Oracle Retail Store Inventory Management Implementation Guide, Volume 1* for instructions.
5. Install the SIM application.
6. Run data-seeding from RMS (Applicable only if SIM integrate with RMS)

2

RAC and Clustering

The Oracle Retail Store inventory Management System has been validated to run in two configurations on Linux:

- Standalone Oracle Application Server or Web Logic Server and Database installations
- Real Application Cluster Database and Oracle Application Server or Web Logic Server Clustering

The Oracle Retail products have been validated against an 11.2.0.4 RAC database. When using a RAC database, all JDBC connections should be configured to use THIN connections rather than OCI connections.

Clustering for Web Logic Server 10.3.6 is managed as an Active-Active cluster accessed through a Load Balancer. Validation has been completed utilizing a RAC 11.2.0.4 Oracle Internet Directory database with the Web Logic 10.3.6 cluster. It is suggested that a Web Tier 11.1.1.7 installation be configured to reflect all application server installations if SSO will be utilized.

References for Configuration:

- Oracle® Fusion Middleware High Availability Guide 11g Release 1 (11.1.1) Part Number E10106-09
- Oracle® Real Application Clusters Administration and Deployment Guide 11g Release 2 (11.2) Part Number E16795-11

3

Database Installation Tasks

Expand the SIM Database Schema Installer Distribution

1. Log in to the UNIX server as a user which has sufficient access to run sqlplus from the Oracle Database installation.
2. Create a new staging directory for the SIM database schema installer distribution (sim-database-change.zip). There should be a minimum of 50 MB disk space available for the database schema installation files. This location is referred to as INSTALL_DIR for the remainder of this chapter.
3. Copy sim-database-change.zip to <INSTALL_DIR> and extract its contents.

Required Database Character Set

SIM 14.0.2 databases should be created with the AL32UTF8 database character set. This will ensure support for characters of all languages supported by SIM and ensure proper integration with other Oracle Retail applications.

Patching the Database

This step will upgrade your database from version 14.0.1 to version 14.0.2

1. Expand the sim-database-change.zip file into <INSTALL_DIR> if not already done.
2. Set the following environment variables:
   - Set the ORACLE_HOME to point to an installation that contains sqlplus. It is recommended that this be the ORACLE_HOME of the SIM database.
   - Set the PATH to: $ORACLE_HOME/bin:$PATH
   - Set the ORACLE_SID to the name of your database
   - Set the NLS_LANG for proper locale and character encoding

     Example: Export NLS_LANG=AMERICAN_AMERICA.AL32UTF8
3. Change the directory to the <INSTALL_DIR>.
4. Login via sqlplus to the SIM database as the SIM schema owner, and run the patch script: `@run_all.sql`
5. `Compile the invalid objects.`
   - For Example:
   - alter package “RESA_FILE_PARSER” compile body;
   - alter package “RESA_POSU_PROCESSOR” compile body;

4

Application Installation tasks

Before proceeding, you must install Oracle WebLogic Server 11g Release 1 (10.3.6), ADF 11.1.1.7 and any patches listed in the Chapter 1 of this document. The Oracle Retail Store Inventory Management application is deployed to a WebLogic Managed server within the WebLogic installation. It is assumed Oracle Database has already been configured and loaded with the appropriate Store Inventory Management schemas for your installation.

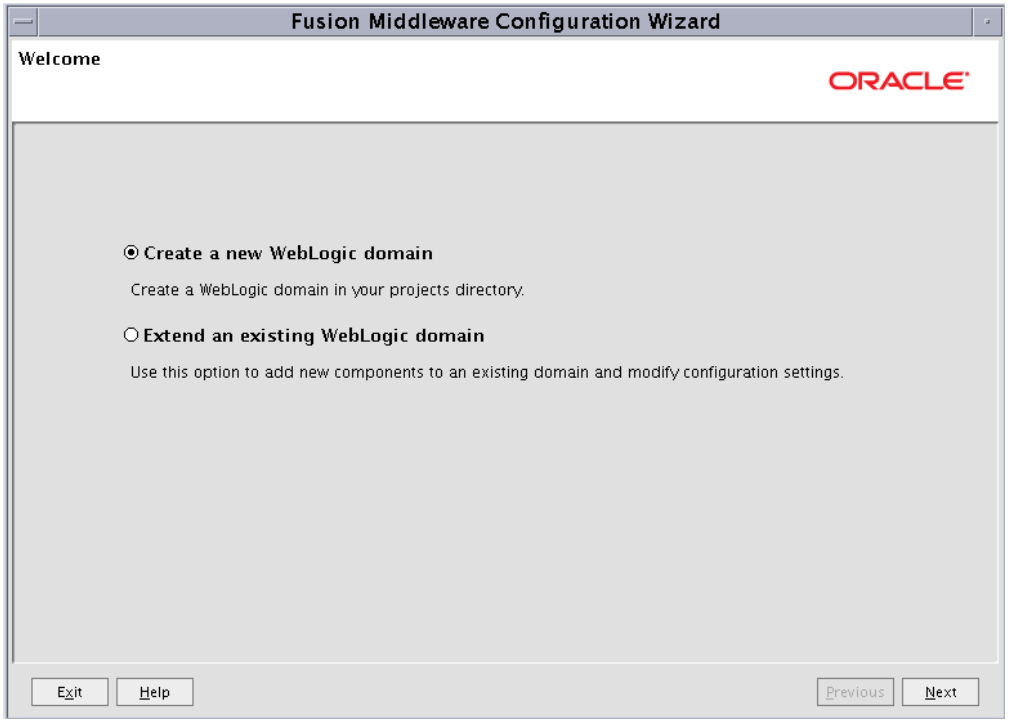
Installing a separate domain is mandated. It can be called "SIMDomain" (or something similar) and will be used to install the managed servers. The ADF libraries should be extended to this domain and the Enterprise Manager application should be deployed.

> **Note:** If this domain is to be setup in a secure mode. Please set up weblogic as SSL and refer to ORACLE Retail Merchandising Security Guide for details on all items to change to be in secure mode. This would best be done before domain and application install. The domain example below is for unsecured setup.

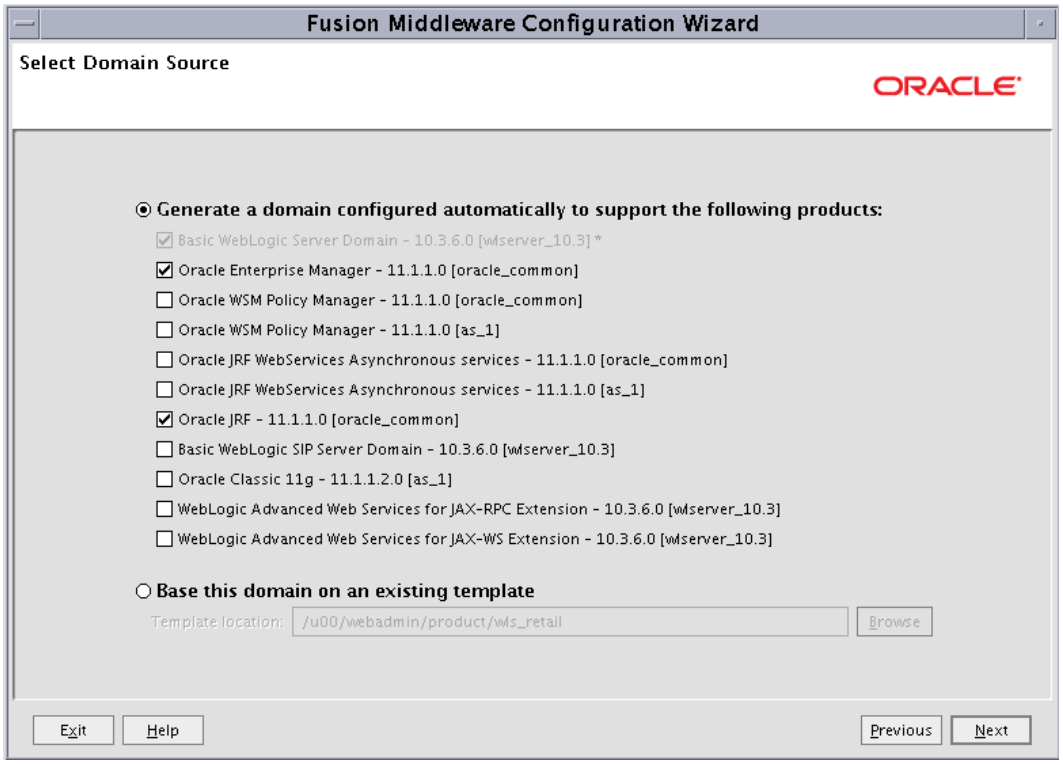
Create the Domain with ADF Libraries and Enterprise Manager

Perform the following procedure to create the domain with ADF libraries and Enterprise Manager.

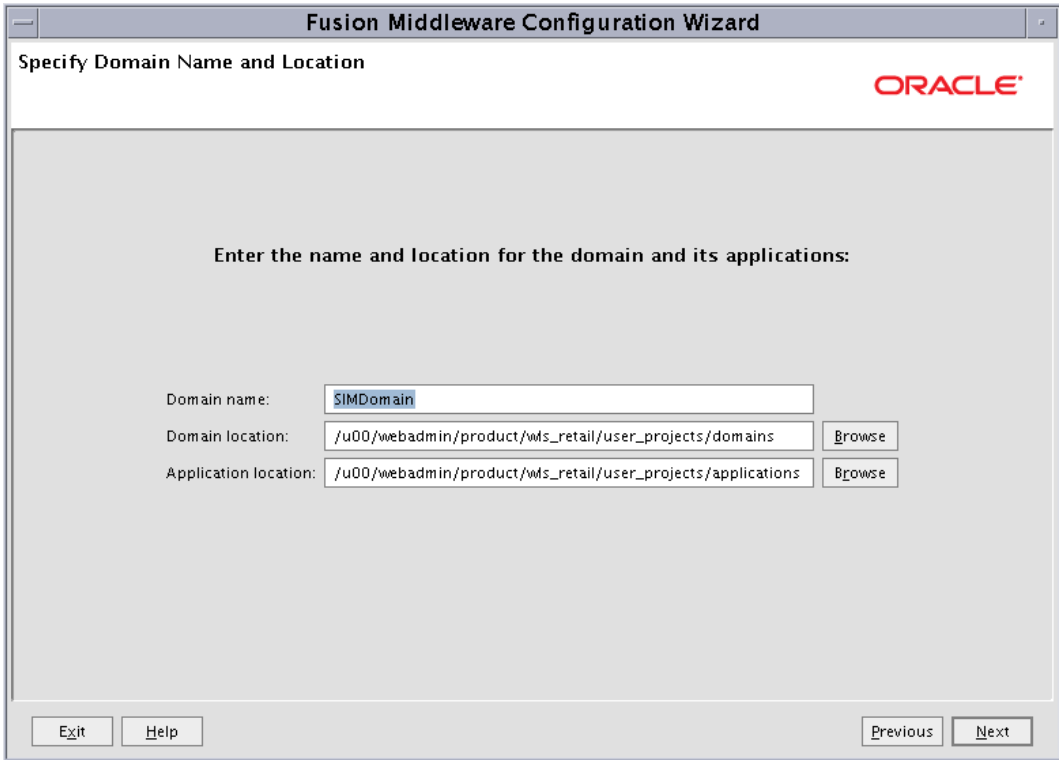
1. Run config.sh present in WebLogic home, wlserver_10.3/common/bin and select the create a new domain option
2. Select **Create a new WebLogic domain** and click **Next**.



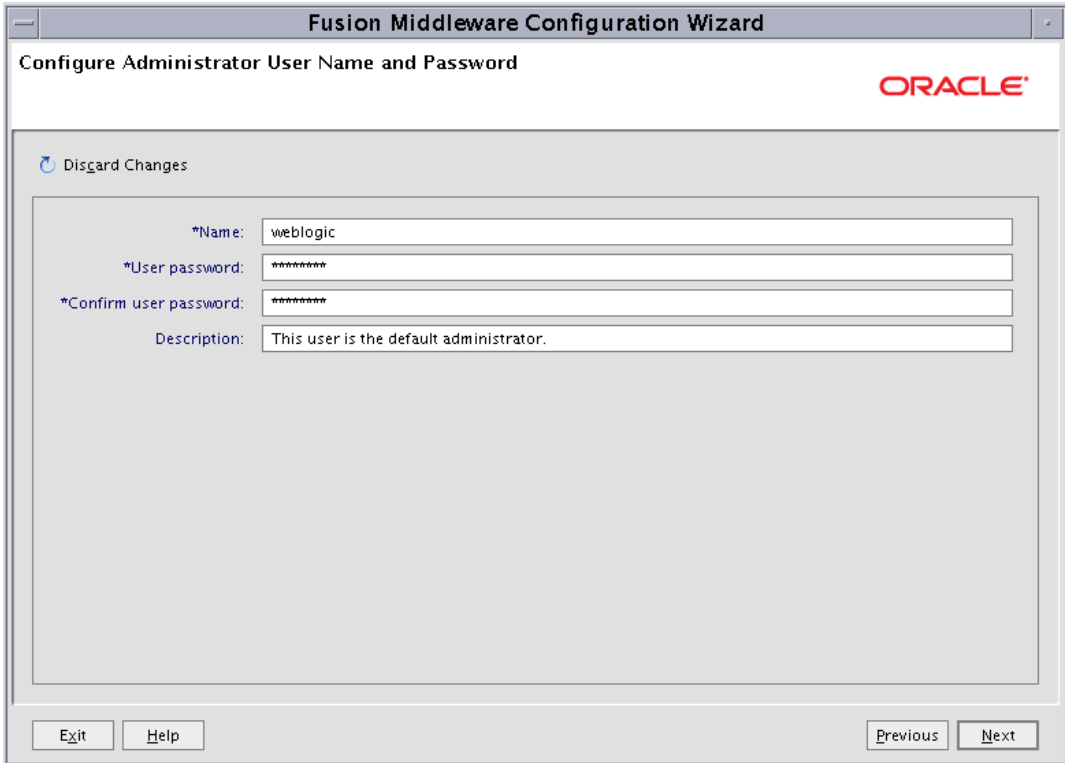
3. Select **Oracle Enterprise Manager** and **Oracle JRF** and click **Next**.



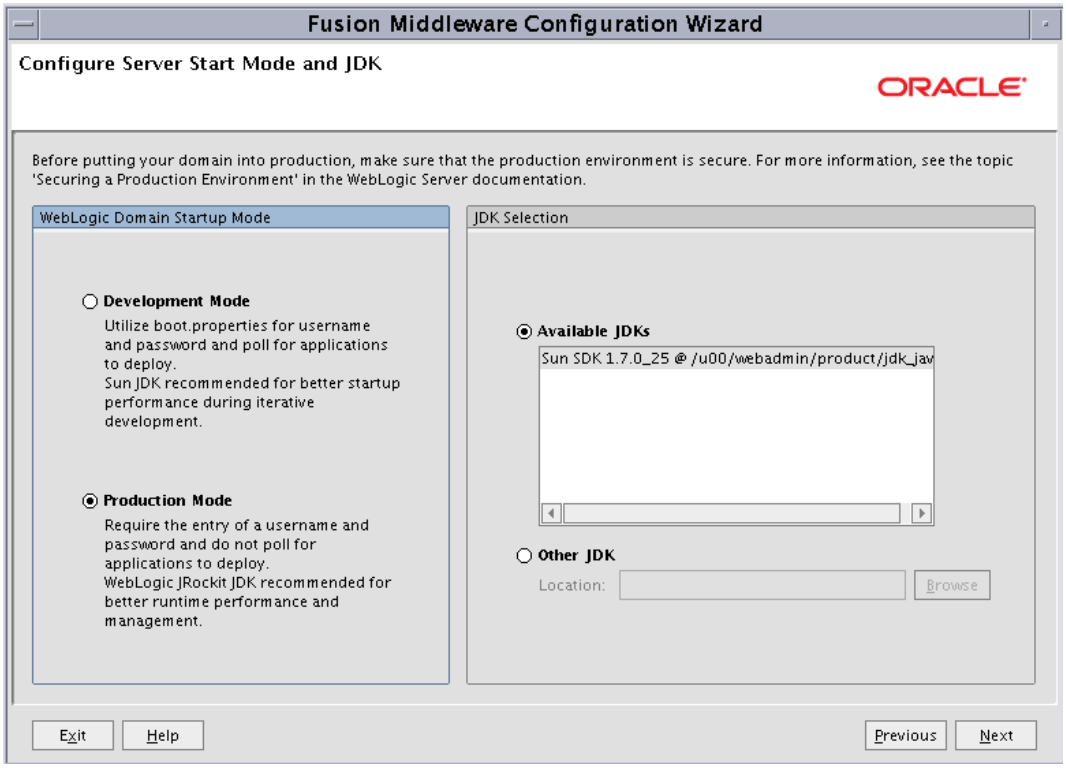
4. Set the Domain name (for example: SIMDomain) and click **Next**.



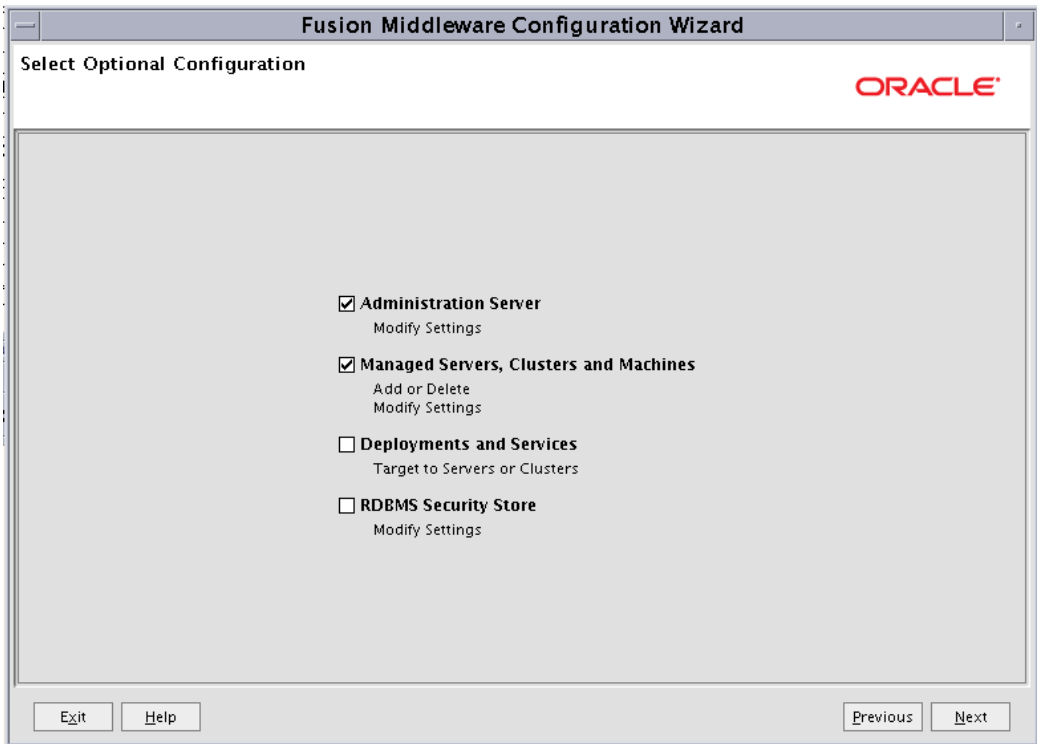
5. Set the Administrator user and password and click **Next**.



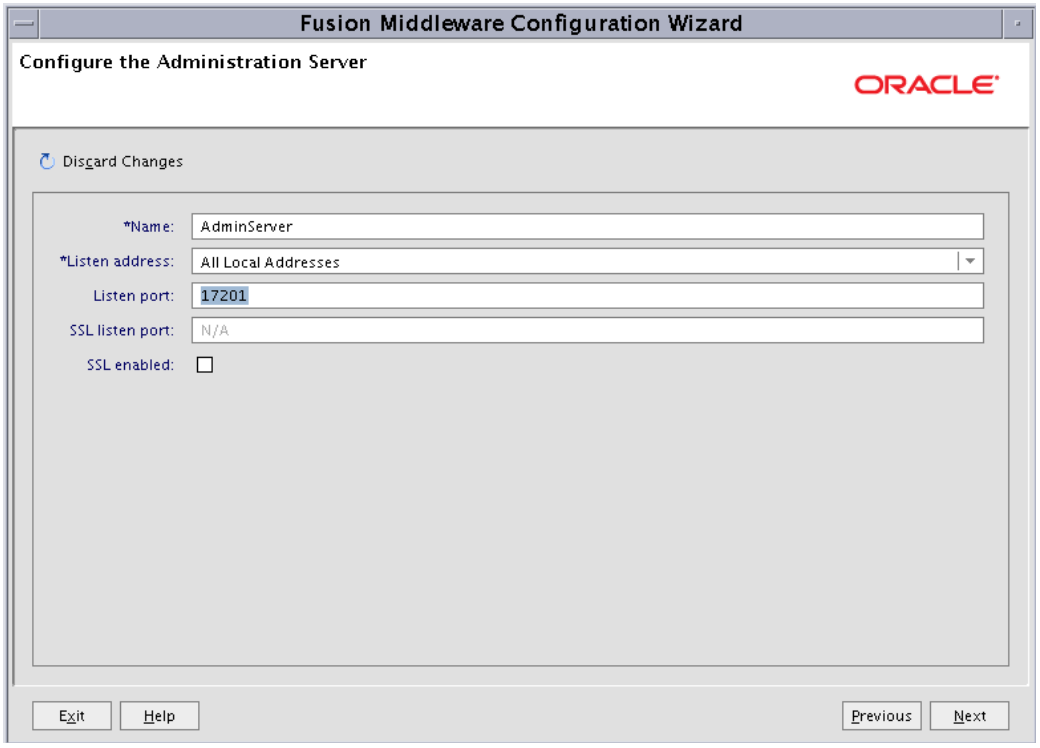
6. Select **Production Mode** and click **Next**.



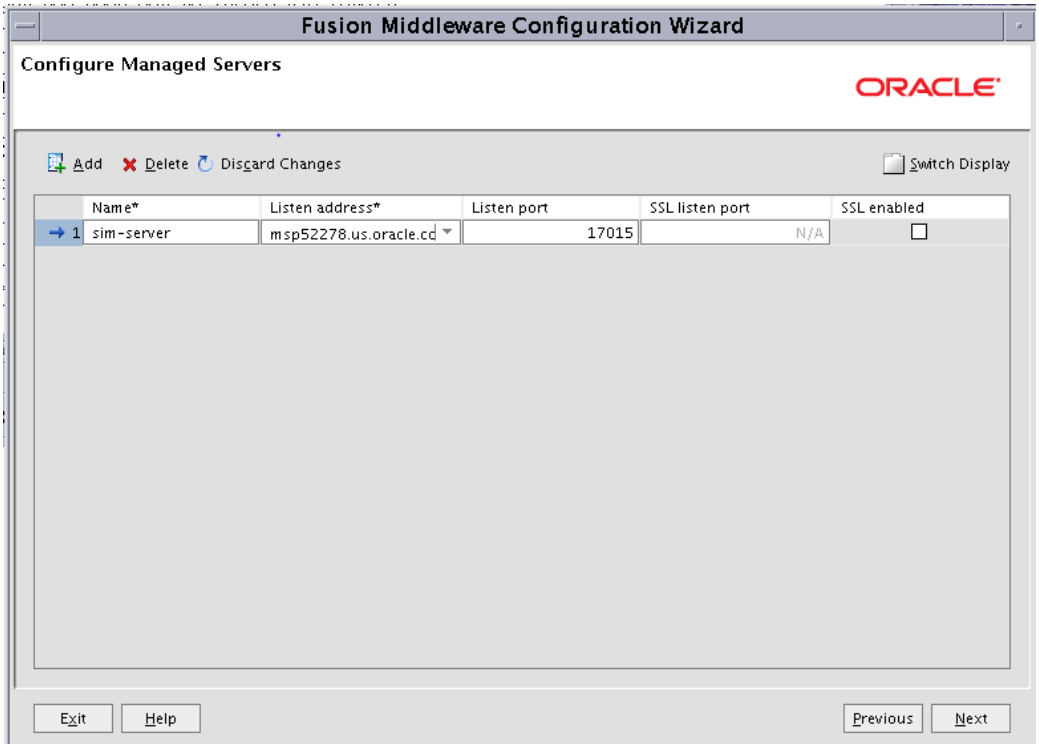
7. Select **Administration Server** and **Managed Servers, Clusters and Machines**. This will allow you to adjust the AdminServer port as well as create the sim-server and nodemanager. Click **Next**.



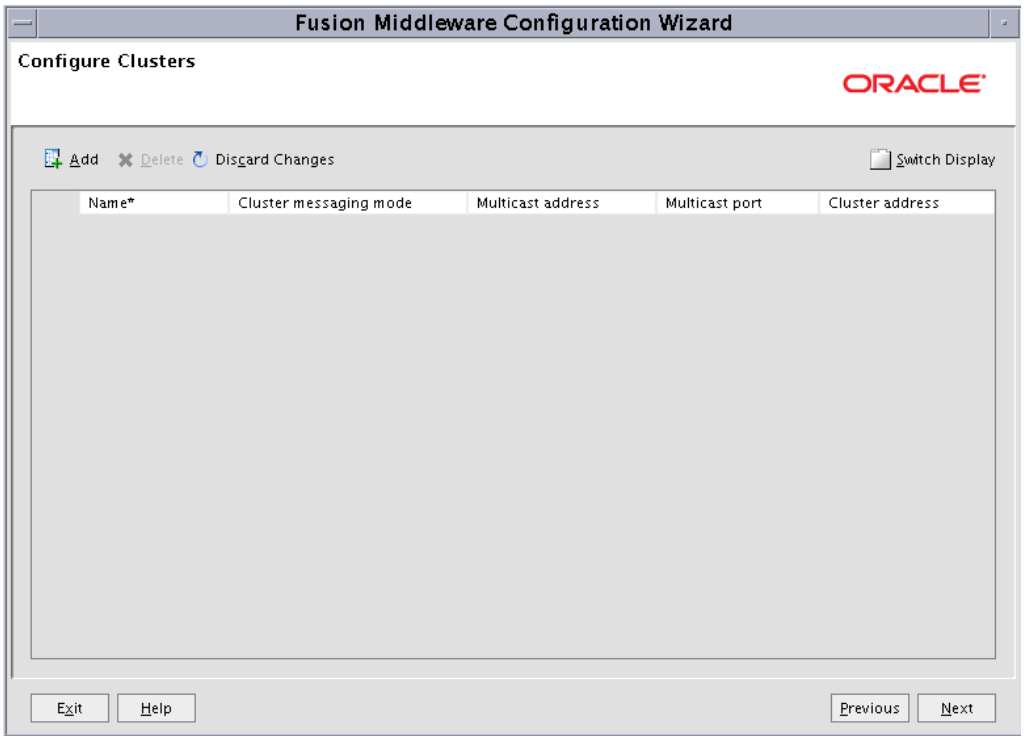
8. Set your AdminServer to an open port and click **Next**.



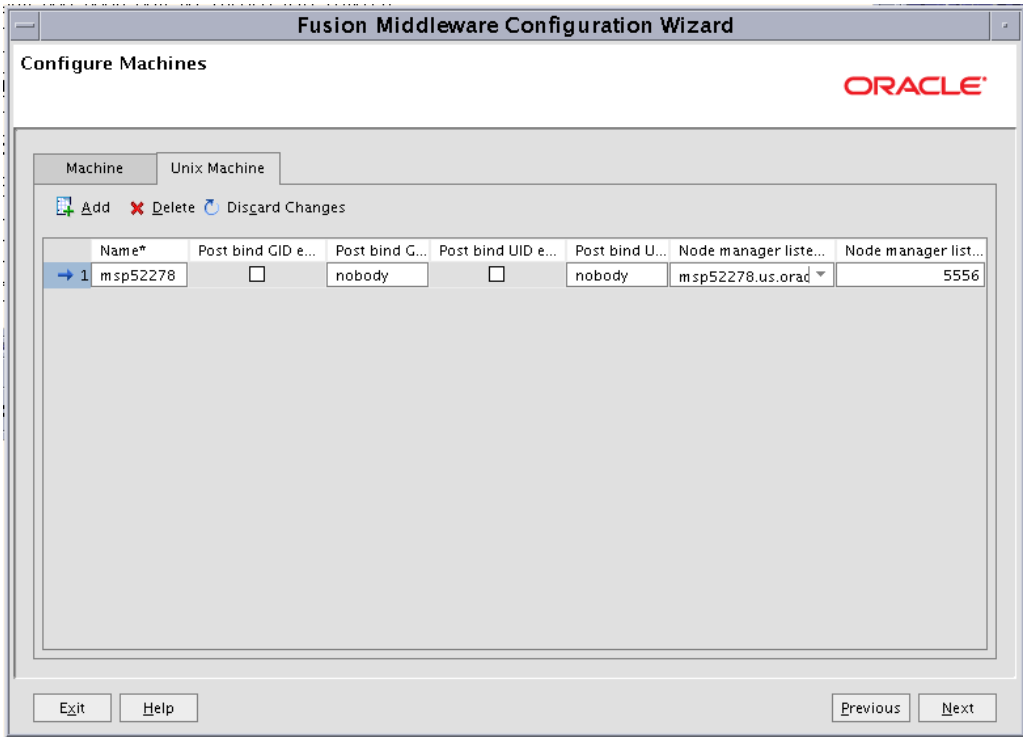
9. Click **Add** and create your sim-server managed server. Set the Listen Address to the server on which WebLogic is installed. Click **Next**.



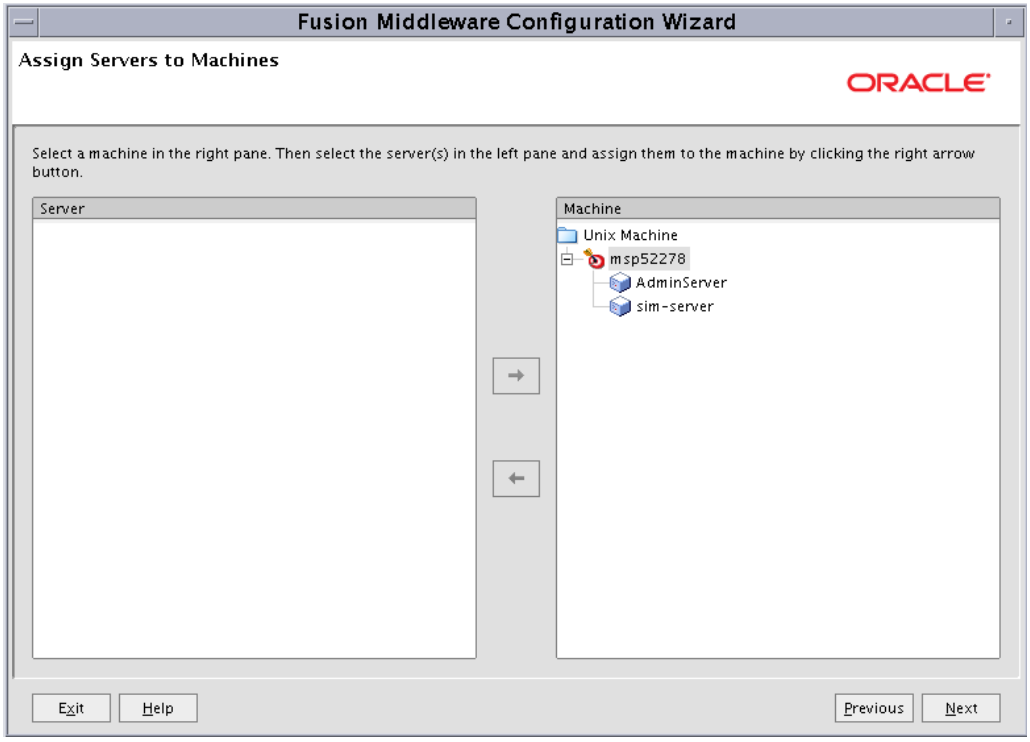
Note: A cluster is not being configured in this install example.



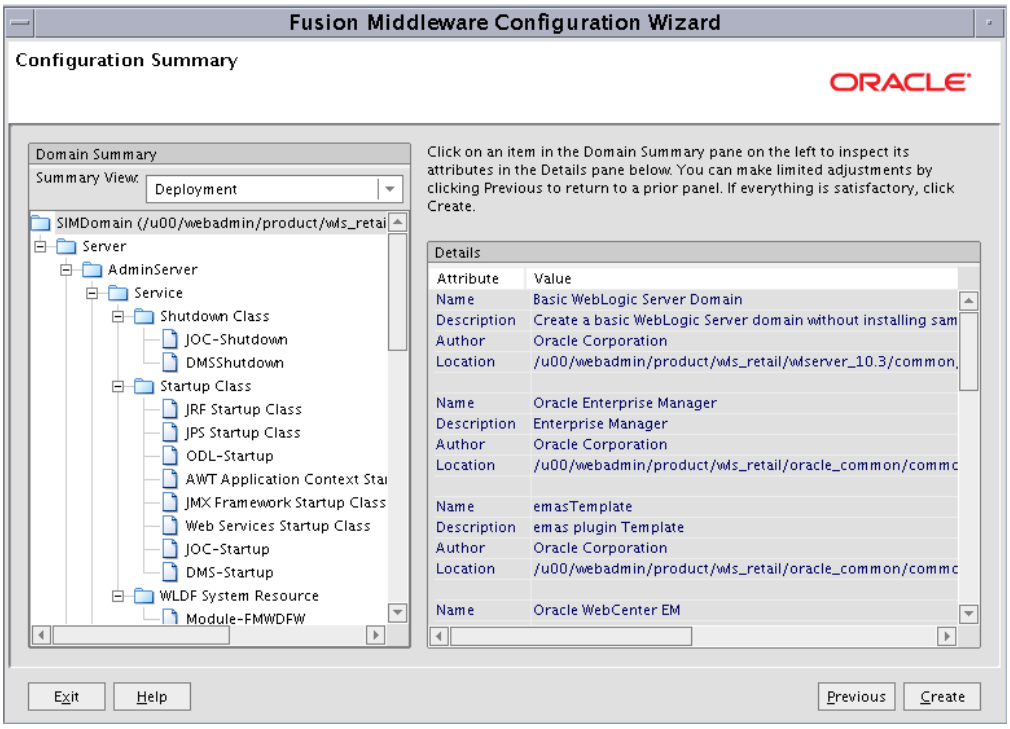
10. Click the Unix Machine tab, click **Add** and create the nodemanager (port 5556 is the default port). Click **Next**.



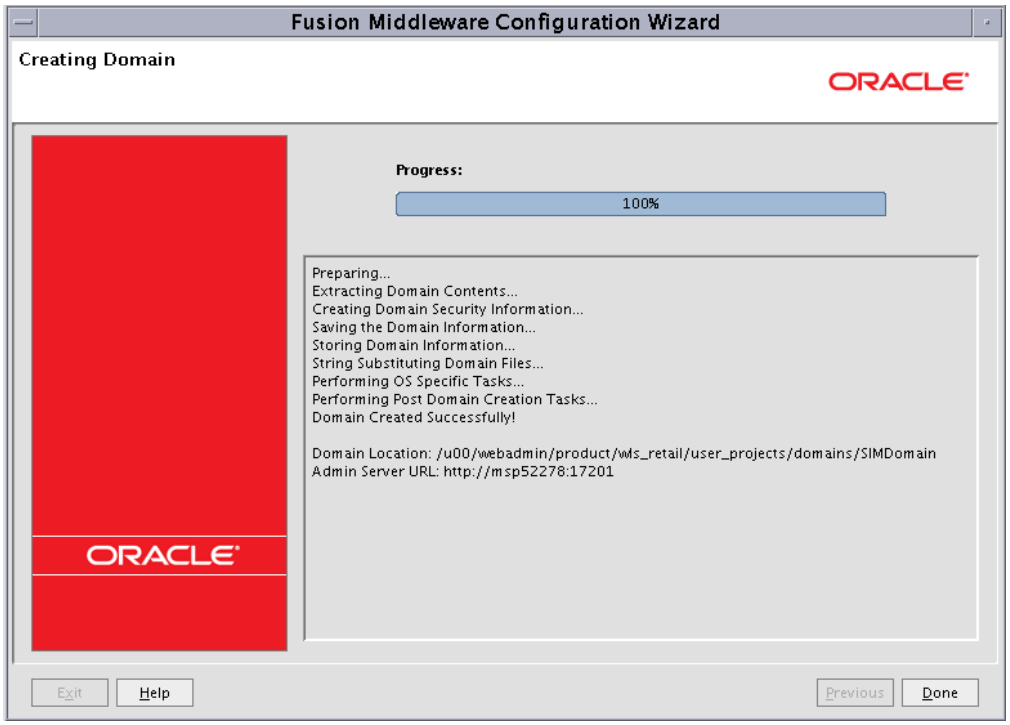
11. Add the AdminServer and sim-server to the nodemanager that was just created and click **Next**.



12. Create your new SIMDomain and click **Create**.



13. Click **Done**.



Note: Save the information for the Domain Location and Admin Server URL as that information is needed for the installation.

Update the WebLogic.policy:

1. After the SIMDomain has been created, update <WLS_HOME>/wlserver_10.3/server/lib/weblogic.policy file with the information below.

Note: If copying the following text from this guide to UNIX, ensure that it is properly formatted in UNIX. Each line entry beginning with "permission" must terminate on the same line with a semi colon. Also, the AdminServer must be restarted for these changes to take effect.

