Oracle[®] Retail Invoice Matching

Installation Guide

Release 14.0.2

E60692-01

January 2015

Oracle® Retail Invoice Matching Installation Guide, Release 14.0.2

Primary Author: Wade Schwarz

Contributors: Nathan Young, Sahithya Sreenath and Kelly Baranick

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 Invoice Matching, 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 new Applications Release Online Documentation CD available on My Oracle Support and www.oracle.com. 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 Invoice Matching Release 14.0.2 documentation set:

- *Oracle Retail Invoice Matching Release Notes*
- *Oracle Retail Merchandising Batch Schedule*

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 explains the tasks required prior to installation.

Check for the Current Version of the Installation Guide

Corrected versions of Oracle Retail installation guides may be published whenever critical corrections are required. For critical corrections, the rerelease of an installation guide may not be attached to a release; the document will simply be replaced on the Oracle Technology Network Web site.

Before you begin installation, check to be sure that you have the most recent version of this installation guide. Oracle Retail installation guides are available on the Oracle Technology Network at the following URL:

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

An updated version of an installation guide is indicated by 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 an installation guide with part number E123456-**01**.

If a more recent version of this installation guide is available, that version supersedes all previous versions. Only use the newest version for your installation.

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 Oracle Retail Invoice Matching 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 11gR2	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

General requirements for an application server capable of running the Oracle Retail Invoice Matching 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) **Java:** ▪ JDK 1.7.0+ 64-bit **Other components:** ▪ Oracle BI Publisher 11g (11.1.1.7) ▪ Oracle Identity Management 11gR1 (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) ▪ ADF 11.1.1.7

Verify Single Sign-On

If ReIM will not be deployed in a Single Sign-On environment, skip this section.

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

Check Supported Client PC and Web Browser Requirements

Requirement	Version
Operating system	Windows 7
Display resolution	1024x768 or higher
Processor	2.6GHz or higher
Memory	1GByte or higher
Networking	intranet with at least 10Mbps data rate
Oracle (Sun) Java Runtime Environment	1.7.0+
Browser	Microsoft Internet Explorer 9 or 11 Mozilla Firefox 24.0

Configure Mozilla Firefox 24.0

If you are using Firefox 24.0, you need to configure the browser to display the list of values pop ups correctly.

1. Open your Firefox browser and type in your address bar as follows:
   ```
   about:config
   ```
2. A warning dialog is displayed. Accept the warning.

   A list of configuration values is displayed.
3. Locate the browser.link.open_newwindow property, right-click on it, and select Modify.
4. Change the value to 2.
5. Close and re-start the browser.

Supported Oracle Retail Products

Requirement	Version
Oracle Retail Merchandising System (RMS)/Oracle Retail Trade Management (RTM)/Oracle Retail Sales Audit (ReSA)	14.0.2
Oracle Retail Store Inventory Management (SIM) (by way of RMS)	14.0.2
Oracle Retail Analytics	14.0.2

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.

Supported Oracle Applications

Requirement	Version
Oracle E-Business Suite (Accounts Payable)	Oracle E-Business Suite 12.1.1 and 12.1.3 integration is supported using the Retail Financial Integration 14.0 for Oracle Retail Merchandising Suite and Oracle E-Business Suite Financials. See the *Oracle Retail Financial Integration for Oracle Retail Merchandise Operations Management and Oracle E-Business Suite or PeopleSoft Financials* for specific version information.
Oracle PeopleSoft Financials	OraclePeopleSoft Financials 9.2, integration is supported using the Oracle Retail Financial Integration for Oracle Retail Merchandising Suite and Oracle PeopleSoft Financials. See the *Oracle Retail Financial Integration for Oracle Retail Merchandise Operations Management and Oracle E-Business Suite or PeopleSoft Financials* for specific version information.

2

RAC and Clustering

Oracle Retail Invoice Matching has been validated to run in two configurations on Linux:

- Standalone WebLogic and Database installations
- Real Application Cluster Database and WebLogic 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. It is suggested that if you do use OCI connections, the Oracle Retail products database be configured in the tnsnames.ora file used by the WebLogic Server installations.

Clustering for WebLogic 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 WebLogic 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

The ReIM database objects are bundled with the RMS database schema installer. To install the ReIM database objects follow the *Oracle Retail Merchandising System Installation Guide* to run the database schema installer, and select the ReIM option on the product selection page.

4

Application Installation Tasks

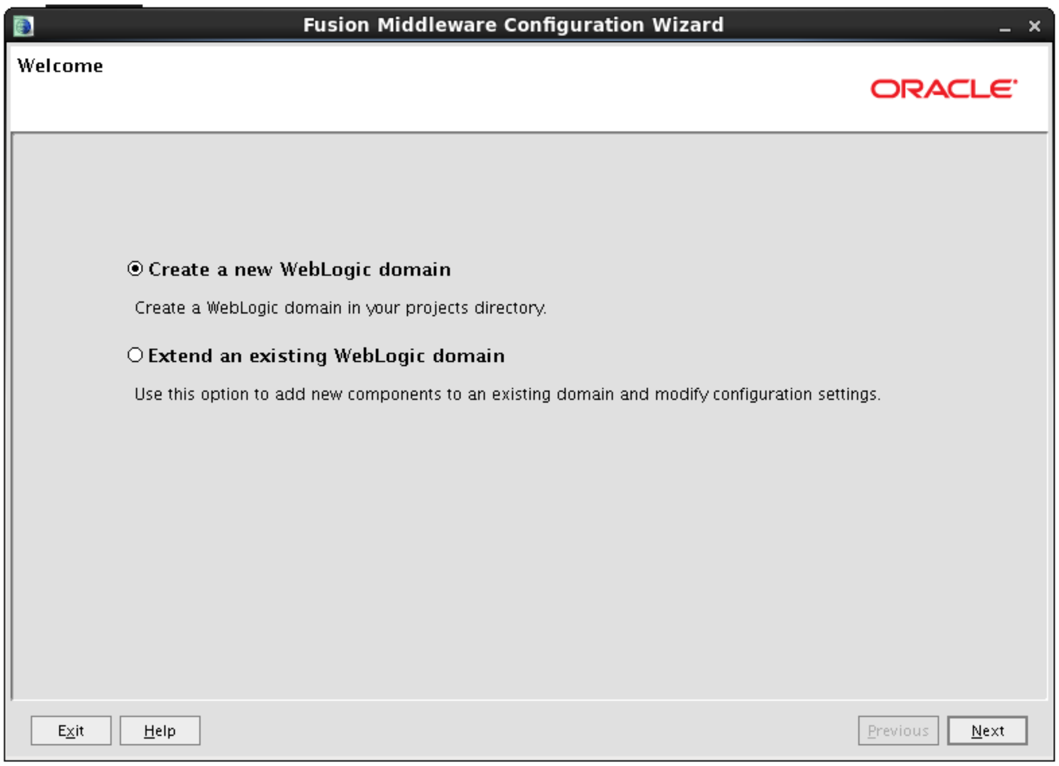
Before proceeding, you must install Oracle WebLogic Server 11g Release 1 (10.3.6) and patches listed in the Chapter 1 of this document. The Oracle Retail Invoice Matching application is deployed to a WebLogic Managed server within the Web Logic installation. It is assumed that Oracle Database has already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

Create WebLogic Domain

Perform the following procedure to create a domain. For example: REIMDomain

> **Note:** It is recommended to use separate domain for different Retail applications

1. Login to the application server. Go to <WEBLOGIC_HOME>/wlserver_10.3/common/bin.
2. Run the script, config.sh. The following screen pops up. Select **Create a new WebLogic domain** and click **Next**.



Fusion Middleware Configuration Wizard

Welcome

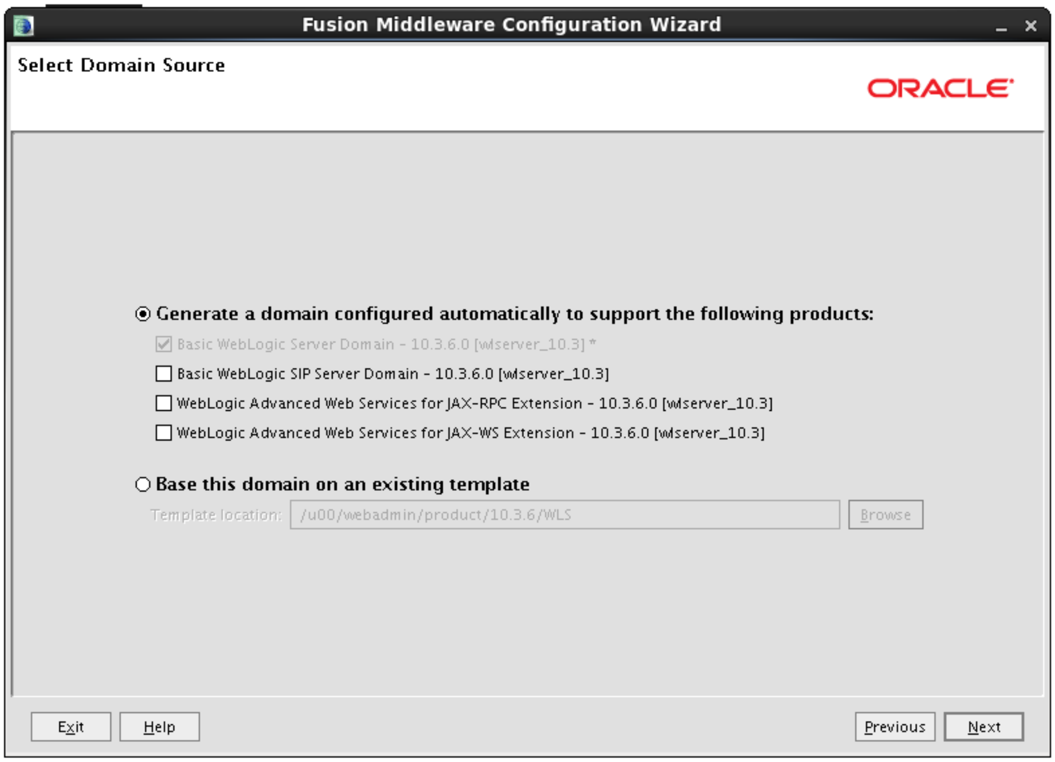
● Create a new WebLogic domain

Create a WebLogic domain in your projects directory.

○ Extend an existing WebLogic domain

Use this option to add new components to an existing domain and modify configuration settings.

3. Select the **Generate a domain configured automatically to support the following products** option and click **Next**.



● Generate a domain configured automatically to support the following products:

☑ Basic WebLogic Server Domain - 10.3.6.0 [wlserver_10.3] *

□ Basic WebLogic SIP Server Domain - 10.3.6.0 [wlserver_10.3]

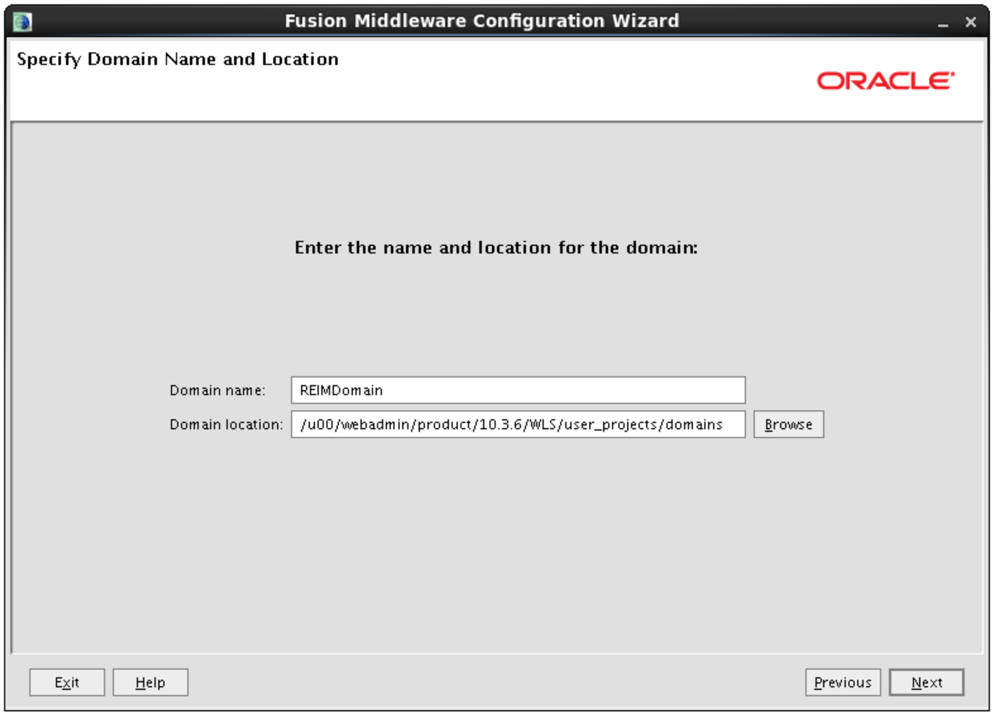
□ WebLogic Advanced Web Services for JAX-RPC Extension - 10.3.6.0 [wlserver_10.3]

□ WebLogic Advanced Web Services for JAX-WS Extension - 10.3.6.0 [wlserver_10.3]

○ Base this domain on an existing template

Template location: /u00/webadmin/product/10.3.6/WLS Browse

4. Enter the name of the domain (for example: REIMDomain) and the Domain Location. Click **Next**.



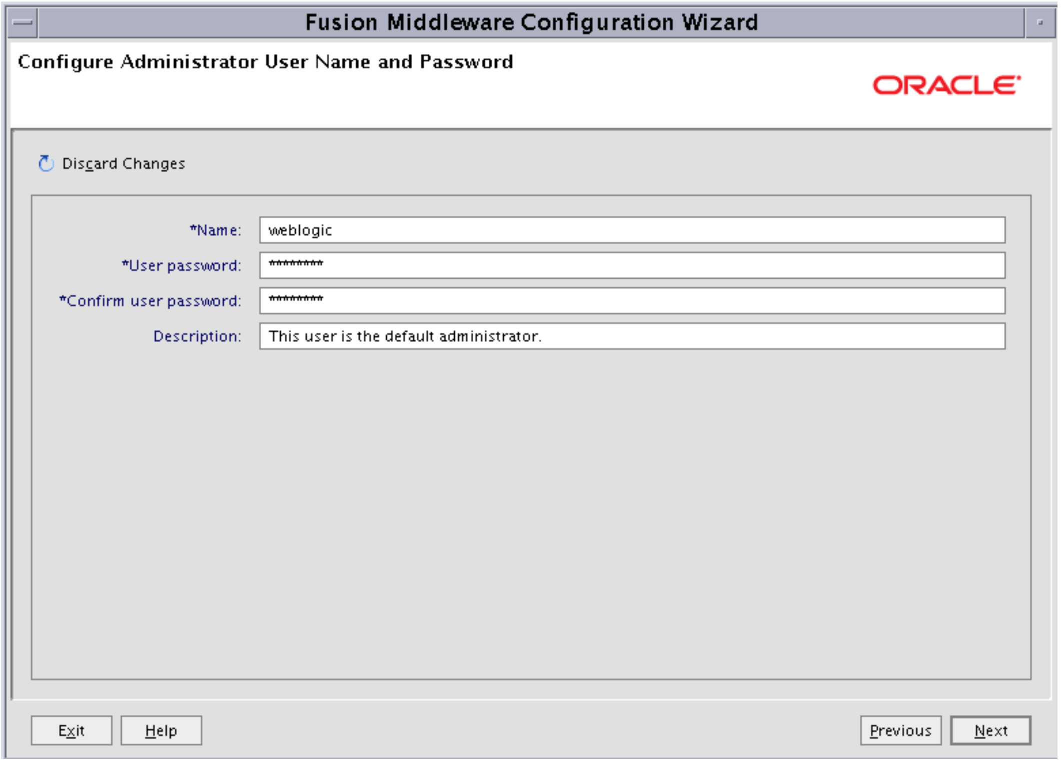
Fusion Middleware Configuration Wizard
Specify Domain Name and Location
ORACLE
Browse
Exit
Help
Previous
Next

Enter the name and location for the domain:

Domain name: REIMDomain

Domain location: /u00/webadmin/product/10.3.6/WLS/user_projects/domains

5. Set Administrator username and password and click **Next**.



Fusion Middleware Configuration Wizard

Configure Administrator User Name and Password

Discard Changes

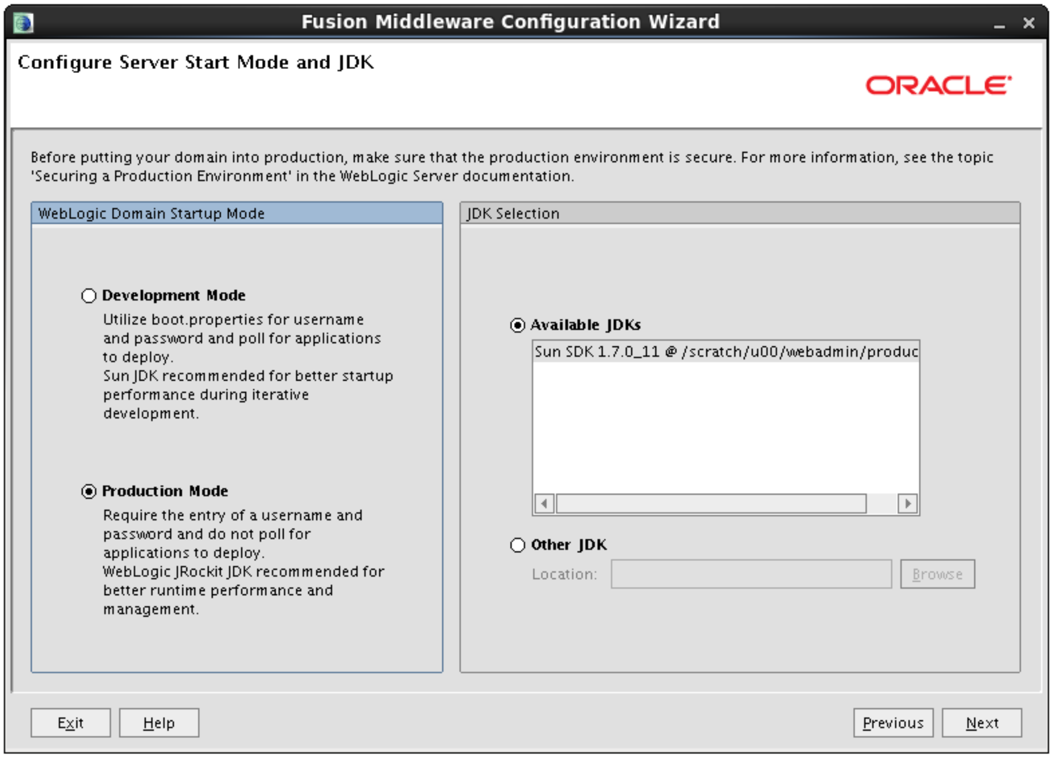
*Name: weblogic

*User password: *********

*Confirm user password: *********

Description: This user is the default administrator.

6. It is recommended that you select **Production Mode**. Make sure that the location to JAVA 1.7+ is provided. Click **Next**.



Fusion Middleware Configuration Wizard

Configure Server Start Mode and JDK

Before putting your domain into production, make sure that the production environment is secure. For more information, see the topic 'Securing a Production Environment' in the WebLogic Server documentation.

WebLogic Domain Startup Mode

○ **Development Mode**
Utilize boot.properties for username and password and poll for applications to deploy.
Sun JDK recommended for better startup performance during iterative development.

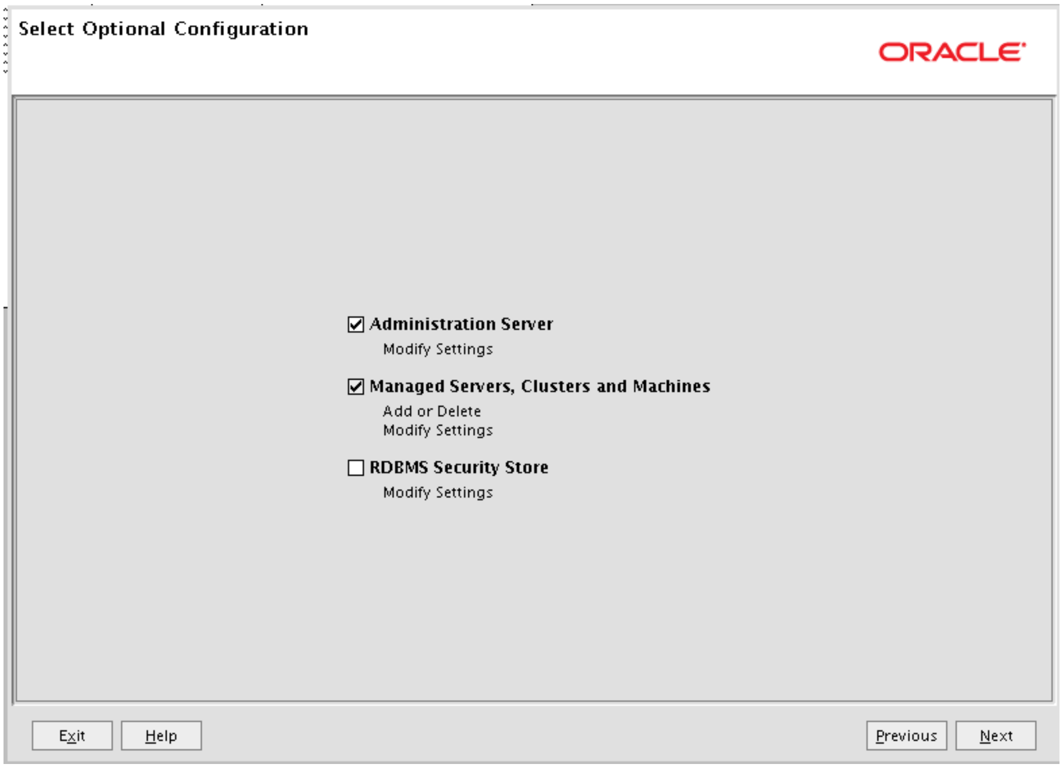
● **Production Mode**
Require the entry of a username and password and do not poll for applications to deploy.
WebLogic JRockit JDK recommended for better runtime performance and management.

JDK Selection

● **Available JDKs**
Sun SDK 1.7.0_11 @ /scratch/u00/webadmin/produc

○ **Other JDK**
Location:

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



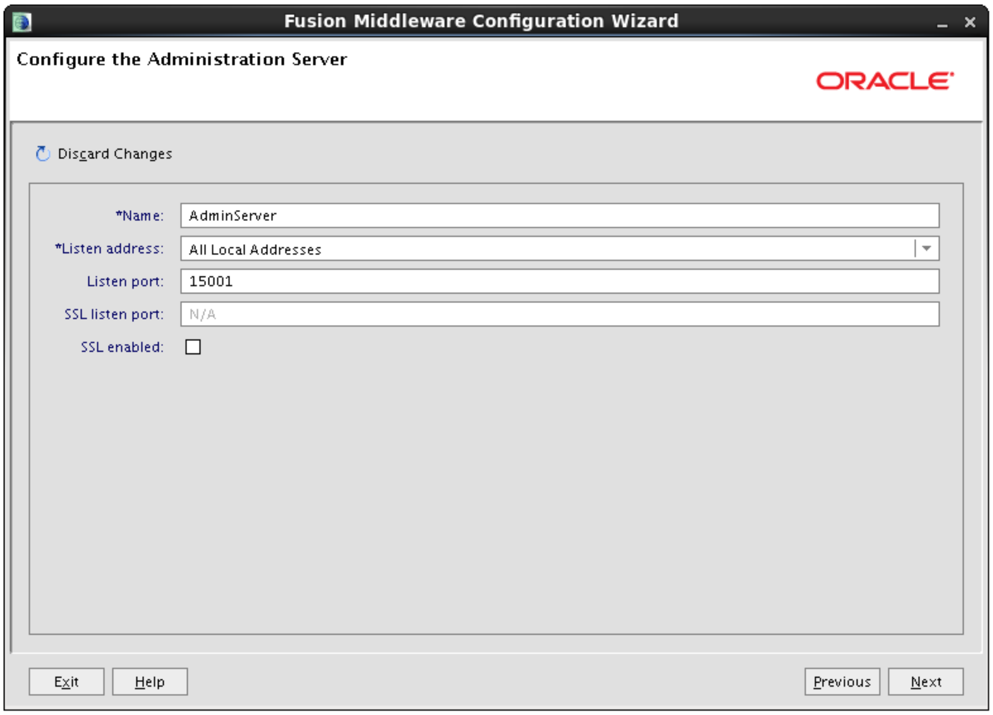
Select Optional Configuration

☑ Administration Server
Modify Settings

☑ Managed Servers, Clusters and Machines
Add or Delete
Modify Settings

☐ RDBMS Security Store
Modify Settings

8. Provide a name for the Administration Server (for example: AdminServer) and a Listen port (for example: 15001). Click **Next**.



Fusion Middleware Configuration Wizard

Configure the Administration Server

Discard Changes

*Name: AdminServer

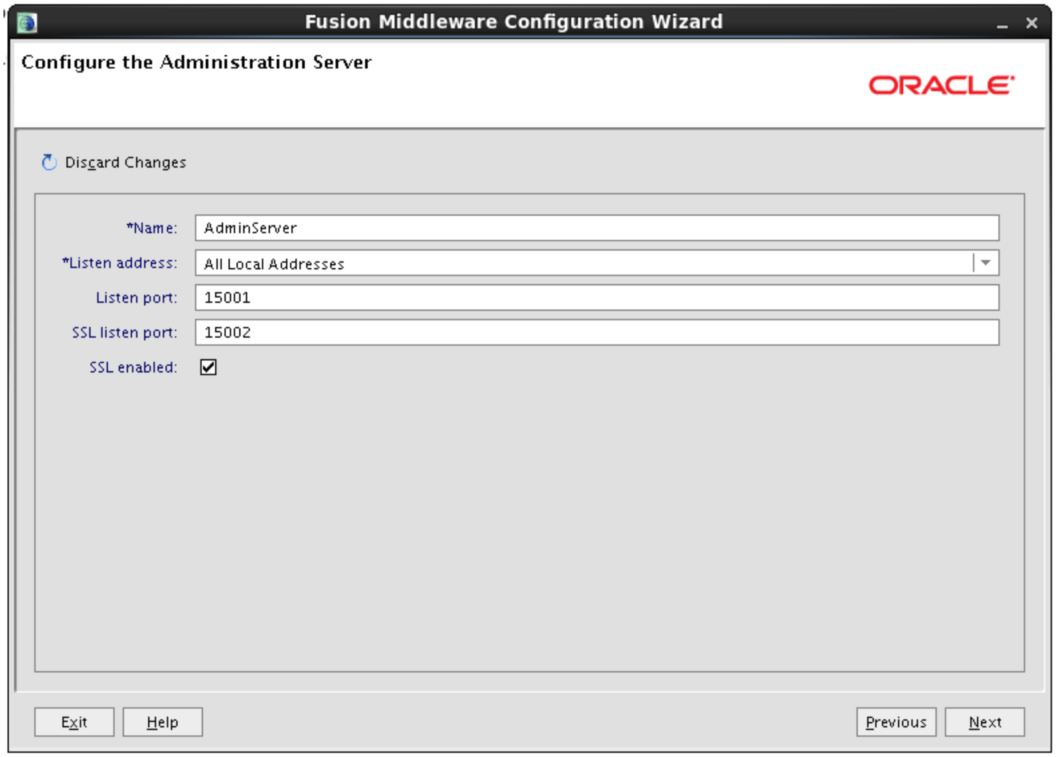
*Listen address: All Local Addresses

Listen port: 15001

SSL listen port: N/A

SSL enabled: ☐

9. If you require an SSL setup of a domain, select **SSL enabled** and provide an SSL listen port (for example: 15002). Click **Next**.



