Oracle® Retail Invoice Matching

Installation Guide
Release 13.2.5
E37580-03

May 2013

ORACLE

Oracle® Retail Invoice Matching Installation Guide, Release 13.2.5

Primary Author: Wade Schwarz

Contributors: Nathan Young

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

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

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

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

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

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

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

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

Contents

Send Us Your Comments

Oracle Retail Invoice Matching Installation Guide, Release 13.2.5

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 13.2.5 documentation set:

- *Oracle Retail Invoice Matching Release Notes*
- *Oracle Retail Invoice Matching Operations Guide*
- *Oracle Retail Merchandising Implementation Guide*
- *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, 13.2) or a later patch release (for example, 13.2.1). If you are installing the base release and additional patch and bundled hot fix releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch and bundled hot fix releases can contain critical information related to the base release, as well as information about code changes since the base release.

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/technology/documentation/oracle_retail.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/technology/documentation/oracle_retail.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.

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 5 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 5 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 6.1, 7.1 (Actual hardware or LPARs) ▪ Solaris 10, 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 (11.2.0.3) with the following specifications: **Components:** ▪ Oracle Partitioning ▪ Examples CD (Formerly the companion CD) **Other components:** ▪ Perl compiler 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:

Note: Files required for Oracle Configuration Manager (OCM) are removed after OPatch is used to patch the WebLogic server. This will cause the product installers and OCM installation to fail. To work around this issue, back up the content of the $ORACLE_HOME/utils/ccr/lib directory prior to applying a patch using OPatch, and recopy the content back after you apply any patches. ORACLE_HOME is the location where WebLogic Server has been installed.

Note: If using an OPatch on Linux 64-bit platforms, see "Installer Fails because of missing .jar in $ORACLE_HOME/utils/ccr/lib" in Appendix: Common Installation Errors.

Supported on	Versions Supported
Application Server OS	OS certified with Oracle Fusion Middleware 11g Release 1 (11.1.1.6). Options are: ▪ Oracle Linux 5 for x86-64 (Actual hardware or Oracle virtual machine). ▪ Red Hat Enterprise Linux 5 for x86-64 (Actual hardware or Oracle virtual machine). ▪ AIX 6.1, 7.1 (Actual hardware or LPARs) ▪ Solaris 10, 11 SPARC (Actual hardware or logical domains) ▪ HP-UX 11.31 Integrity (Actual hardware, HPVM, or vPars)

Supported on	Versions Supported
Application Server	Oracle Fusion Middleware 11g Release 1 (11.1.1.6) **Components:** ▪ Oracle WebLogic Server 11g Release 1 (10.3.6) ▪ Java: JDK 1.6.0+ 64 bit or Jrockit 1.6 R28 build or later, within the 1.6 code line. 64 bit. For Linux and Solaris OS only. **Other components:** ▪ Oracle BI Publisher 10g (10.1.3.4) Oracle Internet Directory 10gR3 (10.1.4) or Oracle Identity Management 11gR1 (11.1.1.6). **IMPORTANT**: If there is an existing WebLogic installation on the server, you must upgrade to WebLogic 10.3.6. All middleware components associated with WebLogic server 10.3.3 or 10.3.4 should be upgraded to 11.1.1.6. Back up the weblogic.policy file ($WLS_HOME/wlserver_10.3/server/lib) before upgrading your WebLogic server, because this file could be overwritten. Copy over the weblogic.policy backup file after the WebLogic upgrade is finished and the post patching installation steps are completed. For information on how to complete the upgrade to WebLogic 10.3.4, see the My Oracle Support document, "How to Upgrade from WebLogic11g 10.3.3 to WebLogic11g 10.3.4" (ID 1432575.1). **Note:** See Installer Fails because of missing .jar in $ORACLE_HOME/utils/ccr/lib in Appendix: Common Installation Errors. This issue occurs only when the application is being installed on the same WebLogic server on which forms based applications are installed. It is valid only for Linux 64-bit.

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 Internet Directory 10gR3 version 10.1.4 or Oracle Identity Management 11gR1 version 11.1.1.6 has been installed along with the components listed in the above Application Server requirements section . Verify the Oracle WebTier Server is registered with the Oracle Access Manager 11gR1 as a partner application.

Check Supported Client PC and Web Browser Requirements

Requirement	Version
Operating system	Windows XP or 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	1.6.0_22+
Browser	Microsoft Internet Explorer version 8 or 9 Mozilla Firefox 3.6 or 10.0

Configure Mozilla Firefox 10.0

If you are using Firefox 10.0, 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)	13.2.5
Oracle Retail Store Inventory Management (SIM) (by way of RMS)	13.2.5
Oracle Retail Analytics	13.2.5

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 Application Integration Architecture (AIA) Media Pack 2.5 Oracle E-Business Suite 12.1.1 and 12.1.3 integration is supported using the Oracle Financial Operations Control Integration Pack for Oracle Retail Merchandising Suite and Oracle E-Business Suite Financials. See the *Oracle® Application Integration Architecture 2.5: Installation and Upgrade Guide* for specific version information.
PeopleSoft Enterprise Financials	Oracle Application Integration Architecture (AIA) Media Pack 2.5 PeopleSoft Enterprise Financials integration is supported using the Oracle Retail Merchandising Integration Pack for PeopleSoft Enterprise Financials: Financial Operations Control. See the *Oracle Application Integration Architecture 2.5: Installation and Upgrade Guide* 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 11.2.0.3 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 11.2.0.2 Oracle Internet Directory database with the WebLogic 10.3.6 cluster. It is suggested that a Web Tier 11.1.1.5 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.

IMPORTANT: If there is an existing WebLogic installation on the server, you must upgrade it to WebLogic 10.3.6. All middleware components associated with WebLogic server 10.3.6 should be upgraded to 11.1.1.6.

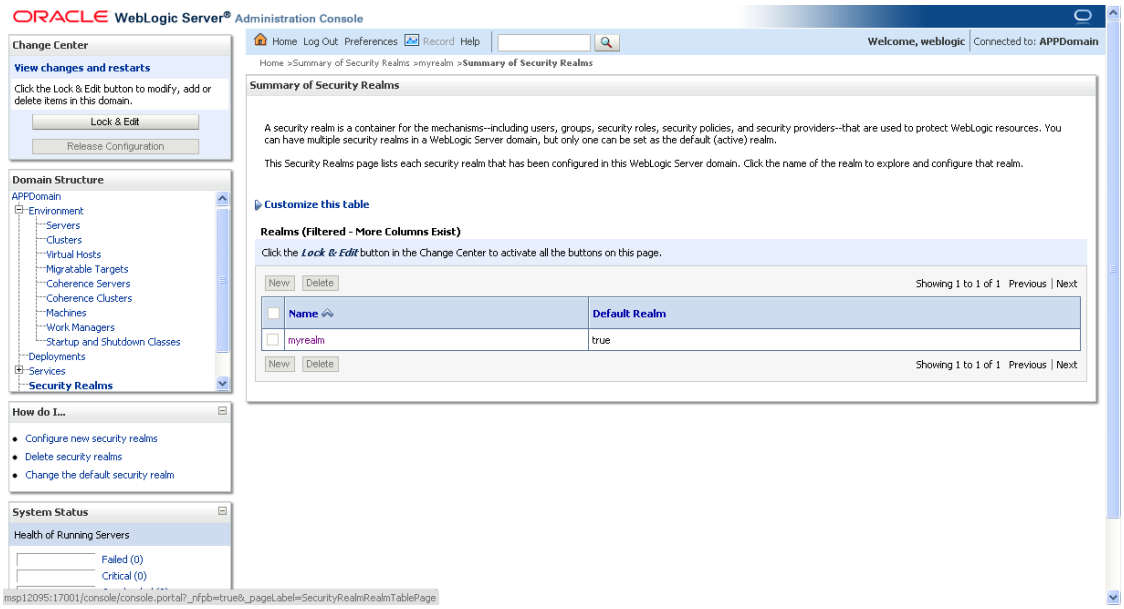
Back up the weblogic.policy file ($WLS_HOME/wlserver_10.3/server/lib) before upgrading your WebLogic server, because this file could be overwritten. Copy over the weblogic.policy backup file after the WebLogic upgrade is finished and the post patching installation steps are completed.

Create Providers

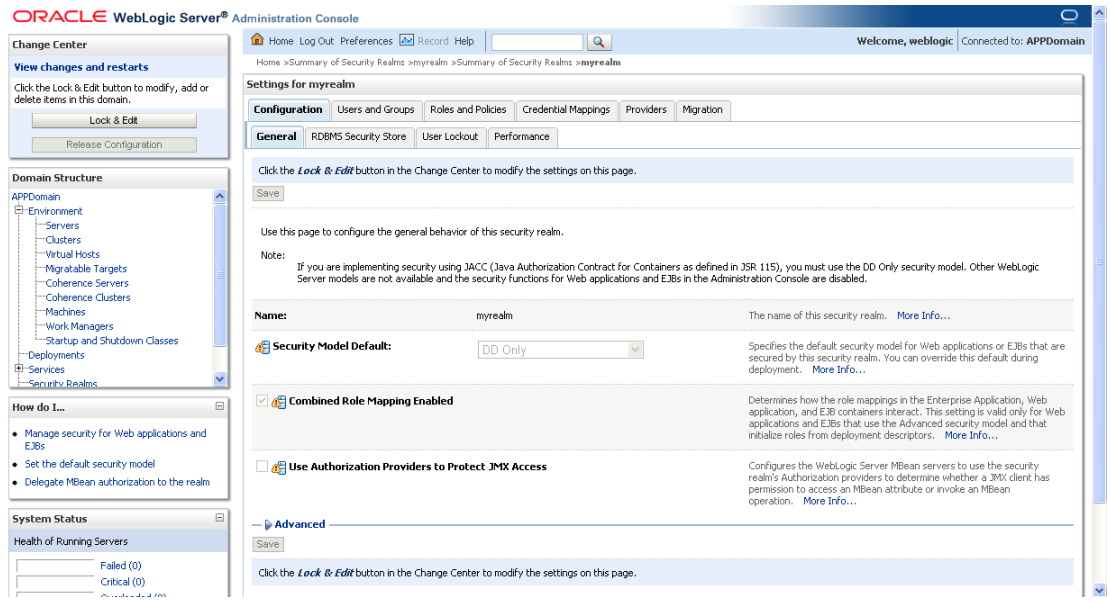
Perform the following procedure to create providers in APPDomain and ClassicDomain.

Note: The following steps are being performed in APPDomain but the steps must be done for both APPDomain and ClassicDomain.

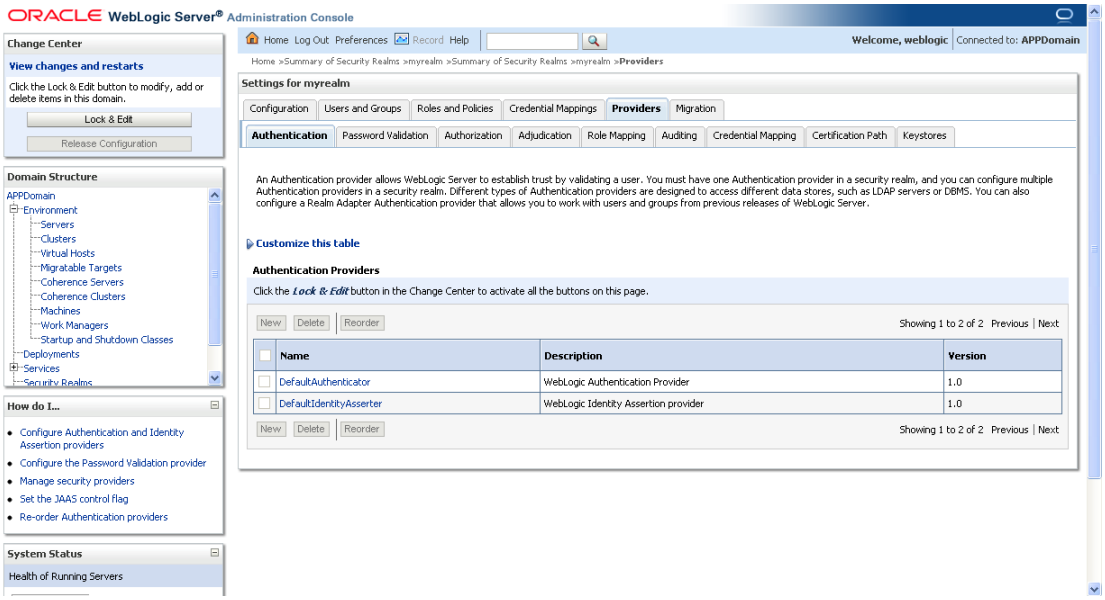
6. Log in to the Administration Console.
   http://<host>:<port>/console/
7. In the Domain Structure frame, click Security Realms.



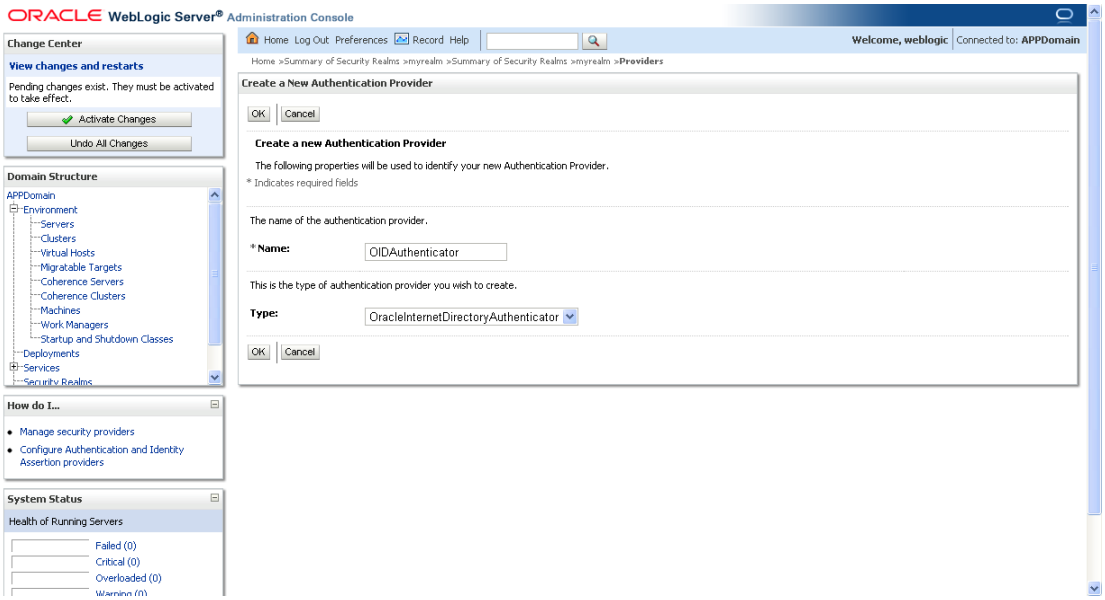
8. In the Realms table, click myrealm. The Settings for myrealm page is displayed.



9. Click the Providers tab.

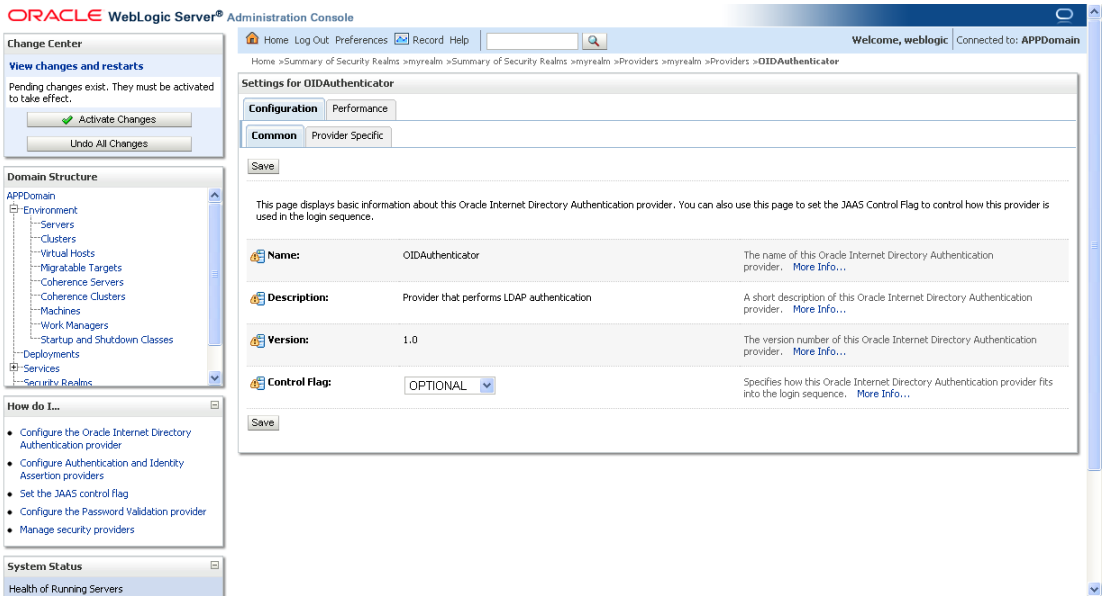


10. Click **Lock & Edit** and then click **New**. The Create a New Authentication Provider page is displayed.

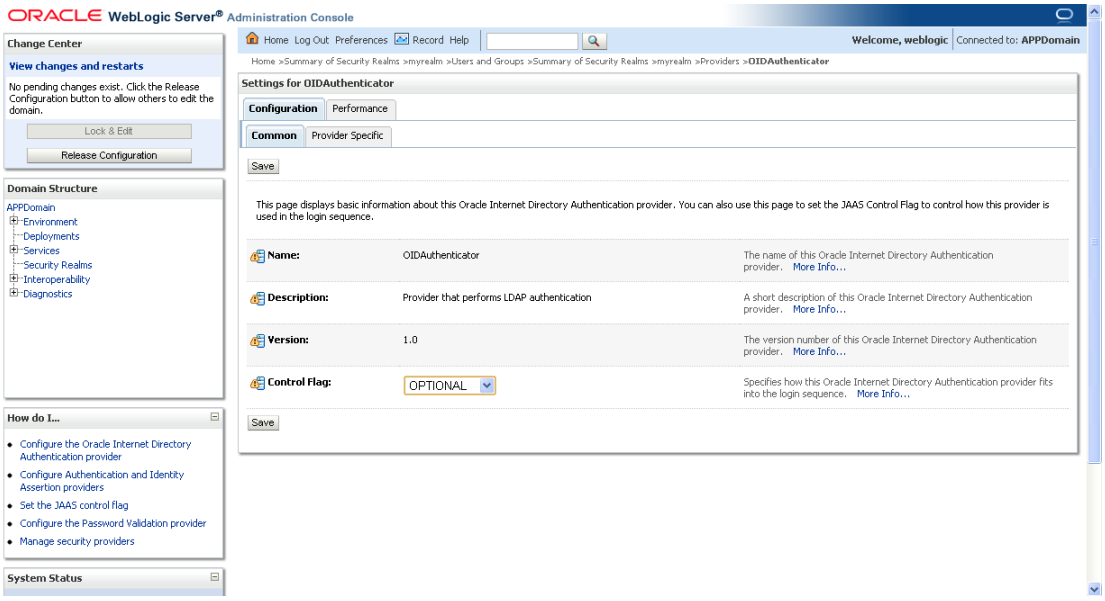


11. Enter OIDAuthenticator in the Name field and select OracleInternetDirectoryAuthenticator as the type.

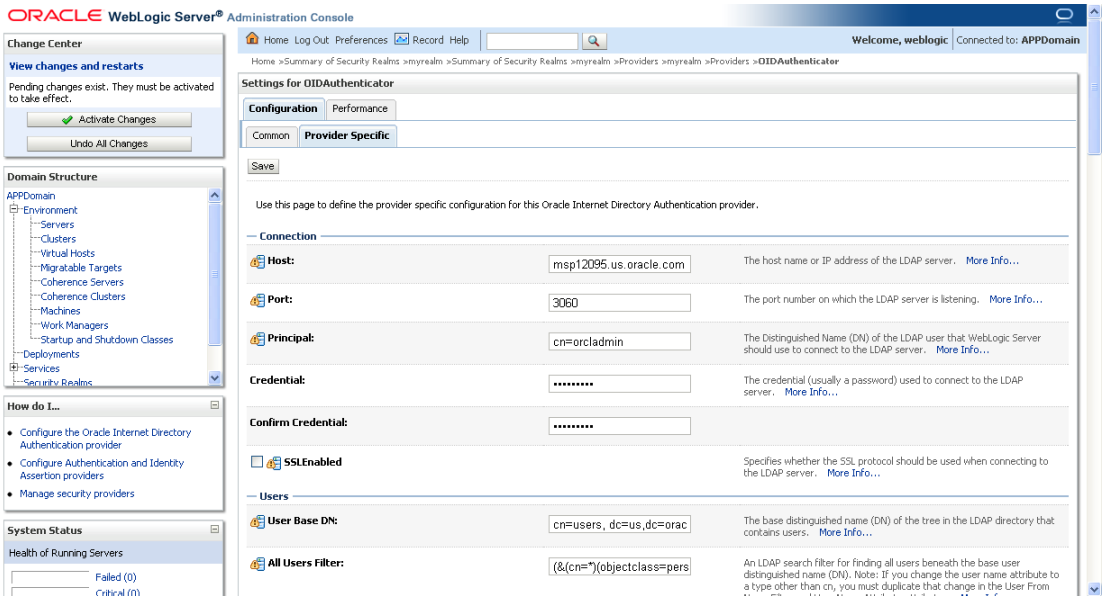
12. Click **OK**. The Settings for OIDAuthenitcator page is displayed.



