

Oracle® Retail Invoice Matching

Installation Guide

Release 15.0.3.1

F37452-01

March 2021

Copyright © 2021, Oracle. All rights reserved.

Primary Author: Preethi Sahu

Contributors: Nathan Young, Sravana Kumar, Sabarish Lakshmikanthaiah

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

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.....	xi
Preface	xiii
Audience	xiii
Customer Support.....	xiii
Review Patch Documentation.....	xiii
Improved Process for Oracle Retail Documentation Corrections	xiv
Oracle Retail Documentation on the Oracle Technology Network.....	xiv
Conventions.....	xiv
1 Preinstallation Tasks.....	1
Check Supported Database Server Requirements.....	1
Check Supported Application Server Requirements	3
Verify Single Sign-On.....	3
Check Supported Client PC and Web Browser Requirements.....	4
Supported Oracle Retail Products	4
UNIX User Account Privileges to Install the Software	4
Supported Oracle Applications.....	5
2 RAC and Clustering.....	7
3 Database Installation Tasks.....	9
4 Application Installation Tasks	11
Middleware Infrastructure and WebLogic Server12c (12.2.1.4.0) Installation.....	11
Install RCU Database Schemas	17
Create a New ADF Domain (with managed server and EM)	27
Start the Node Manager	44
Start the AdminServer (admin console).....	44
Start the Managed Server.....	45
Configuration of OID LDAP Provider in Weblogic Domain:	45
Verify OID Authenticator	51
Configure Oracle Single Sign-On.....	52
Create the SSO provider in the REIMDomain	52
Create mds-CustomPortalDS Datasource using EM.....	52
Steps to Configure WebLogic Work Manager	58
Steps to Create a Named Work Manager	58
Steps to Create Maximum thread constraints.....	61
Load LDIF Files in LDAP.....	66
Oracle Retail Application Administration Console	68
Clustered Installations - Preinstallation Steps.....	69
(Optional) Analyze Changes in the Patch.....	69
Expand the ReIM Application Distribution	69
Run the Oracle Retail Invoice Matching Installer.....	70

Resolving Errors Encountered During Application Installation	70
Post-Installation Steps	71
Clustered Installations – Post-Installation Steps.....	72
Installing the REIM OAS Publisher Templates.....	72
Test the ReIM Application.....	72
reim.properties	73
integration.properties	73
ReIM Batch Scripts	74
Online Help.....	74
Single Sign-On.....	75
Adding Logout URI.....	76
5 Configure the OAS5.5 Environment for Operational Insights.....	79
Terms	79
Install OAS 5.5	79
OAS Server Component Installation Tasks	79
Installation Process Overview	79
Install Oracle Analytics Server 5.5.....	80
Configure OID Provider in OAS 5.5 WebLogic Domain.....	90
Load LDIF Files in LDAP.....	95
Configure Oracle Single Sign-On.....	96
Create the SSO provider in the Oracle Analytics Domain	96
Configure RPD and Set up the Database Connection.....	96
Configure Oracle Retail Operational Insights Roles and Application Roles	103
Language Selection with SSO.....	105
6 Post Installation Tasks and Configuration.....	107
Enable the Oracle BI EE Content to be Displayed in IFrame	107
Configure Charts /Charts/to use HTML5	107
Enable EVALUATE Function in Oracle BI EE	107
Error: for Iframe is not allowed to display the Reports	108
Disable Cache in Oracle BI EE.....	108
Enable the ADF Contextual Event Action in Oracle BI EE.....	109
Single Sign-On Configuration for Oracle BI EE	109
Redirect of analytics to the WebLogic Server	109
Verify the Static Resources using the Oracle Web Tier	110
Configure for In-Context launches of RMS forms.....	110
Restart Oracle BI EE.....	111
Validation.....	111
Troubleshooting	111
7 Data Migration	113
Usage	113
Parameters	113
Error and Restart.....	113

Locking	114
8 Patching Procedures	115
Oracle Retail Patching Process	115
Supported Products and Technologies	115
Patch Concepts	116
Patching Utility Overview	117
Changes with 15.0.....	117
Patching Considerations	117
Patch Types.....	117
Incremental Patch Structure	118
Version Tracking.....	118
Apply all Patches with Installer or ORPatch.....	118
Environment Configuration.....	119
Retained Installation Files.....	119
Reloading Content	119
Java Hotfixes and Cumulative Patches.....	119
Backups	120
Disk Space.....	120
Patching Operations	121
Running ORPatch	121
Merging Patches.....	131
Compiling Application Components	132
Deploying Application Components	134
Maintenance Considerations	135
Database Password Changes.....	135
WebLogic Password Changes.....	136
Infrastructure Directory Changes.....	137
DBManifest Table.....	137
RETAIL_HOME relationship to Database and Application Server.....	137
Jar Signing Configuration Maintenance	137
Customization	139
Patching Considerations with Customized Files and Objects	139
Registering Customized Files.....	140
Custom Compiled Java Code.....	142
Extending Oracle Retail Patch Assistant with Custom Hooks	144
Troubleshooting Patching.....	149
ORPatch Log Files.....	149
Restarting ORPatch.....	149
Manual DBManifest Updates.....	149
Manual Restart State File Updates	151
DISPLAY Settings When Compiling Forms.....	151
JAVA_HOME Setting.....	151

Patching Prior to First Install.....	151
Providing Metadata to Oracle Support.....	152
A Appendix: ReIM Application Installer Screens	155
B Appendix: Installer Silent Mode	183
C Appendix: Single Sign-On for WebLogic	185
What Do I Need for Single Sign-On?	185
Can Oracle Access Manager Work with Other SSO Implementations?	185
Oracle Single Sign-on Terms and Definitions	186
What Single Sign-On is not.....	187
How Oracle Single Sign-On Works	187
Installation Overview	189
User Management.....	189
D Appendix: URL Reference	191
JDBC URL for a Database	191
E Appendix: BI User and Group LDIF Entries	193
BI_User.ldif Entries.....	193
BI_Group.ldifs Entries.....	194
F Appendix: Common Installation Errors.....	195
ConcurrentModificationException in Installer GUI.....	195
Warning: Could not find X Input Context.....	195
GUI screens fail to open when running Installer.....	195
Hostname Verification Error when SSL is used.....	196
G Appendix: Setting Up Password Stores with wallets/credential stores.....	197
About Database Password Stores and Oracle Wallet.....	197
Setting Up Password Stores for Database User Accounts.....	198
Setting up Wallets for Database User Accounts	199
For RMS, RWMS, RPM Batch using sqlplus or sqlldr, RETL, RMS, RWMS, and ARI	199
Setting up RETL Wallets	201
For Java Applications (SIM, ReIM, RPM, RIB, AIP, Alloc, ReSA, RETL).....	202
How does the Wallet Relate to the Application?	205
How does the Wallet Relate to Java Batch Program use?.....	205
Database Credential Store Administration.....	205
Managing Credentials with WSLT/OPSS Scripts	207
listCred	208
updateCred	209
createCred.....	210
deleteCred.....	210
modifyBootstrapCredential	210
addBootstrapCredential	212
Quick Guide for Retail Password Stores (db wallet, java wallet, DB credential stores)	213

H Appendix: Installation Order	223
Enterprise Installation Order.....	223

Send Us Your Comments

Oracle Retail Invoice Matching, Installation Guide, Release 15.0.3.1

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

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, 15.0) or a later patch release (for example, 15.0.3). If you are installing the base release or additional patch releases, read the documentation for all releases that have occurred since the base release before you begin installation. Documentation for patch releases can contain critical information related to the base release, as well as information about code changes since the base release.

Improved Process for Oracle Retail Documentation Corrections

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

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

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

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

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

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

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

(Data Model documents are not available through Oracle Technology Network. You can obtain them through My Oracle Support.)

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

Preinstallation Tasks

This chapter explains the tasks required prior to installation.

Note: Oracle Retail assumes that the retailer has applied all required fixes for supported compatible technologies.

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 12cR1 and 19c Enterprise Edition. Options are: <ul style="list-style-type: none">▪ Oracle Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).▪ Red Hat Enterprise Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine).▪ AIX 7.1 (Actual hardware or LPARs)▪ Solaris 11.x SPARC (Actual hardware or logical domains)

Database Server 12cR1	<p>Oracle Database Enterprise Edition 12cR1 (12.1.0.2) with the following specifications:</p> <p>Components:</p> <ul style="list-style-type: none"> ▪ Oracle Partitioning ▪ Examples CD <p>Oneoffs:</p> <ul style="list-style-type: none"> ▪ 20846438: ORA-600 [KKPAPXFORMFKK2KEY_1] WITH LIST PARTITION ▪ 19623450: MISSING JAVA CLASSES AFTER UPGRADE TO JDK 7 ▪ 20406840: PROC 12.1.0.2 THROWS ORA-600 [17998] WHEN PRECOMPILING BY 'OTHER' USER ▪ 20925154: ORA-39126: WORKER UNEXPECTED FATAL ERROR IN KUPW\$WORKER GATHER_PARSE_ITEMS JAVA ▪ 19672263: Patch 19672263: GTT SESSION LEVEL STATISTICS RETURNS ORA-20006 <p>RAC only:</p> <ul style="list-style-type: none"> ▪ 21260431: APPSST 12C : GETTING ORA-4031 AFTER 12C UPGRADE ▪ 21373473: INSTANCE TERMINATED AS LMD0 AND LMD2 HUNG FOR MORE THAN 70 SECS <p>Other components:</p> <ul style="list-style-type: none"> ▪ Perl interpreter 5.0 or later ▪ X-Windows interface ▪ JDK 1.7
Database Server 19c	<p>Oracle Database Enterprise Edition 19c (19.3.0.0) with the following components:</p> <p>Components:</p> <ul style="list-style-type: none"> ▪ DB HOME ▪ Examples CD <p>Other components:</p> <ul style="list-style-type: none"> ▪ Perl interpreter 5.0 or later ▪ X-Windows interface ▪ JDK 1.8

Note on 12C JDK: By default, JDK is at 1.6. After installing the 12.1.0.2 binary, apply patch 19623450. Follow the instructions on Oracle Database Java Developer's Guide 12c Release 1 to upgrade JDK to 1.7. The Guide is available at: <http://docs.oracle.com/database/121/JJDEV/chone.htm#JJDEV01000>.

Check Supported Application Server Requirements

General requirements for an application server capable of running the Oracle Retail Invoice Matching application include the following:

Supported on:	Versions Supported:
Application Server OS	<p>OS certified with Oracle Fusion Middleware 12c (12.2.1.4). Options are:</p> <ul style="list-style-type: none"> Oracle Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine) Red Hat Enterprise Linux 6 and 7 for x86-64 (Actual hardware or Oracle virtual machine) AIX 7.2 (Actual hardware or LPARs) Solaris 11.x SPARC (Actual hardware or logical domains)
Application Server OS	<p>Oracle Fusion Middleware 12c 12.2.1.4</p> <p>Components:</p> <ul style="list-style-type: none"> Oracle Fusion Middleware Infrastructure 12c (12.2.1.4) (WLS and ADF included) Oracle Enterprise Manager 12.2.1.4 Oracle Identity Management 12c (12.2.1.4) <p>Note: Oracle Internet Directory (OID) is the supported LDAP directory for Oracle Retail products. For alternate LDAP directories, refer to Oracle WebLogic documentation set.</p> <p>Java:</p> <p>JDK 1.8+ 64 bit</p> <p>Optional (for Operational Insights)</p> <ul style="list-style-type: none"> OAS 5.5 <p>Optional (required for SSO)</p> <ul style="list-style-type: none"> OAS 5.5 (for Operational Insights) <p>Oracle WebTier/Webgate 12c (12.2.1.4)</p> <p>Oracle Access Manager 12c(12.2.1.4)</p> <p>Oracle Directory Services Manager (ODSM) 12.2.1.4</p>

Verify Single Sign-On

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

If Single Sign-On is to be used, verify the Oracle Identity Management 12c version has been installed along with the components listed in the above Application Server requirements section. Verify if the Access Manager Agent is registered with the Oracle Access Manager 12.2.1.4 as a partner application.

Check Supported Client PC and Web Browser Requirements

Requirement	Version
Operating system	Windows 10
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	Java 1.8+
Browser	Microsoft Internet Explorer 11 Microsoft Edge 41+ Mozilla Firefox ESR 60+ Chrome 73+

Supported Oracle Retail Products

Requirement	Version
Oracle Retail Merchandising System (RMS)/Oracle Retail Trade Management (RTM)/Oracle Retail Sales Audit (ReSA)	15.0.3.1
Oracle Retail Store Inventory Management (SIM) (by way of RMS)	15.0.3.1
Oracle Retail Insights	15.0.2

UNIX User Account Privileges to Install the Software

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

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

Supported Oracle Applications

Requirement	Version
Oracle E-Business Suite (Accounts Payable)	Oracle E-Business Suite 12.2.4 integration is supported using the Retail Financial Integration 15.0 for Oracle Retail Merchandising Suite and Oracle E-Business Suite Financials. See the <i>RFI installation and upgrade Guide</i> for specific version information.
Oracle PeopleSoft Financials	Oracle PeopleSoft Financials 9.2, integration is supported using the Oracle Retail Financial Integration for Oracle Retail Merchandising Suite and Oracle PeopleSoft Financials. See the <i>Oracle Retail Financial Integration for Oracle Retail Merchandise Operations Management and Oracle E-Business Suite or PeopleSoft Financials</i> for specific version information.

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 a 12.1.0.2 and/or a 19c 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 12.2.1.4.0 is managed as an Active-Active cluster accessed through a Load Balancer. Validation has been completed utilizing a RAC 12.1.0.2 Oracle Internet Directory database with the WebLogic 12c cluster. It is suggested that a Web Tier 12c installation be configured to reflect all application server installations if SSO will be utilized.

References for Configuration:

- Oracle® Fusion Middleware High Availability Guide 12c(12.2.1.4) Part Number E95104-03
- Oracle Real Application Clusters Administration and Deployment Guide 12c Release 1 (12.1) E48838-10 and 19c (19.3) E95728-06.

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.

Application Installation Tasks

Before proceeding, you must install Oracle WebLogic 12.2.1.4 using Fusion Middleware Infrastructure with ADF.

These are the other prerequisites before installing Oracle Retail Invoice Match application
Install WebLogic domain with ADF and EM (Enterprise Manager Fusion Middleware control 12c).

Set up MDS schema Datasource in Enterprise Manager (EM).

Configuration of OID Authenticator in WebLogic domain.

Load LDIF files in LDAP to create Users and Roles.

It is assumed Oracle database has already been configured and loaded with the appropriate RMS and Oracle Retail Invoice Match schemas for your installation.

MDS schema, OPSS schema and other required schemas for ADF must be created using RCU utility. Steps to create the schemas are explained in this document.

Installing a separate domain as part of ADF configuration is recommended.

The Oracle Retail Invoice Match application is deployed to a managed server (example: reim-server) which is created inside the new domain (example: ReimDomain). This managed server must contain all the ADF libraries.

Middleware Infrastructure and WebLogic Server12c (12.2.1.4.0) Installation

Create a directory to install the WebLogic (this will be the ORACLE_HOME):

Example: `mkdir -p /u00/webadmin/products/wls_retail`

1. Set the ORACLE_HOME, JAVA_HOME and DOMAIN_HOME environment variables:

- ORACLE_HOME should point to your WebLogic installation.
- JAVA_HOME should point to the Java JDK 1.8+. This is typically the same JDK which is being used by the WebLogic domain where application is getting installed.

Example:

```
$export ORACLE_HOME=/u00/webadmin/products/wls_retail
$export JAVA_HOME=/u00/webadmin/products/jdk_java
(This should point to the Java which is installed on your server)
$export PATH=$JAVA_HOME/bin:$PATH
```

Going forward we will use the above references for further installations.

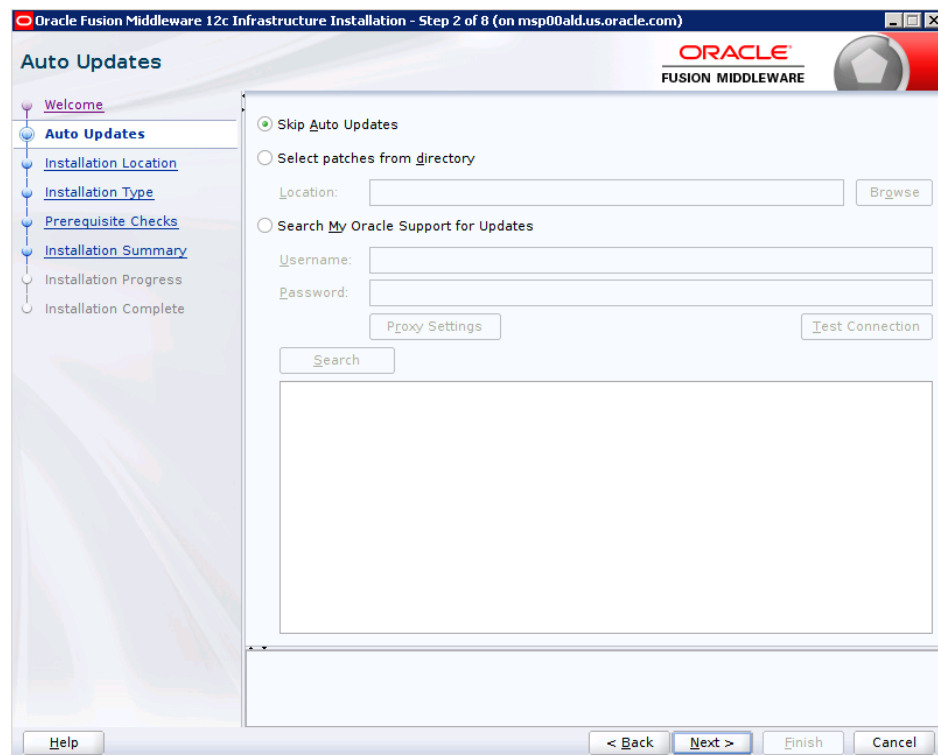
2. Go to location where the weblogic jar is downloaded and run the installer using the following command:

```
java -jar ./fmw_12.2.1.4.0_infrastructure.jar
```

3. Welcome screen appears. Click **Next**.



4. Click **Next**.

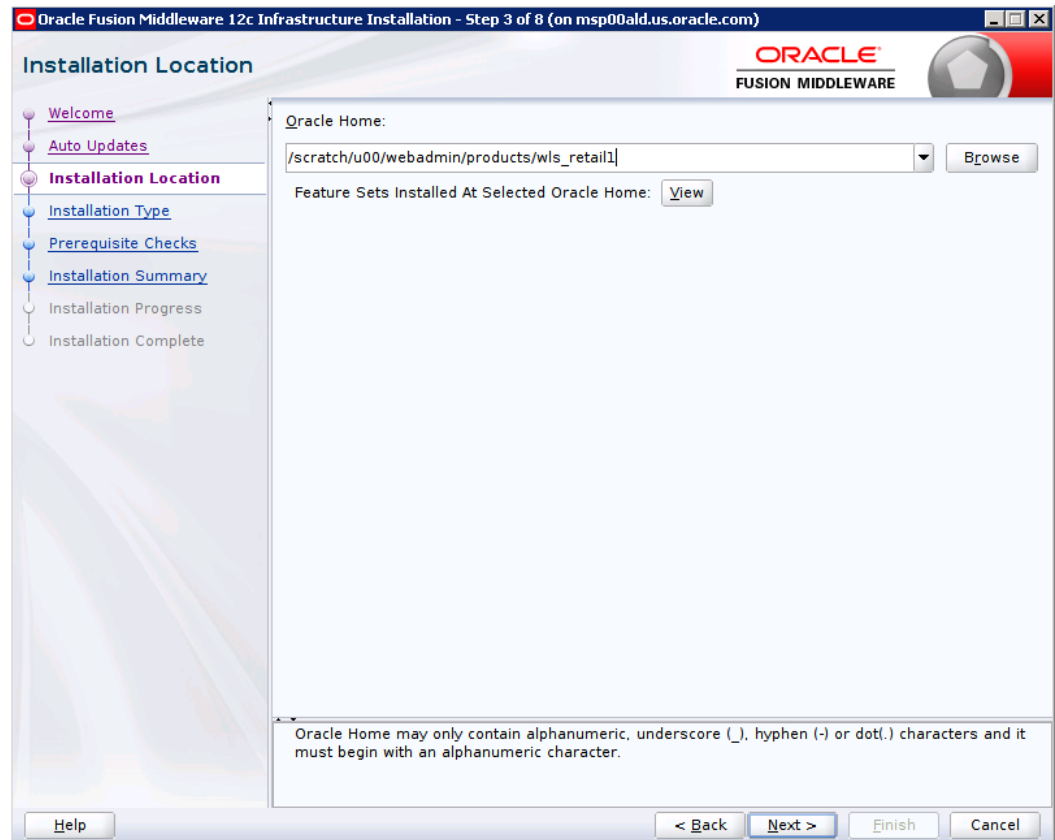


5. Enter the following and click **Next**.

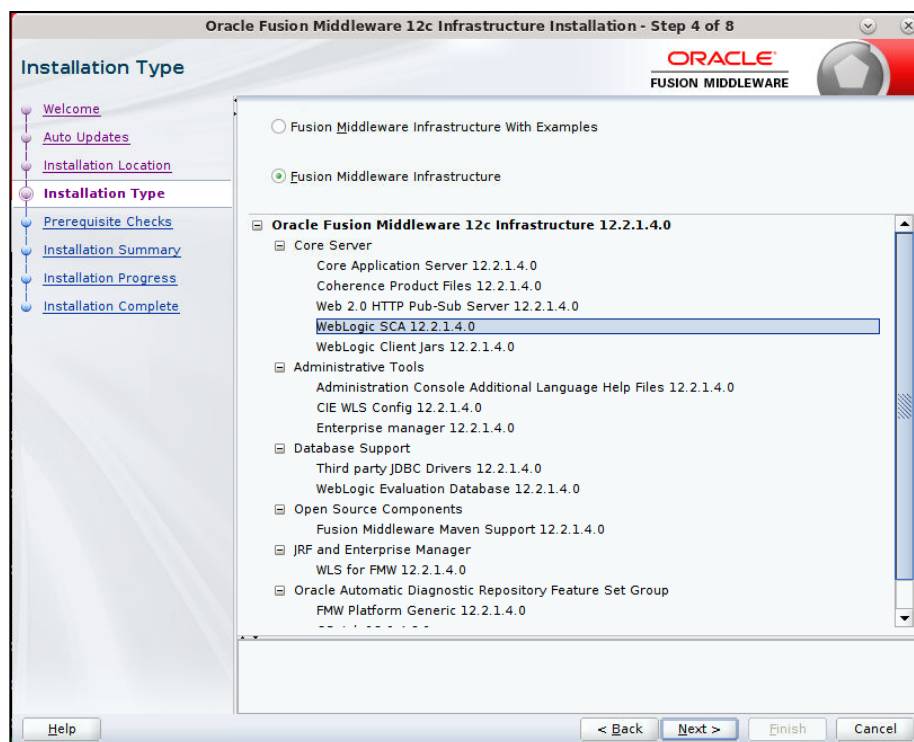
Oracle home =<Path to the ORACLE_HOME>

Example:

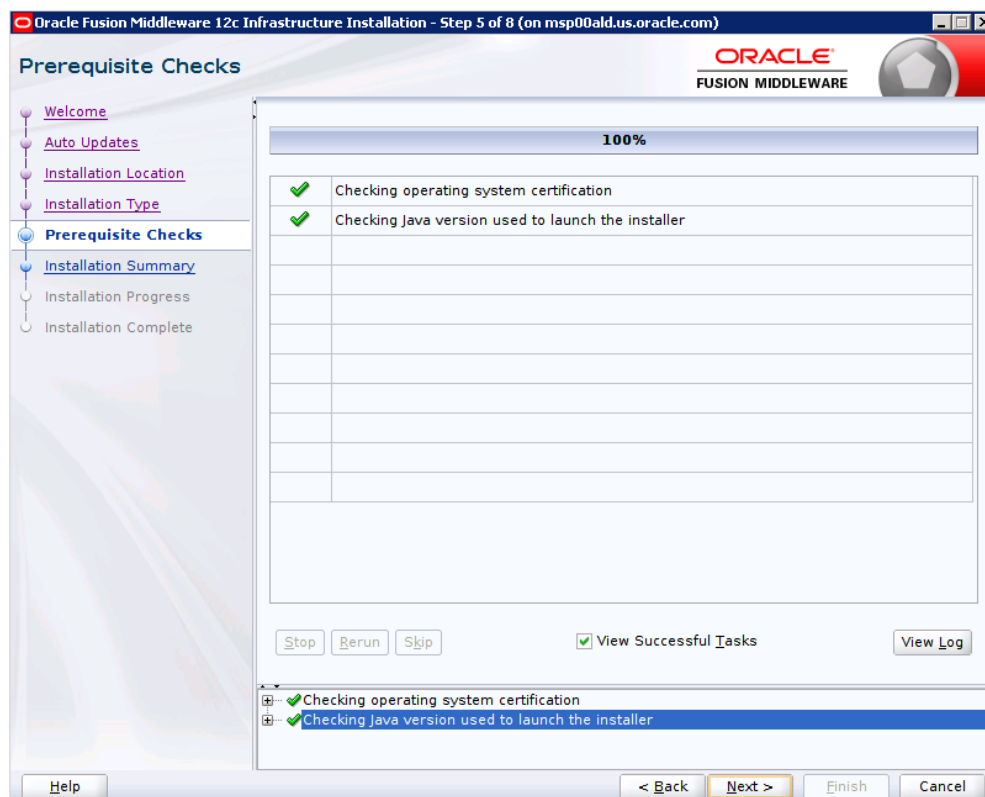
/u00/webadmin/products/wls_retail



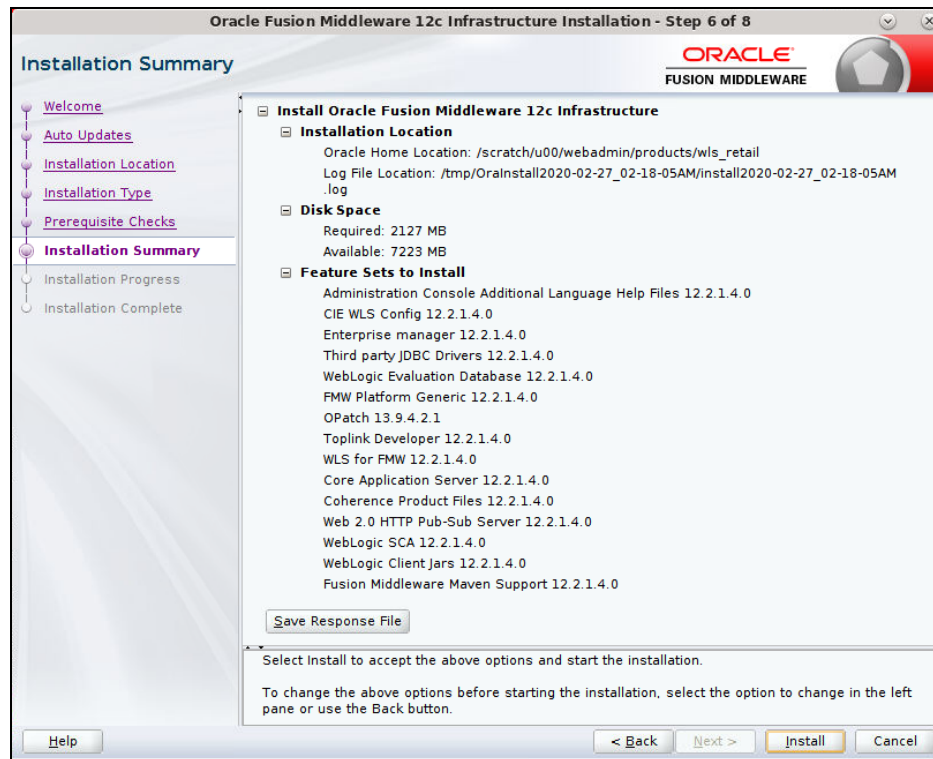
6. Select install type 'Fusion Middleware Infrastructure'. Click **Next**.



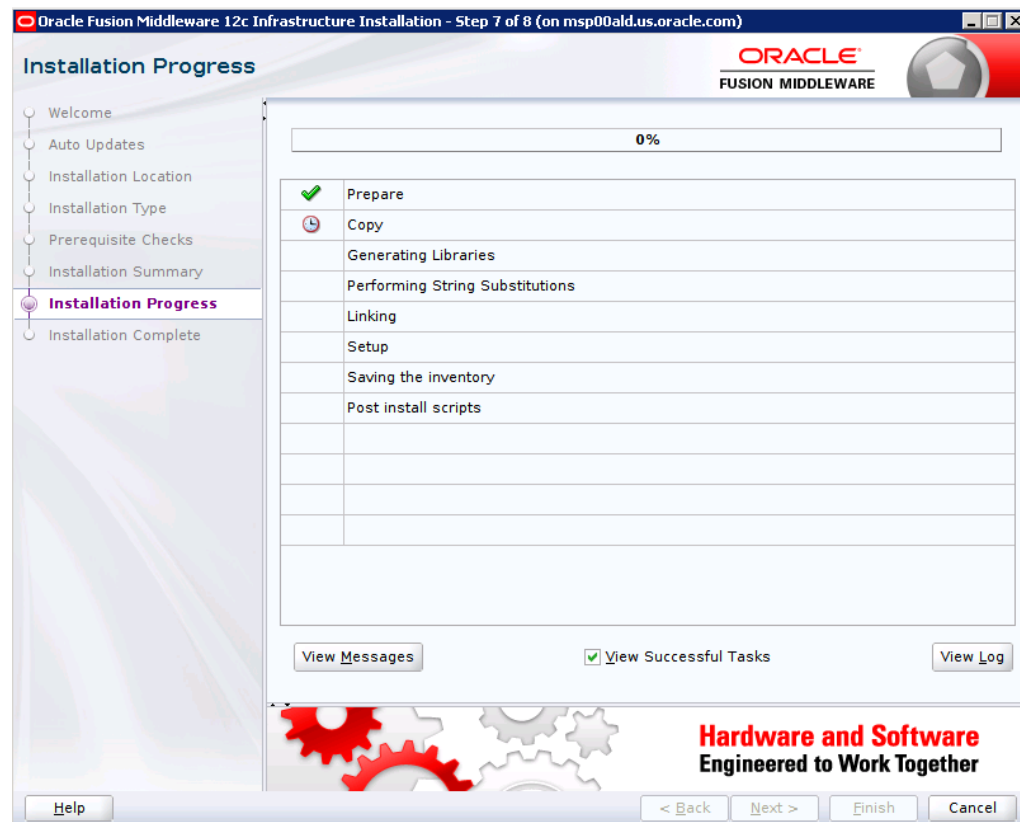
This screen will verify that the system meets the minimum necessary requirements.