Fusion Middleware Configuration Wizard

Configure the Administration Server

*Name: AdminServer

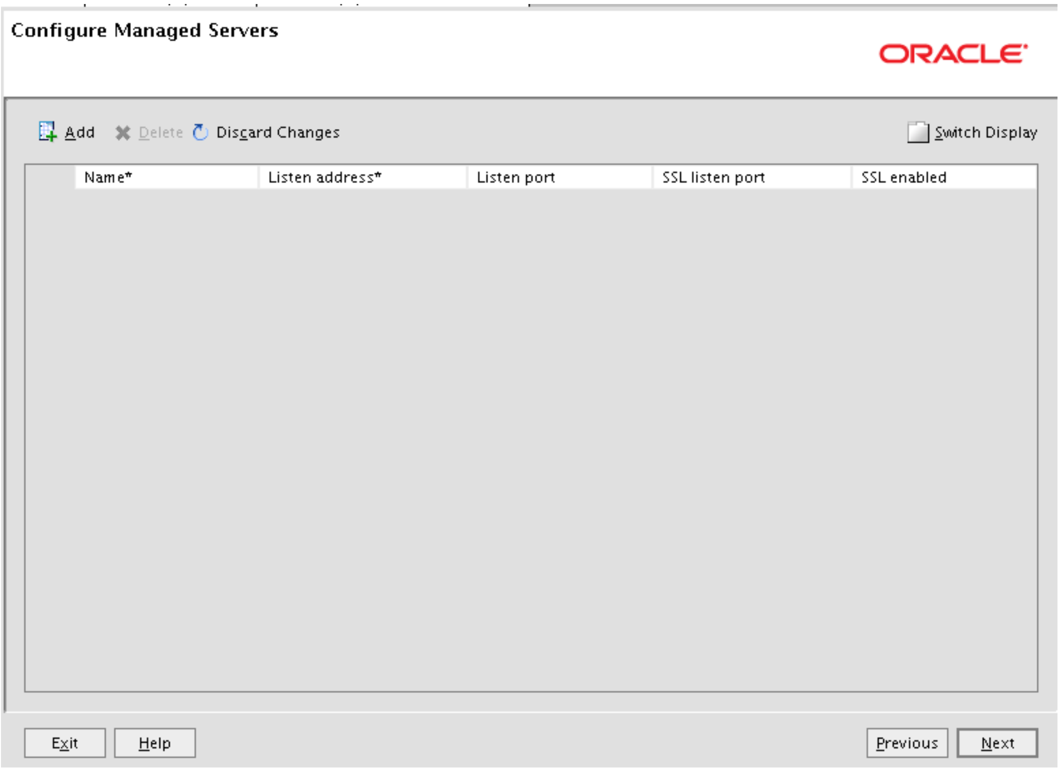
*Listen address: All Local Addresses

Listen port: 15001

SSL listen port: 15002

SSL enabled: ☑

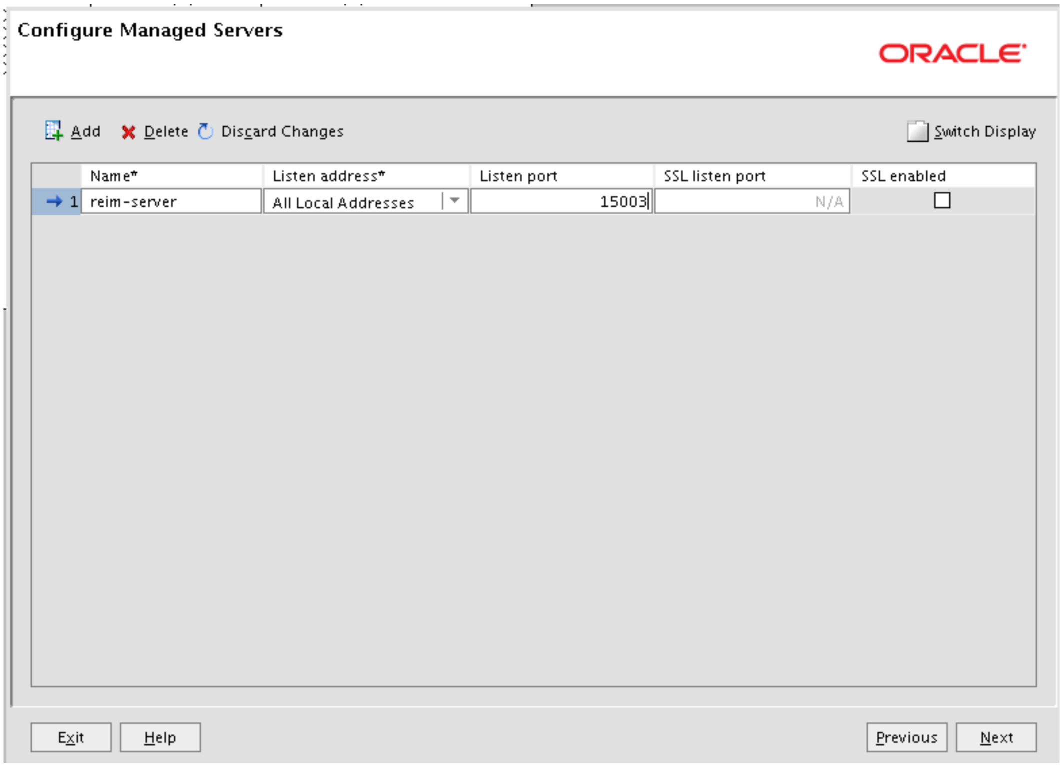
10. This screen allows us to add managed servers. Click **Add**.



Configure Managed Servers

Name*	Listen address*	Listen port	SSL listen port	SSL enabled

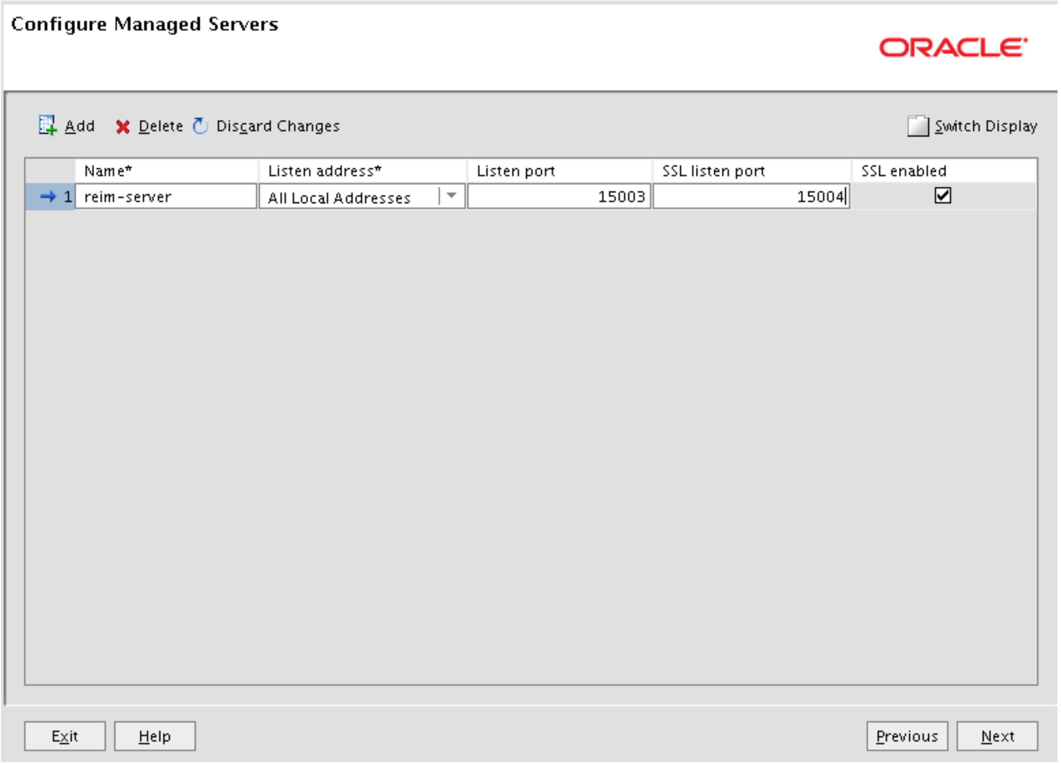
11. Create a managed server.



Configure Managed Servers

	Name*	Listen address*	Listen port	SSL listen port	SSL enabled
1	reim-server	All Local Addresses	15003	N/A	□

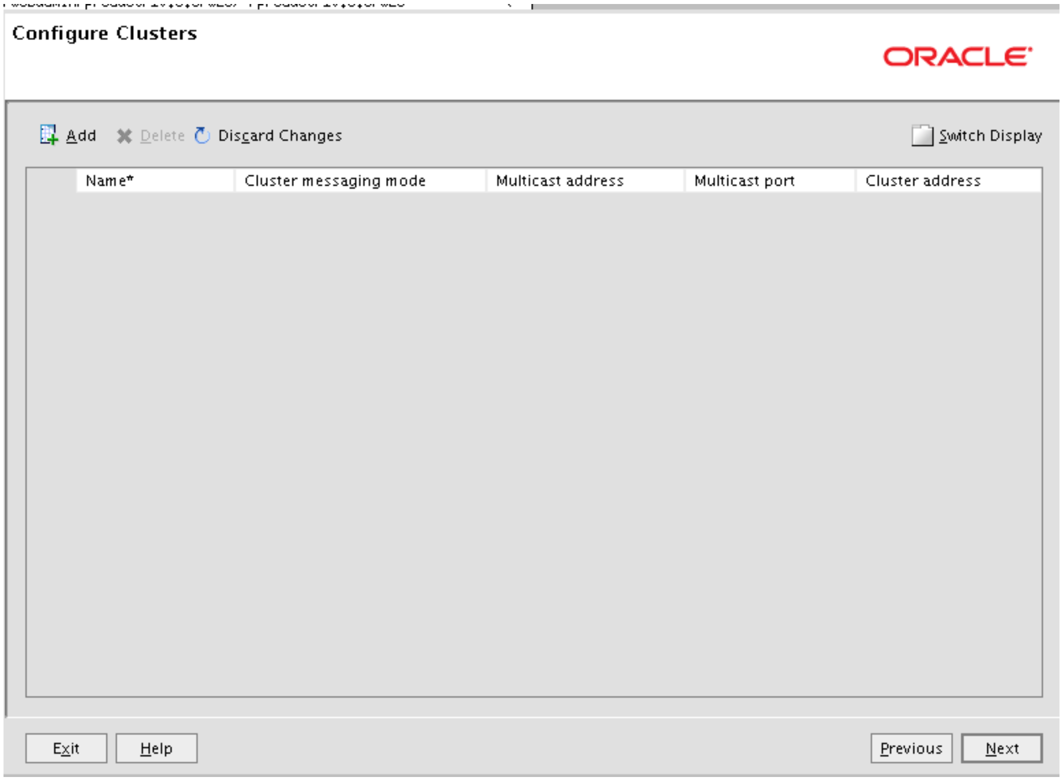
12. If SSL is enabled, update the SSL fields. Click **Next**.



Configure Managed Servers

	Name*	Listen address*	Listen port	SSL listen port	SSL enabled
1	reim-server	All Local Addresses	15003	15004	☑

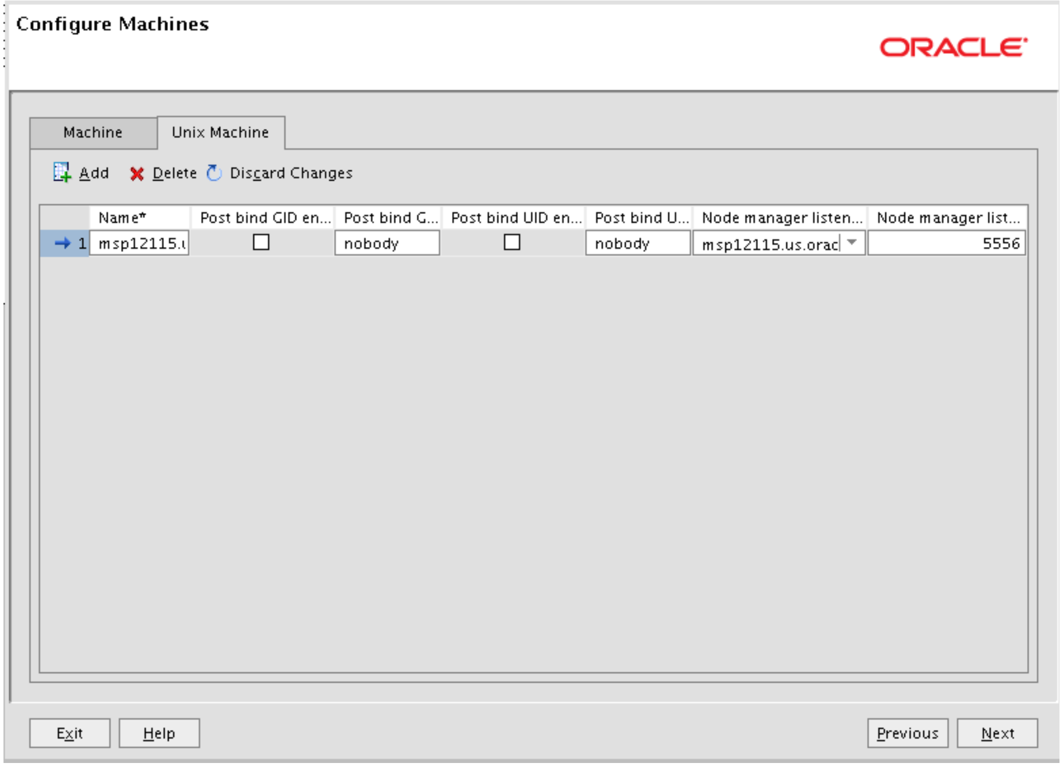
13. If the setup comprises of a cluster, the below screen need is to be filled. If the setup does not involve a cluster, you can skip this screen. Click **Next**.



Configure Clusters

Name*	Cluster messaging mode	Multicast address	Multicast port	Cluster address

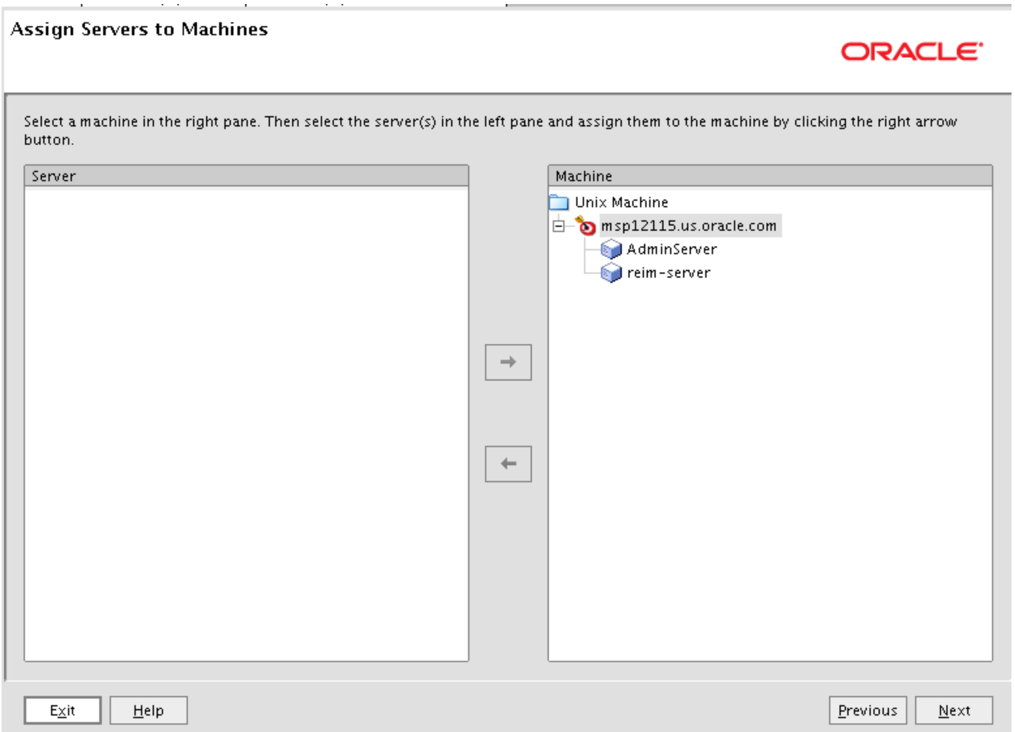
14. Create nodemanager (5556 is the default port). Any free port can be used. Click **Next**.



Configure Machines

	Name*	Post bind GID en...	Post bind G...	Post bind UID en...	Post bind U...	Node manager listen...	Node manager list...
1	msp12115.u	□	nobody	□	nobody	msp12115.us.orac	5556

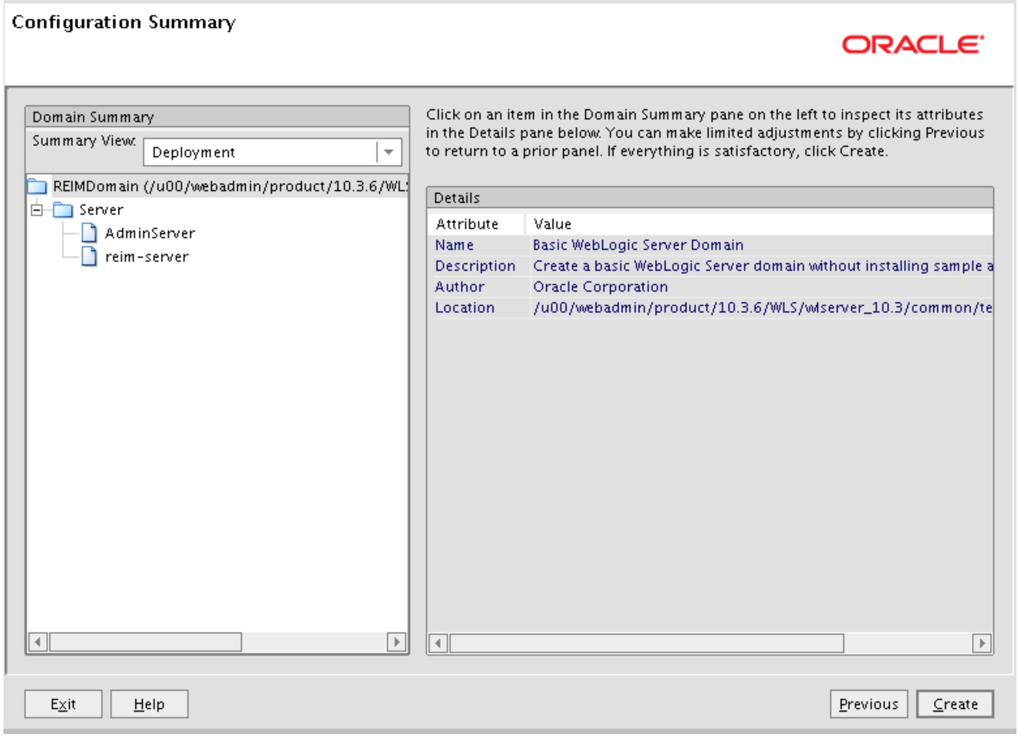
15. Add the AdminServer and the reim-server to the nodemanager we just created. Click **Next**.



Assign Servers to Machines

Select a machine in the right pane. Then select the server(s) in the left pane and assign them to the machine by clicking the right arrow button.

16. Review the installation summary. Click **Create**.



Configuration Summary

Click on an item in the Domain Summary pane on the left to inspect its attributes in the Details pane below. You can make limited adjustments by clicking Previous to return to a prior panel. If everything is satisfactory, click Create.

Summary View: Deployment

Attribute	Value
Name	Basic WebLogic Server Domain
Description	Create a basic WebLogic Server domain without installing sample a
Author	Oracle Corporation
Location	/u00/webadmin/product/10.3.6/WLS/wlserver_10.3/common/te

17. Click **Done** once it is complete.

Start the Node Manager

Start up the nodemanager. 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.

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):

Start up the AdminServer using the REIMDomain/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 REIMDomain/servers/AdminServer/security

vi REIMDomain/servers/AdminServer/security/boot.properties

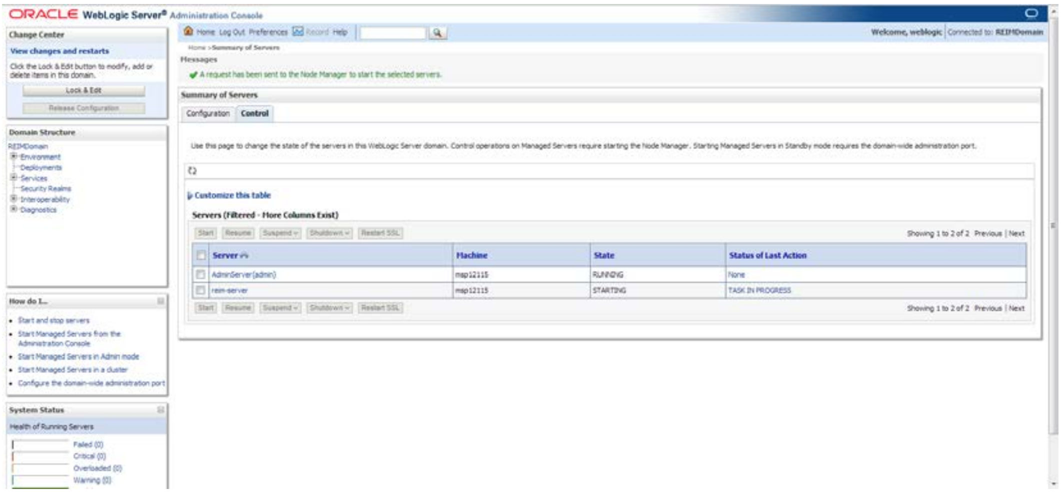
- username=weblogic
- password=<password used at domain creation>

This file will be encrypted after the REIMDomain 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 reim-server and click **start**.



ORACLE WebLogic Server® Administration Console
Home Log Out Preferences Record Help
Welcome, weblogic Connected to: REIMDomain
Home >Summary of Servers
Change Center
View changes and restarts
Click the Lock & Edit button to modify, add or delete items in this domain.
Lock & Edit
Release Configuration
Domain Structure
REIMDomain
Environment
Deployments
Services
Security Realms
Interoperability
Diagnostics
How do I...
Start and stop servers
Start Managed Servers from the Administration Console
Start Managed Servers in Admin mode
Start Managed Servers in a cluster
Configure the domain-wide administration port
System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)
Warning (0)
Summary of Servers
Configuration
Control
Customize this table
Start
Resume
Suspend
Shutdown
Restart SSL
Showing 1 to 2 of 2 Previous | Next

Messages

✓ A request has been sent to the Node Manager to start the selected servers.

Use this page to change the state of the servers in this WebLogic Server domain. Control operations on Managed Servers require starting the Node Manager. Starting Managed Servers in Standby mode requires the domain-wide administration port.

Servers (Filtered - More Columns Exist)

□	Server	Machine	State	Status of Last Action
□	AdminServer(admin)	msp12115	RUNNING	None
□	reim-server	msp12115	STARTING	TASK IN PROGRESS

Expand the ReIM Application Distribution

To expand the ReIM application distribution, do the following.

1. Log in to the UNIX server as the user who owns the WebLogic installation. Create a new staging directory for the ReIM application distribution (reim14application.zip).

   Example: /u00/webadmin/media/reim

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

2. Copy reim14application.zip to INSTALL_DIR and extract its contents.
3. Export WEBLOGIC_DOMAIN_HOME=<full_path_to_domain>.
4. Update <WLS_HOME>/server/lib/weblogic.policy file with the 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 semicolon.

   Note: <WEBLOGIC_DOMAIN_HOME> in the below example is the full path of the Weblogic Domain, <managed_server> is the managed server created for the App and <context_root> correlates to the value entered for the application deployment name/context root of the application during installation. See the example. There should not be a space after **file:** in the following. file:<WEBLOGIC_DOMAIN_HOME>.

```
grant codeBase "file:<WEBLOGIC_DOMAIN_HOME>/servers/<managed_server>/
tmp/_WL_user/<context_root>/-" {
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/10.3.6/WLS/user_projects/domains/
REIMDomain/servers/reim-server/tmp/_WL_user/reim/-" {
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";
}
```

5. Restart WebLogic admin server after making changes to the weblogic.policy file in the previous step.

Clustered Installations – Preinstallation Steps

> **Note:** Skip this section if you are not clustering the application server.

Complete the following preinstallation steps.

1. Make sure that you are able to start and stop the managed servers that are part of the ReIM Cluster from the Administration Console.
2. Update the $WEBLOGIC_HOME/wlserver_10.3/server/lib/weblogic.policy file on all nodes with the same ReIM entries for java security permissions that were entered on the main server. See the Start the Managed Servers section for additional information.

There are no additional steps to take before running the installer for ReIM.

Configure LDAP authentication Preinstallation Steps (Initial Login to ReIM)

In order to Login to ReIM after the installation is done, you need to complete the following pre-installation steps.

1. Make sure that you have access to a working LDAP server.

> **Note:** It is recommended that you use OID 11g (11.1.1.7).