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



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



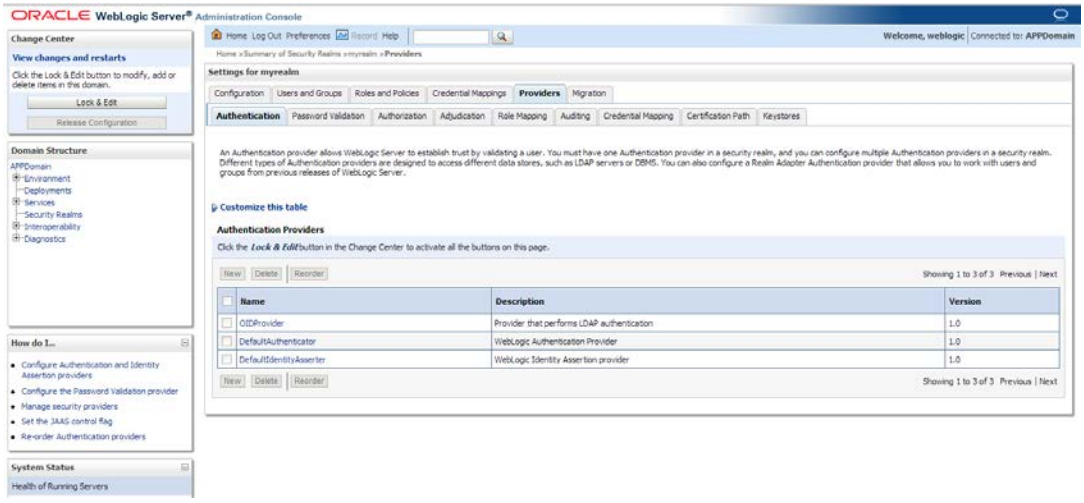
16. Supply your LDAP connection and credentials.

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

    - Host: msp12095.us.oracle.com
    - Port: 3060
    - Principal: cn=orcladmin
    - Credential: <*password*>
    - Confirm Credential: <*password*>
    - User Base DN: cn=users,dc=us,dc=oracle,dc=com
    - Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com
    - Check **Propagate Cause For Login Exception**

17. Click **Save**.

18. Click the Providers tab and click **Lock & Edit**.



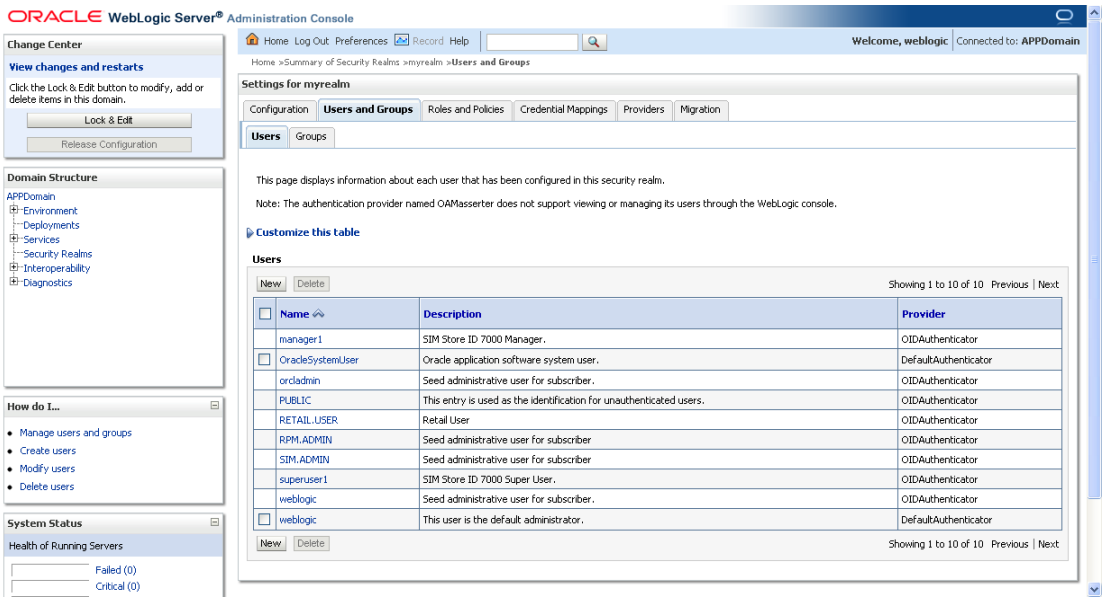
19. Click **Reorder**.

20. Order OIDAuthenticator first and DefaultAuthenticator second.

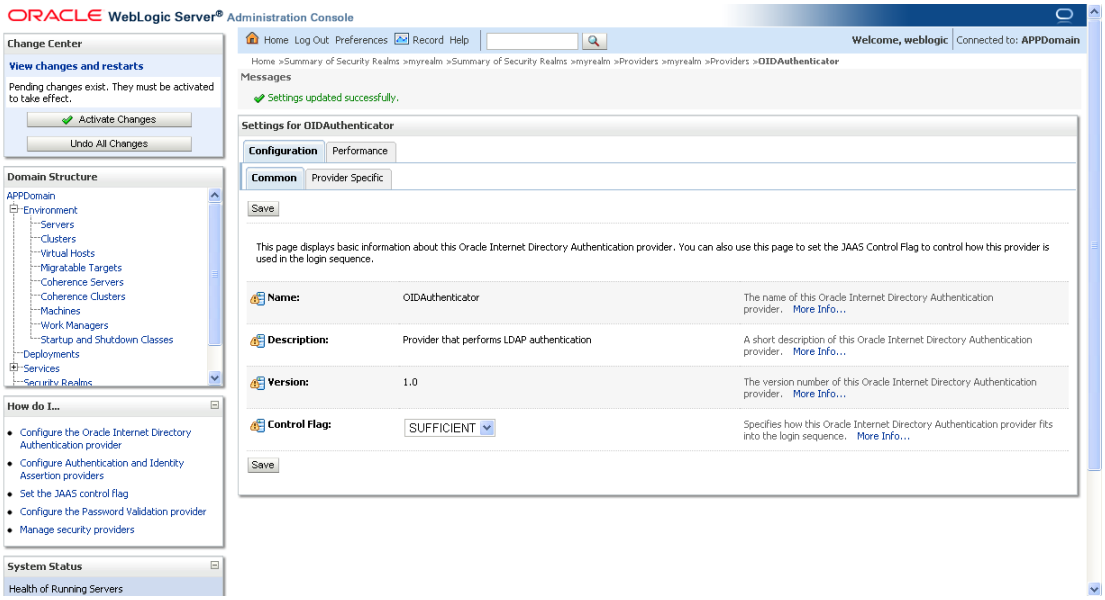
21. Click **Save**.
22. Once your changes are saved, click **Activate Changes**.
23. Shut down all servers and restart the admin server.

Verify and Set OID Authenticator

1. Log in to the Administration Console.
   http://<host>:<port>/console/
2. In the Domain Structure frame, click Security Realms.
3. In the Realms table, click Default Realm Name. The Settings page is displayed.
4. Click the Providers tab.
5. Click the Users and Groups tab to see a list of users and groups contained in the configured authentication providers.
   You should see usernames from the Oracle Internet Directory configuration, which implicitly verifies that the configuration is working.



6. Click the Providers tab and click OIDAuthenticator.



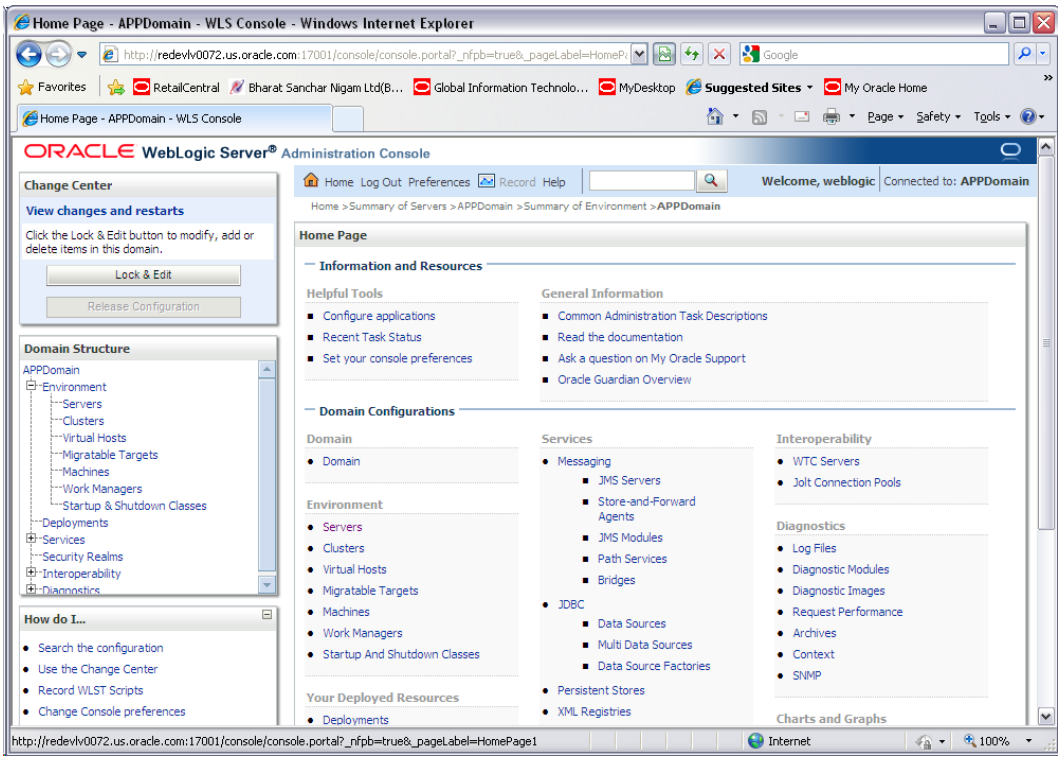
7. Set Control Flag to SUFFICIENT and click **Save**.
8. Click **Activate Changes** and restart the admin server.

Install Managed Server in WebLogic

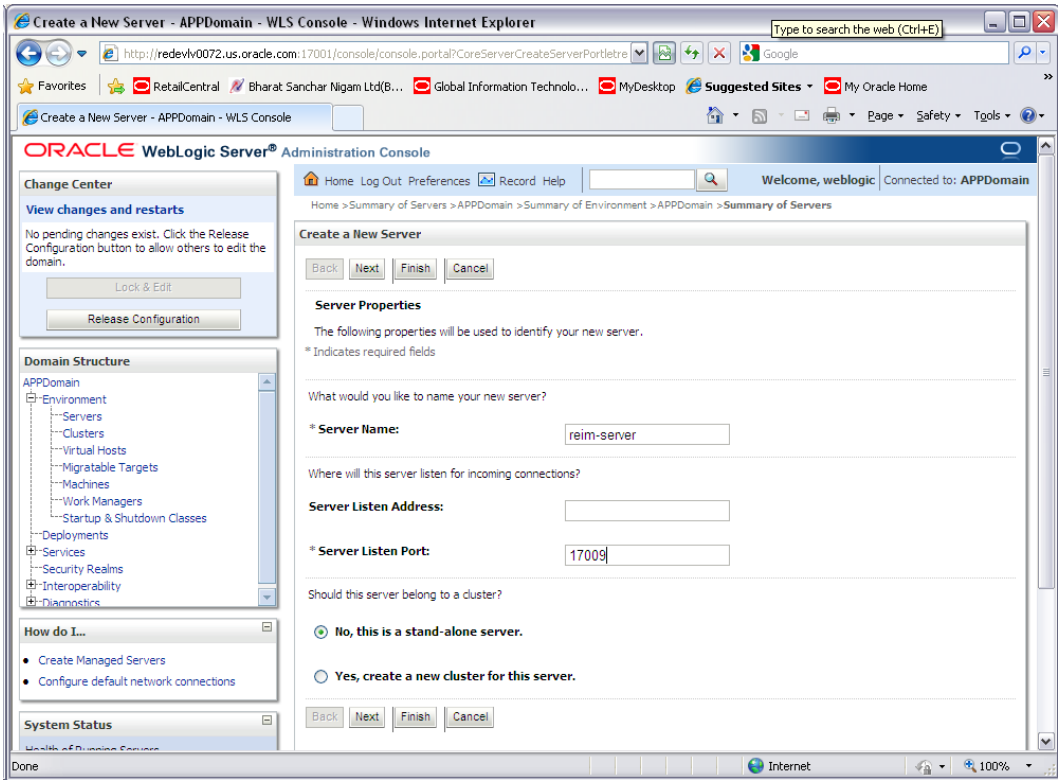
Important Note: Skip this section if a managed server already exists for Oracle Retail Invoice Matching.

Before running the application installer, you must install the managed server in WebLogic if it was not created during the domain install.

1. Log in to the Administration Console.



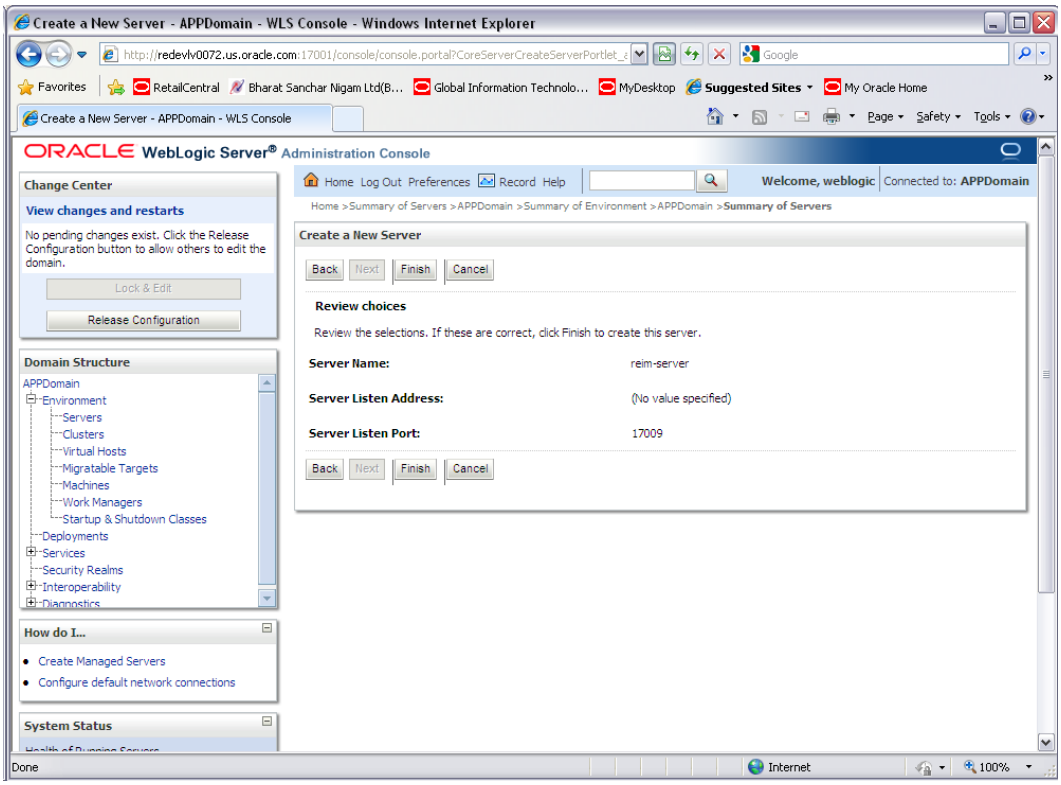
2. Click **Lock & Edit**.
3. Navigate to Environment > Servers and select new tab of the servers on the right side.



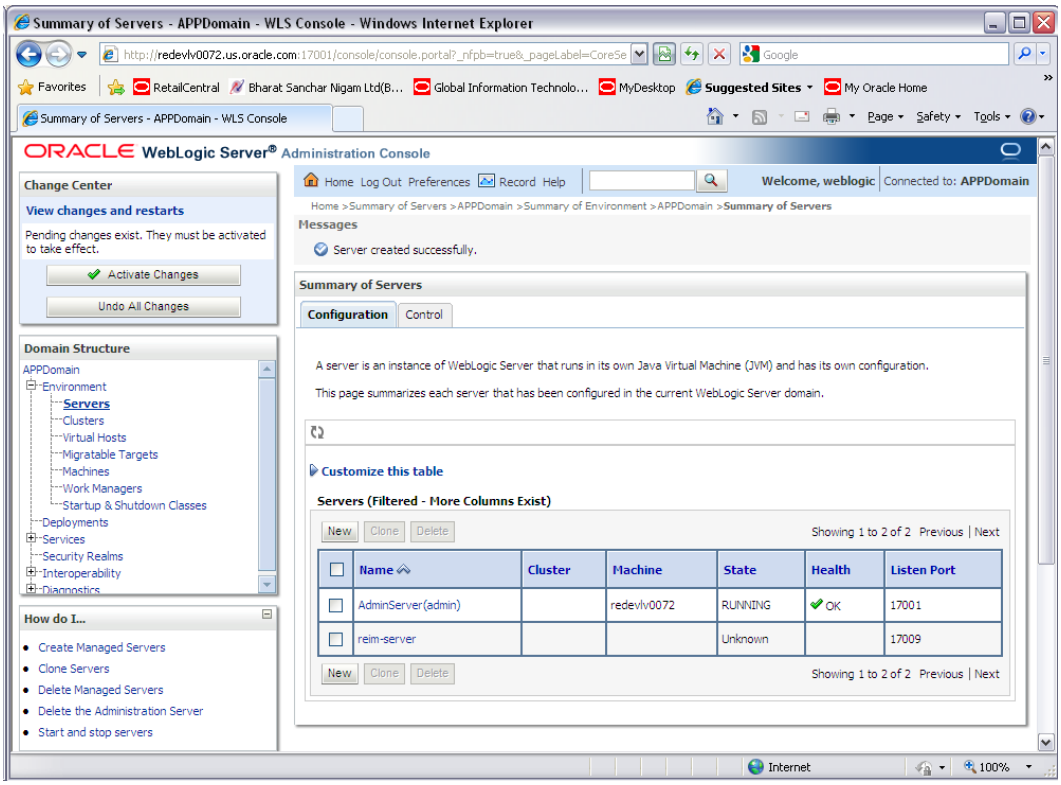
4. Set the following variables:
   - **Server Name**: These should be some name specific to your application targeted (for example, reim-server).

     Server Listen Address: <weblogic server> (for example, redevlv0072.us.oracle.com)
   - **Server Listen Port**: A free port. Check for availability.

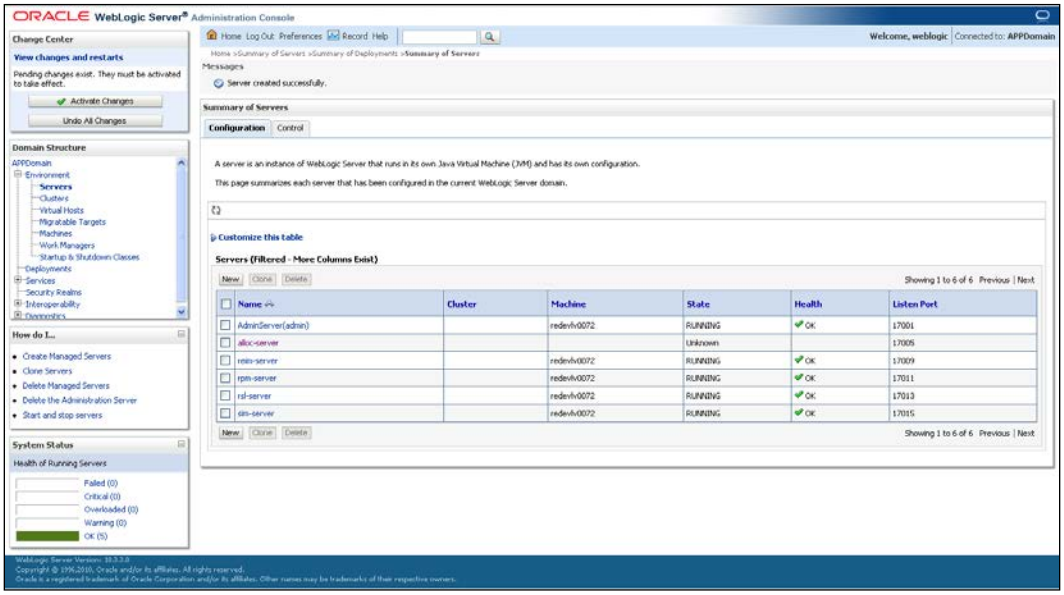
     A suggestion is to increment the AdminServer port by two and keep incrementing by two for each managed server (for example, 17003, 17005, 17007, 17009, and so on.)
5. Click **Next**.



6. Click **Finish**.



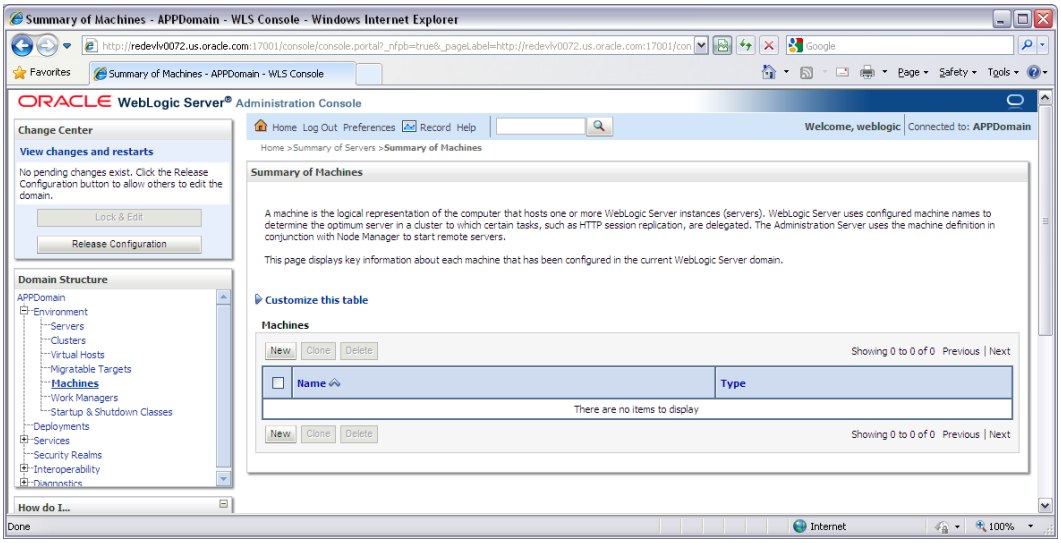
7. Click **Activate Changes** on the left side.