Note: <WEBLOGIC_DOMAIN_HOME> in the example below is the full path of the WebLogic domain; <managed_server> is the SIM managed server created.

```
grant codeBase
“file:<WEBLOGIC_DOMAIN_HOME>/servers/<managed_server>/tmp/_WL_user/-" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore.*", "read,write,update,delete";
};
grant codeBase
"file:<WEBLOGIC_DOMAIN_HOME>/servers/<managed_server>/cache/EJBCompilerCache/-
" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

An example of the full entry that might be entered is:

```
grant codeBase
"file:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/SIMDomain/servers
/sim-server/tmp/_WL_user/-" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission "
credstoressp.credstore.*", "read,write,update,delete";
};

grant codeBase
"file:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/SIMDomain/servers
/sim-server/cache/EJBCompilerCache/-" {
permission java.security.AllPermission;
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore", "read,write,update,delete";
permission oracle.security.jps.service.credstore.CredentialAccessPermission
"credstoressp.credstore.*", "read,write,update,delete";
};
```

Start the NodeManager

1. Start up the nodemanager, the script is located at $WLS_HOME/wlserver_10.3/server/bin/startNodeManager.sh.
2. Edit the nodemanager.properties file at the following location with the below values:

   $WLS_HOME/wlserver_10.3/common/nodemanager/nodemanager.properties

   - StartScriptEnabled=true
   - StartScriptName=startWebLogic.sh
3. After making changes to the nodemanager.properties file, NodeManager must be restarted.

> **Note:** The nodemanager.properties file is created after NodeManager is started for the first time. It is not available before that point.

Start the AdminServer (admin console):

1. Start up the AdminServer using the SIMDomain/bin/startWebLogic.sh script.

   With the initial startup you will be asked for the admin user credentials. Once the AdminServer has started up you can create a boot.properties file containing the credentials for the AdminServer to start up without the need to enter the information each time.

   An example of the boot.properties would be:

```
mkdir SIMDomain/servers/AdminServer/security
vi SIMDomain/servers/AdminServer/security/boot.properties
```

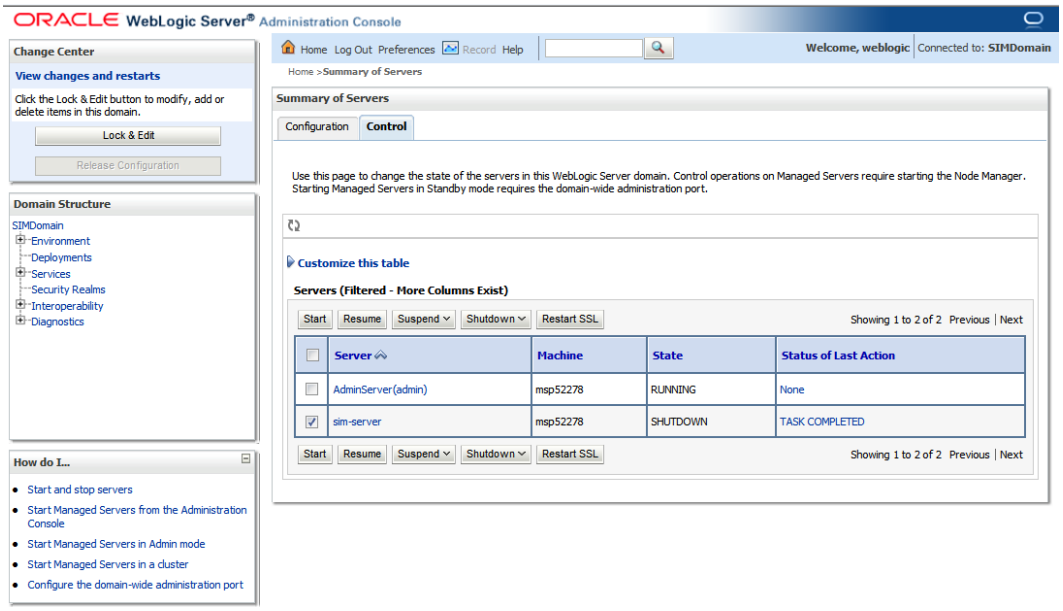
   - username=weblogic
   - password=<password used at domain creation>

   This file will be encrypted after the SIMDomain starts up.

Start the Managed Server

After NodeManager and AdminServer are started, the managed server(s) can be started via the admin console.

1. Navigate to Environments > Servers, Control tab. Select sim-server and click “start”.



Change the default (file based) Credential Store to use the Oracle Database

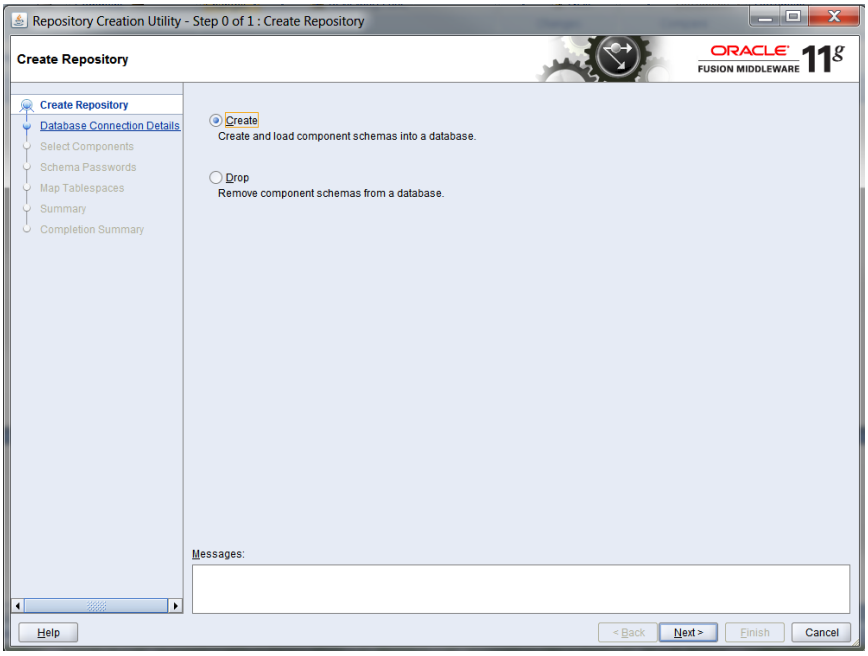
The SIMDomain that was just created will default to use a file based credential store for the wallet and policies. This needs to be changed so that it uses the Oracle Database. This change is for enhanced security and is also a requirement for a clustered SSO authentication setup.

Creation of Required Schemas with RCU

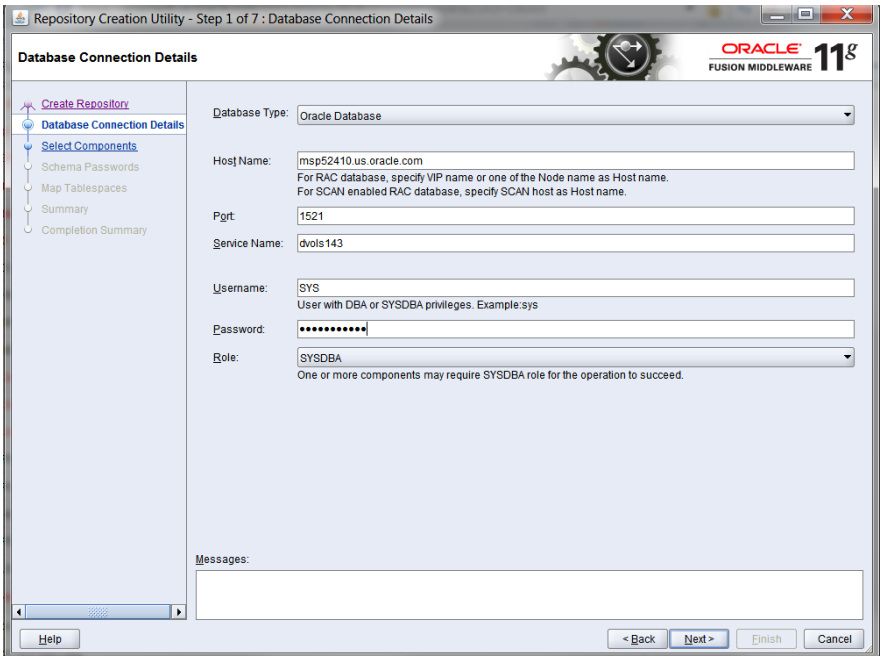
Some RCU database schemas are required to change the credential store, specifically we will need to create the OPSS and MDS schemas.

The following steps will show you the creation of the database schemas required:

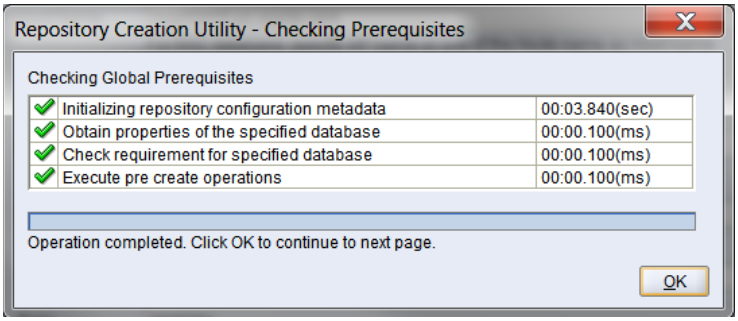
1. Download the RCU 11.1.1.7 zip file and extract it to a new folder named RCU 11.1.1.7. This folder (RCU 11.1.1.7) is used as RCU_HOME for the remainder of this guide. You may use a Windows version of RCU to create the schemas.
2. Go to <RCU_HOME>\BIN and double click rcu.bat.
3. Select **Create** and click **Next**.



4. Enter all the fields as explained below and click **Next**:
   a. Host Name: Database server host name which Application will use.(example: msp52410.us.oracle.com)
   b. Port: Database port (example: 1521)
   c. Service Name Database name (example: dvols143)
   d. Username: SYS
   e. Password: <SYS password>

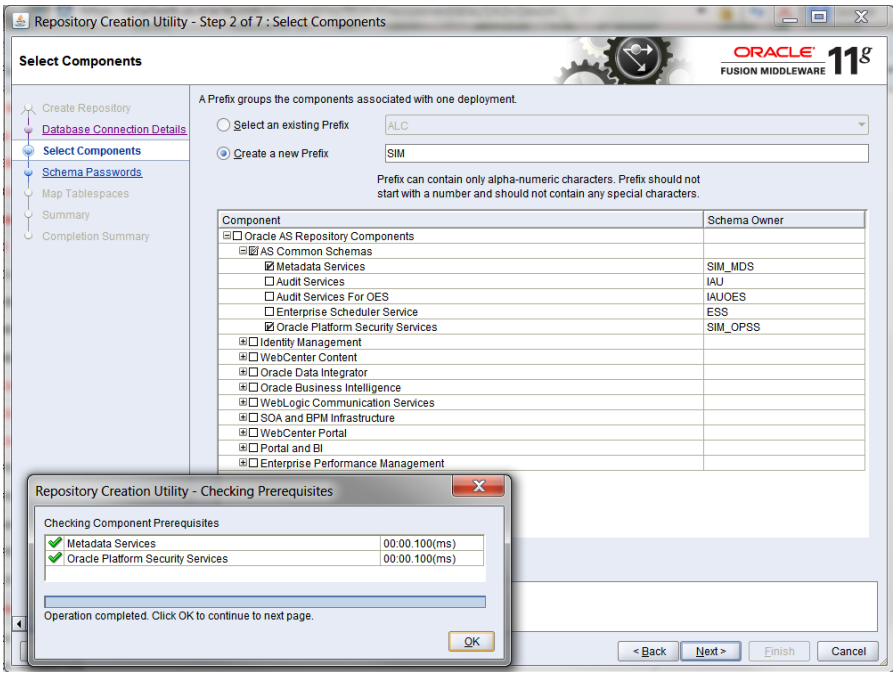


5. Prerequisite requirements are verified and the following screen is displayed, click **OK**.



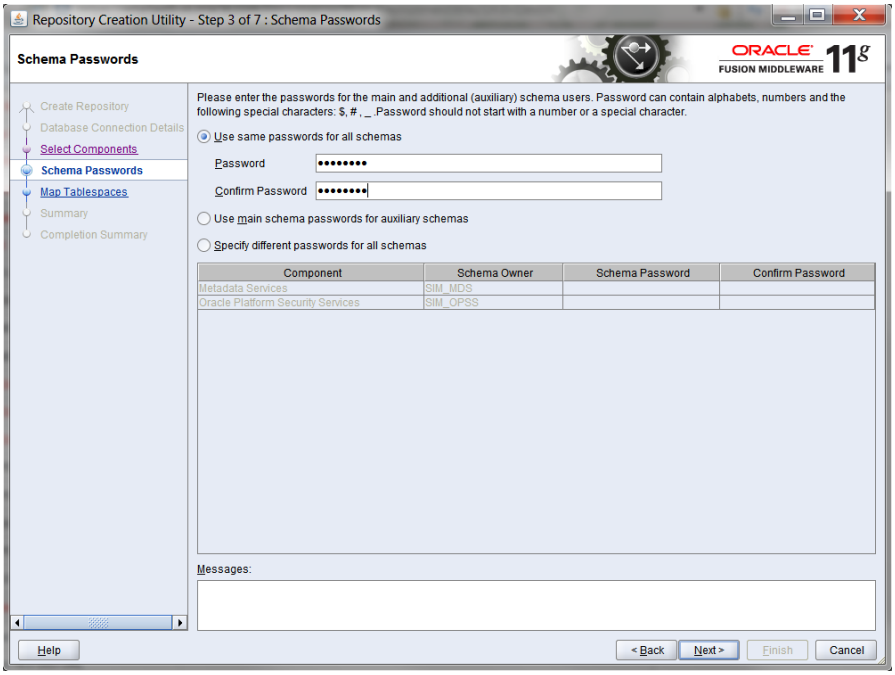
6. Expand "Oracle AS Repository Components" and select Metadata Services and Oracle Platform Security Services checkboxes as shown below. Enter a new prefix if needed (the example uses a prefix of "SIM").

   Click **Next** then **OK** for the prerequisites check.

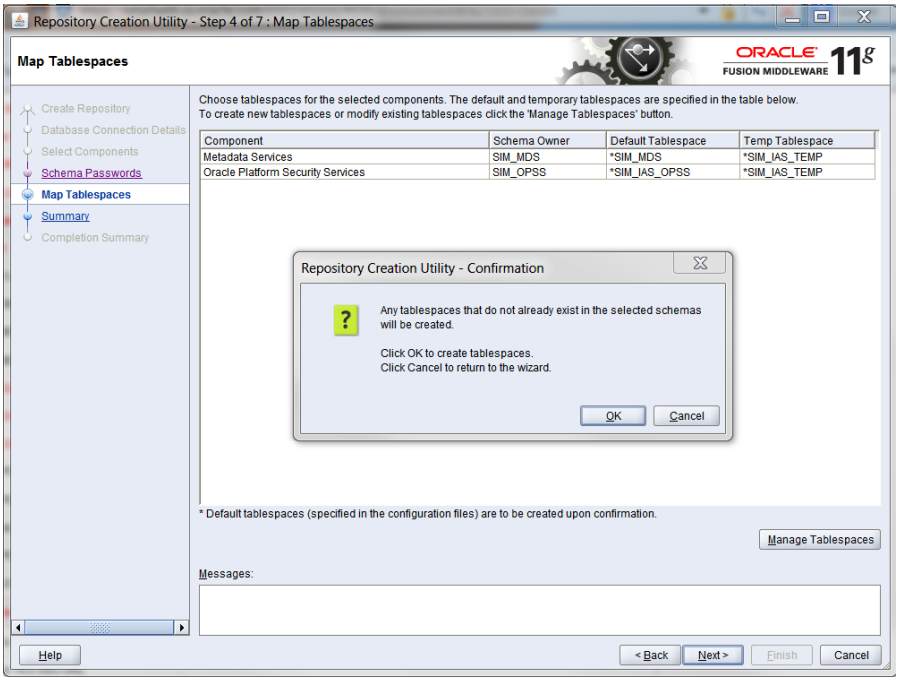


7. Enter and confirm your password and click **Next**.

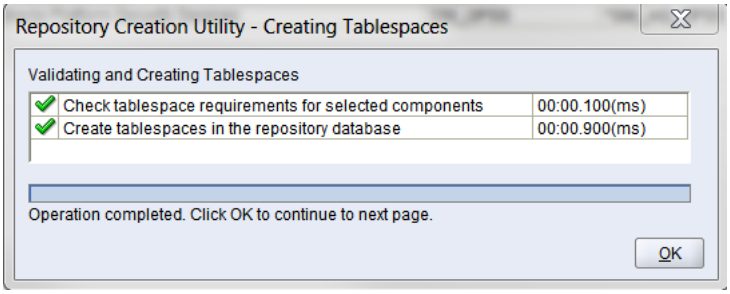
> **Note:** Make a note of the password you give here as it will be used later.



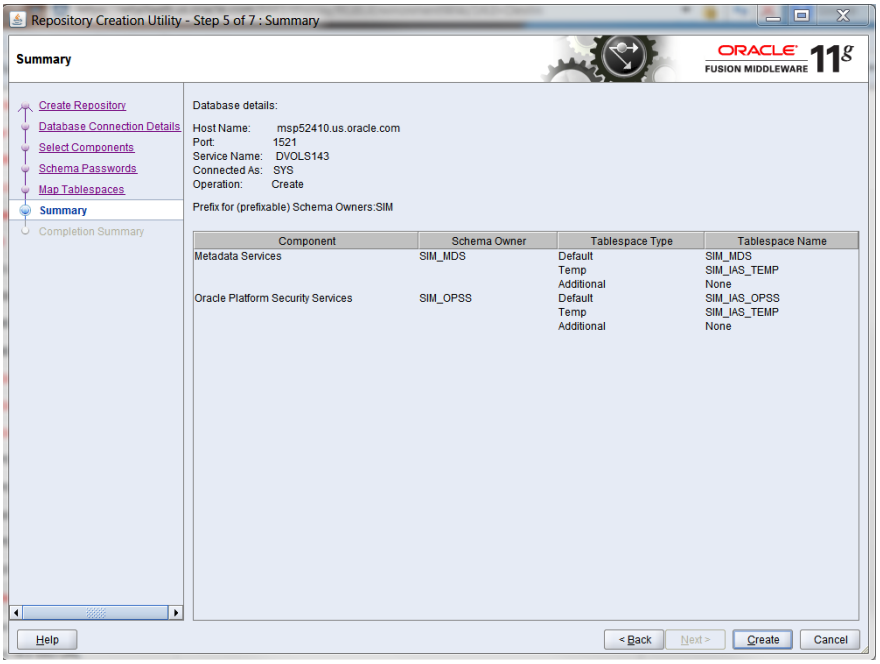
8. Click **Next**, then **OK** when it states it is going to create the tablespaces if they are needed.



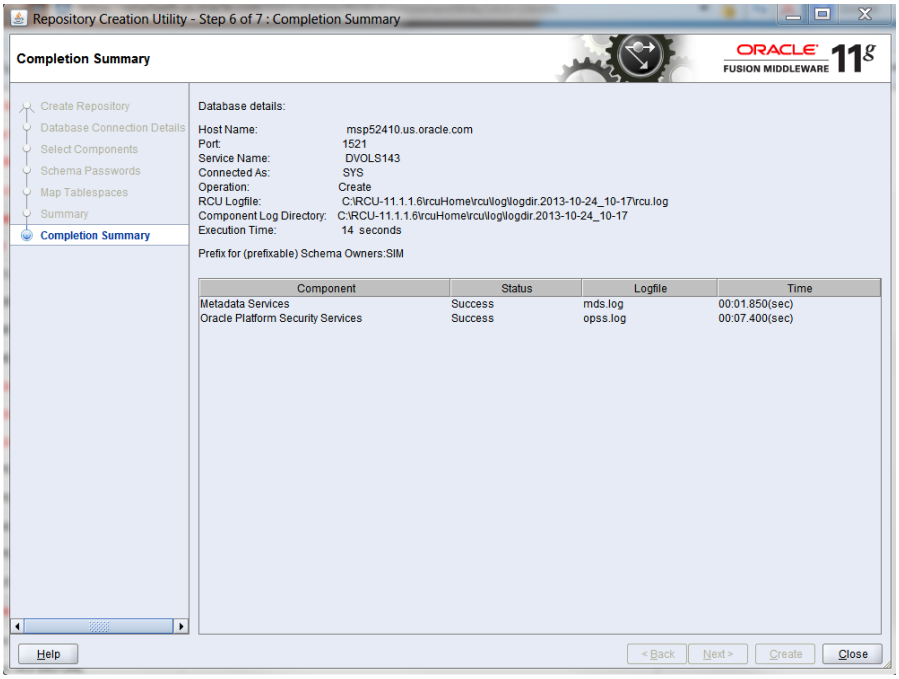
9. Click **OK** when tablespace creation and validation has completed.



10. Click **Create** to create the schemas.



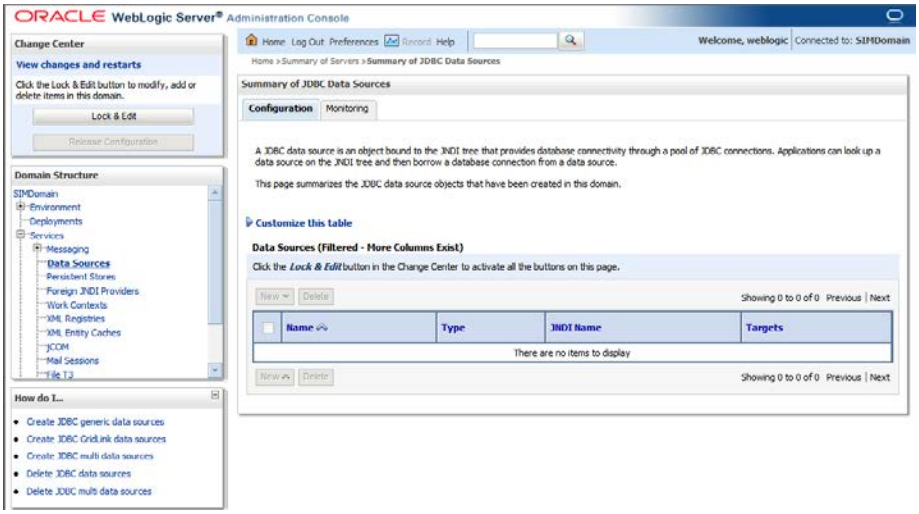
11. When the schemas are created, click **Close** to exit RCU.



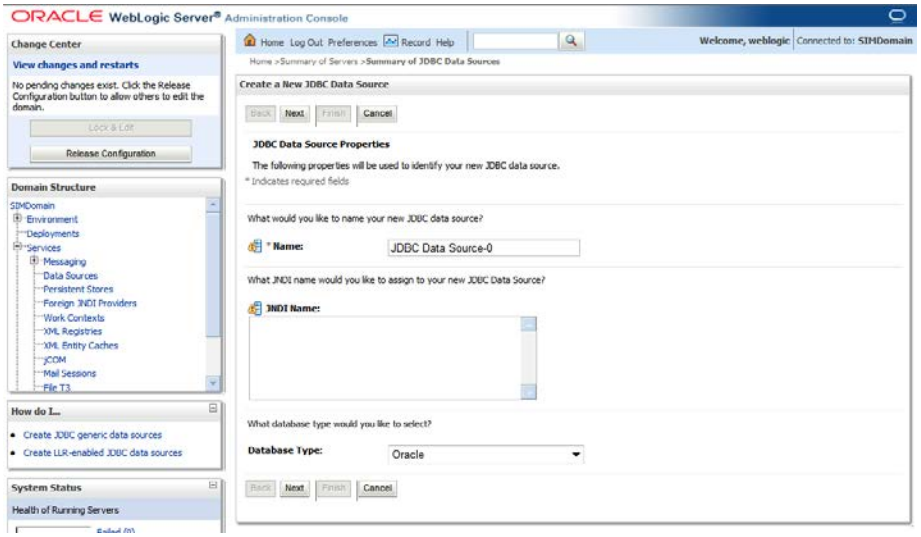
Set up OPSS Schema Datasource in WebLogic domain

Follow the below steps to set up the datasource with OPSS schema in WebLogic domain (SIMDomain).

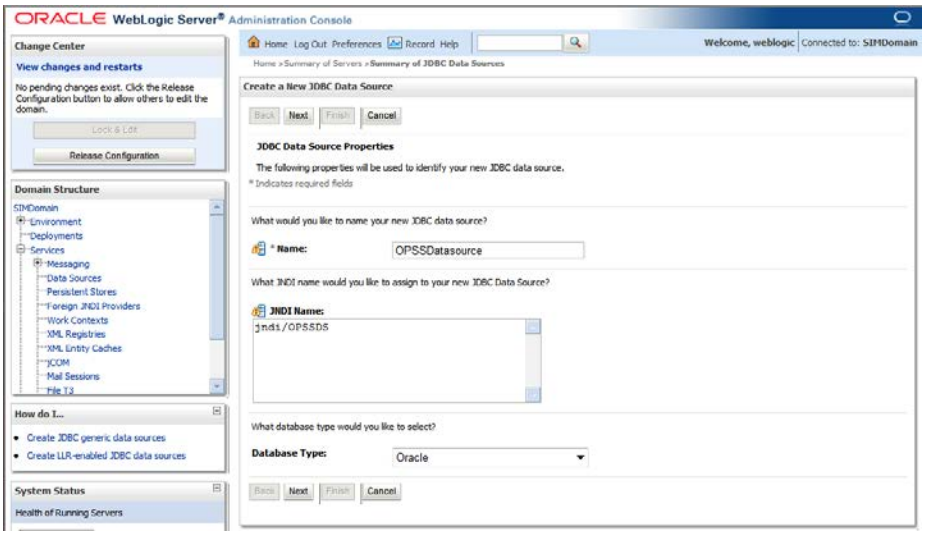
1. Login to the Admin console and go to Services -> Data Sources.



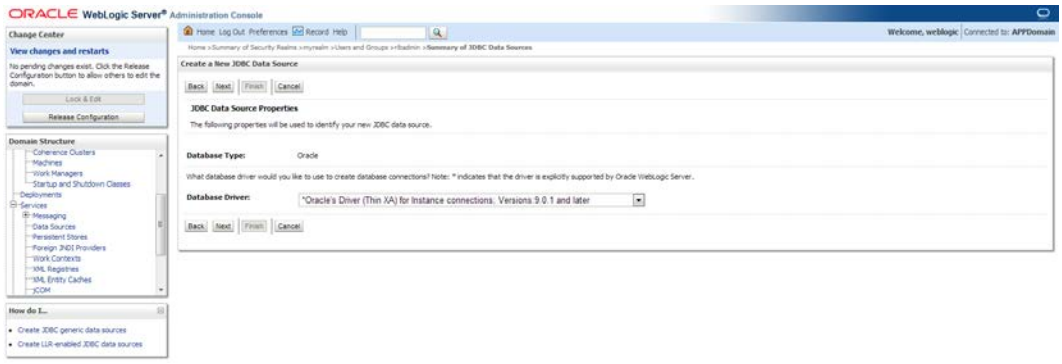
2. Click **Lock & Edit** then click New -> Generic Data Source.



3. Enter the details and click **Next**:
   - Name: OPSSDataSource
   - JNDI Name: jndi/OPSSDS
   - Database Type: Oracle

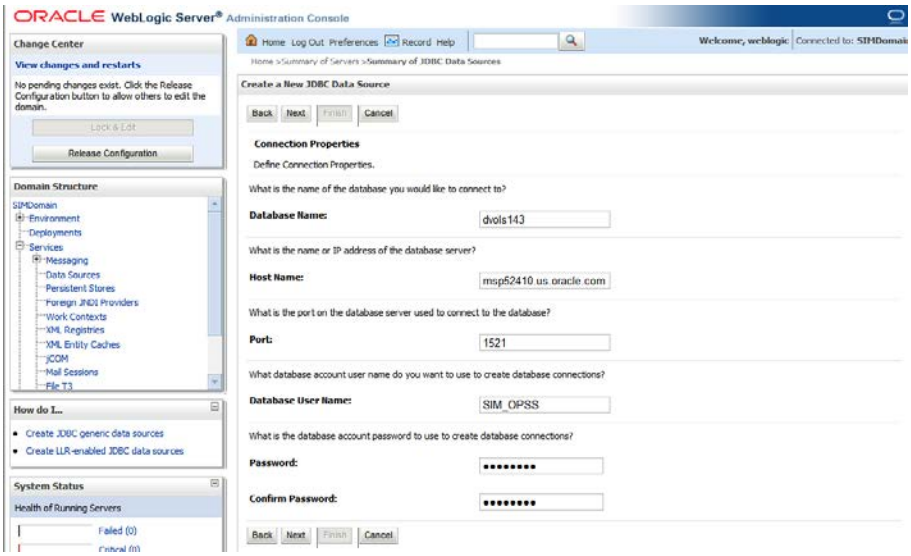


4. Select Oracle's Driver (Thin XA) for Instance connections; Versions: 9.0.1 and later. Click **Next**.

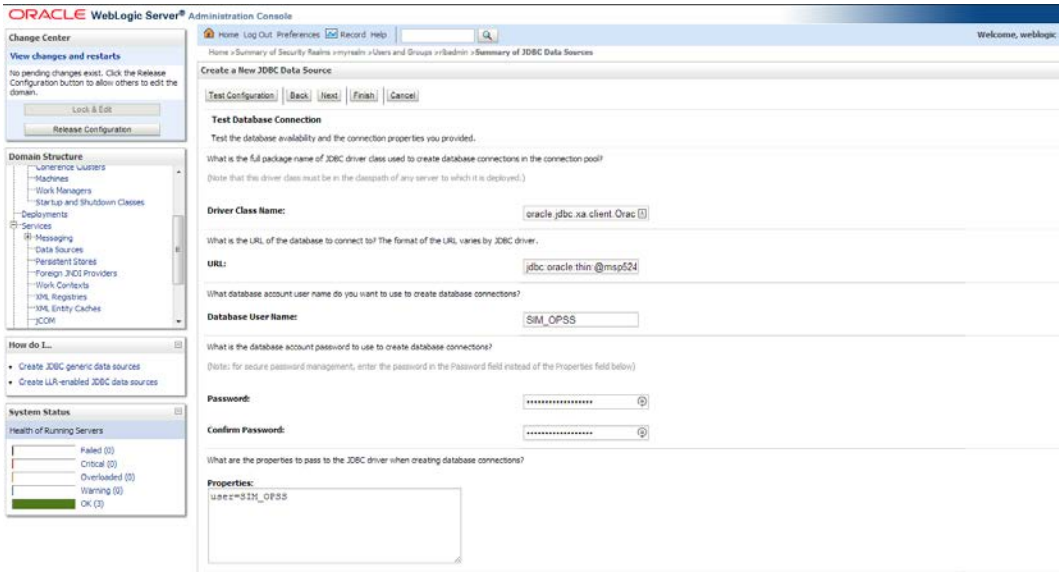


5. Click **Next**.

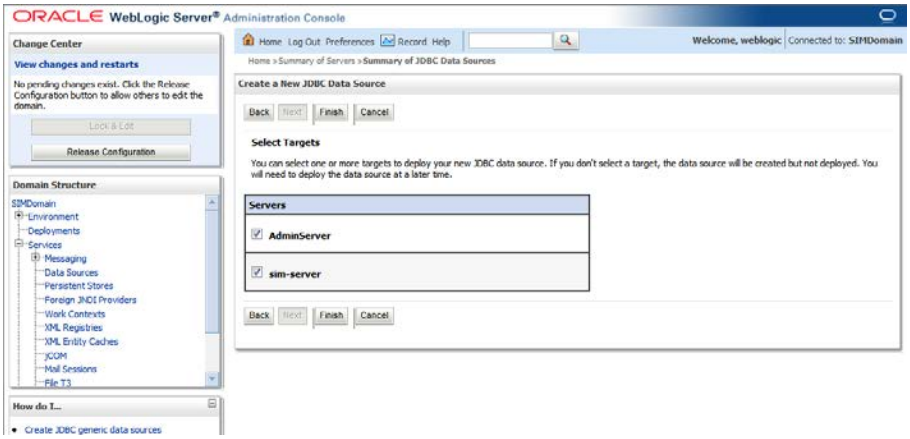
6. Enter the details of the OPSS schema we just created and click **Next**:
   - Database Name: (i.e: dvols143)
   - Host Name: (i.e.: msp52410.us.oracle.com)
   - Port: (i.e.: 1521)
   - Database User Name: SIM_OPSS (This is the OPSS schema which has been created using RCU earlier in this document.)
   - Password: <password (Password given at the time of OPSS schema creation)



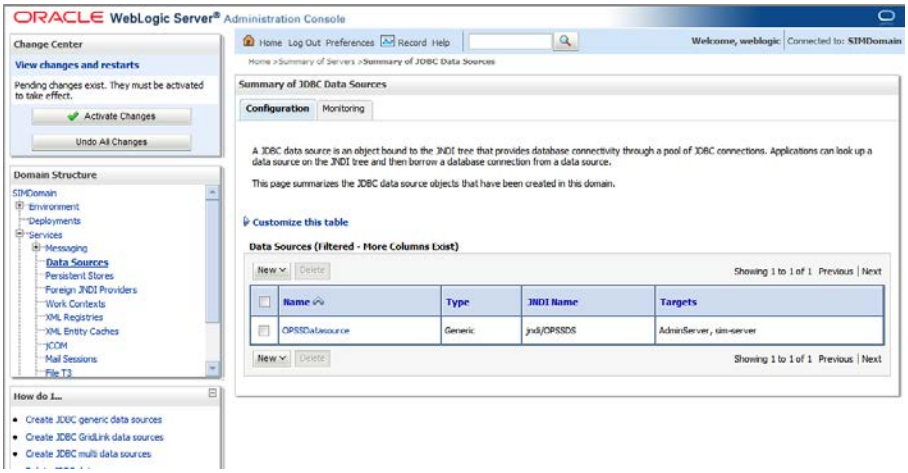
7. Click **Test Configuration** and make sure you can connect to the schema successfully. Click **Next** if ok, click **Back** if it does not connect and check your settings.



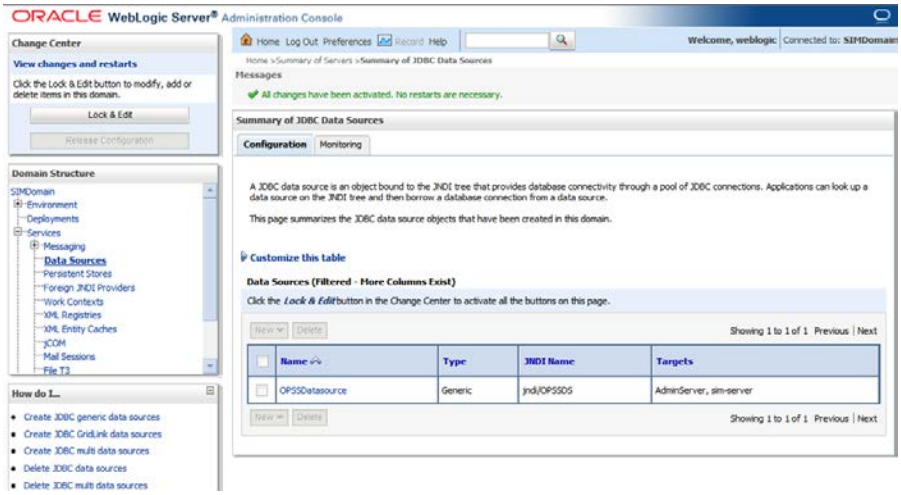
8. Target all the servers (AdminServer & sim-server) and click **Finish**.



9. Click **Activate Changes** to get them incorporated into the domain.



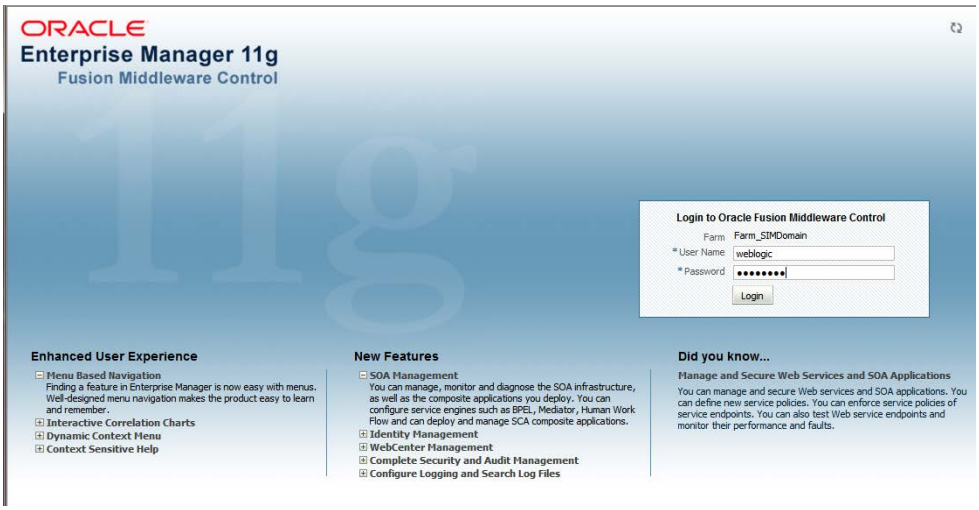
A message is displayed indicating that the changes have been activated.



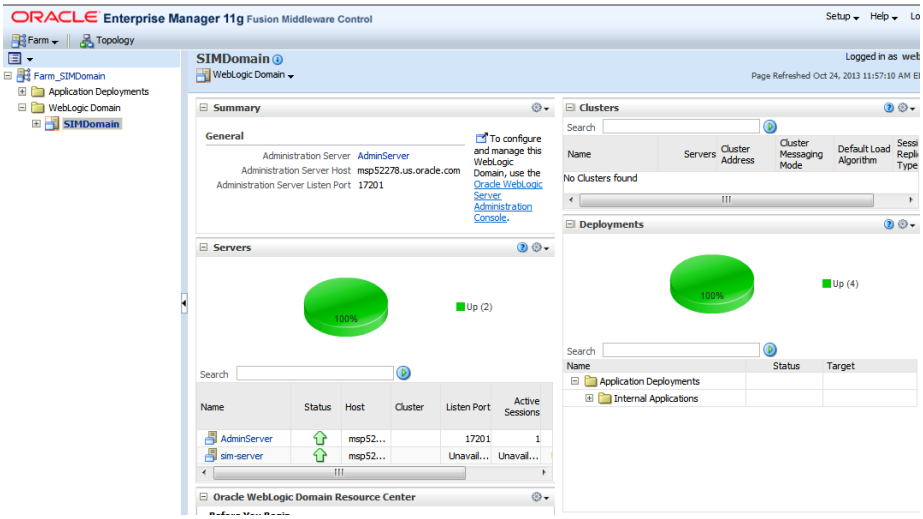
Associate Policy Store to Database

Follow the steps below to re-associate the domain policy store from file based to using the database:

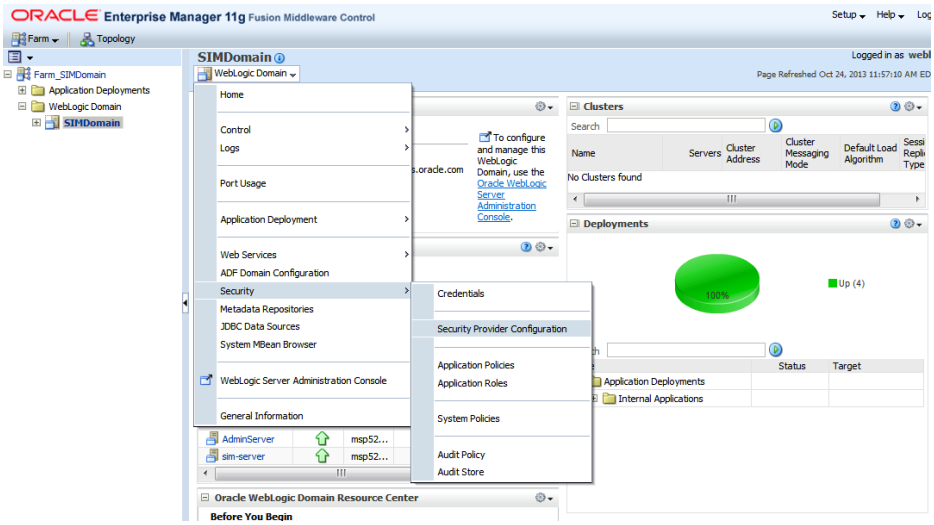
1. Login to the WebLogic EM console using the Administrator credentials (for example: http://msp52278.us.oracle.com:17201/em).



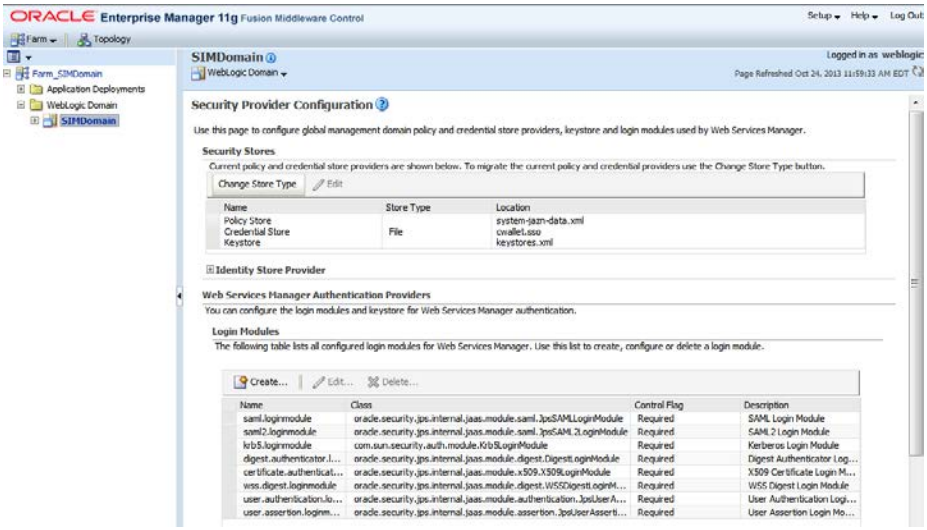
2. Expand the WebLogic Domain and click the SIMDomain.



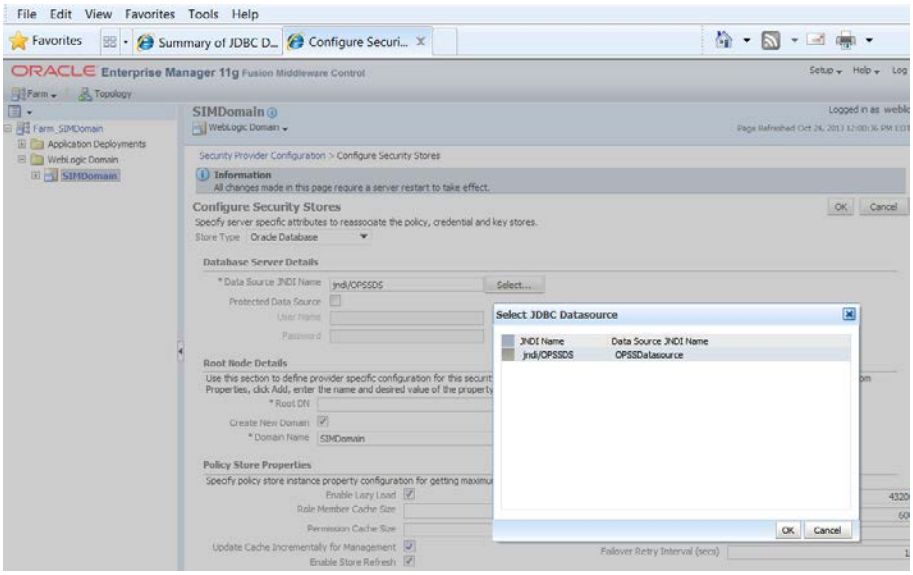
3. Select the dropdown WebLogic Domain->Security->Security Provider Configuration.



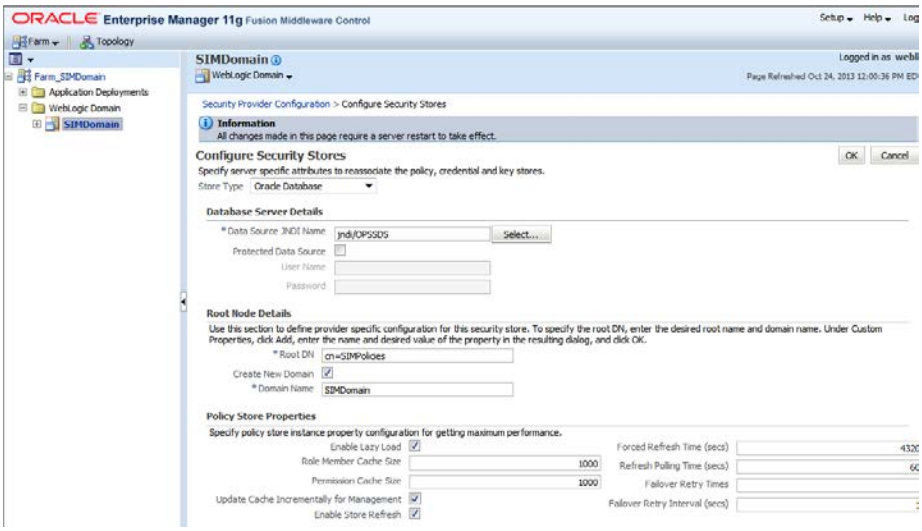
4. Click **Change Store Type**.



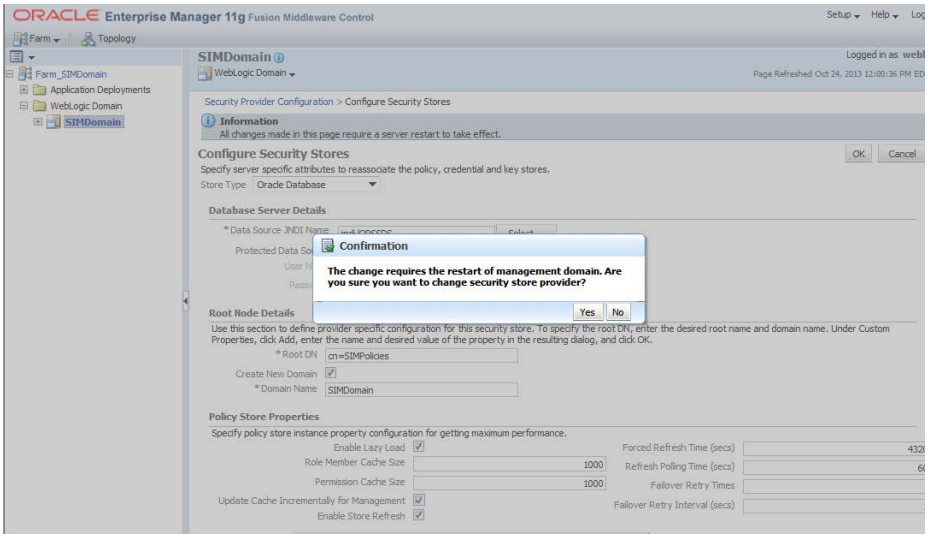
5. Select **Oracle Database** for the store type, then click the select button for the **Data Source JNDI Name** and choose the OPSS datasource we just created.



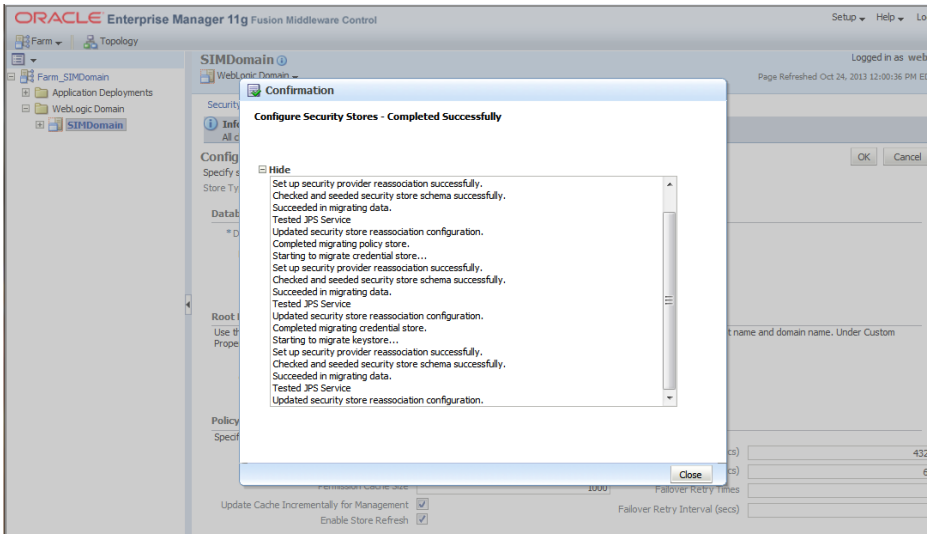
6. Enter the values:
   - Root DN: cn=SIMPolicies
   - Select 'Create New Domain'
   - Domain Name: SIMDomain (This must be the domain name which has been created earlier in this document)



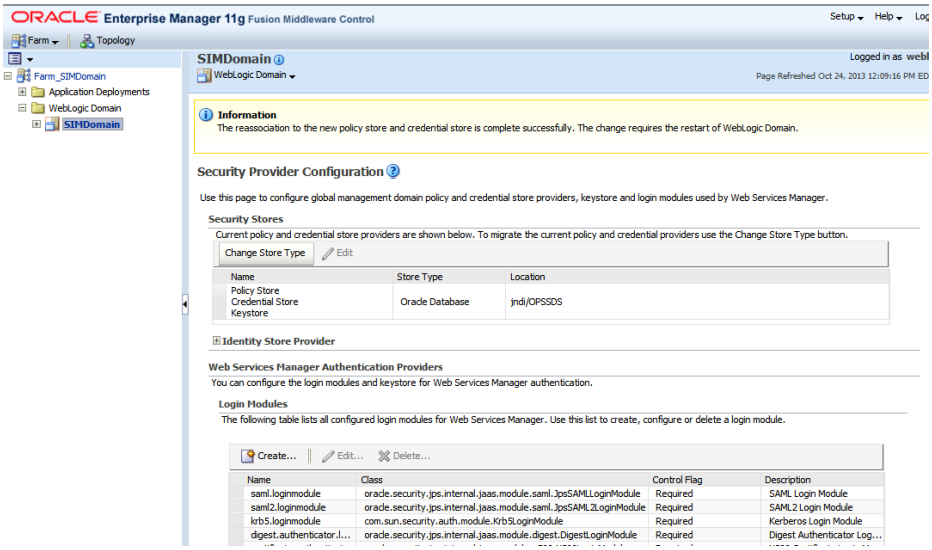
7. Click **OK**, and then click **Yes** when it warns that it will require a restart of the management domain.



8. The message 'Configure Security Stores – Completed Successfully' appears. Click **Close**.



The following confirmation appears:



9. Restart the SIMDomain for the changes to take effect.

Expand the SIM Application Distribution

To expand the SIM application distribution, do the following.

1. Log in to the UNIX server as the user who owns the Web Logic installation. Create a new staging directory for the SIM application distribution (sim14-application.zip). There should be a minimum of 250 MB disk space available for the application installation files.

   This location is referred to as INSTALL_DIR for the remainder of this chapter.

2. Copy sim14-application.zip to <INSTALL_DIR> and extract its contents.

SIM LDAP Users/Groups/Roles Setup

NOTE: This step is only needed if you plan on using LDAP authentication for the SIM application. This can be skipped if DB authentication is going to be used.

LDAP Login requires proper set up of users and roles in LDAP.

Sample ldif files have been provided in the install media. The ldif files are in the 'sim-database-ldap.zip' located at <INSTALL_DIR>/sim/application/sim14/ldap.

Refer to the Setting up LDAP Data for SIM section in Chapter 3: Setup and Configuration of the *SIM 14.0.2 Implementation Guide – Volume One* for the details on setting up the user/roles/object classes in the LDAP.

Once the object classes, roles and users required are created in your LDAP, create a group named 'sim_secure_users' in your Group DN (for example: cn=Groups, dc=us,dc=oracle,dc=com) and add the members below:

- cn=<sim.admin> user (this is the Search User DN which you will provide as input in the installer for the screen 'Screen: LDAP Directory Server Details' .
- cn=<retail.user> (this is the Application User with which you will login to SIM).

Here is a sample LDIF which can be used to create the group 'sim_secure_users.:

sim_secure_users_group.ldif:

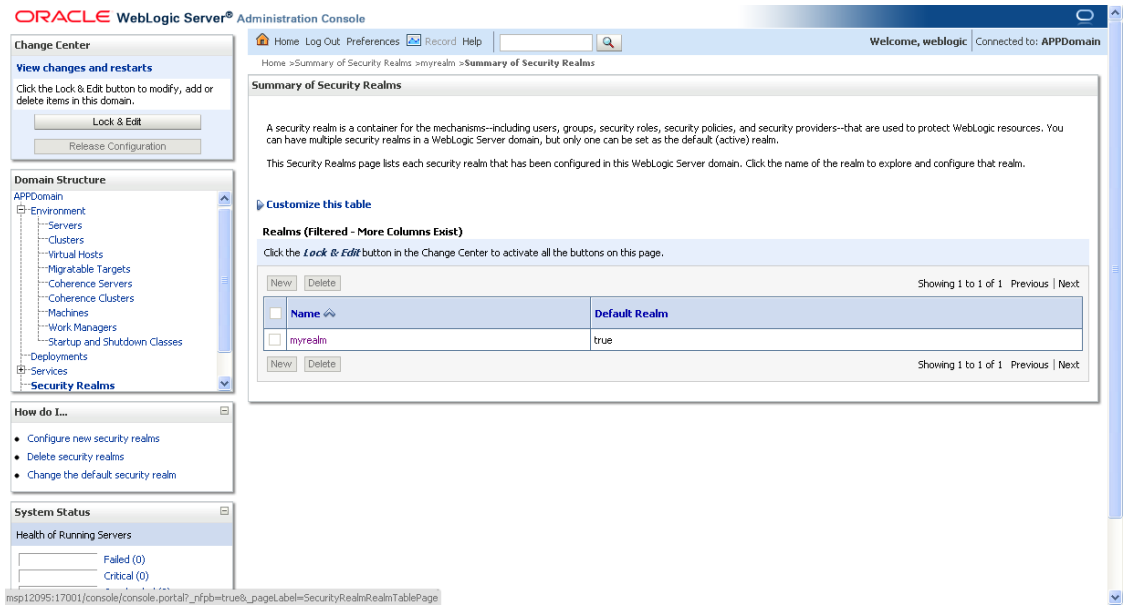
```
dn: cn=sim_secure_users,cn=groups,dc=us,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: orclGroup
objectclass: top
cn: sim_secure_users
description:
displayname:  SIM secure users
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=sim.admin,cn=users,dc=us,dc=oracle,dc=com
```

SIM OID Authentication Provider set up

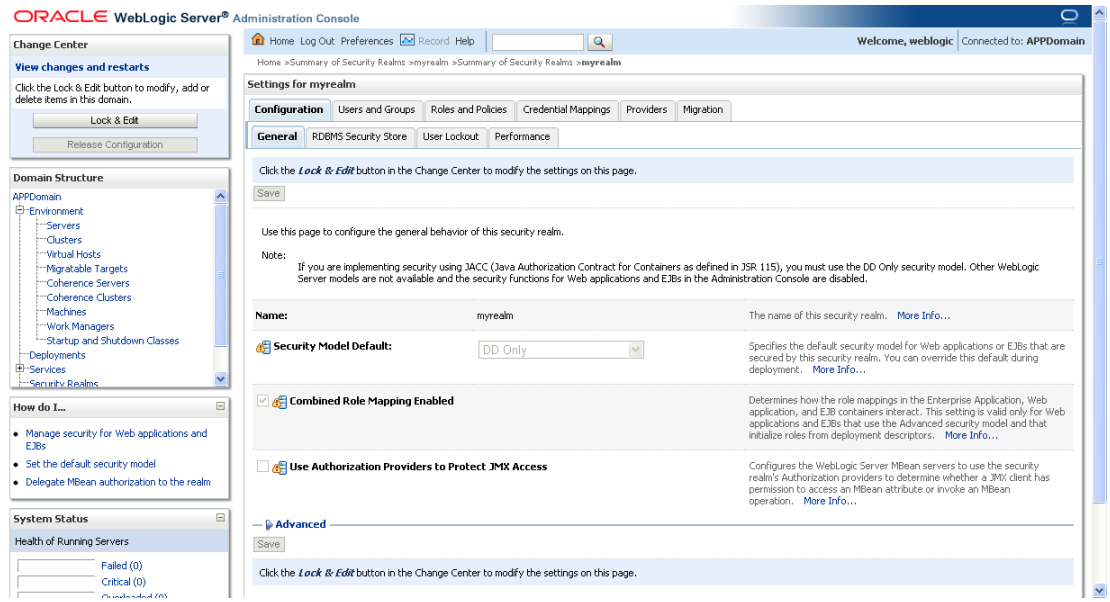
NOTE:

This step is only needed if you plan on using LDAP authentication for the SIM application. This can be skipped if DB authentication is going to be used.

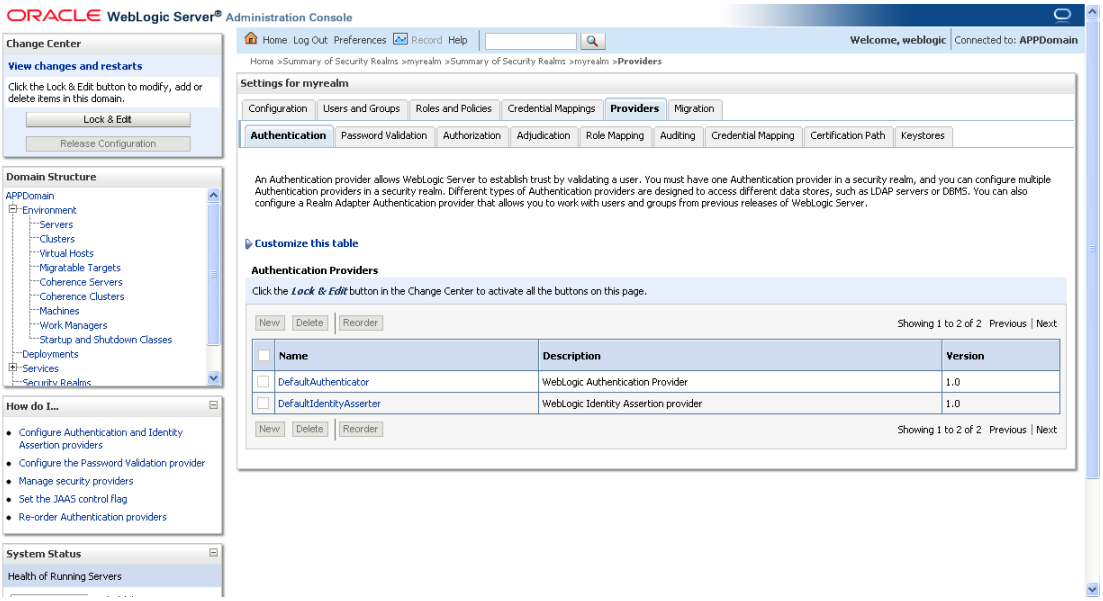
1. Log in to the Administration Console.
   http://<host>:<port>/console/
2. In the Domain Structure frame, click **Security Realms**.



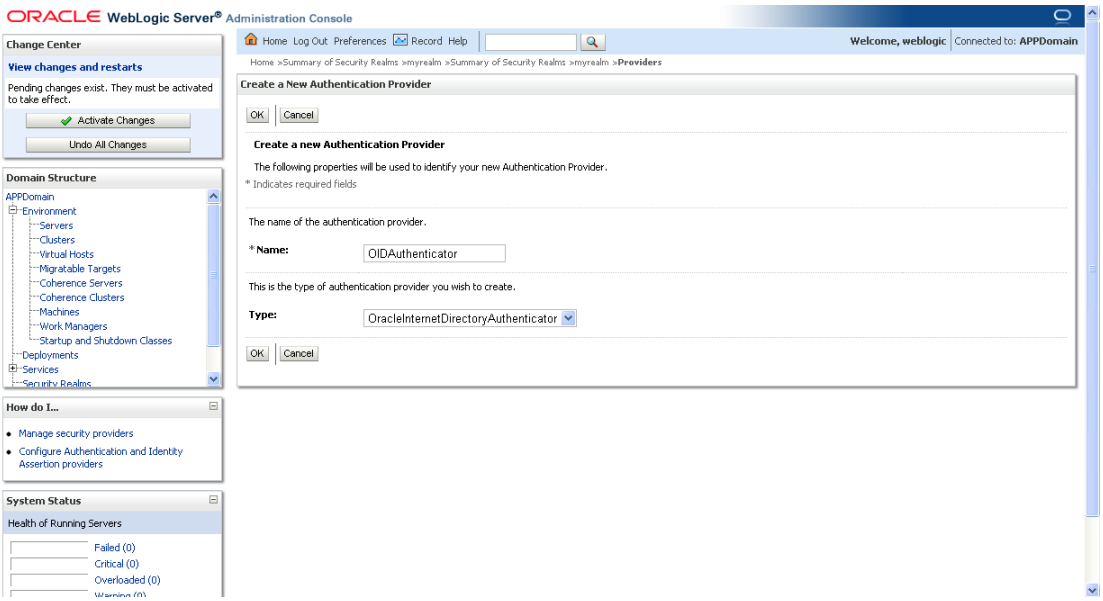
3. In the Realms table, click myrealm. The Settings for myrealm page is displayed.



4. Click the Providers tab.

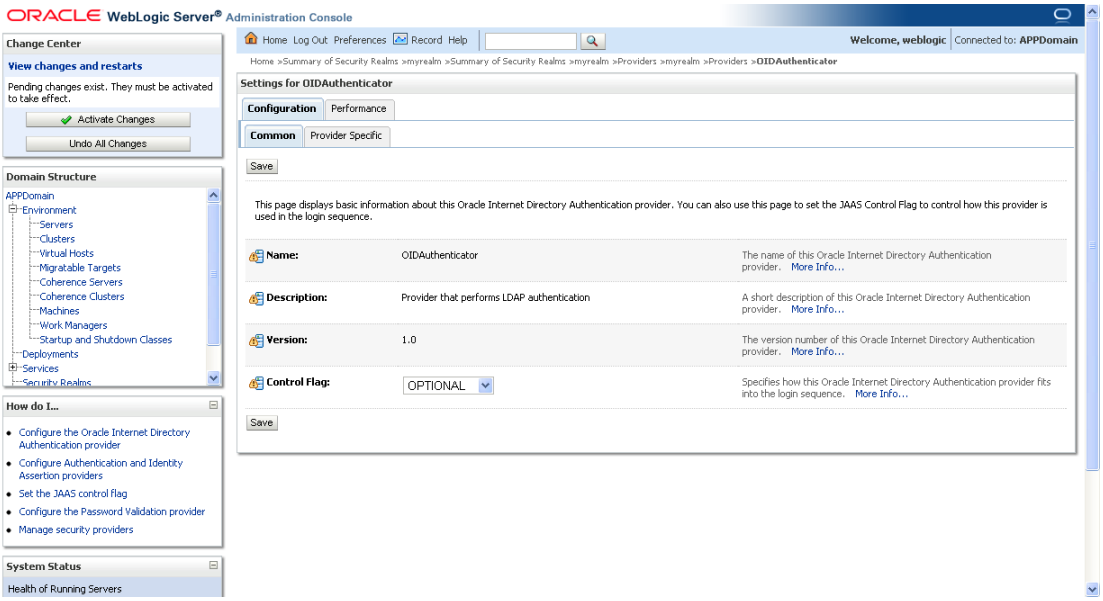


5. Click **Lock & Edit** and then click **New**. The Create a New Authentication Provider page is displayed.

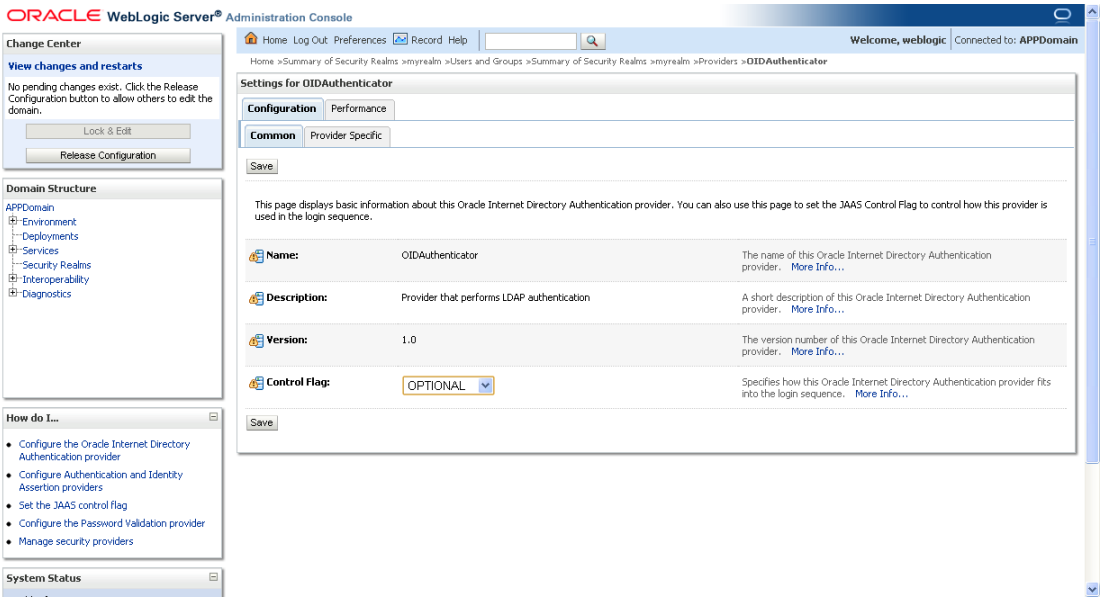


6. Enter **OIDAuthenticator** in the Name field and select **OracleInternetDirectoryAuthenticator** as the type.

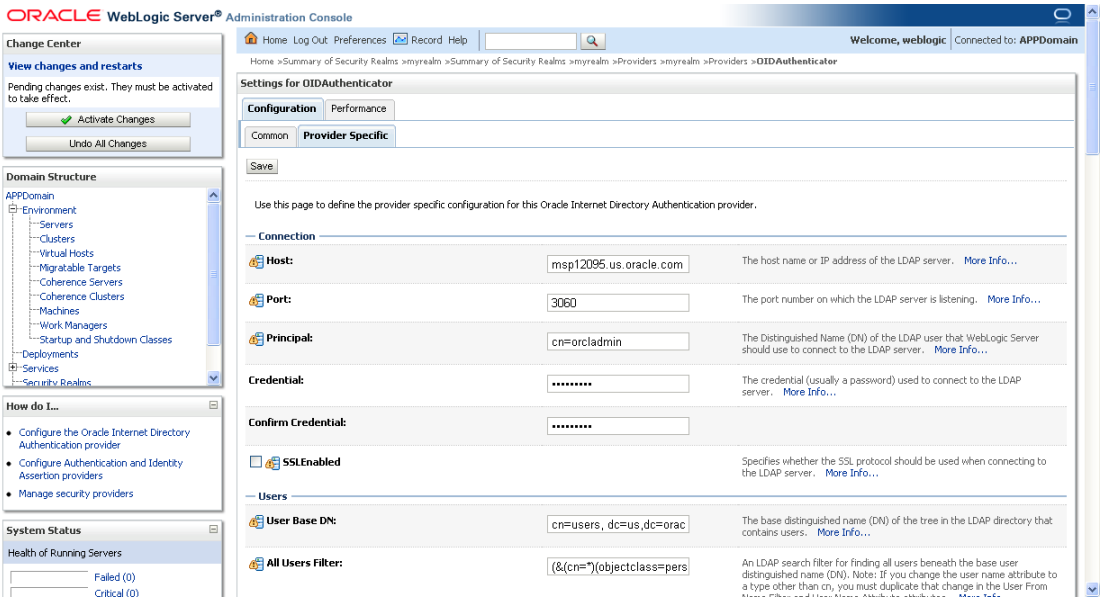
7. Click **OK**. The Settings for OIDAuthenticator page is displayed.



8. Set the Control Flag field to Optional and click **Save**. The Control Flag should be set as Optional so users do not get locked out of the Admin console if there is a typo.
9. Once your changes are saved, click **Activate Changes**.



10. Click the Provider Specific tab and click **Lock & Edit**.



11. Supply your LDAP connection and credentials.

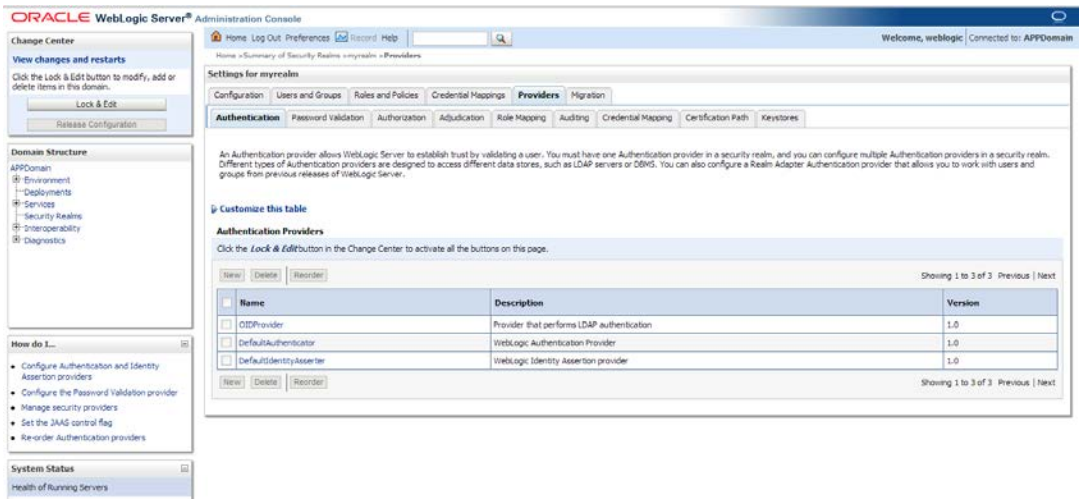
    The entries below are examples only. You should match the entries to your OID. Example:

    - Host: msp12095.us.oracle.com
    - Port: 3060
    - Principal: cn=orcladmin
    - Credential: <*password*>
    - Confirm Credential: <*password*>
    - User Base DN: cn=users,dc=us,dc=oracle,dc=com

      This is the Users DN in your LDAP, where you had set up all your users. This Users DN is installed as part of your OID configuration.
    - Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com

      This is the Groups DN in your LDAP, which has all the groups. This Groups DN is installed as part of your OID configuration.
    - Check **Propagate Cause For Login Exception**

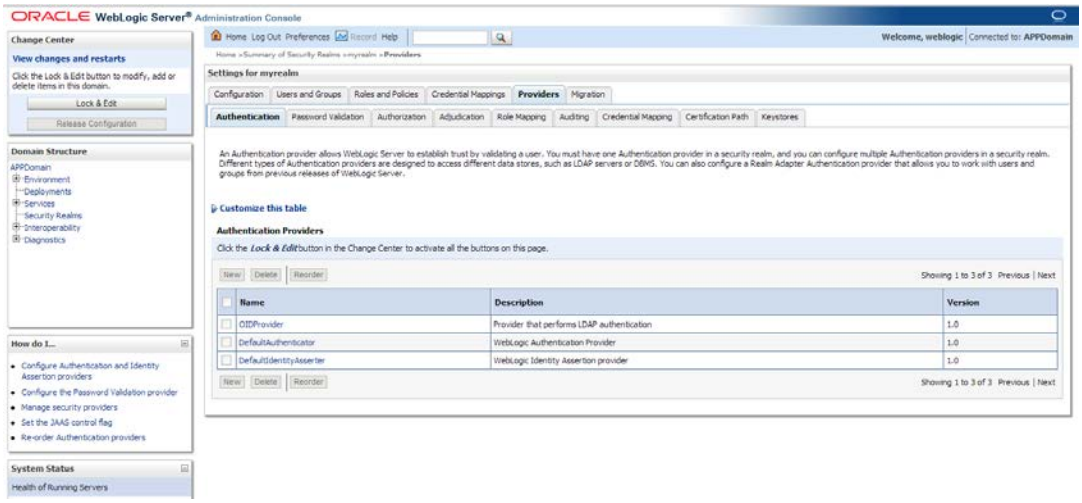
12. Click **Save**.



13. Click **Reorder**.
14. Order OIDAuthenticator first and DefaultAuthenticator second.
15. Click **Save**.
16. Once your changes are saved, click **Activate Changes**.
17. Shut down all servers and restart the admin server.

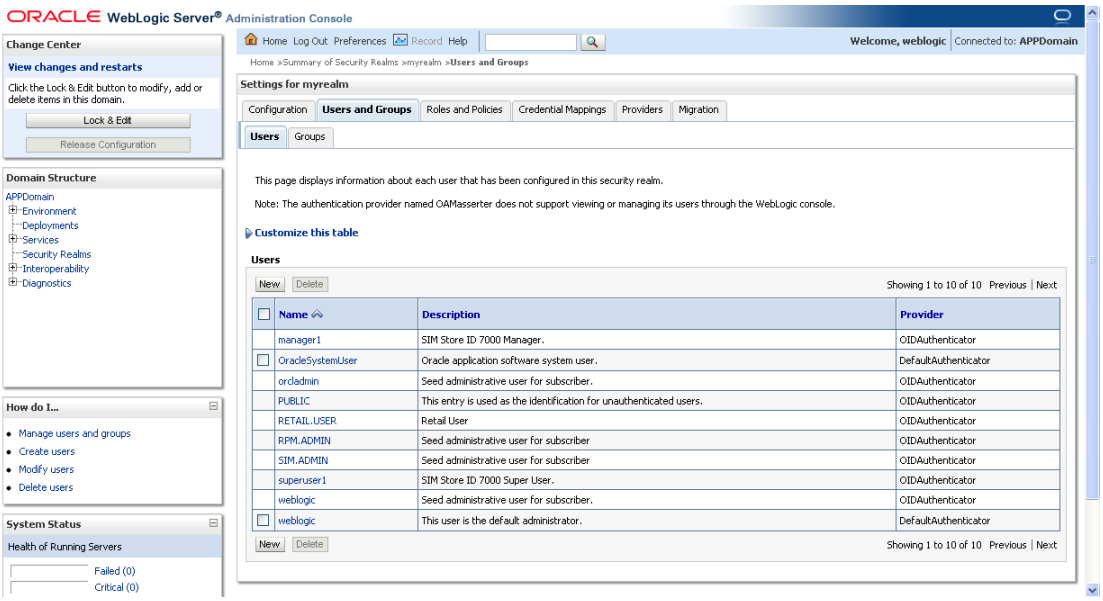
Verify and Set OID Authenticator

1. Log in to the Administration Console.
   http://<host>:<port>/console/
2. In the Domain Structure frame, click Security Realms.
3. In the Realms table, click Default Realm Name. The Settings page is displayed.
4. Click the Providers tab.

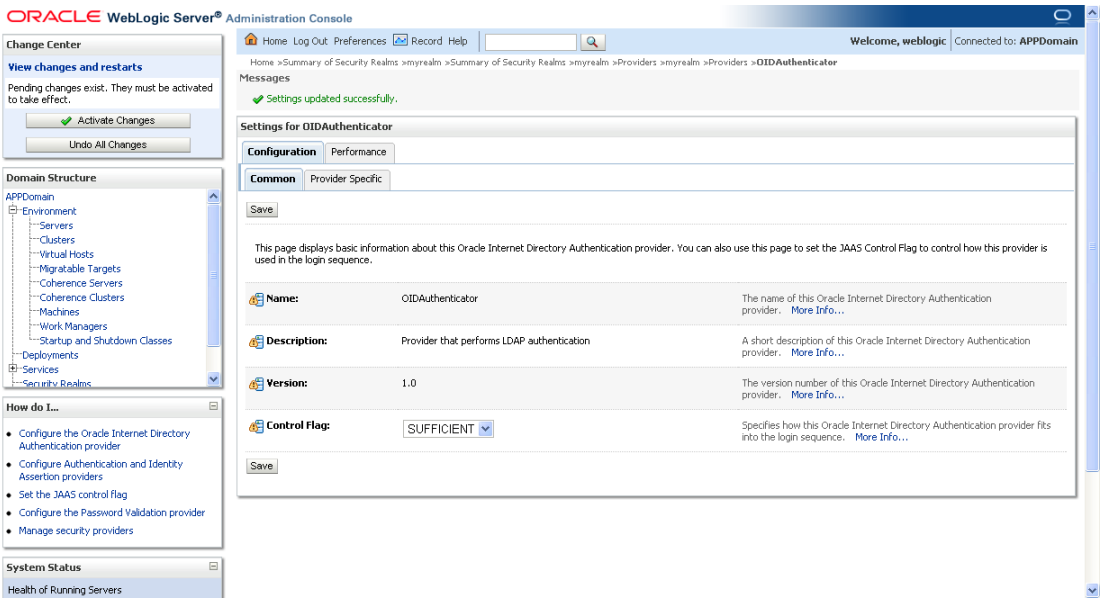


5. Click the Users and Groups tab to see a list of users and groups contained in the configured authentication providers.

   You should see usernames from the Oracle Internet Directory configuration, which implicitly verifies that the configuration is working.



6. Click the Providers tab and click OIDAuthenticator.



7. Set Control Flag to SUFFICIENT and click **Save**.
8. Click **Activate Changes** and restart the entire SIMDomain.

Set the LANG Environment Variable

The LANG environment variable must be set in the profile of the UNIX user who owns the application server ORACLE_HOME files. If you change the value of LANG or set the value for the first time, you must restart the Application Server in order for the change to take effect.

Example:

LANG=en_US

export LANG

Set the Environment Variables for the SIM Installer

1. Set the following environment variables for the SIM installer (the following are just examples, use values for appropriate for your environment):