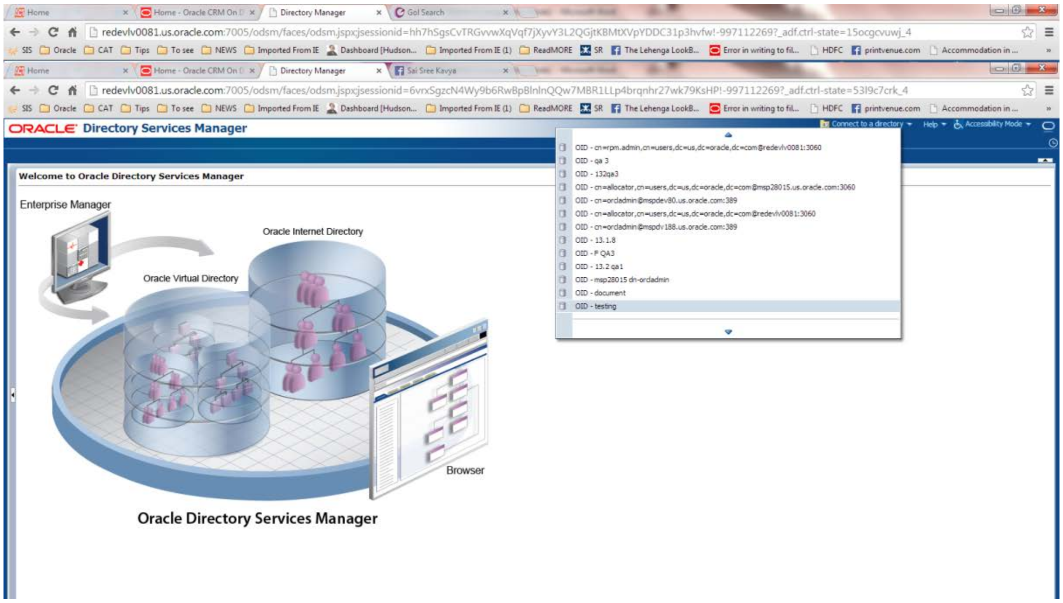
2. Create a Group called "reim". All users need to be a member of this group in order to login to the ReIM application.

> **Note:** The ReIM code looks for a group named "reim" so it is imperative that the group be named "reim".

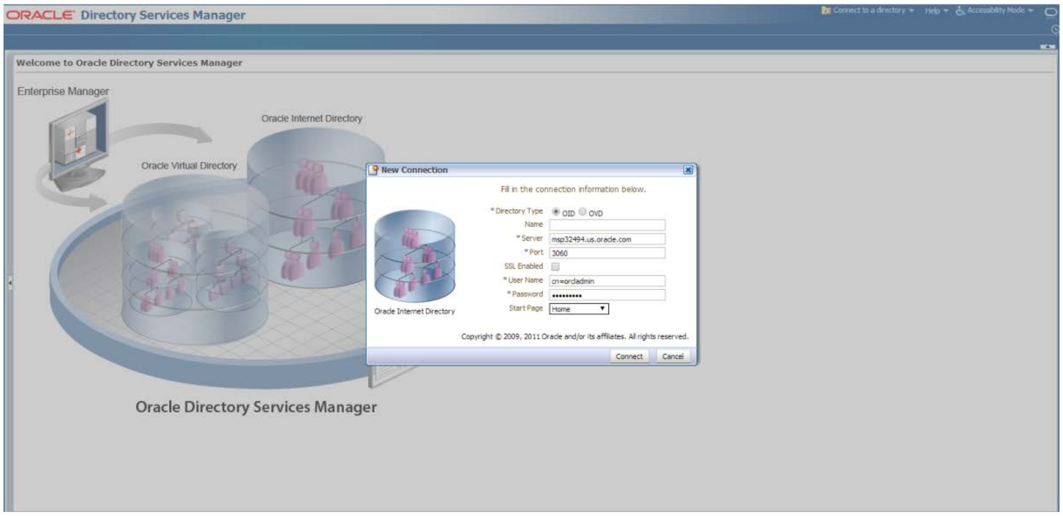
Example: Using OID 11.1.1.7, the steps to follow are:

a. Open your OID connection by launching odsm (Oracle Directory Services Manager). A screen similar to the following is displayed.

b. Click Connect to a directory and select your OID directory.


Directory Manager
ORACLE Directory Services Manager
Connect to a directory
Help
Accessibility Mode
Welcome to Oracle Directory Services Manager
Enterprise Manager
Oracle Internet Directory
Oracle Virtual Directory
Browser
Oracle Directory Services Manager
OID - cn=rpm.admin,cn=users,dc=us,dc=oracle,dc=com@redevlv0081:3060
OID - qa 3
OID - 132qa3
OID - cn=allocator,cn=users,dc=us,dc=oracle,dc=com@msp28015.us.oracle.com:3060
OID - cn=orcladmin@mspdev80.us.oracle.com:389
OID - cn=allocator,cn=users,dc=us,dc=oracle,dc=com@redevlv0081:3060
OID - cn=orcladmin@mspdv188.us.oracle.com:389
OID - 13.1.8
OID - F QA3
OID - 13.2 qa1
OID - msp28015 dn-orcladmin
OID - document
OID - testing

c. From the OID Connect dialog, click the Connect button.


ORACLE Directory Services Manager
Connect to a directory ▾
Help ▾
Accessibility Mode ▾
Welcome to Oracle Directory Services Manager
Enterprise Manager
Oracle Internet Directory
Oracle Virtual Directory
New Connection
Oracle Internet Directory
Connect
Cancel
Oracle Directory Services Manager

Fill in the connection information below.

* Directory Type ● OID ○ OVD

Name

* Server msp32494.us.oracle.com

* Port 3060

SSL Enabled □

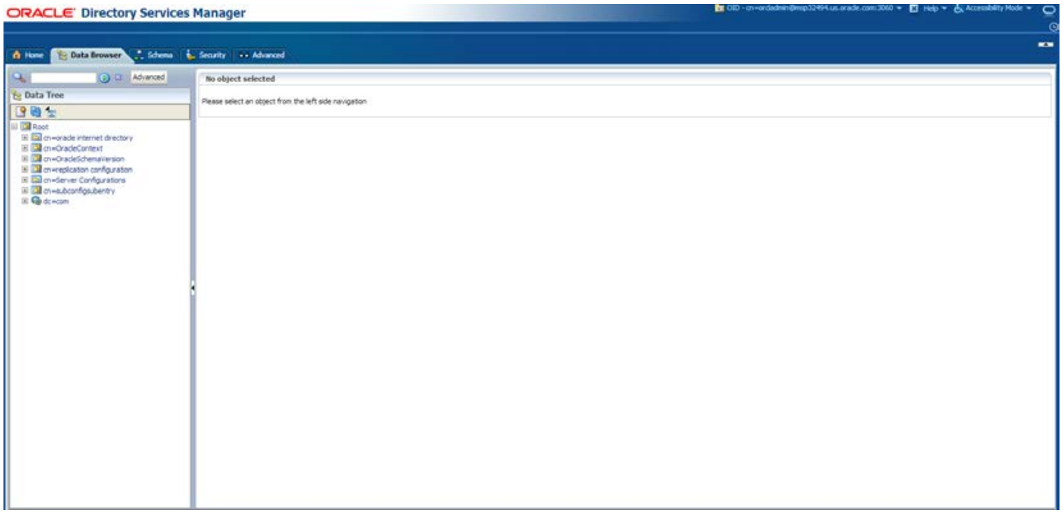
* User Name cn=orcladmin

* Password ••••••••••

Start Page Home ▾

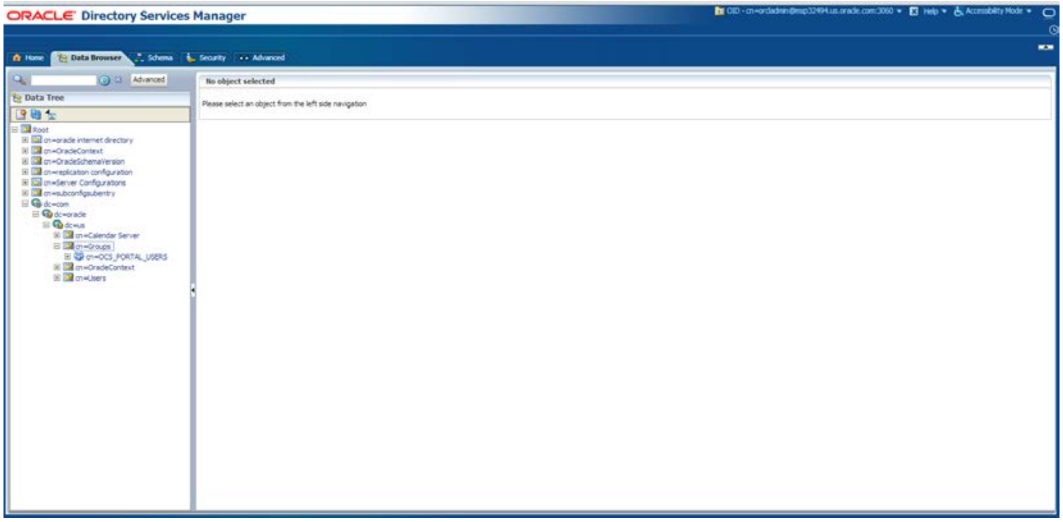
Copyright © 2009, 2011 Oracle and/or its affiliates. All rights reserved.

d. From the Oracle Internet Directory Welcome Screen, select the Data Browser tab. The DataBrowser tree shows how to find the "cn=Group" element



Please select an object from the left side navigation

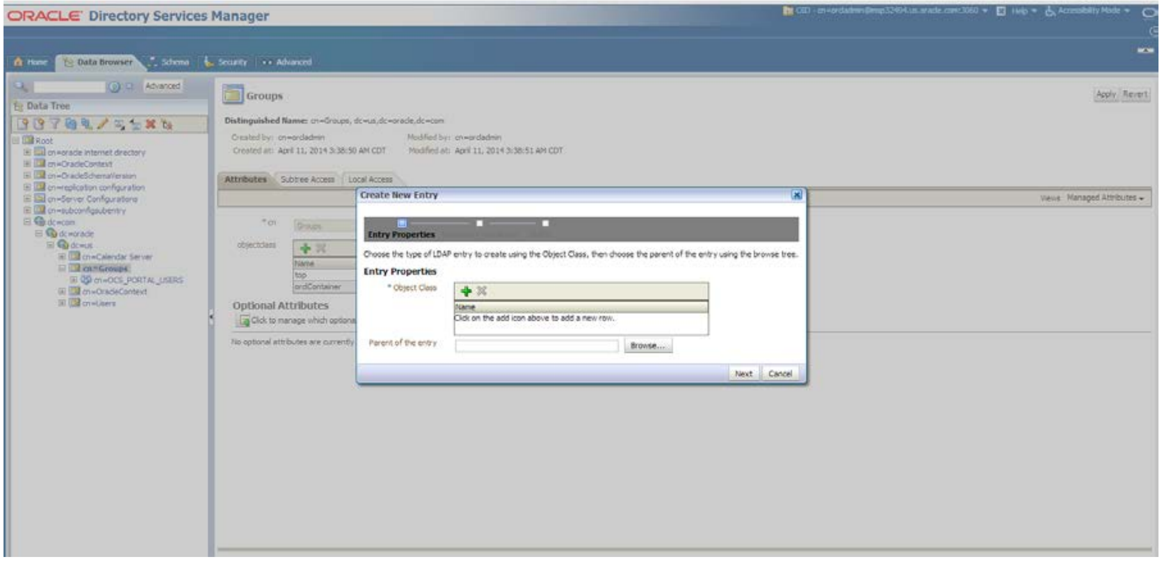
e. From the Data Tree panel of the ODSM screen, navigate to dc=com,dc=oracle,dc=us,cn=Groups.



No object selected

Please select an object from the left side navigation

f. Right-click cn=Groups and select Create.



Groups

Distinguished Name: cn=Groups, dc=us,dc=oracle,dc=com

Created by: cn=orcladmin   Modified by: cn=orcladmin

Created at: April 11, 2014 3:38:50 AM CDT   Modified at: April 11, 2014 3:38:51 AM CDT

Create New Entry

Entry Properties

Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

Entry Properties

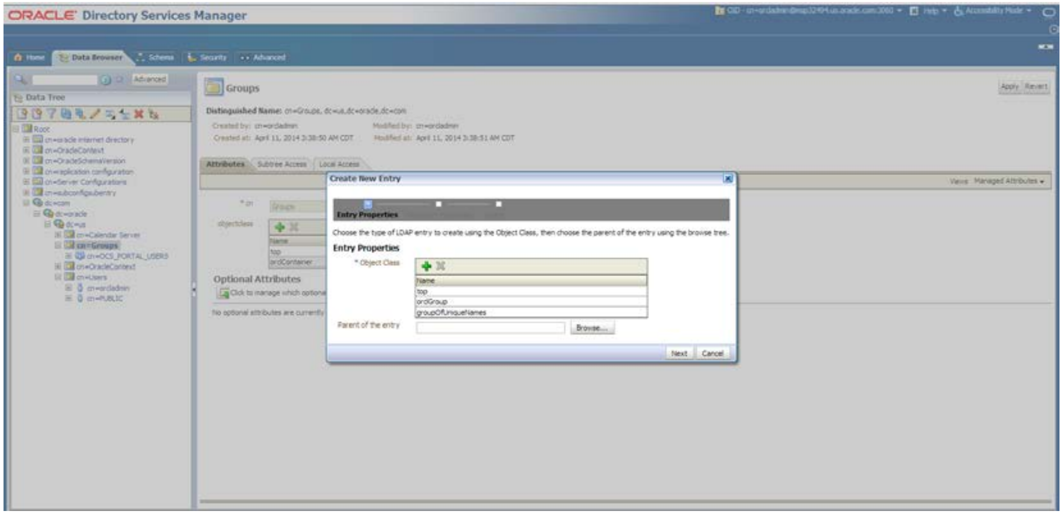
* Object Class

Name

Click on the add icon above to add a new row.

Parent of the entry

- **g.** From the Create New Entry dialog, click the + icon to see the Object Classes in the dropdown menu.
- **h.** From the Add Object Class drop down menu select the below object classes:
  - top
  - orclGroup
  - groupOfUniqueNames



Distinguished Name: cn=Groups, dc=us,dc=oracle,dc=com

Create New Entry

Entry Properties

Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

Entry Properties

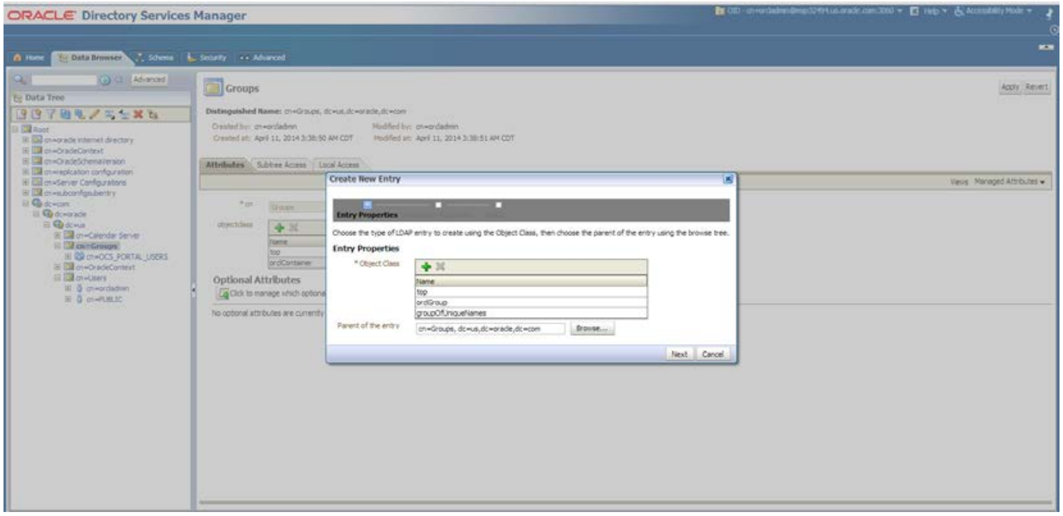
* Object Class

Name
top
orclGroup
groupOfUniqueNames

Parent of the entry:

Browse... Next Cancel

- **i.** On the Field Parent of the Entry field enter: cn=Groups, dc=us,dc=oracle,dc=com.



Distinguished Name: cn=Groups, dc=us,dc=oracle,dc=com

Modified by: cn=orcladmin

Modified at: April 11, 2014 3:38:51 AM CDT

Create New Entry

Entry Properties

Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

Entry Properties

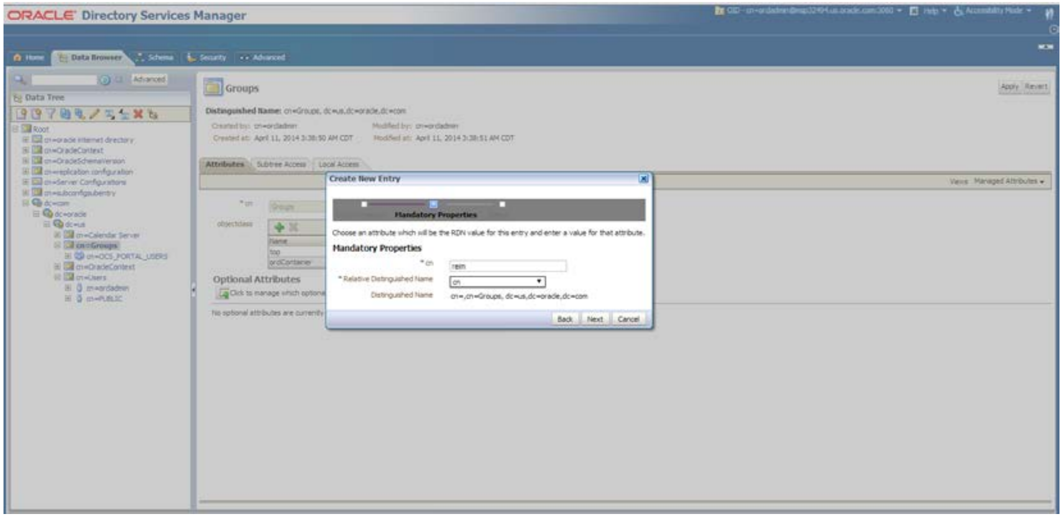
* Object Class

Name
top
orclGroup
groupOfUniqueNames

Parent of the entry: cn=Groups, dc=us,dc=oracle,dc=com

Browse... Next Cancel

- **j.** Click Next.
- **k.** On the "*cn" text field enter: "reim". On Resolved Distinguished Name field enter: cn



Distinguished Name: cn=Groups, dc=us,dc=oracle,dc=com

Modified by: cn=orcladmin

Modified at: April 11, 2014 3:38:51 AM CDT

Choose an attribute which will be the RDN value for this entry and enter a value for that attribute.

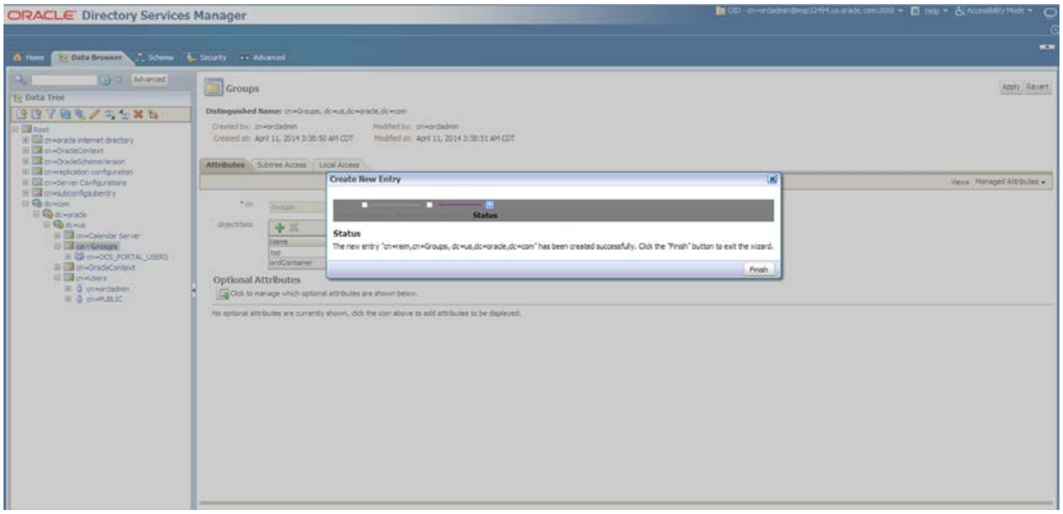
Mandatory Properties

* cn: reim

* Relative Distinguished Name: cn

Distinguished Name: cn=,cn=Groups, dc=us,dc=oracle,dc=com

l. Click Next.



Distinguished Name: cn=Groups, dc=us,dc=oracle,dc=com

Modified by: cn=orcladmin

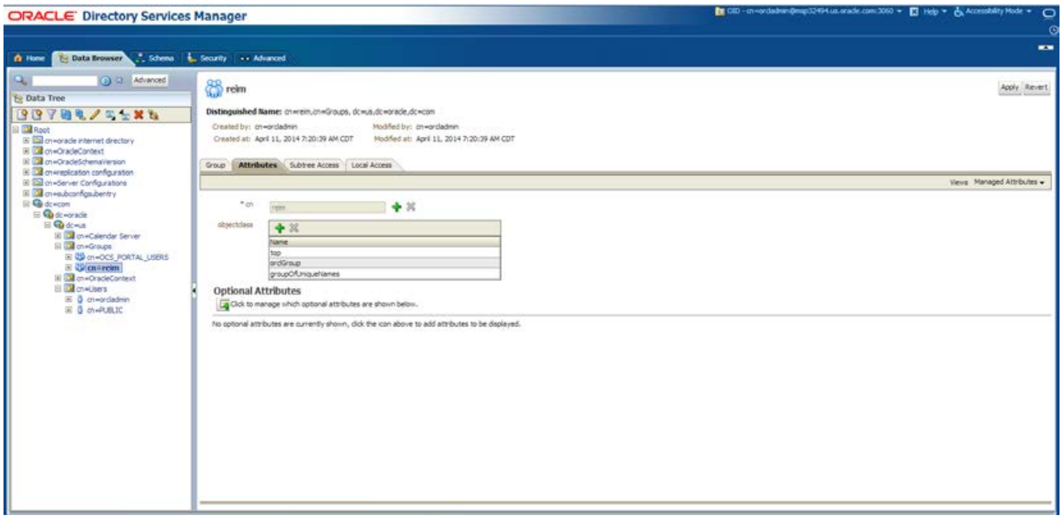
Modified at: April 11, 2014 3:38:51 AM CDT

Status

The new entry "cn=reim,cn=Groups, dc=us,dc=oracle,dc=com" has been created successfully. Click the "Finish" button to exit the wizard.

m. Click Finish.

After applying the changes, your screen should look like this:



Root
cn=oracle internet directory
cn=OracleContext
cn=OracleSchemaVersion
cn=replication configuration
cn=Server Configurations
cn=subconfigsubentry
dc=com
dc=oracle
dc=us
cn=Calendar Server
cn=Groups
cn=OCS_PORTAL_USERS
cn=reim
cn=OracleContext
cn=Users
cn=orcladmin
cn=PUBLIC

reim

Distinguished Name: cn=reim,cn=Groups, dc=us,dc=oracle,dc=com

Created by: cn=orcladmin
Modified by: cn=orcladmin
Created at: April 11, 2014 7:20:39 AM CDT
Modified at: April 11, 2014 7:20:39 AM CDT

* cn: reim

objectclass:

Name
top
orclGroup
groupOfUniqueNames

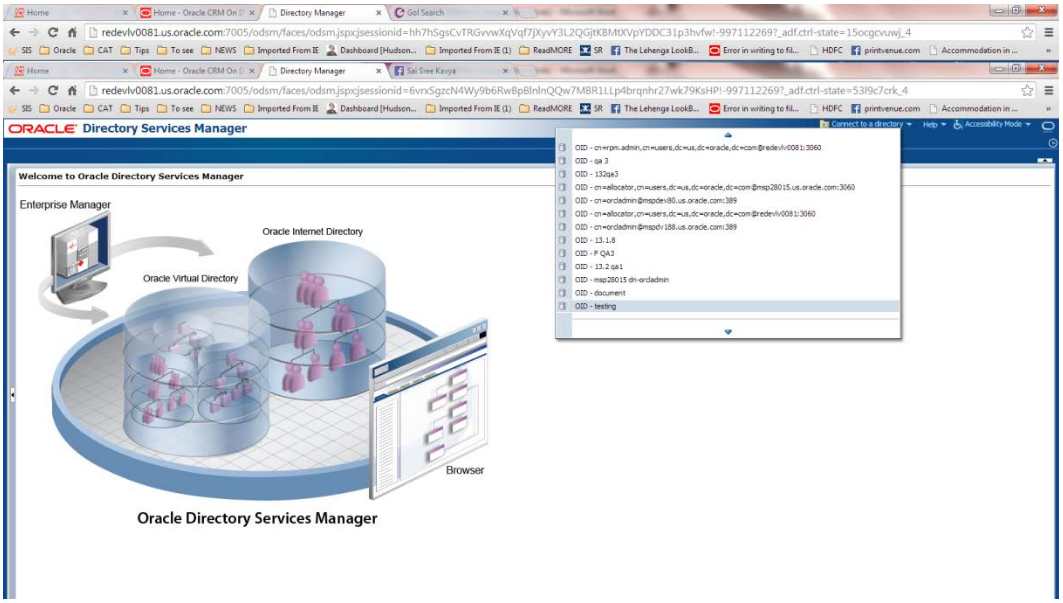
No optional attributes are currently shown, click the icon above to add attributes to be displayed.

3. Create an LDAP connection user with the necessary rights to do sub-tree searches on your users and groups respectively. This user can be named anything but “REIM.ADMIN” is used in this document. This same user should be given as an input for ‘Search User DN’ on the ‘LDAP Directory Server Details’ screen while installing the ReIM application. This is the user which ReIM uses to login to LDAP and perform the necessary search in the LDAP.

   Follow the below steps to create the ‘example:REIM.ADMIN’ user.

   a. Open your OID connection by launching odsm (Oracle Directory Services Manager).

   b. Click Connect to a directory and select your OID directory.