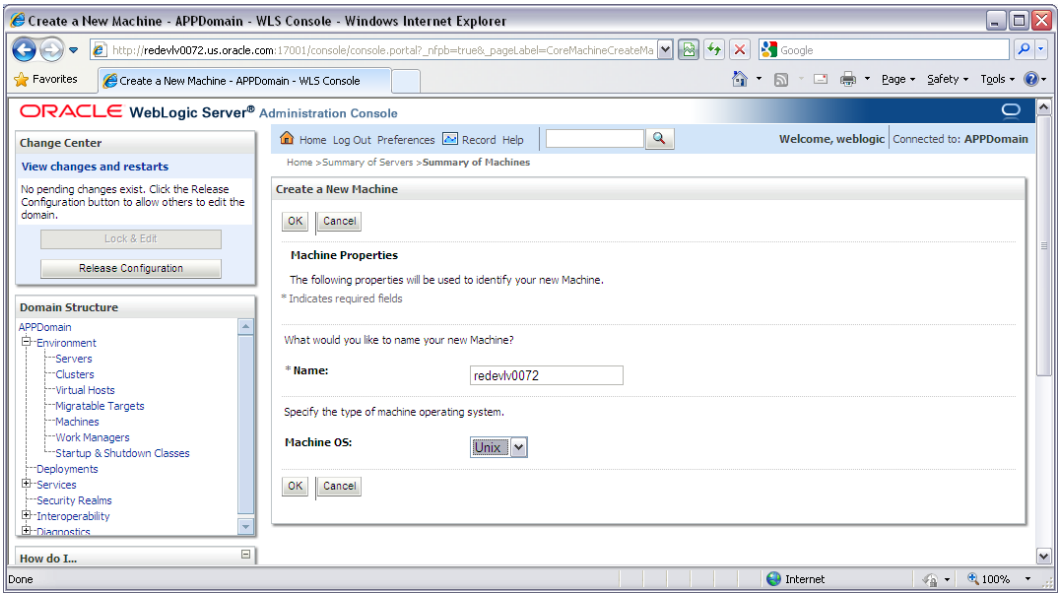
Install Node Manager

Install Node Manager if it was not created during domain install. The node manager is required so that the managed servers can be started and stopped through the Administration Console. Only one node manager is needed per WebLogic install.

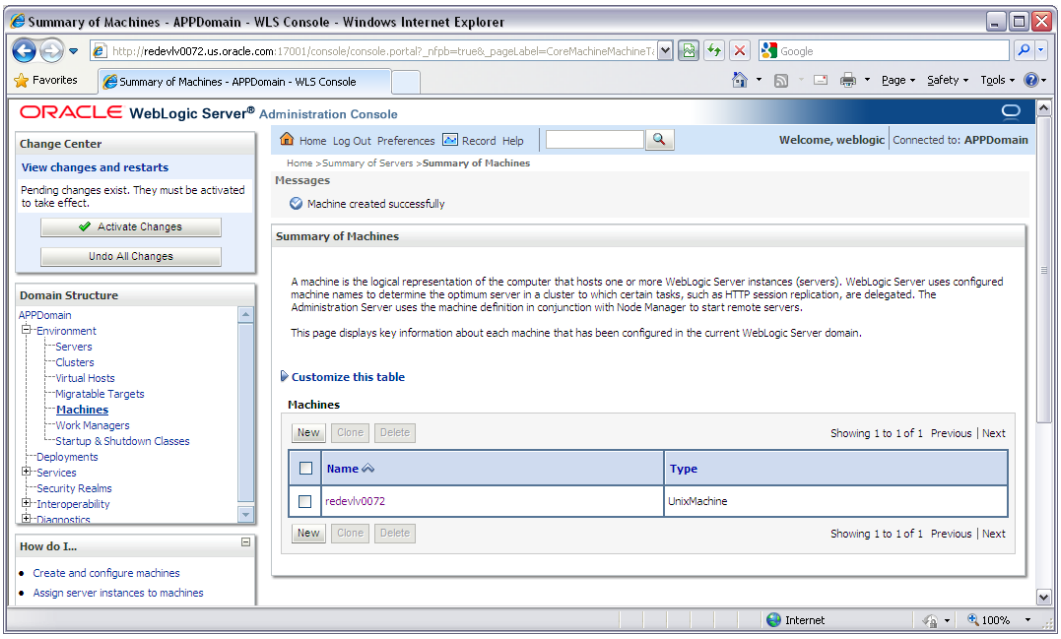
1. Log in to the Administration Console.
2. Click **Lock & Edit** and navigate to Environments > Machines.



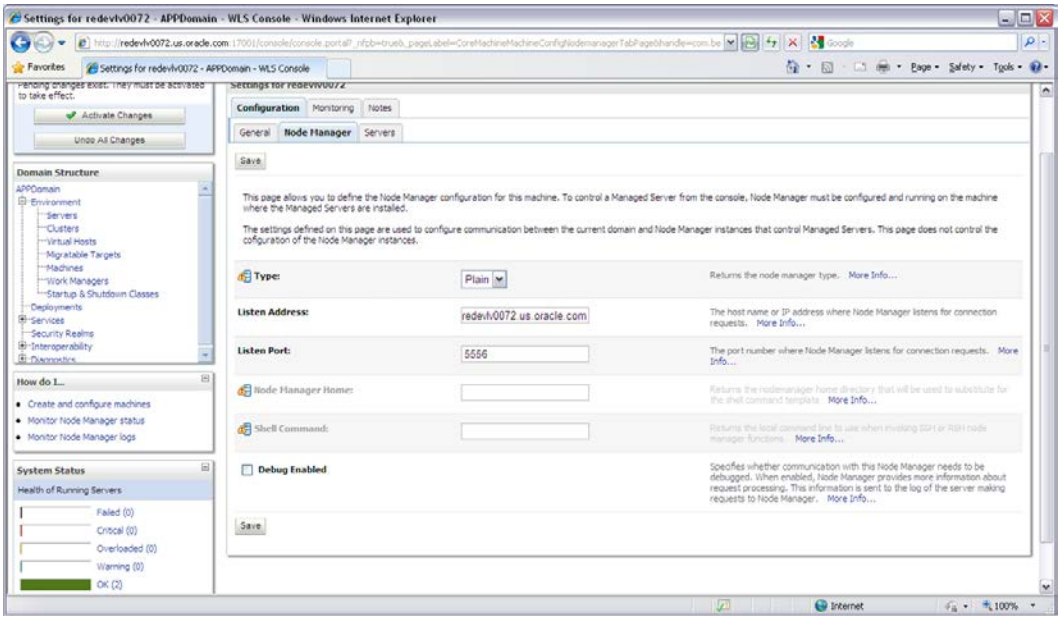
3. Click **New**.



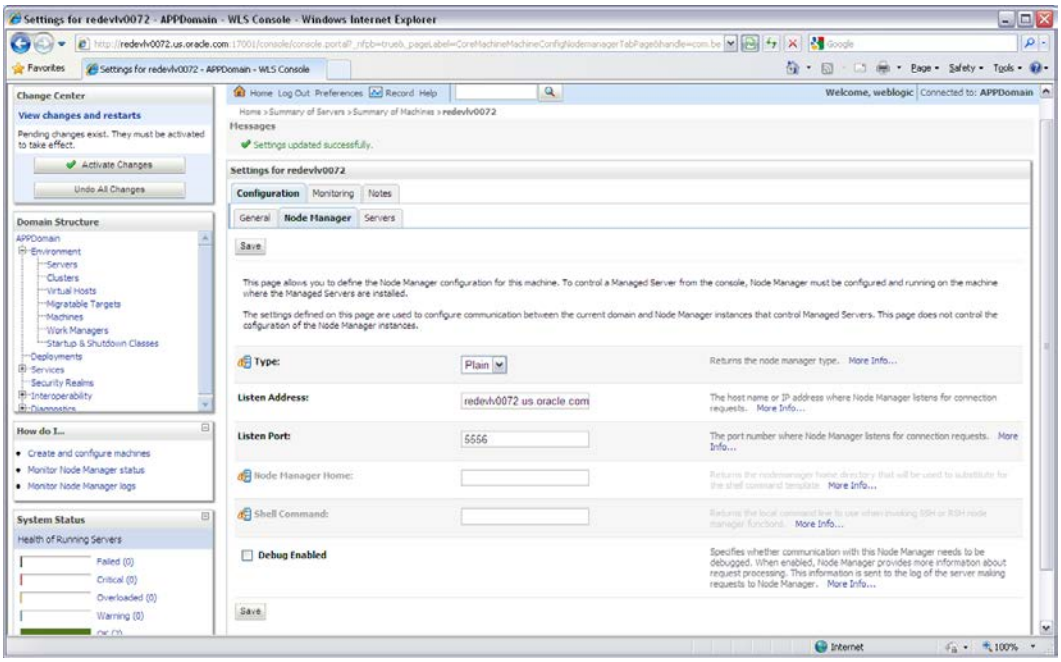
4. Set the following variables.
   - **Name**: Logical machine name
   - **Machine OS**: UNIX
5. Click **OK**.
6. Click on the machine created.



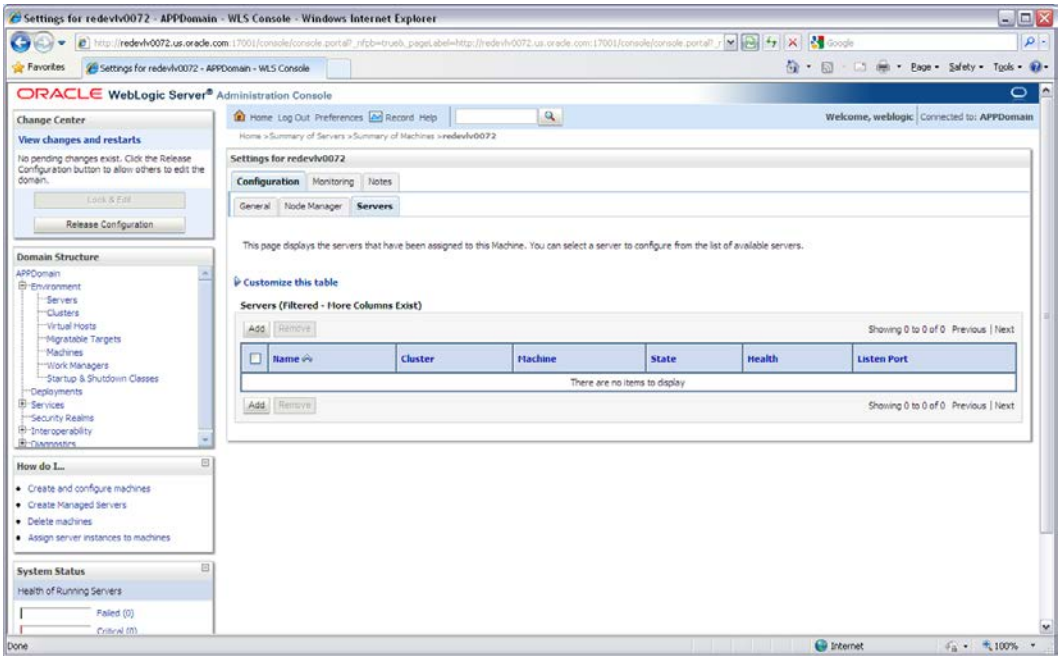
7. Click the Node manager tab and update the details below.
   - **Type**: Plain
   - **Listen Address**: redevlv0072.us.oracle.com
   - **Listen Port**: Default port (for example, 5556) or any available port.



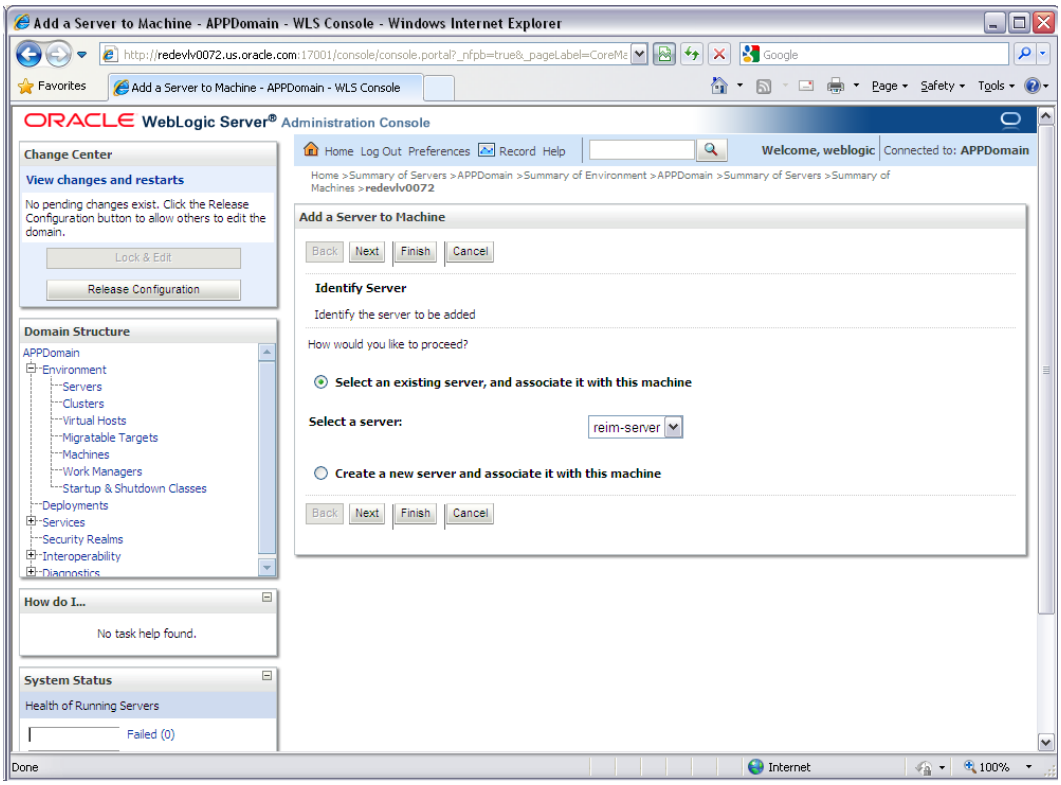
8. Click **Save**.



9. Click **Activate Changes**.
10. Click **Lock & Edit**.
11. Navigate to Environments->machines->click on the machine name and select the Servers tab.



12. Add the managed servers that need to be configured with the Node Manager. Save the changes.
13. Click **Add**.



14. Set the following variables:
    - Server: reim-server
15. Click **Next/Finish**.

16. Click **Activate Changes**.

> **Note:** To activate changes the server needs to be stopped as follows.
>
> $WLS_HOME/user_projects/domains/<APP_Domain>/bin/stopManagedWebLogic.sh reim-server ${server_name}:${server_port}
>
> Go to the managed server that is being added to the machine and click the Server Start tab. In the Class Path box, add the following:
> <full-path-to-domain>/servers/<managed-server>
> For example: /u00/webadmin/product/10.3.x/WLS/user_projects/domains/<Domain_name>/servers/reim-server

17. Start NodeManager from the server using the startNodeManager.sh at $WLS_HOME/wlserver_10.3/server/bin:
18. Edit the nodemanager.properties file at the following location with the below values:
    $WLS_HOME/wlserver_10.3/common/nodemanager/nodemanager.properties
    - SecureListener=false
    - StartScriptEnabled=true
    - StartScriptName=startWebLogic.sh.
19. NodeManager must be restarted after making changes to the nodemanager.properties file.

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

Start the Managed Servers

To start the managed servers, do the following.

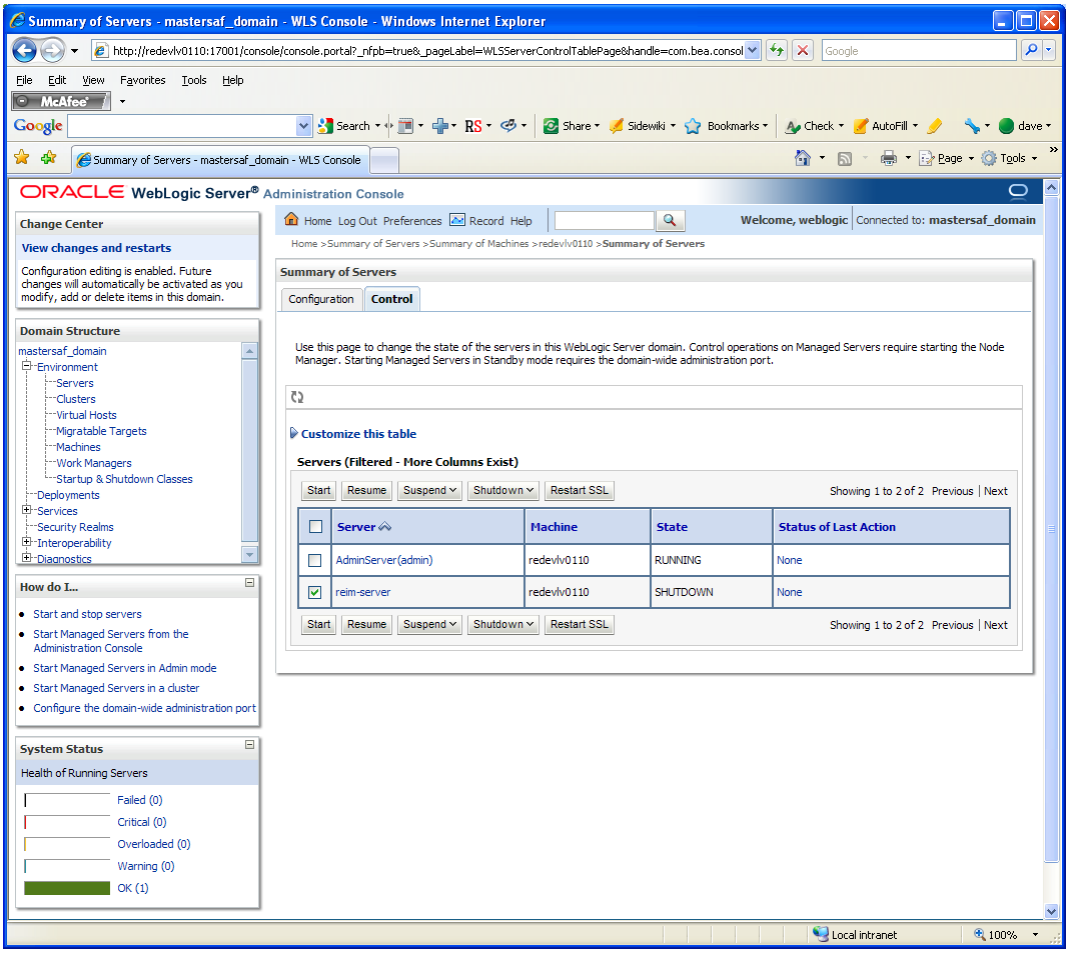
1. Start the Node Manager from the command line if not already done from starting the node manager in the section above this.

   `$WEBLOGIC_HOME/wlserver_10.3/server/bin/startNodeManager.sh`

   After the Node Manager is started, the managed servers can be started through the Administration Console.

2. Navigate to Environments->Servers->select reim-server server and click the Control tab.

3. Click the managed server (reim-server) you want to start and press the **Start** button to start the managed server you clicked to start.