```
export ORACLE_HOME=/u00/webadmin/product/wls_retail
export
WEBLOGIC_DOMAIN_HOME=/u00/webadmin/product/wls_retail/user_projects/domains/SI
MDomain
export JAVA_HOME=/u00/webadmin/product/jdk_java
export PATH=$JAVA_HOME/bin:$PATH
```

2. If a secured datasource is going to be configured you also need to set "ANT_OPTS" so the installer can access the key and trust store that is used for the datasource security:

```
export ANT_OPTS="-Djavax.net.ssl.keyStore=<PATH TO KEY STORE> -
Djavax.net.ssl.keyStoreType=jks -Djavax.net.ssl.keyStorePassword=<KEYSTORE
PASSWORD> -Djavax.net.ssl.trustStore=<PATH TO TRUST STORE> -
Djavax.net.ssl.trustStoreType=jks -
Djavax.net.ssl.trustStorePassword=<TRUSTSTORE PASSWORD>"
```

   An example of this would be:

```
export ANT_OPTS="-
Djavax.net.ssl.keyStore=/u00/webadmin/product/wls_retail
/wlserver_10.3/server/lib/msp52278.keystore -Djavax.net.ssl.keyStoreType=jks -
Djavax.net.ssl.keyStorePassword=retail123 -Djavax.net.ssl.trustStore=/
u00/webadmin/product/wls_retail
/wlserver_10.3/server/lib/msp2278.keystore -Djavax.net.ssl.trustStoreType=jks
-Djavax.net.ssl.trustStorePassword=retail123"
```

Run the SIM Application Installer

This installer configures and deploys the SIM application and Java WebStart client files.

1. If you are using an X server such as Exceed, set the DISPLAY environment variable so that you can run the installer in GUI mode (recommended). If you are not using an X server, or the GUI is too slow over your network, unset DISPLAY for text mode.
2. Verify that the managed server to which SIM will be installed is currently running.
3. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created: <INSTALL_DIR>/sim/application/logs/sim-install-app.<timestamp>.log.

Note: The manual install option in the installer is not functional for this release. See the section, "Files not available to copy at the end of installation, results in non working applications – Weblogic only" in Appendix E: Common Installation Errors.

Note: See Appendix: SIM Application WebLogic Server Installer Screens for details on every screen and field in the WebLogic application installer.

Note: See Appendix: Common Installation Errors for details on common installation errors.

Clustered Installations – Post-Installation Steps

Skip this section if you are not clustering the application server.

If you are installing the SIM application to a clustered Web Logic Server environment, there are some extra steps you need to take to complete the installation. In these instructions, the application server node with the ORACLE_HOME you used for the SIM installer is referred to as the master server. All other nodes are referred to as the remote server.

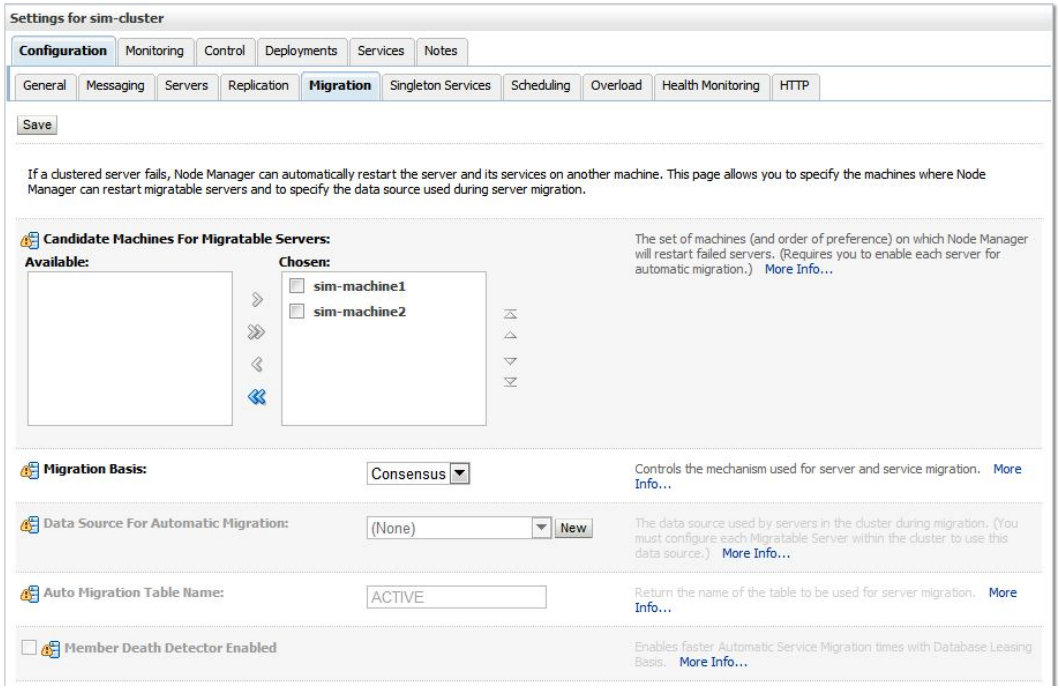
Copy the <weblogic domain path>/retail/sim14 directory from the master server to each remote server that is a member of the cluster that contains the deployed sim application.

In addition, if SIM has been installed in a cluster, the Migration Basis needs to be set to use "consensus" and all machines in the cluster chosen for migration. This is done with the following procedure.

Note: This needs to be done after the SIM application has been successfully installed to the sim-cluster using the SIM installer. If the SIM application is ever re-installed for any reason the following will have to be re-done as well.

1. Click "Lock & Edit" in the Change Center
2. Go to cluster migration screen in the Weblogic Administration Console. i.e.: SIMDomain > Environment > Clusters > sim-cluster > Configuration (tab) > Migration (tab)
3. Set migration basis to Consensus.
4. Select all machines in the SIM cluster as candidates.
5. Hit save.
6. Click "Activate Changes" in the Change Center
7. Restart the servers in the SIM cluster

The migration setup should look similar to the following:

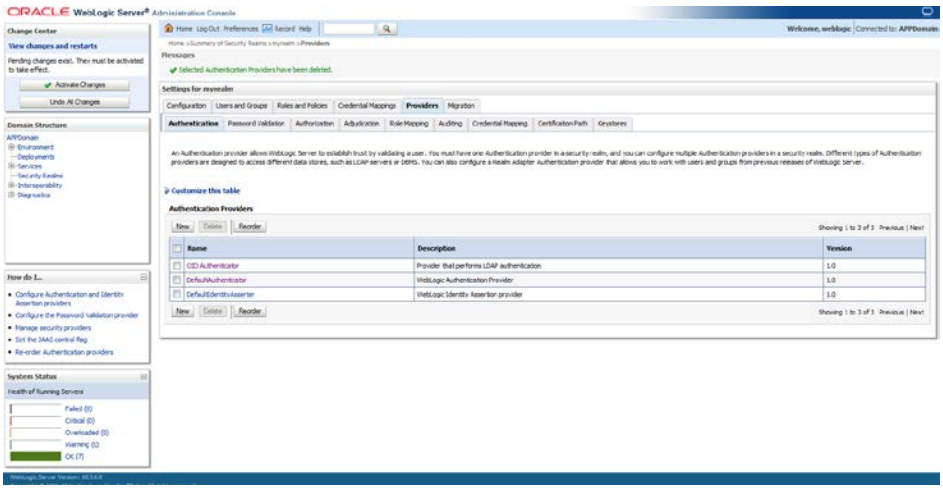


SIM Database Authentication Provider set up (to be done after the application deploy)

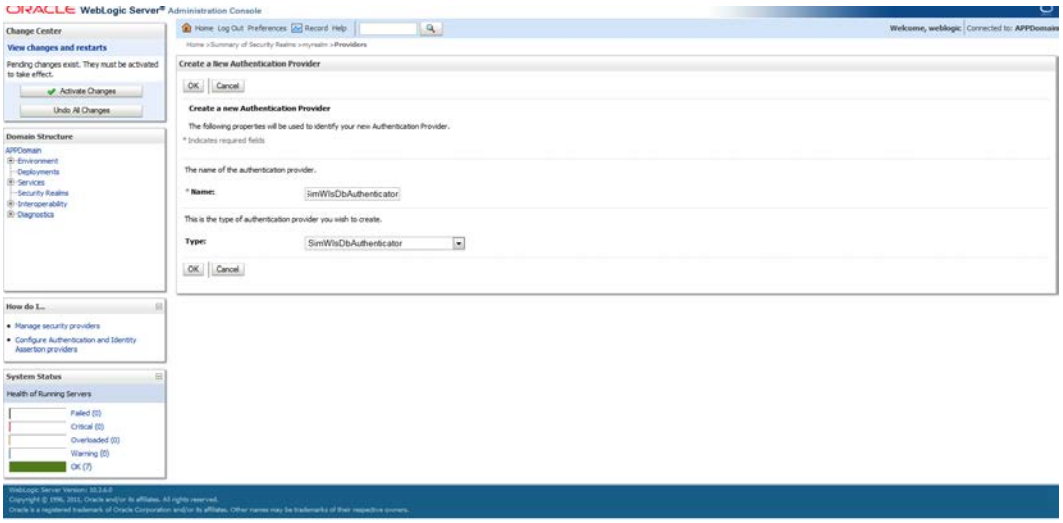
Note: This step is only needed if you plan in using database authentication for the SIM application. This can be skipped if LDAP is going to be used for authentication.

1. Shut down all the servers of the WebLogic Domain created.
2. Once you extract the SIM installer to <INSTALL_DIR> copy the sim-security.zip present in <INSTALL_DIR>/sim/application/sim14 to the WEBLOGIC_DOMAIN_HOME/lib and extract it contents in the folder.
3. Start the domain admin server.
4. Log into the WebLogic console.

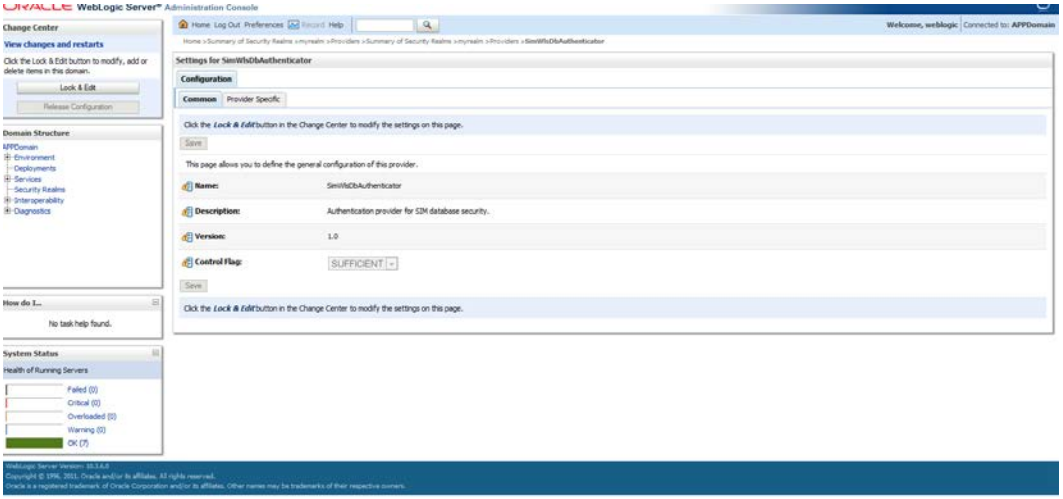
5. Navigate to: security realms -> myrealm (default realm) -> providers.



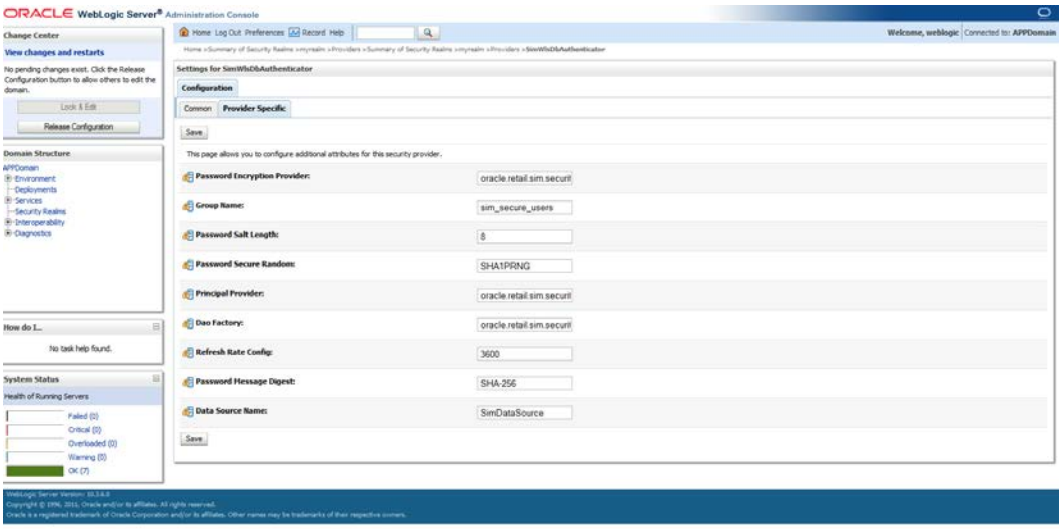
6. Start a Lock and Edit session.
7. Click New provider.
8. Select the provider type from the list: SimWlsDbAuthenticator.
9. Set the provider name (Default: SimWlsDbAuthenticator).



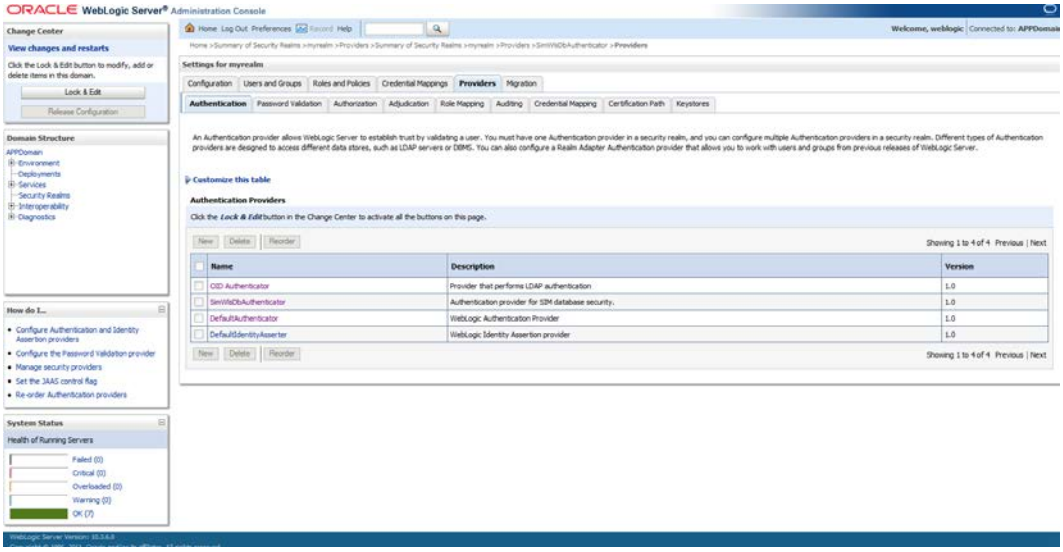
10. Click **Ok**.
11. Open the new provider configuration.
12. Under Common, set the Control Flag to SUFFICIENT.



13. Click **Provider Specific**.
14. The SIM Data Source Name defaults to SimDataSource which is what the SIM installer creates, so it should be left to the default value.



15. Check that the GroupName is set to the name of the group used for SIM secure users.
16. Click **Ok**.
17. On the provider list, click **Reorder**.



18. Move the SimDbAuthenticator to the top of the list, or above the DefaultAuthenticator.
19. Click **Ok**.
20. Click **Activate Changes**.
21. Shutdown the admin server.
22. Start the admin and managed servers for the domain.

Review and/or Configure Oracle Single Sign-On

Note: This step is only needed if you plan on setting up the SIM application using Single Sign On (SSO) authentication. This can be skipped if SSO is not going to be configured for this environment. The Oracle Access manager must be configured and the Oracle http server (Webtier and webgate) must be registered into the Oracle Access Manager.

Create the SIM SSO provider in the SIMDomain

1. Shut down all the servers of the WebLogic Domain created.
2. Once you copy the contents to <INSTALL_DIR> copy the sim-security.zip present in <INSTALL_DIR>/sim/application/sim14 to the WEBLOGIC_DOMAIN_HOME/lib and extract it contents in the folder.
3. Start the domain admin server.
4. Log into the WebLogic console
5. Navigate to: security realms -> myrealm (default realm) -> providers.
6. Start a Lock and Edit session.
7. Click **New provider**.
8. Select the provider type from the list: **SimWlsSsoAuthenticator**.

9. Set the provider name (Default: SimSsoAuthenticator).
10. Click **Ok**.
11. Open the new provider configuration.
12. Under Common, set the Control Flag to SUFFICIENT.
13. Click **Provider Specific**.
14. Check that the GroupName is set to the name of the group used for SIM secure users (sim_secure_users by default).
    - The group 'sim_secure_users' must have been created in the LDAP in cn=Groups container as part of the section 'SIM LDAP Users/Groups/Roles Setup'.
15. All other values under the Provider Specific tab can be left as the default value.
16. Click **Ok**.
17. On the provider list, click **Reorder**.
18. Move the SimWlsSsoAuthenticator to the top of the list, or above the DefaultAuthenticator.
19. Click **Ok**.
20. Click **Activate Changes**.
21. Shutdown the domain.
22. Start the admin and managed servers for the domain.

After the SSO provider is created in the SIMDomain, you will also have to set the protection of the SIM application resources correctly in the Application Domain that has been registered in the Oracle Access Manager.

In the Webtier/Webgate http server you need to set the mod_wl_ohs.conf file to redirect the http call to the where the SIM application has been deployed.

For example, in mod_wl_ohs.conf set:

```
<Location /sim-client >
 WebLogicCluster msp52278.us.oracle.com:17015
 SetHandler weblogic-handler
 ErrorPage downtime.html
</Location>
```

Then in Oracle Access Manager, set the protection of the resources in the Application Domain that has been registered for the SIM application. You must protect the /sim-client/launch resource and unprotect the rest:

Resource URL: /sim-client/launch

Protection Level: Protected

Authentication Policy: Protected Resource Policy

Authorization Policy: Protected Resource Policy

Resource URL: /sim-client/.../*

Protection Level: Unprotected

Authentication Policy: Public Resource Policy

Authorization Policy: Public Resource Policy

SIM Batch Scripts

The SIM batch programs are installed in the location that was specified during application installation.

The batch programs can be run from a different location if you cannot run them from under the application server <WEBLOGIC_DOMAIN_HOME>.. To install the batch files in a different location just copy the entire batch folder to the appropriate destination.

The batch directory is assumed to be located on the same server as the application server. If you copy the SIM batch directory to a location on a different server, then you need to configure the file path to the sim-batch.log file, which is defined in batch/resources/log4j.xml.

See the "Batch Detail" section of the *Oracle Retail Store Inventory Management Operations Guide* for information about how to run batches.

Resolving Errors Encountered During Application Installation

If the application installer encounters any errors, it halts execution immediately. You can run the installer in silent mode so that you do not have to retype the settings for your environment. See Appendix D of this document for instructions on silent mode.

See "Appendix: Common Installation Errors "for a list of common installation errors.

Since the application installation is a full reinstall every time, any previous partial installs are overwritten by the successful installation.

Web Help Files

The application installer automatically copies the web help files to the proper location. They are accessible from the help links within the application.

Starting and Stopping the Wavelink Server

In order to use handheld wireless devices with SIM, the Wavelink server must be running. The SIM application installer installs, configures, and starts the Wavelink server for you, so once the SIM application install is complete, the Wavelink server is ready to be used.

> **Note:** Even if you use the AdminServer to restart SIM, you will still need to restart the Wavelink server manually.

The Wavelink server scripts are installed into the <sim-wireless-directory>/bin.

The following is an example for stopping and starting the Wavelink server:

```
# cd
/u00/webadmin/product/wls_retail/user_projects/domains/SIMDomain/retail/sim14/wire
less/bin
# ./wavelink-shutdown.sh
# ./wavelink-startup.sh
```

Note: The wireless functionality in SIM is dependent on Wavelink and includes a client and server component. Wavelink software ensures that the wireless user interface of SIM can work with various handheld devices.

Server:

The Oracle Retail Wireless Foundation Server is bundled with the SIM server.

Client:

For wireless device to interact correctly with SIM-server, it is required to install appropriate Wavelink studio client on each of the handheld devices.

Please visit the http://www.wavelink.com/download/downloads.aspx site to download studio-client specific to your device.

Please note that only those devices listed with "studio client", will support running of the SIM client.

If the device you need is not listed, you may log an enhancement request with Oracle Retail.

Oracle Retail will work with Wavelink for roadmap considerations.

Each Wavelink studio client has a single session free license. For multiple sessions additional licenses need to be obtained. Please contact your Oracle sales representative or client partner for Wavelink Studio Client and Oracle Retail with your needs.

Note: For configurations of physical handheld devices or wireless network setup, check your hardware manufacturer's manual or Wavelink's studio client information. This information is not covered in this guide.

5

Test the SIM Application

Once SIM database and application are installed, foundation data is imported into SIM, you should have a working SIM application installation. To launch the application client, open a web browser and go to the client URL. You can find the URL in the next steps section of the log file that was produced by the installer.

Example:

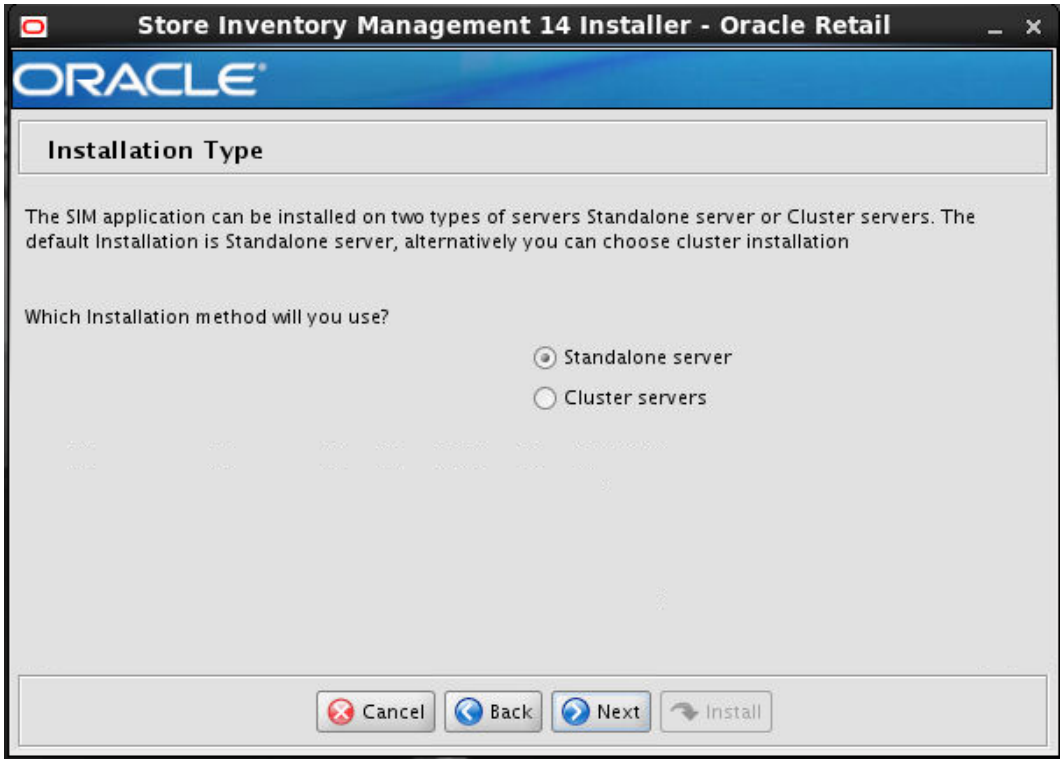
WLS: http://msp52278.us.oracle.com:17015/sim-client/launch

A

Appendix: SIM Application WebLogic Server Installer Screens

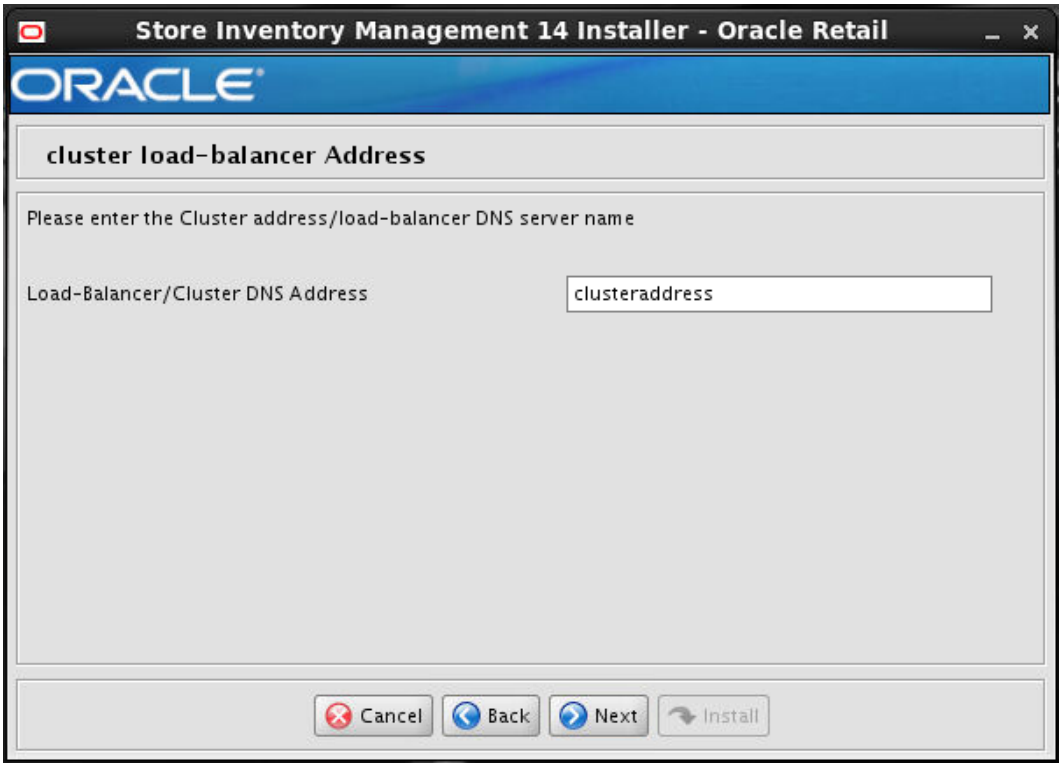
You need the following details about your environment for the installer to successfully deploy the SIM application. Depending on the options you select, you may not see some screens.

Screen: Installation Type



Field Title	Which Installation Method
Field Description	Choosing "Standalone server" will deploy SIM to a non-clustered environment, if "Cluster Servers" is chosen then it will deploy SIM to a cluster of servers defined in WebLogic.

Screen: Cluster load-balancer Address:

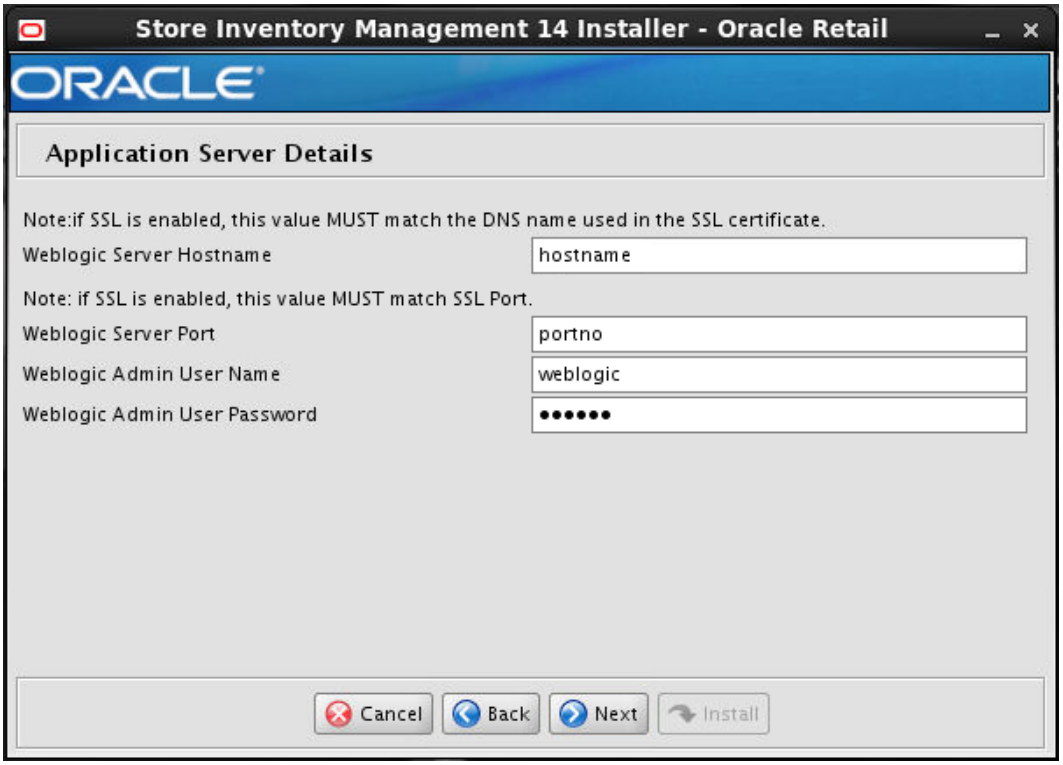


Field Title	Load-Balancer/Cluster DNS Address
Field Description	This contains the IP address of the load balancer that will be used if a SIM is to be deployed to a clustered environment

Screen: Security Details

Field Title	Enable SSL for SIM?
Field Description	Choosing yes will deploy SIM using SSL, and will configure SIM to use SSL. In this case, SSL must be configured and enabled for the admin server and SIM managed server or cluster. Choosing no will deploy and configure SIM without SSL.

Screen: Application Server Details



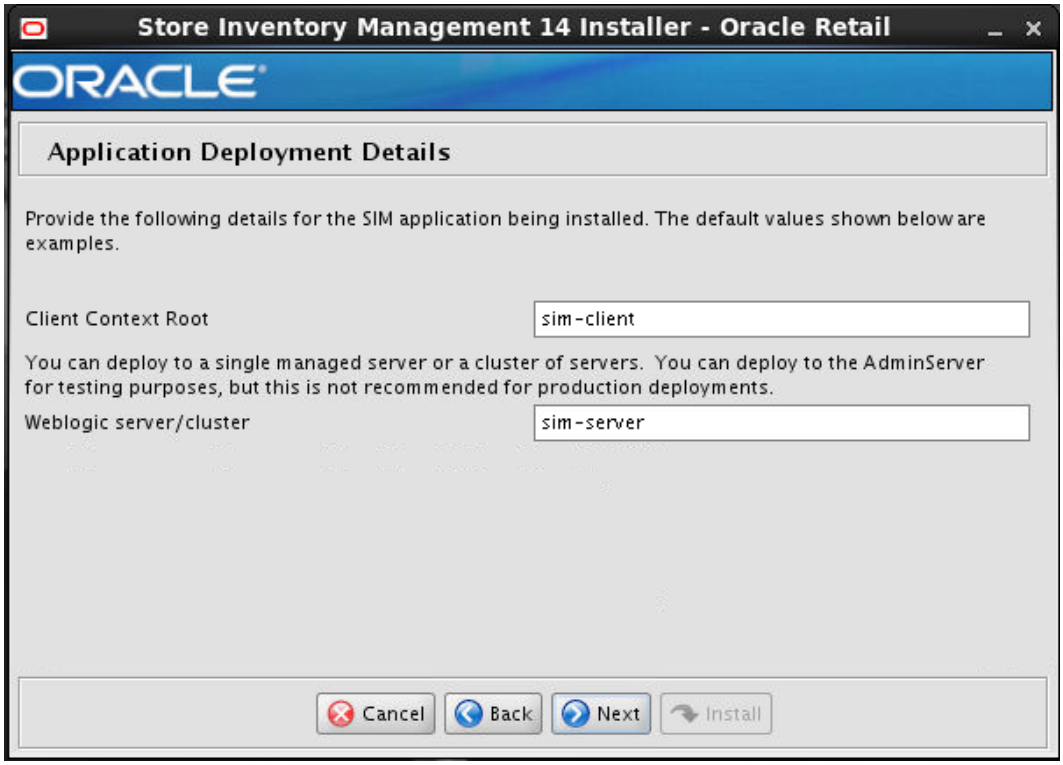
Field Title	WebLogic Server Hostname
Field Description	The hostname of the server where the WebLogic server is installed
Example	msp28076
Notes	Used by installer scripts to deploy EAR and WAR files and to create default inputs for client codebase and JNDI provider URL

Field Title	WebLogic Admin Port
Field Description	Listen port for the WebLogic Admin server
Example	17001

Field Title	WebLogic Admin User
Example	WebLogic
Notes	Used by installer scripts to deploy EAR and WAR files

Field Title	WebLogic Admin Password
Field Description	The password of the WebLogic Admin User
Notes	Used by installer scripts to deploy EAR and WAR files

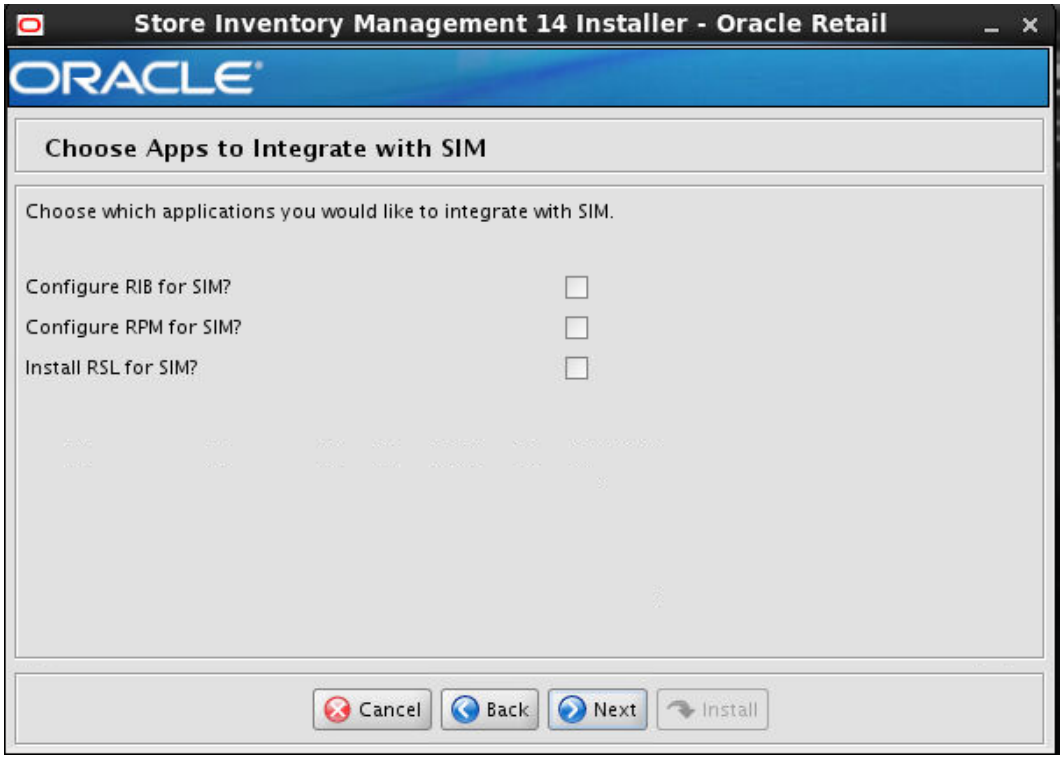
Screen: Application Deployment Details



Field Title	Client Context Root
Field Description	Context root for sim client
Example	sim-client

Field Title	WebLogic server/cluster
Field Description	This the managed server name for standalone deployment and Cluster name for deployment to clustered managed servers
Example	sim-server

Screen: Choose Apps to Integrate with SIM

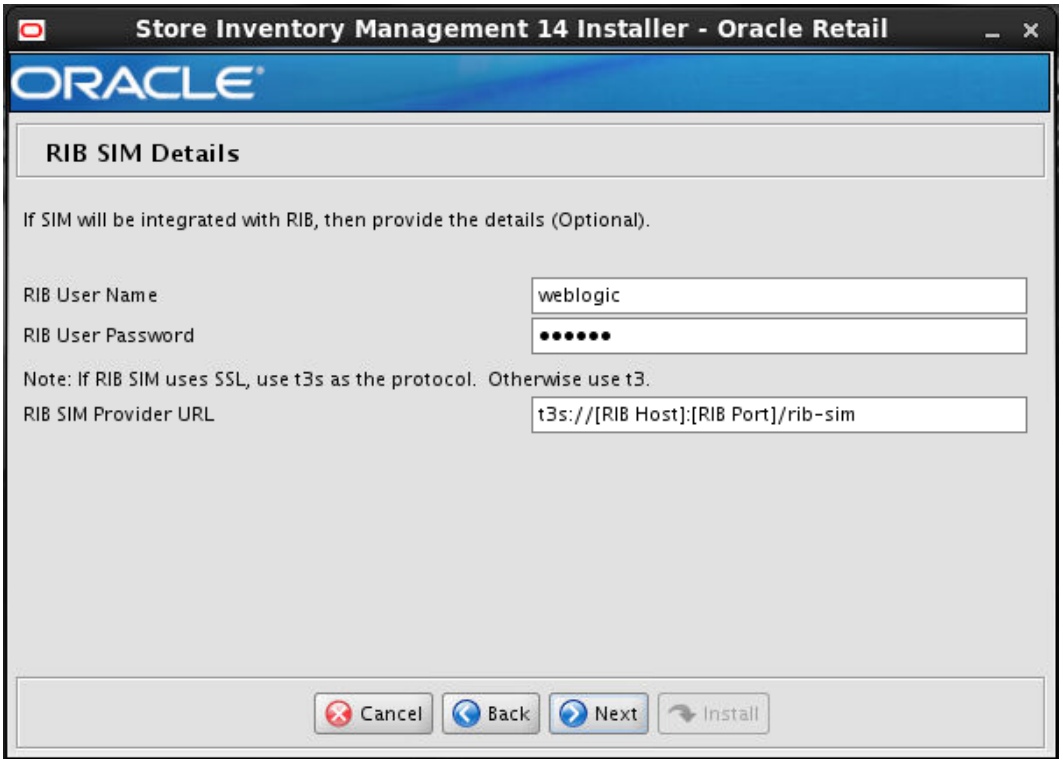


Field Title	Configure RIB for SIM?
Field Description	Select this option if you will be using RIB with SIM.

Field Title	Configure RPM for SIM?
Field Description	Select this option if you will be using RPM with SIM.

Field Title	Install RSL for SIM?
Field Description	Select this option if you will be using RSL with SIM.

Screen: RIB SIM Details

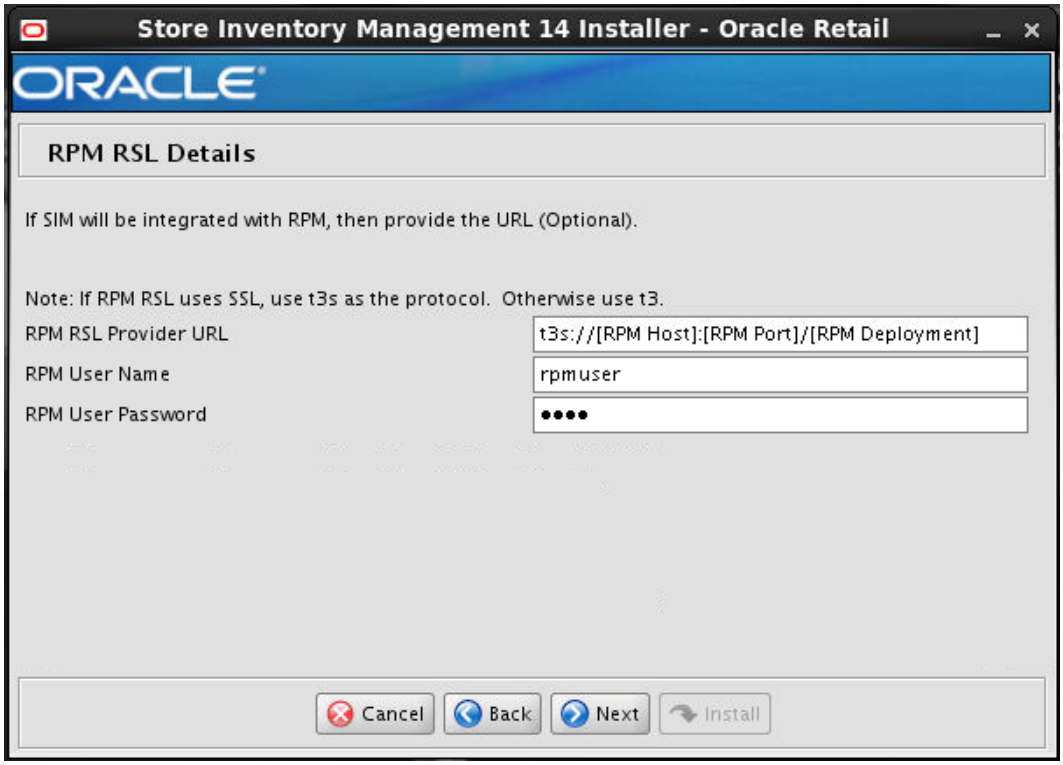


Field Title	RIB User Name
Field Description	This is the user name for the JNDI connection to the RIB Admin Server
Example	WebLogic

Field Title	RIB user password
Field Description	Password for the RIBforSIM 14.0 user.

Field Title	RIB SIM Provider URL
Field Description	This the provider URL of the rib-sim application
Examples	t3://msp52423.us.oracle.com:19106/rib-sim

Screen: RPM RSL Details

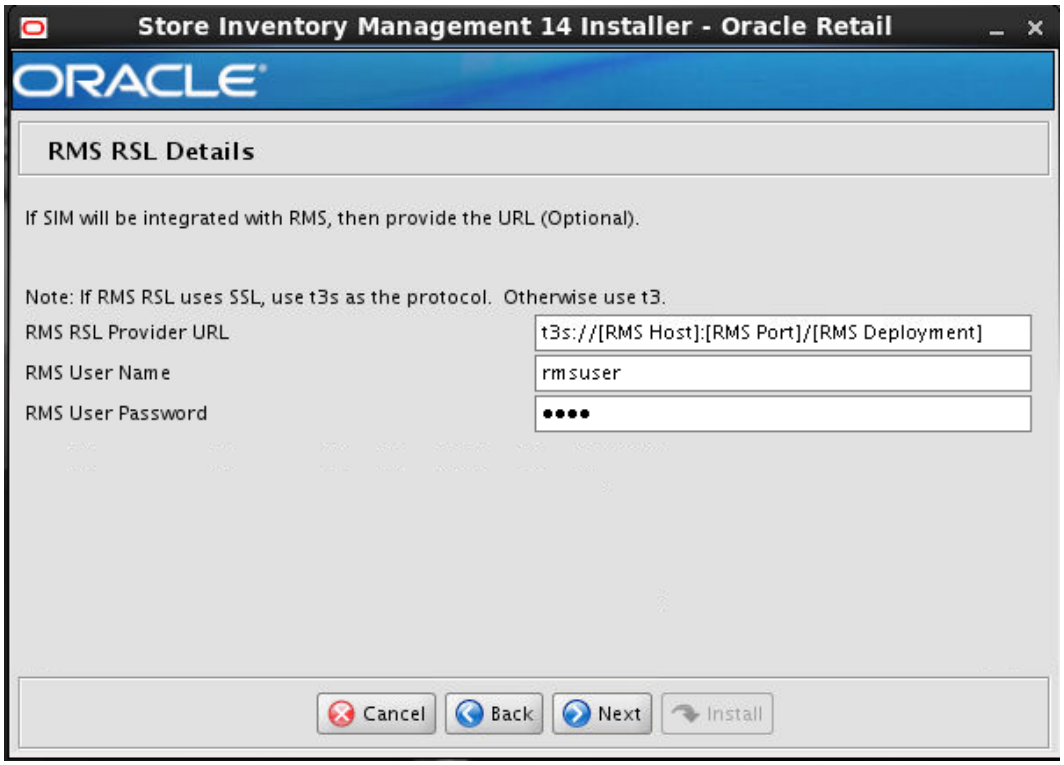


Field Title	RPM RSL Provider URL
Field Description	This is the provider URl for the RPM RSL JNDI connection
Example	t3://msp52278.us.oracle.com:17011/rpm14

Field Title	RPM User Name
Field Description	This is the user which has access to RPM server.
Example	retail.user

Field Title	RPM Password
Field Description	This is the password of the user provided for RPM WebLogic Admin user in the above.

Screen: RMS RSL Details

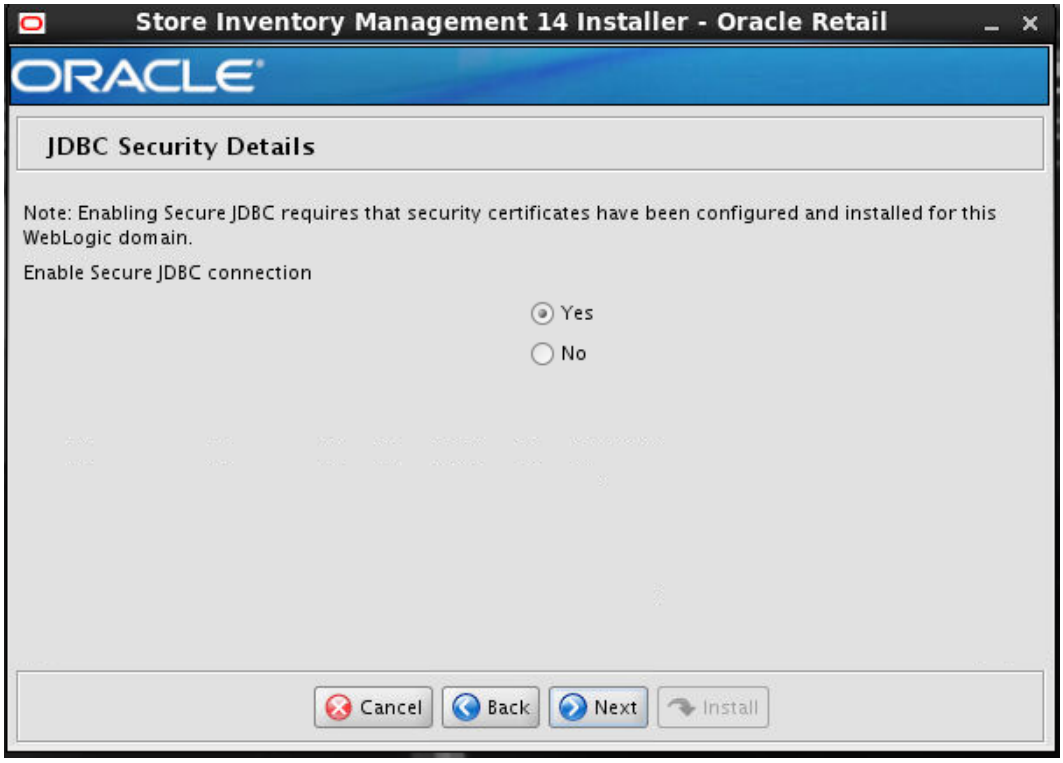


Field Title	RMS RSL Provider URL
Field Description	This is the provider URL for the RSLforRMS
Example	t3://msp52278.us.oracle.com:17013/rsl-rms

Field Title	RMS User Name
Field Description	This is the user name for login to RSL for RSM WebLogic Server.
Example	WebLogic

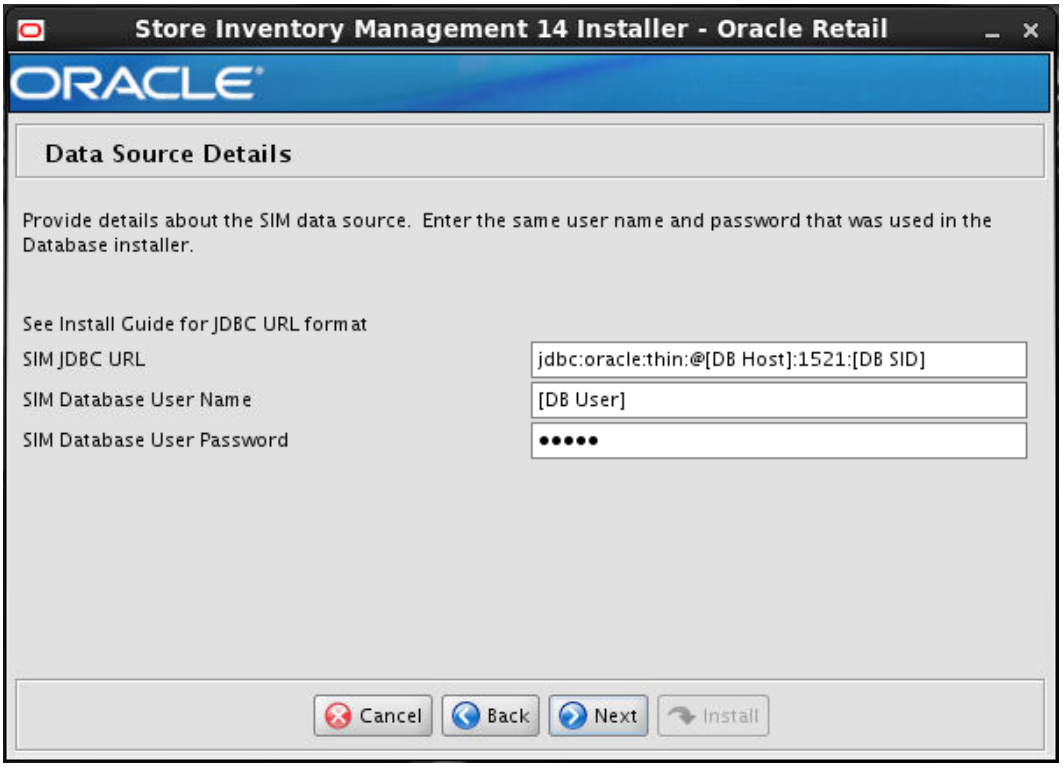
Field Title	RMS User Password
Field Description	This is the password of the user provided for RSL for RMS WebLogic Admin user in the above.

Screen : JDBC Security Details



Field Title	Enable Secure JDBC connection
Field Description	Choose "Yes" if you have a secured datasource already set up, otherwise choose "No"

Screen: Data Source Details

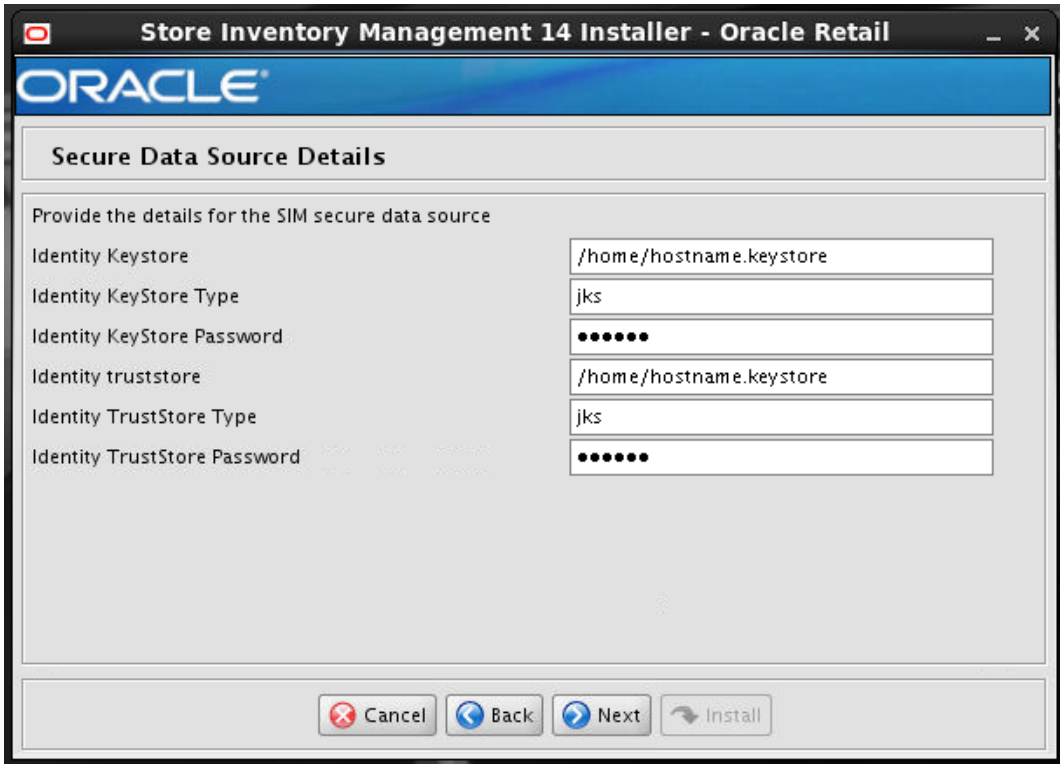


Field Title	SIM JDBC URL
Field Description	URL used by the SIM application to access the SIM database schema.
Destination	WebLogic admin server
Example	Standard Thin Connection: jdbc:oracle:thin:@myhost:1521:mysimsid RAC connection: jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS_LIST =(ADDRESS = (PROTOCOL = TCP)(HOST = myhost1)(PORT = 1521))(ADDRESS = (PROTOCOL = TCP)(HOST = myhost2)(PORT = 1521))(LOAD_BALANCE = yes))(CONNECT_DATA =(SERVICE_NAME = mysimsid))) Secured connection: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL =**tcps**)(HOST=myshost1)(PORT=2484)))(CONNECT_DATA=(SERVICE_NAME =mysimsid)))

Field Title	SIM Database Username
Field Description	The SIM Database schema name
Destination	WebLogic admin server
Notes	The schema name should match the name you provided when you ran the database schema installer.

Field Title	SIM Database User Password
Field Description	The password for the SIM Database Schema
Destination	WebLogic admin server

Screen: Secure Data Source Details (shown if "Secure JDBC connection" enabled):



Field Title	Identity Keystore
Field Description	Path to the identity keystore, i.e.: /u00/webadmin/product/identity.keystore

Field Title	Identity Keystore Type
Field Description	i.e. JKS

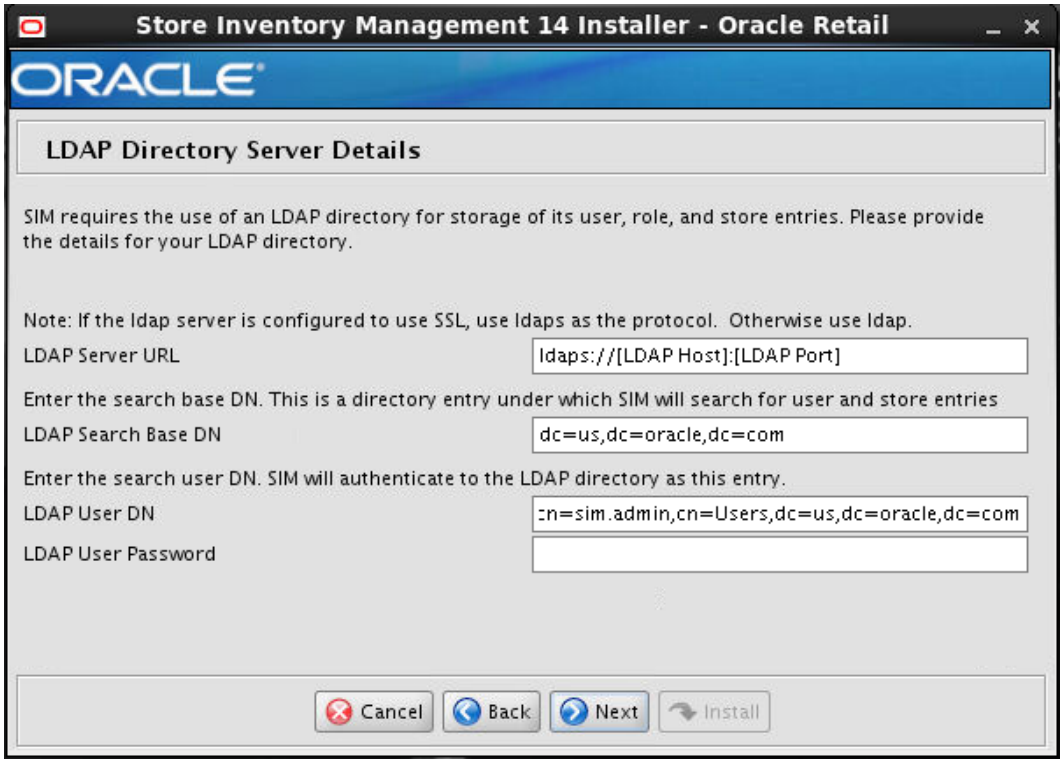
Field Title	Identity Keystore Password
Field Description	Password used to access the identity keystore defined above

Field Title	Identity Trustore
Field Description	Path to the identity truststore. For example: /u00/webadmin/product/identity.truststore

Field Title	Identity Truststore Type
Field Description	For example: JKS

Field Title	Identity Truststore Password
Field Description	Password used to access the identity truststore defined above

Screen: LDAP Directory Server Details



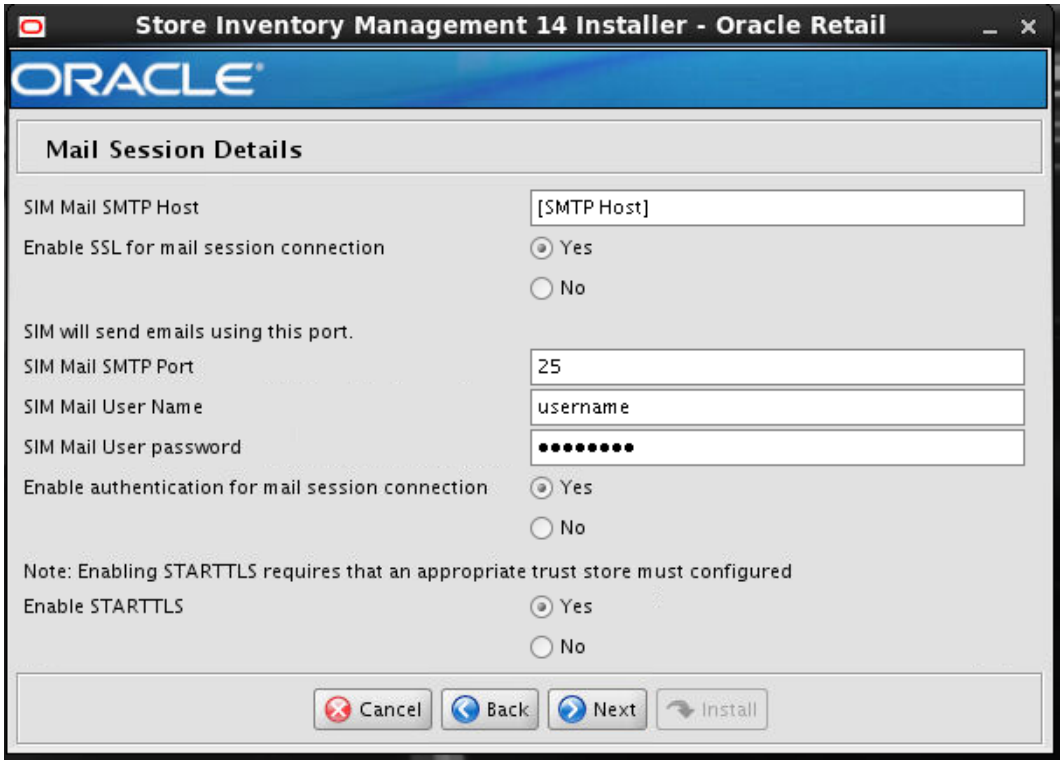
Field Title	LDAP server URL
Field Description	URL for your LDAP directory server.
Example	Non-secured ldap: ldap://myhost:3060/ Secured ldap: ldaps://myhost:3061/

Field Title	LDAP Search Base DN
Field Description	The directory entry under which SIM will search for user and store entries.
Example	dc=us,dc=oracle,dc=com

Field Title	Search User DN
Field Description	Distinguished name of the user that RPM uses to authenticate to the LDAP directory.
Example	cn=sim.admin,cn=Users,dc=us,dc=oracle,dc=com

Field Title	Search User Password
Field Description	Password for the search user DN.

Screen: Mail Session Details



Field Title	SIM Mail SMTP Host
Field Description	The SMTP server that will be used to send notification emails from SIM.
Example	mail.oracle.com

Field Title	Enable SSL for Mail session connection