7. Click Next.

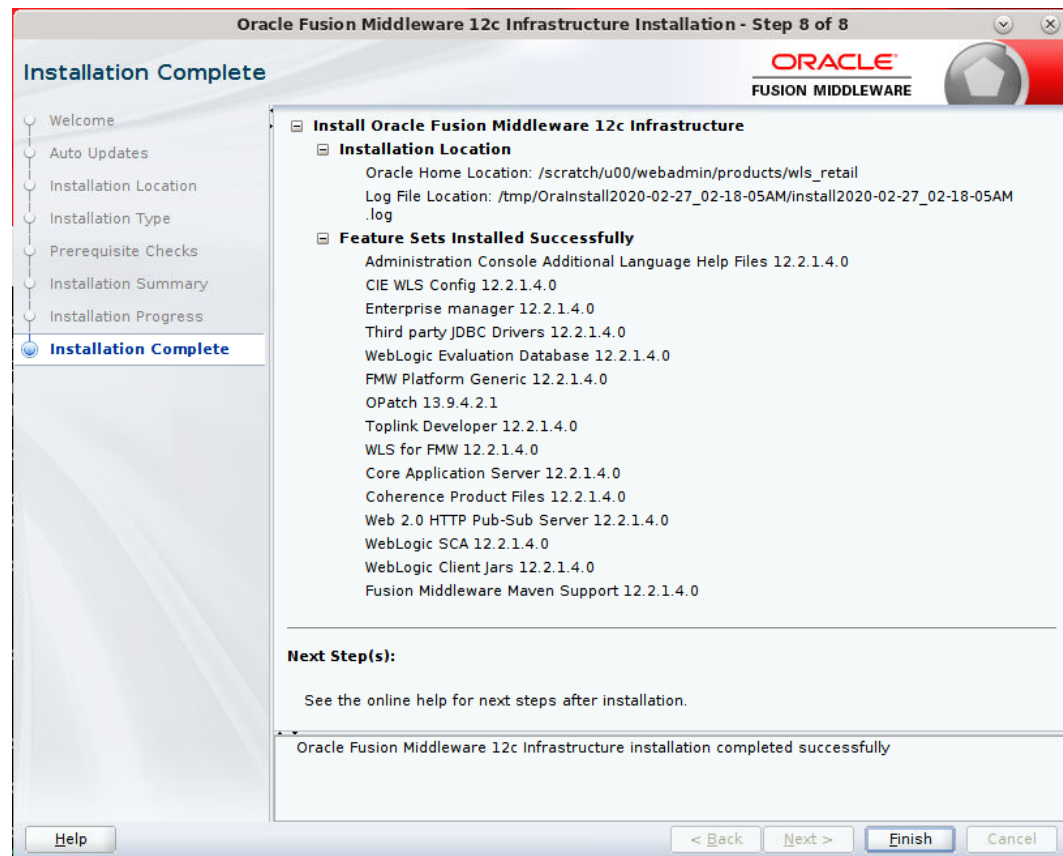


8. If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.
9. If you do not have one or if you want to skip this step, clear the check box and verify your selection in the follow-up dialog box.
10. Click **Next**.



11. Click **Next**.
12. Click **Next**.
13. Click **Yes**, if you wish to remain uninformed of security issues in your configuration.

14. Click **Install**.



15. Click **Finish**.

Install RCU Database Schemas

The RCU database schemas are required for the installation of configuration of domain and retail application.

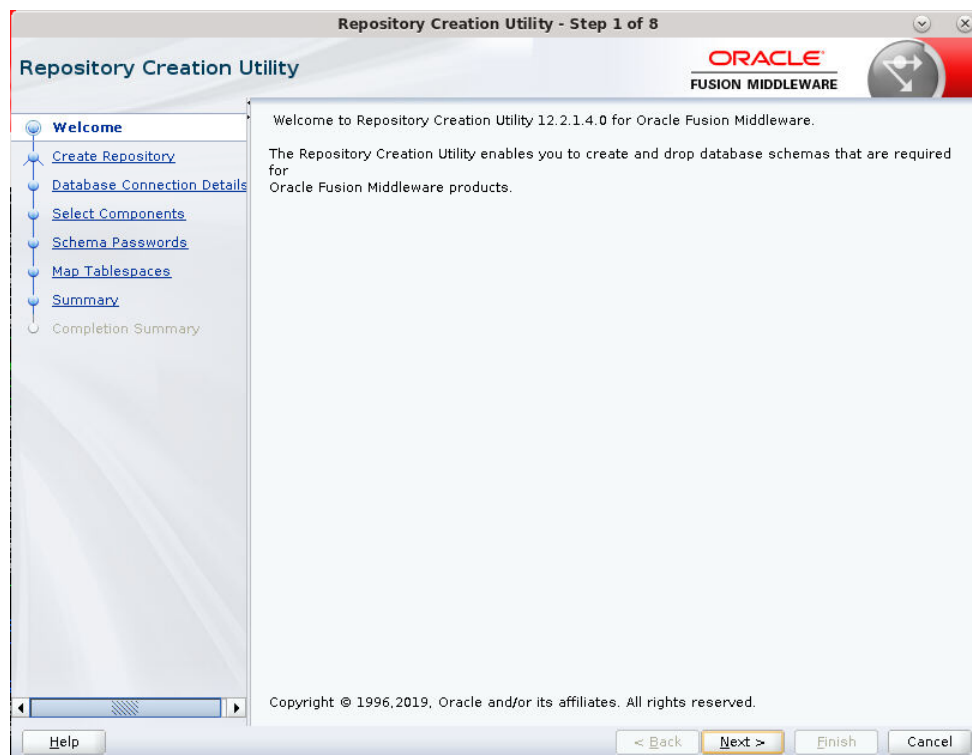
Note: Need user which have sys admin privileges to install the RCU database schemas.

The following steps are provided for the creation of the database schemas:

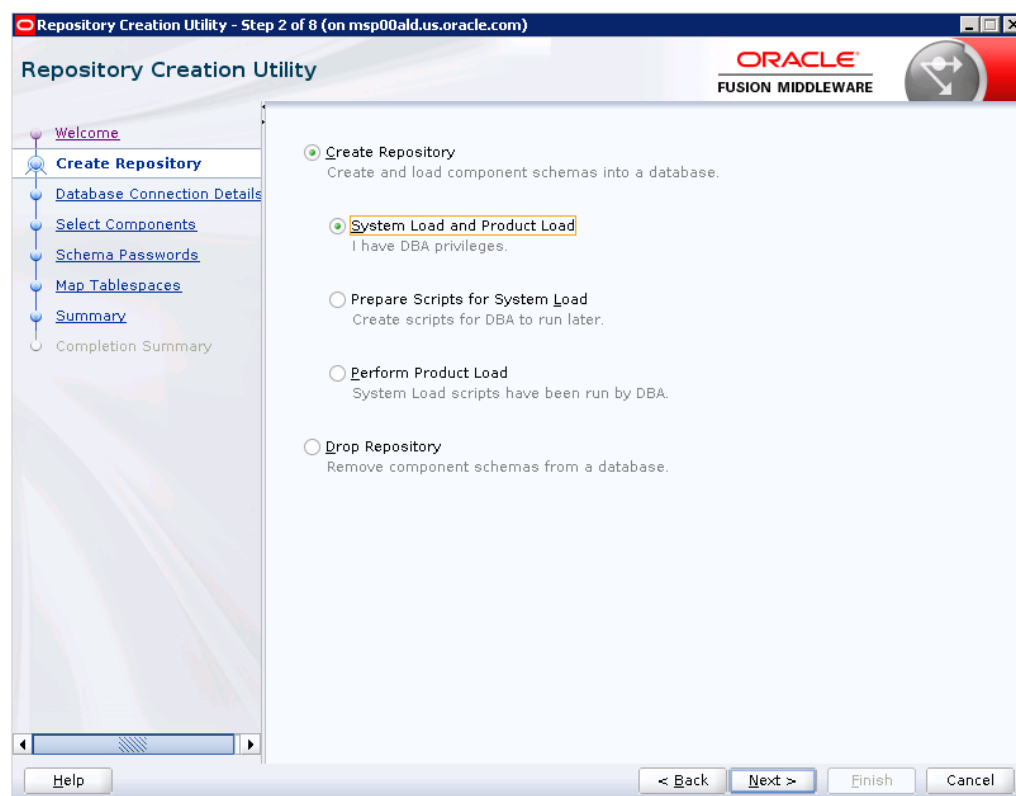
1. Navigate to the directory into which RCU is installed. For example:

```
<ORACLE_HOME>/oracle_common/bin/  
Run "./rcu"
```

2. Click **Next**.



3. Select Create Repository and System Load and Product Load. Click Next.



4. Enter database connection details:

- Database Type: Oracle Database
- Host Name: dbhostname.us.oracle.com
- Port: 1521
- Service Name: db servicename
- Username: sys
- Password: <syspassword>
- Role: SYSDBA

Repository Creation Utility - Step 3 of 8 (on msp00ald.us.oracle.com)

Repository Creation Utility

ORACLE
FUSION MIDDLEWARE

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

Database Type: Oracle Database

Connection String Format: ☒ Connection Parameters ☐ Connection String

Connect String

Host Name: dbhostname.us.oracle.com

Port: 1521

Service Name: pborcl

Username: sys as SYSDBA

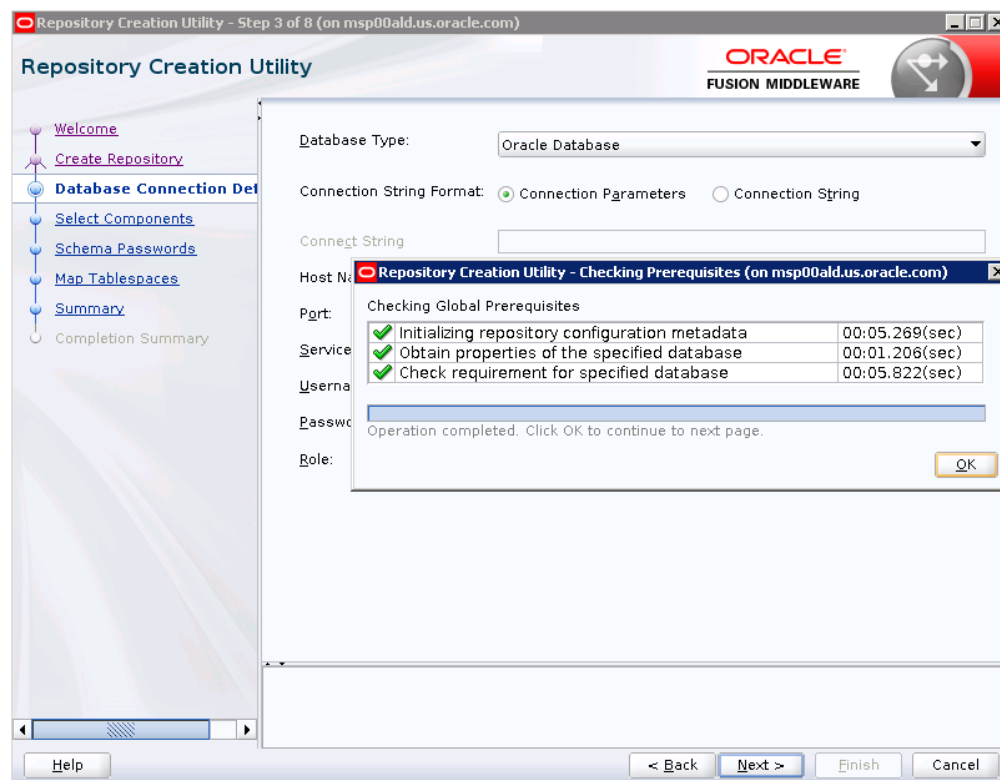
Password:

Role: Normal

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

Help < Back Next > Finish Cancel

5. Click **Next**. The Installer checks prerequisites.
6. When the prerequisite checks are complete, click **OK**. Click **Next**.



7. Click the **Create a new prefix** option, the prefix name for your schemas should be unique to your application environment.
Example: ReIM, ALLOC, ReSA, etc
8. Select the components to create:
 - Meta Data Services
 - Oracle Platform Security Services

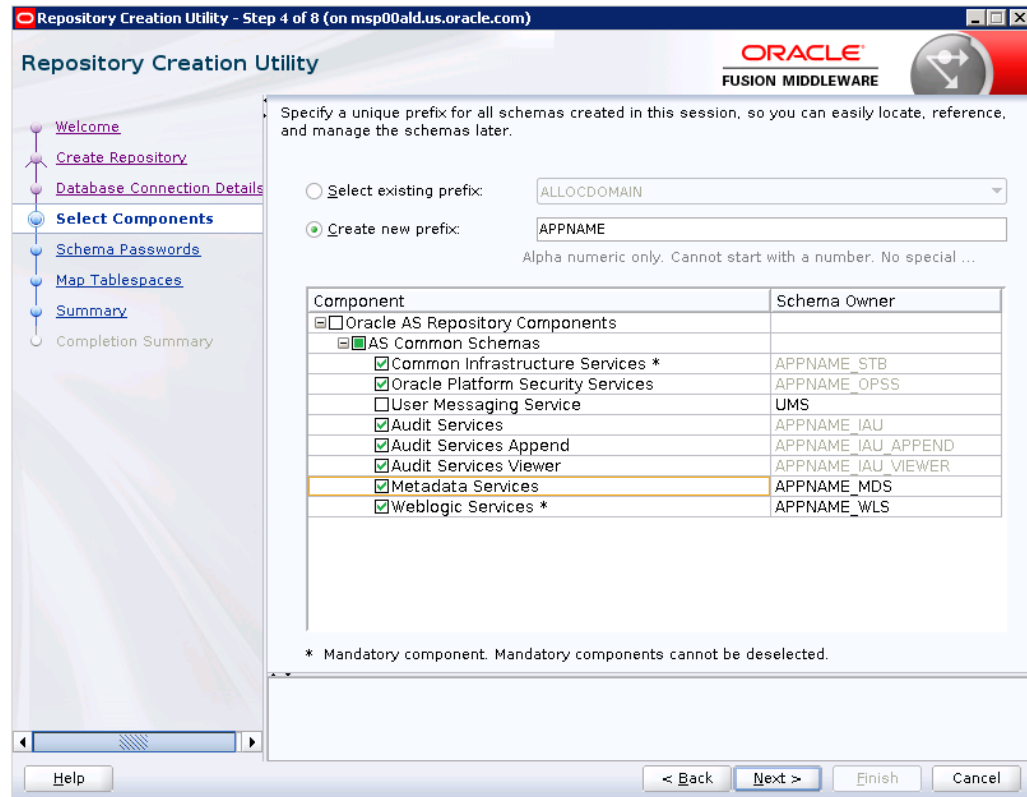
Note: Once OPSS schema is selected, the following dependent schemas will get selected automatically.

Audit Services

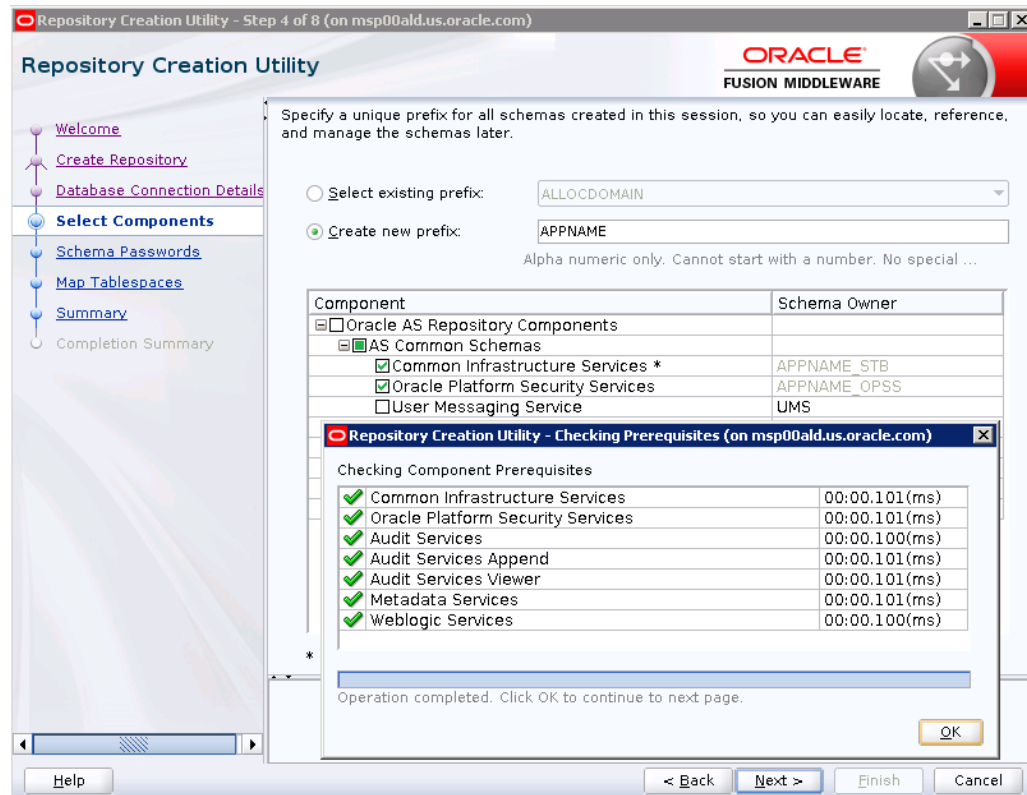
Audit Services Append

Audit Services Viewer

Note: STB schema will be already selected as part of the Common Infrastructure component.



9. Click Next.



10. Enter password of your choice.

Note: This password is needed at the time of ADF domain creation.

Repository Creation Utility - Step 5 of 8 (on msp00ald.us.oracle.com)

Repository Creation Utility

ORACLE
FUSION MIDDLEWARE

Define passwords for main and auxiliary schema users.

☒ Use same passwords for all schemas

Password:

Alpha numeric only. Cannot start with a number.
No special characters except: \$, #, ., _.

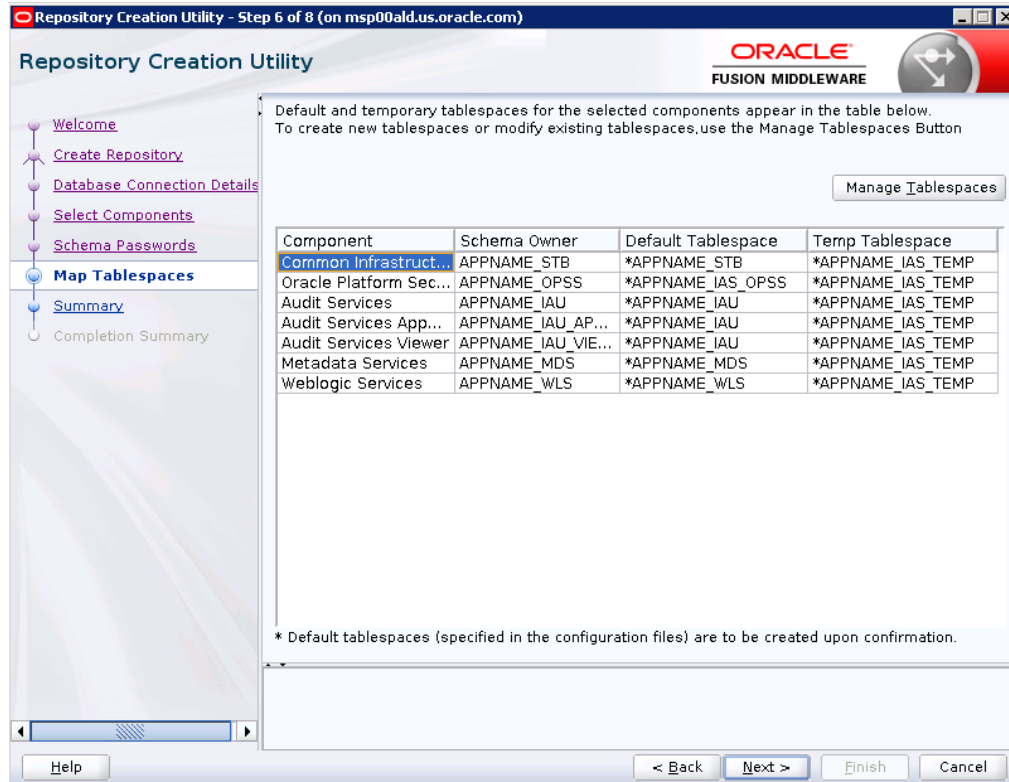
Confirm Password:

☐ Use main schema passwords for auxiliary schemas

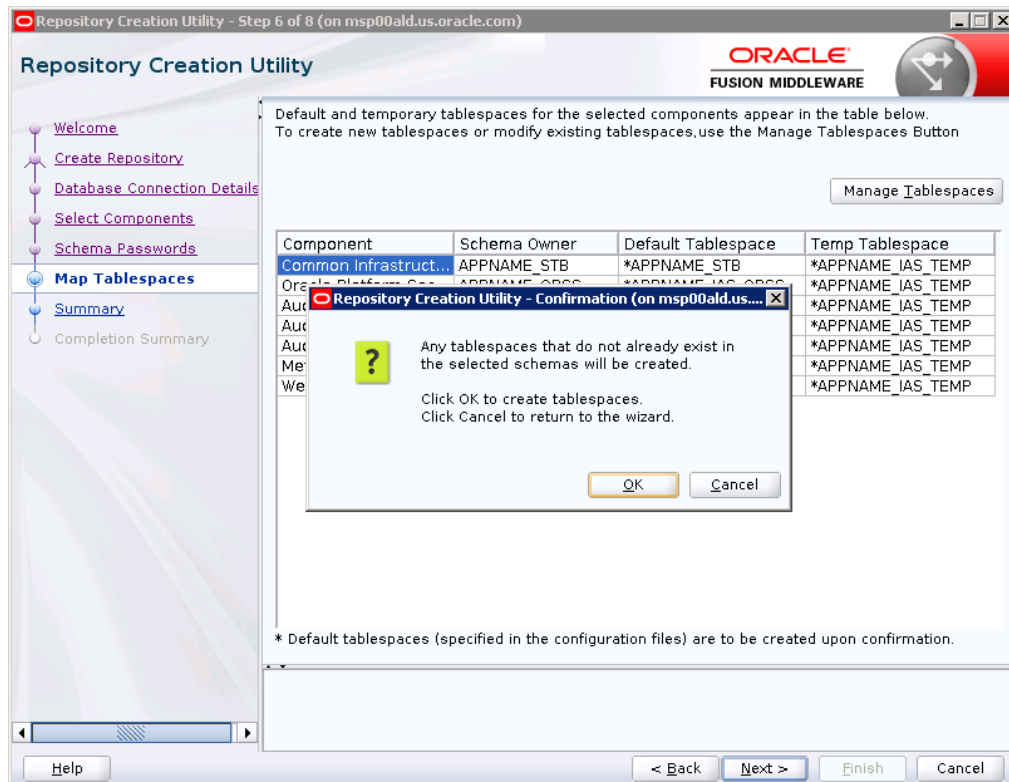
☐ Specify different passwords for all schemas

Help < Back Next > Finish Cancel

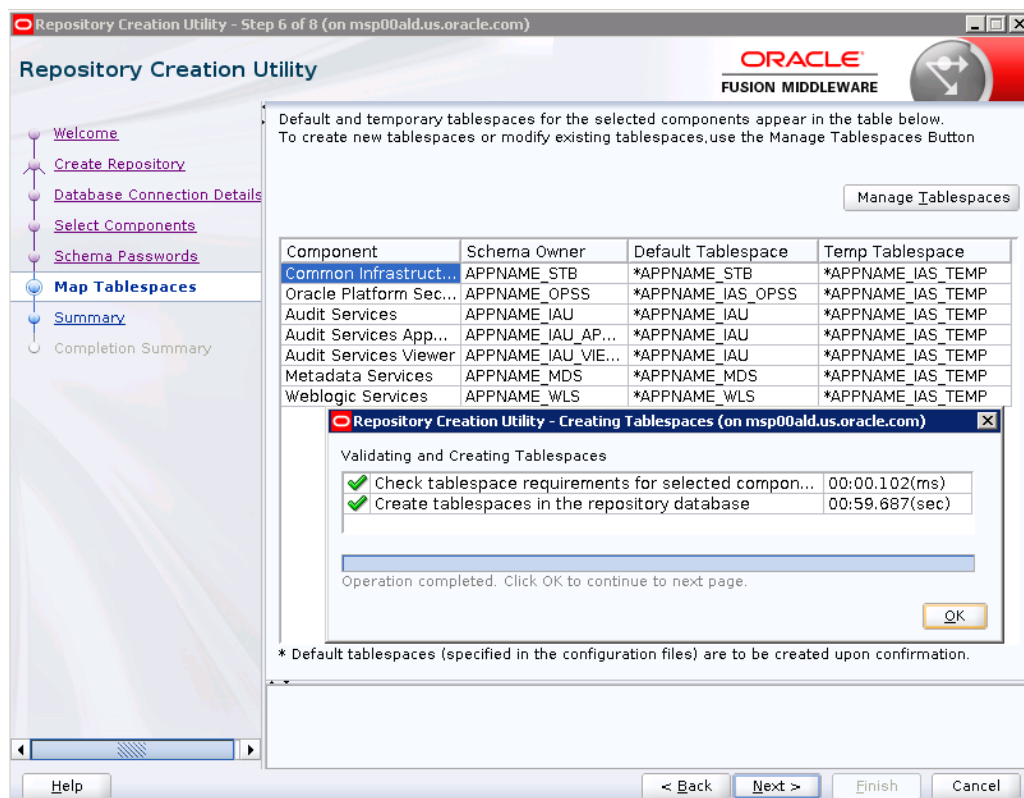
11. Provide the password and click **Next**.



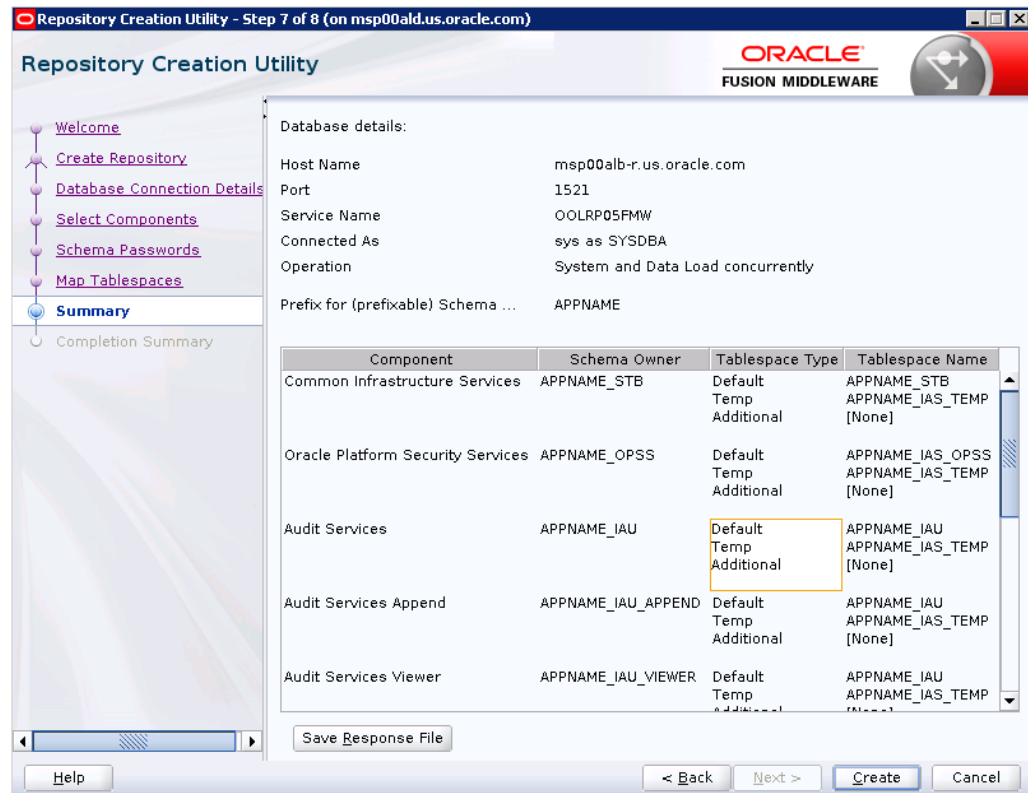
12. Click **Next**. A Repository Creation notification will appear. Click **OK**.



13. Tablespaces are created, and the progress will be displayed in a pop-up notification. When the operation is completed, click **OK**.