4. Update in weblogic console->servers->reim-server->server start tab->Classpath and Arguments, with the following:

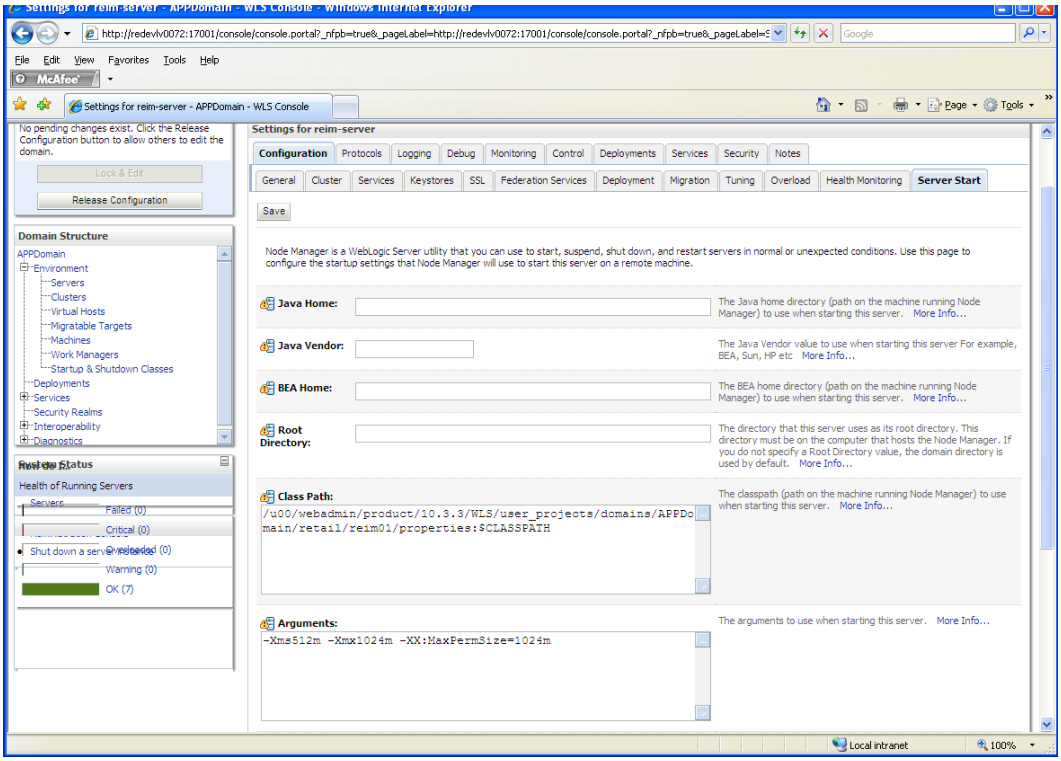
   CLASSPATH: `full_path_to_domain>/retail/<context_root>/properties:$CLASSPATH`