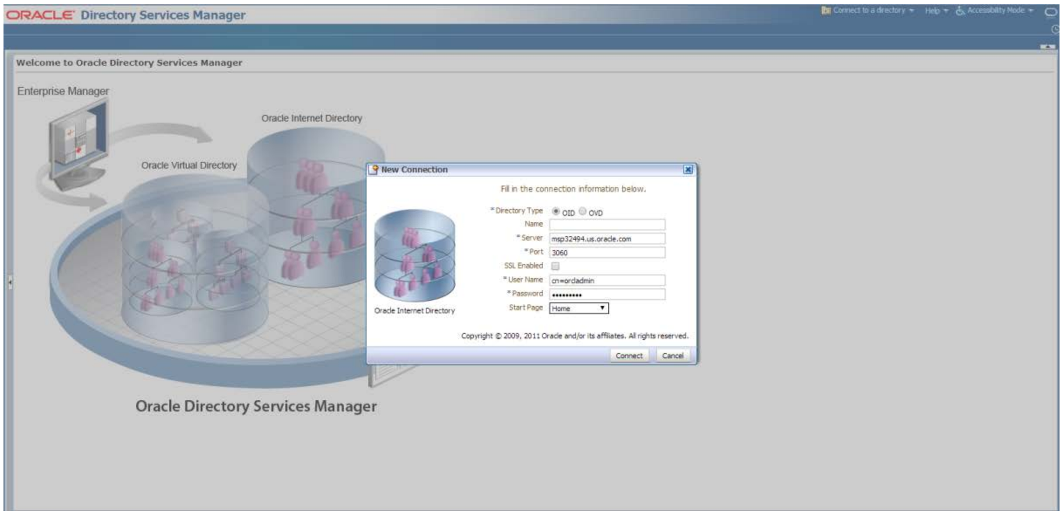


redevlv0081.us.oracle.com:7005/odsm/faces/odsm.jspx;jsessionid=hh7hSgsCvTRGvvwXqVqf7jXyvY3L2QGjtKBMtXVpYDDC31p3hvfw!-997112269?_adf.ctrl-state=15ocgcvuwj_4

redevlv0081.us.oracle.com:7005/odsm/faces/odsm.jspx;jsessionid=6vrxSgzcN4Wy9b6RwBp8lnlnQQw7MBR1LLp4brqnhr27wk79KsHP!-997112269?_adf.ctrl-state=53l9c7crk_4

OID - cn=rpm.admin,cn=users,dc=us,dc=oracle,dc=com@redevlv0081:3060
OID - qa 3
OID - 132qa3
OID - cn=allocator,cn=users,dc=us,dc=oracle,dc=com@msp28015.us.oracle.com:3060
OID - cn=orcladmin@mspdev80.us.oracle.com:389
OID - cn=allocator,cn=users,dc=us,dc=oracle,dc=com@redevlv0081:3060
OID - cn=orcladmin@mspdv188.us.oracle.com:389
OID - 13.1.8
OID - F QA3
OID - 13.2 qa1
OID - msp28015 dn-orcladmin
OID - document
OID - testing

c. From the OID Connect dialog, click the **Connect** button.


ORACLE Directory Services Manager
Connect to a directory
Help
Accessibility Mode
Welcome to Oracle Directory Services Manager
Enterprise Manager
Oracle Internet Directory
Oracle Virtual Directory
Oracle Directory Services Manager
New Connection
Oracle Internet Directory
Connect
Cancel

New Connection

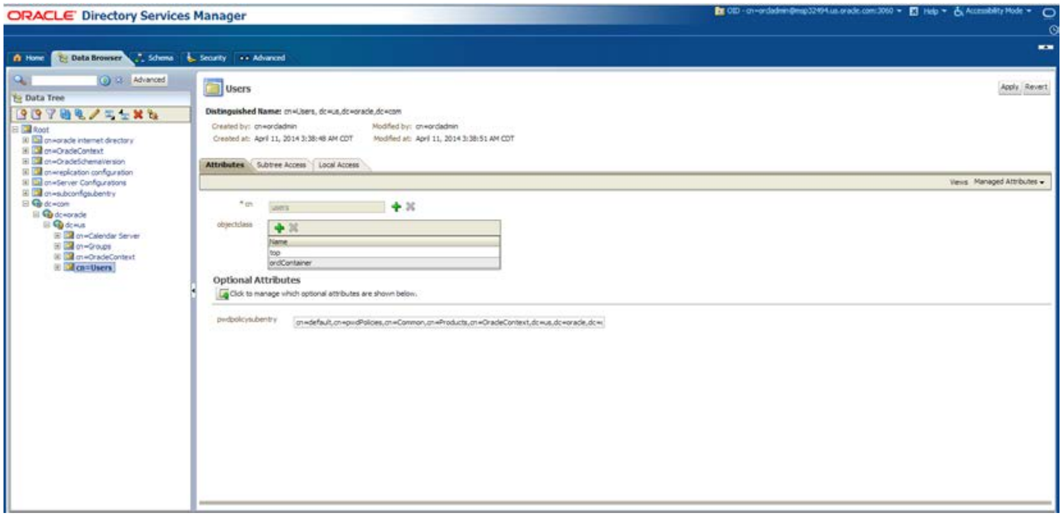
Fill in the connection information below.

- *Directory Type ● OID ○ OVD
- Name
- *Server msp32494.us.oracle.com
- *Port 3060
- SSL Enabled □
- *User Name cn=orcladmin
- *Password ••••••••••
- Start Page Home

Copyright © 2009, 2011 Oracle and/or its affiliates. All rights reserved.

d. From the Oracle Internet Directory Welcome Screen, select the Data Browser tab.

The Data Browser tree shows how to find the “cn=Users” element. From the Data Tree panel of the ODSM screen, navigate to the Users branch.



Data Tree

- Root
  - cn=oracle internet directory
  - cn=OracleContext
  - cn=OracleSchemaVersion
  - cn=replication configuration
  - cn=Server Configurations
  - cn=subconfigsubentry
  - dc=com
    - dc=oracle
      - dc=us
        - cn=Calendar Server
        - cn=Groups
        - cn=OracleContext
        - cn=Users

Users

Distinguished Name: cn=Users, dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by: cn=orcladmin

Created at: April 11, 2014 3:38:48 AM CDT Modified at: April 11, 2014 3:38:51 AM CDT

*cn users

objectclass

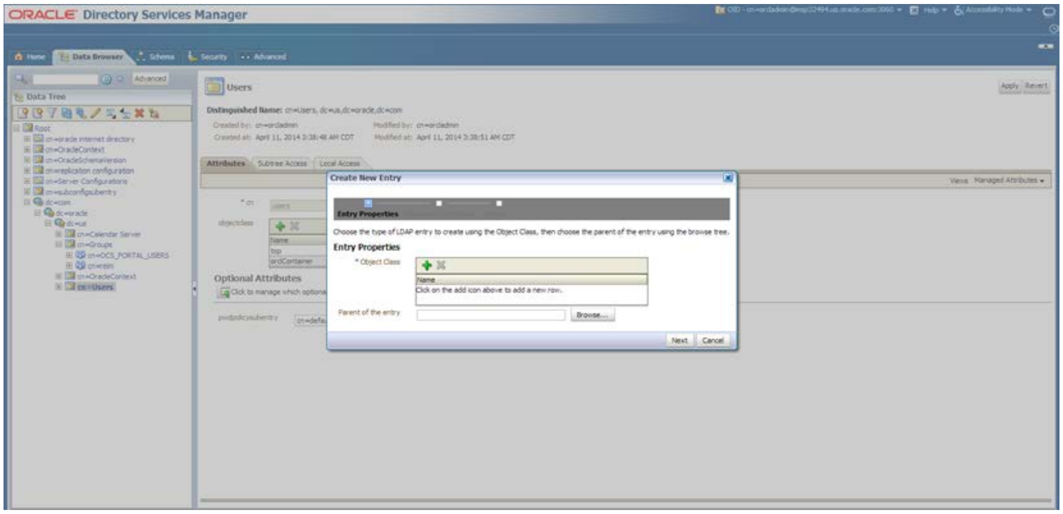
Name
top
orclContainer

Optional Attributes

Click to manage which optional attributes are shown below.

pwdpolicysubentry cn=default,cn=pwdPolicies,cn=Common,cn=Products,cn=OracleContext,dc=us,dc=oracle,dc=

e. On the Users screen, press right mouse button. With cn=Users highlighted, select **Create** from the drop down menu panel.



Distinguished Name: cn=Users, dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by: cn=orcladmin

Created at: April 11, 2014 3:38:48 AM CDT Modified at: April 11, 2014 3:38:51 AM CDT

Create New Entry

Entry Properties

Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

Entry Properties

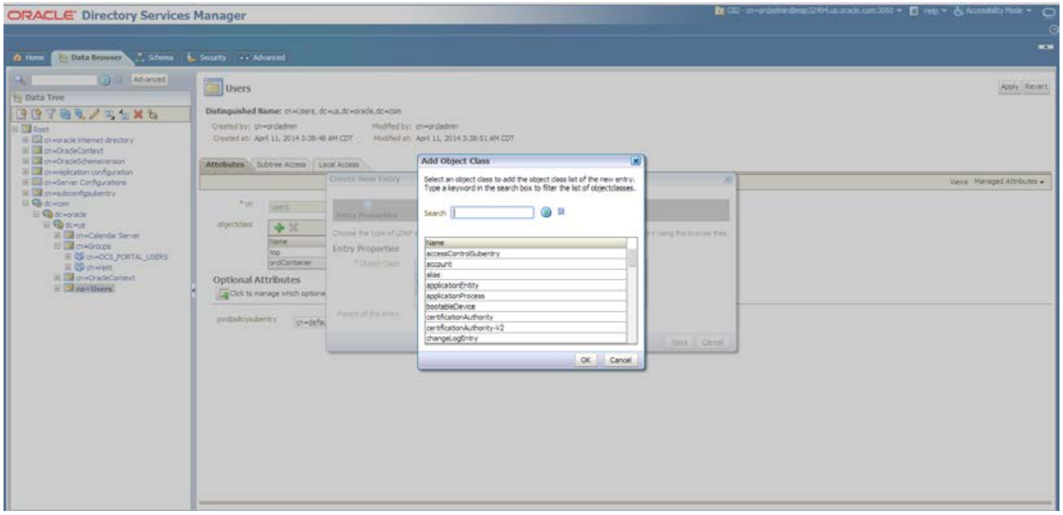
* Object Class

Name
Click on the add icon above to add a new row.

Parent of the entry [Browse...]

[Next] [Cancel]

f. In the Object Class field, click the + icon.



Add Object Class

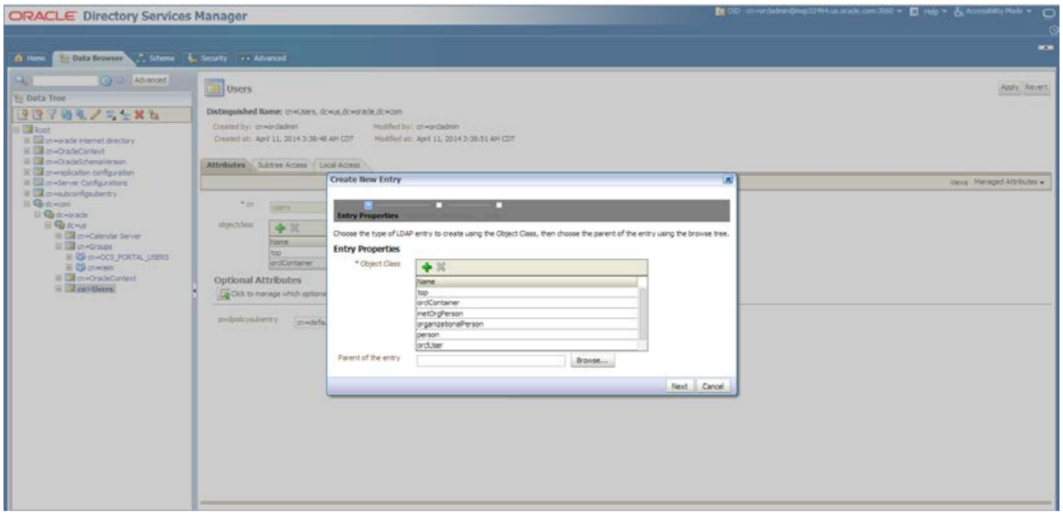
Select an object class to add the object class list of the new entry. Type a keyword in the search box to filter the list of objectclasses.

Search

Name
accessControlSubentry
account
alias
applicationEntity
applicationProcess
bootableDevice
certificationAuthority
certificationAuthority-V2
changeLogEntry

g. From the Add Object Class menu, select the below object classes:

- top
- orclContainer
- organizationalperson
- orcluser
- person
- orcluserv2
- Inetorgperson



Create New Entry

Entry Properties

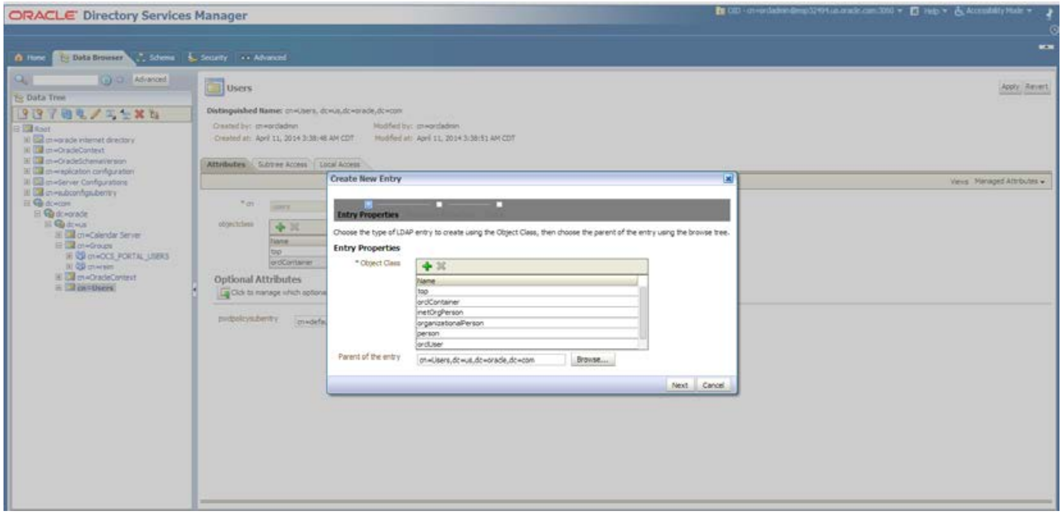
Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

Entry Properties

Name
top
orclContainer
inetOrgPerson
organizationalPerson
person
orclUser

Parent of the entry

h. In the Parent of the Entry field enter the following: cn=Users,dc=us,dc=oracle,dc=com



Create New Entry

Entry Properties

Choose the type of LDAP entry to create using the Object Class, then choose the parent of the entry using the browse tree.

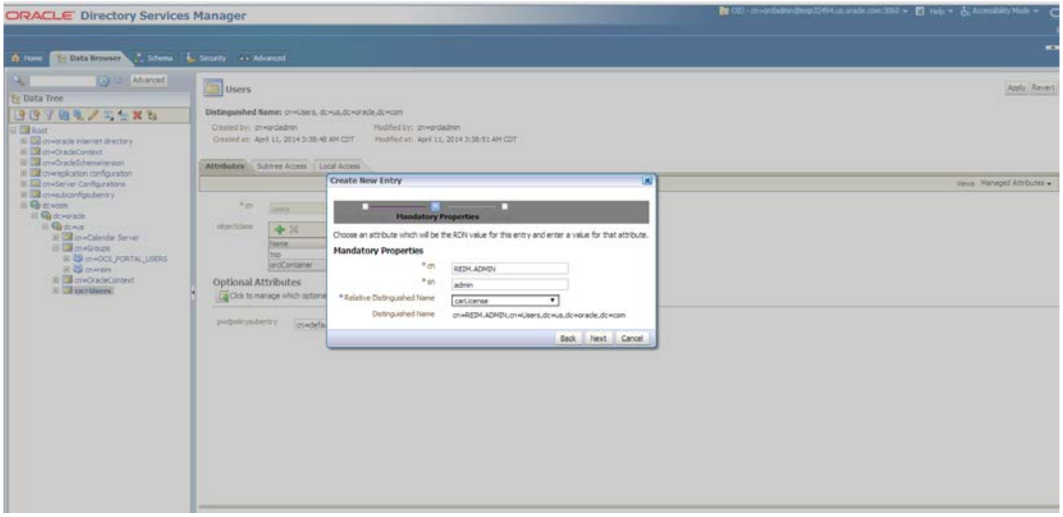
Entry Properties

Name
top
orclContainer
inetOrgPerson
organizationalPerson
person
orclUser

Parent of the entry: cn=Users,dc=us,dc=oracle,dc=com

i. Click **Next**. The Mandatory Properties dialog is displayed.

j. From Mandatory Properties dialog , On the “*cn” text field enter: “reim.admin”. On the “*sn” text field enter: “admin”. On Resolved Distinguished Name field enter: cn



Distinguished Name: cn=Users, dc=us,dc=oracle,dc=com

Modified by: cn=orcladmin

Modified at: April 11, 2014 3:38:51 AM CDT

Create New Entry

Mandatory Properties

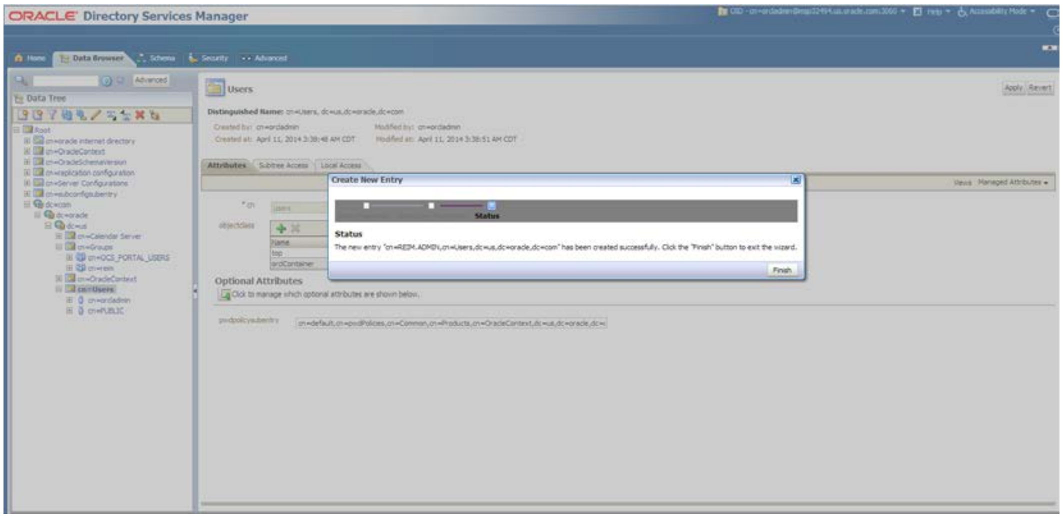
Choose an attribute which will be the RDN value for this entry and enter a value for that attribute.

Mandatory Properties

- * cn: REIM.ADMIN
- * sn: admin
- * Relative Distinguished Name: carLicense
- Distinguished Name: cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com

k. Click Next.

l. Make sure the information on screen is correct. Click **Finish** to create the REIM.ADMIN user.



Distinguished Name: cn=Users, dc=us,dc=oracle,dc=com

Modified by: cn=orcladmin

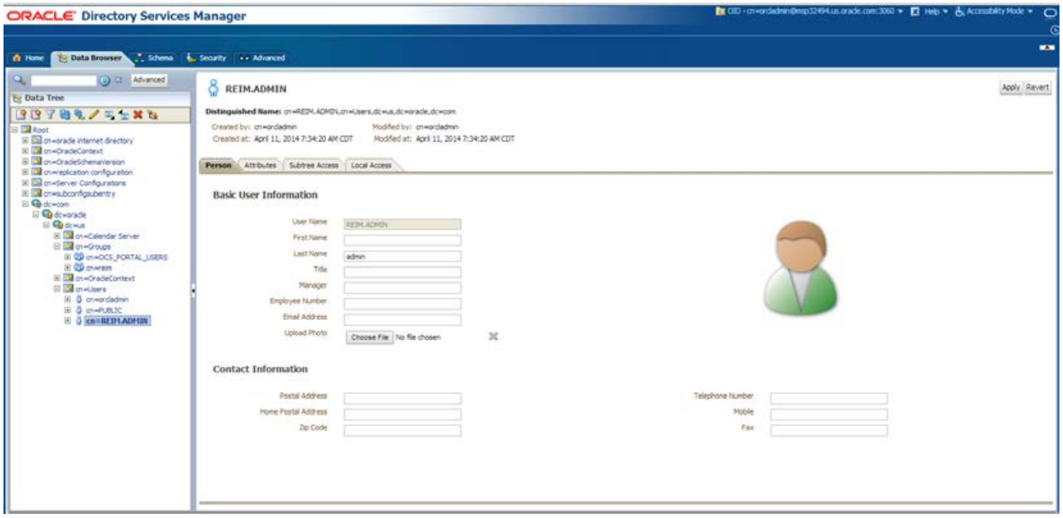
Modified at: April 11, 2014 3:38:51 AM CDT

Create New Entry

Status

The new entry "cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com" has been created successfully. Click the "Finish" button to exit the wizard.

When the “REIM.ADMIN” user is created a screen similar to the one below is displayed.



REIM.ADMIN

Distinguished Name: cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by: cn=orcladmin

Created at: April 11, 2014 7:34:20 AM CDT Modified at: April 11, 2014 7:34:20 AM CDT

Basic User Information

User Name: REIM.ADMIN

First Name:

Last Name: admin

Title:

Manager:

Employee Number:

Email Address:

Upload Photo:

Contact Information

Postal Address:

Home Postal Address:

Zip Code:

Telephone Number:

Mobile:

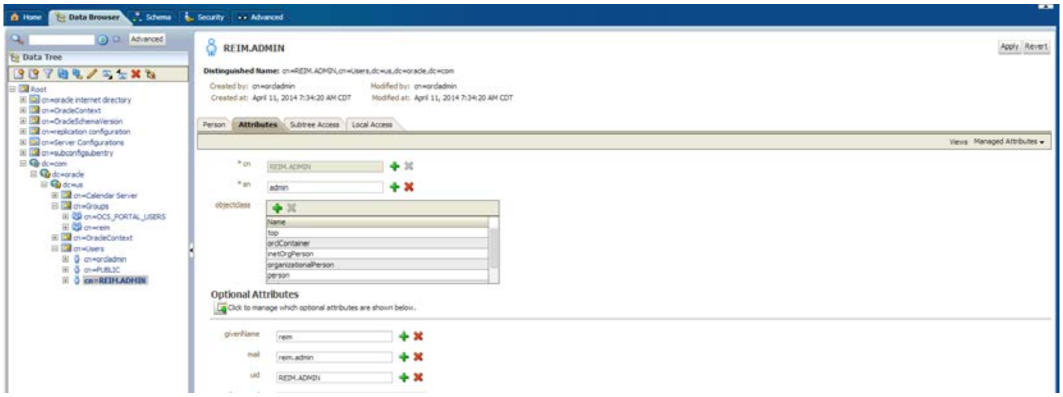
Fax:

m. Click the Person tab and enter the following Basic User Information:

- First Name: <reim>
- Last Name: <admin>
- Email Address: <reim.admin@mycompany.com>

n. Click the Attributes tab and enter the following information:

- Given Name: <reim>
- Mail: <reim.admin@mycompany.com>
- Uid: REIM.ADMIN
- User Password: <password>



REIM.ADMIN

Distinguished Name: cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by: cn=orcladmin

Created at: April 11, 2014 7:34:20 AM CDT Modified at: April 11, 2014 7:34:20 AM CDT

* cn: REIM.ADMIN

* sn: admin

objectclass:

Name
top
orclContainer
inetOrgPerson
organizationalPerson
person

Optional Attributes

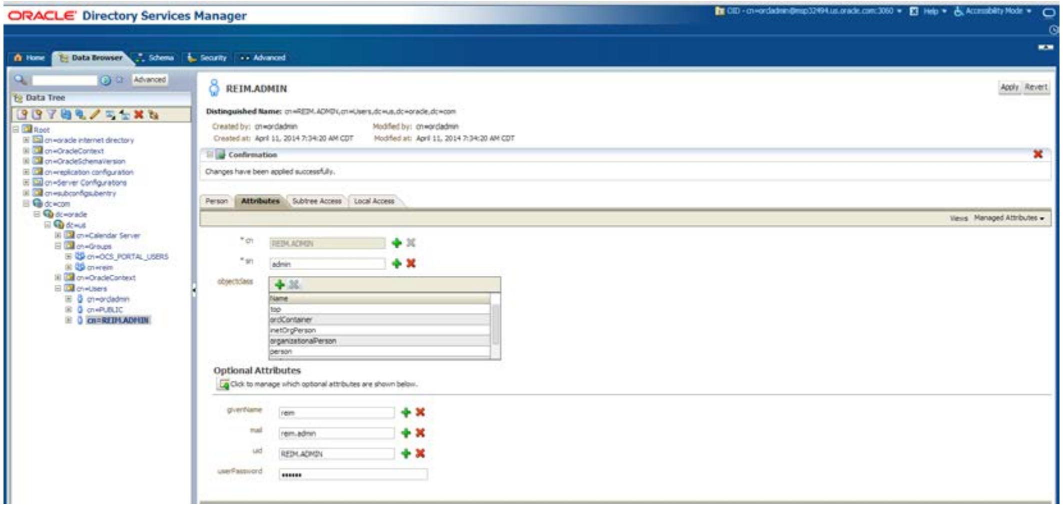
Click to manage which optional attributes are shown below.

givenName: reim

mail: reim.admin

uid: REIM.ADMIN

o. Click **Apply**. After applying the changes, your screen will look similar to the following:



REIM.ADMIN

Distinguished Name: cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by: cn=orcladmin

Created at: April 11, 2014 7:34:20 AM CDT Modified at: April 11, 2014 7:34:20 AM CDT

Confirmation

Changes have been applied successfully.

* cn: REIM.ADMIN

* sn: admin

objectclass:

Name
top
orclContainer
inetOrgPerson
organizationalPerson
person

Optional Attributes

Click to manage which optional attributes are shown below.

givenName: reim

mail: reim.admin

uid: REIM.ADMIN

userPassword: ••••••

4. Create the Application Admin user who will have access (Login) to ReIM.

I f you are installing other Merchandising applications you should have already created RETAIL.USER. If you do not have RETAIL.USER already created in LDAP, create "RETAIL.USER" following the same procedure described for creating the REIM.ADMIN user above or you may use the sample LDIF (RETAIL.USER) file provided at the end of this section to create the attributes and create the user.

a. The following attributes need to be included for the new user:

– Preferred Country: US

– Preferred Language: en

> **Note:** PreferredCountry and PreferredLanguage attributes should be defined using standard ISO codes for language and country.

If the attributes above are not available in LDAP then refer to Create the preferredCountry Attribute, Object Class and User for the details to create the "preferredCountry" attribute and the objectclass "retailUser".

There is a RETAIL.USER.ldif file which has been given as a template for creating the user.

b. The "RETAIL.USER" user should be created under the following container: dc=com,dc=oracle,dc=us,cn=Users

The DN name for "RETAIL.USER" should be:

cn=RETAIL.USER,cn=Users,dc=us,dc=oracle,dc=com

Note: It need not be named as only RETAIL.USER but we refer to RETAIL.USER in this document. Whatever username is chosen to login to the ReIM application, that user should possess the following mandatory attributes with the values added for the attributes in LDAP.