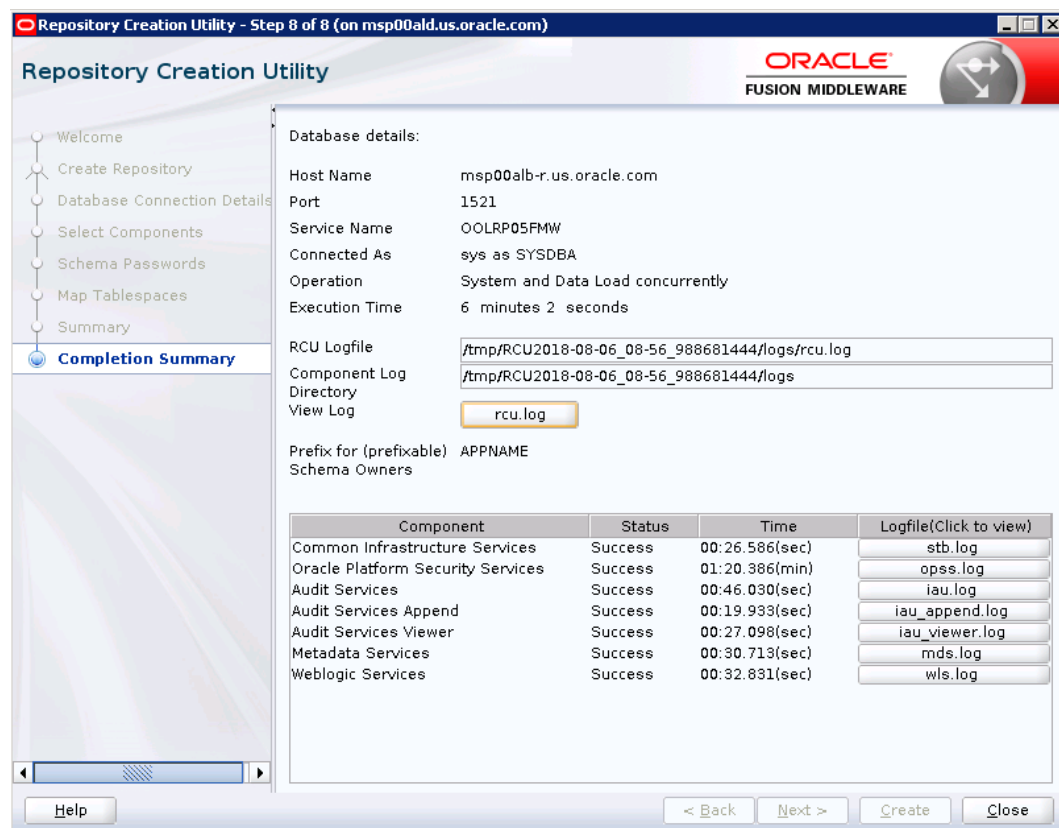


14. Click **Create**. The schema is created.



Upon successful creation of database schemas, a screen will appear with all the schemas created.

15. Click Close.



Create a New ADF Domain (with managed server and EM)

To create a new domain and managed server with ADF libraries and EM, follow the below steps:

1. Set the environment variables:

```
export JAVA_HOME=<JDK_HOME>
(Example:/u00/webadmin/products/jdk_java) [JDK_HOME is the location where
jdk has been installed)
export PATH=$JAVA_HOME/bin:$PATH
export ORACLE_HOME=<ORACLE_HOME>/
(Example:/u00/webadmin/products/wls_retail/)

cd $ORACLE_HOME/oracle_common/common/bin
(ORACLE_HOME is the location where Weblogic has been installed.)
```

2. Run the following command:

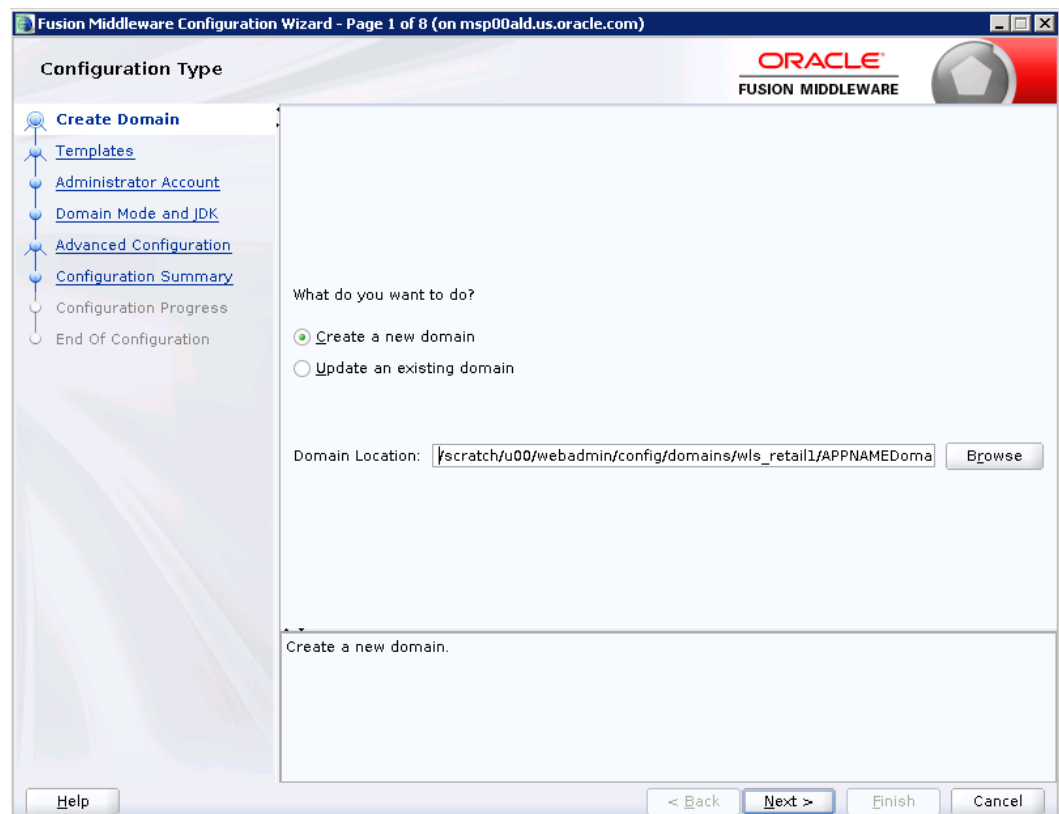
```
./config.sh
```

3. Select **Create a new domain**.

Domain location: Specify the path to the <DOMAIN_HOME>

Example:/u00/webadmin/config/domains/wls_retail/APPNAMEDomain

Click **Next**.



4. Select **Create Domain Using Product Templates**.

5. Check the following components:

Oracle Enterprise Manager

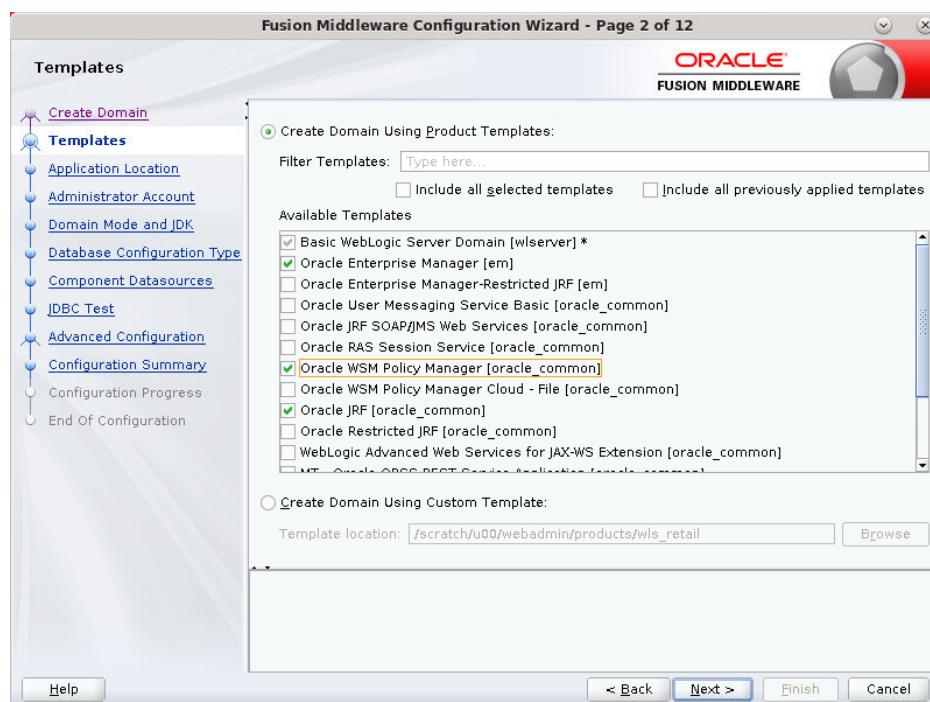
Oracle WSM Policy Manager

Note: When Oracle Enterprise Manager component is selected, the following dependent components are selected automatically:

Oracle JRF

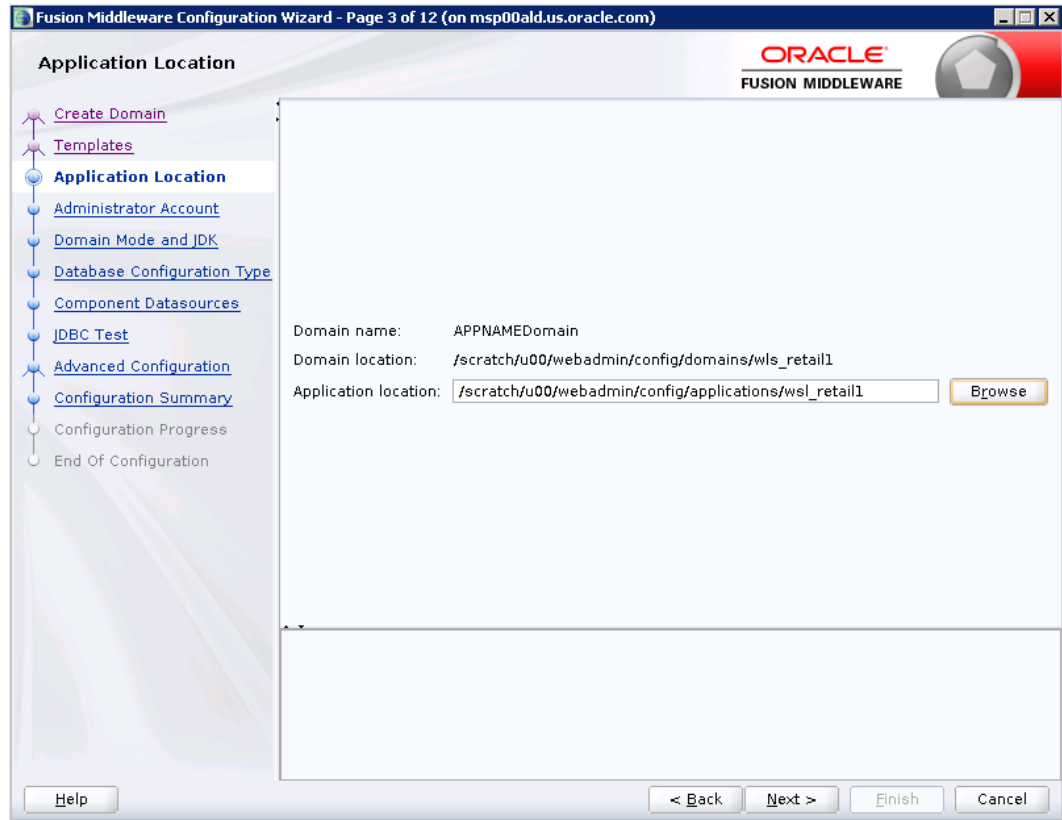
Weblogic Coherence Cluster Extension

6. Click Next.



Application location: Application directory location. Example:
/u00/webadmin/config/applications/wls_retail/APPNAMEDomain

7. Click Next.



8. Provide the WebLogic administrator credentials and click **Next**:

- Username: weblogic
- Password: <Password>

The screenshot shows the 'Administrator Account' step of the Fusion Middleware Configuration Wizard. The left sidebar contains a navigation tree with the following items: Create Domain, Templates, Application Location, Administrator Account (selected), Domain Mode and JDK, Database Configuration Type, Component Datasources, JDBC Test, Advanced Configuration, Configuration Summary, Configuration Progress, and End Of Configuration. The main area has three input fields: 'Name' with the value 'weblogic', 'Password' with masked characters, and 'Confirm Password' with masked characters. Below these fields is a note: 'Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.' At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Fusion Middleware Configuration Wizard - Page 4 of 12 (on msp00ald.us.oracle.com)

Administrator Account

ORACLE
FUSION MIDDLEWARE

Create Domain
Templates
Application Location
Administrator Account
Domain Mode and JDK
Database Configuration Type
Component Datasources
JDBC Test
Advanced Configuration
Configuration Summary
Configuration Progress
End Of Configuration

Name: weblogic
Password: *****
Confirm Password: *****

Must be the same as the password. Password must contain at least 8 alphanumeric characters with at least one number or special character.

Help < Back Next > Finish Cancel

9. Select Domain Mode as Production and the JDK to use (as applicable) and click Next.

The screenshot shows the 'Domain Mode and JDK' step of the Fusion Middleware Configuration Wizard. The left sidebar is the same as in the previous step, with 'Domain Mode and JDK' selected. The main area has two sections. The 'Domain Mode' section has two radio buttons: 'Development' (unselected) and 'Production' (selected). Below 'Production' is a note: 'Require the entry of a username and password, and do not poll for applications to deploy.' The 'JDK' section has two radio buttons: 'Oracle HotSpot 1.8.0_171 /scratch/u00/webadmin/products/jdk_java' (selected) and 'Other JDK Location:' (unselected). The 'Other JDK Location' has a text input field and a 'Browse' button. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Fusion Middleware Configuration Wizard - Page 5 of 12 (on msp00ald.us.oracle.com)

Domain Mode and JDK

ORACLE
FUSION MIDDLEWARE

Create Domain
Templates
Application Location
Administrator Account
Domain Mode and JDK
Database Configuration Type
Component Datasources
JDBC Test
Advanced Configuration
Configuration Summary
Configuration Progress
End Of Configuration

Domain Mode

☐ Development
Utilize boot.properties for username and password, and poll for applications to deploy.

☒ **Production**
Require the entry of a username and password, and do not poll for applications to deploy.

JDK

☒ Oracle HotSpot 1.8.0_171 /scratch/u00/webadmin/products/jdk_java

☐ Other JDK Location: Browse

Help < Back Next > Finish Cancel

10. Select **RCU Data**.

- Vendor: Oracle
- DBMS/Service: db servicename
- Host Name: dbhostname.us.oracle.com
- Port: 1521
- Schema Owner: APPNAME_STB (Example: ALLOC_STB, ReSA_STB, etc)
- Password: <Password>. This password which was used for RCU schema creation.

Fusion Middleware Configuration Wizard - Page 6 of 12 (on msp00ald.us.oracle.com)

Database Configuration Type

Specify AutoConfiguration Options Using:

☒ RCU Data ☐ Manual Configuration

Enter the database connection details using the schema credentials corresponding to Common Infrastructure Services component in the Repository Creation Utility. The Wizard uses this connection to automatically configure the datasources required for components in this domain.

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service connections; ...

☒ Connection Parameters ☐ Connection URL String

Host Name: dbhostname.us.oracle.com

DBMS/Service: pborcl Port: 1521

Schema Owner: APPNAME_STB Schema Password: *****

Get RCU Configuration Cancel

Connection Result Log

Successfully Done.

Click "Get RCU Configuration" button to test the connection and activate the "Next" button.

Help < Back Next > Finish Cancel

11. Click the **Get RCU Configuration** button.

12. Click **Next**.

Fusion Middleware Configuration Wizard - Page 7 of 12 (on msp00ald.us.oracle.com)

JDBC Component Schema

Vendor: Oracle Driver: *Oracle's Driver (Thin) for Service connections; Ve

☒ Connection Parameters ☐ Connection URL String

Host Name: dbhostname.us.oracle.com

DBMS/Service: pborcl Port: 1521

Schema Owner: APPNAME_STB Schema Password: *****

Oracle RAC configuration for component schemas:

☐ Convert to GridLink ☐ Convert to RAC multi data source ☐ Don't convert

Edits to the data above will affect all checked rows in the table below.

	Component Schema	DBMS/Service	Host Name	Port	Schema Ow...	Schema Passw...
<input checked="" type="checkbox"/>	LocalSvcTbl Schema	pborcl	dbhostname.us.	1521	APPNAME_STB	*****
<input checked="" type="checkbox"/>	WLS Schema	pborcl	dbhostname.us.	1521	APPNAME_STB	*****
<input checked="" type="checkbox"/>	OWSM MDS Schema	pborcl	dbhostname.us.	1521	APPNAME_STB	*****
<input checked="" type="checkbox"/>	OPSS Audit Schema	pborcl	dbhostname.us.	1521	APPNAME_STB	*****
<input checked="" type="checkbox"/>	OPSS Audit Viewer S	pborcl	dbhostname.us.	1521	APPNAME_STB	*****
<input checked="" type="checkbox"/>	OPSS Schema	pborcl	dbhostname.us.	1521	APPNAME_STB	*****

Help < Back Next > Finish Cancel

13. Click **Next** and it will test to make sure it can connect to your datasources.

Fusion Middleware Configuration Wizard - Page 8 of 12 (on msp00ald.us.oracle.com)

JDBC Component Schema Test

☐ Status Component Schema JDBC Connection URL

<input checked="" type="checkbox"/>	LocalSvcTbl Schema	jdbc:oracle:thin:@//
<input checked="" type="checkbox"/>	WLS Schema	jdbc:oracle:thin:@//
<input checked="" type="checkbox"/>	OWSM MDS Schema	jdbc:oracle:thin:@//
<input checked="" type="checkbox"/>	OPSS Audit Schema	jdbc:oracle:thin:@//
<input checked="" type="checkbox"/>	OPSS Audit Viewer Schema	jdbc:oracle:thin:@//
<input checked="" type="checkbox"/>	OPSS Schema	jdbc:oracle:thin:@//

Test Selected Connections Cancel Testing

Connection Result Log

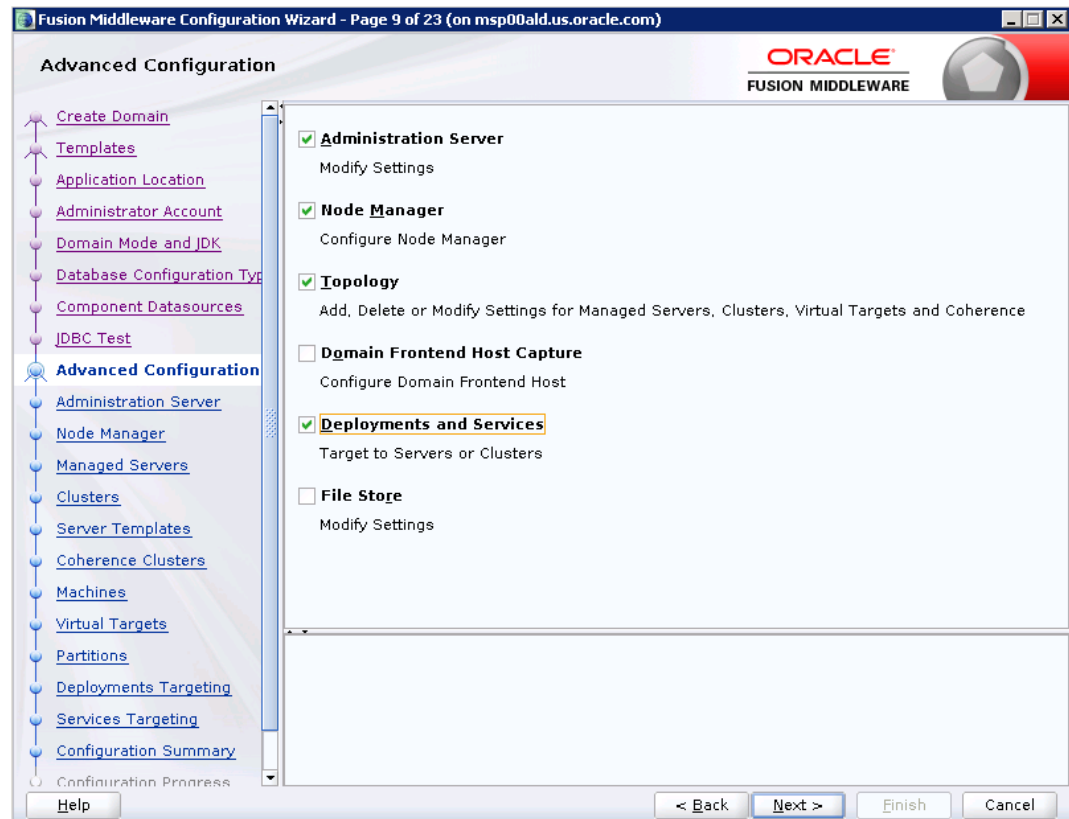
User=APPNAME_STB
Password=*****
SQL Test=ISVALID

CFGFWK-64213: Test Successful
CFGFWK-64213: JDBC connection test was successful.
CFGFWK-64213: No action required.

Component Schema=OWSM MDS Schema

Help < Back Next > Finish Cancel

14. Click **Next** to continue
15. Select advanced configuration for:
 - Administration Server
 - Node manager
 - Managed Servers, Clusters and Coherence
 - Deployments and Services



16. Configure the Administration Server:
 - Server Name: <APP name>_AdminServer
 - Listen address: Appserver Hostname or IPAddress of the Appserver Host.
 - Listen port: <Port for Admin Server> Note: The port that is not already used.
 - Server Groups: Unspecified

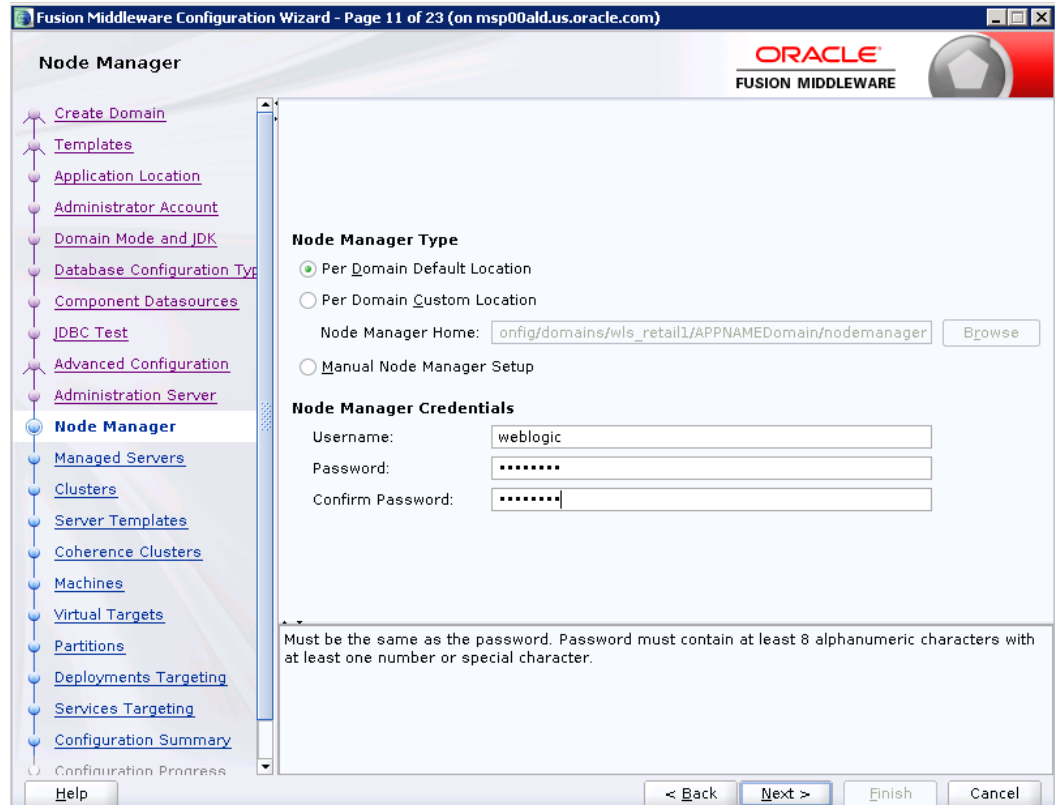
The screenshot shows the 'Administration Server' configuration page of the Fusion Middleware Configuration Wizard. The left sidebar contains a tree of configuration steps, with 'Administration Server' selected. The main area contains the following fields:

- Server Name: AdminServer
- Listen Address: APPhostname.us.oracle.com
- Listen Port: 7001
- Enable SSL: ☐
- SSL Listen Port:
- Server Groups: Unspecified

A note at the bottom states: 'Port number must be between 1 and 65535, and different from SSL listen port and coherence port.' The bottom of the window features navigation buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

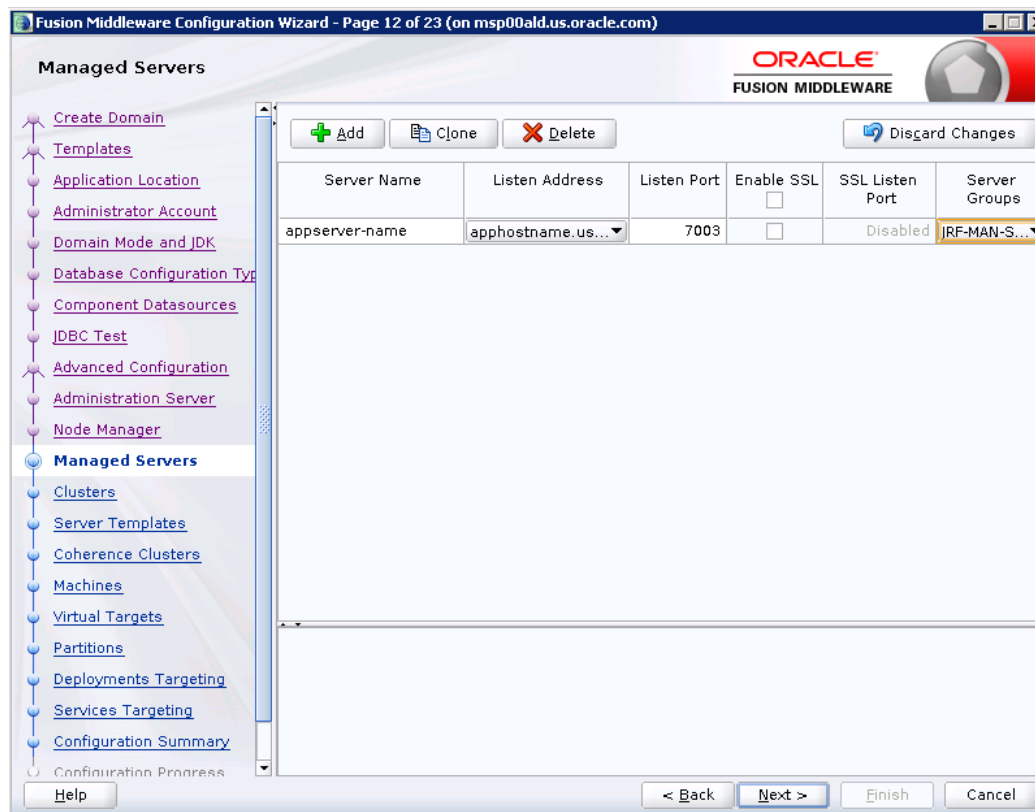
17. Configure Node Manager:

- Node manager type: Per domain default location
- Username: weblogic
- Password: <Password for weblogic>

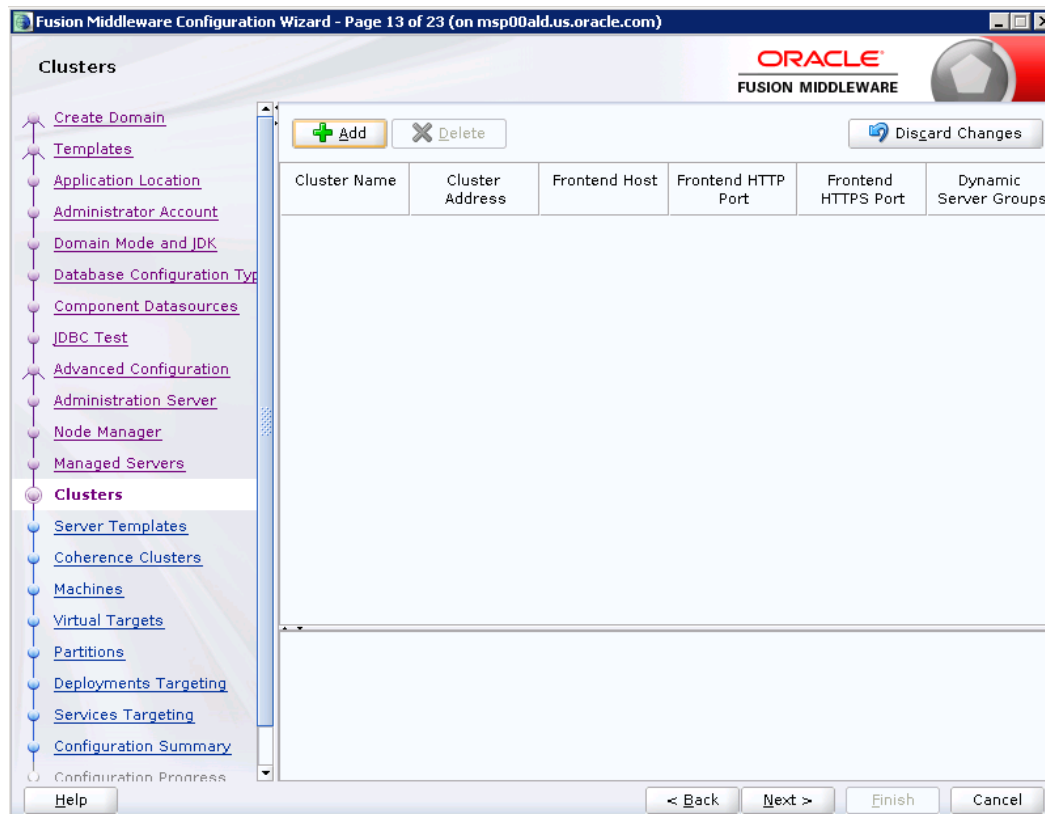


18. Click the Add button.

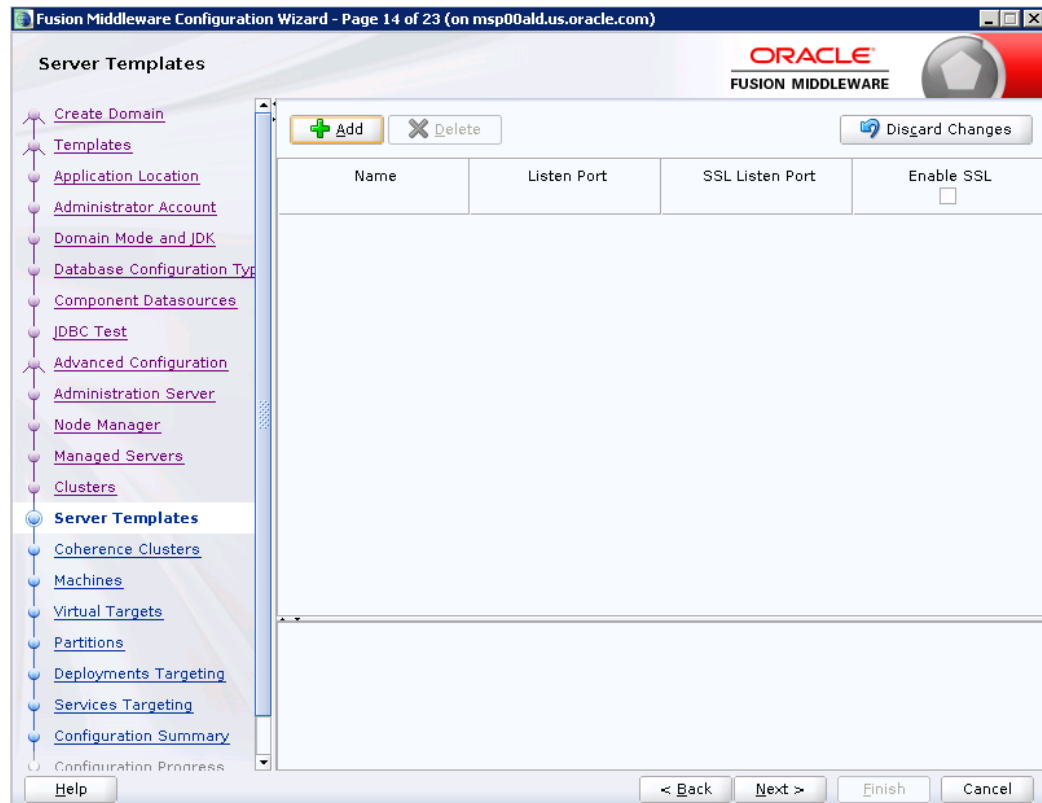
- Server Name: <appname-server>
- Listen address: Appserver Hostname or IPAddress of the Appserver Host
- Listen port: <Port for Managed Server> Note: The port used here must be a free port.
- Server Groups: JRF-MAN-SVR