Arguments for 1.6.0+ JDK

-Xms512m -Xmx1024m -XX:MaxPermSize=1024m

Arguments for Jrockit

If Jrockit is used:-Xms512m -Xmx1024m



5. Export WEBLOGIC_DOMAIN_HOME=<full_path_to_domain>
6. 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.x/WLS/user_projects/domains/APPDomain/servers
/reim-server/tmp/_WL_user/reim01/-" {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";}
```

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

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 (reim13application.zip). There should be a minimum of 120 MB disk space available for the application installation files.

   Example: /u00/webadmin/media/reim

   This location is referred to as INSTALL_DIR for the remainder of this chapter.
2. Copy reim13application.zip to INSTALL_DIR and extract its contents.

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. Insert into $WEBLOGIC_HOME/wlserver_10.3/server/lib/weblogic.policy file, the same ReIM entries for java security permissions you 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 (11.1.1.6). However, OID 10g (10.1.4) is also supported.

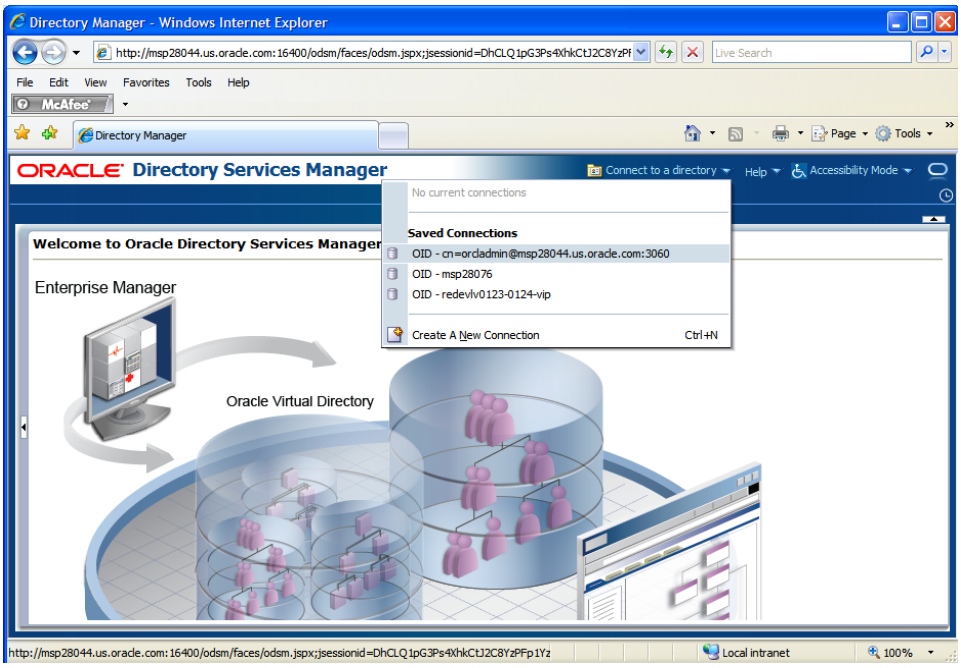
2. Create a Group called “reim”. All users need to be a member of this group in order to login to the ReIM application.

   Note: The ReIM code looks for a group named “reim” so it is imperative that the group be named “reim”.

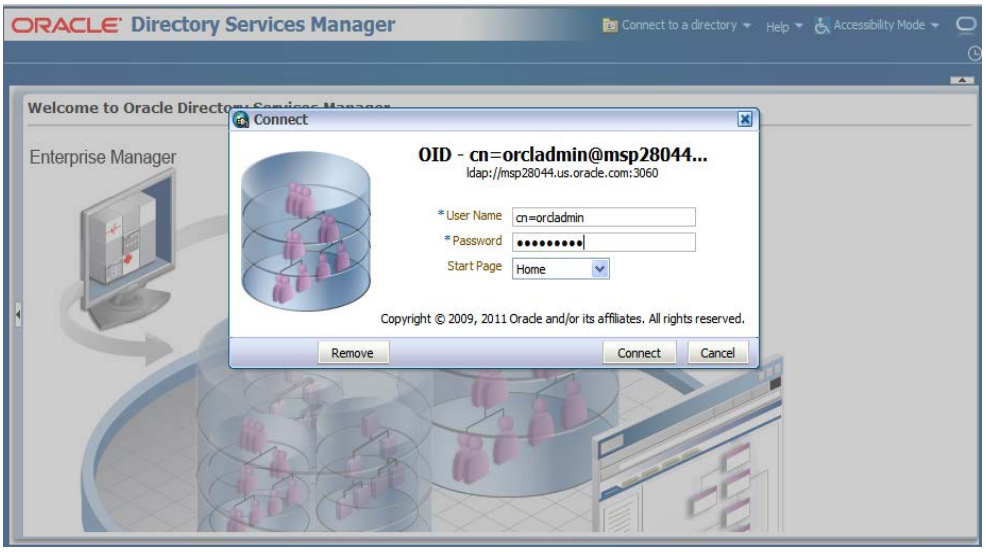
   Example: Using OID 11.1.1.6, the steps to follow are:

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

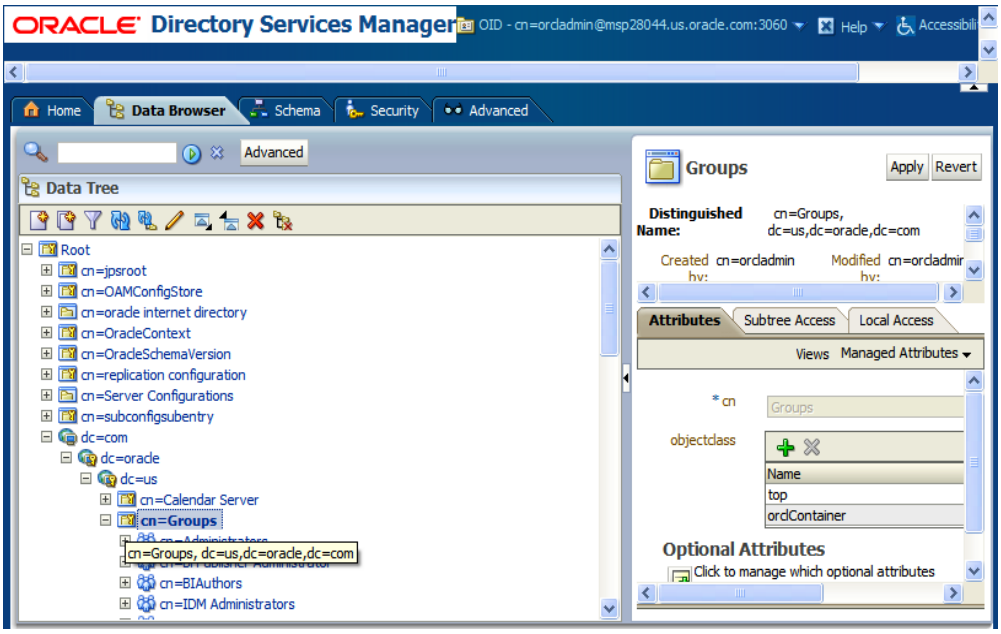
   b. Click Connect to a directory and select your OID directory.



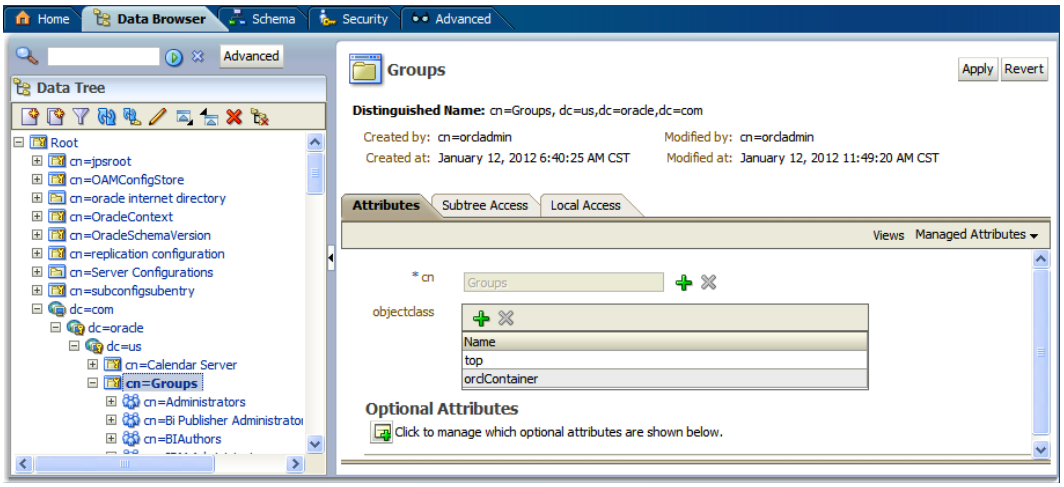
c. From the OID Connect dialog, click the Connect button.



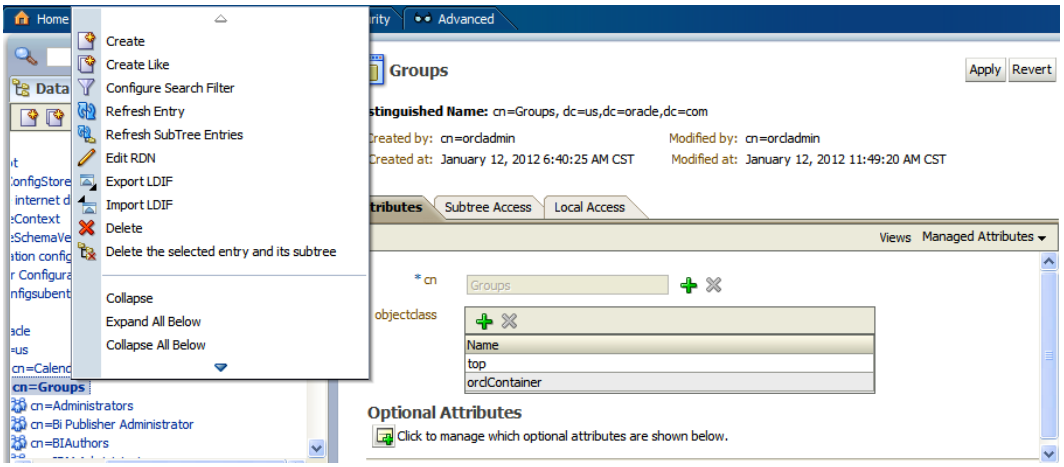
d. From the Oracle Internet Directory Welcome Screen, select the Data Browser tab. The DataBrowser tree shows how to find the "cn=Group" element



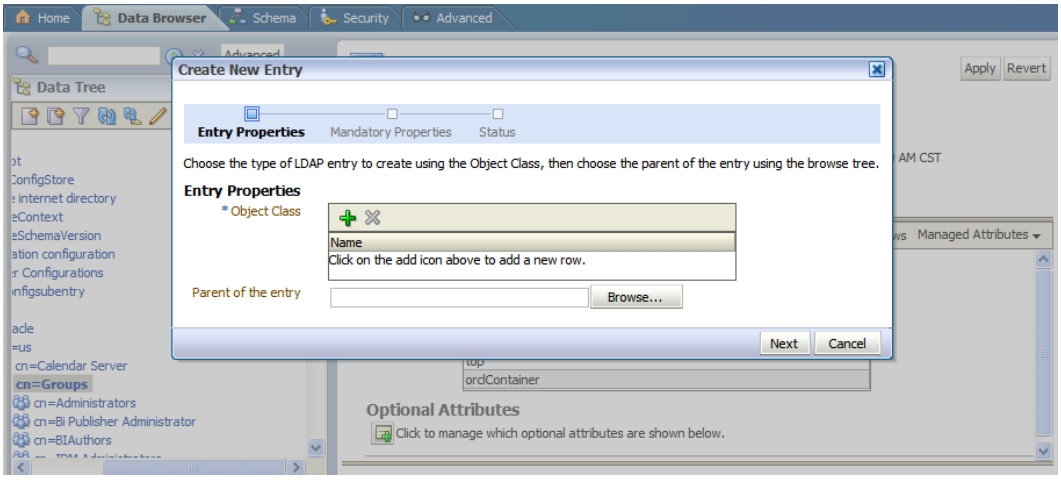
e. From the Data Tree panel of the ODSM screen, navigate to dc=com,dc=oracle,dc=us,cn=Groups.



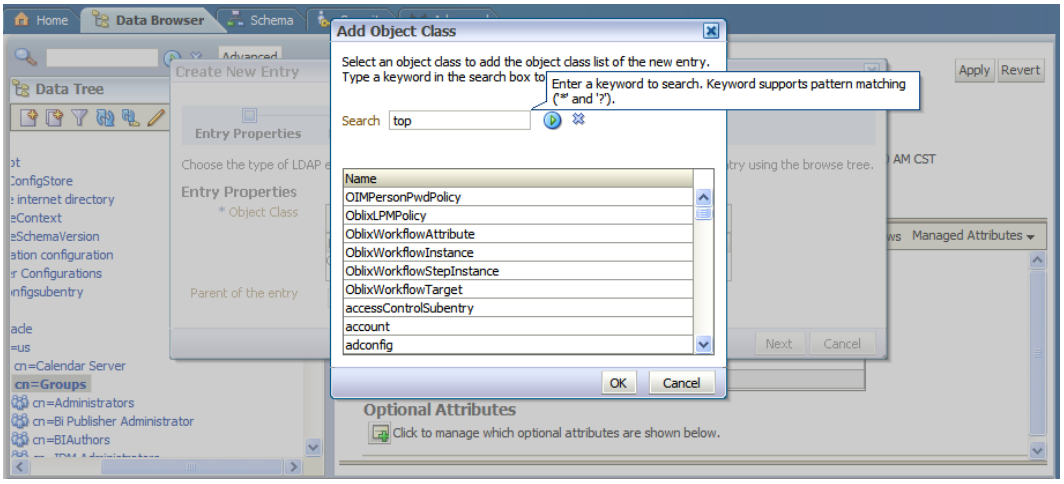
f. Right-click cn=Groups and select Create.



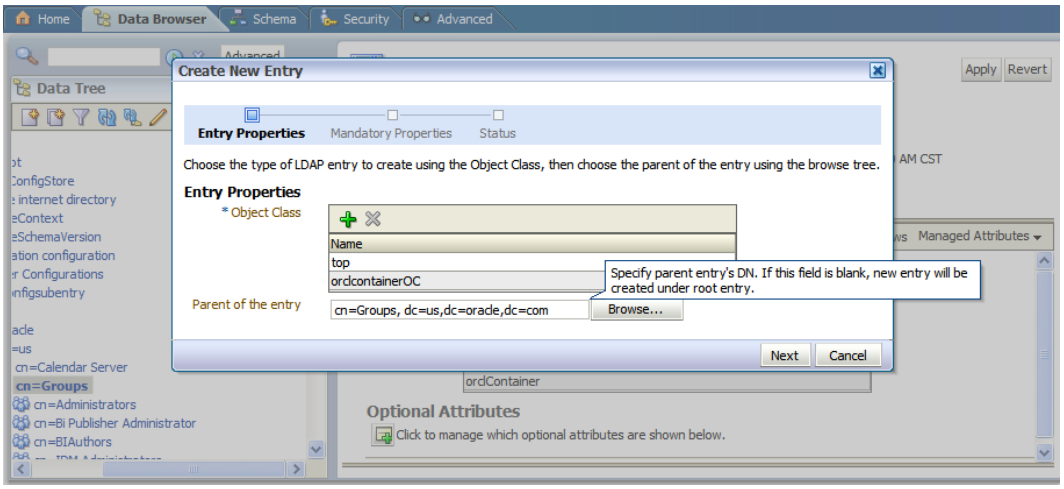
g. From the Create New Entry dialog, click the + icon to see the Object Classes in the dropdown menu.



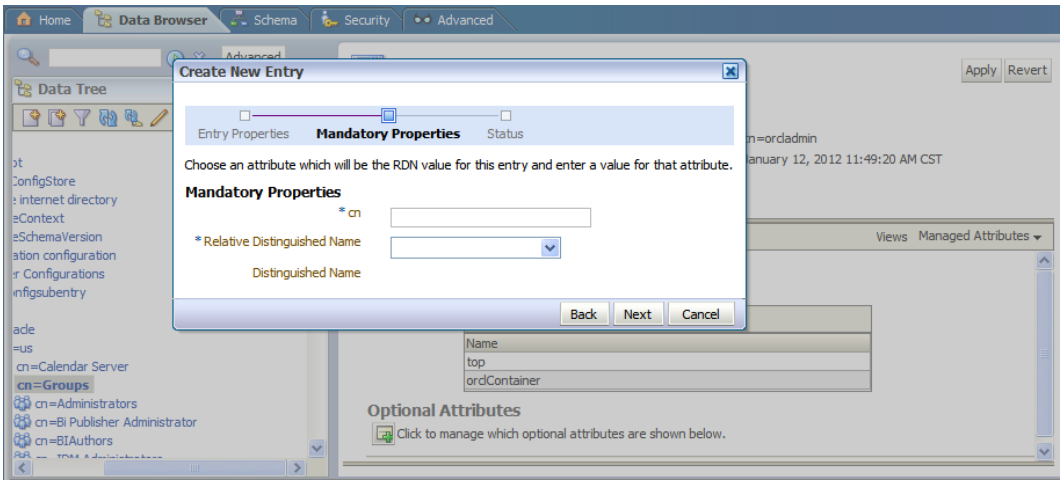
h. From the Add Object Class drop down menu select top and orclContainer.



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

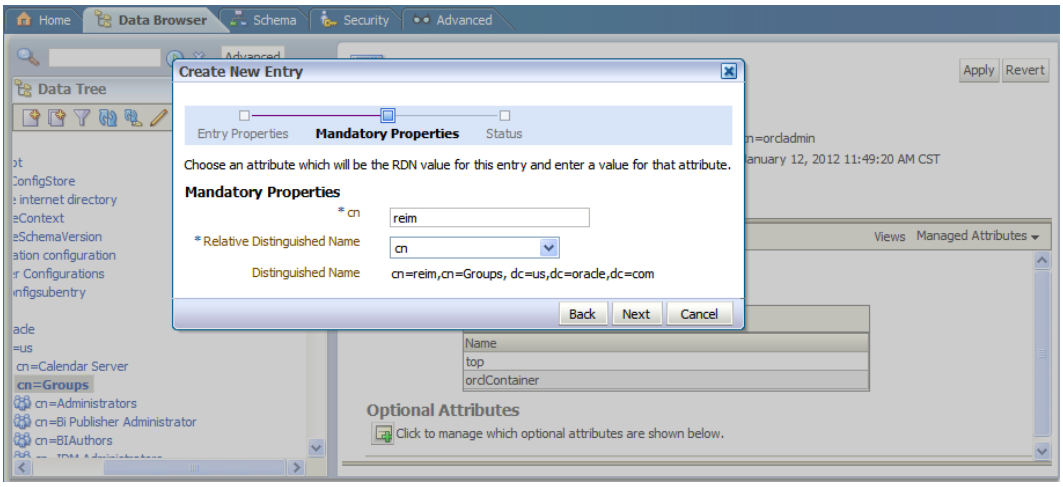


j. Click Next.

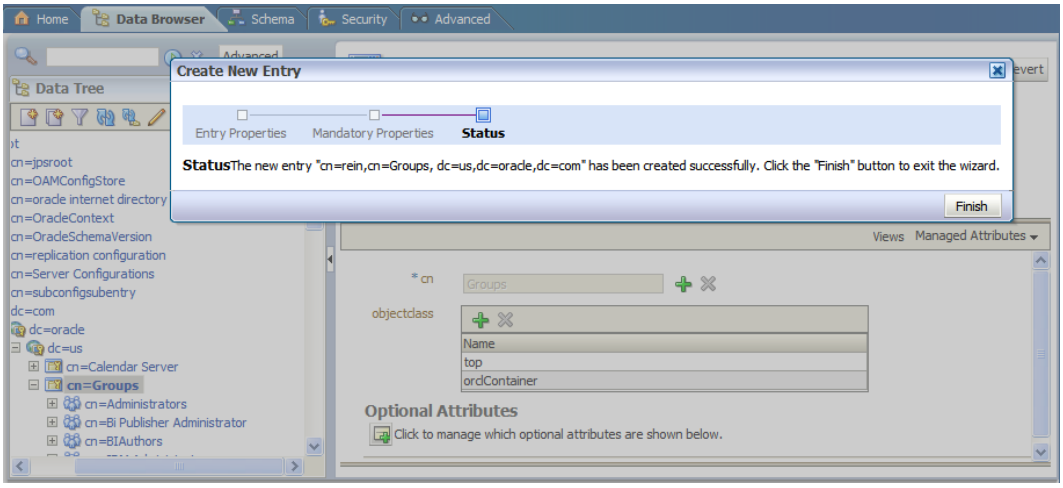


k. On the "*cn" text field enter: "reim".

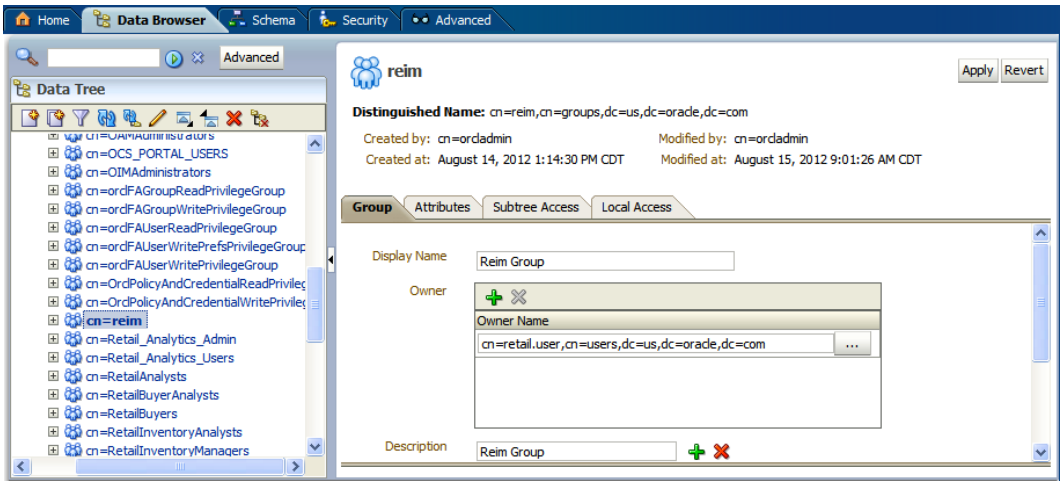
l. On Resolved Distinguished Name field enter: cn and click Next.



m. Click Finish.



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



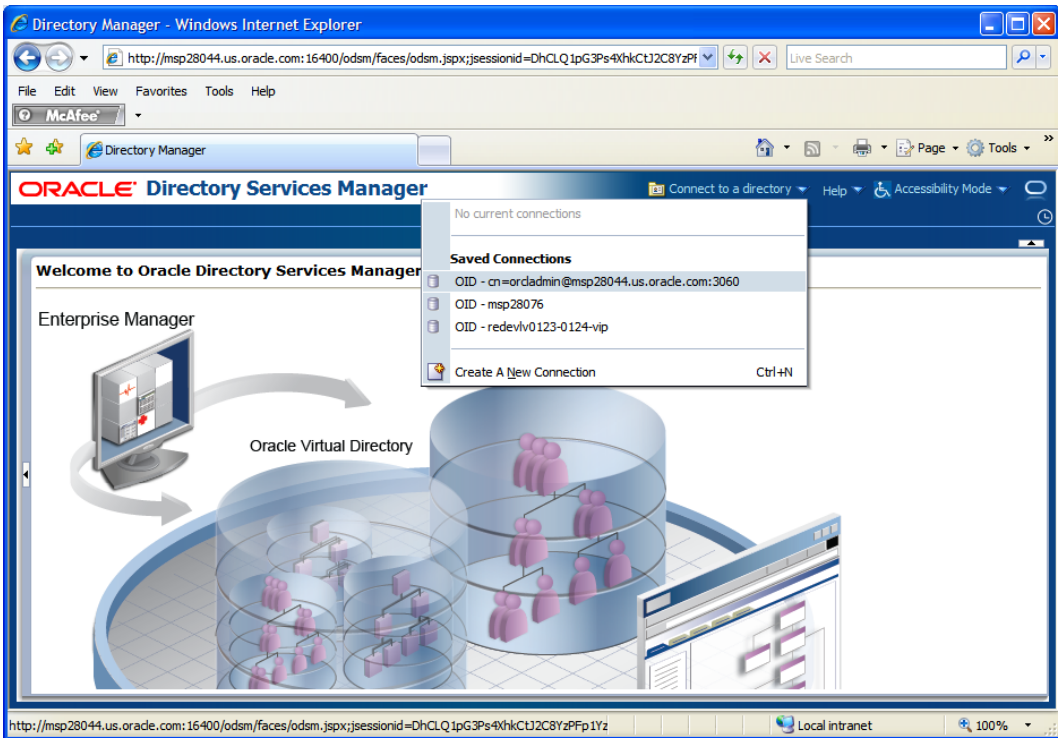
3. Create an LDAP connection user with the necessary rights to do sub-tree searches on your users and groups respectively. This user can be named anything but "REIM.ADMIN" is used in this document. This same user should be given as an input for 'Search User DN' on the 'LDAP Directory Server Details' 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).

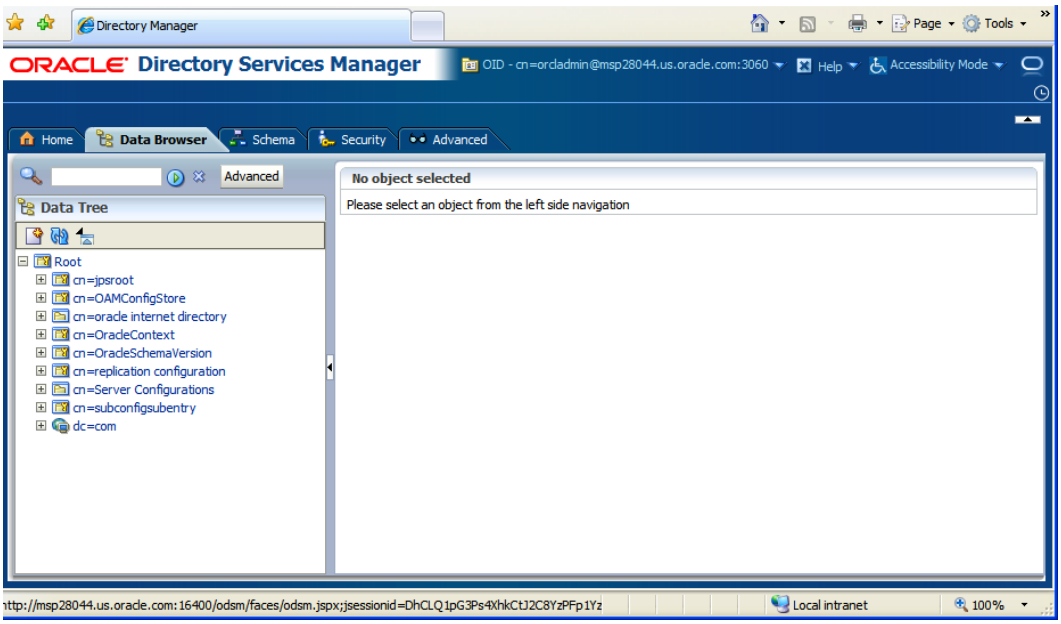
b. Click Connect to a directory and select your OID directory.



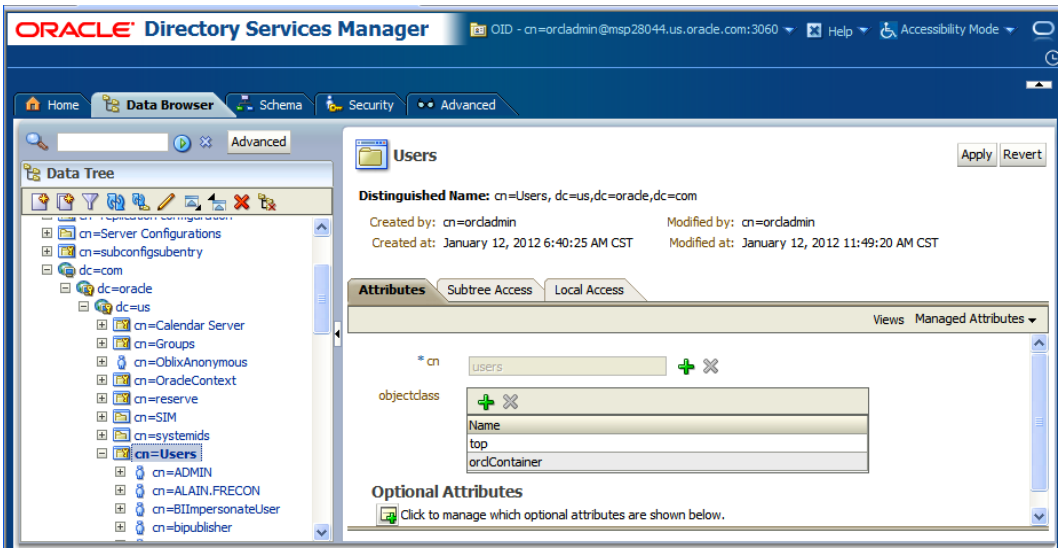
c. From the OID Connect dialog, click the Connect button.

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

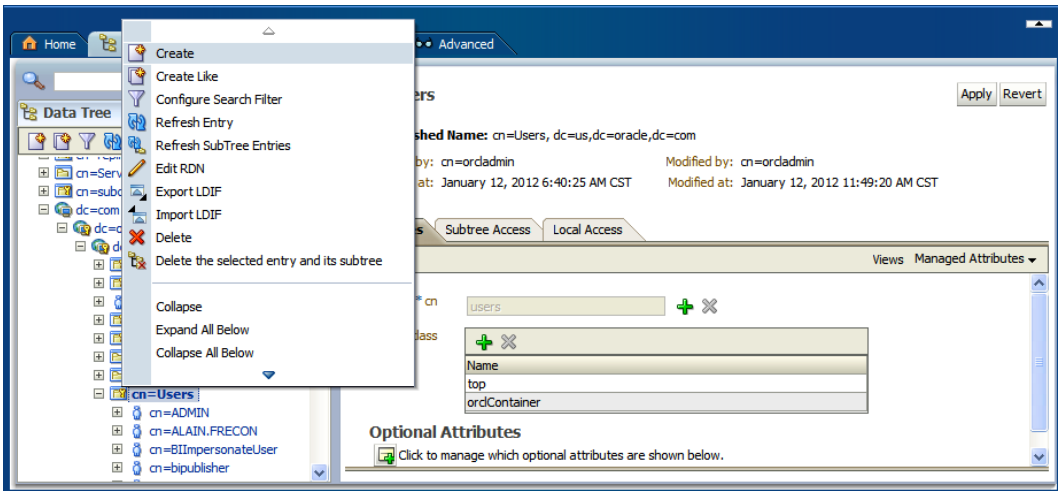
The Data Browser tree shows how to find the "cn=Users" element.



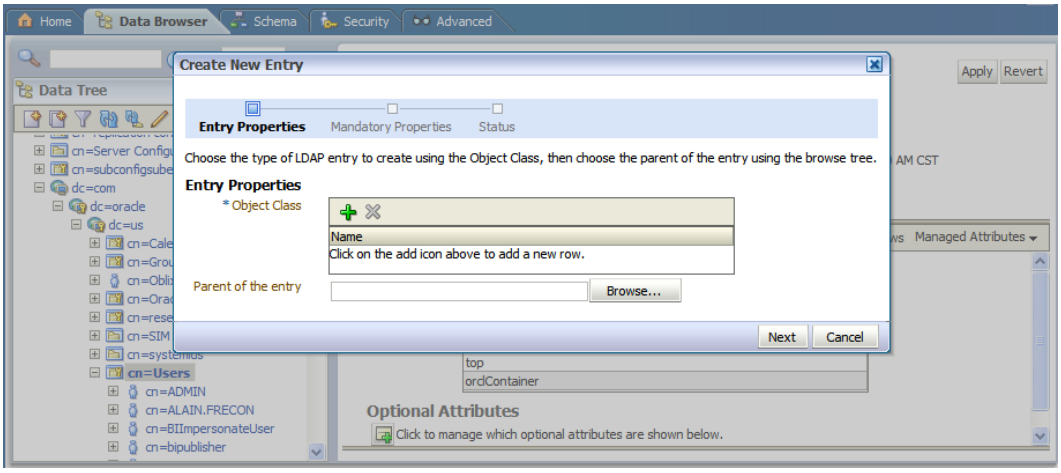
e. From the Data Tree panel of the ODSM screen, navigate to "Users" branch.



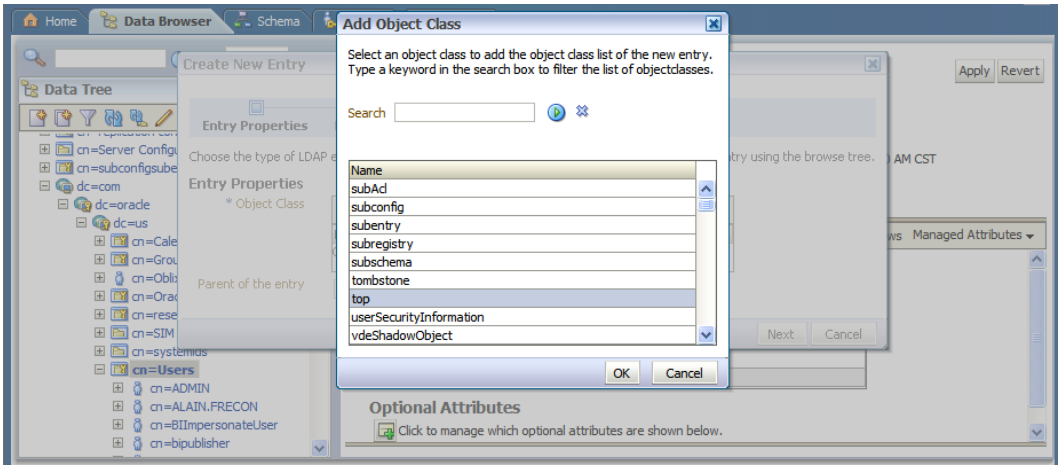
f. On the "Users" screen , press right mouse button with "cn=Users" highlighted and select "Create" from the drop down menu panel



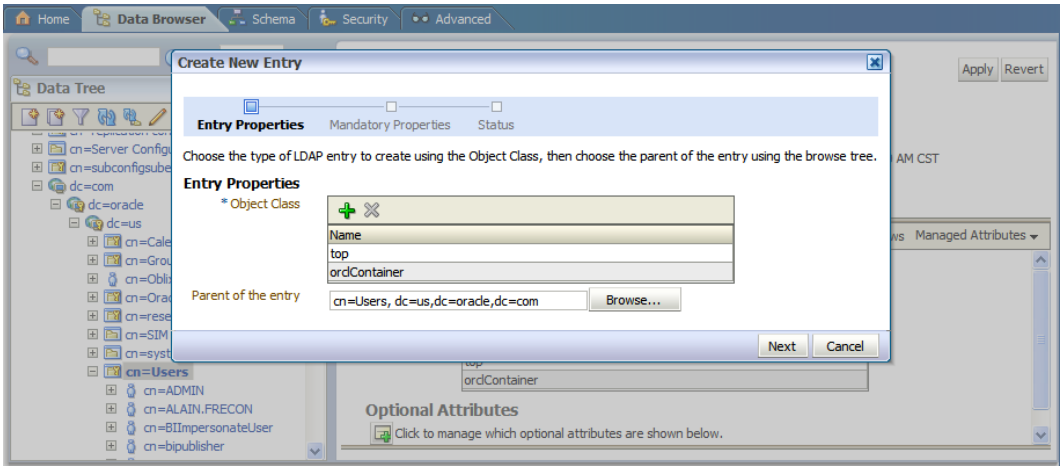
g. In the Object Class field, click the + icon.



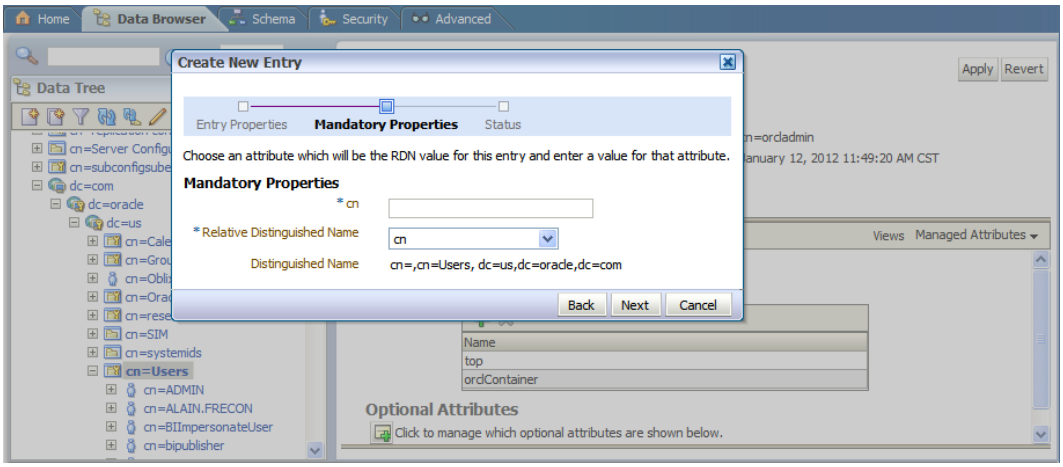
h. From the Add Object Class menu, select the "top" and "orclContainer" object classes.



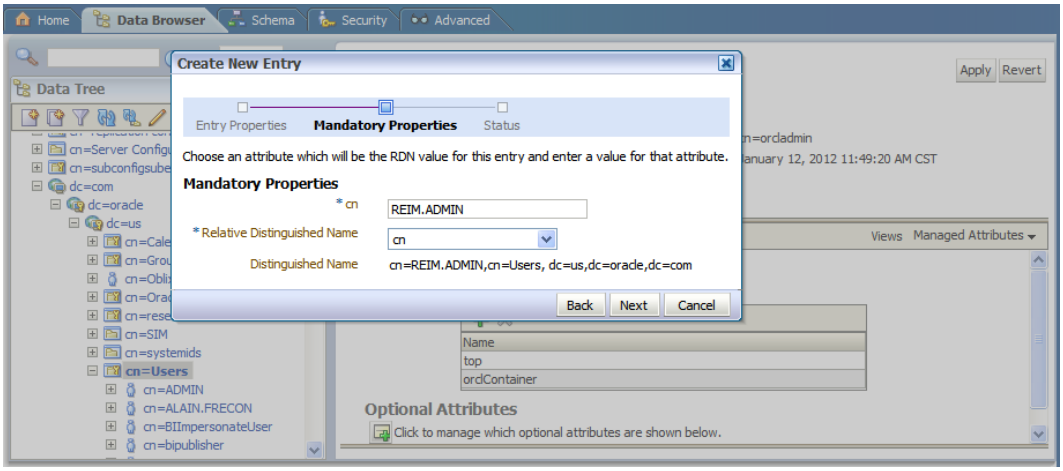
i. In the Parent of the Entry field enter the following:
cn=Users,dc=us,dc=oracle,dc=com



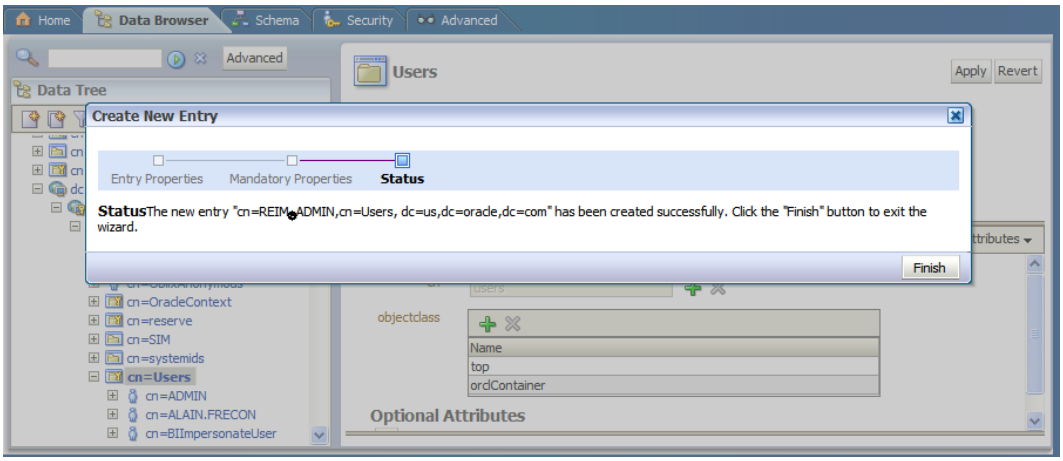
j. Click Next. The Mandatory Properties dialog is displayed.



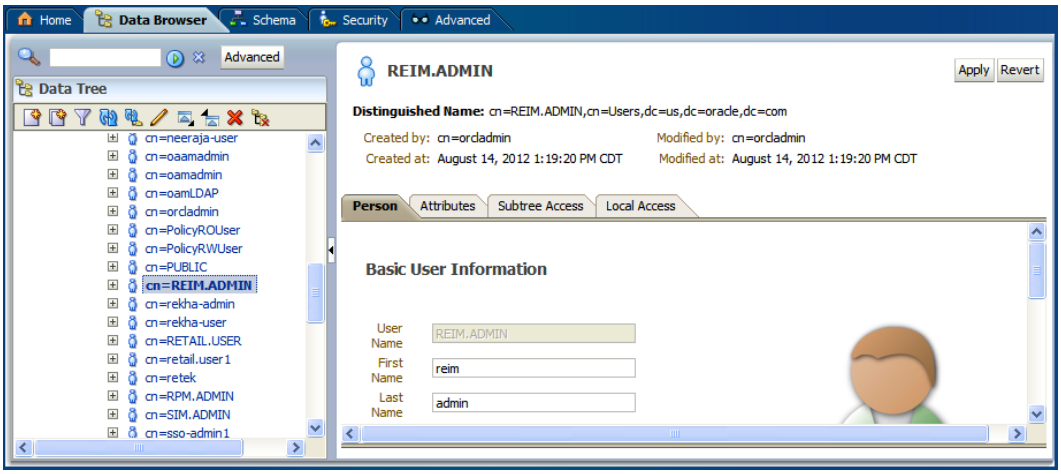
k. From Mandatory Properties dialog, enter "REIM.ADMIN" in the cn field and verify that cn is selected in the Relative Distinguished Name field. Click Next.



l. Make sure the information on screen is correct. Press “Finish” button to create the “REIM.ADMIN” user.



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

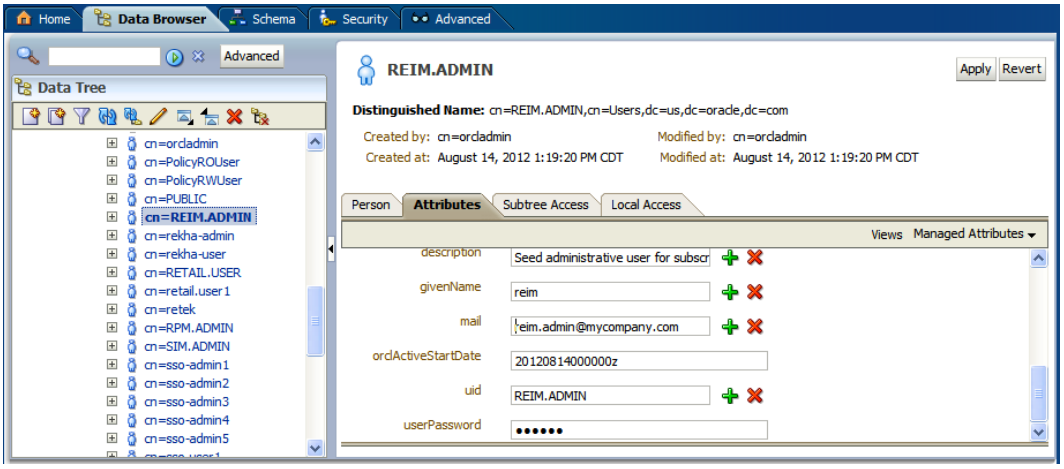


m. Click the Person tab and enter the following Basic User Information:

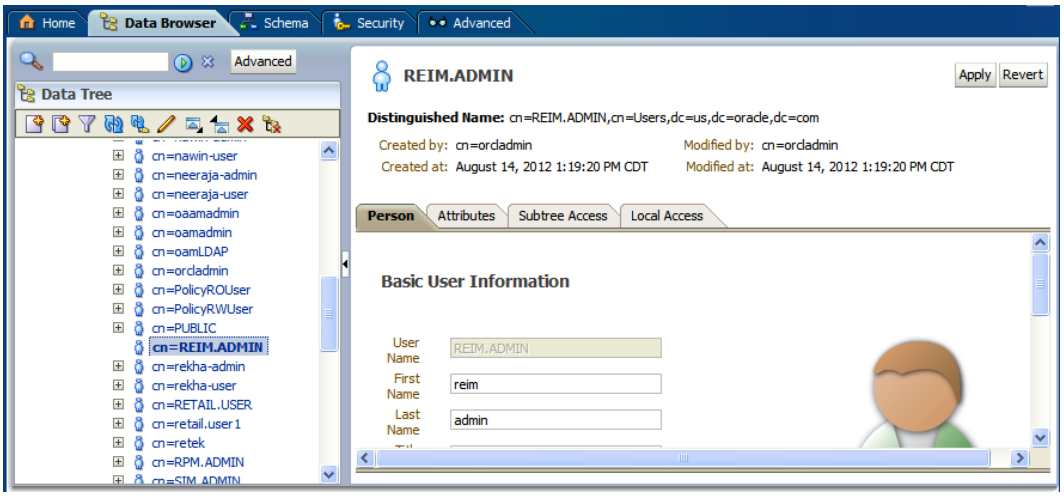
- First Name: <reim>
- Last Name: <admin>
- Email Address: <reim.admin@mycompany.com>

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

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



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



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

I f you are installing other MOM 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: Preferedcountry 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

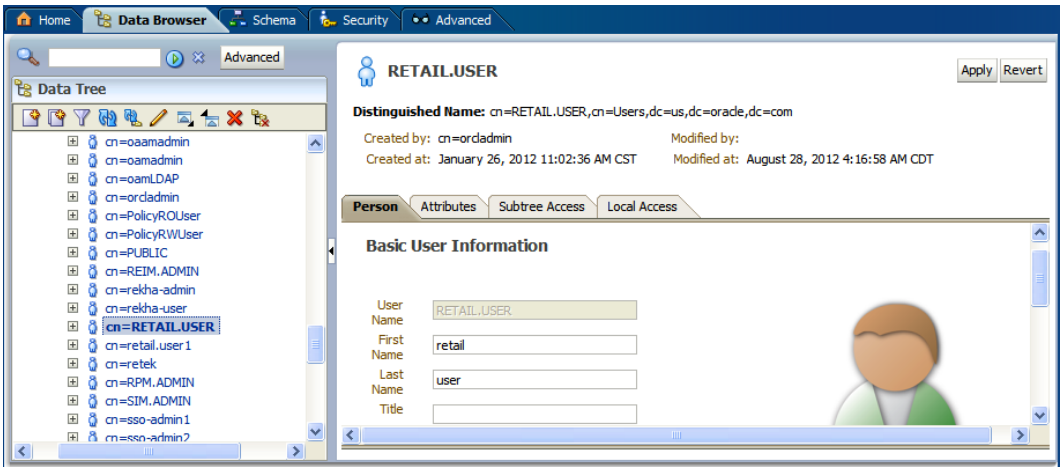
These are considered as the mandatory attributes for the login user (example:RETAIL.USER) which is listed in ldap.properties located on the ReIM server at <DOMAIN_HOME>/servers/<reim-server>/tmp/_WL_user/<reim13>/<xstkfu>/reim13.war/WEB-INF/classes/com/retek/reim/ldap.properties

You can see the following list from ldap.properties:

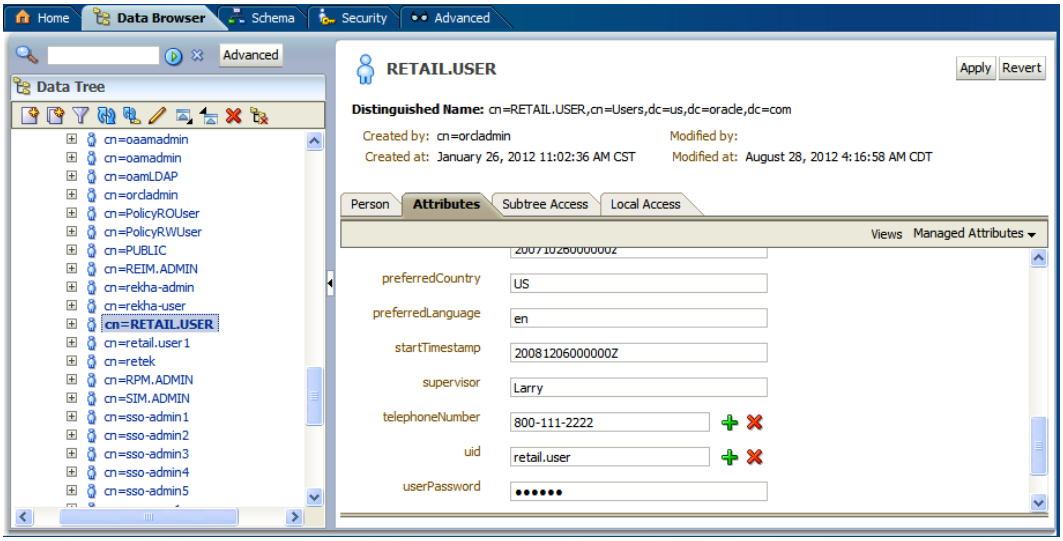
- login_id_attribute_name=uid
- user_first_name_attribute_name=givenname
- user_last_name_attribute_name=sn
- user_email_attribute_name=mail
- user_password_attribute_name=userpassword
- user_language_attribute_name=preferredLanguage
- user_country_attribute_name=preferredcountry
- user_main_key=cn
- # 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).



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 other locale is used, the value needs to be entered based on that locale.



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

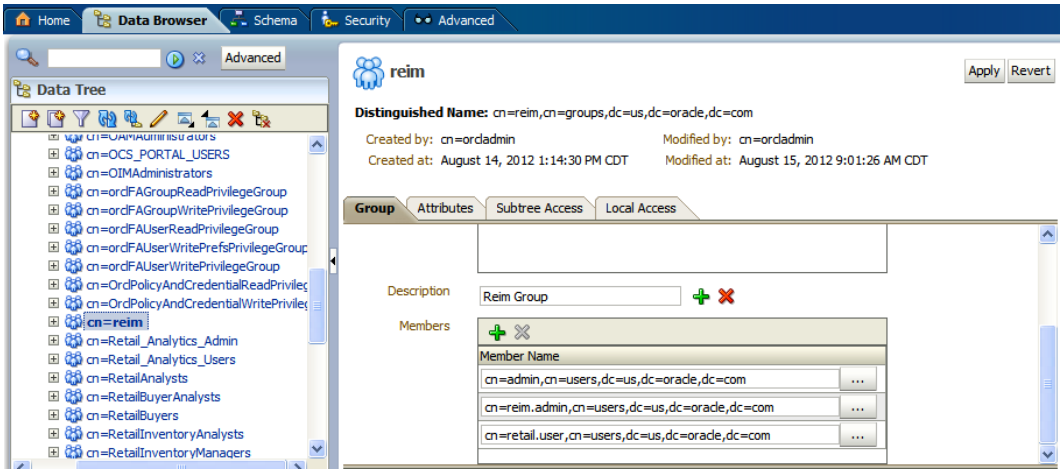
5. Assign the user "RETAIL.USER" and any other users which need to login to ReIM Application to the "reim" group

   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:



c. Press the "Apply" button to save your changes.

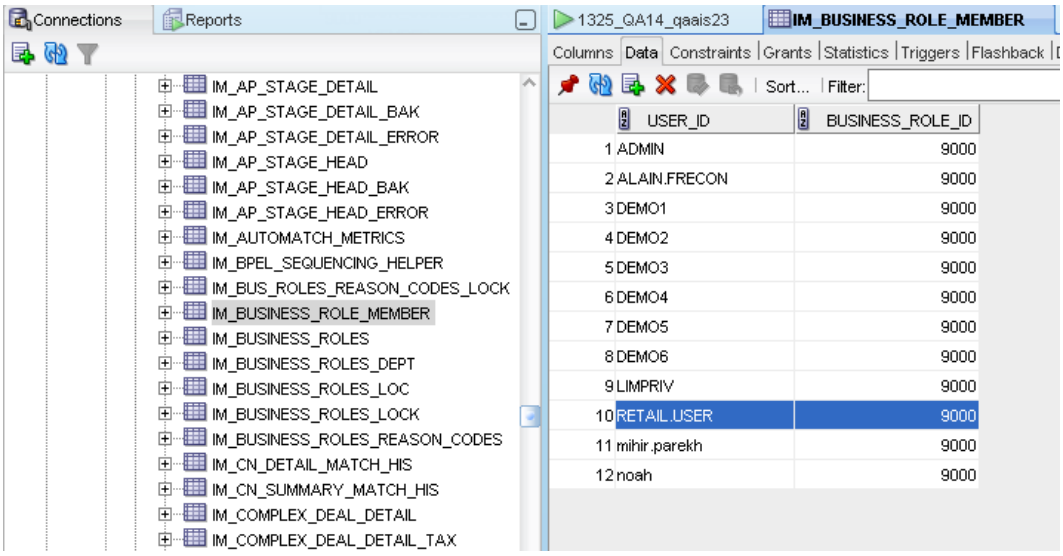
6. Add new user (Example:RETAIL.USER) to the database if not already there.

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