- -uid
- -givenname
- -sn
- -mail
- -userpassword
- -preferredLanguage
- -preferredcountry
- -cn

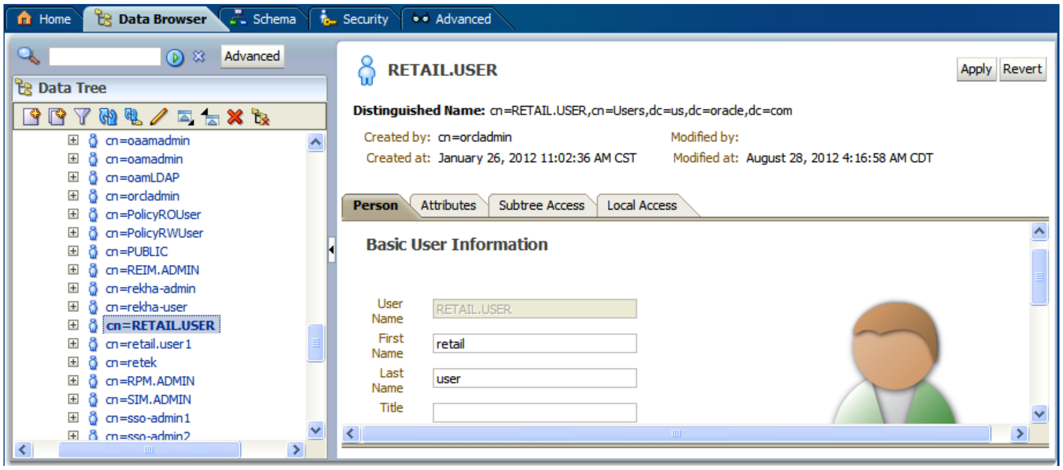
These are considered as the mandatory attributes for the login user (example:RETAIL.USER) which is listed in ldap.properties located on the ReIM server at <DOMAIN_HOME>/servers/<reim-server>/tmp/_WL_user/<reim>/<xstkfu>/reim14.war/WEB-INF/classes/com/retek/reim/ldap.properties

You can see the following list from ldap.properties:

– login_id_attribute_name=uid
– user_first_name_attribute_name=givenname
– user_last_name_attribute_name=sn
– user_email_attribute_name=mail
– user_password_attribute_name=userpassword
– user_language_attribute_name=preferredLanguage
– user_country_attribute_name=preferredcountry
– user_main_key=cn
– # Name of attributes in LDAP for enterprise roles
– role_member = uniqueMember
– role_application = cn

Note: Attributes for enterprise roles will get added as part of assigning users for the group “reim” created in LDAP which is explained further in this document.

In order the ReIM login to work, the above attributes must contain the values in the LDAP for the login user (Example: RETAIL.USER).



cn=oaamadmin
cn=oamadmin
cn=oamLDAP
cn=orcladmin
cn=PolicyROUser
cn=PolicyRWUser
cn=PUBLIC
cn=REIM.ADMIN
cn=rekha-admin
cn=rekha-user
cn=RETAIL.USER
cn=retail.user1
cn=retek
cn=RPM.ADMIN
cn=SIM.ADMIN
cn=sso-admin1
cn=sso-admin2

RETAIL.USER

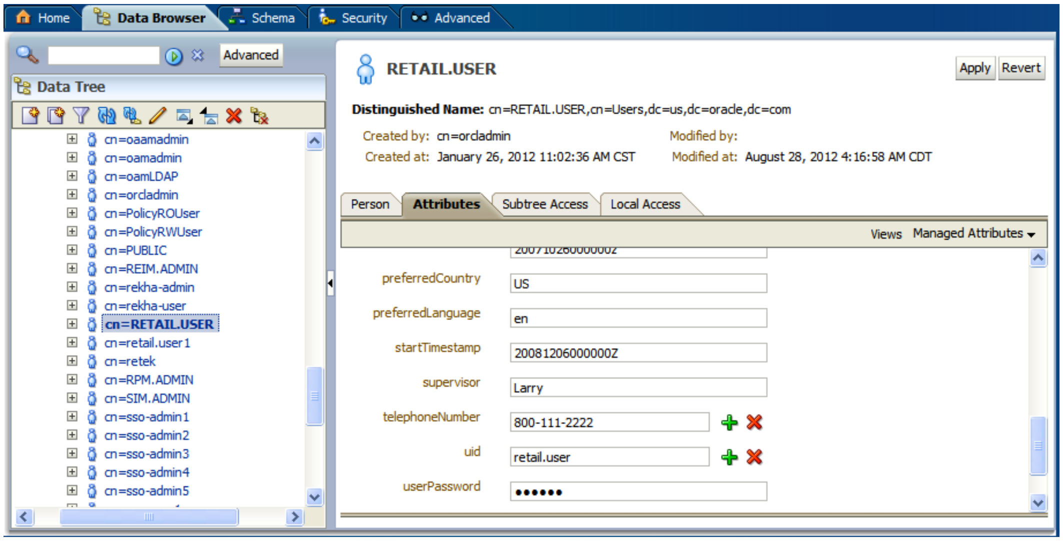
Distinguished Name: cn=RETAIL.USER,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by:
Created at: January 26, 2012 11:02:36 AM CST Modified at: August 28, 2012 4:16:58 AM CDT

Basic User Information

User Name: RETAIL.USER
First Name: retail
Last Name: user
Title:

c. Example value of Preferred Country is: <US> and Preferred Language is <en>. These values can be used if the country is US and language is English. If another locale is used, the value needs to be entered based on that locale.



cn=oaamadmin
cn=oamadmin
cn=oamLDAP
cn=orcladmin
cn=PolicyROUser
cn=PolicyRWUser
cn=PUBLIC
cn=REIM.ADMIN
cn=rekha-admin
cn=rekha-user
cn=RETAIL.USER
cn=retail.user1
cn=retek
cn=RPM.ADMIN
cn=SIM.ADMIN
cn=sso-admin1
cn=sso-admin2
cn=sso-admin3
cn=sso-admin4
cn=sso-admin5

RETAIL.USER

Distinguished Name: cn=RETAIL.USER,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin Modified by:
Created at: January 26, 2012 11:02:36 AM CST Modified at: August 28, 2012 4:16:58 AM CDT

preferredCountry	US
preferredLanguage	en
startTimestamp	20081206000000Z
supervisor	Larry
telephoneNumber	800-111-2222
uid	retail.user
userPassword	••••••

d. Record the password you entered, so that you know it all the time.

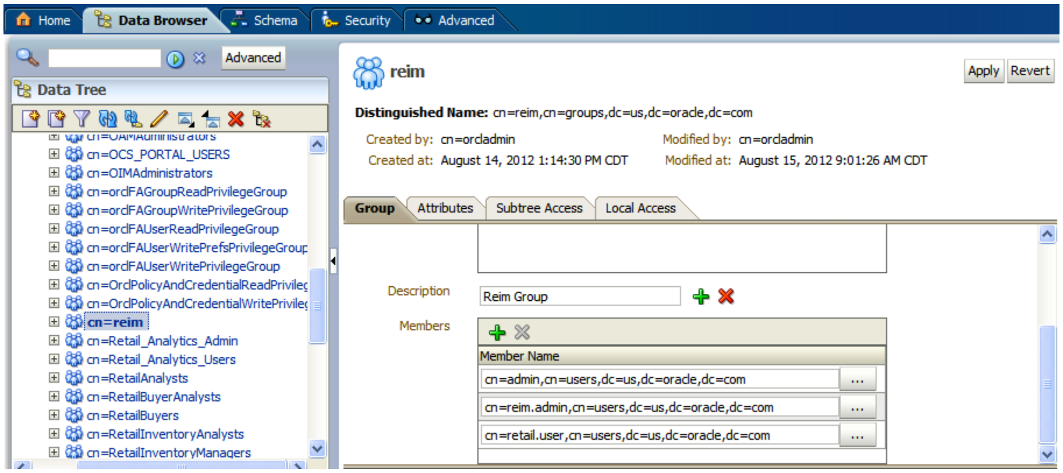
5. Assign the user "RETAIL.USER" and any other users which need to login to ReIM Application to the "reim" group

a. On the "reim" Group screen, on the Group tab, scroll down the right panel until you find the Members section

b. On the Members section insert:

cn=RETAIL.USER,cn=users,dc=us,dc=oracle,dc=com

After applying the changes, the screen should look similar to the following:



cn=OAMAdministrators
cn=OCS_PORTAL_USERS
cn=OIMAdministrators
cn=orclFAGroupReadPrivilegeGroup
cn=orclFAGroupWritePrivilegeGroup
cn=orclFAUserReadPrivilegeGroup
cn=orclFAUserWritePrefsPrivilegeGroup
cn=orclFAUserWritePrivilegeGroup
cn=OrclPolicyAndCredentialReadPrivileg
cn=OrclPolicyAndCredentialWritePrivileg
cn=reim
cn=Retail_Analytics_Admin
cn=Retail_Analytics_Users
cn=RetailAnalysts
cn=RetailBuyerAnalysts
cn=RetailBuyers
cn=RetailInventoryAnalysts
cn=RetailInventoryManagers

reim

Distinguished Name: cn=reim,cn=groups,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin
Created at: August 14, 2012 1:14:30 PM CDT
Modified by: cn=orcladmin
Modified at: August 15, 2012 9:01:26 AM CDT

Description: Reim Group

Members

Member Name
cn=admin,cn=users,dc=us,dc=oracle,dc=com
cn=reim.admin,cn=users,dc=us,dc=oracle,dc=com
cn=retail.user,cn=users,dc=us,dc=oracle,dc=com

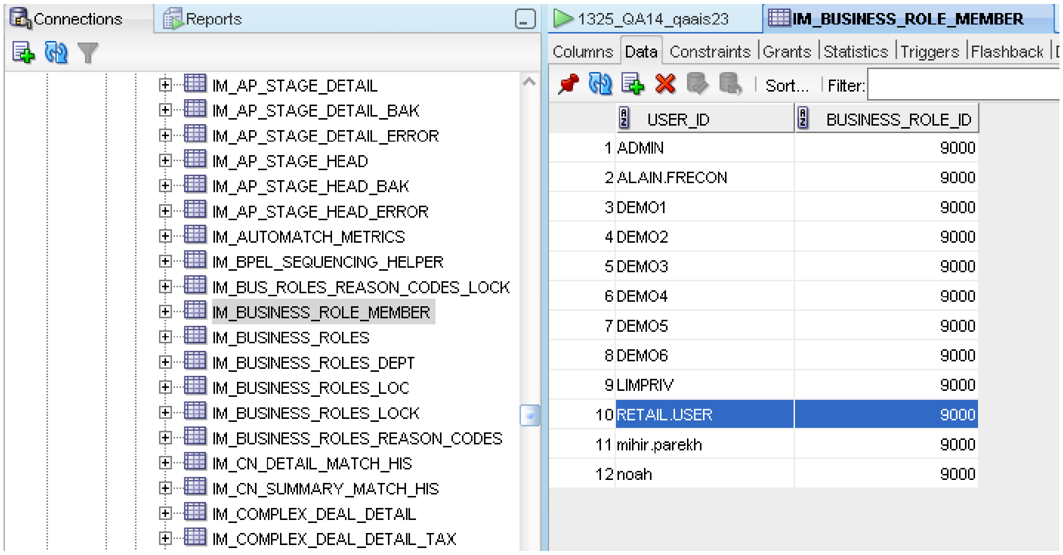
c. Click **Apply** to save your changes.

6. Add new user (Example:RETAIL.USER) to the database if not already there.

   a. Insert the new user (example: RETAIL.USER) into the im_business_role_member database table by entering the following SQL command:

```
insert into im_business_role_member
(USER_ID, BUSINESS_ROLE_ID)
values (‘RETAIL.USER’, 1);
```

> **Note:** The above business role ID=1 value should be mapped with IM_BUSINESS_ROLES database table for that particular user (Example: RETAIL.USER).
>
> It may vary based on the mapping in IM_BUSINESS_ROLES database table for the user you are inserting the record.



IM_AP_STAGE_DETAIL
IM_AP_STAGE_DETAIL_BAK
IM_AP_STAGE_DETAIL_ERROR
IM_AP_STAGE_HEAD
IM_AP_STAGE_HEAD_BAK
IM_AP_STAGE_HEAD_ERROR
IM_AUTOMATCH_METRICS
IM_BPEL_SEQUENCING_HELPER
IM_BUS_ROLES_REASON_CODES_LOCK
IM_BUSINESS_ROLE_MEMBER
IM_BUSINESS_ROLES
IM_BUSINESS_ROLES_DEPT
IM_BUSINESS_ROLES_LOC
IM_BUSINESS_ROLES_LOCK
IM_BUSINESS_ROLES_REASON_CODES
IM_CN_DETAIL_MATCH_HIS
IM_CN_SUMMARY_MATCH_HIS
IM_COMPLEX_DEAL_DETAIL
IM_COMPLEX_DEAL_DETAIL_TAX

	USER_ID	BUSINESS_ROLE_ID
1	ADMIN	9000
2	ALAIN.FRECON	9000
3	DEMO1	9000
4	DEMO2	9000
5	DEMO3	9000
6	DEMO4	9000
7	DEMO5	9000
8	DEMO6	9000
9	LIMPRIV	9000
10	RETAIL.USER	9000
11	mihir.parekh	9000
12	noah	9000

You are now ready to Login to ReIM after product installation.

Create the preferredCountry Attribute, Object Class and User

- The “preferredCountry” and “preferredLanguage” LDAP attributes, must be included in the users created in LDAP for ReIM login.
- The “preferredCountry” LDAP attribute is created as part of the other MOM products that use LDAP authentication.
- The “preferredLanguage” LDAP attribute will be available as part of other object classes (example: inetorgperson) which can be imported to the user to include this attribute for the user. If you do not have the attribute “preferredCountry” in your LDAP installation, it must be created.
- The sample retailuserobjectclass.ldif below creates the attribute “preferredCountry”and the object class “retailuser” and assign the attribute to the new object class “retailuser”.

Use the sample RETAIL.USER.ldif to create the user “RETAIL.USER” in LDAP. This ldif contains the new object class created along with the necessary object classes which will assign the mandatory attributes to the user.

You need to edit these scripts to match your LDAP installation. The object identifier numbers you see in the script follow the standards of a local Oracle installation. The object identifier numbers will be different from those listed in the sample script based on your install. They must be unique among all the other object classes and attributes. The sample ldif scripts should only be used as a template purpose. You are responsible for modifying it according to your LDAP needs. Perform the following steps to run the sample ldif scripts:

1. Copy sample retailuserobjectclass.ldif and RETAIL.USER.ldif scripts (below this section of instructions) to a temp directory in your system.
2. Edit the sample retailuserobjectclass.ldif and RETAIL.USER.ldif scripts to match your LDAP tree structure.
3. Edit the object identifier numbers for the object class and attributes (they must be unique among all the other object classes and attributes).
4. In the temp directory in which you copied the sample ldif scripts, export the environments variables that match your environment:

   Example:

   ```
   export ORACLE_HOME=/u00/webadmin/product/10.3.X_OID/OID/Oracle_IDM1/bin
   (replace with your OID server name)
   export oid_host=redevlv0081.us.oracle (replace with your host)
   export oid_port=3060 (replace with your OID port number)
   export oid_pwd=password for oid administrator, in this case orcladmin
   ```

5. Run the following LDAP commands to run the LDIF files in the LDAP:

   ```
   $ORACLE_HOME/bin/ldapadd -o <retailuserobjectclass_error.ldif> -v -c -h
   $oid_host -p $oid_port -w $oid_pwd -D cn=orcladmin -f
   retailuserobjectclass.ldif

   $ORACLE_HOME/bin/ldapadd -o <retailuser_error.ldif> -v -c -h $oid_host -p
   $oid_port -w $oid_pwd -D cn=orcladmin -f RETAIL.USER.ldif
   ```

Note: retailuserobjectclass.ldif must be run before running RETAIL.USER.ldif.

If you already have RETAIL.USER, then you will need to only run retailuserobjectclass.ldif and import the "retailuser" object class in the user 'RETAIL.USER'.

Sample script retailuserobjectclass.ldif

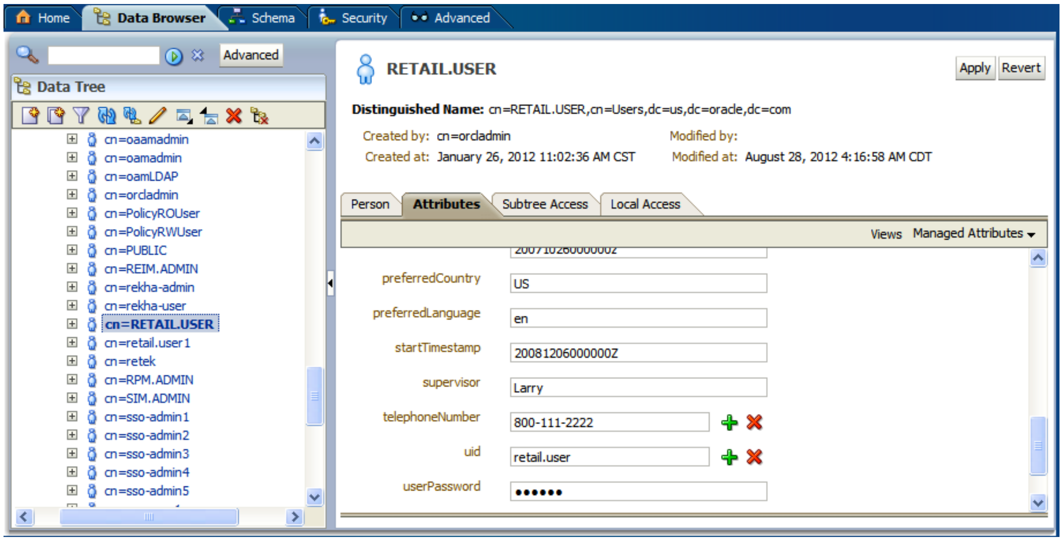
```
# Oracle Retail - ReIM User LDAP Schema
# You WILL need to make some changes to this based upon your #environment and
user you want to add
#
# This schema uses the OID tree starting with:
#       1.3.6.1.4.1.12388.897
# Where 1.3.6.1.4.1.12388 identifies definitions as
# belonging to the private enterprise MyCompany (12388),
# and the 897 identifies the ReIM application.
#
#-----------------------------------------
#-----------------------------------------
# Common Atrributes
#-----------------------------------------
#-----------------------------------------
#
#
dn: cn=subschemasubentry
changetype: modify
add: attributetypes
attributetypes: (1.3.6.1.4.1.11380.97.7.14
  NAME 'preferredCountry' DESC 'REIM User preferred country ISO code'  )

dn: cn=subschemasubentry
changetype: modify
add: objectclasses
objectclasses: (1.3.6.1.4.1.1.11380.97.11
  NAME 'retailuser' DESC 'Oracle Retail Users for MOM' STRUCTURAL
  sup ( top )
  MUST ( sn $ cn )
  MAY ( uid $ userPassword $ preferredCountry) )
```

Sample LDIF script for creating user RETAIL.USER - RETAIL.USER.LDIF

```
# start new entry for user RETAIL.USER
dn: cn=RETAIL.USER,cn=Users,dc=us,dc=oracle,dc=com
changetype: add
objectclass: top
objectclass: organizationalperson
objectclass: orcluser
objectclass: person
objectclass: retailuser
objectclass: orcluserv2
objectclass: inetorgperson
orclactivestartdate: 20121126000000z
givenname: RETAIL
sn: USER
cn: RETAIL.USER
uid: RETAIL.USER
userpassword: <password>
```

```
mail: retail.user@company.domain
preferredCountry: US -> This will change based on the country.
preferredLanguage: en -> This will change based on the locale.
description: Reim Login User
#done
```

The screen below displays the results of the ldif script. The preferredCountry and preferredLanguage are included in the LDAP RETAIL.USER user.



cn=oaamadmin
cn=oamadmin
cn=oamLDAP
cn=orcladmin
cn=PolicyROUser
cn=PolicyRWUser
cn=PUBLIC
cn=REIM.ADMIN
cn=rekha-admin
cn=rekha-user
cn=RETAIL.USER
cn=retail.user1
cn=retek
cn=RPM.ADMIN
cn=SIM.ADMIN
cn=sso-admin1
cn=sso-admin2
cn=sso-admin3
cn=sso-admin4
cn=sso-admin5

RETAIL.USER

Distinguished Name: cn=RETAIL.USER,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin
Created at: January 26, 2012 11:02:36 AM CST
Modified by:
Modified at: August 28, 2012 4:16:58 AM CDT

preferredCountry: US
preferredLanguage: en
startTimestamp: 20081206000000Z
supervisor: Larry
telephoneNumber: 800-111-2222
uid: retail.user
userPassword: ••••••

Run the ReIM Application Installer

When the managed server is configured and started, you can run the ReIM application installer. This installer configures and deploys the ReIM application.

> **Note:** See Appendix: ReIM Application Installer Screens for details on every screen and field in the application installer.

> **Note:** It is recommended that the installer be run as the same UNIX account which owns the application server ORACLE_HOME files.

1. Change directories to INSTALL_DIR/reim/application.
2. Set the ORACLE_HOME and JAVA_HOME environment variables. ORACLE_HOME should point to your WebLogic 11g installation. JAVA_HOME should point to the Java 7.0 (1.7.0) JDK.
3. Set the WEBLOGIC_DOMAIN_HOME environment variable to point to the domain that ReIM will be installed to (for example, /u00/webadmin/product/10.3.6/WLS/user_projects/domains/REIMDomain).
4. 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.
5. Run the install.sh script. This launches the installer. After installation is completed, a detailed installation log file is created (reim14install.<timestamp>.log).

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: Installer Silent Mode in this document for instructions on silent mode.

See Appendix: Common Installation Errors in this document for a list of common installation errors.

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

Clustered Installations– Post-Installation Steps

If you are installing the ReIM application to a clustered WebLogic 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 ReIM installer is referred to as the *master server*. All other nodes are referred to as the *remote server*.

1. The ReIM batch files should be copied from the master server to each of the remote servers under the same path as on the master server. You should take the $WEBLOGIC_DOMAIN_HOME/retail/context root/batch directory and copy it onto the remote servers under the same path.
2. The Oracle Retail Installation creates some security files on $WEBLOGIC_DOMAIN_HOME/retail/context root/config directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.
3. The Oracle Retail Installation creates some properties files on $WEBLOGIC_DOMAIN_HOME/retail/context root/ properties directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node

Backups Created by Installer

The ReIM application installer backs up a previous batch script installation by renaming it from reim-batch to reim-batch.<timestamp>. This is done to prevent the removal of any custom changes you might have. These backup directories can be safely removed without affecting the current installation.

Example: reim-batch.200803011726

Test the ReIM Application

After the application installer completes you should have a working ReIM application installation. To launch the application, open a web browser and go to http://hostname:(managed_server_port)/<context_root>/index.jsp.

If you have configured a WebTier to a front end ReIM application, use httpport instead of managed server port.

Example: http://appserver1:17009/reim01/index.jsp

reim.properties

The reim.properties file contains most of the settings for the ReIM application. Many properties in this file are set by the installer to get a working application up and running, but you may want to modify other settings in this file.

To modify settings in the properties file, you must redeploy the ReIM application. The properties values are stored in the templates/reim.properties file, which is in the directory where you expanded the ReIM installer files (for example, <INSTALL_DIR>/reim/application/templates/reim/properties, where <INSTALL_DIR> is the directory the application installer was unzipped).

Edit the reim.properties file to set the properties to the desired values. Then rerun the installer to deploy ReIM.

ReIM Batch Scripts

The ReIM application installer configures and installs the batch scripts under $ORACLE_HOME/user_projects/domains/<domain>/retail/<app-name>/batch.

Example:
/u00/webadmin/product/10.3.6/WLS/user_projects/domains/REIMDomain/retail/reim14

The batch scripts are copies of the same generic file. Their file names determine which functionality is run. To run batch scripts, use the alias name provided in the installer when ReIM is installed, the one that is written out to the Java wallet (for example, reim_batchpgmname ADMIN).

For the scripts to run correctly, values for the following variables must be provided:

- ORACLE_HOME: WebLogic Home directory where the ReIM application has been deployed.
- JAVA_HOME: Java 7.0 (1.7.0) JDK installation that typically is being used by the WebLogic Application Server.

Example: export
ORACLE_HOME=/u00/webadmin/product/10.3.6/WLS
export
JAVA_HOME=/u00/webadmin/product/10.3.6/jdk7
export PATH=$JAVA_HOME/bin:$PATH

Online Help

The application installer automatically installs Online Help to the proper location. It is accessible from the help links within the application.

Single Sign-On

Skip this section if ReIM is not used within an Oracle Single Sign-On environment.

> **Note:** This section assumes the Oracle WebLogic Server has already been registered with the Oracle Access Manager Webgates. See Oracle Access Manager Webgates documentation for details.

To set up single sign-on, complete the following steps.

1. If you are using Oracle Retail Invoice Matching in an Oracle Single Sign-On environment, then the Invoice Matching root context must be protected. Modify the following files

   - mod_wl_ohs.conf located in <WEBLOGIC_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1

   ```
   LoadModule weblogic_module
   "<WEBLOGIC_HOME>/Oracle_WT1/ohs/modules/mod_wl_ohs.so"
   <IfModule weblogic_module>:q!vi
         WebLogicHost host name
         WebLogicPort  admin port number
         MatchExpression *.jsp
   </IfModule>
   <Location /reim >
        SetHandler weblogic-handler
   </Location>
   ```

Adding New Users to ReIM – Manually (after ReIM has been installed)

When the ReIM installation has been completed you are able to Login to ReIM by using the Admin user (RETAIL.USER) created in the section: Configure LDAP Authentication Pre-Installation Steps (Initial Login to ReIM).

In order to have more users that are able to Login to ReIM, you need to create the new users by following these post-installation steps.

1. Create the new user who will have access to ReIM (ex: RETAIL.USER1)

   a. Create user “retail.user1” by going to dc=com,dc=oracle,dc=us,cn=Users and enter the following:

   ```
   cn=RETAIL.USER1.user,cn=Users,dc=us,dc=oracle,dc=com
   ```

   Record the password you entered, so that you know it all the time.