19. Skip Configure Clusters and click Next.

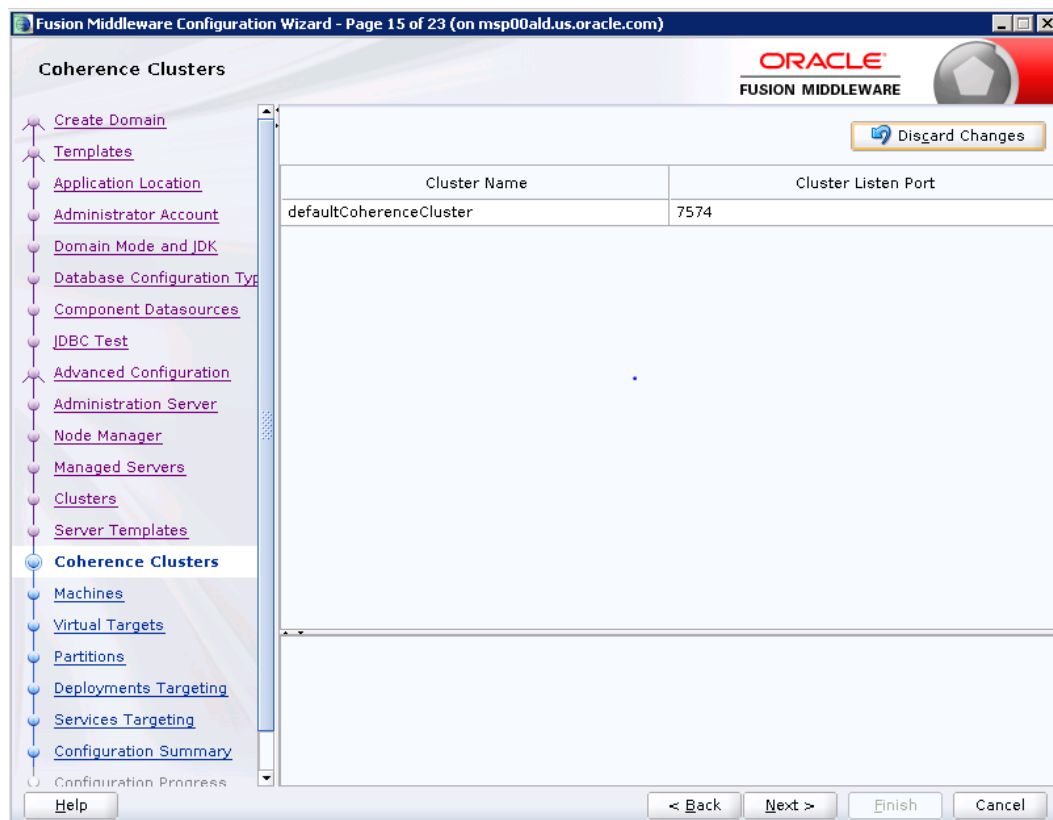


20. No change needed. Click **Next**.



21. Skip Server Templates and click **Next**.

22. Click **Next**.

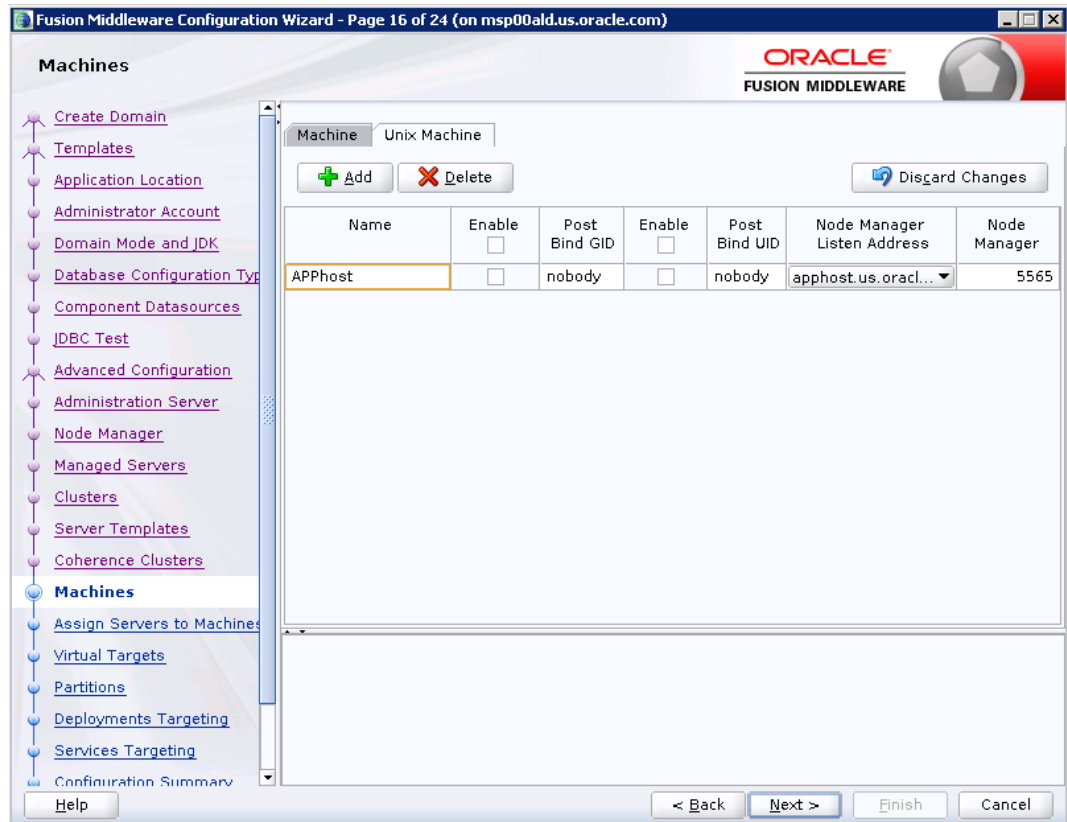


23. Configure Machines

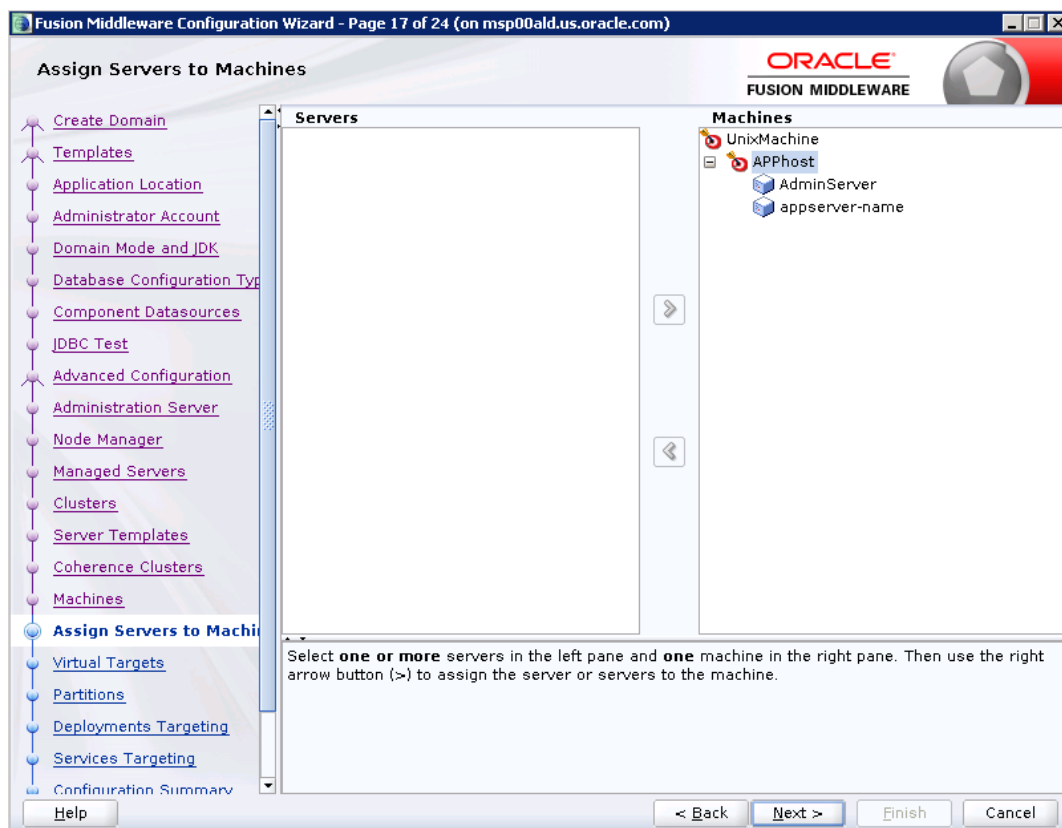
Select unix Machine :

Click the **Add** button.

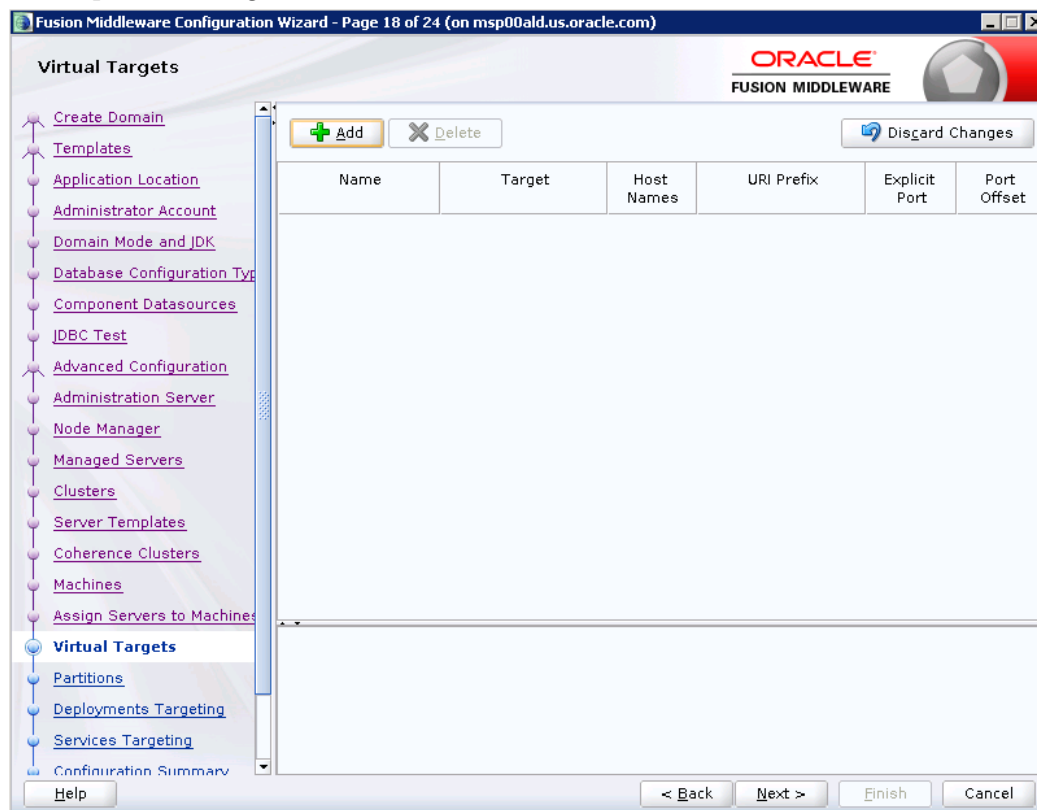
- Name: apphostname_MACHINE
- Listen address: apphostname or IPAddress
- Listen port: <Port for node manager> Note: The port used here must be a free port.



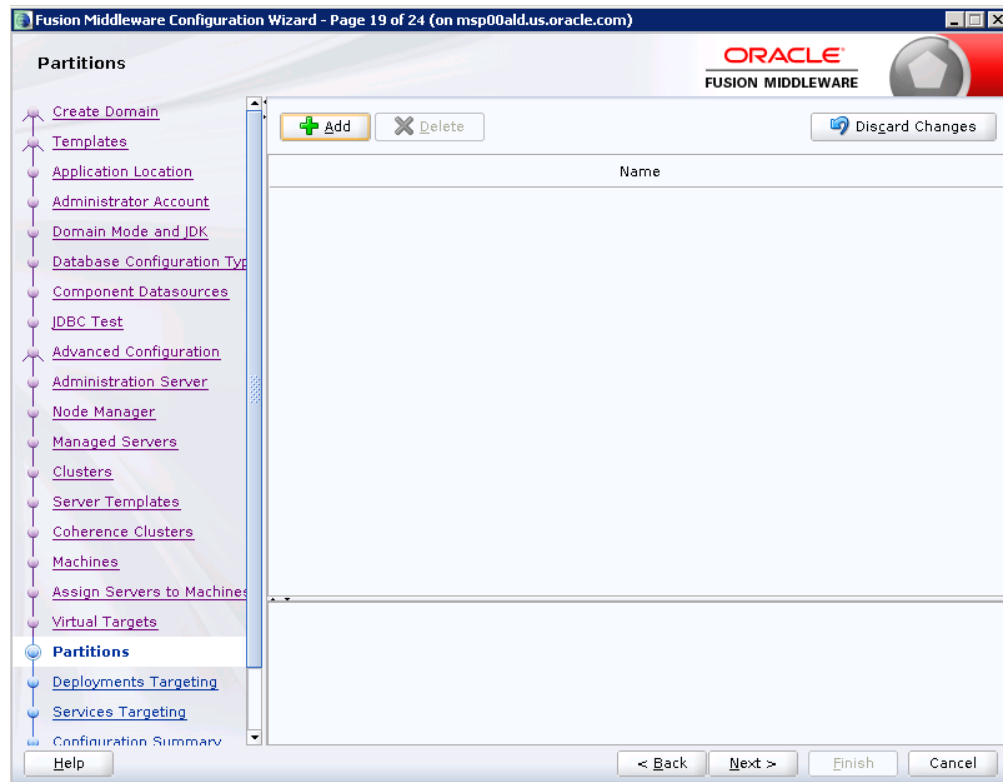
24. Assign the configured Admin server and managed servers to the new machine.



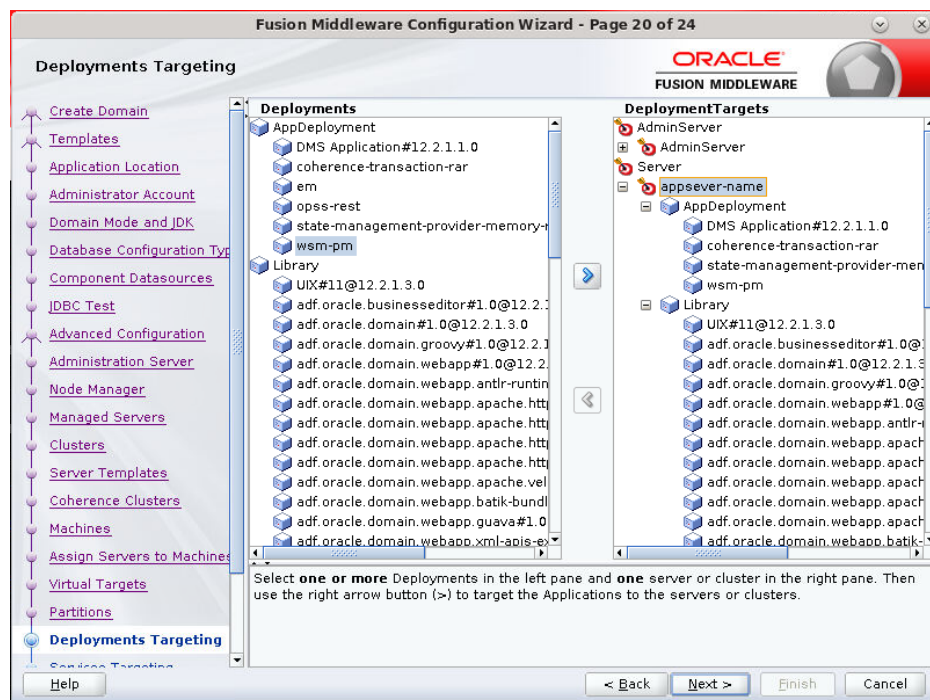
25. Skip Virtual Targets. Click Next.



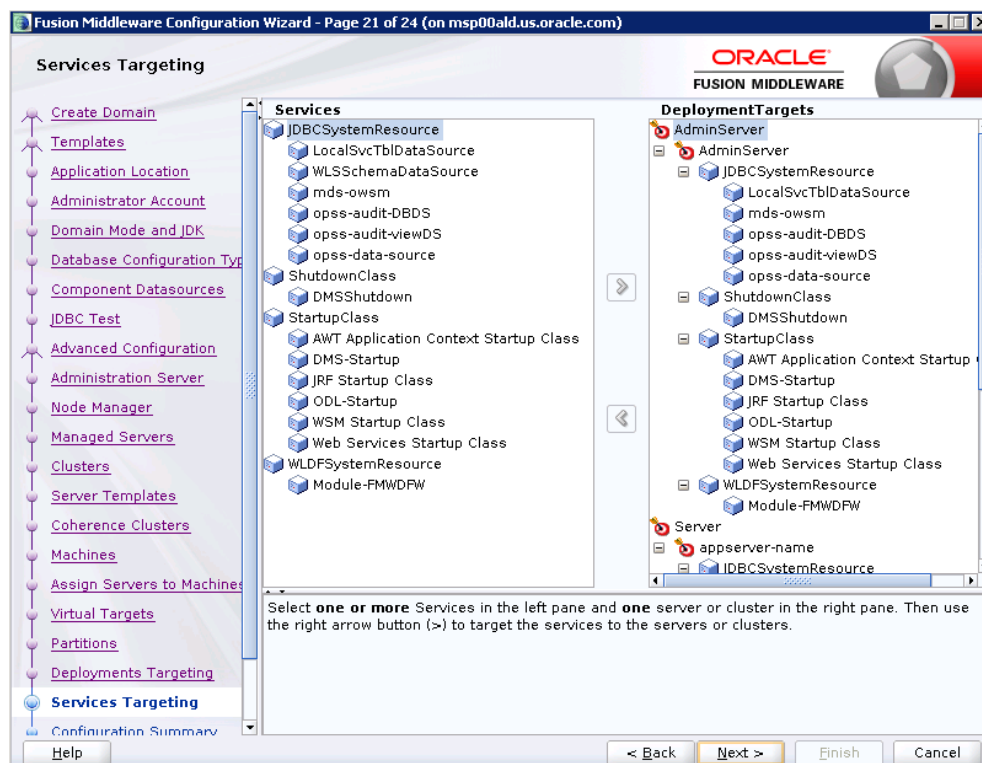
26. Skip Partitions. Click Next.



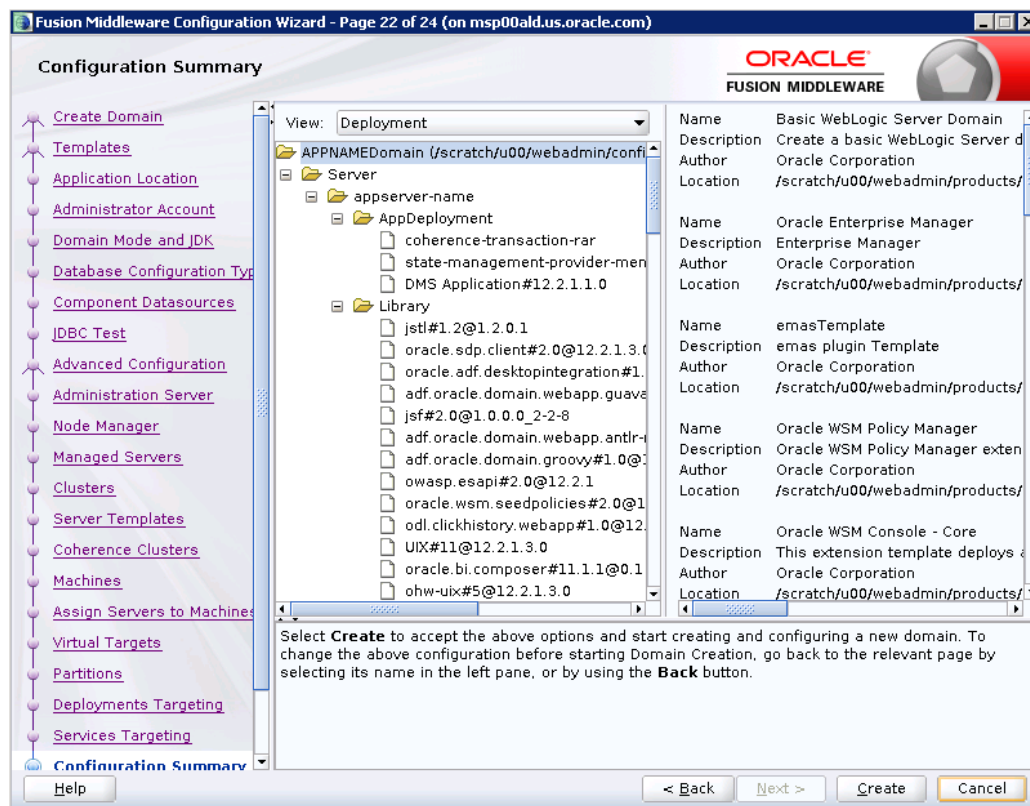
27. Target the “wsm-pm” deployment to APPNAME_AdminServer:



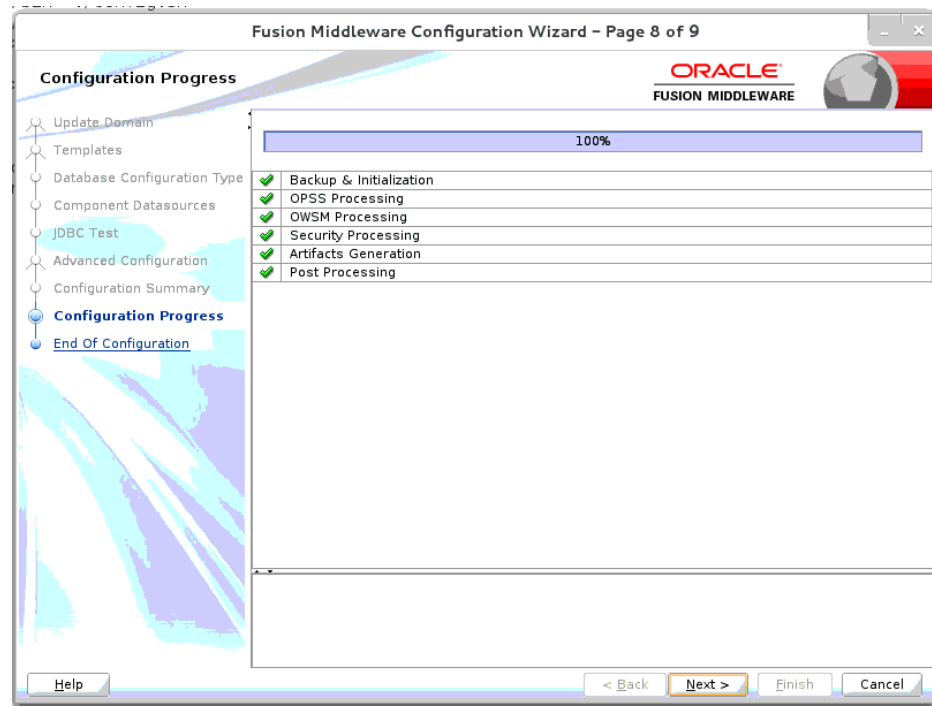
28. Click Next.



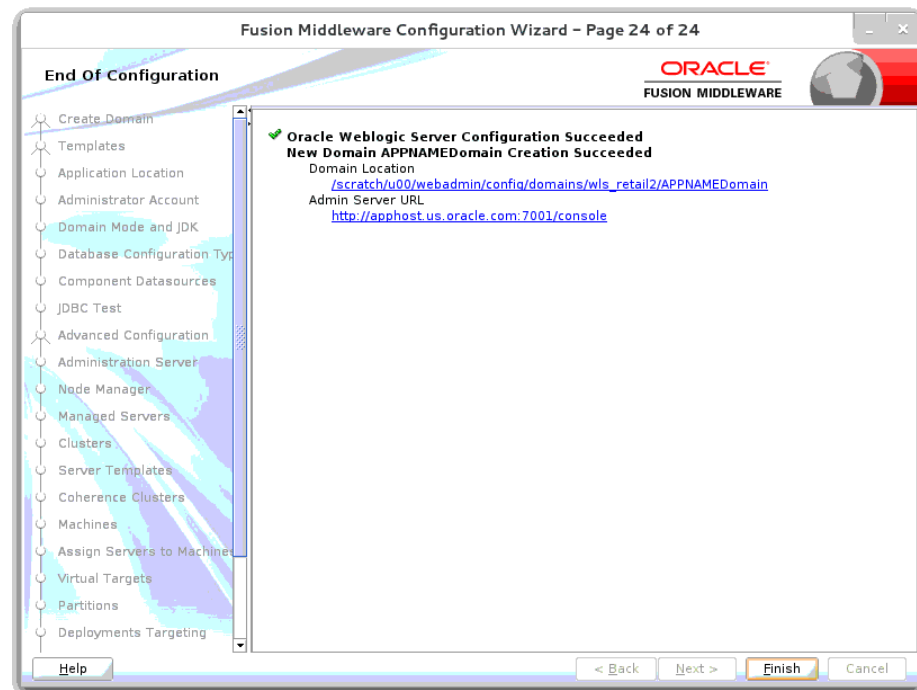
29. Click Create.



30. Click **Next**.



31. When the process completes, click **Finish**.



Start the Node Manager

1. Start the nodemanager from <DOMAIN_HOME>/bin using the following script:
nohup ./startNodeManager.sh &

Start the AdminServer (admin console)

1. Configure boot.properties for starting the Weblogic domain without prompting to username and password using the following command:
2. Create security folder at <DOMAIN_HOME>/servers/<AdminServer>/ and create boot.properties file under <DOMAIN_HOME>/servers/<AdminServer>/security
The file 'boot.properties' should have the following:

```
-----  
username=weblogic  
password=<password>  
-----
```

In the above, the password value is the password of WebLogic domain which is given at the time of domain creation.

Save the boot.properties file and start WebLogic server.