Field Description	"yes" for secure connection 'No" for plain connection

Field Title	SIM Mail SMTP Port
Field Description	Port that the mail client is configured to use

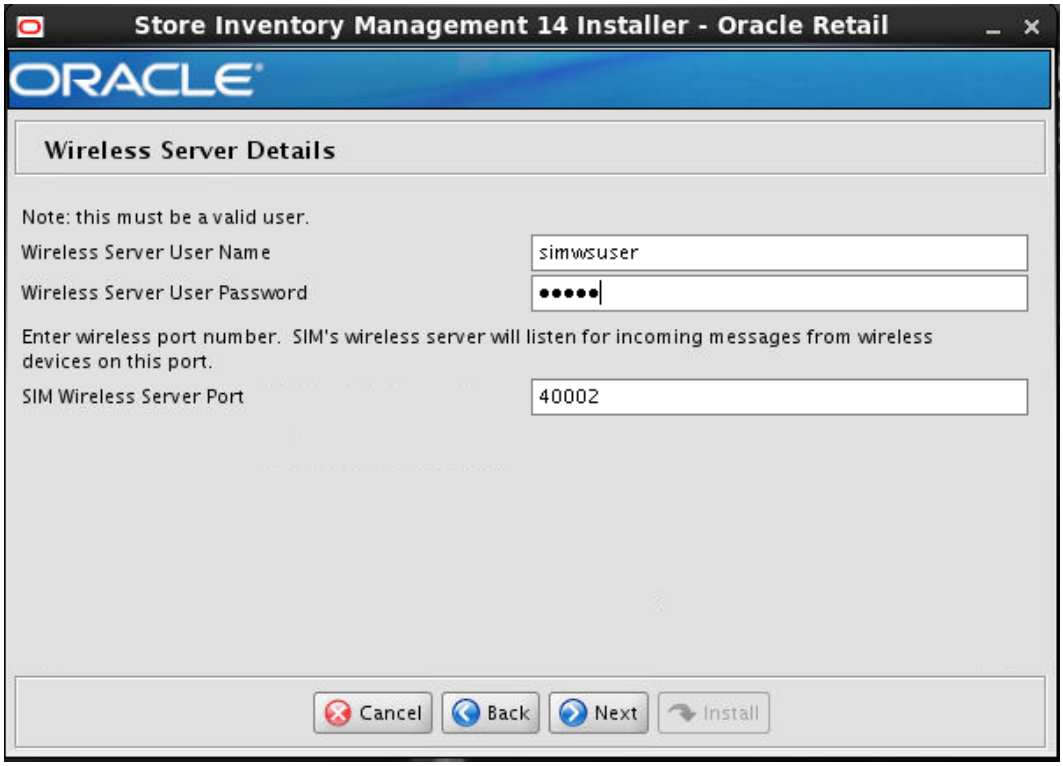
Field Title	SIM Mail User Name
Field Description	Username used to access the mail client

Field Title	SIM Mail User Password
Field Description	Password for the above user

Field Title	Enable authentication for mail session connection
Field Description	Yes or no depending on mail client configuration

Field Title	Enable STARTTLS
Field Description	Yes or No depending on mail client configuration

Screen: Wireless Server Details

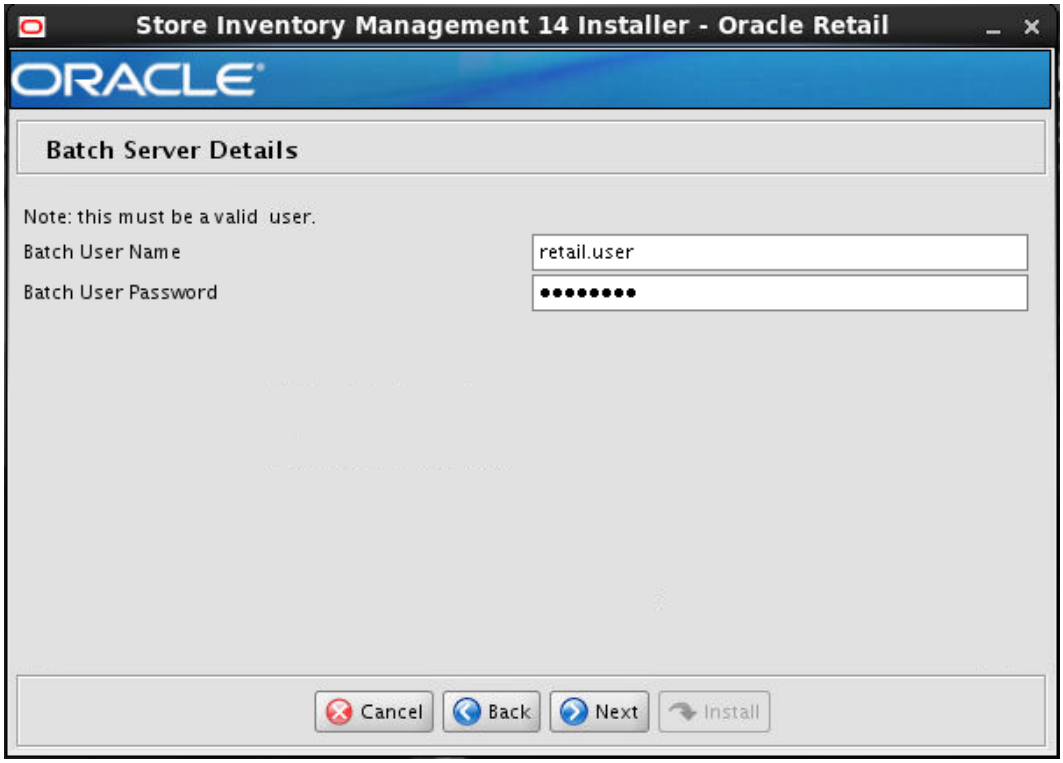


Field Title	Wireless Server User Name
Field Description	User name for wireless server
Destination	Retail config wallet and installer creates WebLogic user with the given name above.

Field Title	Wireless Server User Password
Field Description	Password for wireless server user, the password must follow WebLogic password requirements (at least 8 characters in length and one non-alphabetic character)
Destination	Retail config wallet.

Field Title	SIM Wireless Server Port
Field Description	Choose an available port that the Wavelink server will use to listen for incoming messages from wireless devices
Destination	wireless.cfg, wavelink-startup.sh
Example	40002

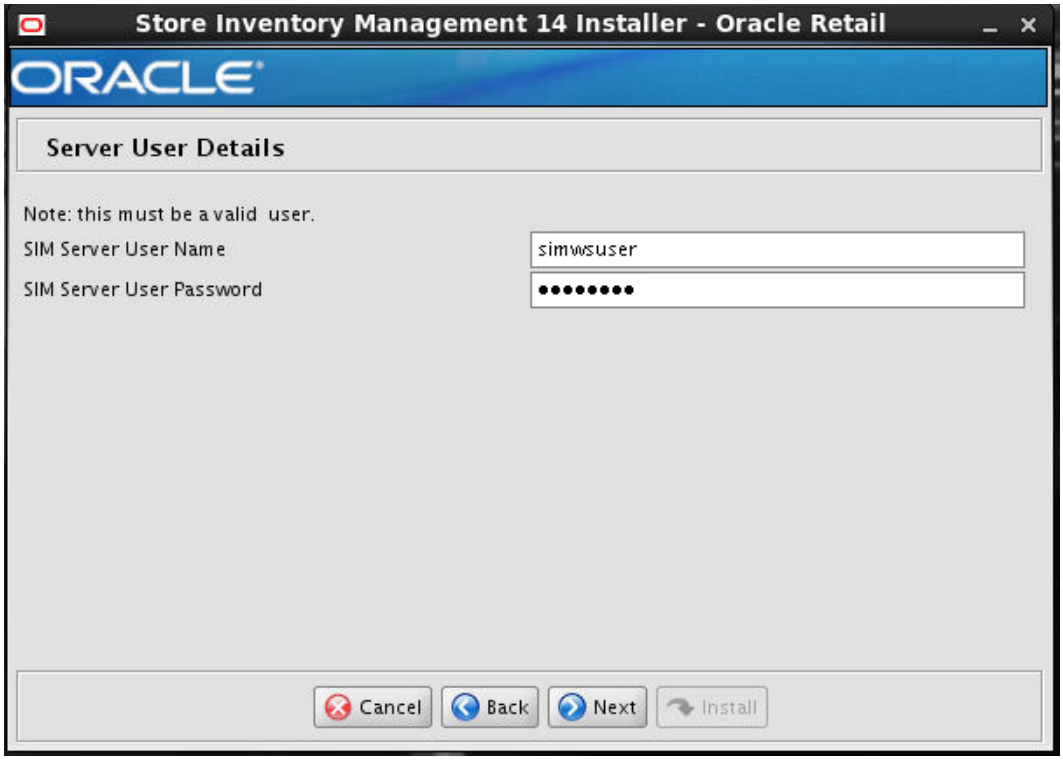
Screen: Batch Server Details



Field Title	Batch User Name
Field Description	User name for Batch
Destination	Retail config wallet and installer creates WebLogic user with the given name above.

Field Title	Batch User Password
Field Description	Password for batch user, the password must follow WebLogic password requirements (at least 8 characters in length and one non-alphabetic character)
Destination	Retail config wallet.

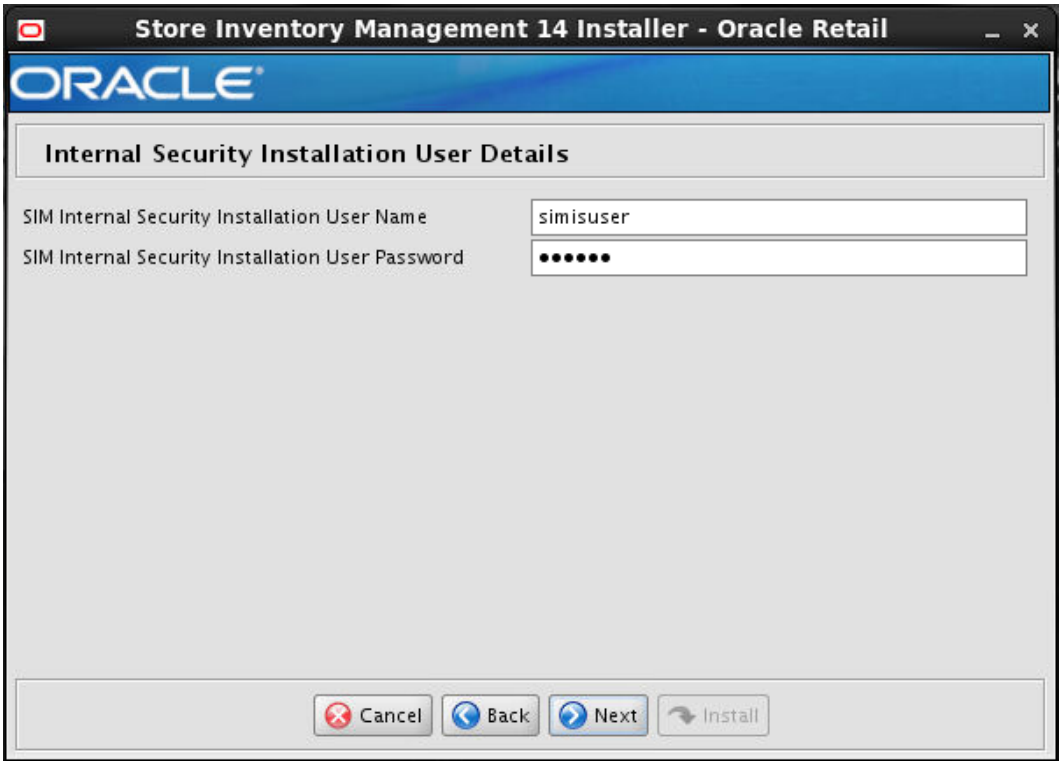
Screen: Server User Details



Field Title	SIM Server User Name
Field Description	User name for SIM Server
Destination	Domain wallet and installer creates WebLogic user with the given name above.

Field Title	SIM Server User Password
Field Description	Password for SIM Server User, the password must follow WebLogic password requirements (at least 8 characters in length and one non-alphabetic character)
Destination	Weblogic Domain wallet/ weblogic default

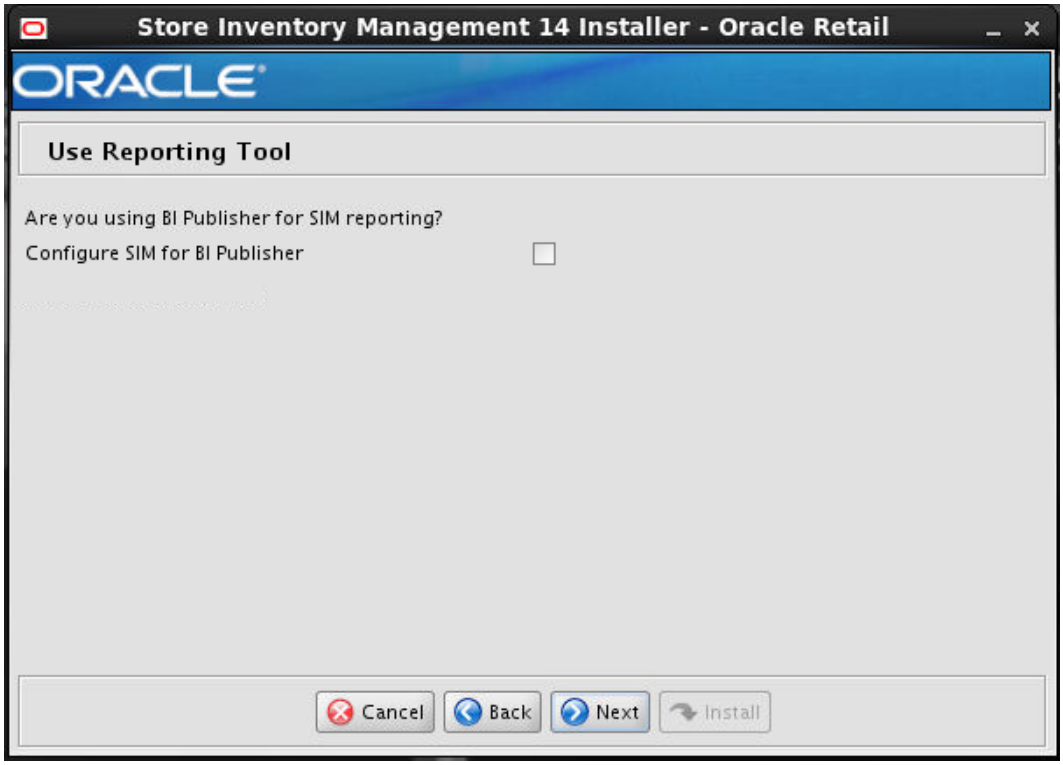
Screen: Internal Security Installation User Details



Field Title	SIM Internal Security Installation User Name
Field Description	User name for SIM Internal Security Installation
Destination	SIM database user for the SIM application and WebLogic user in database provider authentication. SIM stores are tied to this user. Example: orsimadmin

Field Title	SIM Internal Security Installation User Password
Field Description	Password for SIM Internal Security Installation User, the password must follow WebLogic password requirements (at least 8 characters in length and one non-alphabetic character)
Destination	SIM database user for the SIM application and WebLogic user in database provider authentication.

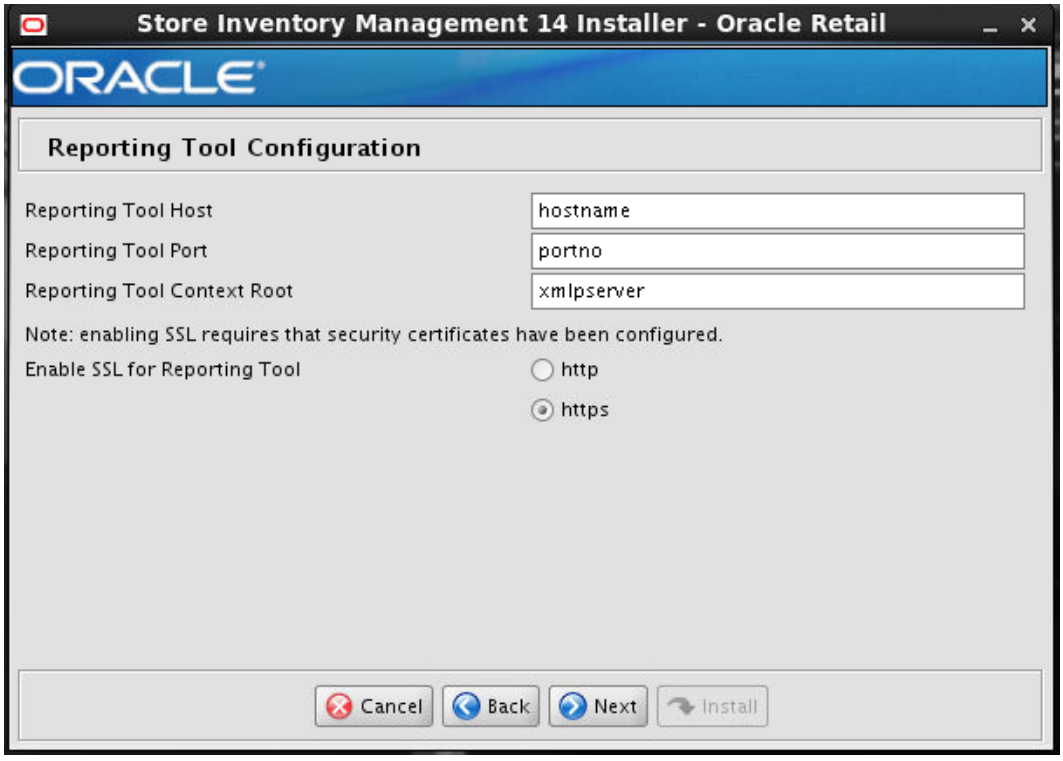
Screen: Use Reporting Tool



Note: See the *Oracle Retail Store Inventory Management Implementation Guide* for SIM reports installation details. If SIM reports will be installed at a later time, leave the reporting configuration values as the default values. These can be configured using the Store and Reporting Tool at a later time.

Field Title	Configure SIM for BI Publisher
Field Description	Toggle field indicating whether or not to configure SIM for BI Publisher Reporting Tool
Example	True
Notes	The following configuration screens will only appear if this checkbox is marked.

Screen: Reporting Tool Configuration

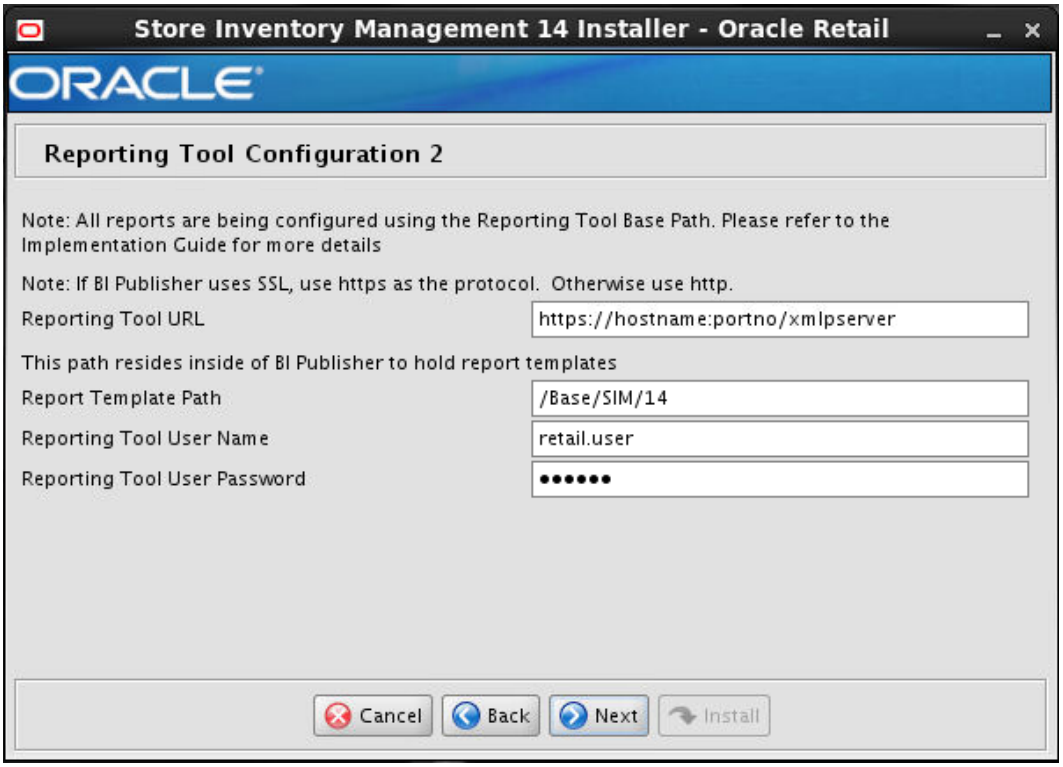


Field Title	Reporting Tool Host
Field Description	Host name where Reporting Tool is installed.
Destination	Updates the reporting tool related default values in SIM database.
Example	redevlv0074.us.oracle.com

Field Title	Reporting Tool Port
Field Description	Port where Reporting Tool is configured.
Destination	Updates the reporting tool related default values in SIM database.
Example	7003

Field Title	Reporting Tool Context Root
Field Description	Context root where Reporting Tool is installed
Destination	Updates the reporting tool related default values in SIM database.
Example	Xmlpserver

Screen: Reporting Tool Configuration 2



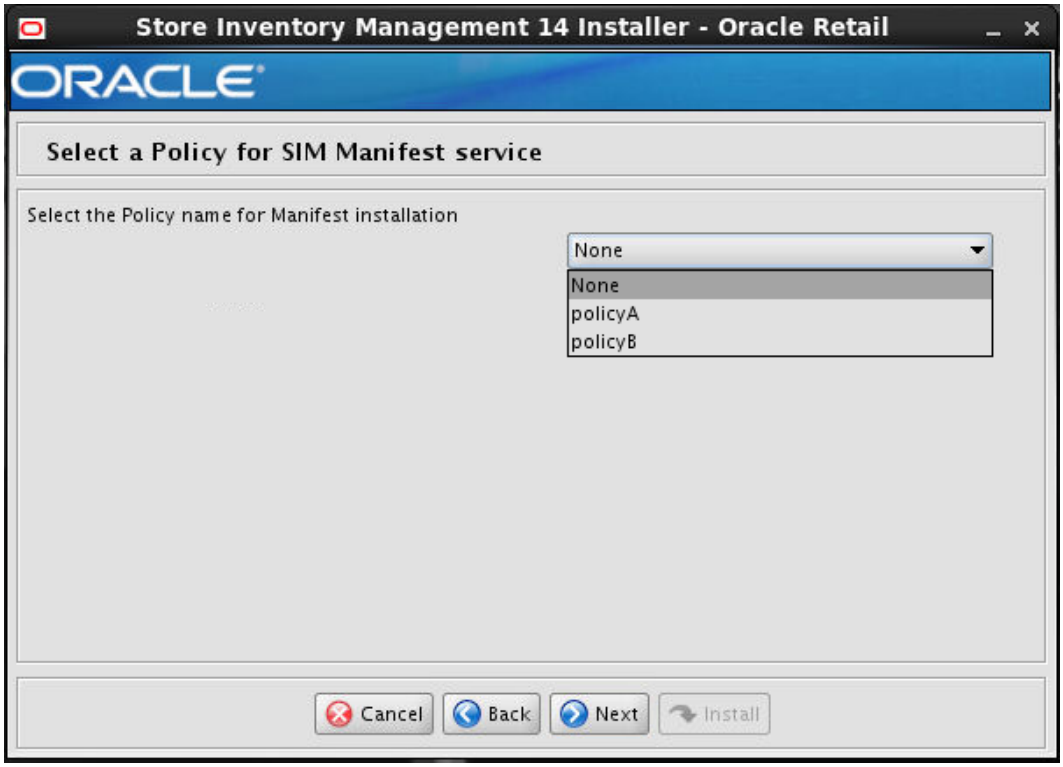
Field Title	Reporting Tool Address URL
Field Description	Confirmation field of address configured from values provided on previous screen
Destination	Updates the reporting tool related default values in SIM database.
Example	http://redevlv0074.us.oracle.com:7003/xmlpserver/servlet/scheduler

Field Title	Report Template Path
Field Description	The root directory in which your SIM report templates are located.
Example	/Base/SIM DSS team: please show example to get this to the path that the reports get stored in with the bipub directions elsewhere in this install guide. An example from this install guide is: `/u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository/Reports/Guest/SIM`

Field Title	Reporting Tool Username
Field Description	From the *Oracle Retail Store Inventory Management Implementation Guide:* <*BIP_REPORTS_USER*> or <*SSO_USER*>
Destination	Updates the reporting tool related default values in SIM database. This user MUST exist as a bipublisher user.
Example	retail.user

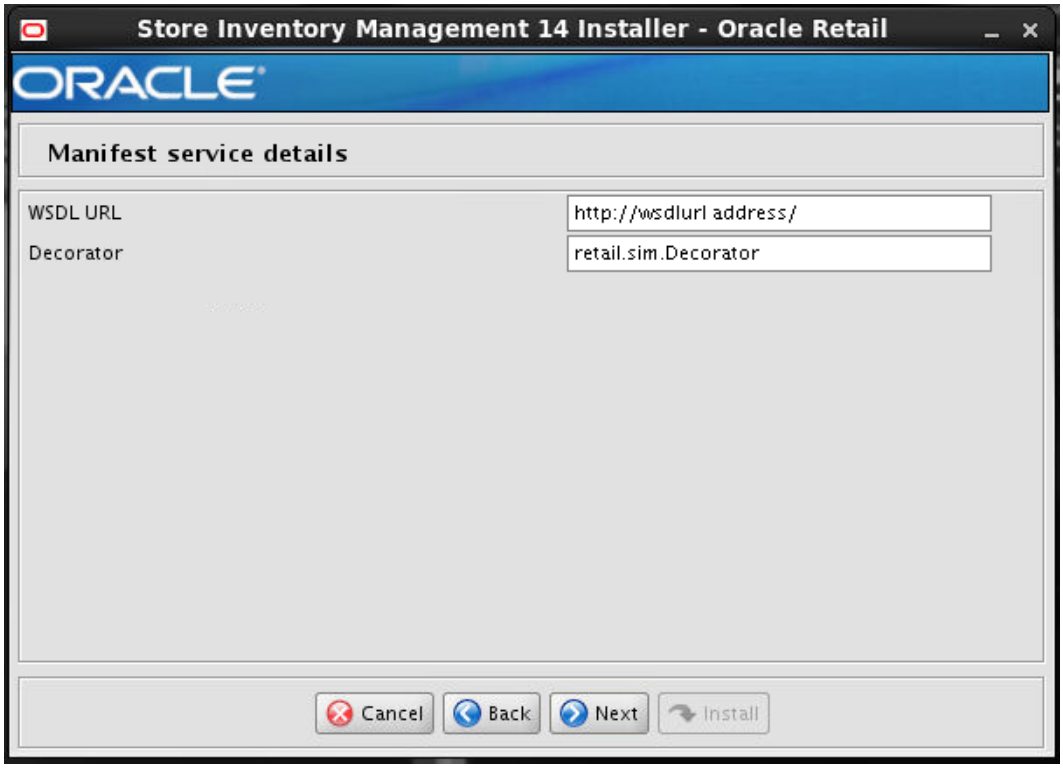
Field Title	Reporting Tool Password
Field Description	From the *Oracle Retail Store Inventory Management Implementation Guide:* <*BIP_REPORTS_USER_PASSWORD*> or <*SSO_PASSWORD*>
Destination	Updates the reporting tool related default values in SIM database.

Screen: Select a Policy for SIM Manifest service



Field Title	Select the policy name for Manifest Installation
Field Description	Select "None" to not apply any policy configuration. If the "Policy A" or "Policy B" policies are desired please refer to the Security Guide for configuration instructions

Screen: Manifest service details



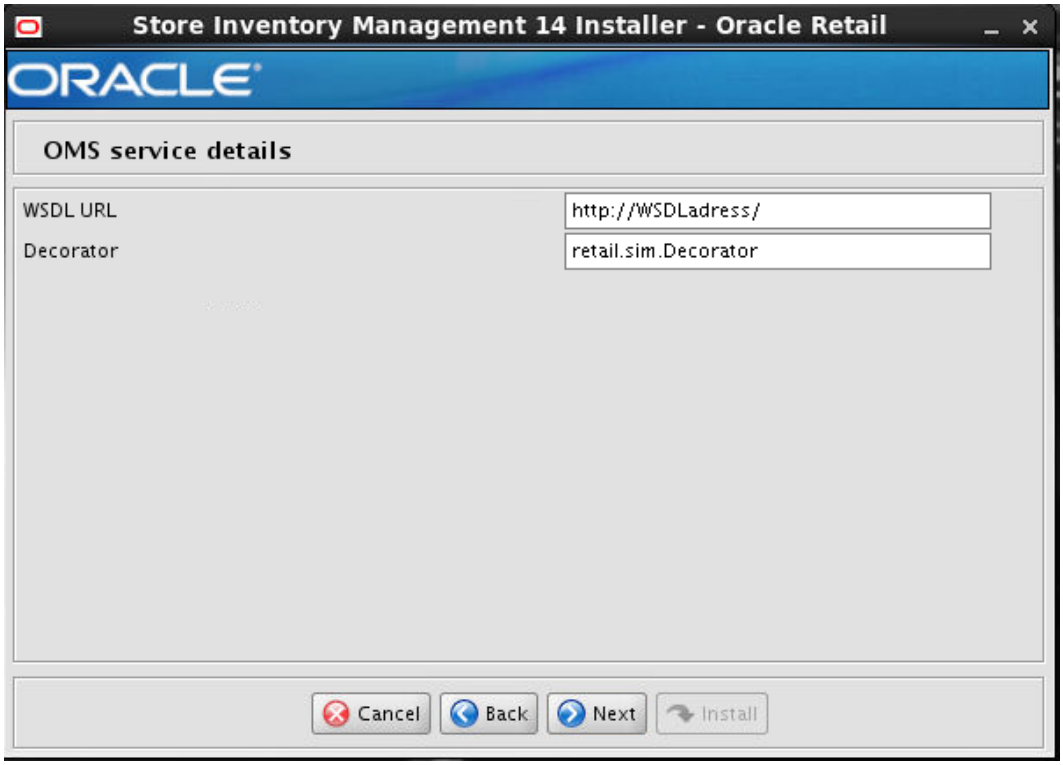
Field Title	WSDL URL for manifest services
Field Description	URL to access the Manifest webservices (leave blank of manifest services are not used)
Example	http://msp28080.us.oracle.com:18008/mms-ShipmentManifest-AppServiceDecorator/ProxyService/ShipmentManifestAppServiceProxy?wsdl

Field Title	Manifest decorator
Field Description	RSB decorator for manifest services
Example	None: <empty> Policy A: oracle.retail.sim.extservice.core.UserNameTokenWlsDecorator Policy B: oracle.retail.sim.extservice.core.UserNameTokenEncryptedMessageWlsDecorator

Screen: Select a Policy for SIM OMS Service

Field Title	Select the policy name for OMS Installation
Field Description	Select "None" to not apply any policy configuration. If the "Policy A" or "Policy B" policies are desired please refer to the Security Guide for configuration instructions

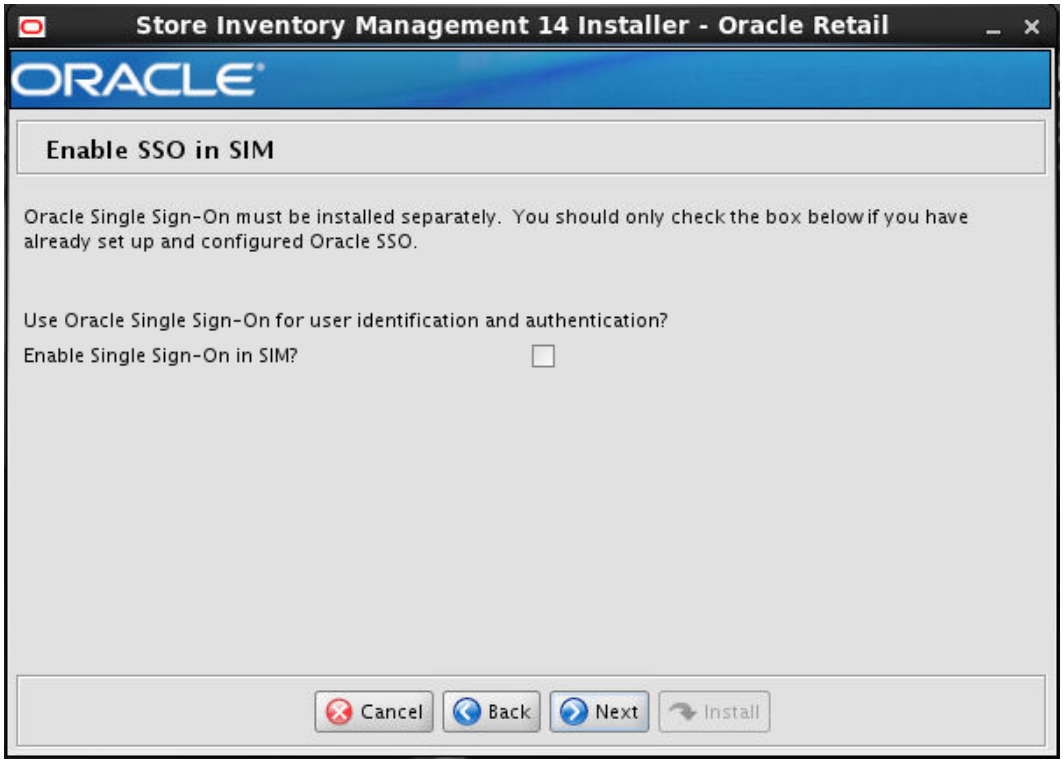
Screen: OMS Service details



Field Title	WSDL URL for OMS services
Field Description	URL to access the OMS services (leave blank if OMS is not used)
Example	http://msp28080.us.oracle.com:18008/oms-CustomerOrder-AppServiceDecorator/ProxyService/CustomerOrderAppServiceProxy?wsdl

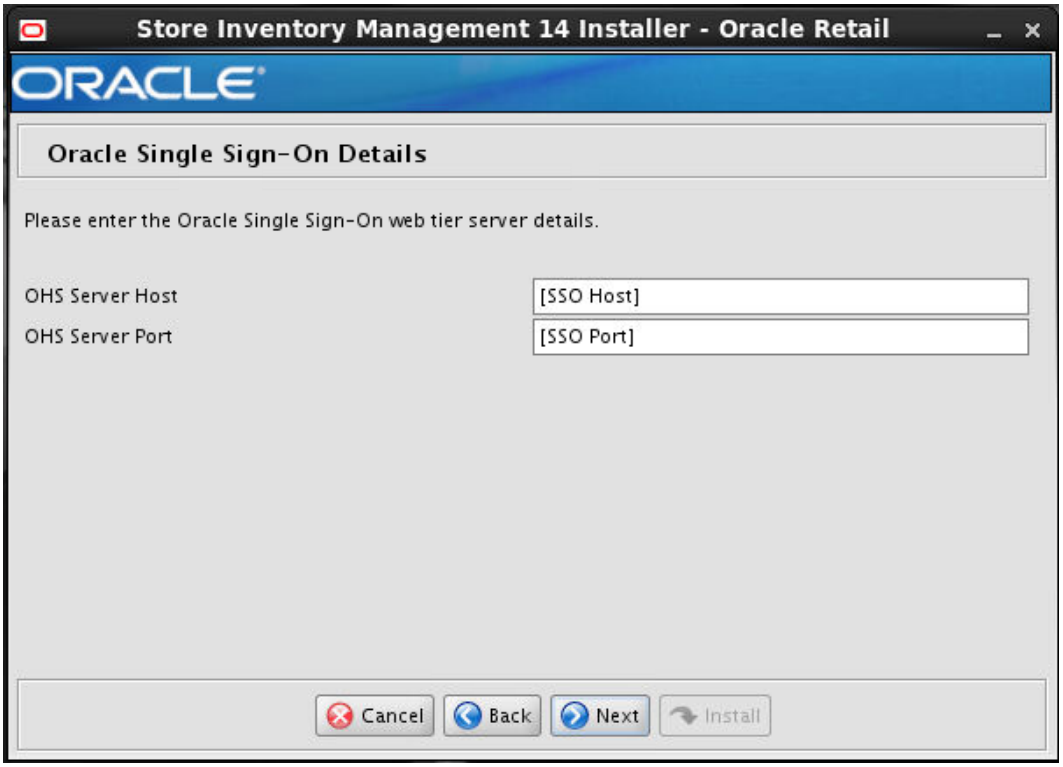
Field Title	OMS Decorator
Field Description	RSB decorator for OMS services
Example	None: <empty> Policy A: oracle.retail.sim.extservice.core.UserNameTokenWlsDecorator Policy B: oracle.retail.sim.extservice.core.UserNameTokenEncryptedMessageWlsDecorator

Screen: Enable SSO in SIM



Field Title	Use Single Sign-On for user identification and authentication?
Field Description	This version of SIM has the option to use Single Sign-On (SSO) technology to authenticate users. If SSO is being used in your environment then click the check box. Leaving the box unchecked will configure SIM to use its own LDAP directory settings for authentication.

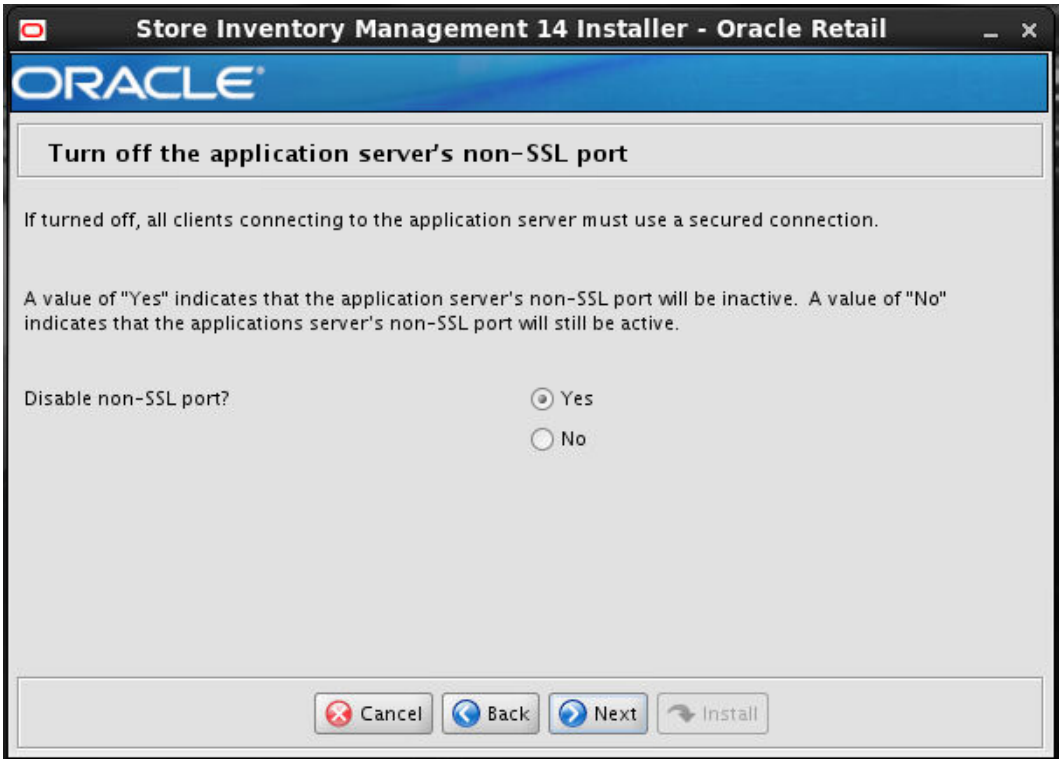
Screen: Single Sign-On Details



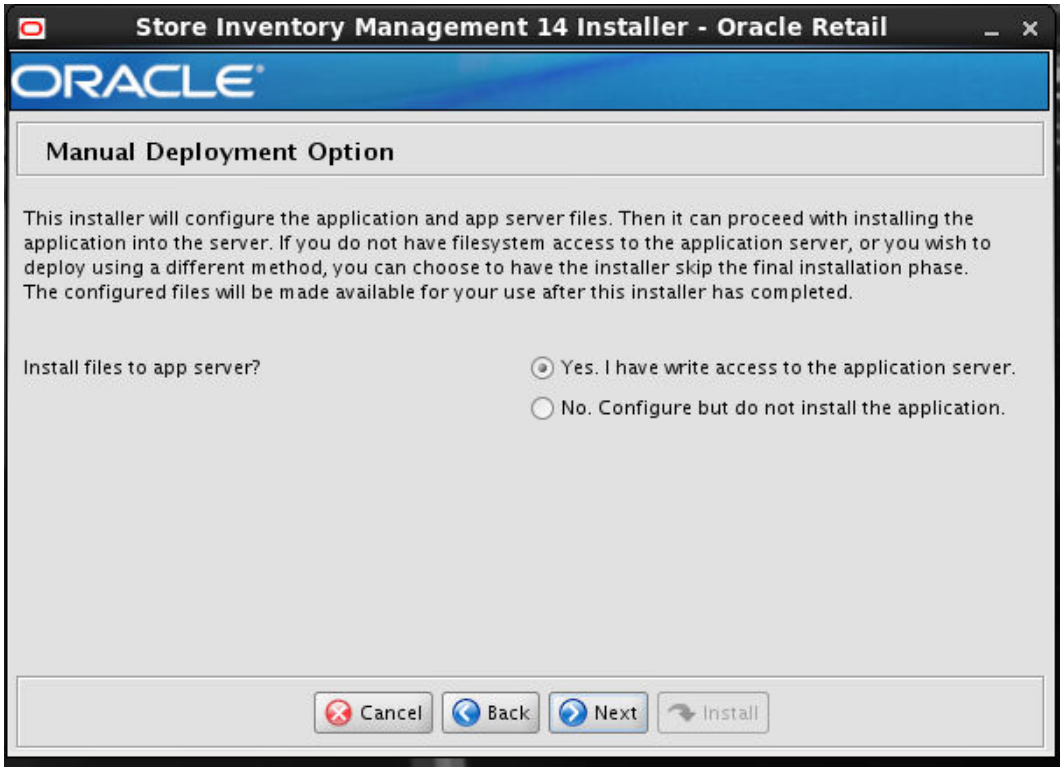
Field Title	OHS Server Host
Field Description	This is the host used to access the Single Sign-On webtier
Example	VIPADDRESS.us.oracle.com

Field Title	OHS Server Port
Field Description	This is the port used to access the Single Sign-On webtier
Example	18888

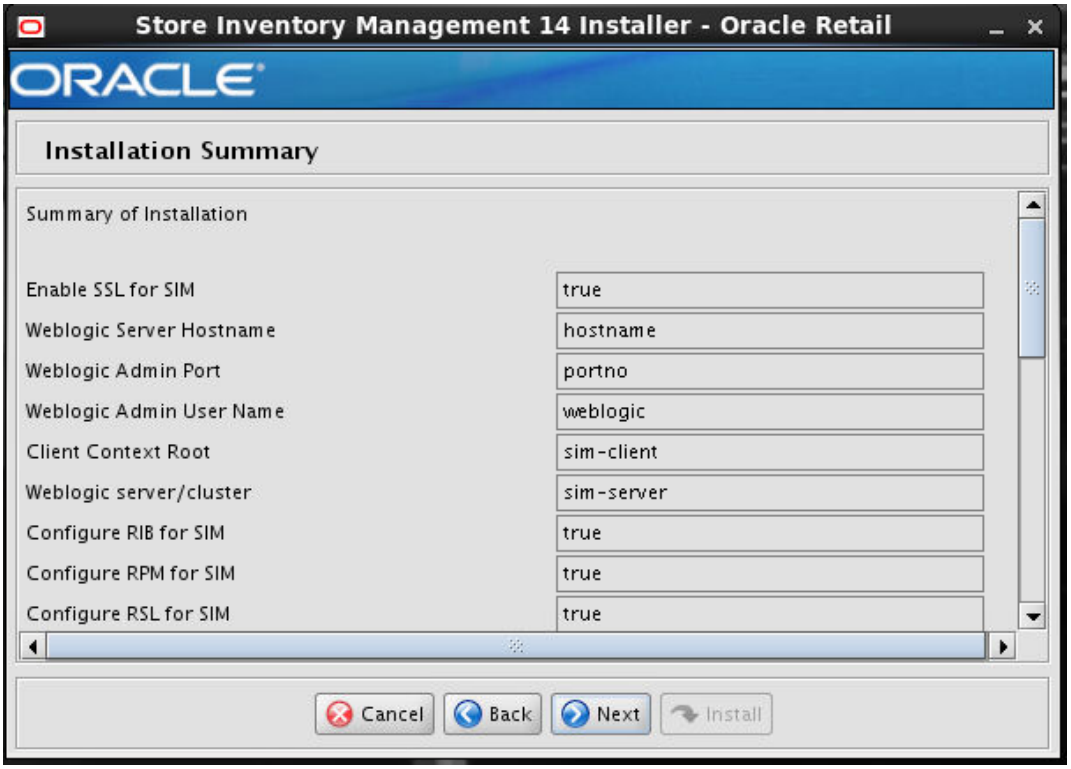
Screen: Turn off the application server's non-SSL port



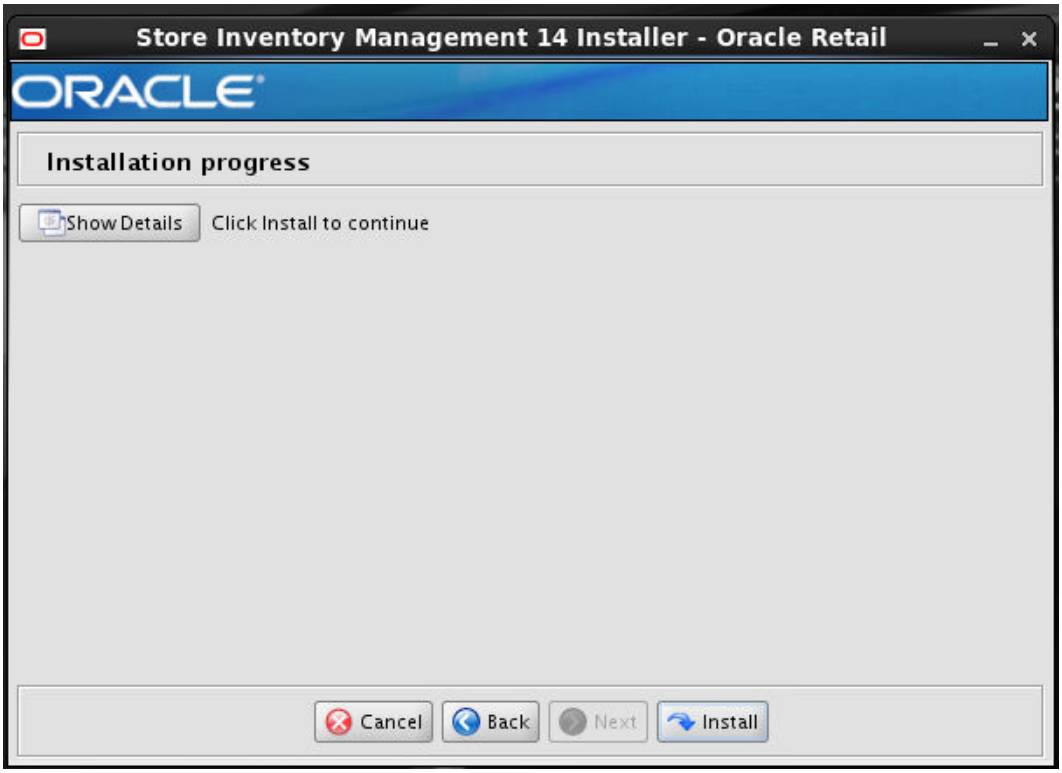
Screen: Manual Deployment Option



Screen: Installation Summary



Screen: Installation Progress



B

Appendix: Common Installation Errors

This section provides some common errors encountered during installation.

EJB Deployment Errors during Installation to WebLogic

Symptom

On servers that are encountering high memory usage, deployment of sim-server.ear will occasionally fail due to WebLogic's inability to start the EJB polling timer service.