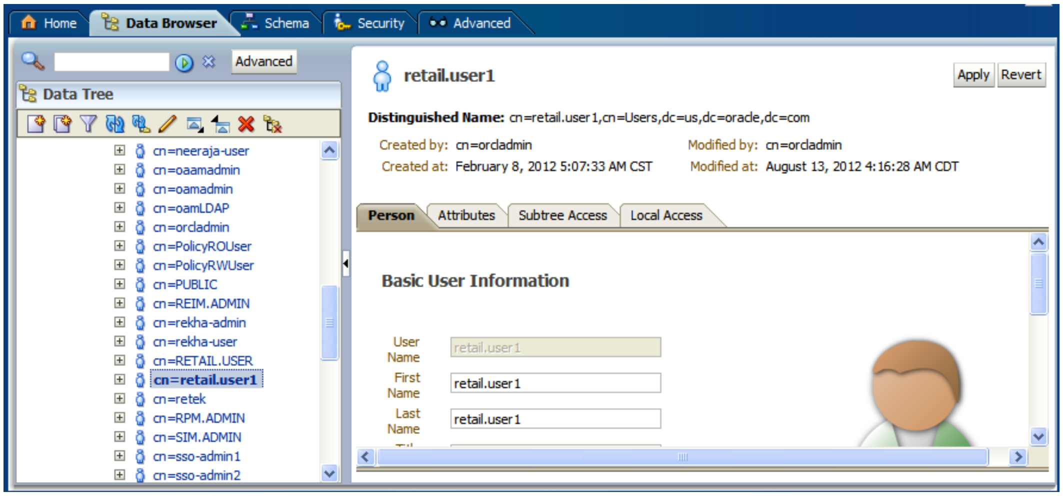
   b. The following additional attributes are needed to Login to ReIM:

   – Preferred Country: US

   – Preferred Language: en

   c. Click **Apply**.

   After applying the changes, your screen should look similar to the following:



cn=neeraja-user
cn=oaamadmin
cn=oamadmin
cn=oamLDAP
cn=orcladmin
cn=PolicyROUser
cn=PolicyRWUser
cn=PUBLIC
cn=REIM.ADMIN
cn=rekha-admin
cn=rekha-user
cn=RETAIL.USER
cn=retail.user1
cn=retek
cn=RPM.ADMIN
cn=SIM.ADMIN
cn=sso-admin1
cn=sso-admin2

retail.user1

Distinguished Name: cn=retail.user1,cn=Users,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin   Modified by: cn=orcladmin

Created at: February 8, 2012 5:07:33 AM CST   Modified at: August 13, 2012 4:16:28 AM CDT

Basic User Information

User Name: retail.user1

First Name: retail.user1

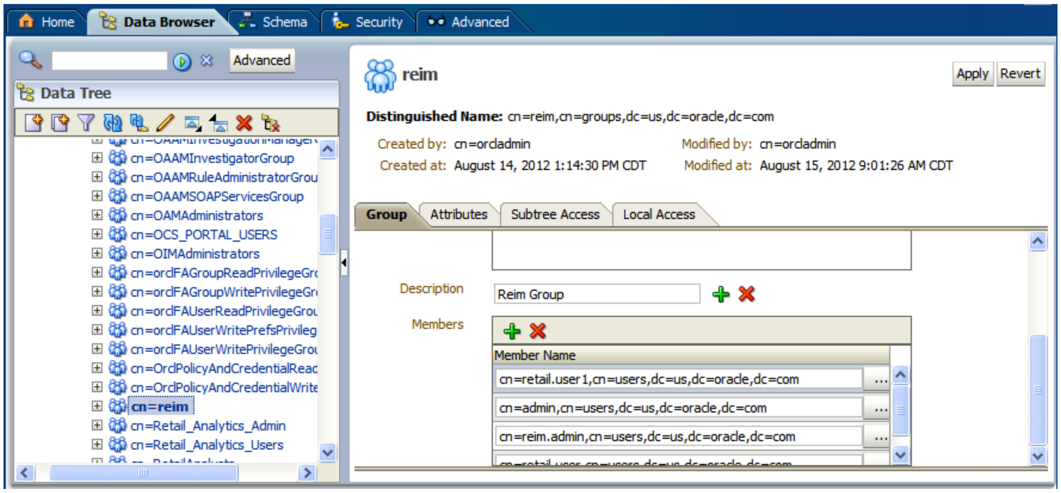
Last Name: retail.user1

2. Assign user “RETAIL.USER1” as member of “reim” Group

   a. Go to cn=reim,cn=groups,dc=us,dc=oracle,dc=com on the right of the screen. Locate the Members section and add the user:

      `cn=retail.user1,cn=users,dc=us,dc=oracle,dc=com`

      After applying the changes, your screen should look similar to the following:



cn=OAAMInvestigationManager
cn=OAAMInvestigatorGroup
cn=OAAMRuleAdministratorGrou
cn=OAAMSOAPServicesGroup
cn=OAMAdministrators
cn=OCS_PORTAL_USERS
cn=OIMAdministrators
cn=orclFAGroupReadPrivilegeGro
cn=orclFAGroupWritePrivilegeGr
cn=orclFAUserReadPrivilegeGrou
cn=orclFAUserWritePrefsPrivileg
cn=orclFAUserWritePrivilegeGrou
cn=OrclPolicyAndCredentialRead
cn=OrclPolicyAndCredentialWrite
cn=reim
cn=Retail_Analytics_Admin
cn=Retail_Analytics_Users
cn=RetailAnalysts

reim

Distinguished Name: cn=reim,cn=groups,dc=us,dc=oracle,dc=com

Created by: cn=orcladmin   Modified by: cn=orcladmin

Created at: August 14, 2012 1:14:30 PM CDT   Modified at: August 15, 2012 9:01:26 AM CDT

Description: Reim Group

Members:

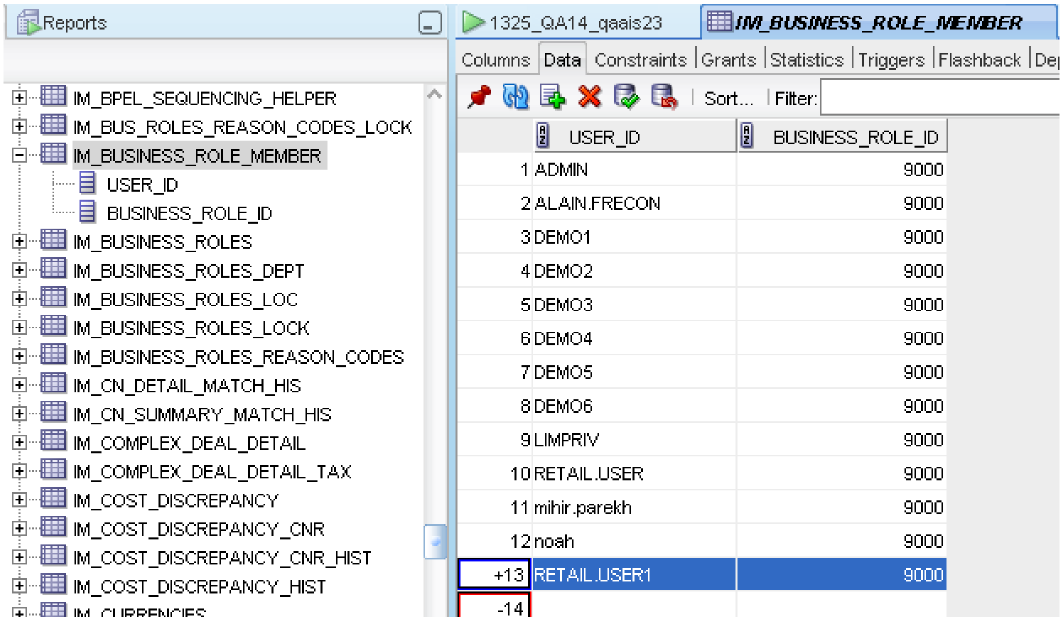
Member Name
cn=retail.user1,cn=users,dc=us,dc=oracle,dc=com
cn=admin,cn=users,dc=us,dc=oracle,dc=com
cn=reim.admin,cn=users,dc=us,dc=oracle,dc=com
cn=retail.user,cn=users,dc=us,dc=oracle,dc=com

3. Add the new user to the ReIM database table im_business_role_member.

   a. You add the new user and assign to the new user a ReIM role, by entering this SQL command:

```
insert into im_business_role_member
(USER_ID, BUSINESS_ROLE_ID)
values (‘RETAIL.USER1’, 9000);
```

After applying the changes, your screen should look similar to the following:



- IM_BPEL_SEQUENCING_HELPER
- IM_BUS_ROLES_REASON_CODES_LOCK
- IM_BUSINESS_ROLE_MEMBER
  - USER_ID
  - BUSINESS_ROLE_ID
- IM_BUSINESS_ROLES
- IM_BUSINESS_ROLES_DEPT
- IM_BUSINESS_ROLES_LOC
- IM_BUSINESS_ROLES_LOCK
- IM_BUSINESS_ROLES_REASON_CODES
- IM_CN_DETAIL_MATCH_HIS
- IM_CN_SUMMARY_MATCH_HIS
- IM_COMPLEX_DEAL_DETAIL
- IM_COMPLEX_DEAL_DETAIL_TAX
- IM_COST_DISCREPANCY
- IM_COST_DISCREPANCY_CNR
- IM_COST_DISCREPANCY_CNR_HIST
- IM_COST_DISCREPANCY_HIST
- IM_CURRENCIES

	USER_ID	BUSINESS_ROLE_ID
1	ADMIN	9000
2	ALAIN.FRECON	9000
3	DEMO1	9000
4	DEMO2	9000
5	DEMO3	9000
6	DEMO4	9000
7	DEMO5	9000
8	DEMO6	9000
9	LIMPRIV	9000
10	RETAIL.USER	9000
11	mihir.parekh	9000
12	noah	9000
+13	RETAIL.USER1	9000
-14		

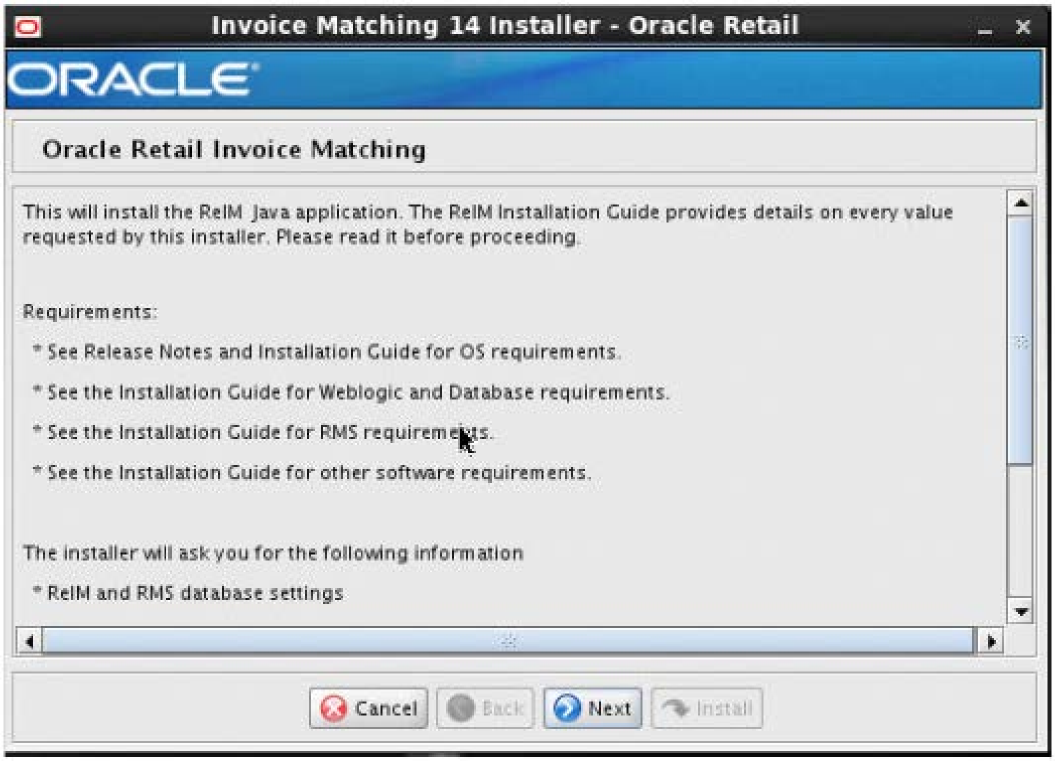
4. The new user "RETAIL.USER1" should be able to Login to ReIM now. Follow the same procedure for any additional users that need to have access to ReIM.

A

Appendix: ReIM Application Installer Screens

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

Screen: Startup


Invoice Matching 14 Installer - Oracle Retail
ORACLE
Oracle Retail Invoice Matching
Cancel
Back
Next
Install

This will install the ReIM Java application. The ReIM Installation Guide provides details on every value requested by this installer. Please read it before proceeding.

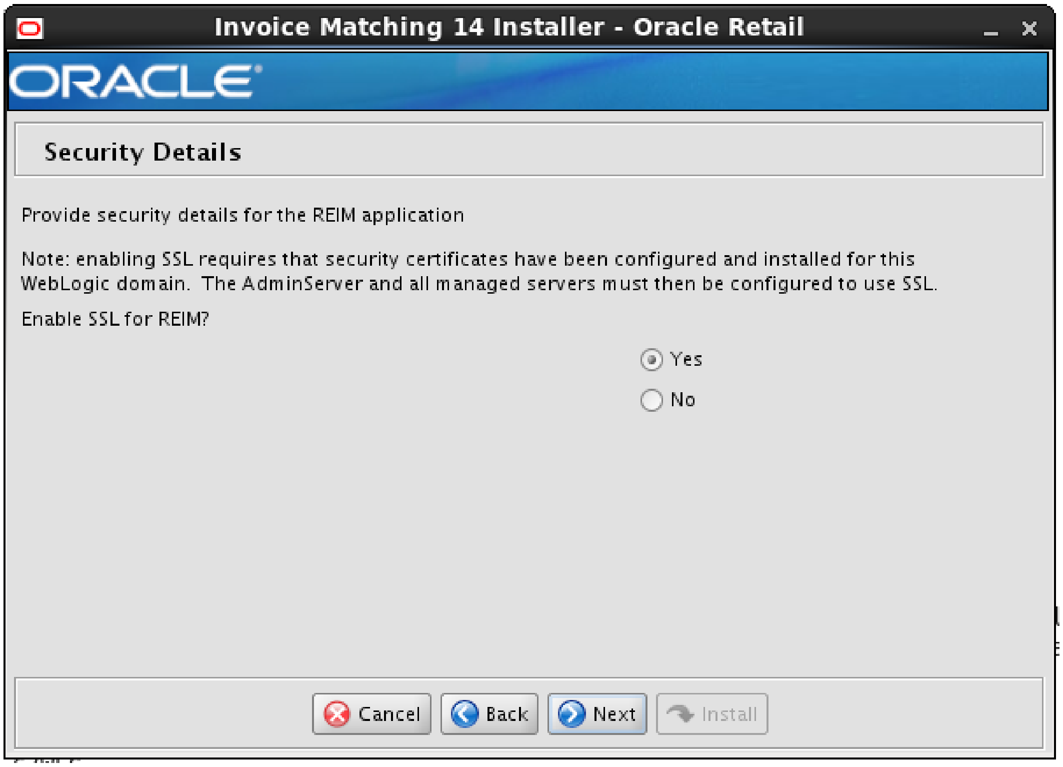
Requirements:

- * See Release Notes and Installation Guide for OS requirements.
- * See the Installation Guide for Weblogic and Database requirements.
- * See the Installation Guide for RMS requirements.
- * See the Installation Guide for other software requirements.

The installer will ask you for the following information

- * ReIM and RMS database settings

Screen: Security Details



Security Details

Provide security details for the REIM application

Note: enabling SSL requires that security certificates have been configured and installed for this WebLogic domain. The AdminServer and all managed servers must then be configured to use SSL.

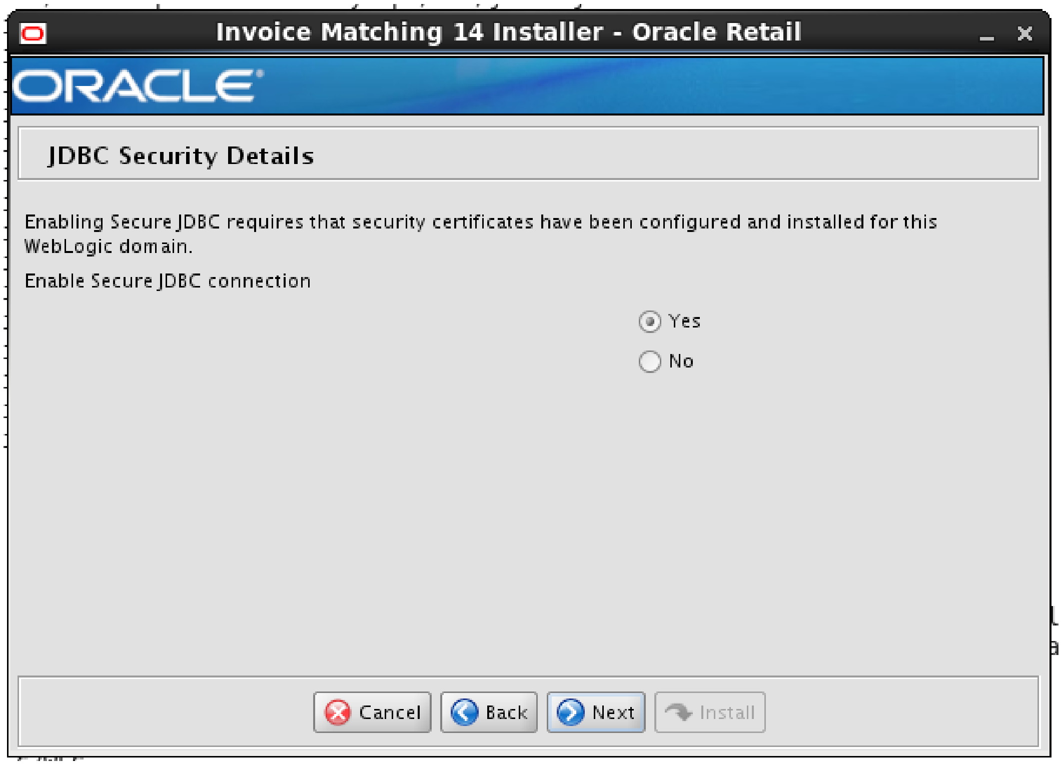
Enable SSL for REIM?

● Yes

○ No

Field Title	Enable SSL for REIM?
Field Description	Choosing Yes will deploy REIM using SSL and configure REIM to use SSL. In this case, SSL must be configured and the ports must be enabled for the AdminServer and REIM managed servers. Choosing No will deploy and configure REIM without SSL. In this case the SSL ports must be enabled for the AdminServer and for the REIM managed servers.

Screen: JDBC Security Details



JDBC Security Details

Enabling Secure JDBC requires that security certificates have been configured and installed for this WebLogic domain.

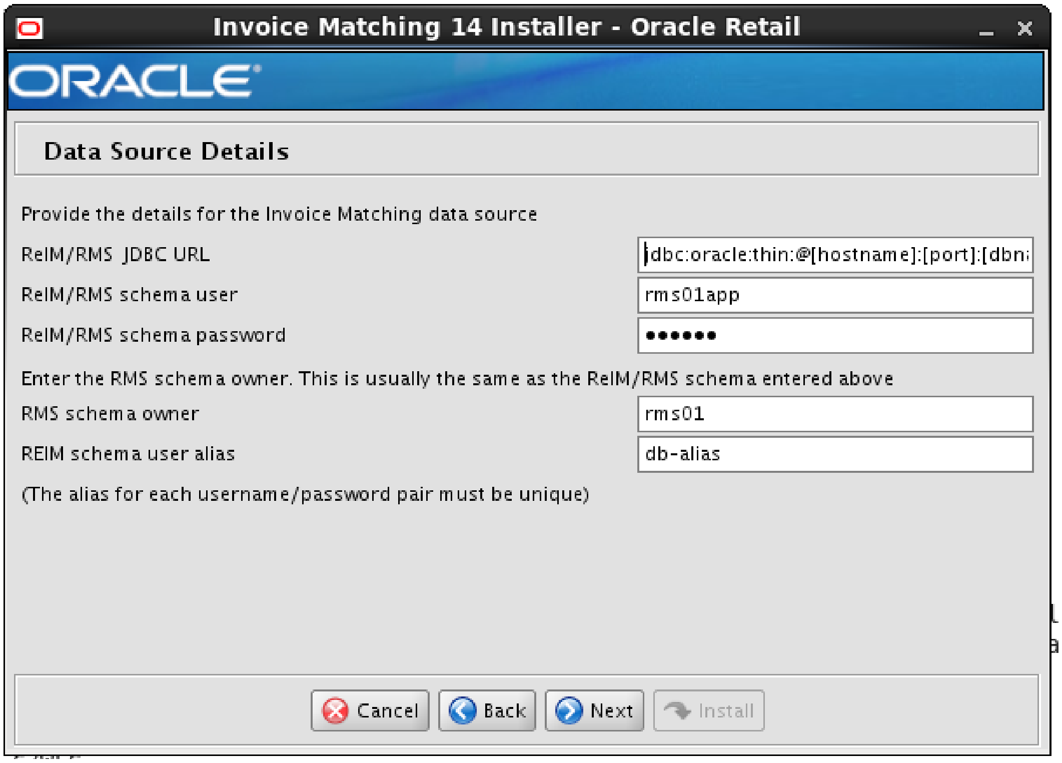
Enable Secure JDBC connection

● Yes

○ No

Field Title	Enable Secure JDBC for REIM?
Field Description	Choosing Yes will configure REIM with secure data connections; it requires keystore locations to be configured with REIM.

Screen: Data Source Details



Data Source Details

Provide the details for the Invoice Matching data source

ReIM/RMS JDBC URL: jdbc:oracle:thin:@[hostname]:[port]:[dbn

ReIM/RMS schema user: rms01app

ReIM/RMS schema password: ●●●●●●

Enter the RMS schema owner. This is usually the same as the ReIM/RMS schema entered above

RMS schema owner: rms01

REIM schema user alias: db-alias

(The alias for each username/password pair must be unique)

Field Title	ReIM/RMS JDBC URL
Field Description	URL used by the ReIM application to access the ReIM/RMS database schema. See Appendix: URL Reference for expected syntax.
Examples	jdbc:oracle:thin:@hostname:1521:dbname

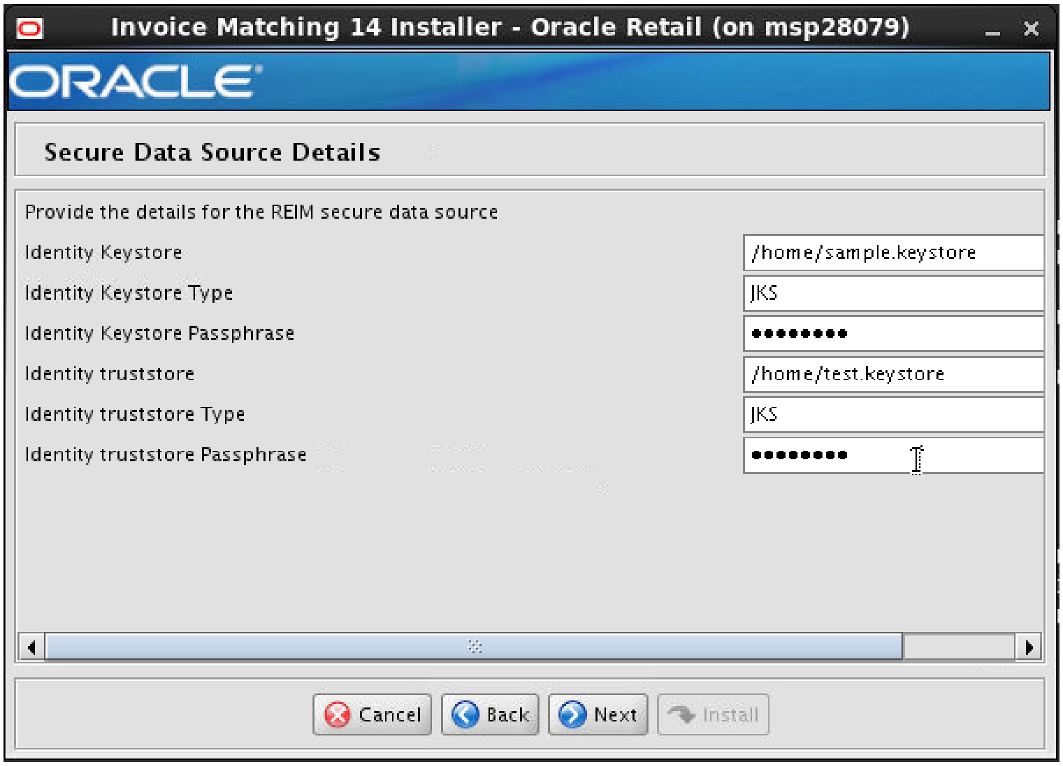
Field Title	ReIM/RMS schema user
Field Description	RMS database user for accessing the ReIM tables. This should match what was given in the **RMS schema** field of the RMS database installer.
Example	rms01app

Field Title	ReIM/RMS schema password
Field Description	Password for the JDBC username. This should match what was given in the **RMS schema password** field of the RMS database installer.

Field Title	RMS schema owner
Field Description	Database user which owns the RMS and ReIM tables. This usually has the same value as the **ReIM/RMS schema** field above.
Example	RMS01

Field Title	REIM schema user alias
Field Description	The alias of the ReIM user.
Example	db-alias
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Screen: Secure Data Source Details


Invoice Matching 14 Installer - Oracle Retail (on msp28079)
ORACLE
Secure Data Source Details
Cancel
Back
Next
Install

Provide the details for the REIM secure data source

Identity Keystore	/home/sample.keystore
Identity Keystore Type	JKS
Identity Keystore Passphrase	••••••••
Identity truststore	/home/test.keystore
Identity truststore Type	JKS
Identity truststore Passphrase	••••••••

Note: This screen appears only if you have enabled SSL for ReIM. Ignore this step in case you have not enabled SSL for ReIM.

Field Title	Identity Keystore
Field Description	Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). This screen lets you provide the keystore to be used for datasource connection These settings help you to manage the security of message transmissions. For further information, please refer *MOM security Guide.* Location or path where identity keystore file is stored.