3. Start the WebLogic Domain (Admin Server) from <DOMAIN_HOME> using the following:

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

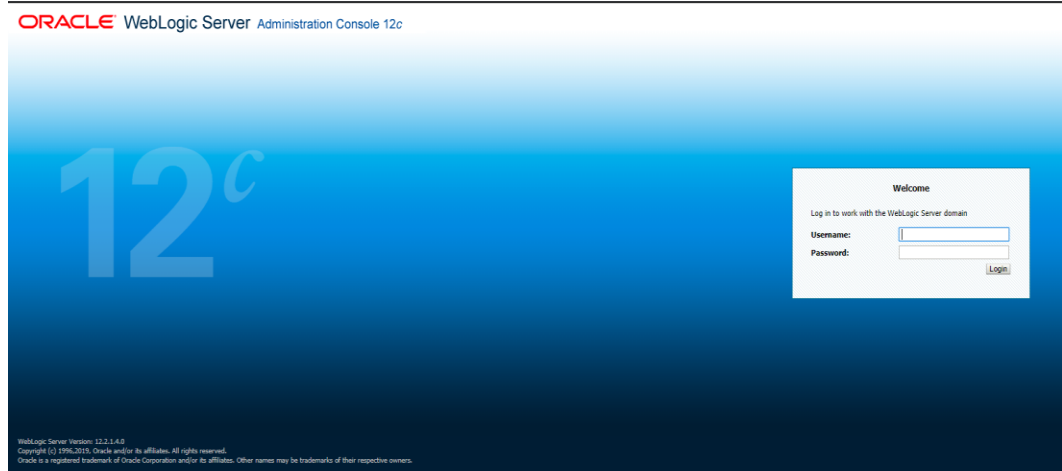
Example:

```
nohup  
/u00/webadmin/config/domains/wls_retail/RPMdomain/startWebLogic.sh &
```

4. Access the Weblogic Admin console

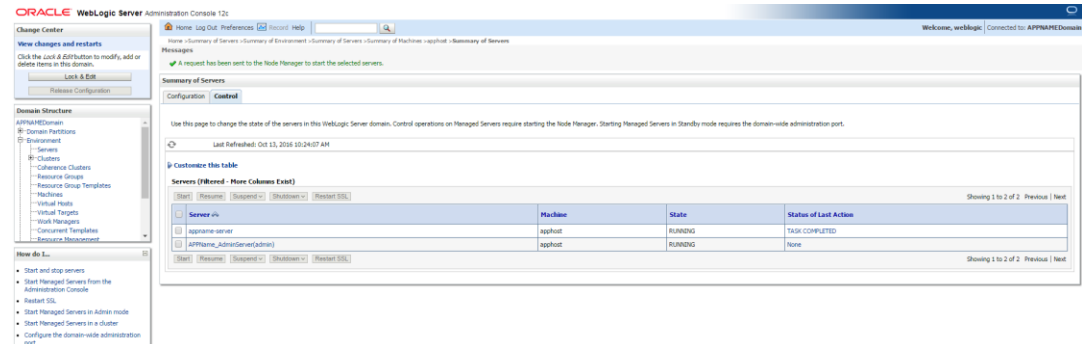
Example: http://<HOST_NAME>:<ADMIN_PORT>/console

In the below screen, provide username=weblogic and password=<weblogic password>



Start the Managed Server

After NodeManager is started, the managed servers can be started via the admin console. Navigate to Environments -> Servers and click the Control tab. Select appname-server and click **Start**.

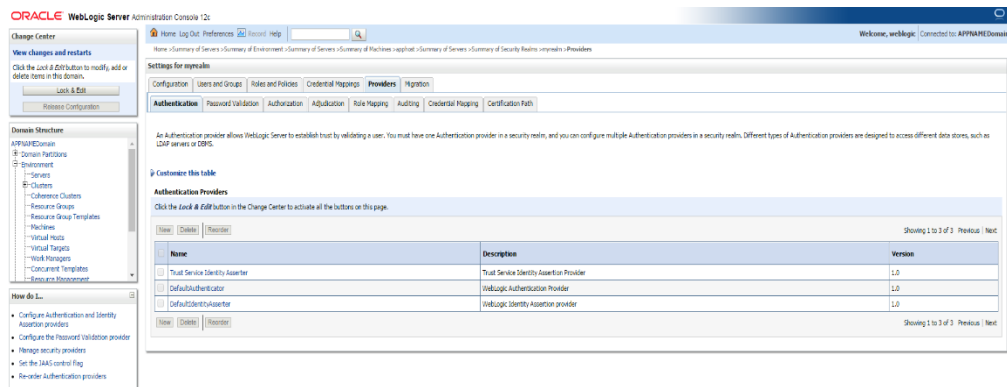


Managed Server should be up and running before configuring further steps

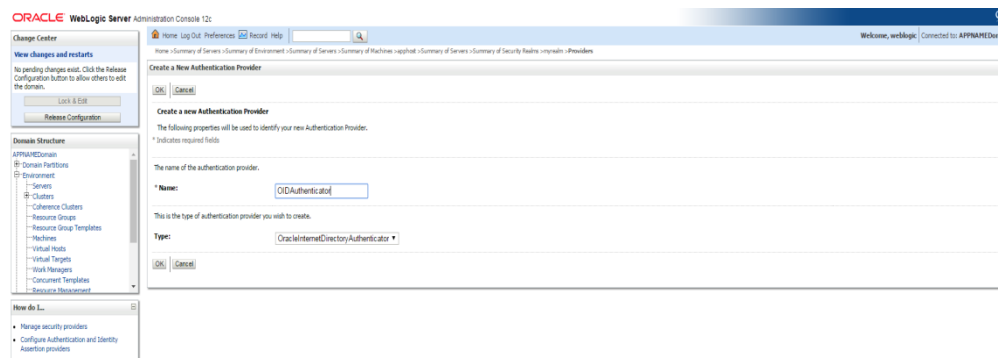
Configuration of OID LDAP Provider in Weblogic Domain:

Perform the following procedure to create LDAP providers in the domains created in the previous steps

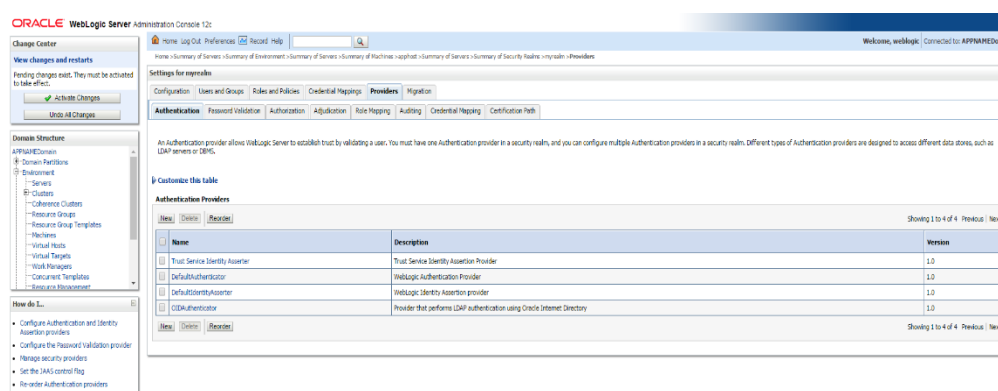
1. Log in to the Administration Console.
`http://<HOSTNAME>:<ADMIN_PORT>/console`
2. In the Domain Structure frame, click **Security Realms**.
3. In the Realms table, click **myrealm**. The Settings for myrealm page is displayed.
4. Click the Providers tab



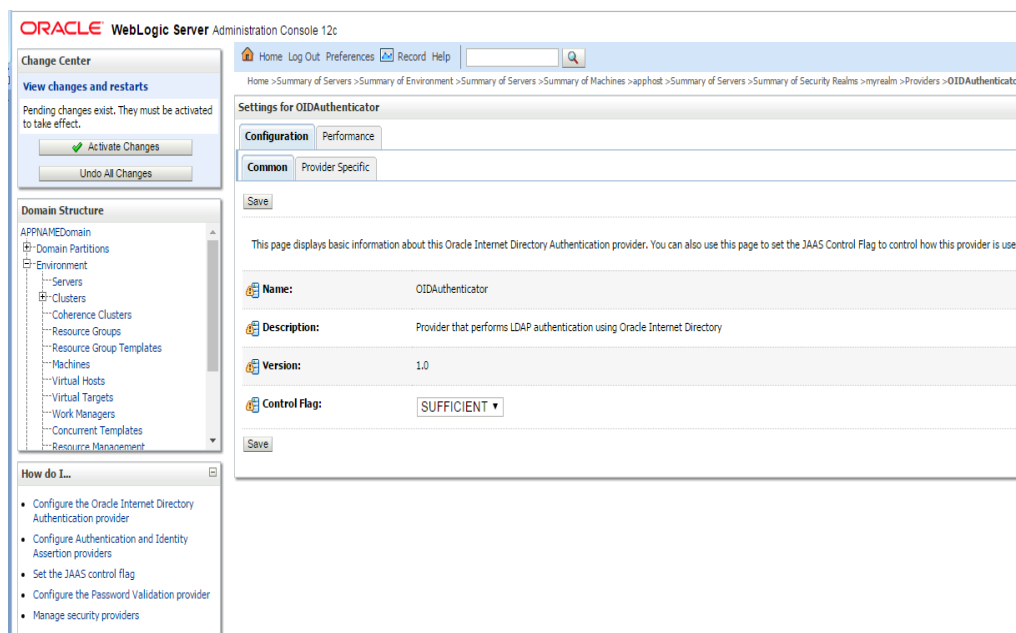
5. Click **Lock & Edit** and then click **New**. The 'Create a New Authentication Provider' page is displayed.



- Enter **OIDAuthenticator** in the Name field and select **OracleInternetDirectoryAuthenticator** as the type. Click **OK**.

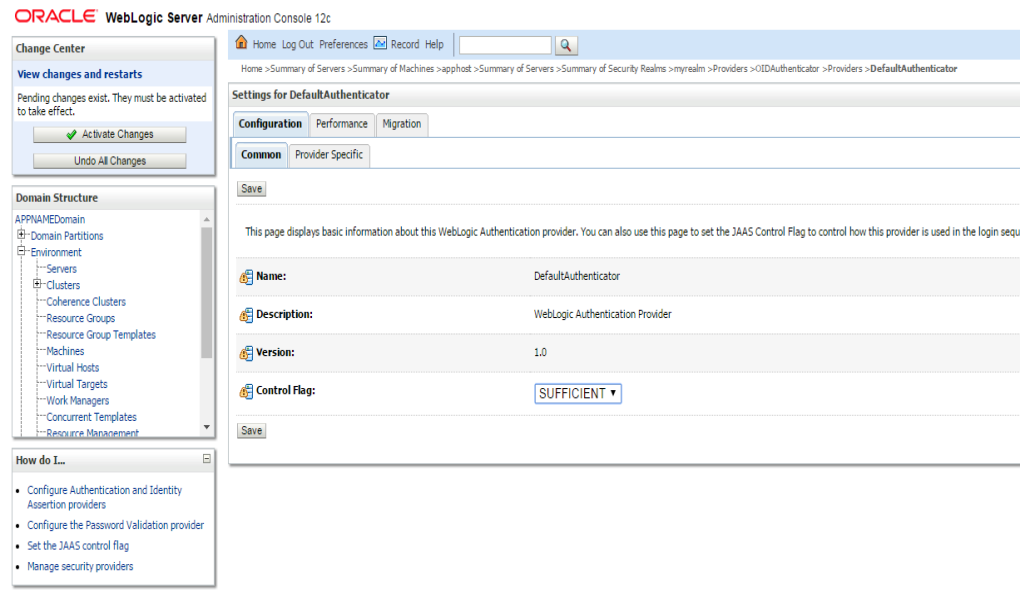


- All the providers are displayed. Click **OID Authenticator**. Settings of **OID Authenticator** are displayed.



- Set the **Control Flag** field to **SUFFICIENT** and click **Save**.

9. From the Providers tab, click on DefaultAuthenticator -> Configuration tab -> Common tab. Update the Control Flag to SUFFICIENT.
10. Click Save.



11. From the Providers tab, click the "OIDAuthenticator" (you just created), in the configuration -> Provider Specific tab enter your LDAP connection details:
The values shown below are examples only. You should match the entries to your OID.
 - Host: <oidhost>
 - Port: <oidport>
 - Principal: cn=orcladmin
 - Credential: <password>
 - Confirm Credential: <password>
 - User Base DN: cn=users,dc=us,dc=oracle,dc=com
 - Enable 'Use Retrieved User Name as principal.'

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to APPNAMEDomain

Settings for ODAAuthentication

Configuration Performance

Common Provider Specific

Save

Use this page to define the provider specific configuration for this Oracle Internet Directory Authentication provider.

Connection

Host: idmhost.us.oracle.com The host name or IP address of the LDAP server. [More Info...](#)

Port: 3060 The port number on which the LDAP server is listening. [More Info...](#)

Principal: cn=orcladmin The Distinguished Name (DN) of the LDAP user that WebLogic Server should use to connect to the LDAP server. [More Info...](#)

Credential: The credential (usually a password) used to connect to the LDAP server. [More Info...](#)

Confirm Credential: The credential (usually a password) used to connect to the LDAP server. [More Info...](#)

☐ SSL Enabled Specifies whether the SSL protocol should be used when connecting to the LDAP server. [More Info...](#)

Users

User Base DN: cn=users,dc=us,dc=oracle,dc=com The base distinguished name (DN) of the tree in the LDAP directory that contains users. [More Info...](#)

All Users Filter: (&(cn=*)(objectclass=person)) An LDAP search filter for finding all users beneath the base user distinguished name (DN). Note: If you change the user name attribute to a name other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. [More Info...](#)

User From Name Filter: (&(cn=%s)(objectclass=person)) An LDAP search filter for finding a user given the name of the user. The user name attribute specified in this filter must match the one specified in the All Users Filter and User Name Attribute attributes. [More Info...](#)

User Search Scope: subtree Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for users. [More Info...](#)

User Name Attribute: cn The attribute of an LDAP user object class that specifies the name of the user. The user name attribute specified must match the one specified in the All Users Filter and User From Name Filter attributes. [More Info...](#)

User Object Class: person The LDAP object class that stores users. [More Info...](#)

☒ Use Retrieved User Name as Principal Specifies whether or not the user name retrieved from the LDAP server should be used as the Principal in the Subject. [More Info...](#)

12. Modify the following:

- Group Base DN: cn=Groups,dc=us,dc=oracle,dc=com

Groups

Group Base DN: cn=groups,dc=us,dc=oracle,dc=com The base distinguished name (DN) of the tree in the LDAP directory that contains groups. [More Info...](#)

All Groups Filter: (&(cn=*)(objectclass=group)) An LDAP search filter for finding all groups beneath the base group distinguished name (DN). Note: If you change the user name attribute to a name other than cn, you must duplicate that change in the User From Name Filter and User Name Attribute attributes. [More Info...](#)

Group From Name Filter: (&(cn=%g)(objectclass=group)) An LDAP search filter for finding a group given the name of the group. The user name attribute specified in this filter must match the one specified in the All Groups Filter and User Name Attribute attributes. [More Info...](#)

Group Search Scope: subtree Specifies how deep in the LDAP directory tree the LDAP Authentication provider should search for groups. [More Info...](#)

Group Membership Searching: unlimited Specifies whether or not the LDAP Authentication provider should search for group members. [More Info...](#)

Max Group Membership Search Level: 0 Specifies the maximum search level for group membership. [More Info...](#)

☐ Ignore Duplicate Membership Specifies whether or not duplicate group membership should be ignored. [More Info...](#)

13. Check Propagate Cause For Login Exception

General

Connection Pool Size:

Connect Timeout:

Connection Retry Limit:

Parallel Connect Delay:

Results Time Limit:

☐ **Keep Alive Enabled**

☒ **Follow Referrals**

☐ **Bind Anonymously On Referrals**

☒ **Propagate Cause For Login Exception**

14. Click **Save**.

15. Click the **Providers** tab.

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Home > apphost > Summary of Servers > Summary of Security Realms > myrealm > Providers > OIDAAuthenticator > Providers > DefaultAuthenticator > OIDAAuthenticator > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

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

An Authentication provider allows WebLogic Server to establish trust by validating a user. You must have one Authentication provider in a security realm, and you can configure it LDAP servers or DBMS.

Customize this table

Authentication Providers

New Delete Reorder

Name	Description
Trust Service Identity Asserter	Trust Service Identity Assertion Provider
DefaultAuthenticator	WebLogic Authentication Provider
DefaultIdentityAsserter	WebLogic Identity Assertion provider
OIDAuthenticator	Provider that performs LDAP authentication using Oracle Internet Directory

New Delete Reorder

Change Center

View changes and restarts

Pending changes exist. They must be activated to take effect.

Activate Changes

Undo All Changes

Domain Structure

APPNAME\Domain

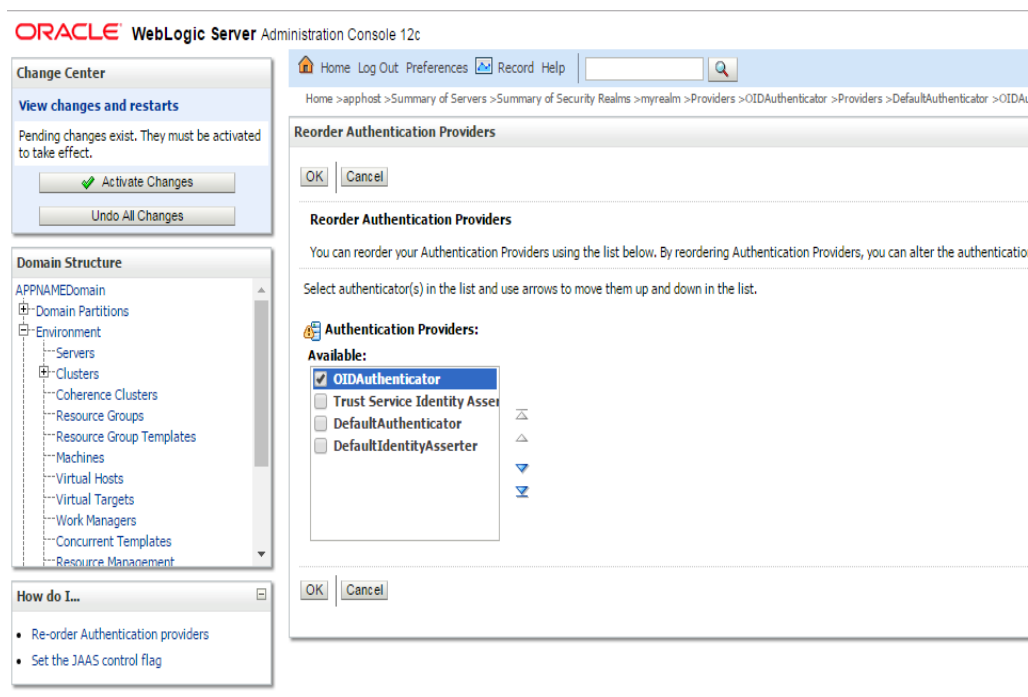
- Domain Partitions
- Environment
 - Servers
 - Clusters
 - Coherence Clusters
 - Resource Groups
 - Resource Group Templates
 - Machines
 - Virtual Hosts
 - Virtual Targets
 - Work Managers
 - Concurrent Templates
 - Resource Management

How do I...

- Configure Authentication and Identity Assertion providers
- Configure the Password Validation provider
- Manage security providers
- Set the JAAS control flag
- Re-order Authentication providers

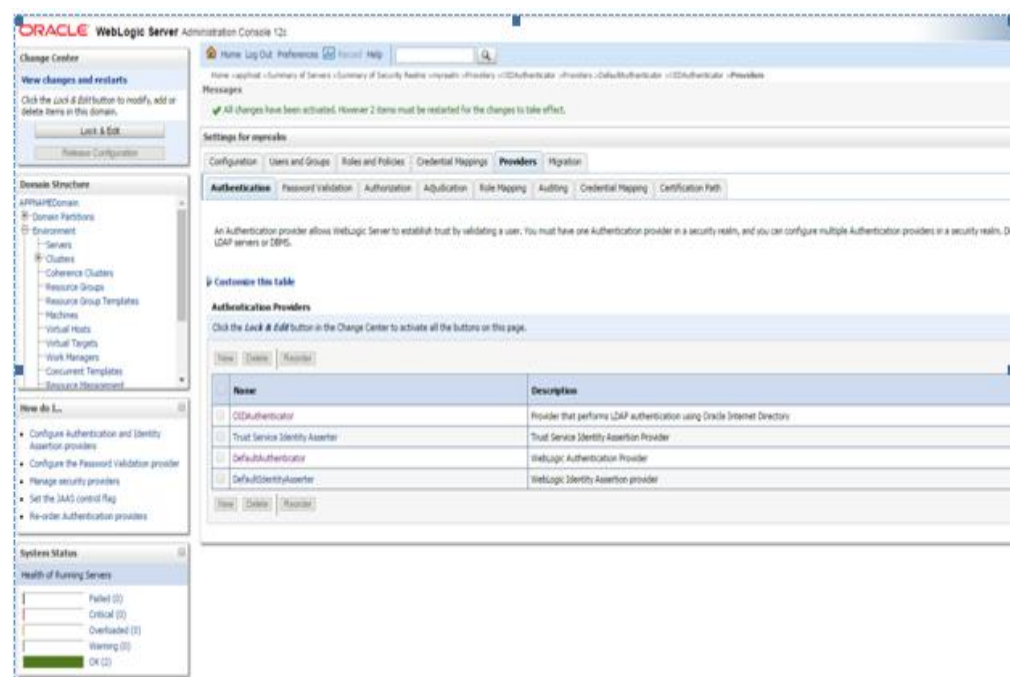
16. Click **Reorder**.

17. Move **OIDAuthenticator** to the top of the providers list.



18. Click **OK**.

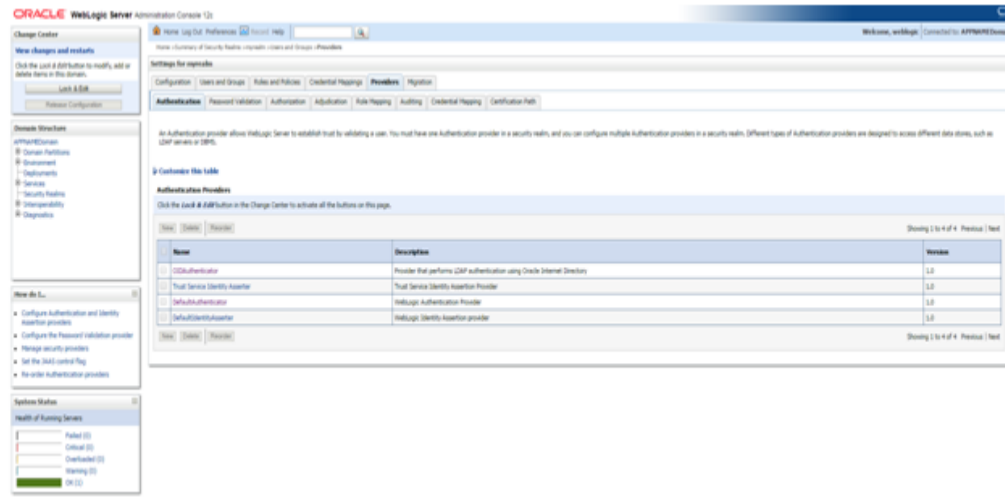
19. Once your changes are saved, click **Activate Changes**.



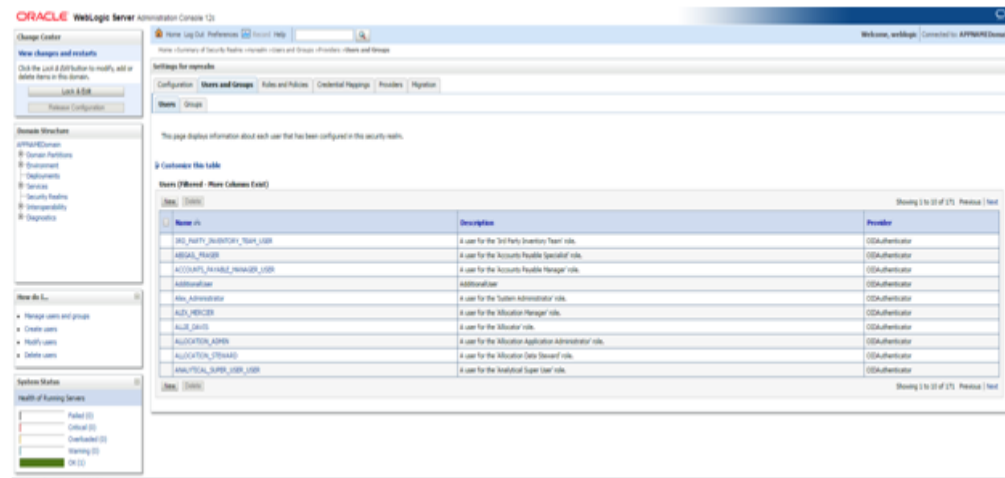
20. Shutdown all servers and restart the admin server using startWebLogic.sh script. Login to Admin Console and restart Managed server.

Verify OID Authenticator

1. Log in to the Administration Console.
http://<HOST_NAME>:<ADMIN_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. You must see the OID Provider in that list.



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



Configure Oracle Single Sign-On

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

Create the SSO provider in the REIMDomain

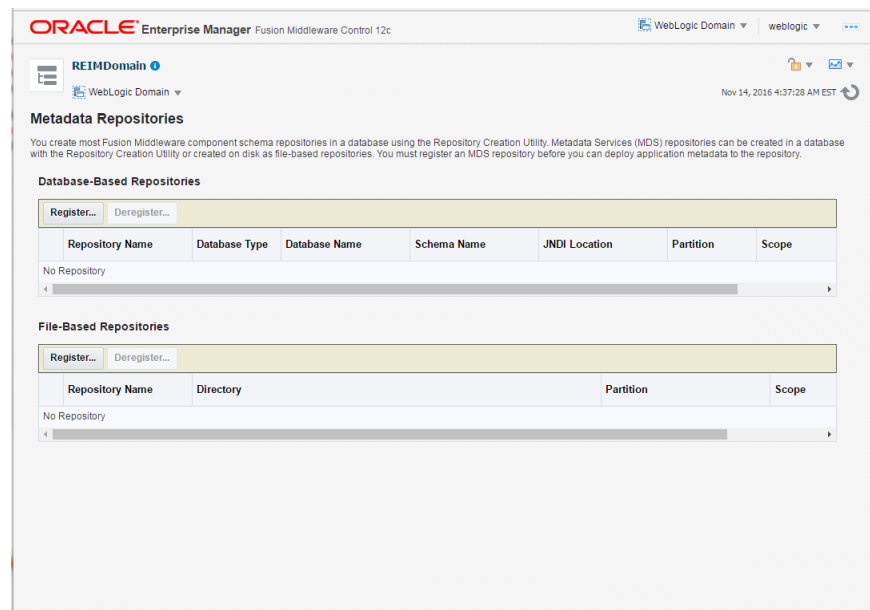
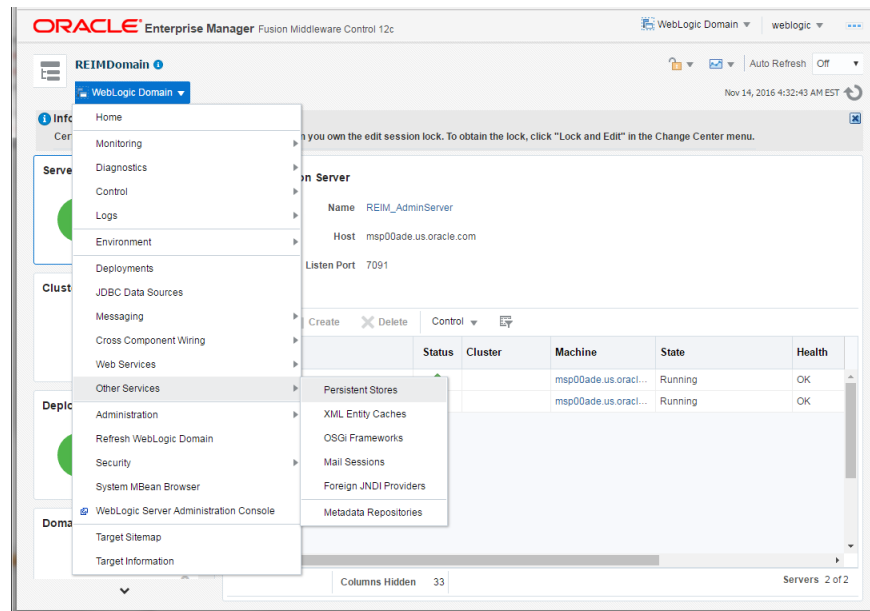
1. Log into the WebLogic console
2. Navigate to: security realms -> myrealm (default realm) -> providers.
3. Start a Lock & Edit session.
4. Click **New provider**.
5. Set the provider name (Default: [OAMIdentityAsserter](#)).
6. Click **Ok**.
7. Open the new provider configuration.
8. Under Common, set the Control Flag to SUFFICIENT.
9. On the provider list, click **Reorder**.
10. Move the [OAMIdentityAsserter](#) to the top of the list, or above the DefaultAuthenticator.
11. Click **Ok**.
12. Click **Activate Changes**.
13. Shutdown the domain.
14. Start the admin and managed servers for the domain.

Create mds-CustomPortalDS Datasource using EM

Follow the below steps to create mds-CustomPortal datasource.

Name	Status	Cluster	Machine	State	Health
reim-server	↑		msp00ade.us.orac...	Running	OK
REIM_AdminServer(admin)	↑		msp00ade.us.orac...	Running	OK

1. Go to WebLogic Domain, Other Services and then MetaData Repositories



2. Under Database-Based Repositories, click the **Register** button.

Register Database-Based Metadata Repository

A repository stores information used by Application Server components and other applications. A metadata repository must be registered to be operational. A database-based repository is created using the Repository Creation Utility. To register, input database connection information and click Query, then select one of the Metadata Repository and click OK button.

Database Connection Information

Database Type: ☒ Oracle ☐ SQL Server ☐ IBM DB2 ☐ MySQL

* Host Name:

* Port:

* Service Name:

* User Name:

* Password:

Role:

Metadata Repository	Is Registered?	Schema Name	Version	Status	Modified Time
No Repository					

Selected Repository

The selected schema can be registered only if it has not already been registered.

Repository Name:

Schema Password:

- Remove weblogic user if it appears in the Username field. Provide the MDS Schema user created in RCU as part of RCU schemas creation.

Example: REIM_MDS

Input the details of Database Hostname, Port number and Service name. Click **Query** and a list of all the schemas will be displayed.

Register Database-Based Metadata Repository

A repository stores information used by Application Server components and other applications. A metadata repository must be registered to be operational. A database-based repository is created using the Repository Creation Utility. To register, input database connection information and click Query, then select one of the Metadata Repository and click OK button.