```
     [java] .....Failed to deploy the application with status failed
     [java] Current Status of your Deployment:
     [java] Deployment command type: deploy
     [java] Deployment State       : failed
     [java] Deployment Message     : weblogic.application.ModuleException:
Exception activating module: EJBModule(
sim-ejb3.jar)
     [java]
     [java]
     [java] weblogic.management.scripting.ScriptException: Error occured while
performing deploy : Deployment Fail
ed.
     [java] Unable to deploy EJB: PollingCoordinatorThreadBean from sim-ejb3.jar:
     [java]
     [java] Error starting Timer service
```

Solution

Delete the WebLogic managed server/cluster where sim was targeted in the Admin Console, and activate the changes. Manually delete the managed server directory <DOMAIN HOME>/servers/<SIM SERVER NAME>. Bounce the WebLogic admin server. Re-create the managed server in the Admin Console, Finally, re-run the installer. If the error persists after re-installation, consider reducing the cpu, disk, and memory load on the server.

Output Freezes during Text Mode Installation to WebLogic

Symptom

The standard output of the installer in text mode will sometimes freeze partway through the installation.

Solution

Open a new terminal to the server and tail the log file located in sim/application/logs.

Database Installer Hangs on Startup

Symptom

When the database schema installer is run, the following is written to the console and the installer hangs indefinitely:

```
Running pre-install checks
Running tnsping to get listener port
```

Solution

The installer startup script is waiting for control to return from the **tnsping** command, but tnsping is hanging. Type Control+C to cancel the installer, and investigate and solve the problem that is causing the **tnsping <sid>** command to hang. This can be caused by duplicate database listeners running.

Warning: Could not create system preferences directory

Symptom

The following text appears in the installer Errors tab:

```
May 22, 2006 11:16:39 AM java.util.prefs.FileSystemPreferences$3 run
WARNING: Could not create system preferences directory. System preferences are
unusable.
May 22, 2006 11:17:09 AM java.util.prefs.FileSystemPreferences
checkLockFile0ErrorCode
WARNING: Could not lock System prefs. Unix error code -264946424.
```

Solution

This is related to Java bug 4838770. The /etc/.java/.systemPrefs directory may not have been created on your system. See http://bugs.sun.com for details.

This is an issue with your installation of Java and does not affect the Oracle Retail product installation.

Warning: Couldn't find X Input Context

Symptom

The following text appears in the console window during execution of the installer in GUI mode:

```
Couldn't find X Input Context
```

Solution

This message is harmless and can be ignored.

ConcurrentModificationException in Installer GUI

Symptom

In GUI mode, the errors tab shows the following error:

```
java.util.ConcurrentModificationException
          at
java.util.AbstractList$Itr.checkForComodification(AbstractList.java:448)
          at java.util.AbstractList$Itr.next(AbstractList.java:419)
… etc
```

Solution

You can ignore this error. It is related to third-party Java Swing code for rendering of the installer GUI and does not affect the retail product installation.

A Second Login Screen Appears After Single Sign-On Login

If you are using Single Sign-On, you should not need to enter a SIM user name and password once SIM is launched. If the SIM login screen pops up, it means something went wrong with the SSO login. This could be caused by any of the following problems:

- There is no SIM user in LDAP for the SSO user name you are using.
- Permissions are not set up correctly for the SSO user in SIM.
- SSO is configured incorrectly on the server.
- SSO timed out. (This can happen especially the first time you launch SIM. Try launching SIM again.)

Symptom

A second login screen appears after you have already logged in to Single Sign-On.

Solution

See the *Oracle Retail Store Inventory Management Implementation Guide* for more information on setting up SIM users and using LDAP and SSO with SIM.

Error Connecting to Database URL

Symptom

After entering database credentials in the installer screens and hitting next, a message pops up with an error like this:

```
Error connecting to database URL <url> as user <user> details...
```

The message prevents you from moving on to the next screen to continue the installation.

Solution

This error occurs when the installer fails to validate the user credentials you have entered on the screen. Make sure that you have entered the credentials properly. If you receive a message similar to this:

```
Error connecting to database URL <url> as user <user> java.lang.Exception:
UnsatisfiedLinkError encountered when using the Oracle driver.
Please check that the library path is set up properly or switch to the JDBC thin
client.
```

It may mean that the installer is using the incorrect library path variables for the platform you are installing on. Open the file <STAGING_DIR>/rms/dbschema/common/preinstall.sh and toggle the variable, use32bit, to True if it is set to False or vice versa. This setting is dependent on the JRE that is being used.

Files not available to copy at the end of installation results in non working applications – WebLogic only

Symptom

If you choose the option **No. Configure but do not install the application** in the installer screen titled **Manual Deployment Option**, necessary wallet files that are required for application run time are deleted at the end of the installation.

Solution

Manual Deployment is not currently available in this installer. Choose **Yes. I have write access to the application server** in the installer screen, **Manual Deployment Option**.

> **Note:** To successfully perform this option, you also need to run the installer as a user with write access to the WebLogic installation.

GUI screens fail to open when running Installer

Symptom

When running the installer in GUI mode, the screens fail to open and the installer ends, returning to the console without an error message. The ant.install.log file contains this error:

```
Fatal exception: Width (0) and height (0) cannot be <= 0
java.lang.IllegalArgumentException: Width (0) and height (0) cannot be <= 0
```

Solution

This error is encountered when Antinstaller is used in GUI mode with certain X Servers. To work around this issue, copy ant.install.properties.sample to ant.install.properties and rerun the installer.

Log in fails with invalid username/password or user unauthorized errors

Symptom

The SIM application log in fails with the following messages: “Invalid username/password” or “User unauthorized or Not authenticated.”

Solution

In SIM Database, in the CONFIG_SYSTEM table, the value for SECURITY_AUTHENTICATION_METHOD should be set to 1 for LDAP authentication.

Check in LDAP to be sure the password is set to the correct value.

Forms 11g Compilations against an 11g Database are Slow or Sometimes Hang

Symptom

While Forms Compilation a query on data dictionary object “ALL_OBJECTS” is very slow / Stuck and forms compilation is slow or Hang.

Solution

For Database version higher than 11.2.0.1 the patch is included in the release , we need to enable to fix by:

```
ALTER SYSTEM SET "_FIX_CONTROL"='8560951:ON';
```

```
For more information about the fix please follow the below metalink note:-
```

Forms 11g and Forms 10gR2: Queries and Compilations against an 11g Database are Slow or Sometimes Hang (Doc ID 880660.1)

C

Appendix: Setting up SIM Reports in BI Publisher

SIM 14.0.2 reports supports BiPublisher 11g.

Upgrading from BiPublisher 10g to 11g is not trivial. Among other things, the BiPublisher report program in 10g is the <report_name>.xdo file. In 11g, this <report_name>.xdo report file gets split into two new folders, a <report_name>.xdo folder along with a <report_name>.xdm folder. Both of these two new folders have report files within them. Your BiPublisher 10g reports program will not work without a change in BiPublisher 11g.

Note: If you are in the middle of implementing or recently implemented RMS and want less changes at this time, you can stay with BiPublisher 10g for this patch. Custom BiPublisher reports or report modification customers may also want to keep BiPublisher 10g for this patch until they can fully plan out the changes needed for this upgrade.

Note: If BIPublisher application 10g or 11g is already deployed to a bipublisher managed server in Weblogic, you can directly go to the "BiPublisher 10g and BiPublisher 11g - Configuring the SIM JDBC connection" section. If not, continue with the "BI Server Component Installation Tasks".

BiPublisher 11g – BI Server Component Installation Tasks

Oracle BI Publisher is used as the main RMS, RWMS, REIM, and SIM reporting engine and can be used in conjunction with external printing solutions like label printing. This section describes the installation of Oracle BI Publisher as a server application within WebLogic 10.3.6. One deployment of BI Publisher can be used for any of the RMS, RWMS, REIM, and SIM reports.

If you are installing BI Publisher as a part the Oracle BI EE suite(which you will if installing BiPublisher 11g), refer to the appropriate Fusion Middleware guides for the installation of the product in a WebLogic server environment.

BiPublisher 11g only - Installation Process Overview

Installing the BI Publisher server as a standalone web application in a WebLogic server involves the following tasks:

1. Run RCU to create BiPublisher related database schemas and other db objects.
2. Install Oracle BI EE under an existing WebLogic Server (WLS) 10.3.6 and choose "software only install".
3. Configure Oracle BI EE, create default bifoundation_domain and configure component "Business Intelligence Publisher" only.
4. Select the BIPlatform schema for update of the ORACLE 11.2.04 DB
5. Configure ports and document and test the URL's that are created.

   The following post-installation tasks are involved once BI Publisher has been installed:
6. Configure the BI Publisher repository. Set security model, add users, assign roles, add reports, add printers, set repository path, set data source, etc.
7. Set up the SIM reports in BIPublisher report repository.
8. Set up for the SIM application specific configuration files to integrate BI Publisher.

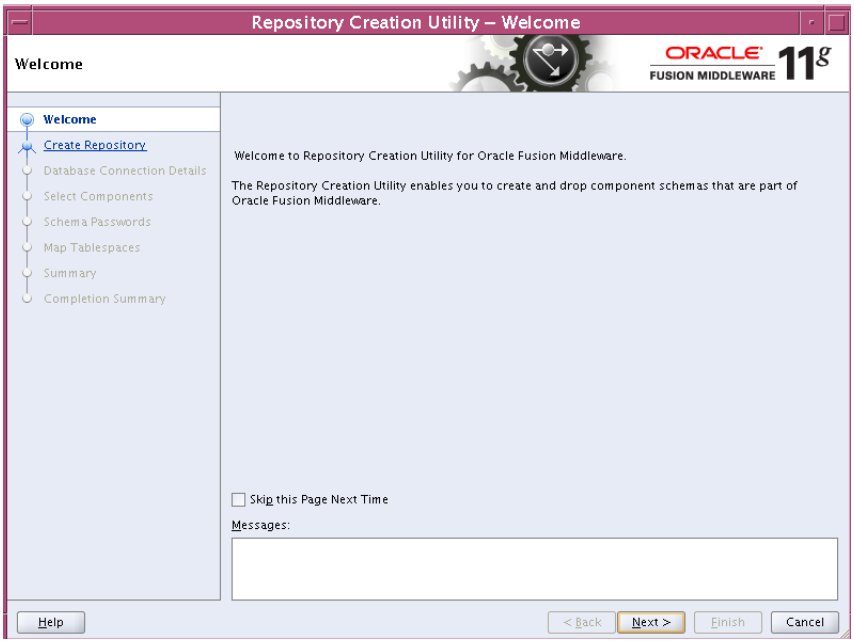
BiPublisher 11g only – Install Oracle BI EE 11g

1. Run the Repository Creation Utility to create the BiPublisher-related database schemas and other database objects. Create the BIPlatform schema into an existing ORACLE 11.2.0.4 DB

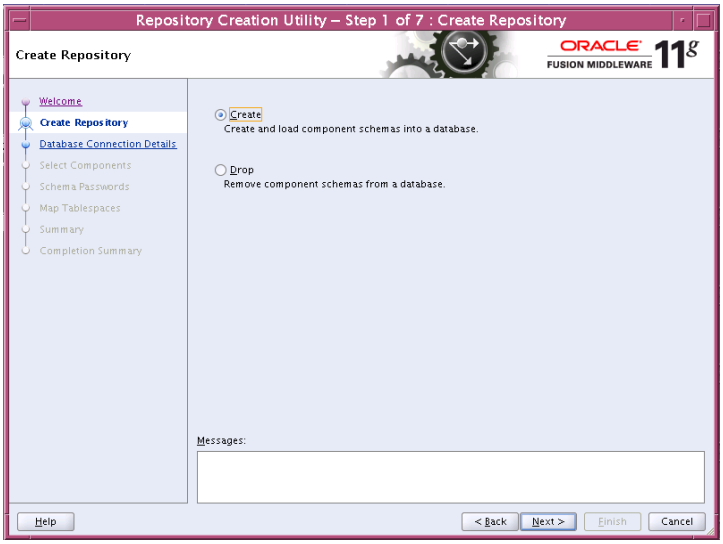
   Note: Download Repository Creation Utility software from http://www.oracle.com/technetwork/middleware/bi-enterprise-edition/downloads/bi-downloads-1525270.html. Install it on your desktop
2. Export your DISPLAY.

   Ex: Export DISPLAY=10.141.10.110:0.0

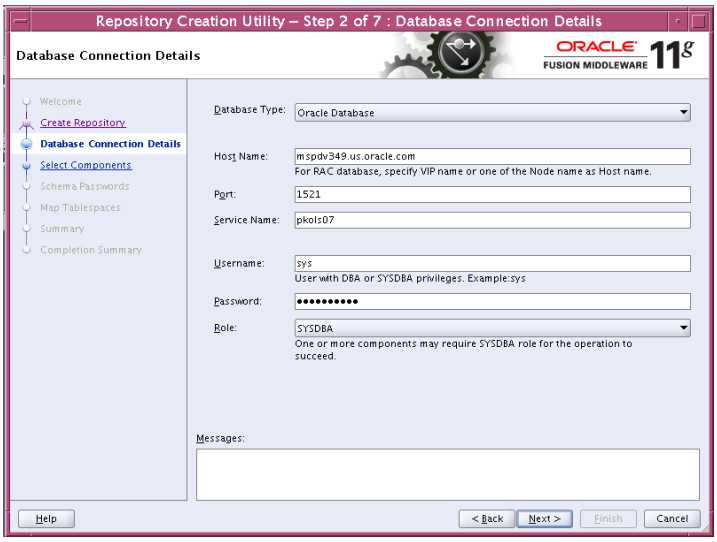
3. Go to $RCU_HOME/bin.
   For example: /linux/x86_64/ofm_11g/RCU_11.1.1.7/rcuHome/bin>
   `Start RCU:  ./rcu`



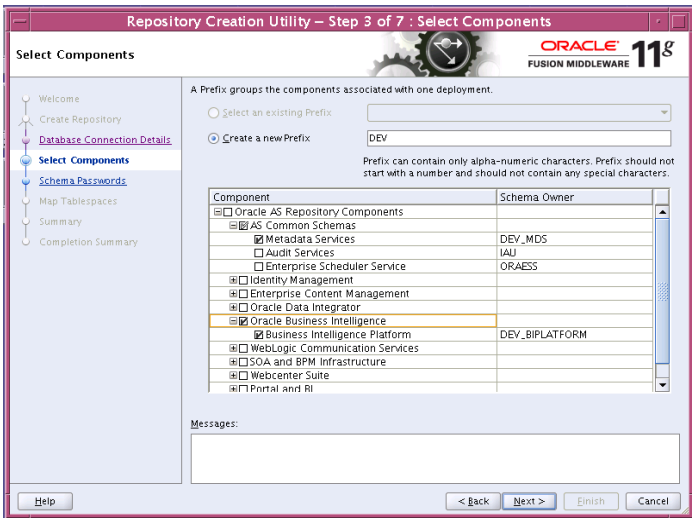
4. Click **Next**.



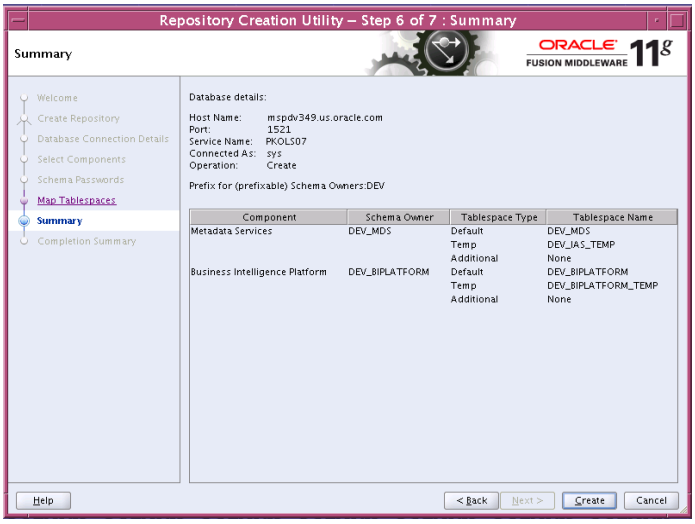
5. Launch Oracle BI EE RCU Repository Creation Utility to create the Oracle BI EE schemas need for the Oracle BI EE BiPublisher installation. On this screen select "Create Repository".



6. On the Database Connection Details screen, enter your Oracle Database information.



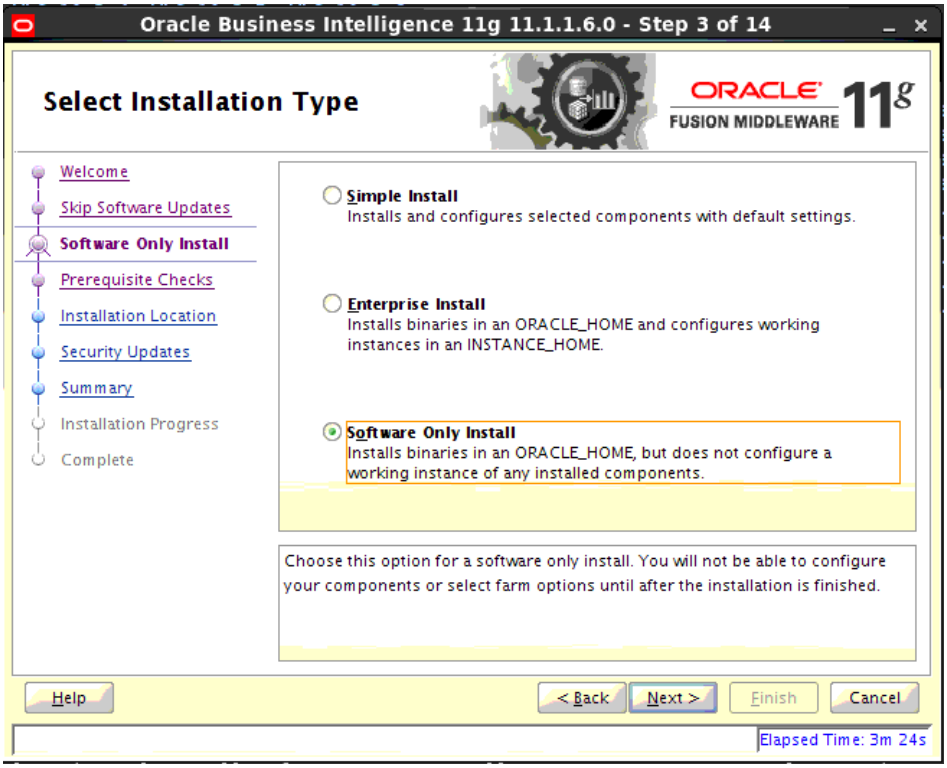
7. On the Select Components screen, select "Oracle Business Intelligence" check box.



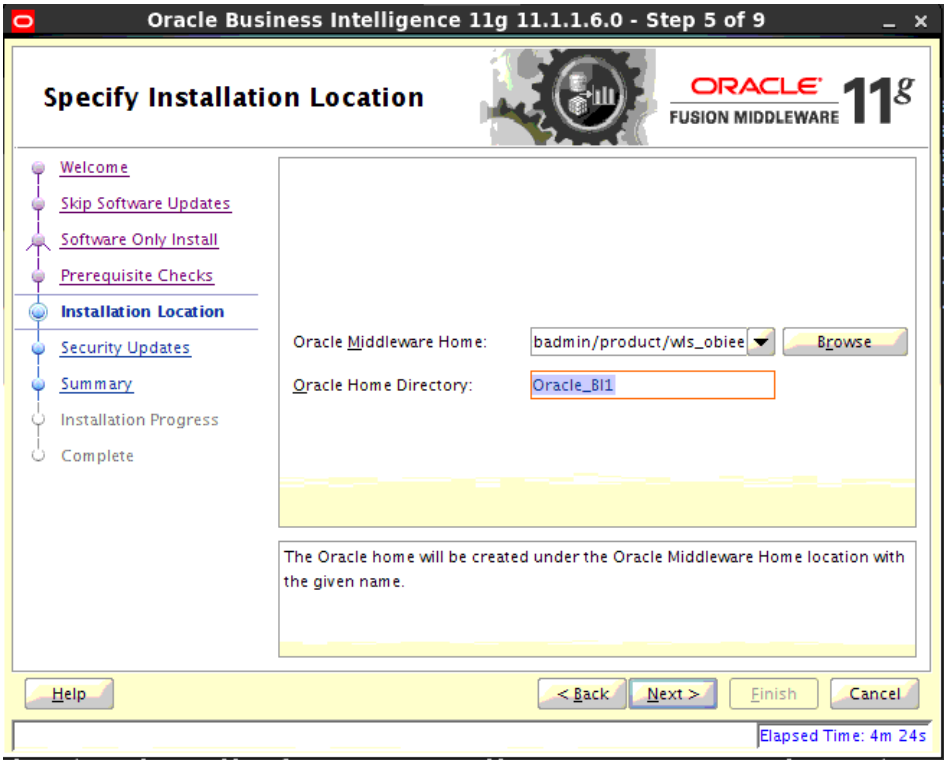
The Summary of the Components created by the RCU tool is displayed.

8. Install a new instance of WebLogic Server 10.3.6 or use an existing one. Having one WebLogic Server for Oracle BI EE-BiPublisher 11g related items is recommended.
9. Install Oracle BI EE and select "Software Only Install". You launch Oracle BI EE by going to OBIEE_INSTALL/obiee11.1.1.7/bishiphome/Disk1 and entering:

   ./runInstaller



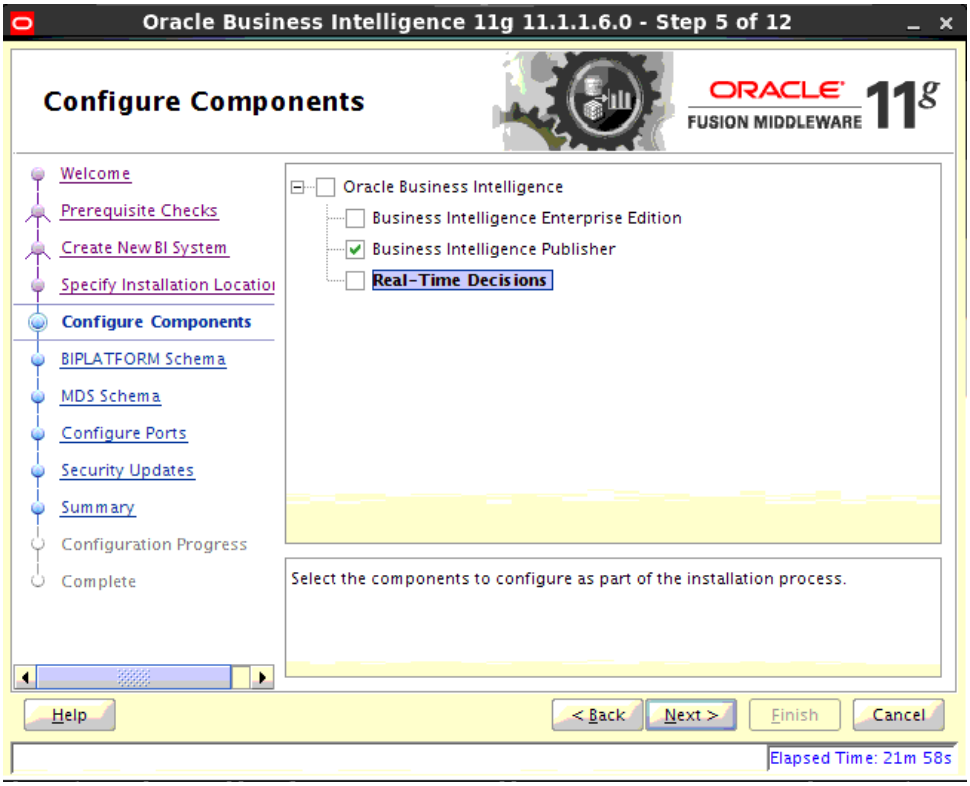
10. Select the WebLogic home where you want to install Oracle BI EE.



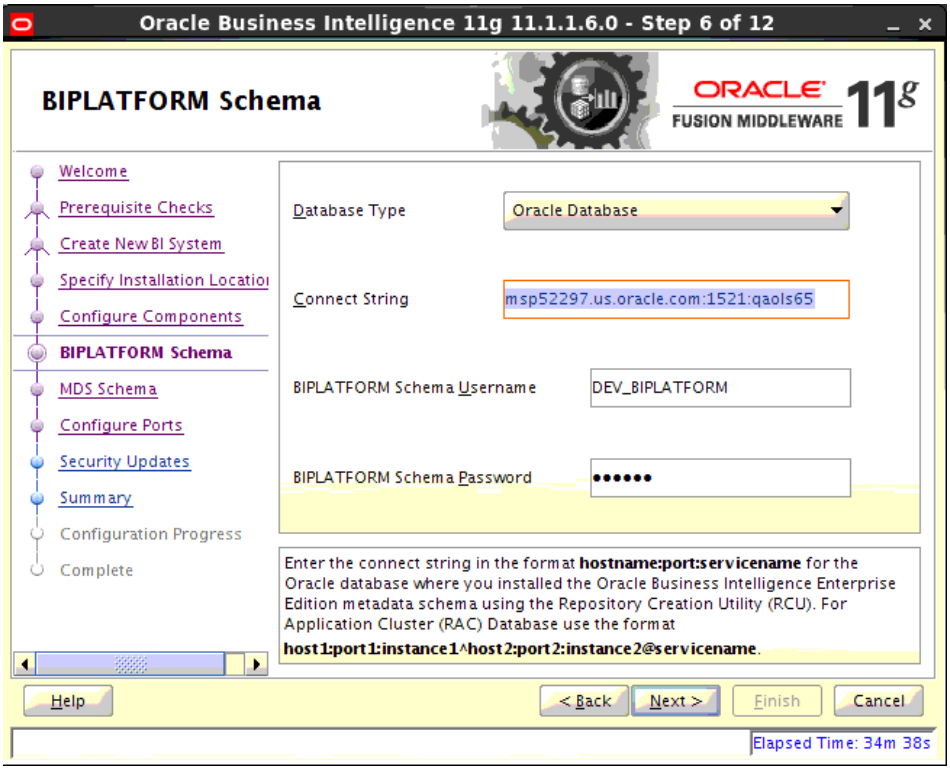
11. Proceed to next and finish up the software install. Then go the <WebLogic home>/Oracle_BI1/bin and run config.sh to configure the bipublisher.

12. On the Create or Scale Out BI System screen, you are asked for the WebLogic password and provided with a recommended a Domain Name. Enter and confirm your WebLogic password and accept the recommended Domain Name; "bifoundation domain"

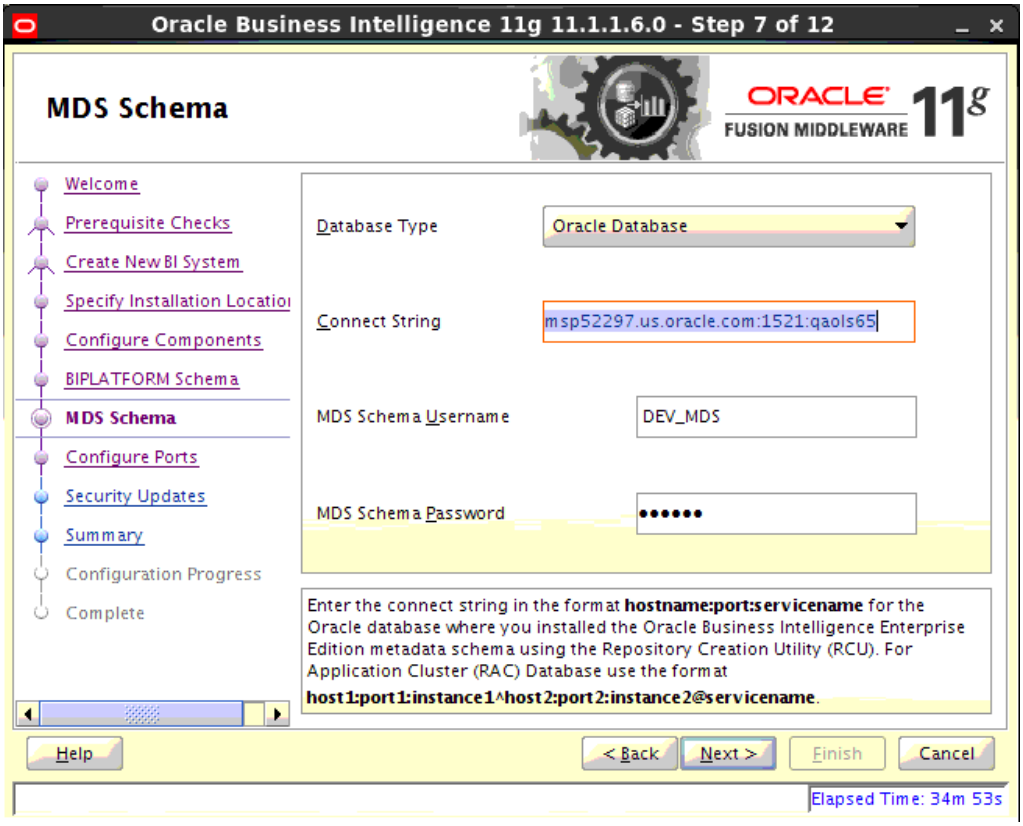
13. Configure Oracle BI EE, create default bifoundation_domain and configure component "Business Intelligence Publisher" only.



14. Enter the data base credentials of the BIPLATFORM schema.



15. Enter the Data base credentials for the MDS Schema.

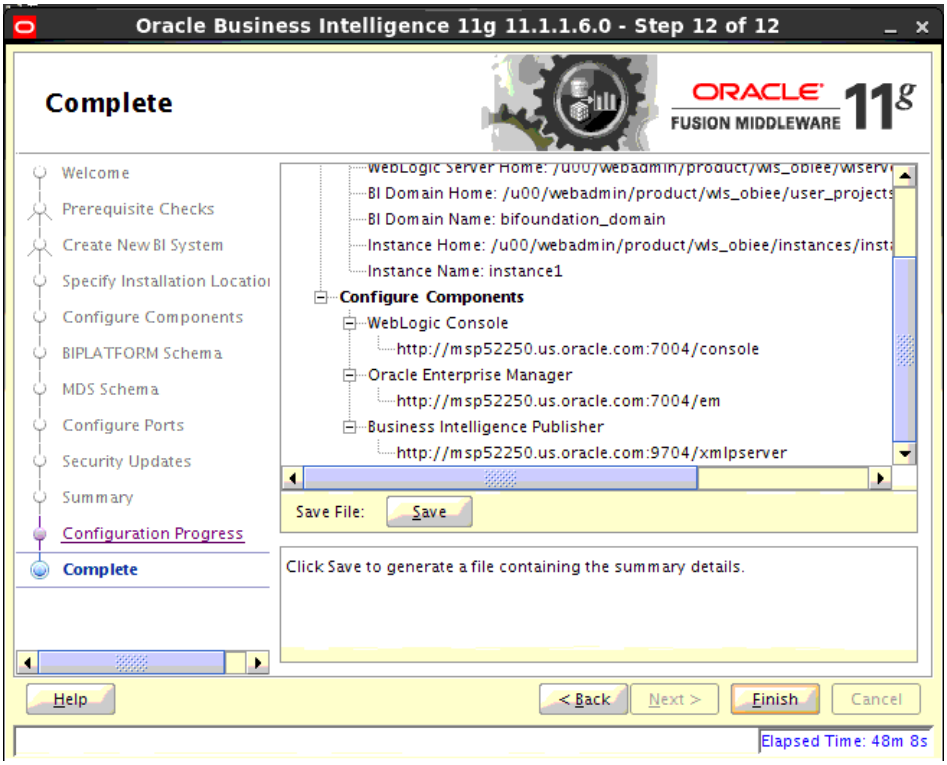


16. Configure your BI ports. This screen allows you to assign Oracle BI EE ports from the staticports.ini file.

    This file is located in the Oracle BI EE software at:
    /obiee11.1.1.7/bishiphome/Disk1/stage/Response/staticports.ini

17. Edit this file to make sure you will have the ports you want for your BiPublisher components. Otherwise the installer will assign default port numbers.

18. Document and test the URLs that are created.
    This screen contains the URL's for the components that got installed.



19. To test your BIPublisher installation, launch xmlpserver. Login with the credentials you entered in your Oracle BI EE configuration (weblogic / password).

20. Post install steps: Configure the BI Publisher repository.

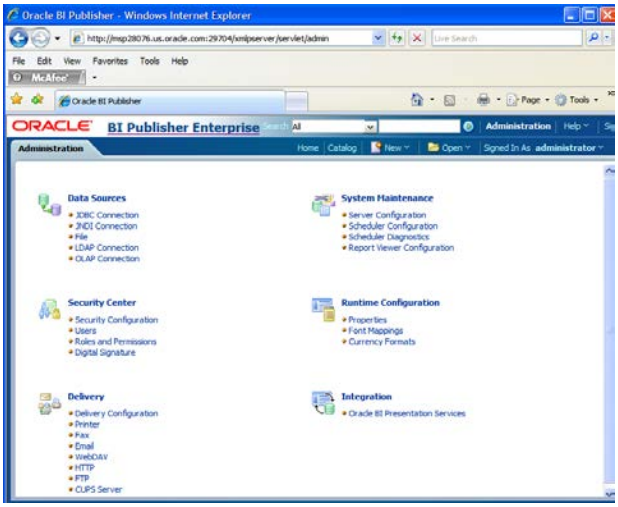
21. On the System Maintenance Section, press Server Configuration.
22. Navigate to the Configuration Screen.

23. On this screen on the Configuration Folder section, enter the path to your repository. On the Catalog section enter Catalog Type: Oracle BI Publisher – File System from the drop down menu.

    This is the path you entered in the Configuration Section and Catalog Section:

    `$OBIEE_HOME/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository`

24. Post install step: Set BiPublisher security model.

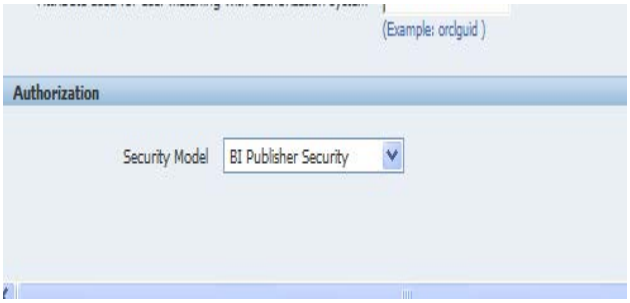


a. On the BiPublisher 11g Administration Screen, click Security Configuration from the Security Center.

b. Enable a superuser by checking the "Enable Local SuperUser" box and by entering name and password on the corresponding fields on this screen.

c. Mark "Allow Guest Access" check box. Enter "Guest" as Guest Folder Name.

d. Scroll down the screen and locate the Authorization section.



e. Select BI Publisher Security from the Security Model list.

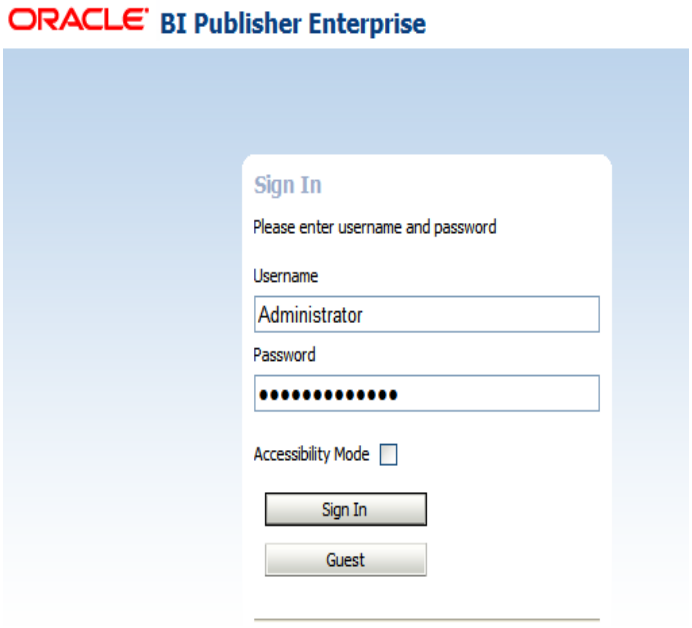
f. The default user name for the BI Publisher Security Model is Administrator.

g. On the password text field, enter a value that you can remember. It is going to be the password for Login to xmlpserver.

h. Save the changes and re-start the BIPublisher server.

i. Launch xmlpserver. To Login you must use the new credentials that you set up in the former step: Username: Administrator Password: password.

> **Note:** You will not be able to login to xmlpserver as weblogic any more because we have already changed the Security Model.



25. Post install step: Set the repository path.

Example:
/u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository In the Oracle BI EE filesystem you will find the repository in the following location:

```
$OBIEE/wls/user_projects/domains/bifoundation_domain/config/bipublisher/repository
```

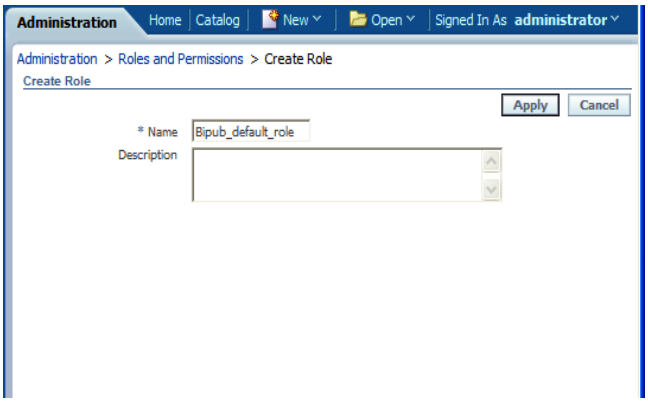
In the repository you will see the following directories:

- Admin
- DemoFiles
- Reports
- Tools
- Users

26. Post install step: Create role Bipub_default_role.

a. From the xmlpserver Administration screen, scroll down to Security Center and click Roles and Permissions.

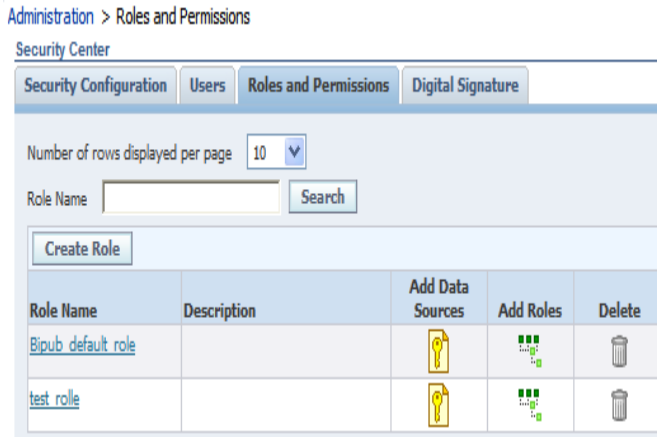
b. On the Roles and Permissions screen, click the Create Role button.



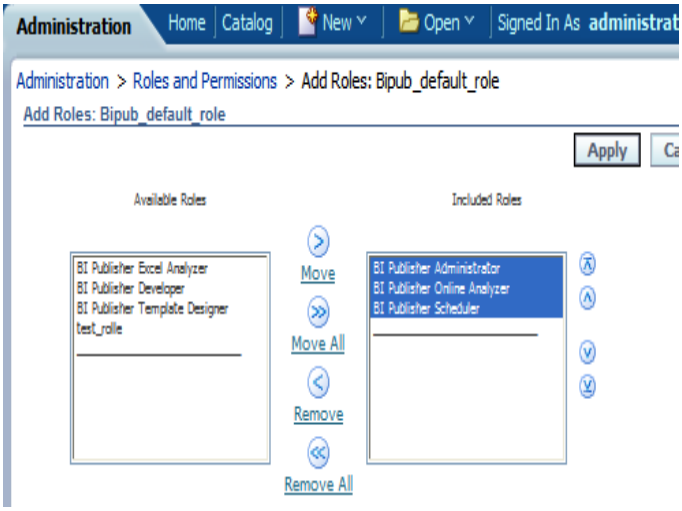
c. Create the Bipub_default_role. Enter in Create Role Section name of the role.

d. When the information has been entered press Apply changes.

27. Post install step: Assign BiPub system roles to the newly created Bipub_default_role.
    a. To assign BiPub system roles to the newly create Bipub_default_role, go to Security Center section and navigate to the Roles and Permissions screen.



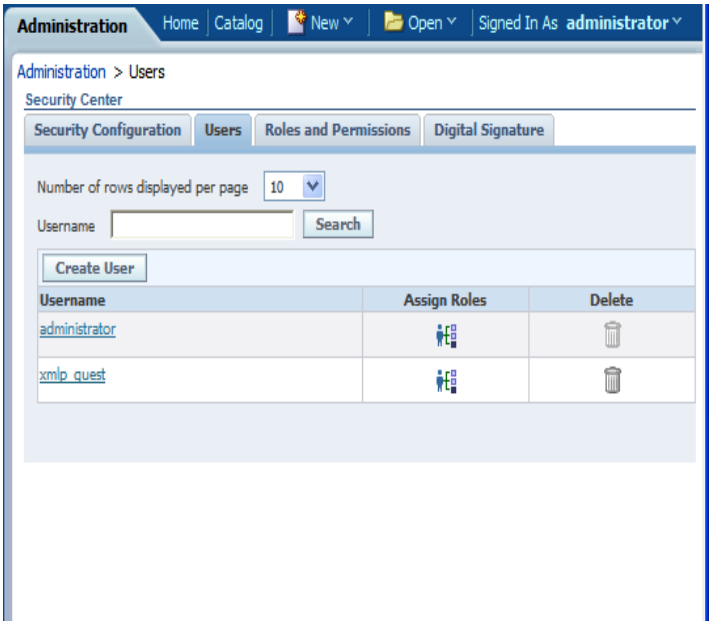
    b. On the Roles and Permissions screen you should see the new role created: “Bipub_default_role” . Add multiple roles to the Bipub_Default_Role by pressing the corresponding green icon on the Add Roles column.



    c. From the “Available Roles” panel, select the ones needed for your reports and move them to the “Included Roles” panel
    d. Press the Apply button to save your changes.

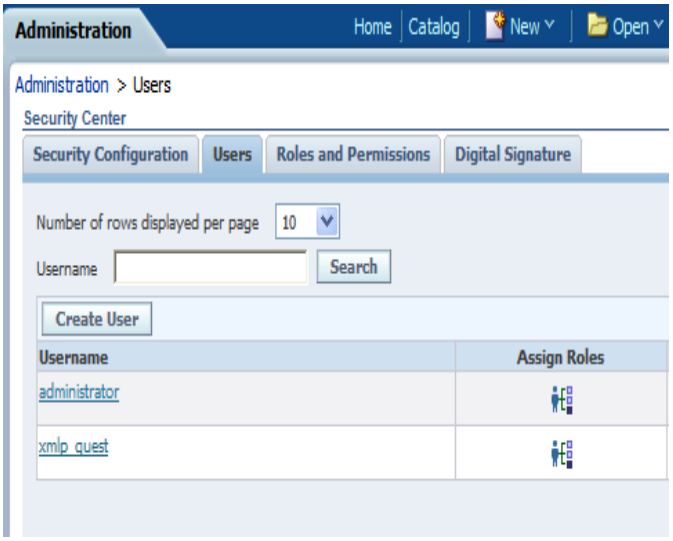
28. Post install step: create Guest (XMLP_GUEST) user.

a. From the xmlpserver Administration screen scroll down to Security Center section and press Users to navigate to the next screen.

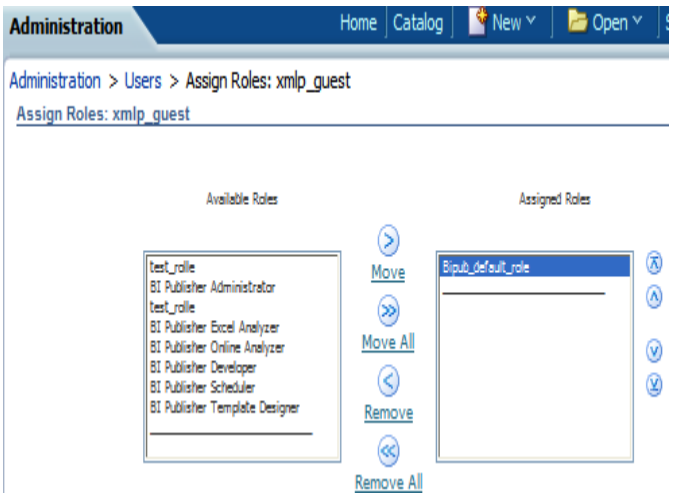


b. Select the "Create User" button to create the "xmlp_guest" user and save the changes

29. Post install step: Adding the Bipub_default_role to XMLP_GUEST user.
    a. Open the Users section:



    b. For xmlp_guest user, press on the "Assign Roles" icon to navigate to the next screen.



    c. On the Assign Roles screen, select the BiPub_default_role from the Available Roles panel to the "Assigned Roles" panel and press the Apply button to save your changes.

BiPublisher 11g – Configuring the SIM JDBC connection

Log in to BI Publisher as the Administrator user. Create the data source for BI Publisher to connect to the SIM schema.

1. Click on the "Admin" tab, and then the "JDBC Connection" link under Data Sources. If there is no SIM data source then a new connection will need to be created, click the "Add Data Source" button and create the data source with your connection info, click the "test connection" before applying to ensure you have the information entered correctly:

Once the data source has been created, the SIM reports need to be moved into the location where BIP can find them.

> **Note:** If using BIPublisher 11g, the Report Repository is available at Administration->System Maintenance->Server Configuration.
>
> The Path given is in the base directory for all the BIP reports.
>
> /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository/

2. Manually copy SIM Reports to Reports repository

   The SIM reports will be copied to the 'Guest' location. Create a directory named 'SIM' under 'Guest' and copy the reports into 'SIM' directory:

   ```
   example,
   /u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/bipublisher/repository/Reports/Guest/SIM
   ```

The reports are included in the SIM application distribution in a zip file. Copy that file from where you installed the SIM application into the new report directory and unzip it:

#

The following are the steps to extract the bip11g reports and copy them to the BIP11g repository:

```
cp <SIM14_MEDIA>/sim/application/sim14/reports/sim-reports.zip <TEMP_DIR> Where
<TEMP_DIR> is a temporary directory where extract sim-reports.zip is extracted.
cd <TEMP_DIR>
unzip sim-reports.zip
cd <TEMP_DIR>/bip11g
```

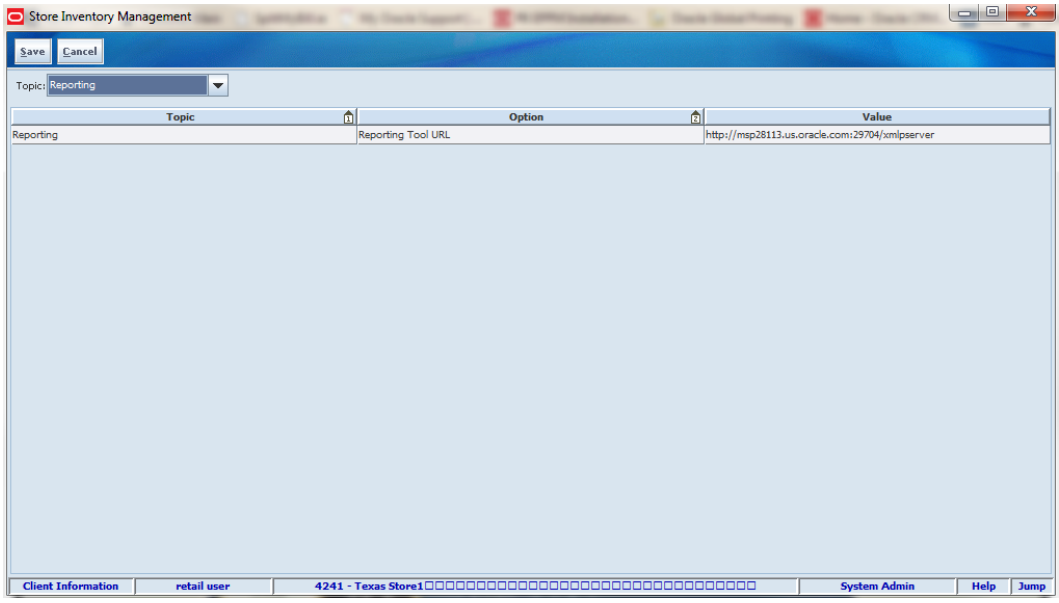
```
cp *
/u00/webadmin/product/10.3.X/WLS/user_projects/domains/bifoundation_domain/config/
bipublisher/repository/Reports/Guest/SIM
```

Bounce the xmlpserver application. The new SIM reports should be available in the "Shared Folders > Guest > SIM" location of BI Publisher.

BiPublisher 11g – Configuring the SIM Application with BIPublisher:

Make sure that the SIM application is set to use the reports. This can be done in the SIM application itself in the below location of SIM Application.

1. From Admin, go to setup -> system admin. Select the reporting topic.



2. Change the above URLs to match the host and port of where BI Publisher is running,

   The above info is put into these fields of the CONFIG_SYSTEM table of the SIM schema.

   REPORTING_TOOL_URL

Validating Reports

To test the reports, log into SIM application and click Reports. It should launch BI Publisher in a browser window. You can navigate to the SIM reports in BIPublisher window.

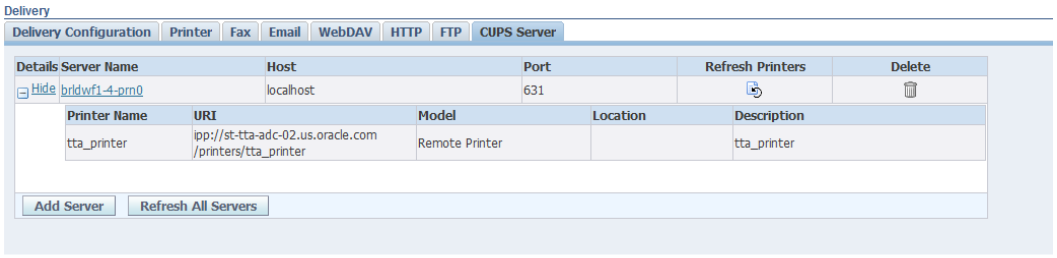
Configuring SIM for CUPS printers using BIPublisher 11g

Prerequisite: CUPS printer has to be set up on the BIPublisher server.

1. Login to BI Publisher using Administrator user and navigate to Administrator user. Example: http://msp52266.us.oracle.com:29704/xmlpserver
2. Click on the CUPS servers.

3. Click Add Servers.

4. After adding, refresh the servers and printers.



D

Appendix: Single Sign-On for WebLogic

Single Sign-On (SSO) is a term for the ability to sign onto multiple Web applications via a single user ID/Password. There are many implementations of SSO. Oracle provides an implementation with Oracle Access Manager.

Most, if not all, SSO technologies use a session cookie to hold encrypted data passed to each application. The SSO infrastructure has the responsibility to validate these cookies and, possibly, update this information. The user is directed to log on only if the cookie is not present or has become invalid. These session cookies are restricted to a single browser session and are never written to a file.

Another facet of SSO is how these technologies redirect a user's Web browser to various servlets. The SSO implementation determines when and where these redirects occur and what the final screen shown to the user is.

Most SSO implementations are performed in an application's infrastructure and not in the application logic itself. Applications that leverage infrastructure managed authentication (such as deployment specifying Basic or Form authentication) typically have little or no code changes when adapted to work in an SSO environment.

What Do I Need for Single Sign-On?

A Single Sign-On system involves the integration of several components, including Oracle Identity Management and Oracle Access Management. This includes the following components:

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.
- An Oracle Access Manager (OAM) 11g Release 1 server and administrative console for implementing and configuring policies for single sign-on.
- A Policy Enforcement Agent such as Oracle Access Manager 11g Agent (WebGate), used to authenticate the user and create the Single Sign-On cookies.
- Oracle Directory Services Manager (ODSM) application in OIM11g, used to administer users and group information. This information may also be loaded or modified via standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OAM system and registering HTTP servers.

Additional WebLogic managed servers will be needed to deploy the business applications leveraging the Single Sign-On technology.

Can Oracle Access Manager Work with Other SSO Implementations?

Yes, Oracle Access Manager has the ability to interoperate with many other SSO implementations, but some restrictions exist.

Oracle Single Sign-on Terms and Definitions

The following terms apply to single sign-on.

Authentication

Authentication is the process of establishing a user's identity. There are many types of authentication. The most common authentication process involves a user ID and password.

Dynamically Protected URLs

A Dynamically Protected URL is a URL whose implementing application is aware of the Oracle Access Manager environment. The application may allow a user limited access when the user has not been authenticated. Applications that implement dynamic protection typically display a Login link to provide user authentication and gain greater access to the application's resources.

Oracle Identity Management (OIM) and Oracle Access Manager (OAM) for 11g

Oracle Identity Management (OIM) 11g includes Oracle Internet Directory and ODSM. Oracle Access Manager (OAM) 11g should be used for SSO using WebGate. Oracle Forms 11g contains Oracle HTTP server and other Retail Applications will use Oracle WebTier11g for HTTP Server.

MOD_WEBLOGIC

mod_WebLogic operates as a module within the HTTP server that allows requests to be proxied from the OracleHTTP server to the Oracle WebLogic server.

Oracle Access Manager 11g Agent (WebGate)

Oracle WebGates are policy enforcement agents which reside with relying parties and delegate authentication and authorization tasks to OAM servers.

Oracle Internet Directory

Oracle Internet Directory (OID) is an LDAP-compliant directory service. It contains user ids, passwords, group membership, privileges, and other attributes for users who are authenticated using Oracle Access Manager.

Partner Application

A partner application is an application that delegates authentication to the Oracle Identity Management Infrastructure. One such partner application is the Oracle HTTP Server (OHS) supplied with Oracle Forms Server or WebTier11g Server if using other Retail Applications other than Oracle Forms Applications.

All partner applications must be registered with Oracle Access Manager (OAM) 11g. An output product of this registration is a configuration file the partner application uses to verify a user has been previously authenticated.

Statically Protected URLs

A URL is considered to be Statically Protected when an Oracle HTTP server is configured to limit access to this URL to only SSO authenticated users. Any unauthenticated attempt to access a Statically Protected URL results in the display of a login page or an error page to the user.

Servlets, static HTML pages, and JSP pages may be statically protected.

What Single Sign-On is not

Single Sign-On is NOT a user ID/password mapping technology.

However, some applications can store and retrieve user IDs and passwords for non-SSO applications within an OID LDAP server. An example of this is the Oracle Forms Web Application framework, which maps Single Sign-On user IDs to a database logins on a per-application basis.

How Oracle Single Sign-On Works

Oracle Access Manager involves several different components. These are:

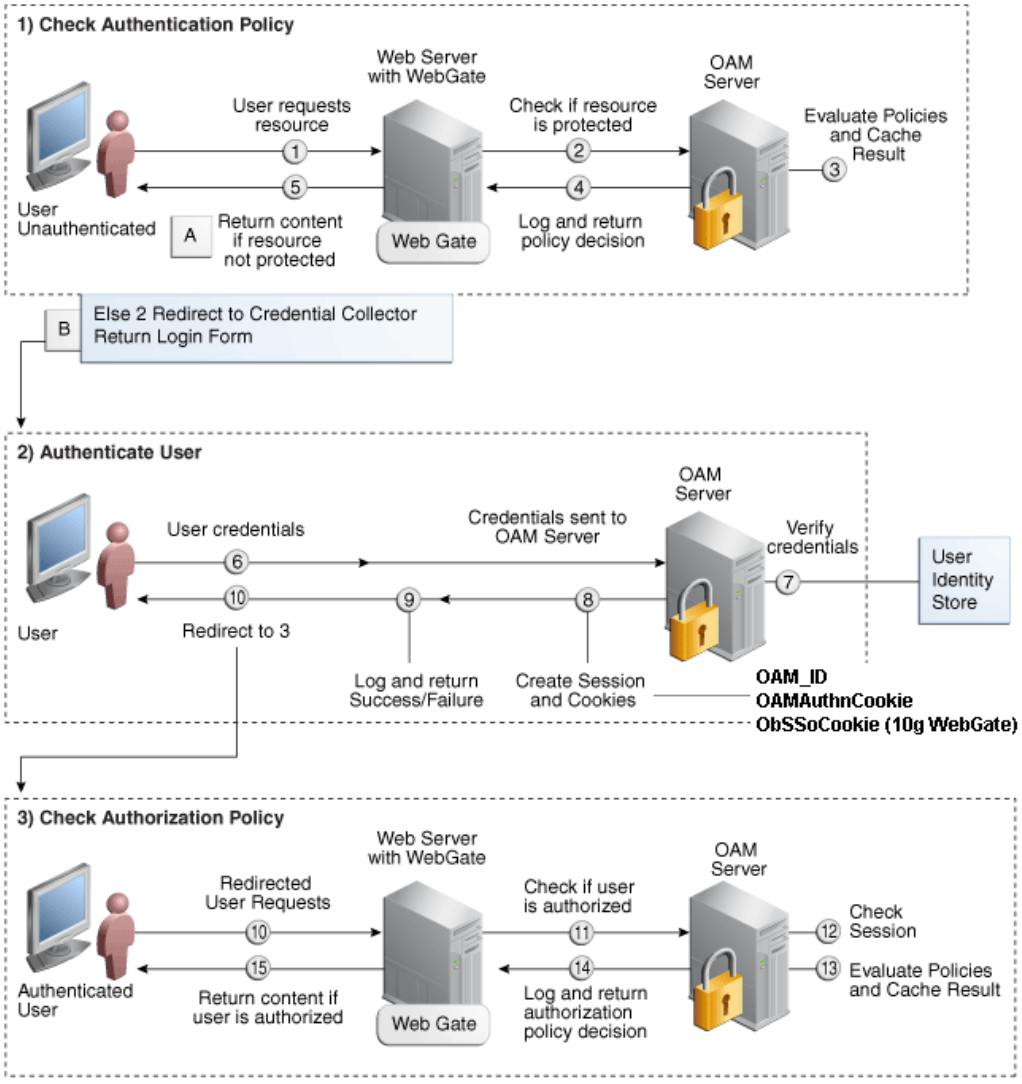
- The Oracle Access Manager (OAM) server, which is responsible for the back-end authentication of the user.
- The Oracle Internet Directory LDAP server, which stores user IDs, passwords, and group (role) membership.
- The Oracle Access Manager Agent associated with the Web application, which verifies and controls browser redirection to the Oracle Access Manager server.
- If the Web application implements dynamic protection, then the Web application itself is involved with the OAM system.

About SSO Login Processing with OAM Agents

1. The user requests a resource.
2. Webgate forwards the request to OAM for policy evaluation
3. OAM:
   a. Checks for the existence of an SSO cookie.
   b. Checks policies to determine if the resource is protected and if so, how?
4. OAM Server logs and returns the decision
5. Webgate responds as follows:
   - **Unprotected Resource:** Resource is served to the user
   - **Protected Resource:**
     Resource is redirected to the credential collector.
     The login form is served based on the authentication policy.
     Authentication processing begins
6. User sends credentials
7. OAM verifies credentials
8. OAM starts the session and creates the following host-based cookies:
   - **One per partner:** OAMAuthnCookie set by 11g WebGates using authentication token received from the OAM Server after successful authentication.
     Note: A valid cookie is required for a session.
   - **One for OAM Server:** OAM_ID
9. OAM logs Success of Failure.
10. Credential collector redirects to WebGate and authorization processing begins.
11. WebGate prompts OAM to look up policies, compare them to the user's identity, and determine the user's level of authorization.
12. OAM logs policy decision and checks the session cookie.
13. OAM Server evaluates authorization policies and cache the result.
14. OAM Server logs and returns decisions

15. WebGate responds as follows:
    - If the authorization policy allows access, the desired content or applications are served to the user.
    - If the authorization policy denies access, the user is redirected to another URL determined by the administrator.

SSO Login Processing with OAM Agents



Installation Overview

Installing an Oracle Retail supported Single Sign-On installation using OAM11g requires installation of the following:

1. Oracle Internet Directory (OID) LDAP server and the Oracle Directory Services Manager. They are typically installed using the Installer of Oracle Identity Management 11gR1 (11.1.1.7). The ODSM application can be used for user and realm management within OID.
2. Oracle Access Manager 11gR1 (11.1.1.5) has to be installed and configured.
3. Additional midtier instances (such as Oracle Forms 11g) for Oracle Retail applications based on Oracle Forms technologies (such as RMS). These instances must be registered with the OAM installed in step 2.
4. Additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities must be registered with OAM installed in step 2.

Infrastructure Installation and Configuration

The Infrastructure installation for Oracle Access Manager (OAM) is dependent on the environment and requirements for its use. Deploying Oracle Access Manager (OAM) to be used in a test environment does not have the same availability requirements as for a production environment. Similarly, the Oracle Internet Directory (OID) LDAP server can be deployed in a variety of different configurations. See the *Oracle Identity Management Installation Guide11g.*

OID User Data

Oracle Internet Directory is an LDAP v3 compliant directory server. It provides standards-based user definitions out of the box.

Customers with existing corporate LDAP implementations may need to synchronize user information between their existing LDAP directory servers and OID. OID supports standard LDIF file formats and provides a JNDI compliant set of Java classes as well. Moreover, OID provides additional synchronization and replication facilities to integrate with other corporate LDAP implementations.

Each user ID stored in OID has a specific record containing user specific information. For role-based access, groups of users can be defined and managed within OID. Applications can thus grant access based on group (role) membership saving administration time and providing a more secure implementation.

User Management

User Management consists of displaying, creating, updating or removing user information. There are many methods of managing an LDAP directory including LDIF scripts or Oracle Directory Services Manager (ODSM) available for OID11g.

ODSM

Oracle Directory Services Manager (ODSM) is a Web-based application used in OID11g is designed for both administrators and users which enables you to configure the structure of the directory, define objects in the directory, add and configure users, groups, and other entries. ODSM is the interface you use to manage entries, schema, security, adapters, extensions, and other directory features.

LDIF Scripts

Script based user management can be used to synchronize data between multiple LDAP servers. The standard format for these scripts is the LDAP Data Interchange Format (LDIF). OID supports LDIF script for importing and exporting user information. LDIF scripts may also be used for bulk user load operations.

User Data Synchronization

The user store for Oracle Access Manager resides within the Oracle Internet Directory (OID) LDAP server. Oracle Retail applications may require additional information attached to a user name for application-specific purposes and may be stored in an application-specific database. Currently, there are no Oracle Retail tools for synchronizing changes in OID stored information with application-specific user stores. Implementers should plan appropriate time and resources for this process. Oracle Retail strongly suggests that you configure any Oracle Retail application using an LDAP for its user store to point to the same OID server used with Oracle Access Manager.

E

Appendix: Setting Up Password Stores with wallets/credential stores

As part of an application installation, administrators must set up password stores for user accounts using wallets/credential stores. Some password stores must be installed on the application database side. While the installer handles much of this process, the administrators must perform some additional steps.

Password stores for the application and application server user accounts must also be installed; however, the installer takes care of this entire process.

ORACLE Retail Merchandising applications now have 3 different types of password stores. They are database wallets, java wallets, and database credential stores. Background and how to administer them below are explained in this appendix

About Database Password Stores and Oracle Wallet

Oracle databases have allowed other users on the server to see passwords in case database connect strings (username/password@db) were passed to programs. In the past, users could navigate to `ps –ef|grep <username>` to see the password if the password was supplied in the command line when calling a program.

To make passwords more secure, Oracle Retail has implemented the Oracle Software Security Assurance (OSSA) program. Sensitive information such as user credentials now must be encrypted and stored in a secure location. This location is called password stores or wallets. These password stores are secure software containers that store the encrypted user credentials.

Users can retrieve the credentials using aliases that were set up when encrypting and storing the user credentials in the password store. For example, if `username/password@db` is entered in the command line argument and the alias is called `db_username`, the argument to a program is as follows:

```
sqlplus /@db_username
```

This would connect to the database as it did previously, but it would hide the password from any system user.

After this is configured, as in the example above, the application installation and the other relevant scripts are no longer needed to use embedded usernames and passwords. This reduces any security risks that may exist because usernames and passwords are no longer exposed.

When the installation starts, all the necessary user credentials are retrieved from the Oracle Wallet based on the alias name associated with the user credentials.

There are three different types of password stores. One type explain in the next section is for database connect strings used in program arguments (such as `sqlplus /@db_username`). The others are for Java application installation and application use.

Setting Up Password Stores for Database User Accounts

After the database is installed and the default database user accounts are set up, administrators must set up a password store using the Oracle wallet. This involves assigning an alias for the username and associated password for each database user account. The alias is used later during the application installation. This password store must be created on the system where the application server and database client are installed.

This section describes the steps you must take to set up a wallet and the aliases for the database user accounts. For more information on configuring authentication and password stores, see the *Oracle Database Security Guide*.

> **Note:** In this section, <wallet_location> is a placeholder text for illustration purposes. Before running the command, ensure that you specify the path to the location where you want to create and store the wallet.

To set up a password store for the database user accounts, perform the following steps:

1. Create a wallet using the following command:

   ```
   mkstore -wrl <wallet_location> -create
   ```

   After you run the command, a prompt appears. Enter a password for the Oracle Wallet in the prompt.

   > **Note:** The mkstore utility is included in the Oracle Database Client installation.

   The wallet is created with the auto-login feature enabled. This feature enables the database client to access the wallet contents without using the password. For more information, refer to the *Oracle Database Advanced Security Administrator's Guide.*

2. Create the database connection credentials in the wallet using the following command:

   ```
   mkstore -wrl <wallet_location> -createCredential <alias-name> <database-user-name>
   ```

   After you run the command, a prompt appears. Enter the password associated with the database user account in the prompt.

3. Repeat Step 2 for all the database user accounts.

4. Update the sqlnet.ora file to include the following statements:

   ```
   WALLET_LOCATION = (SOURCE = (METHOD = FILE) (METHOD_DATA = (DIRECTORY = <wallet_location>)))
   SQLNET.WALLET_OVERRIDE = TRUE
   SSL_CLIENT_AUTHENTICATION = FALSE
   ```

5. Update the tnsnames.ora file to include the following entry for each alias name to be set up.

   ```
   <alias-name> =
       (DESCRIPTION =
        (ADDRESS_LIST =
              (ADDRESS = (PROTOCOL = TCP) (HOST = <host>) (PORT = <port>))
           )
           (CONNECT_DATA =
               (SERVICE_NAME = <service>)
            )
        )
   ```

In the previous example, <alias-name>, <host>, <port>, and <service> are placeholder text for illustration purposes. Ensure that you replace these with the relevant values.

For Java Applications (SIM, ReIM, RPM, RIB, RSL, AIP, Alloc batch, RETL)

For Java applications, consider the following:

- For database user accounts, ensure that you set up the same alias names between the password stores (database wallet and Java wallet). You can provide the alias name during the installer process.
- Document all aliases that you have set up. During the application installation, you must enter the alias names for the application installer to connect to the database and application server.
- Passwords are not used to update entries in Java wallets. Entries in Java wallets are stored in partitions, or application-level keys. In each retail application that has been installed, the wallet is located in <WEBLOGIC_DOMAIN_HOME>/retail/<appname>/config Example: /u00/webadmin/product/10.3.6/WLS/user_projects/domains/14_mck_soa_domain/retail/reim14/config
- Application installers should create the Java wallets for you, but it is good to know how this works for future use and understanding.
- Scripts are located in <WEBLOGIC_DOMAIN_HOME>/retail/<appname>/retail-public-security-api/bin for administering wallet entries.
- Example:
- /u00/webadmin/product/10.3.6/WLS/user_projects/domains/REIMDomain/retail/reim14/retail-public-security-api/bin
- In this directory is a script to help you update each alias entry without having to remember the wallet details. For example, if you set the RPM database alias to rms01user, you will find a script called update-RMS01USER.sh.

  Note: These scripts are available only with applications installed by way of an installer.

- Two main scripts are related to this script in the folder for more generic wallet operations: dump_credentials.sh and save_credential.sh.
- If you have not installed the application yet, you can unzip the application zip file and view these scripts in <app>/application/retail-public-security-api/bin.
- Example:
- /u00/webadmin/reim14/application/retail-public-security-api/bin

update-<ALIAS>.sh

update-<ALIAS>.sh updates the wallet entry for this alias. You can use this script to change the user name and password for this alias. Because the application refers only to the alias, no changes are needed in application properties files.

Usage:

```
update-<username>.sh <myuser>
```

Example:

```
mspdev71:[1034WLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/RPMDomain/retail/rpm14/reta
il-public-security-api/bin> ./update-RMS01USER.sh
usage: update-RMS01USER.sh <username>
<username>: the username to update into this alias.
Example: update-RMS01USER.sh myuser
Note: this script will ask you for the password for the username that you pass in.
mspdev71:[1034WLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/RPMDomain/retail/rpm14/reta
il-public-security-api/bin>
```

dump_credentials.sh

dump_credentials.sh is used to retrieve information from wallet. For each entry found in the wallet, the wallet partition, the alias, and the user name are displayed. Note that the password is not displayed. If the value of an entry is uncertain, run save_credential.sh to resave the entry with a known password.