```
insert into im_business_role_id
(USER_ID, BUSINESS_ROLE_ID)
values ('RETAIL.USER', 9000);
```

Note: The above business role ID=9000 value should be mapped with IM_BUSINESS_ROLES TABLE for that particular user (Example: RETAIL.USER).

It may vary based on the mapping in IM_BUSINESS_ROLES_TABLE for the user you are inserting the record.



You are ready to Login to ReIM.

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.

Use the sample retailuserobjectclass.ldif below to create the attribute "preferredCountry", create an 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

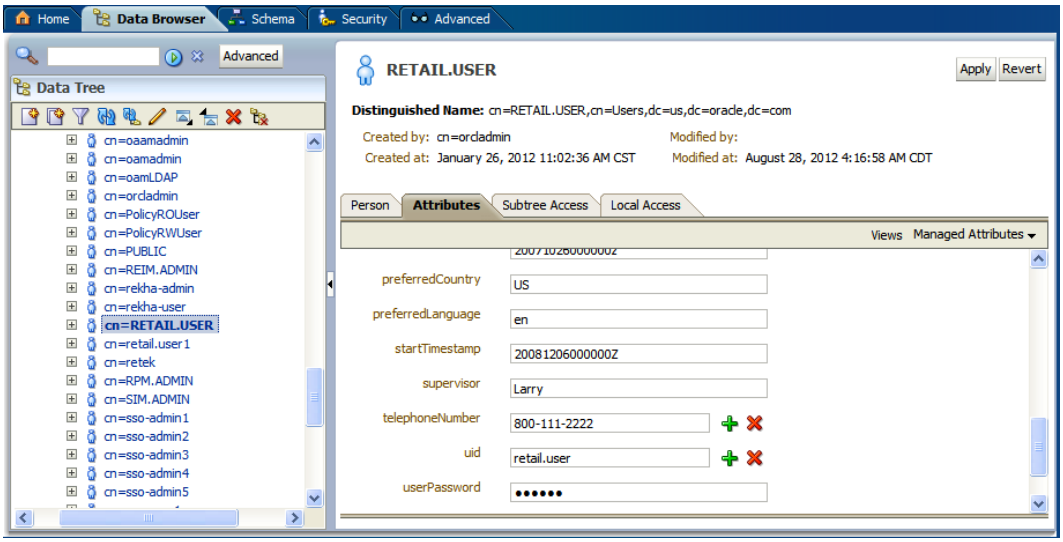
```
# Oracle Retail - ReIM User LDAP Schema
# You WILL need to make some changes to this based upon your #environment and
user you want to add
#
# This schema uses the OID tree starting with:
#       1.3.6.1.4.1.12388.897
# Where 1.3.6.1.4.1.12388 identifies definitions as
# belonging to the private 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: (1.3.6.1.4.1.11380.97.11
  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.



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 6.0 (1.6.0) JDK or Jrockit 1.6 Build 28 or higher (within the 1.6 code line) for Linux and Solaris OS only.
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.x/WLS/user_projects/domains/132_mck_soa_domain).
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 (reim13install.<timestamp>.log).
6. Prior to running the ReIM batch programs, run the following command.

```
cp
$WEBLOGIC_DOMAIN_HOME/retail/reim13/properties/com/retek/reim/reim.properties
$WEBLOGIC_DOMAIN_HOME/retail/reim13/batch/WEB-INF/classes/com/retek/reim/
```

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.

Oracle Configuration Manager

The Oracle Retail OCM Installer packaged with this release installs the latest version of OCM.

The following document is available through My Oracle Support Access My Oracle Support at the following URL:

`https://support.oracle.com`

Oracle Configuration Manager Installer Guide (ID 1071030.1)

This guide describes the procedures and interface of the Oracle Retail Oracle Configuration Manager Installer that a retailer runs at the beginning of the installation process.

OCM Documentation Link

`http://www.oracle.com/technology/documentation/ocm.html`

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.

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:// (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:// redevlv0072: 17009/reim01/index.jsp

Oracle Retail provides test cases that allow you to smoke test your installation. See the My Oracle support document, "Oracle Retail Merchandising Installation Test Cases" (ID 1277131.1).

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>/reim-batch.

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 6.0 (1.6.0) JDK or Jrockit 1.6 Build 28 or higher (within the 1.6 code line) installation that typically is being used by the WebLogic Application Server.

Example: export ORACLE_HOME=/u00/webadmin/product/10.3.x/WLS
export JAVA_HOME=/u00/webadmin/product/10.3.x/jdk16
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 Single Sign-On server through the regsso.sh script. See Oracle Single Sign-On 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>
           WebLogicHost host name
           WebLogicPort  admin port number
           MatchExpression *.jsp
     </IfModule>
     <Location /reim_sso >
          SetHandler weblogic-handler
     </Location>
     ```

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

     ```
     LoadModule osso_module
     "<WEBLOGIC_HOME>/Oracle_WT1/ohs/modules/mod_osso.so"
     <IfModule mod_osso.c>
         OssoIpCheck off
         OssoIdleTimeout off
         OssoSecureCookies off
         OssoConfigFile
     <WEBLOGIC_HOME>/Oracle_WT1/instances/instance1/config/OHS/ohs1/osso/osso.c
     onf
     <Location /reim_sso >
           WebLogicHost host name
           WebLogicPort port number of managed server
           require valid-user
           AuthType Osso
        </Location>
     </IfModule>
     ```

2. The descriptor files, web.xml and weblogic.xml, must be adjusted to include entries related to security constraints.

   - Your web.xml should look like this:

     ```
     <security-constraint>
               <display-name>Security Constraint</display-name>
               <web-resource-collection>
                  <web-resource-name>SecurePages</web-resource-name>
                  <description>These pages are only accessible by authorized
     users.</description>
                  <url-pattern>/reim</url-pattern>
                  <url-pattern>/reim/*</url-pattern>
     ```

```
            <http-method>GET</http-method>
         </web-resource-collection>
         <auth-constraint>
            <description>These are the roles who have access to
ReIM.</description>
            <role-name>Users</role-name>
         </auth-constraint>
         <user-data-constraint>
            <description>This is how the user data must be
transmitted.</description>
            <transport-guarantee>NONE</transport-guarantee>
         </user-data-constraint>
      </security-constraint>
      <login-config>
         <auth-method>CLIENT-CERT</auth-method>
         <realm-name>myrealm</realm-name>
      </login-config>
      <security-role>
         <description>These are the roles who have access to
ReIM.</description>
         <role-name>Users</role-name>
      </security-role>
```

- Your weblogic.xml file should look like this:

```
<security-role-assignment>
      <role-name>Users</role-name>
      <principal-name>users</principal-name>
   </security-role-assignment>
   <security-permission>
      <description>ReIM Security Permissions</description>
      <security-permission-spec>
          grant { permission java.net.SocketPermission "*", "resolve";  };
      </security-permission-spec>
   </security-permission>
```

Add "-Xms512m -Xmx1024m -XX:MaxPermSize=1024m -Dweblogic.http.enableRemoteUserHeader=true") to server start of reim-server.

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).

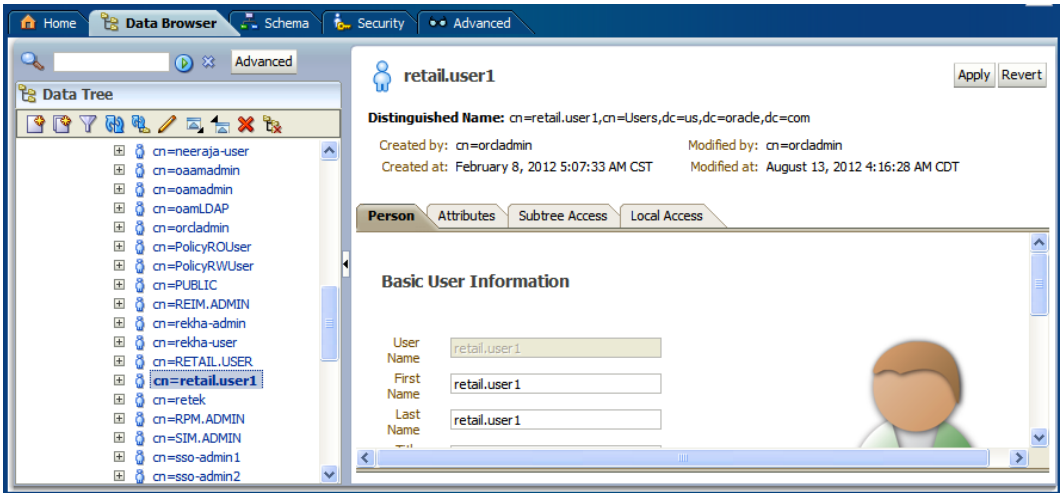
In order to have more users that are able to Login to ReIM, you need to create the new users by following these post-installation steps.

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 the Apply button.