Database Connection Information

Database Type: ☒ Oracle ☐ SQL Server ☐ IBM DB2 ☐ MySQL

* Host Name:

* Port:

* Service Name:

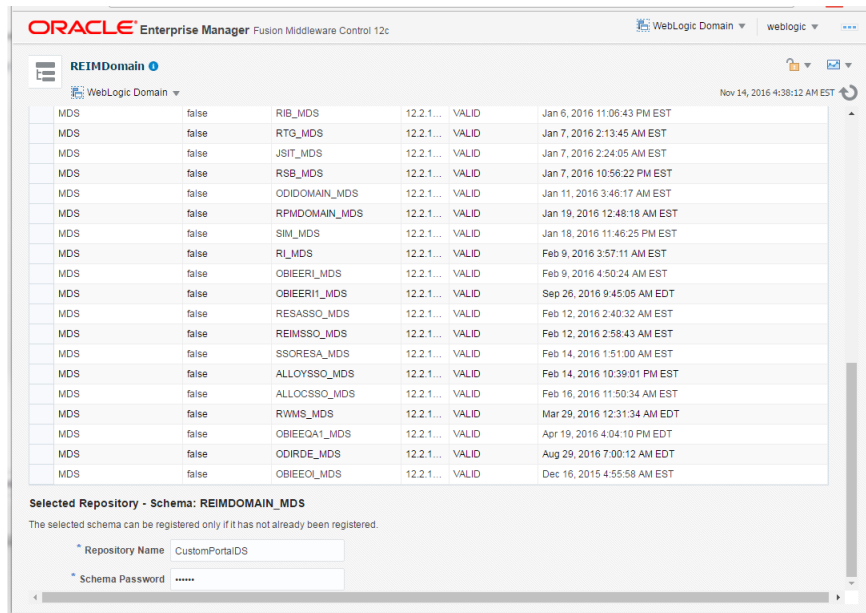
* User Name:

* Password:

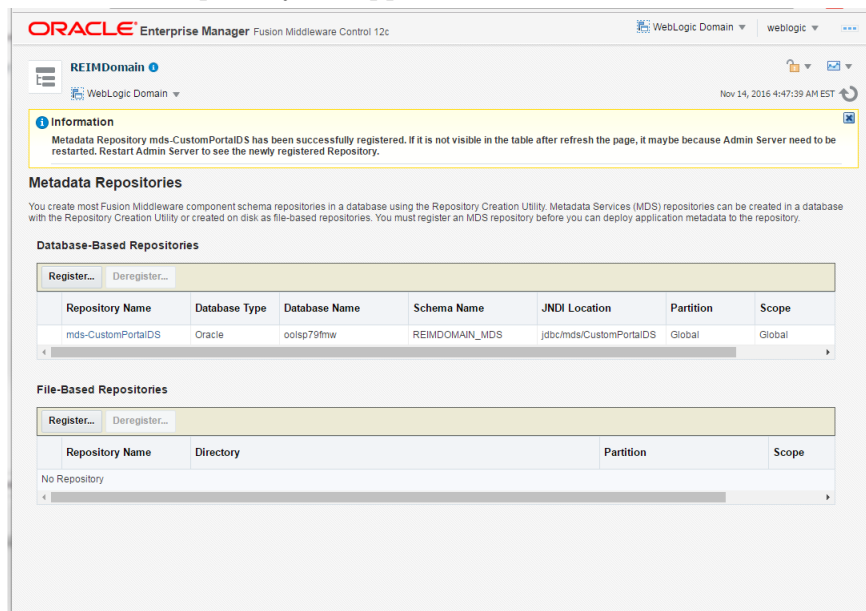
Role:

Metadata Repository	Is Registered?	Schema Name	Version	Status	Modified Time
MDS	false	RAF_MDS	12.2.1...	VALID	Dec 11, 2015 12:50:56 PM EST
MDS	false	RI2_MDS	12.2.1...	VALID	Oct 18, 2016 5:58:40 AM EDT
MDS	false	ALLOYDOMAIN_MDS	12.2.1...	VALID	Dec 31, 2015 1:45:02 AM EST
MDS	false	REIMDOMAIN_MDS	12.2.1...	VALID	Jan 4, 2016 10:19:36 PM EST
MDS	false	RESADOMAIN_MDS	12.2.1...	VALID	Jan 4, 2016 10:32:33 PM EST
MDS	false	FORMS_MDS	12.2.1...	VALID	Jan 5, 2016 3:29:34 AM EST
MDS	false	ALLOY1213_MDS	12.1.3...	VALID	Jan 5, 2016 8:24:09 AM EST
MDS	false	ALLOCDOMAIN_MDS	12.2.1...	VALID	Jan 6, 2016 3:00:20 AM EST
MDS	false	ALLOYQA2_MDS	12.2.1...	VALID	Jan 6, 2016 12:17:05 PM EST
MDS	false	RPMQA2_MDS	12.2.1...	VALID	Jan 6, 2016 12:20:32 PM EST
MDS	false	RIB_MDS	12.2.1...	VALID	Jan 6, 2016 11:06:43 PM EST
MDS	false	RTG_MDS	12.2.1...	VALID	Jan 7, 2016 2:13:45 AM EST
MDS	false	JSIT_MDS	12.2.1...	VALID	Jan 7, 2016 2:24:05 AM EST
MDS	false	RSB_MDS	12.2.1...	VALID	Jan 7, 2016 10:56:22 PM EST
MDS	false	ODIDOMAIN_MDS	12.2.1...	VALID	Jan 11, 2016 3:46:17 AM EST

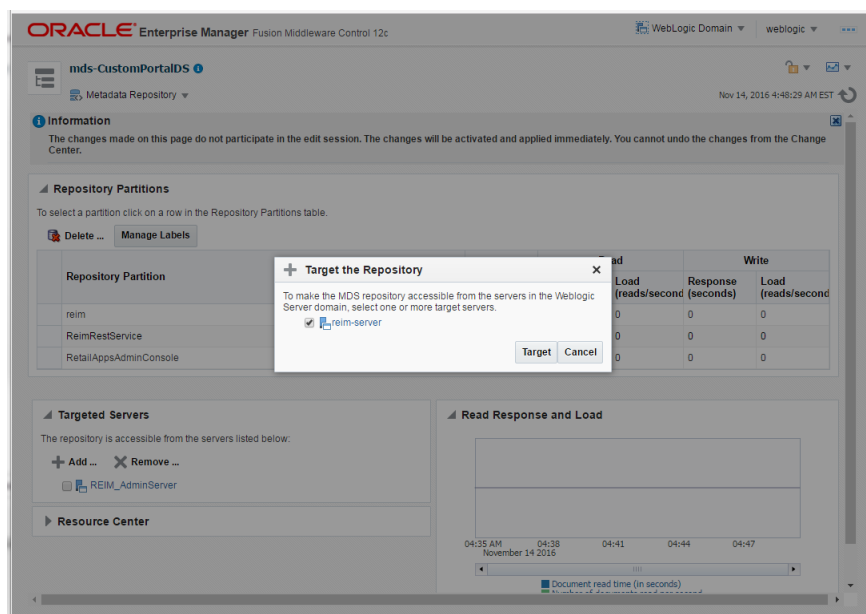
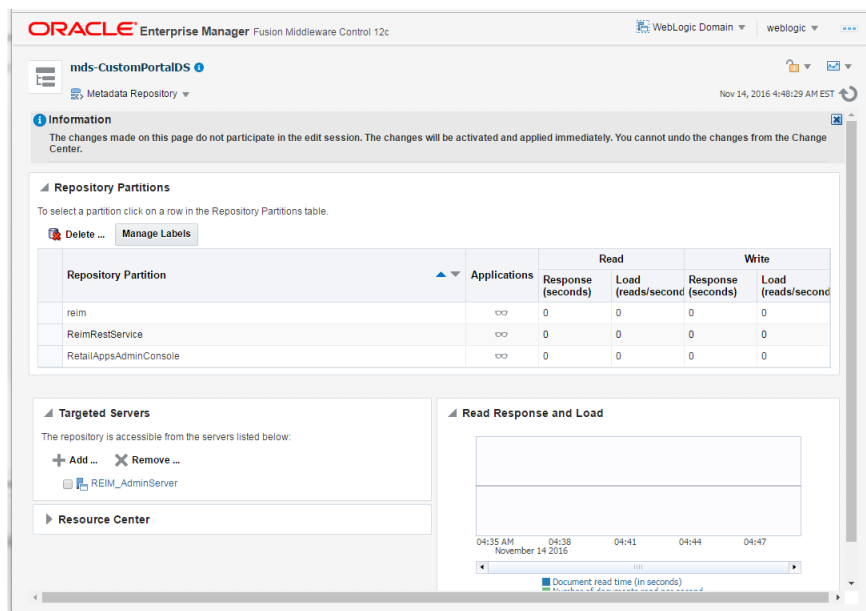
- Select the <REIM_MDS> schema and enter the repository name 'CustomPortalDS' and password and click the **OK** button.



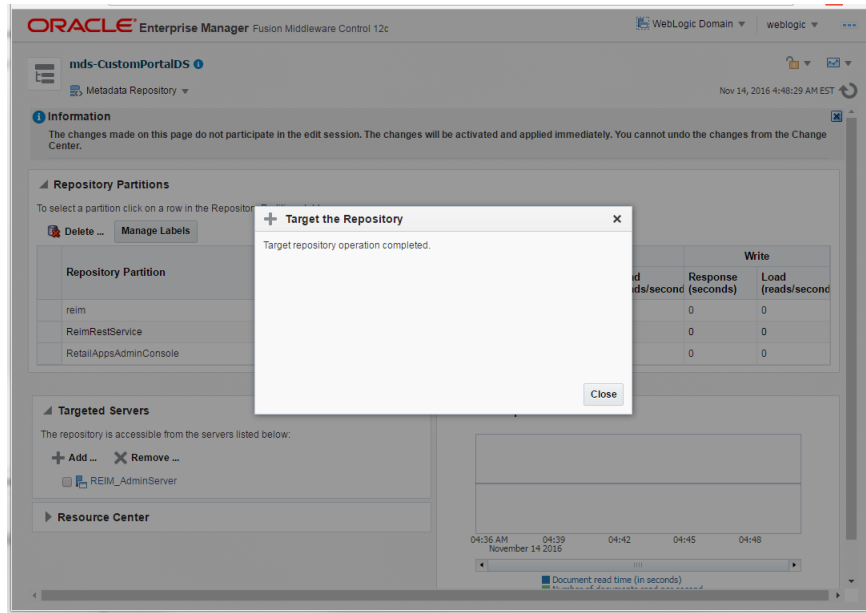
5. The MDS Repository will appear. Click on mds-CustomPortalDS.



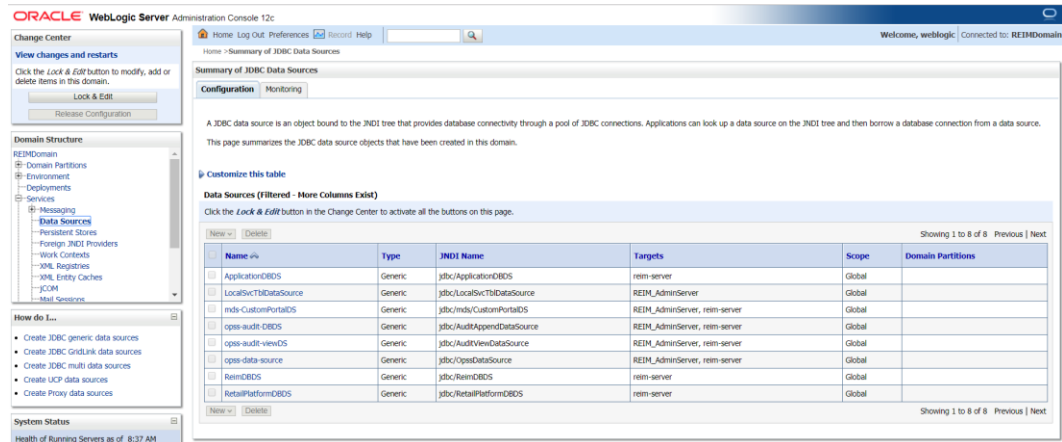
6. Under Targeted Servers, Click add and add the managed server 'reim-server'. Click Target.



7. A message 'Target repository operation completed' is displayed. Click **Close**.



8. Restart the Admin server and the Managed server. Login to the Admin console URL and verify mds-CustomPortalDS datasource exists.



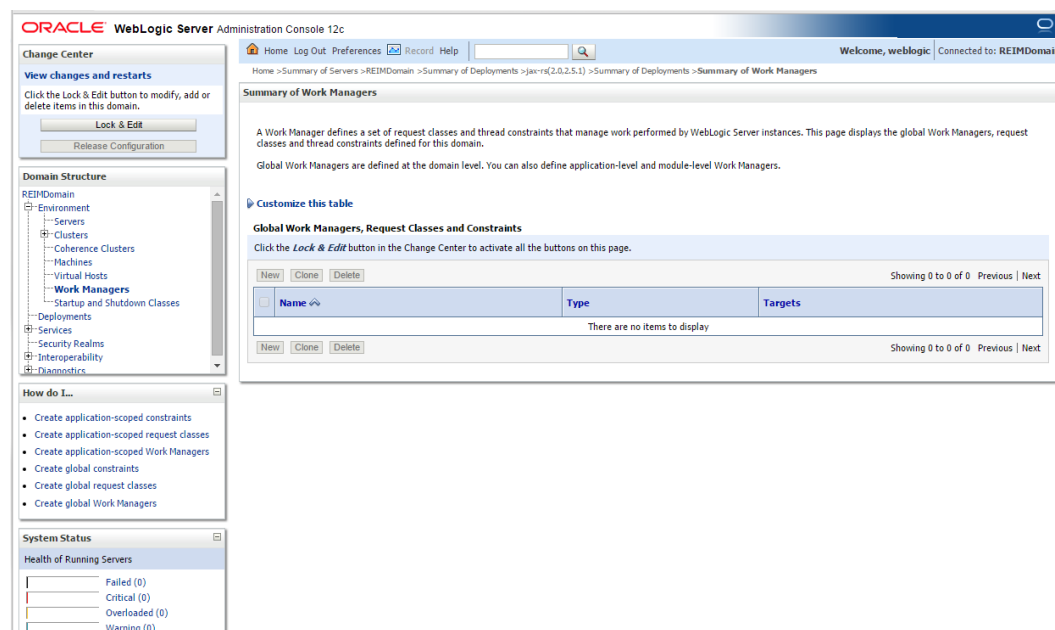
Steps to Configure WebLogic Work Manager

For the Invoice Matching Batch programs to use independent work managers for the thread processing, we need to create a work manager for each batch program. The names of the work managers need to be exactly the same as the ones mentioned in the table below. In case a named work manager is not created, the default work manager will be used by the server.

Batch Name	Work Manager
Automatch	AutoMatchWM
Edi Injector	EdiInjectorWM
Credit note automatch	CNAutoMatchWM
Complex deal upload	CDUploadWM
Fixed deal upload	FDUploadWM
Financial Posting	PostingWM

Steps to Create a Named Work Manager

1. From WebLogic Console navigate to Work Manager pane (Domain->Environment->Work Manager)



2. Click Lock & Edit.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Change Center' with a 'Lock & Edit' button, the 'Domain Structure' tree with 'Work Managers' selected, the 'How do I...' section, and the 'System Status' section. The main content area is titled 'Summary of Work Managers' and contains a table for 'Global Work Managers, Request Classes and Constraints'. The table is currently empty, displaying 'Showing 0 to 0 of 0' items.

Oracle WebLogic Server Administration Console 12c

Home | Summary of Servers | REIMDomain | Summary of Deployments | jaxrs(2.0.2.5.1) | Summary of Deployments | Summary of Work Managers

Welcome, weblogic | Connected to: REIMDomain

Change Center
View changes and restarts
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.
[Lock & Edit] [Release Configuration]

Domain Structure
REIMDomain
├── Environment
│ ├── Servers
│ ├── Clusters
│ │ ├── Coherence Clusters
│ │ ├── Virtual Hosts
│ │ └── **Work Managers**
│ ├── Startup and Shutdown Classes
├── Deployments
├── Services
│ ├── Security Realms
│ ├── Interoperability
└── Diagnostics

How do I...
• Create application-scoped constraints
• Create application-scoped request classes
• Create application-scoped Work Managers
• Create global constraints
• Create global request classes
• Create global Work Managers

System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)

Summary of Work Managers
A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the global Work Managers, request classes and thread constraints defined for this domain.
Global Work Managers are defined at the domain level. You can also define application-level and module-level Work Managers.

Customize this table

Global Work Managers, Request Classes and Constraints

Name	Type	Targets
There are no items to display		

Showing 0 to 0 of 0 Previous | Next

3. Click New. This will take us to the screen which allows us to create work managers and other related classes like constraints. Click Next.

The screenshot shows the 'Create a New Work Manager Component' page in the Oracle WebLogic Server Administration Console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Create a New Work Manager Component' and contains a 'Select Work Manager Definition type' section. The 'Work Manager' radio button is selected.

Oracle WebLogic Server Administration Console 12c

Home | Summary of Servers | REIMDomain | Summary of Deployments | jaxrs(2.0.2.5.1) | Summary of Deployments | Summary of Work Managers

Welcome, weblogic | Connected to: REIMDomain

Change Center
View changes and restarts
No pending changes exist. Click the Release Configuration button to allow others to edit the domain.
[Lock & Edit] [Release Configuration]

Domain Structure
REIMDomain
├── Environment
│ ├── Servers
│ ├── Clusters
│ │ ├── Coherence Clusters
│ │ ├── Virtual Hosts
│ │ └── **Work Managers**
├── Deployments
├── Services
│ ├── Security Realms
│ ├── Interoperability
└── Diagnostics

How do I...
• Create application-scoped constraints
• Create application-scoped request classes
• Create application-scoped Work Managers
• Create global constraints
• Create global request classes
• Create global Work Managers

System Status
Health of Running Servers
Failed (0)
Critical (0)
Overloaded (0)

Create a New Work Manager Component
[Back] [Next] [Finish] [Cancel]

Select Work Manager Definition type
What type of Work Manager, Request Class or Constraint do you want to create?

☒ **Work Manager**
☐ Response Time Request Class
☐ Fair Share Request Class
☐ Context Request Class
☐ Maximum Threads Constraint
☐ Minimum Threads Constraint
☐ Capacity Constraint

[Back] [Next] [Finish] [Cancel]

4. Provide the name of the work manager as mentioned in the table above. Example: AutoMatchWM

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: REIMDomain

Home > Summary of Servers > REIMDomain > Summary of Deployments > jax-rs(2.0.2.5.1) > Summary of Deployments > Summary of Work Managers

Create a New Work Manager Component

Back Next Finish Cancel

Work Manager Properties

The following properties will be used to identify your new Work Manager.

* Indicates required fields

What would you like to name your new Work Manager?

* Name:

Back Next Finish Cancel

5. Target it to both Admin Server and the managed server (<Example>: REIM_AdminServer and reim-server).

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: REIMDomain

Home > Summary of Servers > REIMDomain > Summary of Deployments > jax-rs(2.0.2.5.1) > Summary of Deployments > Summary of Work Managers

Create a New Work Manager Component

Back Next Finish Cancel

Select deployment targets

You can target the Work Manager to any of these WebLogic Server instances or Clusters. Select the same targets on which you will deploy applications that reference the Work Manager.

Available targets :

Servers
<input checked="" type="checkbox"/> reim-server
<input checked="" type="checkbox"/> REIM_AdminServer

Back Next Finish Cancel

6. Click Finish.

ORACLE WebLogic Server Administration Console 12c

Home Log Out Preferences Record Help

Welcome, weblogic Connected to: REIMDomain

Home > Summary of Servers > REIMDomain > Summary of Deployments > jax-rs(2.0.2.5.1) > Summary of Deployments > Summary of Work Managers

Messages

Work Manager created successfully

Summary of Work Managers

A Work Manager defines a set of request classes and thread constraints that manage work performed by WebLogic Server instances. This page displays the global Work Managers, request classes and thread constraints defined for this domain.

Global Work Managers are defined at the domain level. You can also define application-level and module-level Work Managers.

Customize this table

Global Work Managers, Request Classes and Constraints

Name	Type	Targets
AutoMatchWM	Work Manager	reim-server, REIM_AdminServer

New Clone Delete

Showing 1 to 1 of 1 Previous Next

7. Click Activate Changes.

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the following sections:

- Change Center**: View changes and restarts. Click the Lock & Edit button to modify, add or delete items in this domain. Buttons: Lock & Edit, Release Configuration.
- Domain Structure**: A tree view showing the hierarchy: REIMDomain > Environment > Servers > Clusters > Coherence Clusters > Machines > Virtual Hosts > **Work Managers** (selected) > Startup and Shutdown Classes.
- How do I...**: A list of links for creating various components.
- System Status**: Health of Running Servers. A bar chart showing status counts: Failed (0), Critical (0), Overloaded (0), Warning (0).

The main content area shows the **Summary of Work Managers** page. It includes a message: "All changes have been activated. No restarts are necessary." Below this is a table titled "Global Work Managers, Request Classes and Constraints". The table has columns: Name, Type, and Targets. It contains one row: "AutoMatchWMM", "Work Manager", and "reim-server, REIM_AdminServer".

You can see the named work managers created in the list.

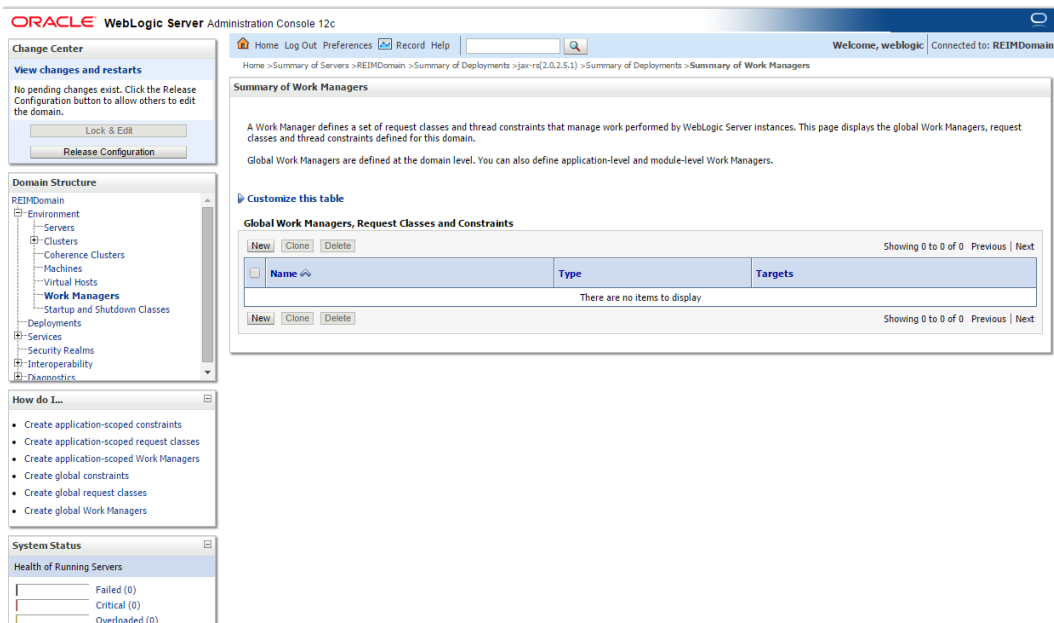
Steps to Create Maximum thread constraints

Maximum thread constraints can be assigned to work managers. Steps to create constraints and to assign them to work managers are as below:

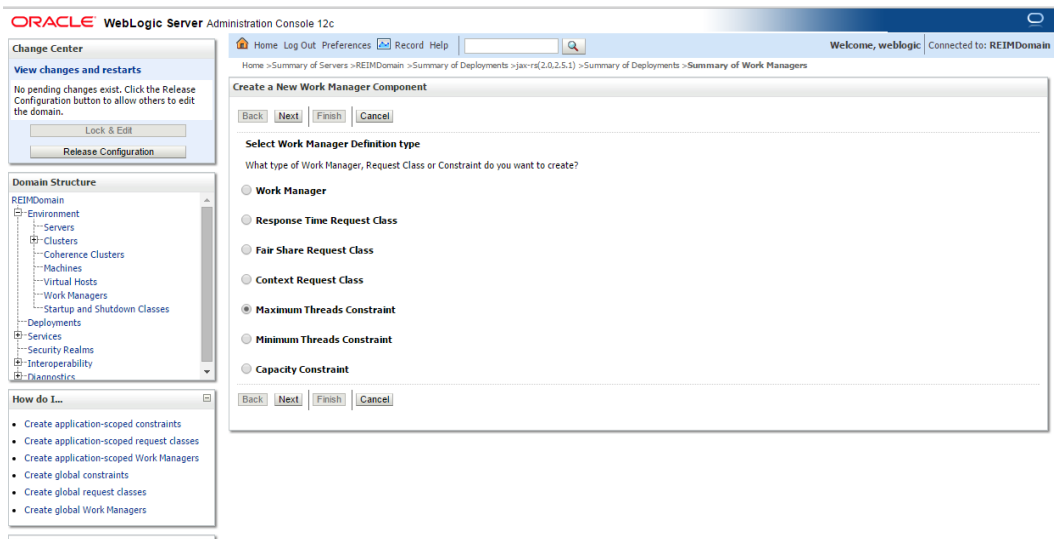
1. From WebLogic Console navigate to Work Manager pane (Domain->Environment->Work Manager)

This screenshot is similar to the previous one, showing the Oracle WebLogic Server Administration Console. The left sidebar is identical. The main content area shows the **Summary of Work Managers** page. The message "All changes have been activated. No restarts are necessary." is present. However, the table titled "Global Work Managers, Request Classes and Constraints" is empty, displaying "There are no items to display".

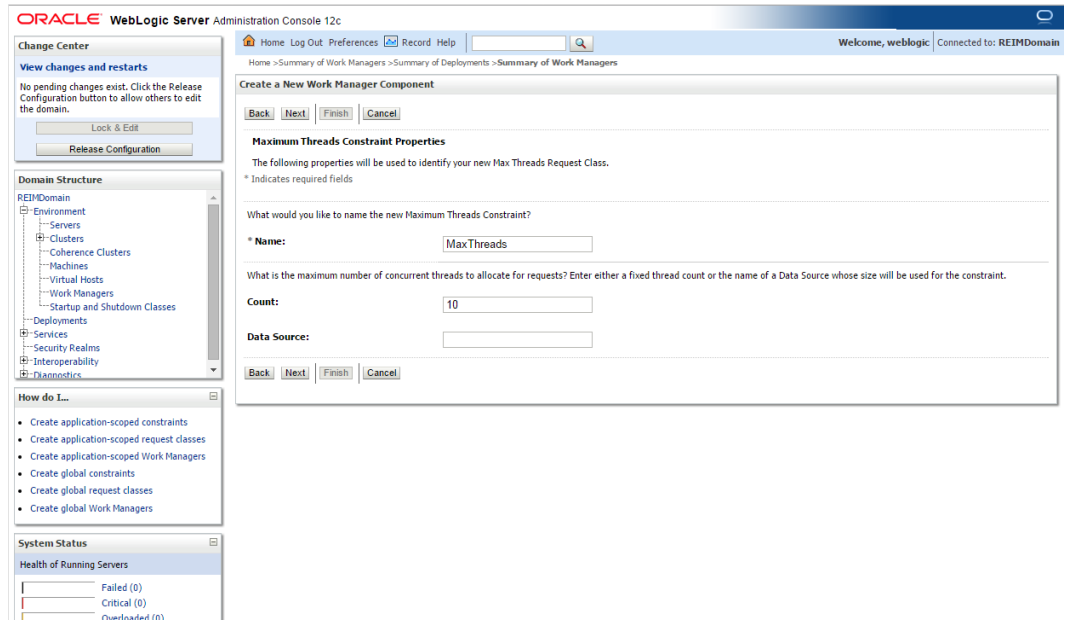
2. Click Lock & Edit.



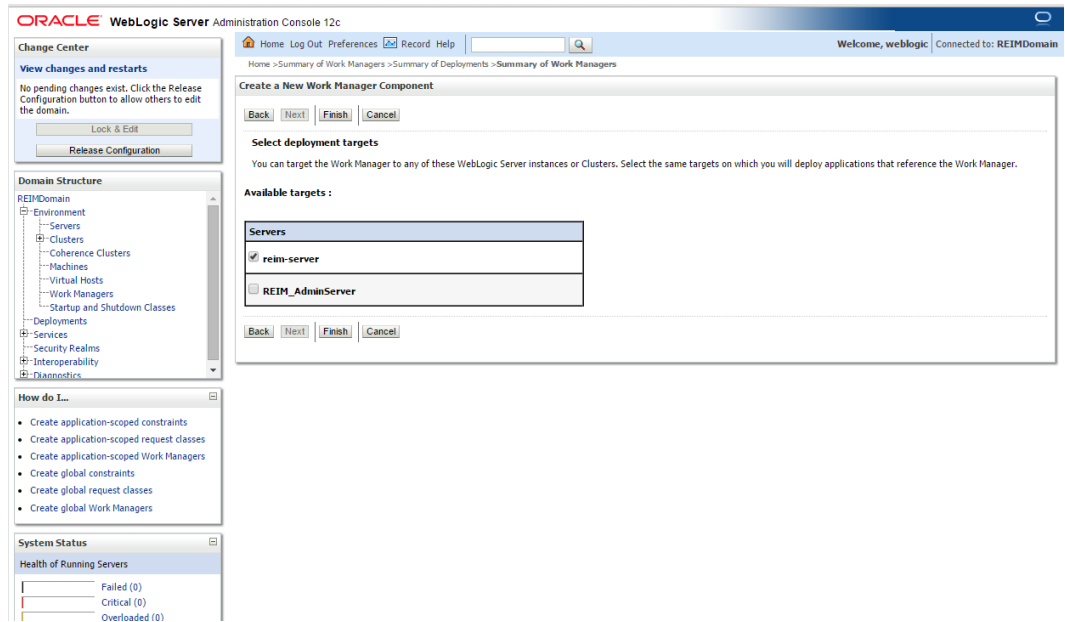
3. Click New. This will take us to the screen which allows us to create constraints.