Field Title	Identity Keystore Type
Field Description	Type of the identity keystore used. Exampe: jks

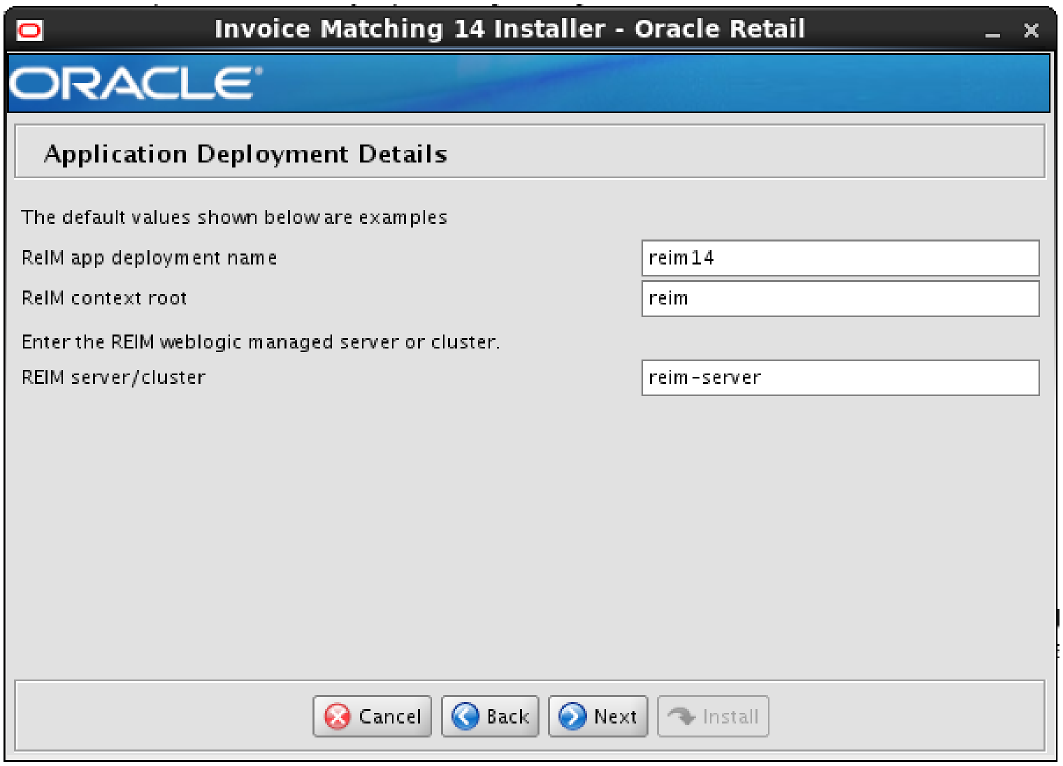
Field Title	Identity Keystore Passphrase
Field Description	Please provide password to access the keystore mentioned above

Field Title	Identity truststore
Field Description	Location or path where identity truststore file is stored.

Field Title	Identity truststore Type
Field Description	Type of the identity truststore used. Exampe: jks

Field Title	Identity truststore Passphrase
Field Description	Please provide password to access the truststore mentioned above.

Screen: Application Deployment Details



Application Deployment Details

The default values shown below are examples

ReIM app deployment name: reim14

ReIM context root: reim

Enter the REIM weblogic managed server or cluster.

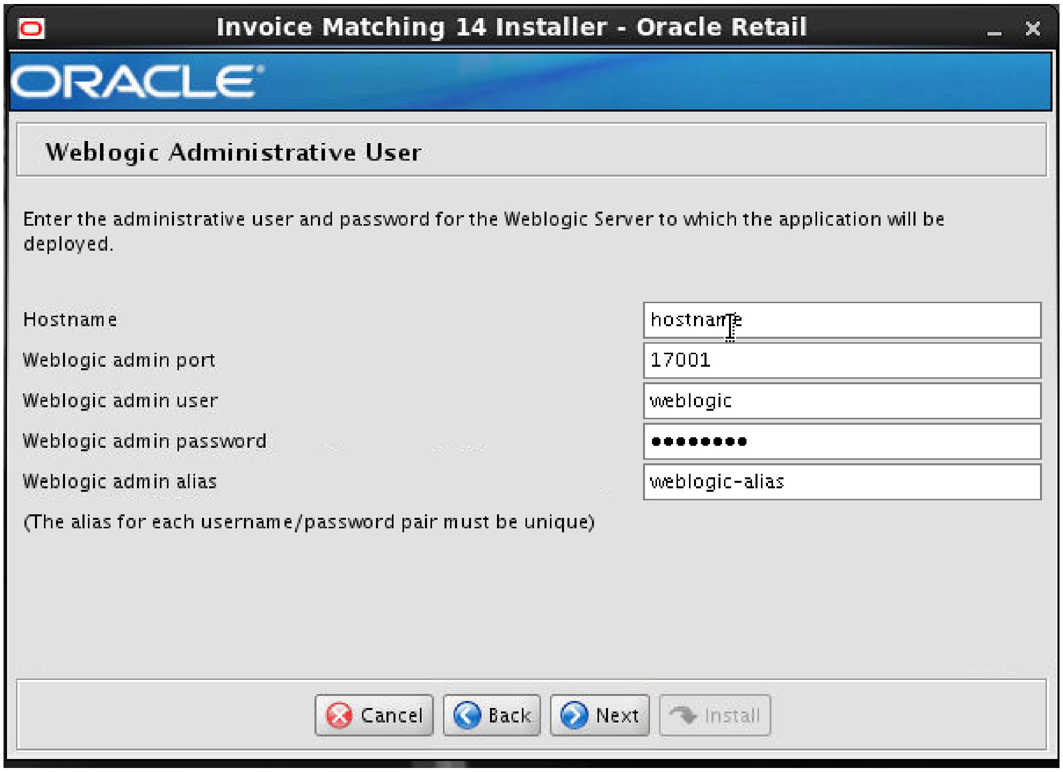
REIM server/cluster: reim-server

Field Title	ReIM app deployment name
Field Description	Name by which this ReIM application is identified in the application server. This value must match the <context_root> added to the weblogic.policy file when the managed server for ReIM was created.
Example	Reim14

Field Title	ReIM context root
Field Description	Path under the HTTP URL used to access the ReIM application (for example, a context root of reim results in the application accessed at http://host:port/reim/index.jsp). This value must match the <context_root> added to the weblogic.policy file when the managed server for ReIM was created.
Example	reim

Field Title	ReIM server/cluster
Field Description	Name of the ReIM WebLogic managed server or cluster.
Example	reim-server

Screen: WebLogic Administrative User



Weblogic Administrative User

Enter the administrative user and password for the Weblogic Server to which the application will be deployed.

Hostname	hostname
Weblogic admin port	17001
Weblogic admin user	weblogic
Weblogic admin password	●●●●●●●●
Weblogic admin alias	weblogic-alias

(The alias for each username/password pair must be unique)

Field Title	Hostname
Field Description	Hostname of the application server
Example	appserver

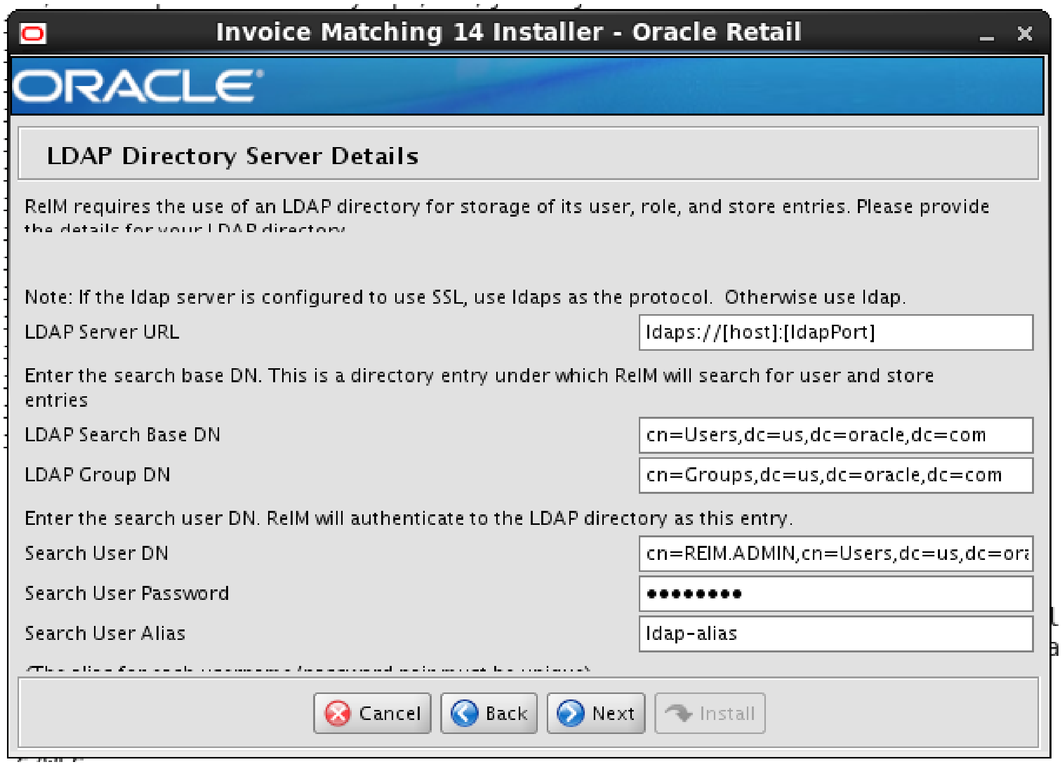
Field Title	WebLogic admin port
Field Description	This is the port of Administration Console.
Example	15001

Field Title	WebLogic admin user
Field Description	User name of the admin user for the WebLogic instance to which the ReIM application is being deployed.
Example	weblogic

Field Title	WebLogic admin password
Field Description	Password for the WebLogic admin user. You chose this password when you created the WebLogic instance or when you started the instance for the first time.

Field Title	WebLogic admin alias
Field Description	An alias for the WebLogic admin user.
Example	Weblogic-alias
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and problems issues with the application.

Screen: LDAP Directory Server Details



LDAP Directory Server Details

ReIM requires the use of an LDAP directory for storage of its user, role, and store entries. Please provide the details for your LDAP directory

Note: If the ldap server is configured to use SSL, use ldaps as the protocol. Otherwise use ldap.

LDAP Server URL: ldaps://[host]:[ldapPort]

Enter the search base DN. This is a directory entry under which ReIM will search for user and store entries

LDAP Search Base DN: cn=Users,dc=us,dc=oracle,dc=com

LDAP Group DN: cn=Groups,dc=us,dc=oracle,dc=com

Enter the search user DN. ReIM will authenticate to the LDAP directory as this entry.

Search User DN: cn=REIM.ADMIN,cn=Users,dc=us,dc=ora

Search User Password: ●●●●●●●●

Search User Alias: ldap-alias

(The alias for each username/password pair must be unique)

Field Title	LDAP server URL
Field Description	URL for your LDAP directory server. See Appendix: URL Reference for expected syntax.
Example	ldap://hostname:ldapport

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

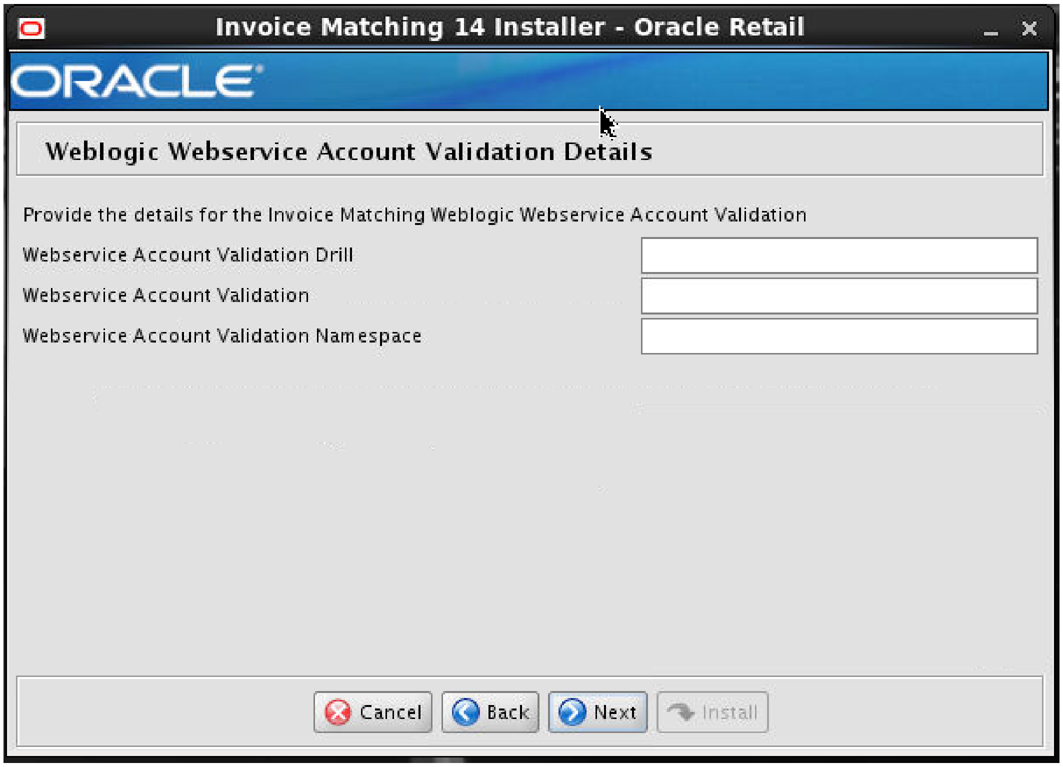
Field Title	LDAP Group DN
Field Description	Distingused name of the group that RPM uses to authenticate to the LDAP directory
Example	cn=Groups,dc=us,dc=oracle,dc=com

Field Title	Search User DN
Field Description	Search User DN that ReIM will authenticate to the ldap directory
Example	cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com

Field Title	Search user password
Field Description	Search User DN Password that ReIM will authenticate to the ldap directory
Example	Search User Password

Field Title	Search User Alias
Field Description	The alias for the search user DN.
Example	Ldap-user-alias
Notes	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Screen: WebLogic Webservice Account Validation Details



Weblogic Webservice Account Validation Details

Provide the details for the Invoice Matching Weblogic Webservice Account Validation

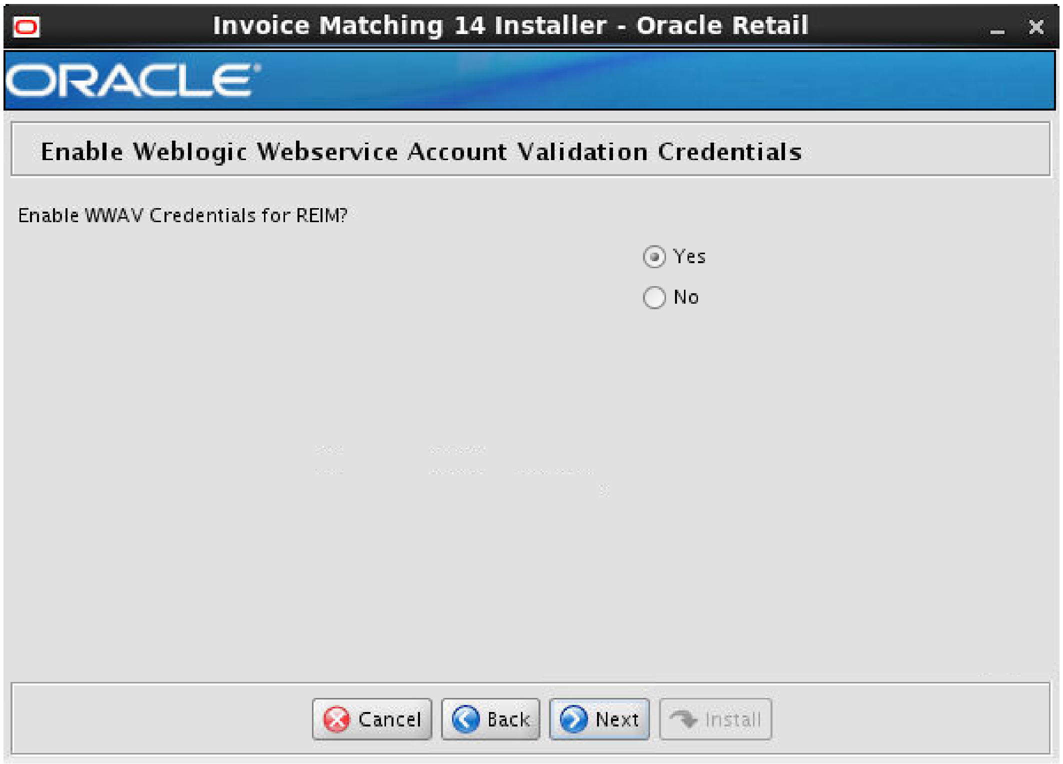
Webservice Account Validation Drill	
Webservice Account Validation	
Webservice Account Validation Namespace	

Field Title	Webservice Account Validation Drill
Field Description	The Web service provider URL used for drilling forward from the ReIM application. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.
Example	http://oracle.apps.aia.drillbackforward/

Field Title	Webservice Account Validation
Field Description	The URL for validating Web service accounts. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.
Example	http://host:7869/orabpel/default/ProcessGLAccountValidationRetailReqABCSImpl/1.0?wsdl

Field Title	Webservice Account Validation Namespace
Field Description	The URL for validating the Web service namespace. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.
Example	http://xmlns.oracle.com/ABCSImpl/Retail/Core/ProcessGLAccountValidationRetailReqABCSImpl/V1

Screen: Enable WebLogic Webservice Account Validation Credentials



Enable Weblogic Webservice Account Validation Credentials

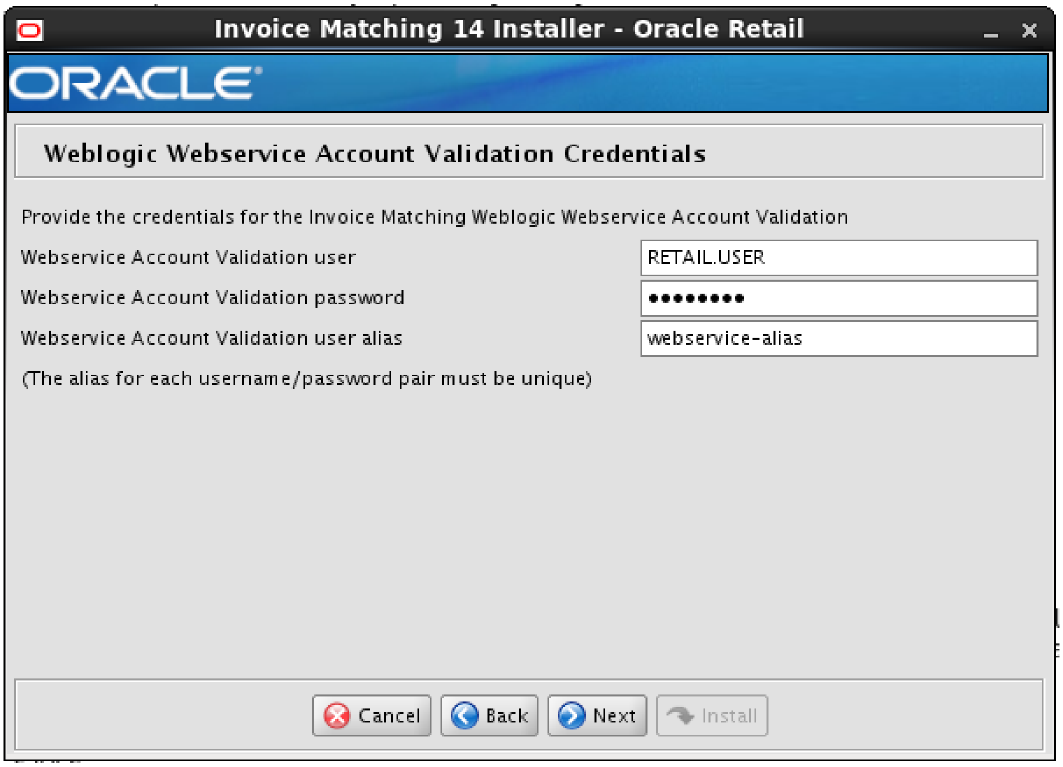
Enable WWAV Credentials for REIM?

● Yes

○ No

Field Title	Enable WWAV Credentials for REIM?
Field Description	Choosing Yes will navigate you to the screen asking for WebLogic Webservice Account Validation Credentials.

Screen: WebLogic Webservice Account Validation Credentials



Weblogic Webservice Account Validation Credentials

Provide the credentials for the Invoice Matching Weblogic Webservice Account Validation

Webservice Account Validation user: RETAIL.USER

Webservice Account Validation password: ●●●●●●●●●

Webservice Account Validation user alias: webservice-alias

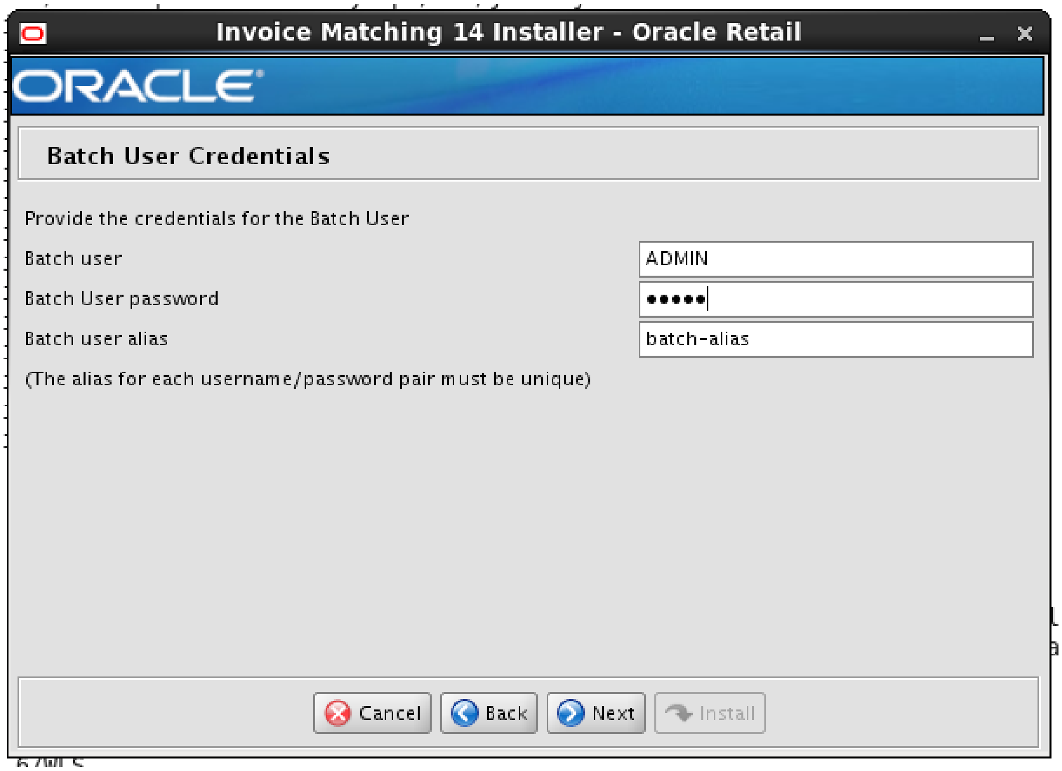
(The alias for each username/password pair must be unique)

Field Title	Webservice Account Validation user
Field Description	The user for validating the Web service user name. A value is required in this field, even if you are not using Web service integration. The field is not validated, so enter any value.
Example	RETAIL.USER

Field Title	Webservice Account Validation Password
Field Description	The password for validating Web service accounts. A value is required in this field, even if you are not using Web service integration. The field is not validated, so enter any value.

Field Title	Webservice Account Validation Alias
Field Description	The alias for the Web service account user names A value is required in this field, even if you are not using Web service integration. The field is not validated, so enter any value.
Example	webservice-alias
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Screen: Batch User Credentials



Batch User Credentials

Provide the credentials for the Batch User

Batch user: ADMIN

Batch User password: •••••

Batch user alias: batch-alias

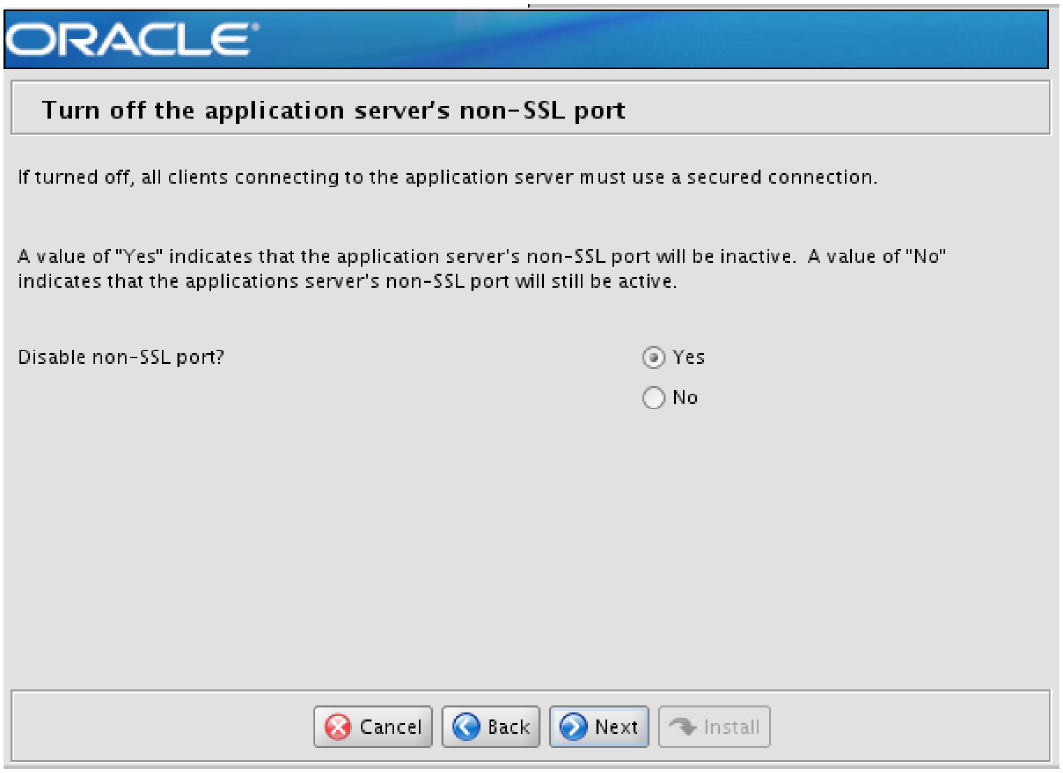
(The alias for each username/password pair must be unique)

Field Title	Batch User
Field Description	The ReIM user name of the person running ReIM batch. It must be a valid ReIM user that already exists in the database and LDAP. It does not have to exist already in the database on the database table (IM_BUSINESS_ROLE_MEMBER), but it must exist when you try to use the alias created in this step to run batches. Using one of the user names you will supply in subsequent screens (such as Setup Application Users) is recommended. ADMIN is the default user for the ReIM application.
Example	ADMIN

Field Title	Batch User Password
Field Description	The wallet password must match the database password on the database IM_USER_AUTHORIZATION table. The ReIM default scripts include User= ADMIN with and password=retek..