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

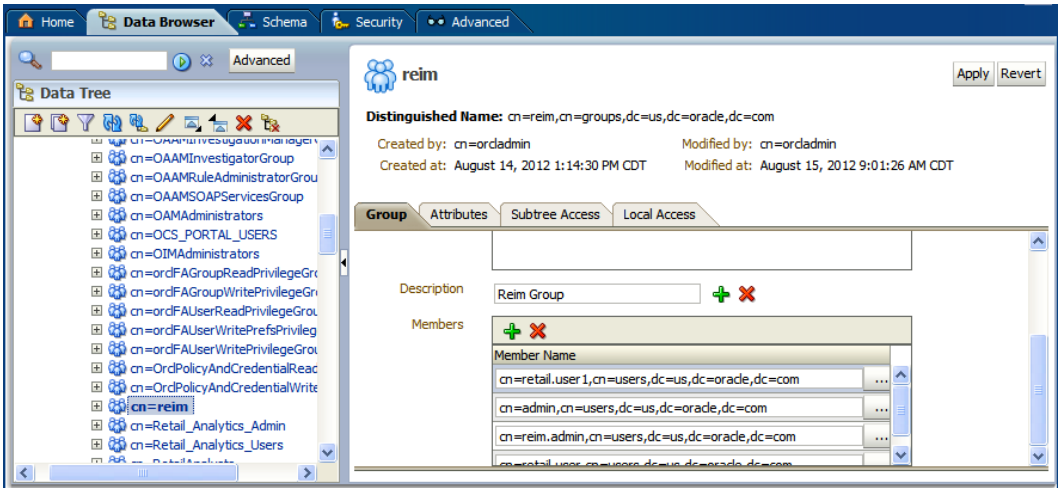


2. Assign user "RETAIL.USER1" as member of "reim" Group

   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`

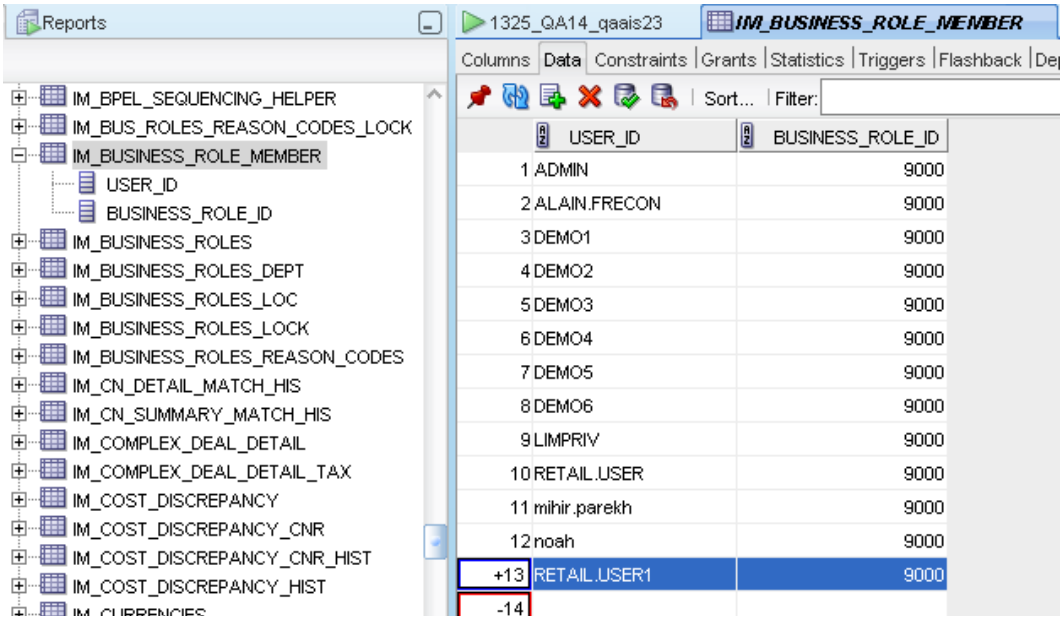
   After applying the changes, your screen should look similar to the following:



3. Add the new user to the ReIM database table im_business_role_id.
   a. You add the new user and assign to the new user a ReIM role, by enterinf this SQL command:

```
insert into im_business_role_id
(USER_ID, BUSINESS_ROLE_ID)
values ('RETAIL.USER1', 9000);
```

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



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.

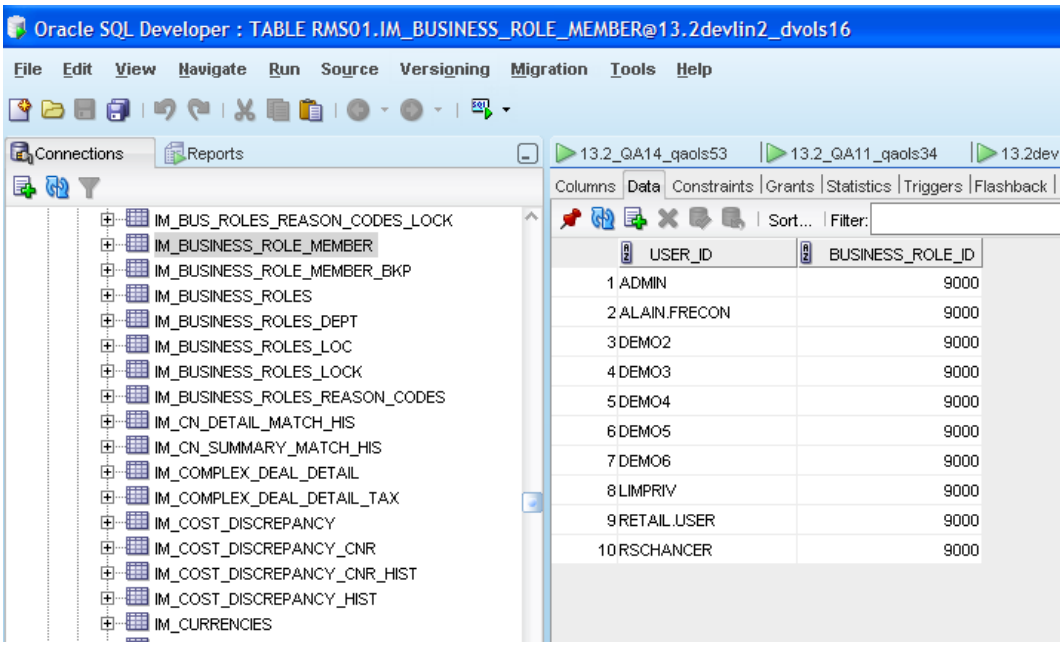
Migrate 13.2.4 ReIM users to LDAP

The users from 13.2.4 ReIM will not work on 13.2.5 ReIM. They also need to be creaed in LDAP and then, added as members of the “reim” LDAP group

To migrate the users included in the ReIM database table IM_BUSINESS_ROLE_ID you need to create for each of these users an entry in LDAP, following the instructions explained in the former section: Adding New Users To ReIM – Manually. Once these users are created in LDAP they need to be added as members of the “reim” LDAP group.

Ex: In the next screen we see the IM_BUSINESS_ROLE_ID table with some users.

If you need all of these the users to be able to login to ReIM, they have to be included in LDAP.

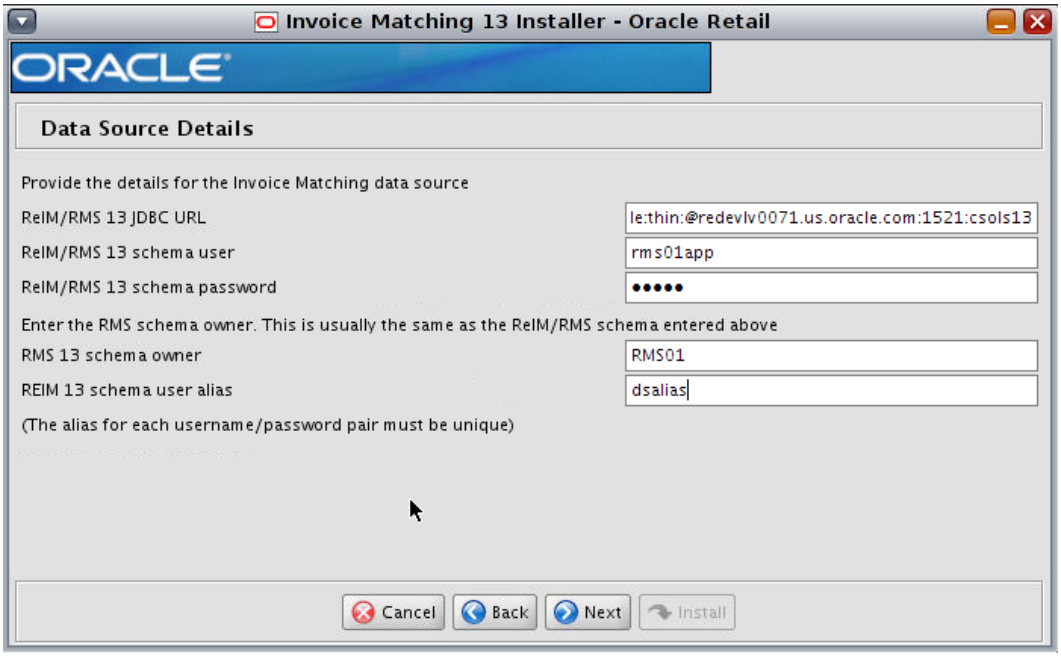


A

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: Data Source Details



Field Title	ReIM/RMS 13 JDBC URL
Field Description	URL used by the ReIM application to access the ReIM/RMS database schema. See Appendix: URL Reference for expected syntax.
Destination	reim.properties
Examples	jdbc:oracle:thin:@redevlv0071.us.oracle.com:1521:csols13

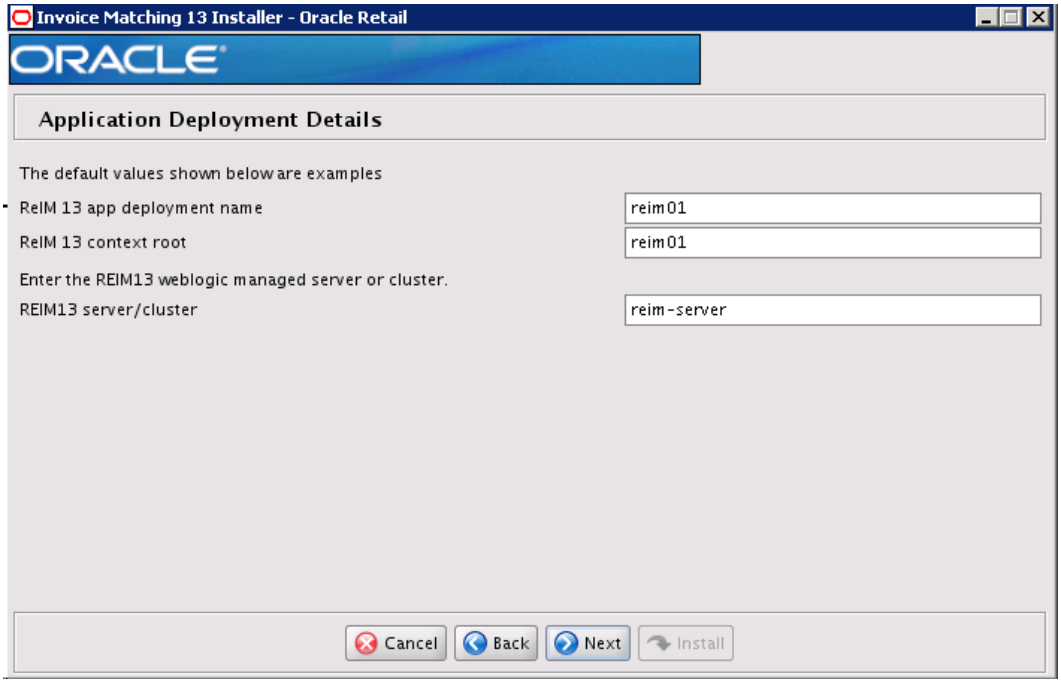
Field Title	ReIM/RMS 13 schema user
Field Description	RMS database user for accessing the ReIM tables. This should match what was given in the **RMS 13 schema** field of the ReIM database installer.
Destination	reim.properties
Example	rms01app

Field Title	ReIM/RMS 13 schema password
Field Description	Password for the JDBC username. This should match what was given in the **ReIM 13 schema password** field of the ReIM database installer.
Destination	wallet

Field Title	RMS 13 schema owner
Field Description	Database user which owns the RMS and ReIM tables. This usually has the same value as the **ReIM/RMS 13 schema** field above.
Destination	reim.properties
Example	RMS01

Field Title	REIM 13 schema user alias
Field Description	The alias of the ReIM user.
Destination	reim.properties
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: Application Deployment Details

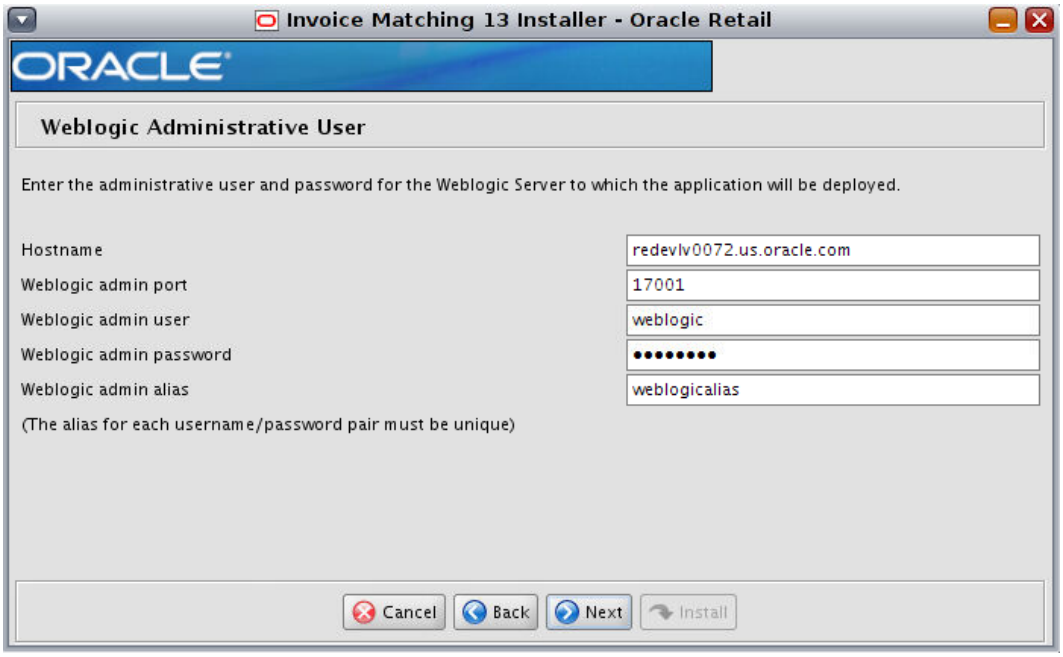


Field Title	ReIM 13 app deployment name
Field Description	Name by which this ReIM application is identified in the application server. This value must match the <context_root> added to the weblogic.policy file when the managed server for ReIM was created.
Example	reim01

Field Title	ReIM 13 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/reim01/index.jsp). This value must match the <context_root> added to the weblogic.policy file when the managed server for ReIM was created.
Example	reim01

Field Title	ReIM 13 server/cluster
Field Description	Name of the ReIM WebLogic managed server or cluster.
Example	reim-server

Screen: WebLogic Administrative User



Field Title	Hostname
Field Description	Hostname of the application server
Example	redevlv0072.us.oracle.com

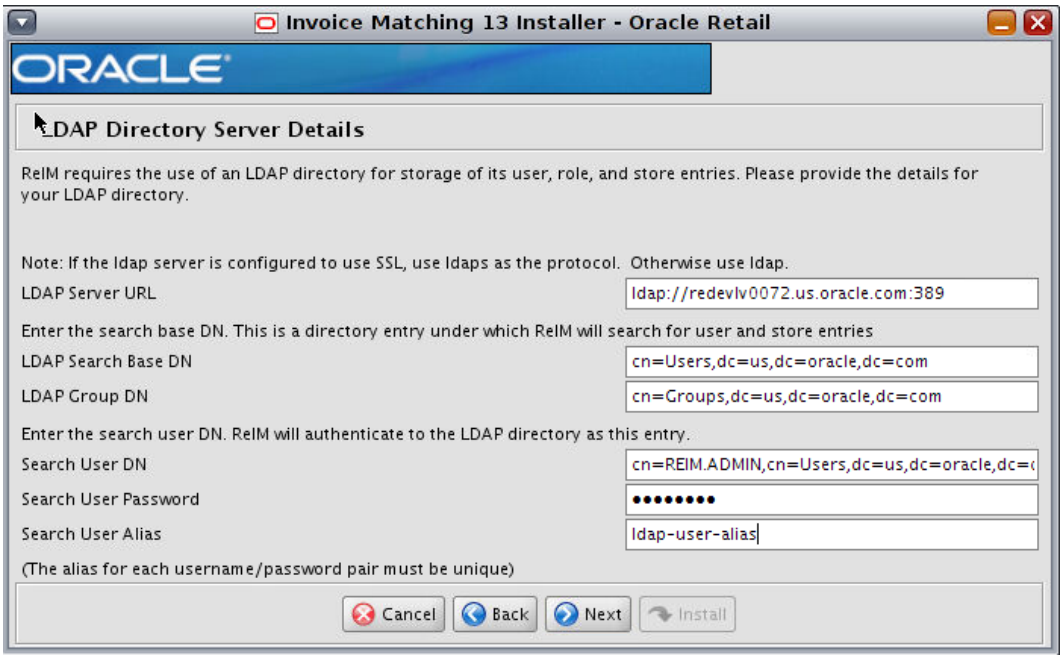
Field Title	WebLogic admin port
Field Description	This is the port of Administration Console.
Example	17001

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	Weblogicalias
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 Details



Field Title	LDAP server URL
Field Description	URL for your LDAP directory server. See Appendix: URL Reference for expected syntax.
Destination	ldap.properties
Example	ldap://redevlv0072.us.oracle.com:389

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

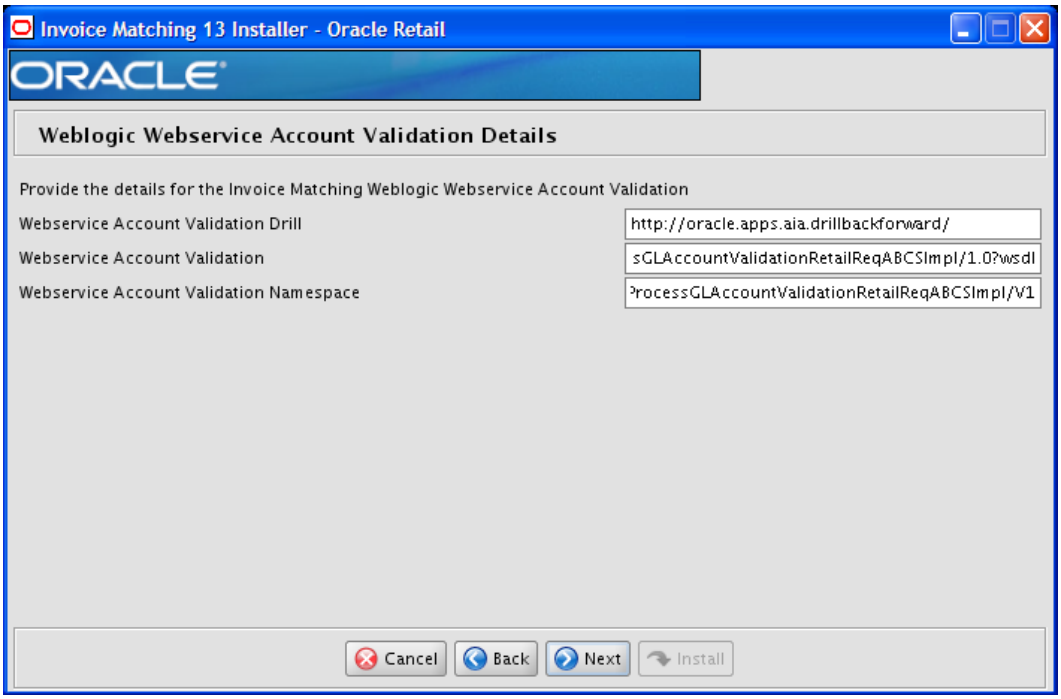
Field Title	LDAP Group DN
Field Description	Distingused name of the group that RPM uses to authenticate to the LDAP directory
Destination	ldap.properties
Example	cn=Groups,dc=us,dc=oracle,dc=com

Field Title	Search User DN
Field Description	Search User DN that ReIM will authenticate to the ldap directory
Destination	ldap.properties
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.
Destination	Ldap.properties
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

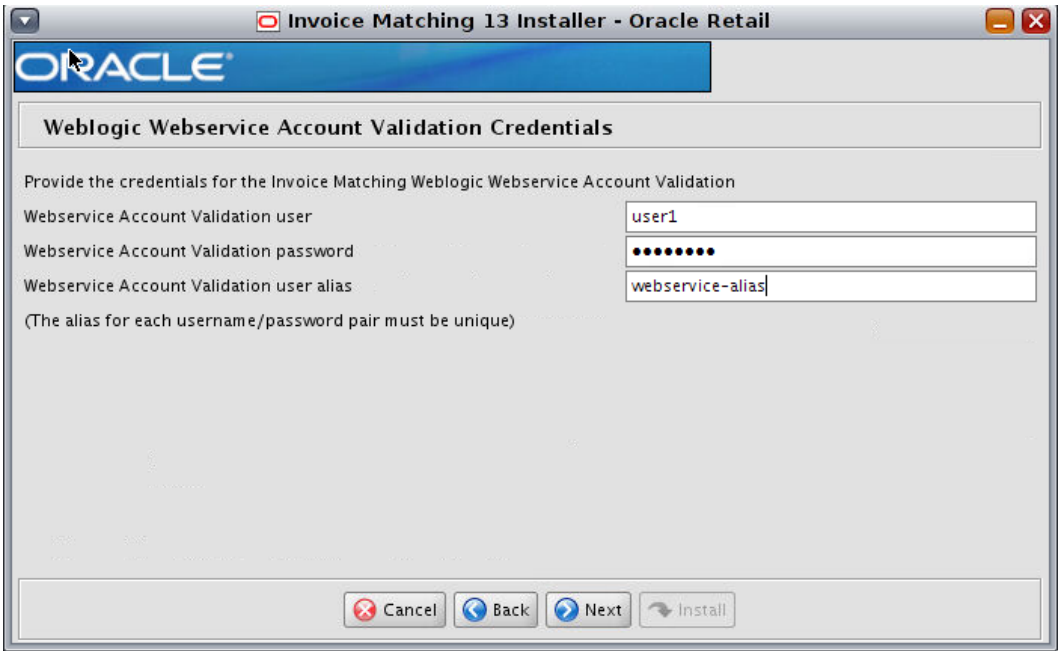


Field Title	Webservice Account Validation Drill
Field Description	The Web service provider URL used for drilling forward from the ReIM application. This information is from the financial application to which you are integrating (for example, PeopleSoft and Oracle E-Business Suite). Leave this field blank 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, PeopleSoft and 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, PeopleSoft and 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: WebLogic Webservice Account Validation Credentials

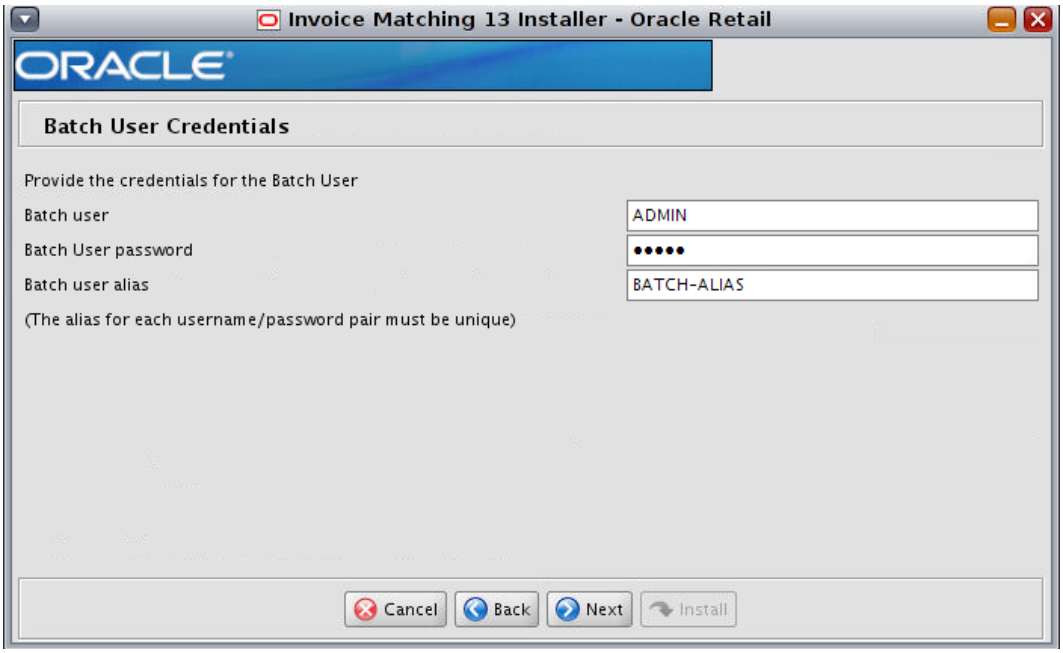


Field Title	Webservice Account Validation user
Field Description	The user for validating the Web service user name. A value is required in this field, even if you are not using Web service integration. The field is not validated, so enter any value.
Example	user1

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



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 or through LDAP—or it must be a valid ReIM user that will be built in the database. It does not have to exist already in the database on the database table (IM_BUSINESS_ROLE_ID), 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.