4. Select the Maximum Thread Constraint radio button and click **Next**.
5. Give a Name (MaxThreads) and specify maximum number of consumers needed for your Application. Click **Next**.



6. Select Target as <reim-server> and click **Finish**.



7. Click **Activate Changes**.

The screenshot shows the Oracle WebLogic Server Administration Console. In the left-hand 'Change Center' panel, the 'View changes and restarts' section displays a message: 'Pending changes exist. They must be activated to take effect.' Below this message are two buttons: 'Activate Changes' (highlighted with a green checkmark icon) and 'Undo All Changes'. The 'Domain Structure' tree on the left shows the hierarchy: REIMDomain > Environment > Servers > Clusters > Coherence Clusters > Machines > Virtual Hosts > **Work Managers** (selected). The 'How do I...' section lists various tasks, including 'Create global Work Managers'. The main content area shows a 'Summary of Work Managers' page with a table of global work managers and constraints.

Global Work Managers, Request Classes and Constraints

Name	Type	Targets
AutoMatchWM	Work Manager	reim-server, REIM_AdminServer
MaxThreads	Maximum Threads Constraint	reim-server

8. Summary of the work managers will be displayed.

The screenshot shows the Oracle WebLogic Server Administration Console after the changes have been activated. In the 'Change Center' panel, the 'View changes and restarts' section now shows a message: 'All changes have been activated. No restarts are necessary.' The 'Lock & Edit' button is now visible. The 'Domain Structure' tree remains the same. The main content area shows the 'Summary of Work Managers' page, which now includes a note: 'Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.' The table of global work managers and constraints is displayed below.

Global Work Managers, Request Classes and Constraints

Name	Type	Targets
AutoMatchWM	Work Manager	reim-server, REIM_AdminServer
MaxThreads	Maximum Threads Constraint	reim-server

The 'System Status' panel at the bottom shows the 'Health of Running Servers' with indicators for Failed (0), Critical (0), and Overloaded (0) servers.

9. Click the work manager link from the Summary of work managers. Example: AutoBatchWM

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Change Center' with a 'Lock & Edit' button, a 'Domain Structure' tree showing the hierarchy from REIMDomain down to Work Managers, and a 'System Status' section. The main content area is titled 'Settings for AutoMatchWM' and includes tabs for 'Configuration', 'Targets', and 'Notes'. A 'Save' button is at the top. Below, a table lists various settings for the work manager, including Name, Request Class, Minimum Threads Constraint, Maximum Threads Constraint, Capacity Constraint, Stuck Thread Action, Max Stuck Thread Time, Stuck Thread Count, and a checkbox for 'Resume When Unstuck'. Each setting has a dropdown menu or input field and a 'More Info...' link.

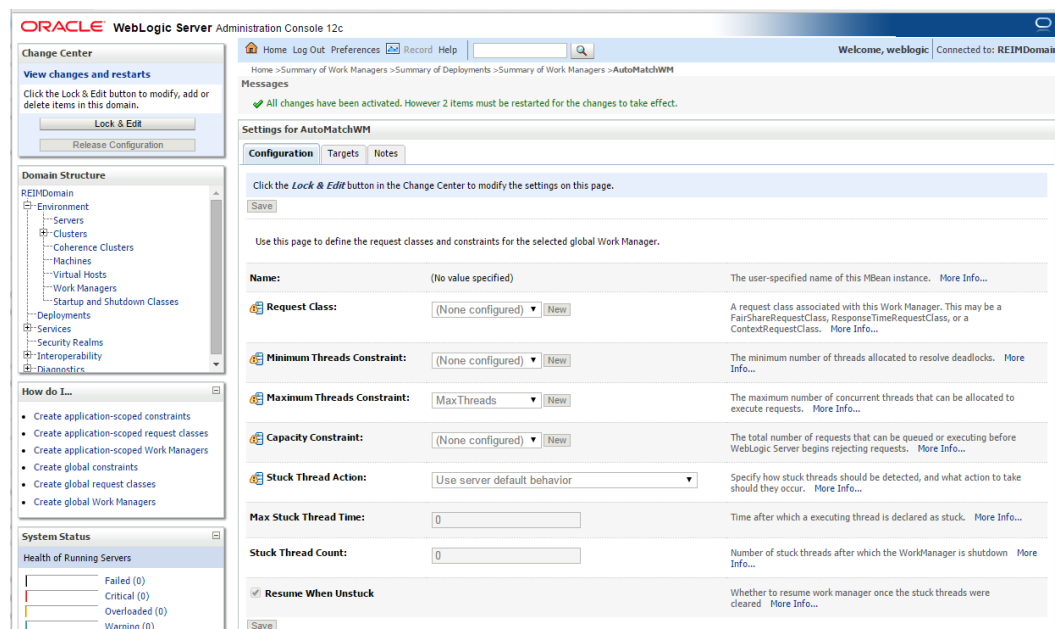
10. Click Lock & Edit.

11. From the Maximum Thread Constraint dropdown, select the constraint you have created earlier.

This screenshot is similar to the previous one, but the 'Maximum Threads Constraint' dropdown menu is now set to 'MaxThreads' instead of '(None configured)'. The 'Save' button is visible at the bottom of the settings table.

12. Click **Save**.

13. Click **Activate Changes**.



14. Restart Weblogic Adminserver and Managed server.

Load LDIF Files in LDAP

The OID (Oracle Internet Directory 11.1.1.9) must be set up in order to perform the configuration of OID Authenticator in WebLogic Domain.

There are four sample LDIF files provided in the application zip (INSTALL_DIR/reim/application/reim/ldif):

RGBU-oid-create-groups.ldif

RGBU-oid-create-users.ldif

RGBU-oid-delete-groups.ldif

RGBU-oid-delete-users.ldif

Note: You may use the existing users and existing groups if the enterprise users map to the appropriate groups for 15.0. For more information, refer to the Retail Role Hierarchy section in the Implementing Functional Security of the *Oracle Retail Invoice Matching 15.0 Operation Guide*.

IMPORTANT Note: If you are using the above LDIF files to set up the users and groups, you must update the 'RGBU-oid-create-user.ldif' LDIF file with your password for the 'userpassword' attribute for all the users mentioned in the RGBU-oid-create-user.ldif LDIF file. The changes must be done before importing the users LDIF file 'RGBU-oid-create-users.ldif' into the LDAP. Once the users are imported into the LDAP, remove the 'userpassword' attribute value from the LDIF file. Refer to the *Oracle Internet Directory Administration Guide* for OID password policies for setting up passwords.

User DN and Group DN values (example:dc=us,dc=oracle,dc=com) may need to be updated based on the DN values in your OID.

Once the LDIF files are updated for your configuration, the LDIF files can be loaded into LDAP using the ldapadd tool that is included in the OID installation. LDIF files can also be imported in other ways like ODSM.

For example to load RGBU-oid-create-users.ldif using ldapadd (this is done on the OID host)

```
export ORACLE_HOME=/u00/webadmin/products/wls_idm/ORACLE_IDM (this is the ORACLE_HOME of your OID install)
```

```
export PATH=$ORACLE_HOME/bin:$PATH
```

```
$ORACLE_HOME/bin/ldapadd -v -c -h <OID_HOST> -p 3060 -w <ORCLADMIN  
PASSWORD> -D "cn=orcladmin" -f RGBU-oid-create-users.ldif
```

The LDIF 'RGBU-oid-delete-groups.ldif' can be used as needed if you need to delete the groups created from the groups creation LDIF 'RGBU-oid-create-groups.ldif'.

The LDIF 'RGBU-oid-delete-users.ldif' can be used if you need to delete the users created from the users LDIF file 'RGBU-oid-create-users.ldif'.

1. Users in the LDIF will be imported and Users can be verified in your User DN location, example: cn=Users,dc=us,dc=oracle,dc=com.

The group cn=Administrators and user cn=weblogic must have been added to your OID as part of OID documentation. If it is not added already, create the cn=weblogic user **and** cn=Administrators group and add cn=weblogic user as a uniquemember in cn=Administrators group. **Following LDIF scripts can be used for the creation of the user (cn=weblogic) and group (cn=Administrators).**

Note: DN value need to be changed based on your DN value in OID.

For Example:

cn=weblogic user LDIF:

```
dn: cn=weblogic,cn=Users,dc=us,dc=oracle,dc=com
description: A user for the 'Administrators' role.
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orcluser
objectclass: orcluserV2
objectclass: orclIDXPperson
cn: weblogic
orclsamaccountname: weblogic
```

```

sn: weblogic
uid: weblogic
givenname: weblogic
displayname: weblogic
userpassword: <your password here>
employeeNumber:
middleName:
orclHireDate:
telephoneNumber:
facsimileTelephoneNumber:
mail: weblogic@rgbu.generated.oracle.com
postalAddress:
street:
postalCode:
title:
employeeType:

```

cn= Administrators group LDIF:

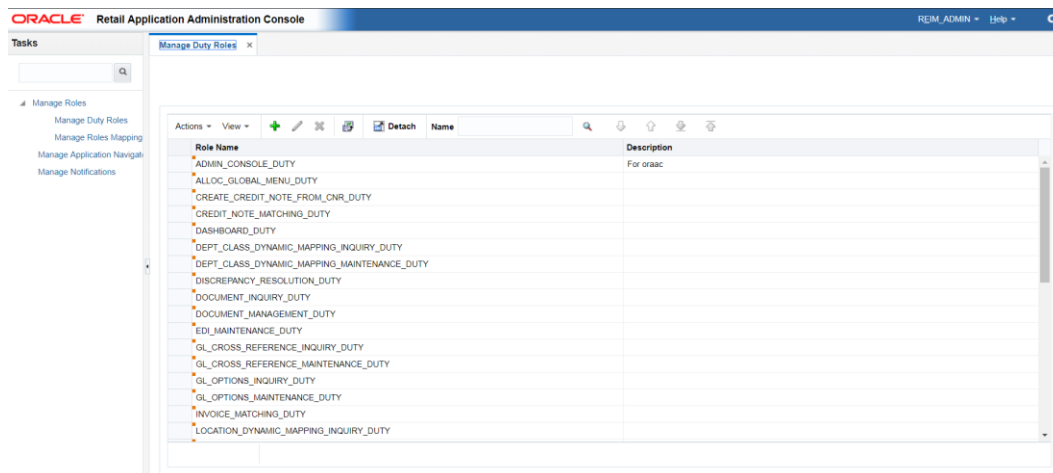
```

dn: cn=Administrators,cn=groups,dc=us,dc=oracle,dc=com
objectclass: groupOfUniqueNames
objectclass: orclGroup
objectclass: top
cn: Administrators
description: Administrators
displayname: Administrators
uniquemember: cn=weblogic,cn=users,dc=us,dc=oracle,dc=com

```

Oracle Retail Application Administration Console

Oracle Retail Application Administration Console (ORAAC) is a tool used by an administrator to manage application roles, manage the application navigator and manage notifications. It facilitates the customization of default RGBU role mappings to suit the retailer's business role model. ORAAC is deployed along with the ReIM application and accessed from the user menu of the ReIM application's user interface.



Only the user with ReIM Application Administrator privilege can access RAAC from the ReIM application.

As part of the Retail Invoice Matching Application install, RAAC gets installed with one default role REIM_APPLICATION_ADMINISTRATOR_JOB role. The same job role will also exist in ReIM's jazn-data.xml file. The below options can be used for the set up.

Option 1:

Create the REIM_APPLICATION_ADMINISTRATOR_JOB role in your LDAP and assign that role to a user who intends to execute the role mapping process.

Option 2:

Create a Job role in your LDAP and map the intended job role in the LDAP to the REIM_APPLICATION_ADMINISTRATOR_JOB role using enterprise manager.

Since the user is part of the REIM_APPLICATION_ADMINISTRATOR_JOB role, the user first access the REIM application app and then launch RASRM for role mapping from the user menu of the REIM application.

Note: The REIM_APPLICATION_ADMINISTRATOR_JOB role must have been already created if using the sample LDIF files which are provided as part of the Retail Invoice Matching Application zip file.

Clustered Installations – Preinstallation Steps

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

1. Make sure that you are able to start and stop the managed servers that are part of the ReIM Cluster from the WebLogic Admin Console.

There are no additional steps before running the installer for Retail Invoice Matching.

(Optional) Analyze Changes in the Patch

Note: See [Appendix: Analyze Tool](#) for details and instructions to run the Analyze Tool. This appendix also contains screens and fields in the tool.

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 (reim15application.zip). There should be a minimum of 300 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 reim15application.zip to INSTALL_DIR and extract its contents.

Example: unzip reim15application.zip

Run the Oracle Retail Invoice Matching Installer

Once you have a managed server that is configured and started, you can run the Oracle Retail Invoice Matching application installer. This installer configures and deploys the Oracle Retail Invoice Matching application.

Note: See [Appendix: Oracle Retail Invoice Matching Application Installer Screens](#) for details about 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`, `JAVA_HOME`, and `WEBLOGIC_DOMAIN_HOME` environment variables. `ORACLE_HOME` should point to your WebLogic installation. `JAVA_HOME` should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where Application is getting installed. `WEBLOGIC_DOMAIN_HOME` should point to the full path of the domain into which ReIM will be installed.
3. If a secured datasource is going to be configured you also need to set “`ANT_OPTS`” so the installer can access the key and trust store that is used for the datasource security:

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

An example of this would be:

```
export ANT_OPTS="-
Djavax.net.ssl.keyStore=/u00/webadmin/product/identity.keystore -
Djavax.net.ssl.keyStoreType=jks -Djavax.net.ssl.keyStorePassword=retail123 -
Djavax.net.ssl.trustStore=/u00/webadmin/product/identity.truststore -
Djavax.net.ssl.trustStoreType=jks -
Djavax.net.ssl.trustStorePassword=retail123"
```

4. If you are using an X server such as Xceed, 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 (`reinstall.<timestamp>.log`). See [Appendix: Oracle Retail Invoice Matching Application Installer Screens](#) for illustrations of installer screens and details about what information needs to be entered on each screen.

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.

Post-Installation Steps

Update the following settings in WebLogic:

Transaction Time Out

The transaction time out is set at the Domain Level in Weblogic console

1. Login to the WebLogic Console.
2. Navigate to REIMDomain/Configuration/JTA/Timeout Seconds.
3. Set Timeout Seconds to 1200000.

Data Source Capacity

Depending on your planned load, you may need to increase the capacity on the ReIM data sources to accommodate more concurrent connections. When increasing this setting, ensure that your ReIM database has processes setting large enough to accommodate the new maximum.

1. Login to the WebLogic Console.
2. Click the Data Sources link on the Home Screen. The Data Source screen is displayed.
3. Under the list of Data Sources, click the ApplicationDBDS data source.
4. Click the Connection Pool tab.
5. Set the Maximum Capacity to 1000.
6. Repeat for all data sources.

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 <retailhome>/batch directory and copy it onto the remote servers under the same path.
2. The Oracle Retail Installation creates some security files on \$WEBLOGIC_DOMAIN_HOME/retail/context root/config directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node.
3. The Oracle Retail Installation creates some properties files on \$WEBLOGIC_DOMAIN_HOME/retail/context root/properties directory. Copy this directory to each remote node of the Cluster, matching the full path of the location of this directory on main node

Installing the REIM OAS Publisher Templates

In this section we will outline how the REIM report templates are installed into the appropriate BI server repositories which will be referred to as BI_REPOSITORY

Example: <DOMAIN_HOME>/config/bipublisher/repository

Report files are available from - "INSTALL_DIR/reim/reports" and have to be copied into the newly created directory within the Reports directory under the BI Publisher Guest folder.

1. Create the directory to hold the reports under <BI_REPOSITORY>
`mkdir <BI_REPOSITORY>/Reports/Guest/REIM`
2. Change directory to the INSTALL_DIR/reports. This directory contains subdirectories whose names reflect the names of report templates provided with REIM.
 - a. Copy each report directory into the directory created above

For example,

```
cp -R * <BI_REPOSITORY>/Reports/Guest/REIM
```

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://AppHostName:(managed_server_port)/ReimViewController/faces/Home`

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

Example:`http://AppHostName:7091/ReimViewController/faces/Home`

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.

integration.properties

The below changes need to be done only if WWAV credentials have been enabled for reim during deployment.

The integration.properties can be found under

<DOMAIN_HOME>/retail/<reim app deployment name>/<6m8whs>/reim.war/WEB-INF/classes/com/rettek/reim/integration.properties

Before changes, the integration.properties would look like the below:

```
#Drill Forward - start
#webservice.financial.drill.forward=https://hostname.us.oracle.com:7068/fin-DrillBackForwardUrl-AppServiceDecorator/ProxyService/DrillBackForwardUrlAppServiceProxy?wsdl
webservice.financial.drill.forward.wsdl=@deploy.webservice.drill.forward.wsdl@

#The below entries are not required as per Dev Team.
#webservice.financial.drill.forward.url.targetnamespace=@deploy.webservice.drill.f
orward.url.targetnamespace@
#webservice.financial.drill.forward.targetsystem=@deploy.webservice.drill.forward.
targetsysteem@
#Drill Forward - end

#webservice provider URL for account validation
webservice.financial.account.validation=https://msp00abq.us.oracle.com:7068/fin-
GlAccountValidation-AppServiceDecorator/ProxyService/GlAccountValidationAppServiceProxy?wsdl
webservice.financial.account.validation.namespace=http://www.oracle.com/retail/fin
/integration/services/GlAccountValidationService/v1
webservice.financial.account.validation.local.code=GlAccountValidationService

#webservice user alias for account validation
webservice.financial.account.validation.credential.alias=${webservice.account.vali
dation.credential.alias.trimmed.upper}

#enable webservice credentials
enable.webservice.account.validation.credentials=@deploy.enable.webservice.account
.validation.credentials@
```

After the changes have been made, integration.properties should look like the below:

```
#webservice provider URL for drill forward
#Drill Forward - start
#webservice.financial.drill.forward=@deploy.webservice.drill.forward@
```

```
webservice.financial.drill.forward.wsdl=http://hostname.us.oracle.com:18008/fin-
DrillBackForwardUrl-
AppServiceDecorator/ProxyService/DrillBackForwardUrlAppServiceProxy?wsdl

#The below entries are not required as per Dev Team.
#webservice.financial.drill.forward.url.targetnamespace=http://www.oracle.com/reta
il/fin/integration/services/DrillBackForwardUrlService/v1
#webservice.financial.drill.forward.targetsystem=@deploy.webservice.drill.forward.
targetsysteem@
#Drill Forward - end

#webservice provider URL for account validation
webservice.financial.account.validation=https://msp00abq.us.oracle.com:7068/fin-
GlAccountValidation-
AppServiceDecorator/ProxyService/GlAccountValidationAppServiceProxy?wsdl
webservice.financial.account.validation.namespace=http://www.oracle.com/retail/fin
/integration/services/GlAccountValidationService/v1
webservice.financial.account.validation.local.code=GlAccountValidationService

#webservice user alias for account validation
webservice.financial.account.validation.credential.alias=${webservice.account.vali
dation.credential.alias.trimmed.upper}

#enable webservice credentials
enable.webservice.account.validation.credentials=@deploy.enable.webservice.account
.validation.credentials@

Bounce the domain once the changes have been made.
```

ReIM Batch Scripts

The ReIM application installer configures and installs the batch scripts under <retailhome>/reim-batch.

Example: /u00/projects/j2ee/reim/rem-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 7.0 (1.7.0) JDK installation that typically is being used by the WebLogic Application Server.

Example: export
ORACLE_HOME=/u00/webadmin/products/wls_retail
export JAVA_HOME=/u00/webadmin/products/jdk_java
export PATH=\$JAVA_HOME/bin:\$PATH

Online Help

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

Single Sign-On

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

Note: This section assumes the Oracle WebLogic Server has already been registered with the Oracle Access Manager (OAM) via the oamreg tool. See the Oracle Single Sign-On (OAM using webgate) 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 <WEBLOGIC_HOST>
    WebLogicPort <WEBLOGIC_PORT>
    Debug ON
    WLogFile /tmp/weblogic.log
    MatchExpression *.jsp
</IfModule>

<Location /ReimViewController >
SecureProxy ON
WebLogicHost <WEBLOGIC_HOST>
WebLogicPort <WEBLOGIC_PORT>
SetHandler weblogic-handler
WLCookieName REIMSESSIONID
WLProxySSL ON
    WLProxySSLPassThrough ON
    WLSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/h
ost_name"
</Location>

<Location /RetailAppsAdminConsole-REIM >
WebLogicHost <WEBLOGIC_HOST>
WebLogicPort <WEBLOGIC_PORT>
SetHandler weblogic-handler
WLCookieName REIMSESSIONID
WLProxySSL ON
WLProxySSLPassThrough ON
SecureProxy ON
WLSLWallet
"${ORACLE_INSTANCE}/config/${COMPONENT_TYPE}/${COMPONENT_NAME}/keystores/h
ost_name"
```

Adding Logout URI

After verifying default authenticator's control flag set correctly as per the OAM documentation, and order of the providers are correct, follow the below steps to configure REIM Application SSO url logout using wlst tool

1. Navigate to <ORACLE_HOME>/oracle_common/common/bin and run wlst.sh
2. Connect REIM domain using admin credentials created during Weblogic domain creation and add OAM SSO Provider.