Field Title	Batch User Alias
Field Description	The alias for the user running ReIM batch. This alias is part of ORACLE wallet implementation. You will use this alias when running ReIM batch scripts.
Example	BATCH-ALIAS
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

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



Turn off the application server's non-SSL port

If turned off, all clients connecting to the application server must use a secured connection.

A value of "Yes" indicates that the application server's non-SSL port will be inactive. A value of "No" indicates that the applications server's non-SSL port will still be active.

Disable non-SSL port? ● Yes ○ No

Note: This screen appears only if you have enabled SSL for ReIM. Ignore this step in case you have not enabled SSL for ReIM.

Field Title	Disable non-SSL port?
Field Description	Choosing Yes disables the non SSL port on the managed server. Choosing no will the leave the non SSL port of the managed server active.

B

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:

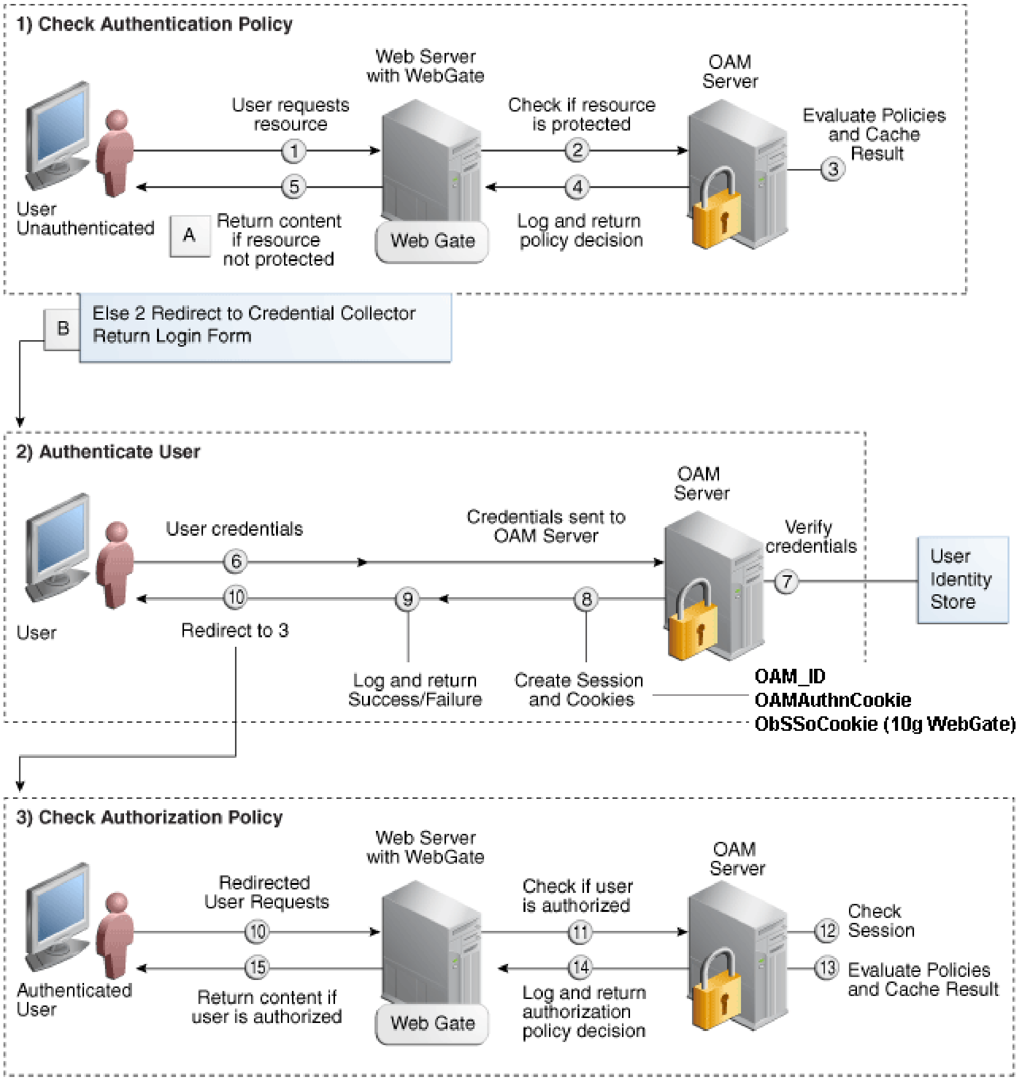
- The Oracle Access Manager (OAM) server, which is responsible for the back-end authentication of the user.
- The Oracle Internet Directory LDAP server, which stores user IDs, passwords, and group (role) membership.
- The Oracle Access Manager Agent associated with the Web application, which verifies 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


1) Check Authentication Policy
User Unauthenticated
User requests resource
1
5
Web Server with WebGate
Web Gate
Check if resource is protected
2
4
OAM Server
Evaluate Policies and Cache Result
3
A
Return content if resource not protected
Log and return policy decision
B
Else 2 Redirect to Credential Collector Return Login Form
2) Authenticate User
User
User credentials
6
10
Redirect to 3
9
Log and return Success/Failure
8
Create Session and Cookies
Credentials sent to OAM Server
OAM Server
Verify credentials
7
User Identity Store
OAM_ID
OAMAuthnCookie
ObSSoCookie (10g WebGate)
3) Check Authorization Policy
Authenticated User
Redirected User Requests
10
15
Return content if user is authorized
Web Server with WebGate
Web Gate
Check if user is authorized
11
14
Log and return authorization policy decision
OAM Server
12
Check Session
13
Evaluate Policies and Cache Result

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 (11.1.1.7) 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.

C

Appendix: URL Reference

Both the database schema and application installers for the Invoice Matching product require certain URLs, including the following.

JDBC URL for a Database

Used by the Java application and by the installer to connect to the database.

Thick Client Syntax: jdbc:oracle:thin:@<sid>

<sid>: system identifier for the database

Example: jdbc:oracle:oci:@mysid

Thin Client Syntax: jdbc:oracle:thin:@<host>:<port>:<sid>

<host>: hostname of the database server

<port>: database listener port

<sid>: system identifier for the database

Example: jdbc:oracle:thin:@myhost:1521:mysid

D

Appendix: Common Installation Errors

This section provides some common errors encountered during installation of ReIM.

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.

Warning: Could not 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.

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.

Hostname Verification Error when SSL is used

Symptom:

The Application installer fails saying that the reim-server could not restart with the below error.

```
[exec] This Exception occurred at Thu Nov 14 04:20:39 EST 2013.
     [exec] javax.naming.CommunicationException [Root exception is
java.net.ConnectException: t3s://msp52420:15004: Destination unreachable; nested
exception is:
     [exec]     javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain
received from msp52420 - 10.141.53.240 failed hostname verification check.
Certificate contained msp52420.us.oracle.com but check expected msp52420; No
available router to destination]
```

Solution:

Provide the complete hostname in the “Host Details” field of the installer screen (i.e., msp52420.us.oracle.com instead of msp5240) and the install will go through successfully.

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 three 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.

Setting up Wallets for Database User Accounts

The following examples show how to set up wallets for database user accounts for the following applications:

- For RMS, RWMS, RPM Batch using sqlplus or sqlldr, RETL, RMS, RWMS, and ARI

For RMS, RWMS, RPM Batch using sqlplus or sqlldr, RETL, RMS, RWMS, and ARI

To set up wallets for database user accounts, do the following.

1. Create a new directory called wallet under your folder structure.

```
cd /projects/rms14/dev/
mkdir .wallet
```

> **Note:** The default permissions of the wallet allow only the owner to use it, ensuring the connection information is protected. If you want other users to be able to use the connection, you must adjust permissions appropriately to ensure only authorized users have access to the wallet.

2. Create a sqlnet.ora in the wallet directory with the following content.

```
WALLET_LOCATION =   (SOURCE =     (METHOD = FILE)     (METHOD_DATA =
(DIRECTORY =  /projects/rms14/dev/.wallet)) )
SQLNET.WALLET_OVERRIDE=TRUE
SSL_CLIENT_AUTHENTICATION=FALSE
```

> **Note**: WALLET_LOCATION must be on line 1 in the file.

3. Setup a tnsnames.ora in the wallet directory. This tnsnames.ora includes the standard tnsnames.ora file. Then, add two custom tns_alias entries that are only for use with the wallet. For example, `sqlplus /@dvols29_rms01user`.

```
ifile = /u00/oracle/product/11.2.0.1/network/admin/tnsnames.ora

dvols29_rms01user =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
  (host = mspxxxxx.us.oracle.com) (Port = 1521)))
    (CONNECT_DATA = (SID = dvols29) (GLOBAL_NAME = dvols29)))

dvols29_rms01user.world =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
  (host = mspxxxxx.us.oracle.com) (Port = 1521)))
    (CONNECT_DATA = (SID = dvols29) (GLOBAL_NAME = dvols29)))
```

> **Note**: It is important to not just copy the tnsnames.ora file because it can quickly become out of date. The ifile clause (shown above) is key.

4. Create the wallet files. These are empty initially.

   a. Ensure you are in the intended location.

   ```
   $ pwd
   /projects/rms14/dev/.wallet
   ```

   b. Create the wallet files.

```
$ mkstore -wrl . –create
```

c. Enter the wallet password you want to use. It is recommended that you use the same password as the UNIX user you are creating the wallet on.

d. Enter the password again.

   Two wallet files are created from the above command:

   – ewallet.p12

   – cwallet.sso

5. Create the wallet entry that associates the user name and password to the custom tns alias that was setup in the wallet's tnsnames.ora file.

   ```
   mkstore –wrl . –createCredential <tns_alias> <username> <password>
   ```

Example: `mkstore –wrl . –createCredential dvols29_rms01user rms01user passwd`

6. Test the connectivity. The ORACLE_HOME used with the wallet must be the same version or higher than what the wallet was created with.

   ```
   $ export TNS_ADMIN=/projects/rms14/dev/.wallet /* This is very import to use
   wallet to point at the alternate tnsnames.ora created in this example */

   $ sqlplus /@dvols29_rms01user

   SQL*Plus: Release 11

   Connected to:
   Oracle Database 11g

   SQL> show user
   USER is "rms01user"
   ```

   Running batch programs or shell scripts would be similar:

   ```
   Ex: dtesys /@dvols29_rms01user
   script.sh /@dvols29_rms01user

   Set the UP unix variable to help with some compiles :

   export UP=/@dvols29_rms01user
   for use in RMS batch compiles, and RMS, RWMS, and ARI forms compiles.
   ```

As shown in the example above, users can ensure that passwords remain invisible.

Additional Database Wallet Commands

The following is a list of additional database wallet commands.

- Delete a credential on wallet

  ```
  mkstore –wrl . –deleteCredential dvols29_rms01user
  ```

- Change the password for a credential on wallet

  ```
  mkstore –wrl . –modifyCredential dvols29_rms01user rms01user passwd
  ```

- List the wallet credential entries

  ```
  mkstore –wrl . –list
  ```

  This command returns values such as the following.

  ```
  oracle.security.client.connect_string1
  oracle.security.client.user1
  oracle.security.client.password1
  ```

- View the details of a wallet entry

  ```
  mkstore –wrl . –viewEntry oracle.security.client.connect_string1
  ```

  Returns the value of the entry:

  ```
  dvols29_rms01user
  mkstore –wrl . –viewEntry oracle.security.client.user1
  ```

  Returns the value of the entry:

  ```
  rms01user
  ```

  ```
  mkstore –wrl . –viewEntry oracle.security.client.password1
  ```

  Returns the value of the entry:

  ```
  Passwd
  ```

Setting up RETL Wallets

RETL creates a wallet under $RFX_HOME/etc/security, with the following files:

- cwallet.sso
- jazn-data.xml
- jps-config.xml
- README.txt

To set up RETL wallets, perform the following steps:

1. Set the following environment variables:
   - `ORACLE_SID=<retaildb>`
   - `RFX_HOME=/u00/rfx/rfx-13`
   - `RFX_TMP=/u00/rfx/rfx-13/tmp`
   - `JAVA_HOME=/usr/jdk1.6.0_12.64bit`
   - `LD_LIBRARY_PATH=$ORACLE_HOME`
   - `PATH=$RFX_HOME/bin:$JAVA_HOME/bin:$PATH`
2. Change directory to $RFX_HOME/bin.
3. Run setup-security-credential.sh.
   - Enter 1 to add a new database credential.
   - Enter the dbuseralias. For example, `retl_java_rms01user`.
   - Enter the database user name. For example, `rms01user.`
   - Enter the database password.
   - Re-enter the database password.
   - Enter D to exit the setup script.
4. Update your RETL environment variable script to reflect the names of both the Oracle Networking wallet and the Java wallet.

   For example, to configure RETLforRPAS, modify the following entries in `$MMHOME/RETLforRPAS/rfx/etc/rmse_rpas_config.env.`
   - The RETL_WALLET_ALIAS should point to the Java wallet entry:
     – `export RETL_WALLET_ALIAS="retl_java_rms01user"`
   - The ORACLE_WALLET_ALIAS should point to the Oracle network wallet entry:
     – `export ORACLE_WALLET_ALIAS="dvols29_rms01user"`
   - The SQLPLUS_LOGON should use the ORACLE_WALLET_ALIAS:
     – `export SQLPLUS_LOGON="/@${ORACLE_WALLET_ALIAS}"`

5. To change a password later, run `setup-security-credential.sh`.
   - Enter 2 to update a database credential.
   - Select the credential to update.
   - Enter the database user to update or change.
   - Enter the password of the database user.
   - Re-enter the password.

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?

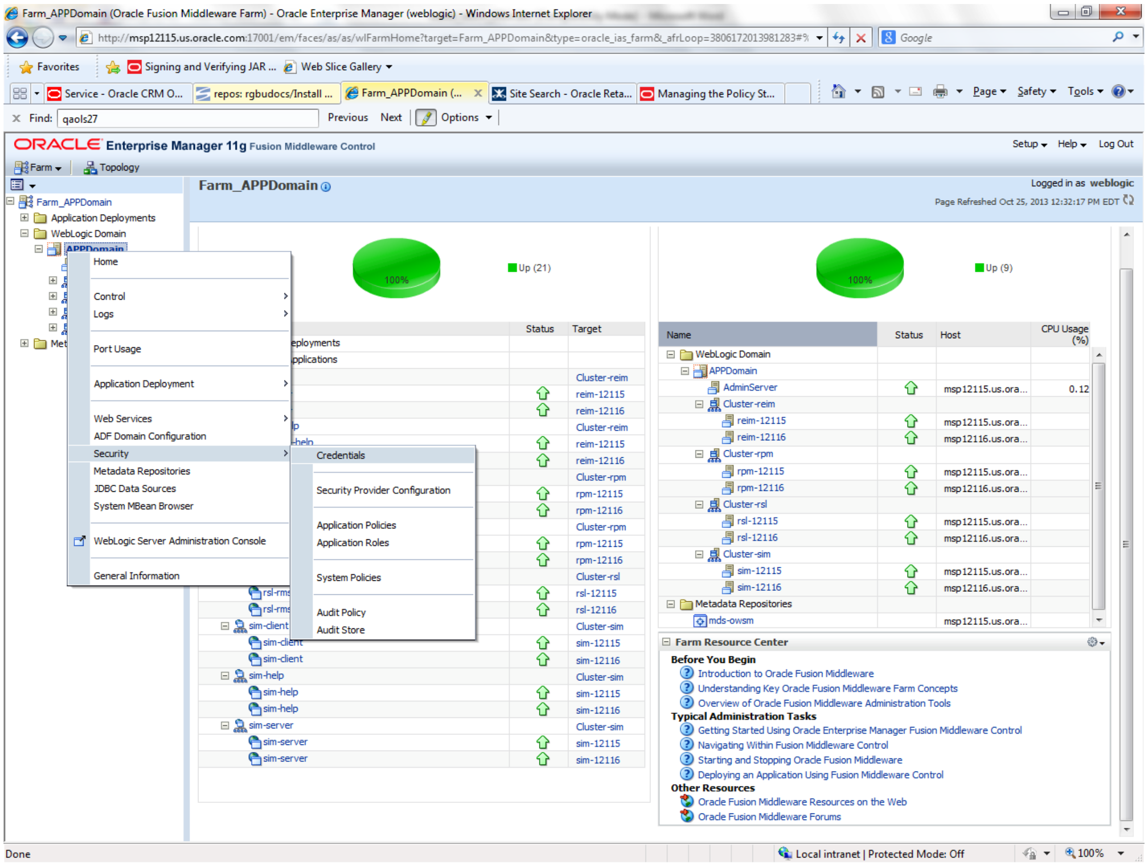
Some of the ORACLE Retail Java batch applications have an alias to use when running Java batch programs. For example, alias REIMBAT-ALIAS maps through the wallet to dbuser RMS01APP, already on the database. To run a ReIM batch program the format would be: reimbatchpgmname REIMBAT-ALIAS <other arguments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

Database Credential Store Administration

ORACLE Retail 14.0.2 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 14.0.2 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**



Name	Status	Host	CPU Usage (%)
WebLogic Domain			
APPDomain			
AdminServer	⇧	msp12115.us.ora...	0.12
Cluster-reim			
reim-12115	⇧	msp12115.us.ora...	
reim-12116	⇧	msp12116.us.ora...	
Cluster-rpm			
rpm-12115	⇧	msp12115.us.ora...	
rpm-12116	⇧	msp12116.us.ora...	
Cluster-rsl			
rsl-12115	⇧	msp12115.us.ora...	
rsl-12116	⇧	msp12116.us.ora...	
Cluster-sim			
sim-12115	⇧	msp12115.us.ora...	
sim-12116	⇧	msp12116.us.ora...	
Metadata Repositories			
mds-owsm		msp12115.us.ora...	

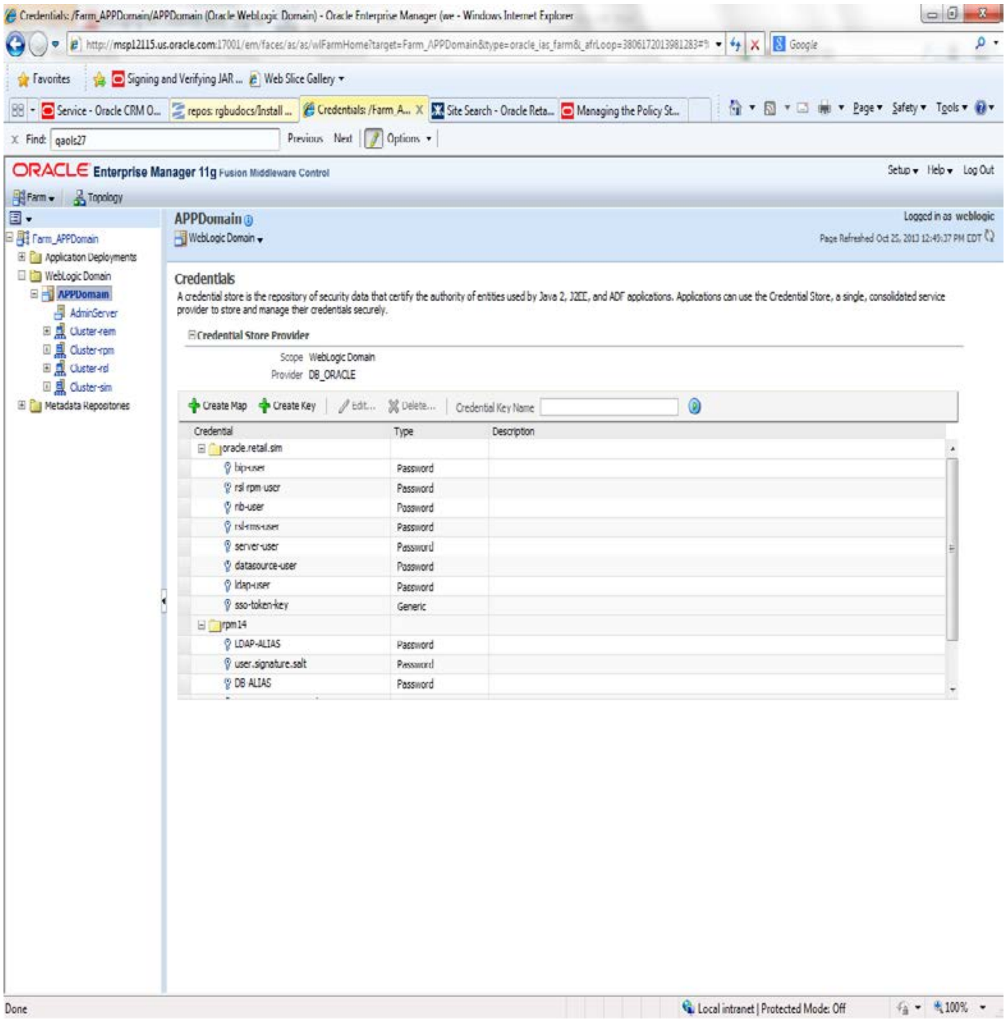
Farm Resource Center

Before You Begin
- Introduction to Oracle Fusion Middleware
- Understanding Key Oracle Fusion Middleware Farm Concepts
- Overview of Oracle Fusion Middleware Administration Tools

Typical Administration Tasks
- Getting Started Using Oracle Enterprise Manager Fusion Middleware Control
- Navigating Within Fusion Middleware Control
- Starting and Stopping Oracle Fusion Middleware
- Deploying an Application Using Fusion Middleware Control

Other Resources
- Oracle Fusion Middleware Resources on the Web
- Oracle Fusion Middleware Forums

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
http://msp12115.us.oracle.com:17001/em/faces/as/as/wlFarmHome?target=Farm_APPDomain&type=oracle_ias_farm&_afrLoop=380617201398l283#
Google
Favorites
Signing and Verifying JAR ...
Web Slice Gallery
Service - Oracle CRM O...
repos: rgbudocs/Install ...
Credentials: /Farm_A...
Site Search - Oracle Reta...
Managing the Policy St...
Page
Safety
Tools
Find: qaols27
Previous
Next
Options
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
Page Refreshed Oct 25, 2013 12:49:37 PM EDT
Create Map
Create Key
Edit...
Delete...
Credential Key Name
Done
Local intranet | Protected Mode: Off
100%

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

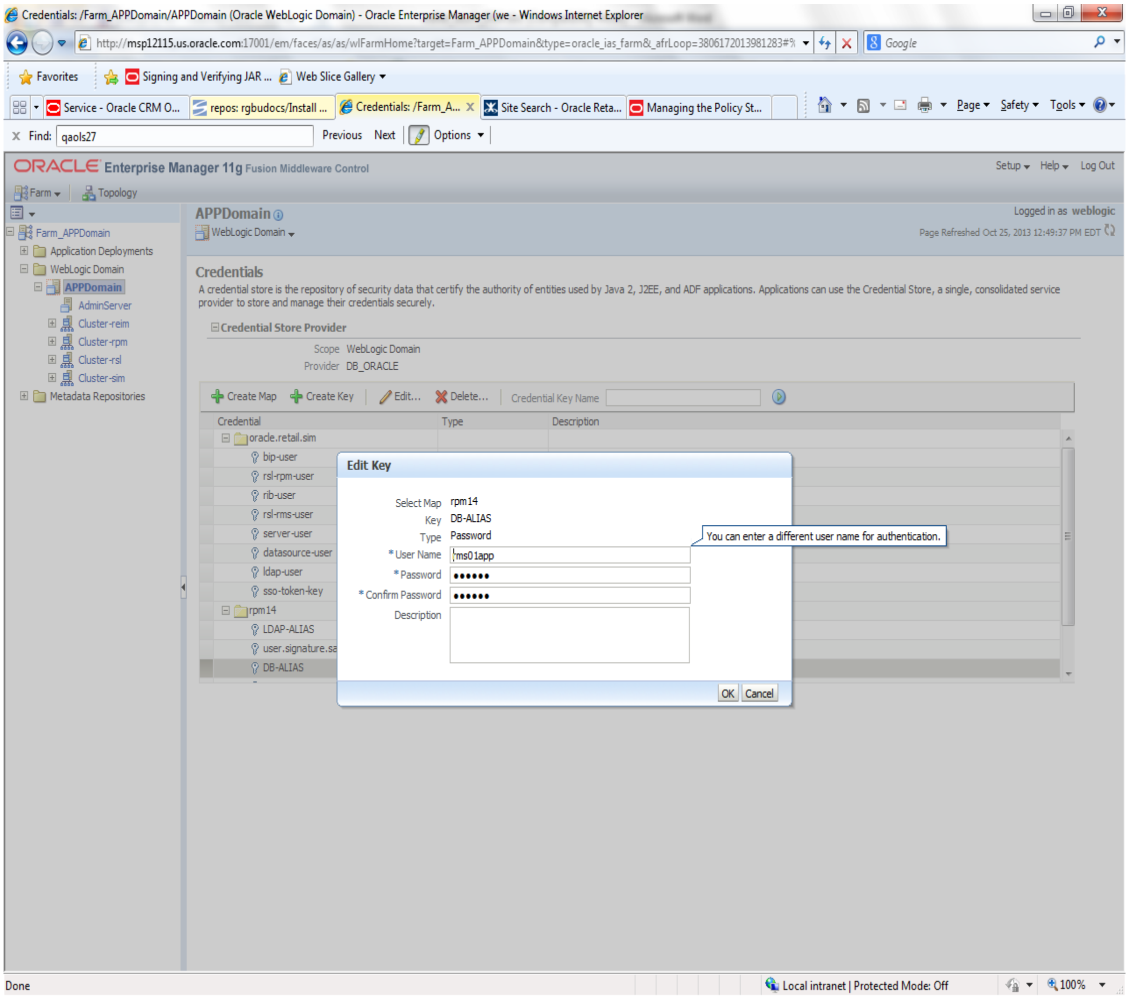
Scope WebLogic Domain

Provider DB_ORACLE

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	

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:


Credentials: /Farm_APPDomain/APPDomain (Oracle WebLogic Domain) - Oracle Enterprise Manager (we - Windows Internet Explorer

http://msp12115.us.oracle.com:17001/em/faces/as/as/wlFarmHome?target=Farm_APPDomain&type=oracle_ias_farm&_afrLoop=3806172013981283#%

Find: qaols27

APPDomain

WebLogic Domain

Logged in as weblogic

Page Refreshed Oct 25, 2013 12:49:37 PM EDT

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

Credential	Type	Description
oracle.retail.sim		
bip-user		
rsl-rpm-user		
rib-user		
rsl-rms-user		
server-user		
datasource-user		
ldap-user		
sso-token-key		
rpm14		
LDAP-ALIAS		
user.signature.sa		
DB-ALIAS		

Edit Key

Select Map rpm14
Key DB-ALIAS
Type Password
* User Name rms01app
* Password ••••••
* Confirm Password ••••••
Description

You can enter a different user name for authentication.

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: 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 only some 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