B

Appendix: Oracle 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 currently provides two different implementations: Oracle Single Sign-On (OSSO), and Oracle Access Manager (provides more comprehensive user access capabilities).

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 Oracle Single Sign-On?

The nexus of an Oracle Single Sign-On system is the Oracle Identity Management Infrastructure installation. This consists of 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 HTTP Server 11g Release 1 as a front end to the Oracle WebLogic Server. The Oracle HTTP Server is included in the Oracle Web Tier Utilities 11g Release 1 (11.1.1).
- An Oracle Single Sign-On Plug-in, used to authenticate the user and create the OSSO session cookie. This is available in the Oracle Fusion Middleware 11g Web Tier Utilities (11.1.1.6) package. For Oracle Forms applications like RMS and RWMS, HTTP server will be used.
- The Delegated Administration Services (DAS) application in OID10g and 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 OSSO system and registering HTTP servers.

Additional WebLogic managed servers will be needed to deploy the business applications leveraging the OSSO technology.

Can Oracle Single Sign-On Work with Other SSO Implementations?

Yes, OSSO 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 OSSO environment. The application may allow a user limited access when the user has not been authenticated. Applications that implement dynamic OSSO protection typically display a Login link to provide user authentication and gain greater access to the application's resources.

Identity Management Infrastructure for 10g, Oracle Identity Management (OIM) and Oracle Access Manager (OAM) Oracle Access Manager (OAM) for 11g

If using OSSO 10g, The Identity Management Infrastructure is the collection of product and services which provide Oracle Single Sign-on functionality. For OSSO 10g, this includes the Oracle Internet Directory, an Oracle HTTP server, and the Oracle Single Sign-On services. The Oracle Application Server deployed with these components is typically referred as the Infrastructure instance.

If using SSO with OAM11g, Oracle Identity Management (OIM) 11g includes Oracle Internet Directory and ODSM. Oracle Access Manager (OAM) 11g should be used for SSO using osso agent. Oracle Forms 11g contains Oracle HTTP server and other Retail Applications will use WebTier11g for HTTP.

MOD_OSSO

mod_osso is an Apache Web Server module an Oracle HTTP Server uses to function as a partner application within an Oracle Single Sign-On environment. The Oracle HTTP Server is based on the Apache HTTP Server.

MOD_WEBLOGIC

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

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 Single Sign-On.

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. OHS or WebTier uses the MOD_OSSO module to configure this functionality.

All partner applications must be registered with the Oracle Single Sign-On server if using OSSO10g and all partner applications must be registered with Oracle Access Manager (OAM) 11g if using OAM11g for SSO implementation. An output product of this registration is a configuration file the partner application uses to verify a user has been previously authenticated.

Realm

A Realm is a collection users and groups (roles) managed by a single password policy. This policy controls what may be used for authentication (for example, passwords, X.509 certificates, and biometric devices). A Realm also contains an authorization policy used for controlling access to applications or resources used by one or more applications.

A single OID can contain multiple Realms. This feature can consolidate security for retailers with multiple banners or to consolidate security for multiple development and test environments.

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 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.

Note: Dynamically Protected URL and Statically Protected URL are within the context of the Oracle Software Security Assurance (OSSA). The static protection for URLs is a common JEE feature.

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 OSSO user IDs to a database logins on a per-application basis.

How Oracle Single Sign-On Works

Oracle Single Sign-On involves a couple of different components. These are:

- The Oracle Single Sign-On (OSSO) servlet, 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 HTTP Server associated with the Web application, which verifies and controls browser redirection to the OSSO servlet.
- If the Web application implements dynamic protection, then the Web application itself is involved with the OSSO system.

Statically Protected URLs

When an unauthenticated user accesses a statically protected URL, the following occurs:

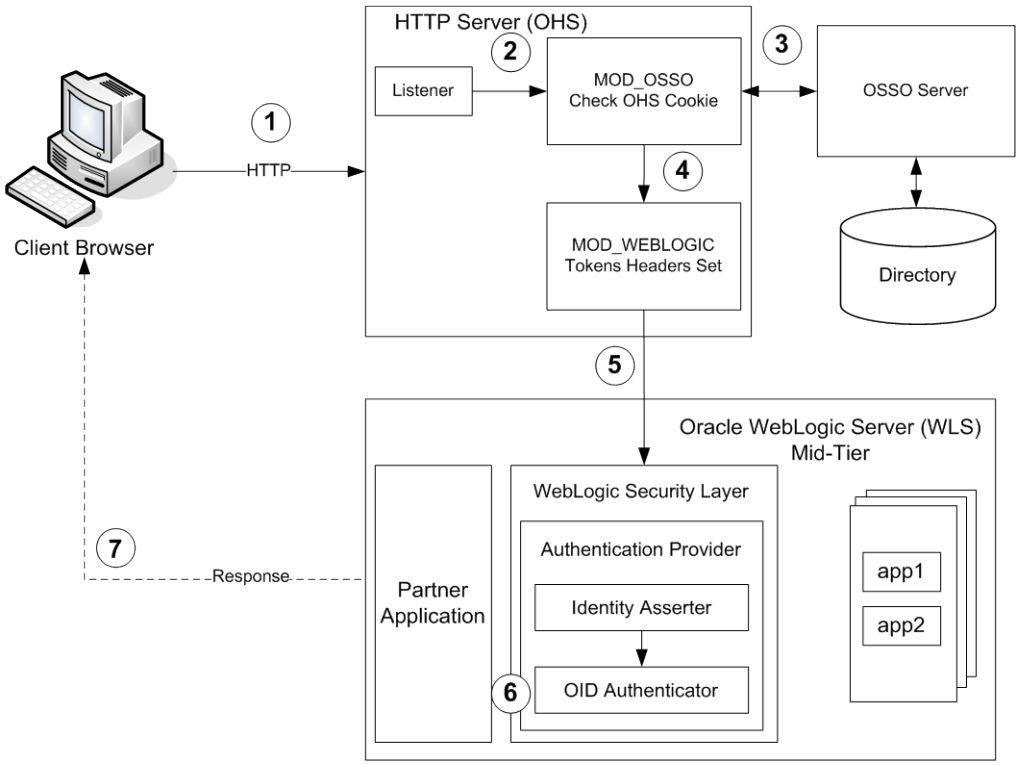
1. The user's Web browser makes an HTTP request to a protected URL serviced by the Oracle HTTP Server (OHS).
2. The Oracle HTTP Server processses the request and routes it to the mod_oss module.
3. This module determines whether the user is already authenticated. If the authentication is required, it directs the browser to the OSSO server. The OSSO server checks for a secure cookie containing the authentication information. If the cookie is not found, the following occurs:
    a. The OSSO servlet determines the user must authenticate, and displays the OSSO login page.
    b. The user must sign in via a valid user ID and password. If the OSSO servlet has been configured to support multiple Realms, a valid realm must also be entered. The user ID, password, and realm information is validated against the Oracle Internet Directory LDAP server. The browser is then redirected back to the Oracle HTTP Server with the encrypted authentication credentials. It does NOT contain the user's password.
4. The mod_osso module then decrypts the user credentials and sets HTTP headers with relevant user attributes, marking the user's session as authenticated.
5. The mod_WebLogic module (within the Oracle HTTP Server) then forwards the request to the Oracle WebLogic Server.
6. The Oracle WebLogic Server then invokes the configured authentication providers that decode the headers and provide the user's role membership. In an OSSO implementation, ensure that the OSSO Identity Asserter is invoked and Oracle Internet Directory (OID) Authenticator is executed to provide the user's role membership.
7. Once the authentication is established, the relevant application logic is initiated and the response is sent back to the user through the Oracle HTTP Server.
   Because the Web browser session is now authenticated, subsequent requests in that session are not redirected to the OSSO server for authentication.

Dynamically Protected URLs

When an unauthenticated user accesses a dynamically protected URL, the following occurs:

1. The user's Web browser makes an HTTP request to a protected URL serviced by the Oracle HTTP Server (OHS). The Oracle HTTP server recognizes the user has not been authenticated, but allows the user to access the URL.
2. The application determines the user must be authenticated and send the Oracle HTTP Server a specific status to begin the authentication process.
3. The Oracle HTTP Server processes the request and routes it to the mod_oss module.
4. This module determines whether the user is already authenticated. If the authentication is required, it directs the browser to the OSSO server. The OSSO server checks for a secure cookie containing the authentication information. If the cookie is not found, the following occurs:
   a. The OSSO servlet determines the user must authenticate, and displays the OSSO login page.
   b. The user must sign in via a valid user ID and password. If the OSSO servlet has been configured to support multiple Realms, a valid realm must also be entered. The user ID, password, and realm information is validated against the Oracle Internet Directory LDAP server. The browser is then redirected back to the Oracle HTTP Server with the encrypted authentication credentials. It does NOT contain the user's password.
5. The mod_osso module then decrypts the user credentials and sets HTTP headers with relevant user attributes, marking the user's session as authenticated.
6. The mod_WebLogic module (within the Oracle HTTP Server) then forwards the request to the Oracle WebLogic Server.
7. The Oracle WebLogic Server then invokes the configured authentication providers that decode the headers and provide the user's role membership. In an OSSO implementation, ensure that the OSSO Identity Asserter is invoked and Oracle Internet Directory (OID) Authenticator is executed to provide the user's role membership.
8. Once the authentication is established, the relevant application logic is initiated and the response is sent back to the user through the Oracle HTTP Server.
   Because the Web browser session is now authenticated, subsequent requests in that session are not redirected to the OSSO server for authentication.

Single Sign-on Topology



Installation Overview

Installing Oracle Single Sign-On 10g requires installation of the following:

1. Oracle Internet Directory (OID) LDAP server and the Infrastructure Oracle Application Server (OAS). They are typically installed using a single session of the Oracle Universal Installer and are performed at the same time. OID requires an Oracle relational database. If one is not available, the installer will install this as well.

   The Infrastructure OAS includes the Delegated Administration Services (DAS) application as well as the OSSO servlet. The DAS application can be used for user and realm management within OID.
2. 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 Infrastructure OAS installed in step 1. For additional information on SSO 10g installation, see the Creating a High-Availability Environment Whitepaper (My Oracle Support Doc ID: 1311392.1).
3. Additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities.

Installing Oracle Single Sign-On 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 (11.1.1.6). The ODSM application can be used for user and realm management within OID.
2. Oracle Access Manager 11gR1 (11.1.1.5) has to be installed and configured.

3. Additional midtier instances (such as Oracle Forms 11g) for Oracle Retail applications based on Oracle Forms technologies (such as RMS). These instances must be registered with the OAM installed in step 2.
4. Additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities must be registered with OAM installed in step 2. For additional information on SSO 11g installation, see the Oracle Access Manager and Single Sign-On Whitepaper (My Oracle Support Doc ID 1492047.1).

Infrastructure Installation and Configuration

The Infrastructure installation for OSSO and Oracle Access Manager (OAM) is dependent on the environment and requirements for its use. Deploying an Infrastructure OAS or 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 Application Server Installation Guide and the Oracle Internet Directory Installation Guide (if using OSSO 10g) for more details and Oracle Identity Management Installation Guide11g (if using OAM11).*

OID User Data

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

The current version of Oracle Single Sign-On only supports OID as its user storage facility. 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.

OID with Multiple Realms

OID and OSSO can be configured to support multiple user Realms. Each realm is independent from each other and contains its own set of user IDs. As such, creating a new realm is an alternative to installing multiple OID and Infrastructure instances. Hence, a single Infrastructure OAS can be used to support development and test environments by defining one realm for each environment.

Realms may also be used to support multiple groups of external users, such as those from partner companies. For more information on Realms, see the *Oracle Internet Directory Administrators Guide*.

User Management

User Management consists of displaying, creating, updating or removing user information. There are two basic methods of performing user management: LDIF scripts and the Delegate Administration Services (DAS) application available for OID10g or Oracle Directory Services Manager (ODSM) available for OID11g.

OID DAS

The DAS application is a Web-based application used in OID10g is designed for both administrators and users. A user may update their password, change their telephone number of record, or modify other user information. Users may search for other users based on partial strings of the user's name or ID. An administrator may create new users, unlock passwords, or delete users.

The DAS application is fully customizable. Administrators may define what user attributes are required, optional or even prompted for when a new user is created.

Furthermore, the DAS application is secure. Administrators may also what user attributes are displayed to other users. Administration is based on permission grants, so different users may have different capabilities for user management based on their roles within their organization.

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 Single Sign-On 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 Single Sign-On.

C

Appendix: Installer Silent Mode

In addition to the GUI and text interfaces of the ReIM installer, there is a silent mode that can be run. This mode is useful if you wish to run a repeat installation attempt without going through the installer screens again.

The installer runs in two distinct phases. The first phase involves gathering settings from the user. At the end of the first phase, a properties file named ant.install.properties is created with the settings that were provided. Then the second phase begins, where this properties file is used to provide your settings for the installation.

To skip the first phase and re-use the ant.install.properties file from a previous run, follow these instructions:

1. Edit the ant.install.properties file and correct any invalid settings that may have caused the installer to fail in the previous run.
2. Run the installer again with the **silent** argument.
   ```
   install.sh silent
   ```

D

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:oci:@<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

E

Appendix: Common Installation Errors

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

Database installer hangs on startup

Symptom

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

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

Solution

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

Unreadable buttons in the Installer

If you are unable to read the text within the installer buttons, it could mean that your JAVA_HOME is pointed to an older version of the JDK than is supported by the installer. Set JAVA_HOME to the appropriate Java 1.6 (JDK 1.6.0) that is being used by the WebLogic Application Server and run the installer again.

Warning: Could not create system preferences directory

Symptom

The following text appears in the installer Errors tab:

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

Solution

This is related to Java bug 4838770. The /etc/.java/.systemPrefs directory may not have been created on your system.

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

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.

Warning: Lower case user IDS supplied with the application do not work

Symptom

The default user supplied with the ReIM application (for example, retail.user, where password = retek) does not work to for signing on to the application.

Solution

The user/password combination does not work because the password hashing is incorrect in the database scripts run by the installer code that affect only lower case user IDs/user names.

Run this code instead of the ReIM database to fix the passwords for the lower case user IDs supplied as part of the ReIM application:

update im_user_authorization iua

set password = reim_security_sql .hash(username, password) where lower (username) = username;

commit;

Installer fails because of missing .jar in $ORACLE_HOME/utils/ccr/lib

Symptom

The jar file expected by the installer (emocmclnt.jar) is overwritten after the OPatch patch 6880880 is applied, and any other patch is applied afterward using that OPatch. If you try to run the installer after patching, as outlined in the installation guides, the installer fails. All applications that are installed in the same WebLogic server that hosts any of the forms applications will be affected by this issue. This is because of required Oracle patches for Linux 64-bit systems that are applied to the forms server using OPatch.

Solution

Back up the content of the $ORACLE_HOME/utils/ccr/lib directory prior to applying OPatch patch 6880880, and recopy the content back after you apply any patches using that Opatch.

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.

F

Appendix: Setting Up Password Stores with Oracle Wallet

As part of an application installation, administrators must set up password stores for database user accounts using Oracle Wallet. These 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.

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

About 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 two different types of password stores or wallets. One type is for database connect strings used in program arguments (such as `sqlplus /@db_username`). The other type is 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, RETL, RMS, RWMS, and ARI
- For Java Applications (SIM, ReIM, RPM, Alloc, RIB, RSL, AIP, RETL)

For RMS, RPM Plsql Batch, RETL DB, RWMS batch, and ARI

Complete the following steps.

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

```
cd /projects/rms13.2/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/rms13.2/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 = mspdv311.us.oracle.com) (Port = 1521)))
    (CONNECT_DATA = (SID = dvols29) (GLOBAL_NAME = dvols29)))

dvols29_rms01user.world =
  (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
  (host = mspdv311.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/rms13.2/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/rms13.2/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 value of the entry:

  ```
  rms01user
  ```

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

  Returns value of the entry:

  ```
  passwd
  ```

For Java Applications (SIM, ReIM, RPM, Alloc, RIB, RSL, AIP, 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: mspdv351:[103x_WLS] /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/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:

  mspdv351:[103x_WLS] /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/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 application 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:

  mspdv351:[103x_WLS] /u00/webadmin/reim/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:[103xWLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/java_domain/retail/rpm1
32test/retail-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:[103xWLS]
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/java_domain/retail/rpm1
32test/retail-public-security-api/bin>
```

dump_credentials.sh

dump_credentials.sh is used to retrieve information from the 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 /u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/retail/reim13/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/132_mck_soa_domain/retail/reim13/config

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

Application level key partition name:reim13
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:rms132mock
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. You can add new or update using save_credential.sh as shown below:

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

Example:

```
mspdv351:[103x_WLS]
/u00/webadmin/mock132_testing/rtil/rtil/application/retail-public-security-
api/bin> save_credential.sh –l
/u00/webadmin/product/10.3.x/WLS/user_projects/domains/132_mck_soa_domain/reta
il/reim13/config
-a RMS-ALIAS -p reim13 -u rms132mock

=========================================
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 = reim13 to retrieve the password for application use.

Reim.properties code sample:

```
datasource.url=jdbc:oracle:thin:@mspdv349.us.oracle.com:1521:pkols07
datasource.schema.owner=rms132mock
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/132_mck_soa
_domain/retail/reim13/config
csm.wallet.partition.name=reim13
```

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 REIM app user reimbat, 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>.

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-13.2.0`
   - `RFX_TMP=/u00/rfx/rfx-13.2.0/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.

Quick Guide for Retail Wallets

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	
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	rwms13inst	
			<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
			aip13	<AIP weblogic user alias>	<AIP weblogic user name>	App use	Installer	aip-weblogic-alias	
			aip13	<AIP database schema user alias>	<AIP database schema user name>	App use	Installer	aip01user-alias	
			aip13	<rib-aip weblogic user alias>	<rib-aip weblogic user name>	App use	Installer	rib-aip-weblogic-alias	
RPM app	JAVA	<weblogic domain home>/retail/<deployed rpm app name>/config							Each alias must be unique
			rpm13	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	
			rpm13	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			rpm13	<rpm application user one alias>	<rpm application user one name>	App use	Installer	user1-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			rpm13	<rpm application user two alias>	<rpm application user two name>	App use	Installer	user2-alias	
			rpm13	<rpm batch user alias>	<rpm batch user name>	App, batch use	Installer	rpmbatch-alias	
			rpm13	<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>	<reim weblogic user alias>	<reim weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name>	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			<installed app name>	<reim webservice validation user alias>	<reim webservice validation user name>	App use	Installer	reimwebservice-alias	
			<installed app name>	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbat-alias	
Alloc app	JAVA	<weblogic domain home>/retail/<deployed alloc app name>/config							Each alias must be unique

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name>	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name>	<rms shema 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	
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	JAVA	<weblogic domain home>/retail/<deployed sim app name>/config							
			rpm	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	
			rms	<rsl for rms weblogic user alias>	<rsl for rms weblogic user name>	App use	Installer	rsl-rms-weblogic-alias	
			rib-sim	<rib-sim weblogic user alias>	<rib-sim weblogic user name>	App use	Installer	rib-sim-weblogic-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
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
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

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
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	

G

Appendix: Installation Order

This section provides a guideline as to the order in which the Oracle Retail applications should be installed. If a retailer has chosen to use 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) or Back Office with Labels and Tags (ORLAT)
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 Replenishment Optimization (RO)

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