```
dump_credentials.sh <wallet location>
```

Example:

```
dump_credentials.sh
location:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/REIMDomain/retail/
reim14/config

Retail Public Security API Utility
==========================================
```

Below are the credentials found in the wallet at the location:/u00/webadmin/product/10.3.x/WLS/user_projects/domains/REIMDomain/retail/reim14/config

```
==========================================

Application level key partition name:reim14
User Name Alias:WLS-ALIAS User Name:weblogic
User Name Alias:RETAIL-ALIAS User Name:retail.user
User Name Alias:LDAP-ALIAS User Name:RETAIL.USER
User Name Alias:RMS-ALIAS User Name:rms14mock
User Name Alias:REIMBAT-ALIAS User Name:reimbat
```

save_credential.sh

save_credential.sh is used to update the information in wallet. If you are unsure about the information that is currently in the wallet, use dump_credentials.sh as indicated above.

```
save_credential.sh -a <alias> -u <user> -p <partition name>  –l <path of the
wallet file location where credentials are stored>
```

Example:

```
mspdv351:[1036_WLS] /u00/webadmin/mock14_testing/rtil/rtil/application/retail-
public-security-api/bin> save_credential.sh -l wallet_test -a myalias -p
mypartition -u myuser

==========================================
Retail Public Security API Utility
==========================================

Enter password:
Verify password:
```

> **Note:** -p in the above command is for partition name. You must specify the proper partition name used in application code for each Java application.
>
> save_credential.sh and dump_credentials.sh scripts are the same for all applications. If using save_credential.sh to add a wallet entry or to update a wallet entry, bounce the application/managed server so that your changes are visible to the application. Also, save a backup copy of your cwallet.sso file in a location outside of the deployment path, because redeployment or reinstallation of the application will wipe the wallet entries you made after installation of the application. To restore your wallet entries after a redeployment/reinstallation, copy the backed up cwallet.sso file over the cwallet.sso file. Then bounce the application/managed server.

Usage

```
==========================================
Retail Public Security API Utility
==========================================
usage: save_credential.sh -au[plh]
E.g. save_credential.sh -a rms-alias -u rms_user -p rib-rms -l ./
 -a,--userNameAlias <arg>              alias for which the credentials
needs to be stored
 -h,--help                             usage information
 -l,--locationofWalletDir <arg>        location where the wallet file is
created.If not specified, it creates the wallet under secure-credential-wallet
directory which is already present under the retail-public-security-api/
directory.
 -p,--appLevelKeyPartitionName <arg>   application level key partition name
 -u,--userName <arg>                   username to be stored in secure
credential wallet for specified alias*
```

How does the Wallet Relate to the Application?

The ORACLE Retail Java applications have the wallet alias information you create in an <app-name>.properties file. Below is the reim.properties file. Note the database information and the user are presented as well. The property called datasource.credential.alias=RMS-ALIAS uses the ORACLE wallet with the argument of RMS-ALIAS at the csm.wallet.path and csm.wallet.partition.name = reim14 to retrieve the password for application use.

Reim.properties code sample:

```
datasource.url=jdbc:oracle:thin:@mspxxxxx.us.oracle.com:1521:pkols07
datasource.schema.owner=rms14mock
datasource.credential.alias=RMS-ALIAS
# ===============================================================
# ossa related Configuration
#
# These settings are for ossa configuration to store credentials.
# ===============================================================

csm.wallet.path=/u00/webadmin/product/10.3.x/WLS/user_projects/domains/REIMDomain/
retail/reim14/config
csm.wallet.partition.name=reim14
```

How does the Wallet Relate to Java Batch Program use?

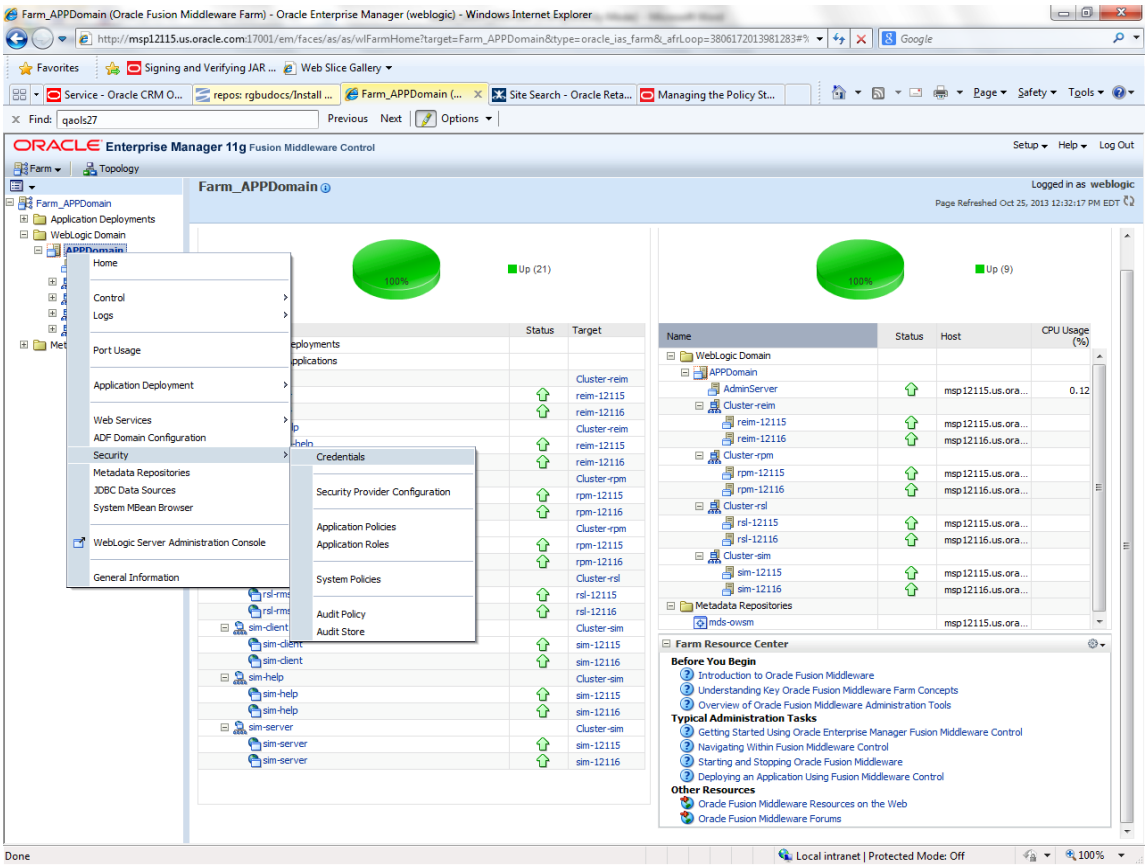
Some of the ORACLE Retail Java batch applications have an alias to use when running Java batch programs. For example, alias REIMBAT-ALIAS maps through the wallet to dbuser RMS01APP, already on the database. To run a ReIM batch program the format would be: reimbatchpgmname REIMBAT-ALIAS <other arguments as needed by the program in question>

Database Credential Store Administration

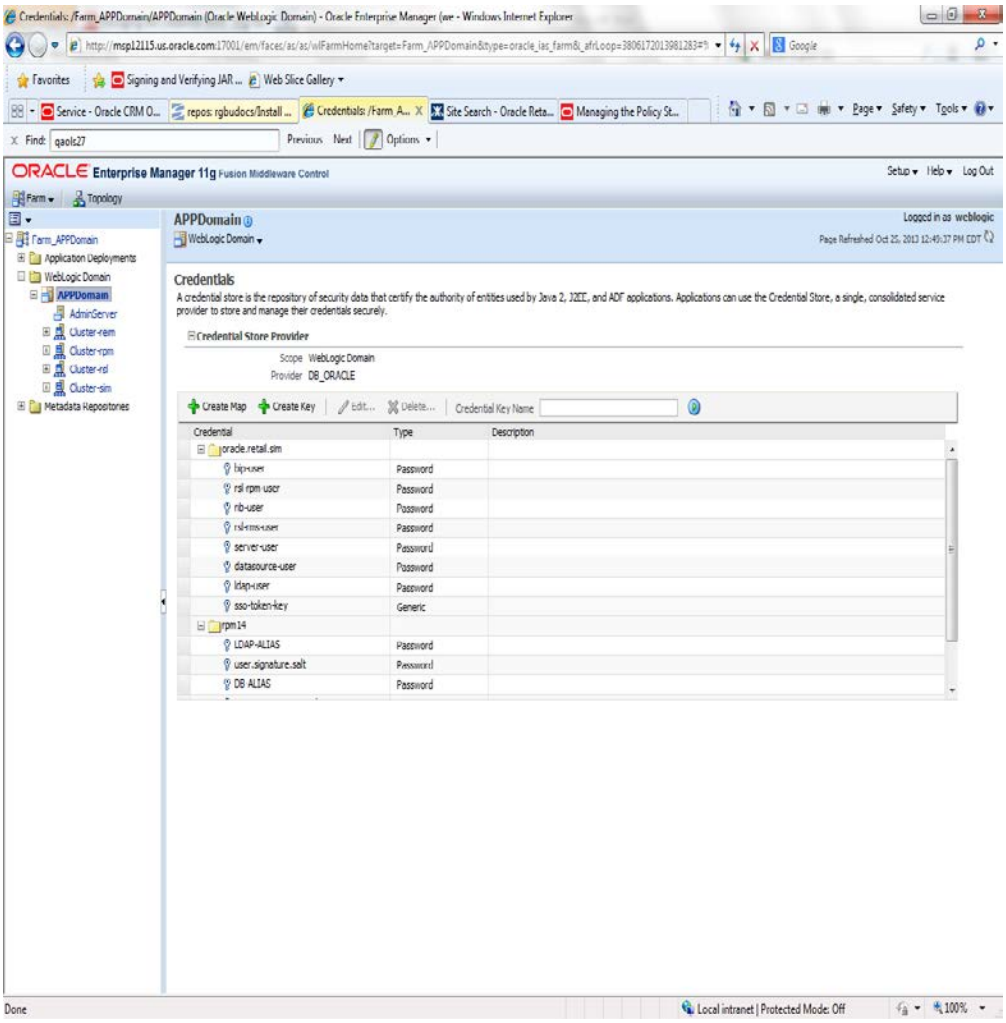
ORACLE Retail 14.0 brings something new into the password stores. A domain level database credential store. This is used in RPM login processing, SIM login processing, and Allocation login processing and policy information for application permission. Setting up the database credential store is addressed in the RPM, SIM, and Alloc 14.0 install guides.

The following sections show an example of how to administer the password stores thru ORACLE Enterprise Manger Fusion Middleware Control, a later section will show how to do this thru WLST scripts.

1. The first step is to use your link to Oracle Enterprise Manager Fusion Middleware Control for the domain in question. Locate your domain on the left side of the screen and do a right mouse click on the domain and select **Security** > **Credentials**

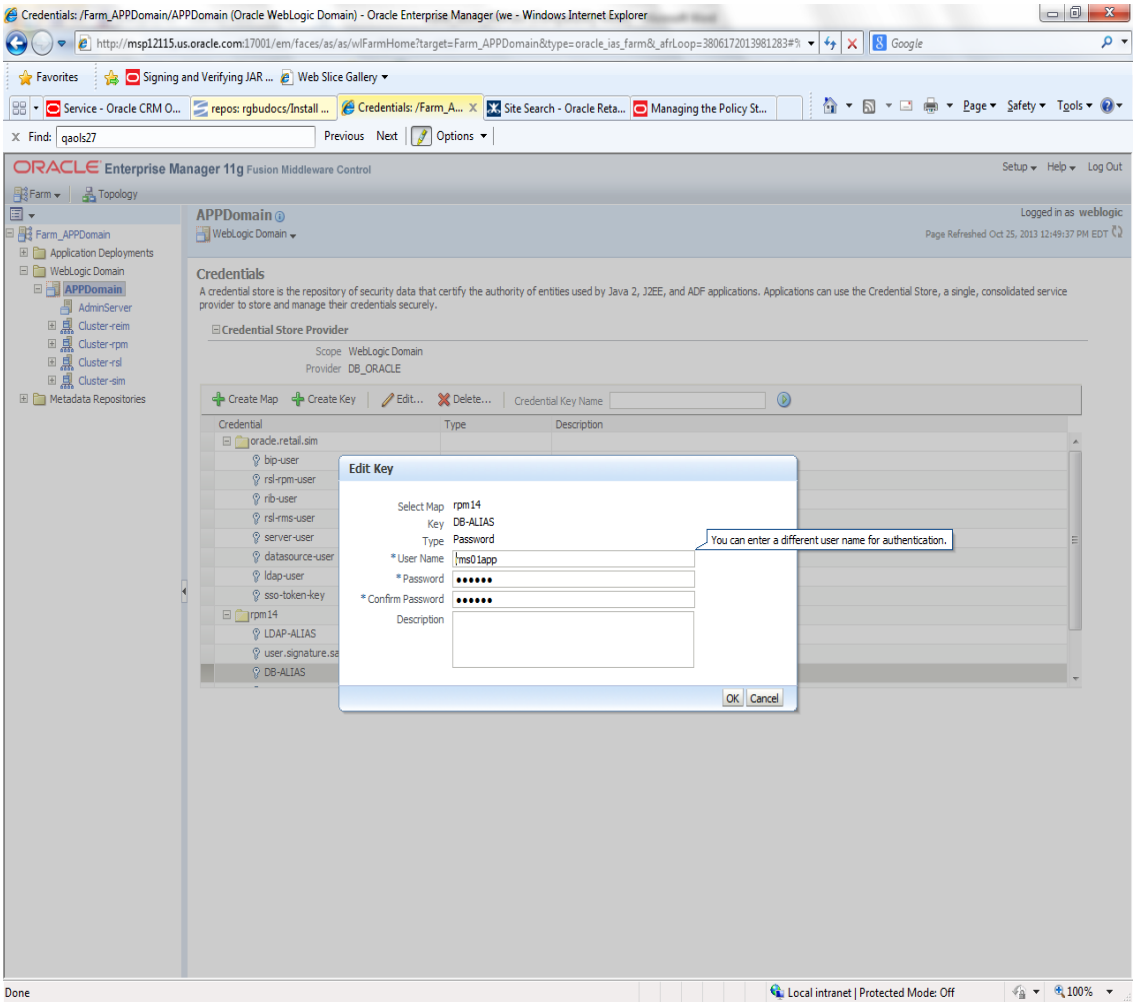


2. Click on Credentials and you will get a screen similar to the following. The following screen is expanded to make it make more sense. From here you can administer credentials.


Credentials: /Farm_APPDomain/APPDomain (Oracle WebLogic Domain) - Oracle Enterprise Manager (we - Windows Internet Explorer
ORACLE Enterprise Manager 11g Fusion Middleware Control
Setup
Help
Log Out
Farm
Topology
Farm_APPDomain
Application Deployments
WebLogic Domain
APPDomain
AdminServer
Cluster-rem
Cluster-rpm
Cluster-rsl
Cluster-sim
Metadata Repositories
APPDomain
WebLogic Domain
Logged in as weblogic
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
Scope WebLogic Domain
Provider DB_ORACLE
Create Map
Create Key
Edit...
Delete...
Credential Key Name
Credential
Type
Description
oracle.retail.sim
bip-user
Password
rsl rpm user
Password
rib-user
Password
rsl-rms-user
Password
server-user
Password
datasource-user
Password
ldap-user
Password
sso-token-key
Generic
rpm14
LDAP-ALIAS
Password
user.signature.salt
Password
DB ALIAS
Password
Done
Local intranet | Protected Mode: Off
100%

The Create Map add above is to create a new map with keys under it. A map would usually be an application such as rpm14. The keys will usually represent alias to various users (database user, WebLogic user, LDAP user, etc). The application installer should add the maps so you should not often have to add a map.

Creation of the main keys for an application will also be built by the application installer. You will not be adding keys often as the installer puts the keys out and the keys talk to the application. You may be using EDIT on a key to see what user the key/alias points to and possibly change/reset its password. To edit a key/alias, highlight the key/alias in question and push the edit icon nearer the top of the page. You will then get a screen as follows:



The screen above shows the map (rpm14) that came from the application installer, the key (DB-ALIAS) that came from the application installer (some of the keys/alias are selected by the person who did the application install, some are hard coded by the application installer in question), the type (in this case password), and the user name and password. This is where you would check to see that the user name is correct and reset the password if needed. REMEMBER, a change to an item like a database password WILL make you come into this and also change the password. Otherwise your application will NOT work correctly.

Managing Credentials with WSLT/OPSS Scripts

This procedure is optional as you can administer the credential store through the Oracle enterprise manager associated with the domain of your application install for RPM, SIM, or Allocation.

An Oracle Platform Security Scripts (OPSS) script is a WLST script, in the context of the Oracle WebLogic Server. An online script is a script that requires a connection to a running server. Unless otherwise stated, scripts listed in this section are online scripts and operate on a database credential store. There are a few scripts that are offline, that is, they do not require a server to be running to operate.

Read-only scripts can be performed only by users in the following WebLogic groups: Monitor, Operator, Configurator, or Admin. Read-write scripts can be performed only by users in the following WebLogic groups: Admin or Configurator. All WLST scripts are available out-of-the-box with the installation of the Oracle WebLogic Server.

WLST scripts can be run in interactive mode or in script mode. In interactive mode, you enter the script at a command-line prompt and view the response immediately after. In script mode, you write scripts in a text file (with a py file name extension) and run it without requiring input, much like the directives in a shell script.

For platform-specific requirements to run an OPSS script, see http://docs.oracle.com/cd/E21764_01/core.1111/e10043/managepols.htm#CIHIBBDJ

The weakness with the WLST/OPSS scripts is that you have to already know your map name and key name. In many cases, you do not know or remember that. The database credential store way through enterprise manager is a better way to find your map and key names easily when you do not already know them. A way in a command line mode to find the map name and alias is to run orapki. An example of orapki is as follows:

msp12115:[1036_APP] /u00/webadmin/product/wls_apps/oracle_common/bin>
./orapki wallet display –wallet
/u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmwconfig

(where the path above is the domain location of the wallet)

Output of orapki is below. This shows map name of rpm14 and each alias in the wallet:

Oracle PKI Tool : Version 11.1.1.7.0

Copyright (c) 2004, 2011, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:

User Certificates:

Oracle Secret Store entries:

rpm14@#3#@DB-ALIAS

rpm14@#3#@LDAP-ALIAS

rpm14@#3#@RETAIL.USER

rpm14@#3#@user.signature.salt

rpm14@#3#@user.signature.secretkey

rpm14@#3#@WEBLOGIC-ALIAS

rpm14@#3#@WLS-ALIAS

Trusted Certificates:

Subject: OU=Class 1 Public Primary Certification Authority,O=VeriSign\, Inc.,C=US

OPSS provides the following scripts on all supported platforms to administer credentials (all scripts are online, unless otherwise stated. You need the map name and the key name to run the scripts below

- listCred
- updateCred
- createCred
- deleteCred
- modifyBootStrapCredential
- addBootStrapCredential

listCred

The script `listCred` returns the list of attribute values of a credential in the credential store with given map name and key name. This script lists the data encapsulated in credentials of type password only.

Script Mode Syntax

```
listCred.py -map mapName -key keyName
```

Interactive Mode Syntax

```
listCred(map="mapName", key="keyName")
```

The meanings of the arguments (all required) are as follows:

- `map` specifies a map name (folder).
- `key` specifies a key name.

Examples of Use:

The following invocation returns all the information (such as user name, password, and description) in the credential with map name `myMap` and key name `myKey`:

```
listCred.py -map myMap -key myKey
```

The following example shows how to run this command and similar credential commands with WLST:

```
msp12115:[1036_APP] /u00/webadmin/product/wls_apps/oracle_common/common/bin>
sh wlst.sh

Initializing WebLogic Scripting Tool (WLST)...

Welcome to WebLogic Server Administration Scripting Shell


wls:/offline> connect('weblogic','password123','msp12115.us.oracle.com:17001')
Connecting to t3://msp12115.us.oracle.com:17001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'APPDomain'.

wls:/APPDomain/serverConfig> listCred(map="rpm14",key="DB-ALIAS")
Already in Domain Runtime Tree

[Name : rms01app, Description : null, expiry Date : null]
PASSWORD:retail
*The above means for map rpm14 in APPDomain, alias DB-ALIAS points to database
user rms01app with a password of retail
```

updateCred

The script `updateCred` modifies the type, user name, and password of a credential in the credential store with given map name and key name. This script updates the data encapsulated in credentials of type password only. Only the interactive mode is supported.

Interactive Mode Syntax

updateCred(map="mapName", key="keyName", user="userName", password="passW",

[desc="description"])

The meanings of the arguments (optional arguments are enclosed by square brackets) are as follows:

- `map` specifies a map name (folder) in the credential store.
- `key` specifies a key name.
- `user` specifies the credential user name.
- `password` specifies the credential password.
- `desc` specifies a string describing the credential.

Example of Use:

The following invocation updates the user name, password, and description of the password credential with map name `myMap` and key name `myKey`:

updateCred(map="myMap", key="myKey", user="myUsr", password="myPassw")

createCred

The script `createCred` creates a credential in the credential store with a given map name, key name, user name and password. This script can create a credential of type password only. Only the interactive mode is supported.

Interactive Mode Syntax

```
createCred(map="mapName", key="keyName", user="userName", password="passW",
[desc="description"])
```

The meanings of the arguments (optional arguments are enclosed by square brackets) are as follows:

- `map` specifies the map name (folder) of the credential.
- `key` specifies the key name of the credential.
- `user` specifies the credential user name.
- `password` specifies the credential password.
- `desc` specifies a string describing the credential.

Example of Use:

The following invocation creates a password credential with the specified data:

```
createCred(map="myMap", key="myKey", user="myUsr", password="myPassw")
```

deleteCred

The script `deleteCred` removes a credential with given map name and key name from the credential store.

Script Mode Syntax

```
deleteCred.py -map mapName -key keyName
```

Interactive Mode Syntax

```
deleteCred(map="mapName",key="keyName")
```

The meanings of the arguments (all required) are as follows:

- `map` specifies a map name (folder).
- `key` specifies a key name.

Example of Use:

The following invocation removes the credential with map name `myMap` and key name `myKey`:

```
deleteCred.py -map myMap -key myKey
```

modifyBootStrapCredential

The offline script `modifyBootStrapCredential` modifies the bootstrap credentials configured in the default jps context, and it is typically used in the following scenario: suppose that the policy and credential stores are LDAP-based, and the credentials to access the LDAP store (stored in the LDAP server) are changed. Then this script can be used to seed those changes into the bootstrap credential store.

This script is available in interactive mode only.

Interactive Mode Syntax

```
modifyBootStrapCredential(jpsConfigFile="pathName", username="usrName",
password="usrPass")
```

The meanings of the arguments (all required) are as follows:

- `jpsConfigFile` specifies the location of the file `jps-config.xml` relative to the location where the script is run. Example location: /u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmwconfig. Example location of the bootstrap wallet is /u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmwconfig/bootstrap
- `username` specifies the distinguished name of the user in the LDAP store.
- `password` specifies the password of the user.

Example of Use:

Suppose that in the LDAP store, the password of the user with distinguished name `cn=orcladmin` has been changed to `welcome1`, and that the configuration file `jps-config.xml` is located in the current directory.Then the following invocation changes the password in the bootstrap credential store to `welcome1`:

```
modifyBootStrapCredential(jpsConfigFile='./jps-config.xml',
username='cn=orcladmin', password='welcome1')
```

Any output regarding the audit service can be disregarded.

addBootStrapCredential

The offline script `addBootStrapCredential` adds a password credential with given map, key, user name, and user password to the bootstrap credentials configured in the default jps context of a jps configuration file.

Classloaders contain a hierarchy with parent classloaders and child classloaders. The relationship between parent and child classloaders is analogous to the object relationship of super classes and subclasses. The bootstrap classloader is the root of the Java classloader hierarchy. The Java virtual machine (JVM) creates the bootstrap classloader, which loads the Java development kit (JDK) internal classes and `java.*` packages included in the JVM. (For example, the bootstrap classloader loads `java.lang.String`.)

This script is available in interactive mode only.

Interactive Mode Syntax

addBootStrapCredential(jpsConfigFile="pathName", map="mapName", key="keyName",

username="usrName", password="usrPass")

The meanings of the arguments (all required) are as follows:

- `jpsConfigFile` specifies the location of the file `jps-config.xml` relative to the location where the script is run. Example location: /u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmwconfig
- `map` specifies the map of the credential to add.
- `key` specifies the key of the credential to add.
- `username` specifies the name of the user in the credential to add.
- `password` specifies the password of the user in the credential to add.

Example of Use:

The following invocation adds a credential to the bootstrap credential store:

```
addBootStrapCredential(jpsConfigFile='./jps-config.xml', map='myMapName',
key='myKeyName', username='myUser', password ='myPass')
```

Quick Guide for Retail Password Stores (db wallet, java wallet, DB credential stores)

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RMS batch	DB	<RMS batch install dir (MMHOME)>/.wallet	n/a	<Database SID>_<Database schema owner>	<rms schema owner>	Compile, execution	Installer	n/a	Alias hard-coded by installer
RMS forms	DB	<forms install dir>/base/.wallet	n/a	<Database SID>_<Database schema owner>	<rms schema owner>	Compile	Installer	n/a	Alias hard-coded by installer
ARI forms	DB	<forms install dir>/base/.wallet	n/a	<Db_Ari01>	<ari schema owner>	Compile	Manual	ari-alias	
RMWS forms	DB	<forms install dir>/base/.wallet	n/a	<Database SID>_<Database schema owner>	<rwms schema owner>	Compile forms, execute batch	Installer	n/a	Alias hard-coded by installer
RPM app	DB	<RPM batch install dir>/.wallet	n/a	<rms schema owner alias>	<rms schema owner>	Execute batch	Manual	rms-alias	RPM plsql and sqlldr batches
RWMS auto-login	JAVA	<forms install dir>/base/.javawallet							
			<RWMS Installation name>	<RWMS database user alias>	<RWMS schema owner>	RWMS forms app to avoid dblogin screen	Installer	rwms14inst	
			<RWMS Installation name>	BI_ALIAS	<BI Publisher administrative user>	RWMS forms app to connect to BI Publisher	Installer	n/a	Alias hard-coded by installer

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
AIP app	JAVA	<weblogic domain home>/retail/<deployed aip app name>/config							Each alias must be unique
			aip14	<AIP weblogic user alias>	<AIP weblogic user name>	App use	Installer	aip-weblogic-alias	
			aip14	<AIP database schema user alias>	<AIP database schema user name>	App use	Installer	aip01user-alias	
			aip14	<rib-aip weblogic user alias>	<rib-aip weblogic user name>	App use	Installer	rib-aip-weblogic-alias	
RPM app	DB credential store		Map=rpm14 or what you called the app at install time.	Many for app use					<weblogic domain home>/config/fmwconfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.
RPM app	JAVA	<weblogic domain home>/retail/<deployed rpm app name>/config							Each alias must be unique
			rpm14	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			rpm14	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			rpm14	<rpm application user one alias>	<rpm application user one name>	App use	Installer	user1-alias	
			rpm14	<rpm application user two alias>	<rpm application user two name>	App use	Installer	user2-alias	
			rpm14	<rpm batch user alias>	<rpm batch user name>	App, batch use	Installer	rpmbatch-alias	
			rpm14	<rib-rpm weblogic user alias>	<rib-rpm weblogic user name>	App use	Installer	rib-rpm-weblogic-alias	
ReIM app	JAVA	<weblogic domain home>/retail/<deployed reim app name>/config							Each alias must be unique
			<installed app name, ex: reim14>	<reim weblogic user alias>	<reim weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name, ex: reim14>	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			<installed app name, ex: reim14>	<reim webservice validation user alias>	<reim webservice validation user name>	App use	Installer	reimwebservice-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name, ex: reim14>	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbat-alias	
Alloc app	DB credential store		Map=alloc 14 or what you called the app at install time	Many for login and policies					<weblogic domain home>/config/fmwconfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file. The bootstrap directory under this directory has bootstrap cwallet.sso file.
Alloc app	JAVA	<weblogic domain home>/retail/<deployed alloc app name>/config							Each alias must be unique
			<installed app name>	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name>	<rms schema user alias>	<rms shema user name>	App use	Installer	rms01user-alias	
			<installed app name>	<rsl for rms weblogic user alias>	<rsl for rms weblogic user name>	App use	Installer	rsl-rms-weblogic-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name>	<alloc batch user alias>	<SYSTEM_ ADMINISTRATOR>	Batch use	Installer	alloc14	
RSL app	JAVA	<RSL INSTALL DIR>/rsl-rms/security/config							Each alias must be unique
			rsl-rsm	<rsl weblogic user alias>	<rsl weblogic user name>	App use	Installer	weblogic-alias	
			rsl-rsm	<rms shema user alias>	<rms shema user name>	App use	Installer	rms01user-alias	
SIM app	DB credential store		Map=oracle.retail.sim	Aliases required for SIM app use					<weblogic domain home>/config/fmwconfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.
	JAVA	<weblogic domain home>/retail/<deployed sim app name>/config	<installed sim app name>	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	
			<installed sim app name>	<rsl for rms weblogic user alias>	<rsl for rms weblogic user name>	App use	Installer	rsl-rms-weblogic-alias	
			<installed sim app name>	<rib-sim weblogic user alias>	<rib-sim weblogic user name>	App use	Installer	rib-sim-weblogic-alias	
RETL	JAVA	<RETL home>/etc/security	n/a	<target application user alias>	<target application db userid>	App use	Manual	retl_java_rms01user	User may vary depending on RETL flow's target application

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RETL	DB	<RETL home>/.wallet	n/a	<target application user alias>	<target application db userid>	App use	Manual	<db>_<user>	User may vary depending on RETL flow's target application
RIB	JAVA	<RIBHOME DIR>/deployment-home/conf/security							<app> is one of aip, rfm, rms, rpm, sim, rwms, tafr
JMS			jms<1-5>	<jms user alias> for jms<1-5>	<jms user name> for jms<1-5>	Integration use	Installer	jms-alias	
WebLogic			rib-<app>-app-server-instance	<rib-app weblogic user alias>	<rib-app weblogic user name>	Integration use	Installer	weblogic-alias	
Admin GUI			rib-<app>#web-app-user-alias	<rib-app admin gui user alias>	<rib-app admin gui user name>	Integration use	Installer	admin-gui-alias	
Application			rib-<app>#user-alias	<app weblogic user alias>	<app weblogic user name>	Integration use	Installer	app-user-alias	Valid only for aip, rpm, sim
DB			rib-<app>#app-db-user-alias	<rib-app database schema user alias>	<rib-app database schema user name>	Integration use	Installer	db-user-alias	Valid only for rfm, rms, rwms, tafr
Error Hospital			rib-<app>#hosp-user-alias	<rib-app error hospital database schema user alias>	<rib-app error hospital database schema user name>	Integration use	Installer	hosp-user-alias	
RFI	Java	<RFI-HOME>/retail-financial-integration-solution/service-based-integration/conf/security							

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name>	rfiAppServerAdminServerUserAlias	<rfi weblogic user name>	App use	Installer	rfiAppServerAdminServerUserAlias	
			<installed app name>	rfiAdminUiUserAlias	<ORFI admin user>	App use	Installer	rfiAdminUiUserAlias	
			<installed app name>	rfiDataSourceUserAlias	<ORFI schema user name>	App use	Installer	rfiDataSourceUserAlias	
			<installed app name>	ebsDataSourceUserAlias	<EBS schema user name>	App use	Installer	ebsDataSourceUserAlias	
			<installed app name>	smtpMailFromAddressAlias	<From email address>	App use	Installer	smtpMailFromAddressAlias	

F

Appendix: Database Parameter File

```
##############################################################################
# Oracle 11.2.0.x Parameter file
#
# NOTES: Before using this script:
#        1.  Change <datafile_path>, <admin_path>, <utl_file_path>, <diag_path>
and <hostname>
#            values as appropriate.
#        2.  Replace the word SID with the database name.
#        3.  Size parameters as necessary for development, test, and production
environments.
# ----------------------------------------------------------------------
# MAINTENANCE LOG
#
# Date     By          Parameter           Old/New         Notes
# +------+ +---------+ +-----------------+ +-------------+ +-------------+
#
#
##############################################################################
# ------------------------------------------------------------------------------
# The policy is to give 60% for sga and 40% for PGA out of Memory Target at
startup
# ------------------------------------------------------------------------------
memory_target                           = 3000M
# ------------------------------------------------------------------------------
audit_file_dest              = <admin_path>/adump
compatible            = 11.2.0
control_files                           = (<datafile_path>/control01.ctl
                                          ,<datafile_path>/control02.ctl)
db_block_size             = 8192      # Default is 2k; adjust before db creation,
cannot change after db is created
db_cache_size             = <A mimumum starting value >
db_file_multiblock_read_count        = 16        # Platform specific (max io
size)/(block size)
db_name               = SID
diagnostic_dest                         = '<diag_path>'
java_pool_size            = 100M
job_queue_processes           = 5         # Oracle Retail required; number of
cpu's + 1
local_listener                =
"(ADDRESS=(PROTOCOL=TCP)(HOST=<hostname>)(PORT=1521))"
nls_calendar                            = GREGORIAN
nls_date_format               = DD-MON-RR # Oracle Retail required; if RDW
database see later entry for proper format
nls_language              = AMERICAN  # Default
nls_numeric_characters        = ".,"      # Should be explicitly set to ensure all
users/batch get the same results
nls_sort              = BINARY    # Should be explicitly set to ensure all
sessions get the same order
nls_territory             = AMERICA   # Default
open_cursors              = 900       # Oracle Retail required (minimum=900);
default is 50
plsql_optimize_level                    = 2         # 10g change; use this setting
to optimize plsql performance
processes             = 2000       # Max number of OS  processes that can connect
to the db
```

```
query_rewrite_enabled         = TRUE      # Oracle Retail required for function-
based indexes
session_cached_cursors                    = 900       # Oracle Retail required;
shared_pool_size          = <A minimum starting value >
shared_pool_reserved_size     = < 10% of the shared_pool_size >
undo_management           = AUTO
undo_retention            = 1800      # Currently set for 30 minutes; set to avg
length of transactions in sec
undo_tablespace           = undo_ts
utl_file_dir                              = <utl_file_path>
workarea_size_policy                      = auto          # Should be set to auto
when pga_aggregate_target is set
#
# ***  Set these parameters for Oracle Retail Data Warehouse (RDW) database ***
#nls_date_format              = DD-MON-RRRR  # Required by MicroStrategy
#query_rewrite_integrity                  = TRUSTED
#star_transformation_enabled              = TRUE
#utl_file_dir                             = <Windows_utl_file_path>,
<UNIX_util_file_path>
#
# ***  Archive Logging, set if needed  ***
#log_archive_dest_1                       = 'location=<admin_path>/arch/'
#log_archive_format               = SIDarch_%r_%s_%t.log
#log_buffer           = 10485760    # Set to (512K or 128K)*CPUs
#log_checkpoint_interval                  = 51200     # Default:0 - unlimited
#log_checkpoint_timeout                   = 7200      # Default:1800 seconds
```

G

Appendix: Installation Order

This section provides a guideline as to the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use some, but not all, of the applications the order is still valid less the applications not being installed.

> **Note:** The installation order is not meant to imply integration between products.

Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM), Oracle Retail Sales Audit (ReSA). Optional: Oracle Retail Fiscal Management (ORFM)

   > **Note:** ORFM is an optional application for RMS if you are implementing Brazil localization.

2. Oracle Retail Service Layer (RSL)
3. Oracle Retail Extract, Transform, Load (RETL)
4. Oracle Retail Active Retail Intelligence (ARI)
5. Oracle Retail Warehouse Management System (RWMS)
6. Oracle Retail Invoice Matching (ReIM)
7. Oracle Retail Price Management (RPM)

   > **Note:** During installation of RPM, you are asked for the RIBforRPM provider URL. Because RIB is installed after RPM, make a note of the URL you enter. To change the RIBforRPM provider URL after you install RIB, edit the remote_service_locator_info_ribserver.xml file.

8. Oracle Retail Allocation
9. Oracle Retail Central Office (ORCO)
10. Oracle Retail Returns Management (ORRM)
11. Oracle Retail Back Office (ORBO)
12. Oracle Retail Store Inventory Management (SIM)

    > **Note:** During installation of SIM, you are asked for the RIB provider URL. Because RIB is installed after SIM, make a note of the URL you enter. To change the RIB provider URL after you install RIB, edit the remote_service_locator_info_ribserver.xml file.

13. Oracle Retail Predictive Application Server (RPAS)
14. Oracle Retail Demand Forecasting (RDF)
15. Oracle Retail Category Management (CM)
16. Oracle Retail Modeling Engine (ORME)
17. Oracle Retail Assortment Space Optimization (OASO)

18. Oracle Retail Replenishment Optimization (RO)
19. Oracle Retail Analytic Parameter Calculator Replenishment Optimization (APC RO)
20. Oracle Retail Regular Price Optimization (RPO)
21. Oracle Retail Merchandise Financial Planning (MFP)
22. Oracle Retail Size Profile Optimization (SPO)
23. Oracle Retail Assortment Planning (AP)
24. Oracle Retail Item Planning (IP)
25. Oracle Retail Item Planning Configured for COE (IP COE)
26. Oracle Retail Advanced Inventory Planning (AIP)
27. Oracle Retail Integration Bus (RIB)
28. Oracle Retail Service Backbone (RSB)
29. Oracle Retail Financial Integration (ORFI)
30. Oracle Retail Point-of-Service (ORPOS)
31. Oracle Retail Markdown Optimization (MDO)
32. Oracle Retail Clearance Optimization Engine (COE)
33. Oracle Retail Analytic Parameter Calculator for Markdown Optimization (APC-MDO)
34. Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
35. Oracle Retail Analytics