```
connect ('<WEBLOGIC_ADMIN_USERNAME>',
'<<WEBLOGIC_ADMIN_PASSWORD>', 't3://<APP_HOSTNAME>:<ADMIN_PORT>')
wls:/crmodssso/serverConfig>domainRuntime()
wls:/crmodssso/serverConfig>addOAMSSOProvider(loginuri="/${app.context}/adfAuth
entication",logouturi="/oamssso/logout.html", autologinuri="/obrar.cgi")
```

3. Login to Weblogic Admin Console and click on Lock & Edit
4. Enable “Weblogic Plugin Enabled” under REIM Domain→Web Applications Tab.

The screenshot shows the Oracle WebLogic Server Administration Console interface. The left sidebar contains navigation options like 'Change Center', 'Domain Structure', and 'How do I...'. The main content area is titled 'Settings for REIMDomain' and includes tabs for 'Configuration', 'Monitoring', 'Control', 'Security', 'Web Service Security', 'ZDT Control', and 'Notes'. The 'Configuration' tab is active, and the 'Web Applications' sub-tab is selected. The 'Filter Dispatched Requests' section is expanded, showing a table of settings. The 'Weblogic Plugin Enabled' checkbox is checked, and the 'X-Powered-By Header' is set to 'X-Powered-By HTTP not be sent'.

Setting	Value	Description
Filter Dispatched Requests	Enabled	Indicates whether or not to apply filters to dispatched requests. This is a backward compatibility flag. Until version 8.1, WebLogic Server applied ServletFilters (if configured for the web application) on request dispatches (and includes/forwards). Servlet 2.4 has introduced the "dispatcher" element to make this behavior explicit. The default value is Dispatcher=REQUEST. In order to be compliant with the Java EE specification, the default value for FilterDispatchedRequestsEnabled is false beginning with WebLogic Server 8.0. Note that if you are using old descriptors (meaning web.xml does not have version=2.4), then WebLogic Server automatically sets FilterDispatchedRequestsEnabled = true for the web applications, unless their registered requests-enabled is explicitly set to false in weblogic.xml. This means that old applications will work fine without any modification. Additionally, during migration of old domains to the 8.0 domain, the migration plug-in automatically sets this flag to true. More Info...
Overload Protection Enabled	Enabled	This parameter is used to enable overload protection in the web application container against low memory conditions. When a low memory situation occurs, new session creation attempts will result in weblogic.servlet.SessionCreationException. The application code needs to catch this exception and take proper action. Alternatively, appropriate error pages can be configured in web.xml against weblogic.servlet.SessionCreationException. This check is performed only on memory and registered sessions. More Info...
X-Powered-By Header	X-Powered-By HTTP not be sent	WebLogic Server uses the X-Powered-By HTTP header, as recommended by the Servlet 2.4 specification, to publish its implementation information. More Info...
File Name Mapping Files	./config/mnamemappings.properties	Returns the name of the file containing name-mappings for the domain. More Info...
Optimistic Serialization	Enabled	When OptimisticSerialization is turned on, WebLogic Server does not serialize-deserialize content and instead attributes upon getAttributeNames() when a request gets dispatched from across several contexts. This means you will need to make sure that the attributes concern to web applications are scoped to a consistent parent (ideally they are application-scoped) or passed in the system (throughout if the two web applications do not belong to the same application. When OptimisticSerialization is turned off (which is the default), WebLogic Server does session-deserialize content and request attributes upon getAttributeNames() to avoid the possibility of ClassCastException. The value of OptimisticSerialization can also be overridden for specific web applications by setting the optimistic-serialization value in weblogic.xml. More Info...
Error on Name request time value	Enabled	Global property which determines the behavior of the JSP compiler when the global attribute "name" has a request time value. Without this property set to "true", the JSP compiler throws an error for a JSP using a request time value for the "name" attribute as mandated by the JSP 2.0 specification. This property exists for backward compatibility. More Info...
Client Cert Proxy Enabled	Enabled	Specifies whether or not to honor the WL Proxy Client-Cert header coming with the request. More Info...
HTTP Trace Support Enabled	Enabled	Returns the value of HTTPTraceSupportEnabled. More Info...
Weblogic Plugin Enabled	Enabled	Specifies whether or not the programmatic Proxy Client ID header should be honored. (This is needed only when WebLogic Server plug-in are configured.) More Info...

5. Save it and click on Activate Changes
6. Restart REIM Domain servers and verify Application url is logging out properly by displaying OAM page.

Welcome

Enter your Single Sign-On credentials below

Username:

Password:

[Forgot Password](#)

[Register New Account](#)

[Track User Registration](#)

Configure the OAS5.5 Environment for Operational Insights

This section provides the details on how to configure Operational Insights Installation. This is an optional section as you can choose not to use Operational Insights. Single Sign-On configuration for ReIM, Allocation, ReSA and OAS 5.5 is optional for configuring Operational Insights.

Terms

The following terms apply to the Operational Insights installation and configuration:

OAS_PORT - The port where the OAS5.5 administration server is running.

OAS_MS_PORT - The OAS5.5 Managed server port.

OAS_ORACLE_HOME - The OAS5.5 installation path

OAS_DOMAIN_HOME - The OAS5.5 WebLogic domain path.

RMS_HOST - The host where RMS is installed in WebLogic.

Install OAS 5.5

OAS Server Component Installation Tasks

Oracle OAS Publisher is used as the main RMS, RWMS, REIM, and SIM reporting engine and can be used in conjunction with external printing solutions like label printing. This section describes the installation of Oracle OAS Publisher as a server application within WebLogic 12.2.1.4.0. One deployment of OAS Publisher can be used for any of the RMS, RWMS, REIM, and SIM reports.

When installing OAS Publisher, refer to the appropriate Fusion Middleware guides for the installation of the product in a WebLogic server environment.

Installation Process Overview

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

1. Install Oracle Analytics Server under an existing WebLogic Server (WLS) 12.2.1.4 infrastructure home.
2. Configure Oracle Analytics Server components "OAS Publisher" only for hosting reports. Select both "OAS Enterprise Edition and OAS Publisher" for configuring Operational Insights (OI).
3. Select the OAS Platform schema for update of the ORACLE 19c DB.
4. Configure ports and document and test the URL's that are created.

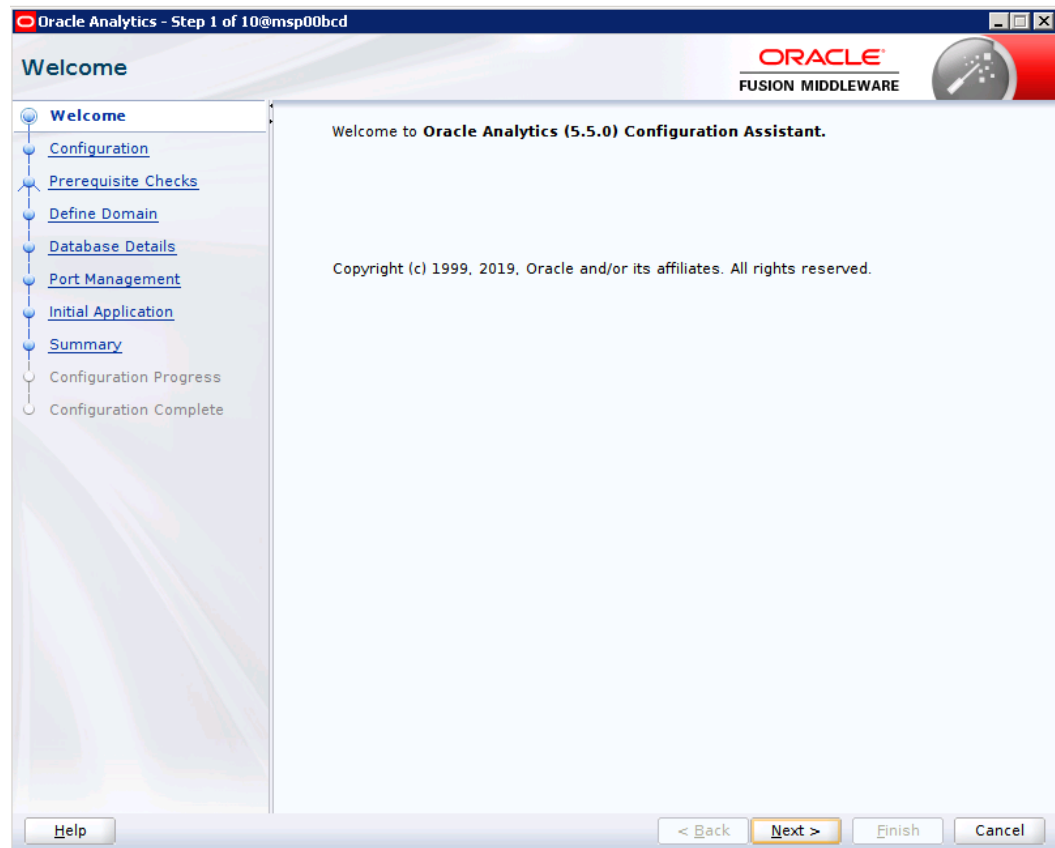
The following post-installation tasks are involved once OAS Publisher has been installed:

5. Configure the OAS Publisher repository. Set security model, add users, assign roles, add reports, add printers, set repository path, set data source, etc.
6. Set up and copy the RMS OAS Publisher Report Templates produced for RMS.

7. Set up for the RMS application specific configuration files to integrate OAS Publisher with the RMS online app.

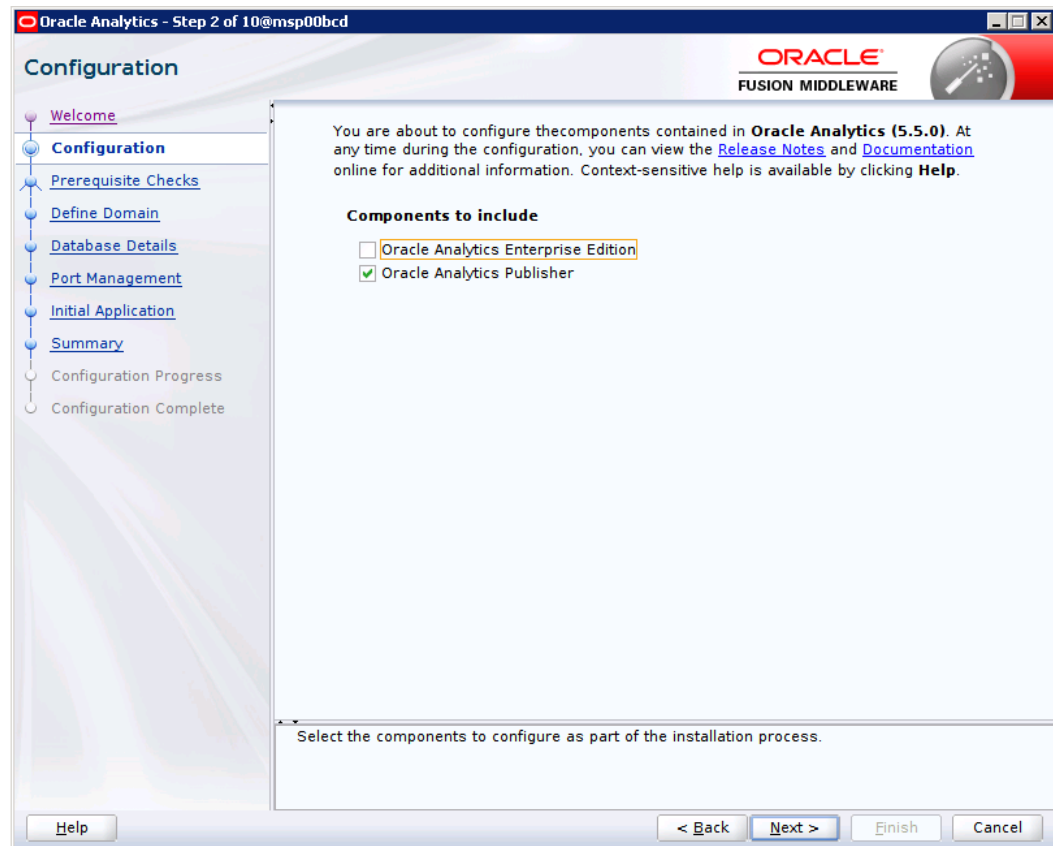
Install Oracle Analytics Server 5.5

1. Install JDK 1.8 as per product certification
2. For Example, /u01/product/fmw/wls_oas
3. Export your DISPLAY.
4. Example: export DISPLAY=10.141.10.110:0.0
5. Install Oracle Fusion Middleware Infrastructure in OAS Product Home (fmw_12.2.1.4.0_infrastructure_generic.jar)
JDK_HOME/bin/java -jar fmw_12.2.1.4.0_infrastructure.jar
6. Install Oracle Analytics Server 5.5
JDK_HOME/bin/java -jar Oracle_Analytics_Server_5.5.0.jar
For more details, refer *Installing and Configuring Oracle Analytics Server 5.5.0 F27232-04 Guide*
7. Launch Oracle Analytics configuration Assistant by executing
Go to \$OAS_HOME/bi/bin
Example: /u01/product/fmw/wls_oas/bi/bin
Start configuring domain: ./config.sh
8. Click Next.

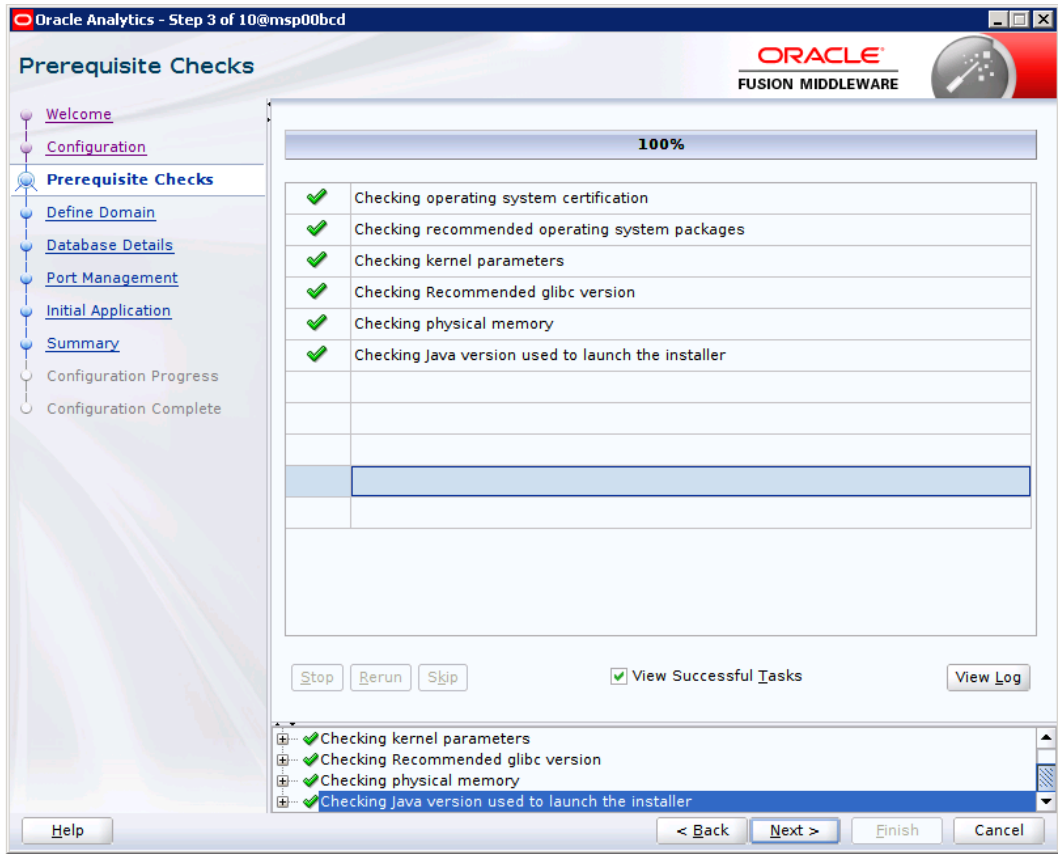


9. Select Oracle Analytics Publisher for configuring reports only

Note: Select both components for Configuring Operational Insights (Optional)



10. Click Next.



11. Provide Domain Directory and Name. Create Admin Username and Password

The screenshot shows the 'Define Domain' step of the Oracle Analytics installation. The window title is 'Oracle Analytics - Step 4 of 10@msp00bcd'. The Oracle Fusion Middleware logo is in the top right. A left-hand navigation pane lists the steps: Welcome, Configuration, Prerequisite Checks, Define Domain (selected), Database Details, Port Management, Initial Application, and Summary. Below these are 'Configuration Progress' and 'Configuration Complete' indicators. The main content area explains the domain concept and provides input fields for domain location and credentials. The 'Domains Directory' field contains '/scratch/u01/domains/wls_oas/' with a 'Browse' button. The 'Domain Name' field contains 'OAS PUBDomain'. The 'Domain Home' field contains '/scratch/u01/domains/wls_oas//OAS PUBDomain'. Under 'Credentials for new domain', the 'Username' field contains 'weblogic', and both 'Password' and 'Confirm Password' fields contain masked characters. A note at the bottom specifies password requirements: minimum 8 characters, maximum 30 alphanumeric characters, must begin with an alphabetic character, and can include underscore, dollar, or pound characters.

Define Domain

Welcome
Configuration
Prerequisite Checks
Define Domain
Database Details
Port Management
Initial Application
Summary
Configuration Progress
Configuration Complete

The domain is the basic unit of WebLogic administration. All Oracle Analytics components reside in one domain. The domain needs a place to store files, and initial administrator credentials.

The domain files include configuration files, log files, and data files.

The credentials define the initial administrator account. For security reasons no other default accounts are created. Use this initial account to create individual accounts for your users.

Location of new domain

Domains Directory

Domain Name

Domain Home

Credentials for new domain

Username

Password

Confirm Password

Confirm the password by entering it again.
The password must be a minimum of 8 and not exceed 30 alphanumeric characters. It must begin with an alphabetic character, use only alphanumeric, underscore (_), dollar (\$) or pound (#) characters and include at least 1 digit.

12. Select Create New schemas. Enter your Oracle Database information. Simple connect string like <DBHOST>:1521:<PDB>

Oracle Analytics - Step 5 of 10@msp00bcd

Database Schema

Database schemas are required for storage of internal housekeeping information. These schemas are distinct from any data sources which you plan to analyse in Oracle Analytics.

The simplest option is to create new database schemas here. Alternatively you can use existing schemas you created earlier using the Repository Creation utility (RCU). Using RCU in advance gives you additional options, such as choosing tablespaces. RCU is available in directory /scratch/u01/product/fmw/wls_oas/oracle_common/bin.

☒ Create new schemas

Schema prefix: OASPUB

Schema password:

Confirm schema password:

Database type: Oracle Database

Username: sys

Password:

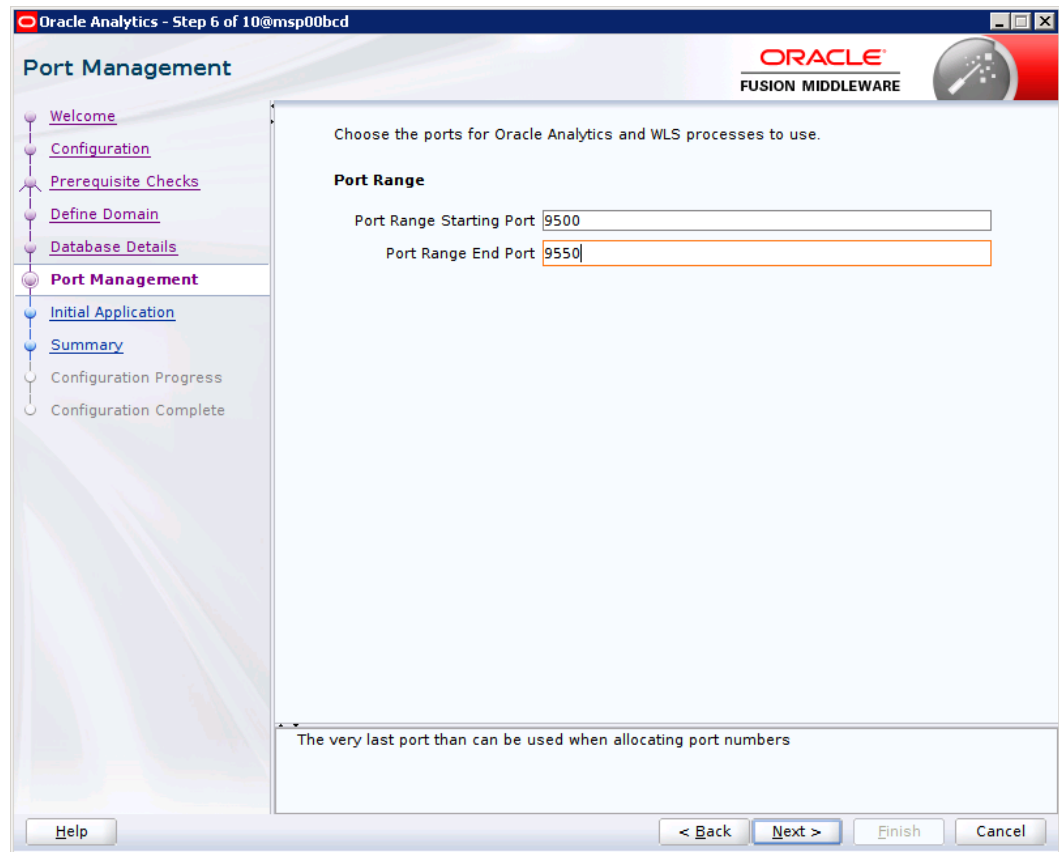
Simple connect string: <DB_HOST>:1521:<PDB>

☐ Use existing schemas

Enter the connect string in the format hostname:port:service_name for the Oracle database. Use only for non-RAC databases. Use the separate Oracle RAC option for all RAC databases, included those accessed using an Oracle Single Client Access Name (SCAN) address

Help < Back Next > Finish Cancel

13. Choose Port Range



The screenshot shows the 'Port Management' window in the Oracle Analytics installation wizard. The window title is 'Oracle Analytics - Step 6 of 10@msp00bcd'. The Oracle Fusion Middleware logo is in the top right. On the left is a navigation pane with links: Welcome, Configuration, Prerequisite Checks, Define Domain, Database Details, Port Management (selected), Initial Application, Summary, Configuration Progress, and Configuration Complete. The main area is titled 'Port Management' and contains the instruction 'Choose the ports for Oracle Analytics and WLS processes to use.' Below this, under the heading 'Port Range', are two input fields: 'Port Range Starting Port' with the value '9500' and 'Port Range End Port' with the value '9550'. At the bottom of the main area, a note states 'The very last port than can be used when allocating port numbers'. The bottom of the window has a 'Help' button on the left and '< Back', 'Next >', 'Finish', and 'Cancel' buttons on the right.

Oracle Analytics - Step 6 of 10@msp00bcd

Port Management

Choose the ports for Oracle Analytics and WLS processes to use.

Port Range

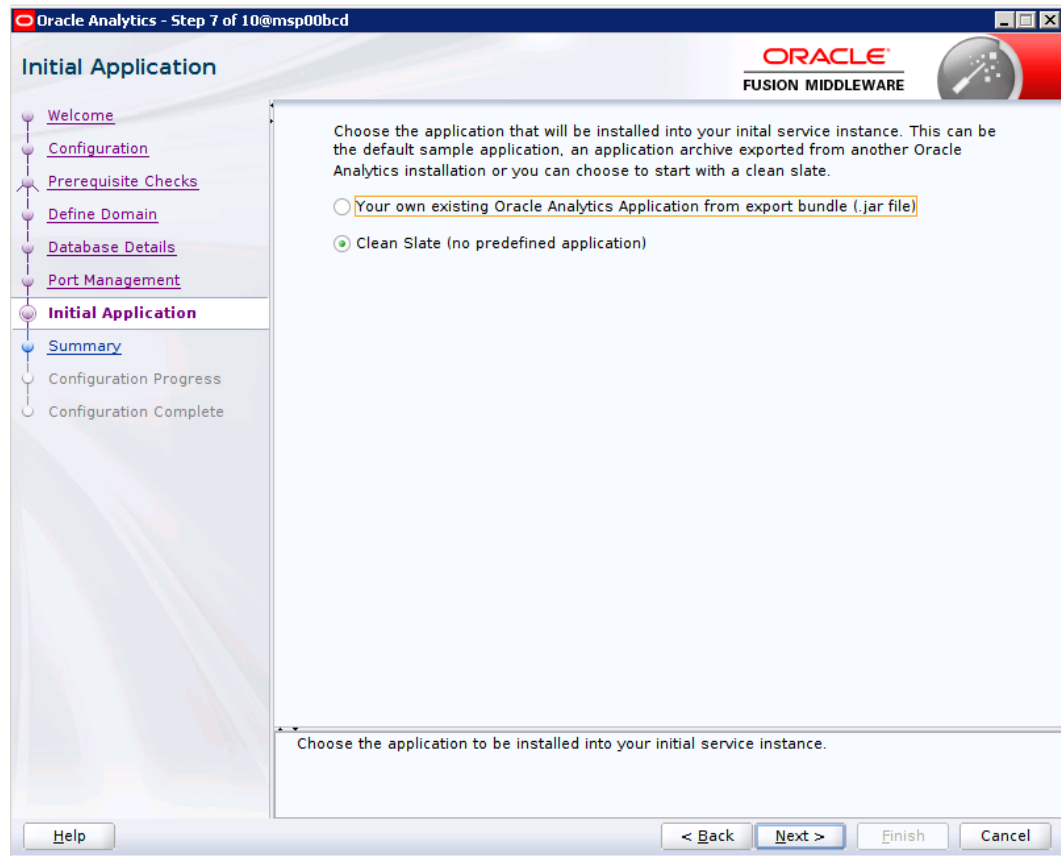
Port Range Starting Port: 9500

Port Range End Port: 9550

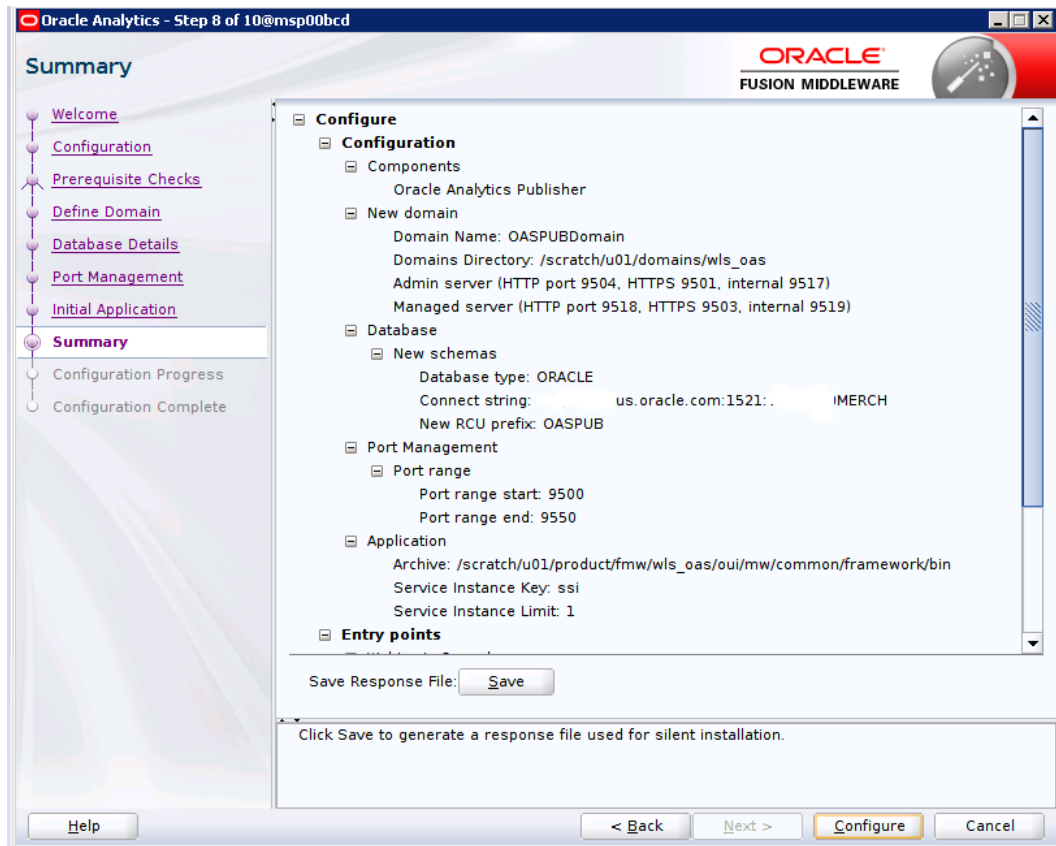
The very last port than can be used when allocating port numbers

Help < Back Next > Finish Cancel

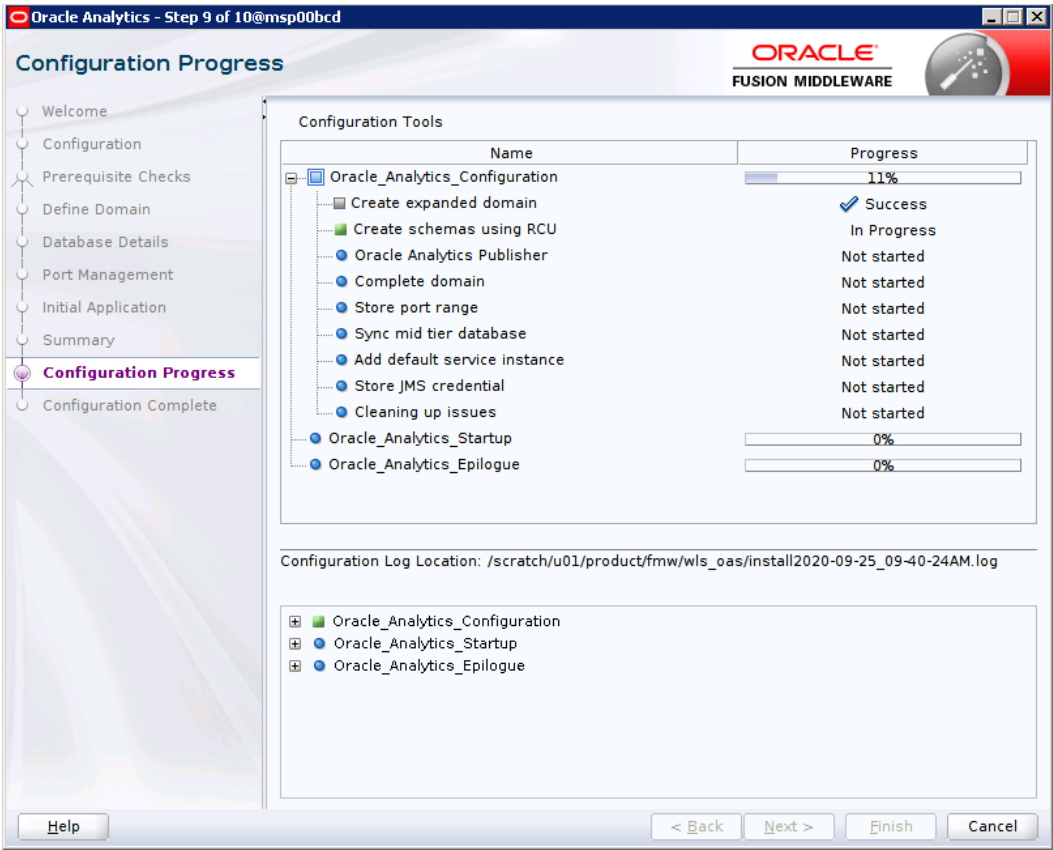
14. Select Clean Slate

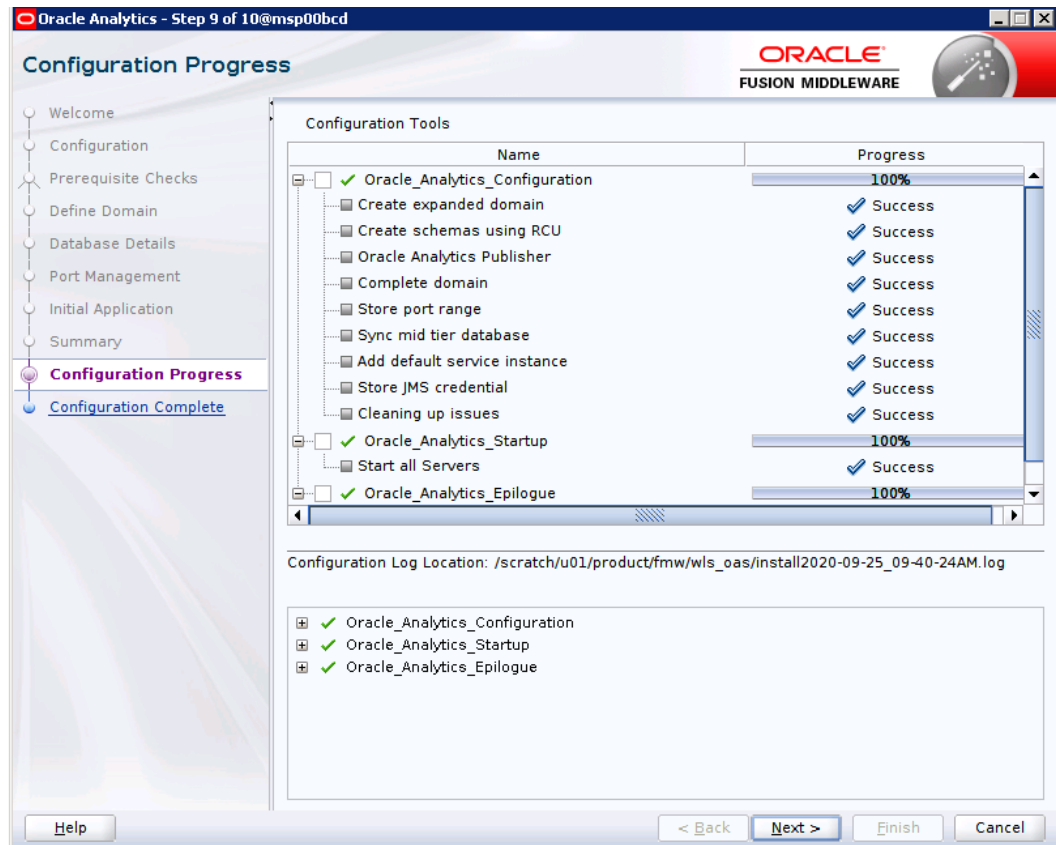


15. Click on Configure

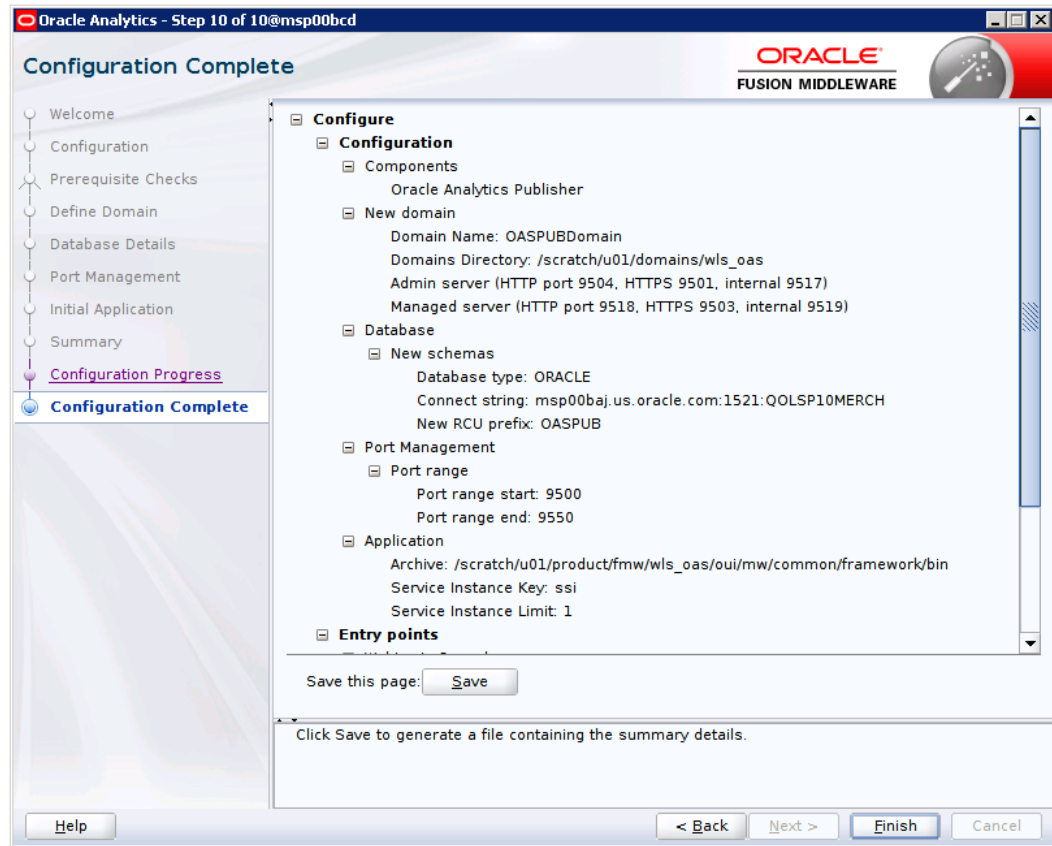


16. Click Next





17. Click Finish



Configure OID Provider in OAS 5.5 WebLogic Domain

The OID Provider needs to be configured in OAS 5.5 WebLogic domain.

Note: In this section, the base DN “dn=us,dn=oracle,dn=com” is used as an example. Modify this value as per the organisation’s ldap settings.

Perform the following procedure to create providers in the domains created in the previous steps.

1. Log in to the Administration Console.
`http://<OAS_HOST>:<OAS_PORT>/console/`
2. In the Domain Structure frame, click **Security Realms**.
3. In the Realms table, click **myrealm**. The Settings for myrealm page is displayed.
4. Click the Providers tab.
5. Click **Lock & Edit** and then click **New**. The ‘Create a New Authentication Provider’ page is displayed.

Home Log Out Preferences Record Help

Home > Summary of Servers > Summary of Machines > apphost.us.oracle.com > Summary of Servers > Summary of Security Realms > myrealm > Providers

Create a New Authentication Provider

OK Cancel

Create a new Authentication Provider

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

* Indicates required fields

The name of the authentication provider.

* **Name:**

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

Type:

OK Cancel

- Enter **OIDAuthenticator** in the Name field and select **OracleInternetDirectoryAuthenticator** as the type. Click **OK**.

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

Home > Summary of Servers > Summary of Machines > apphost.us.oracle.com > Summary of Servers > Summary of Security Realms > myrealm > Providers

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

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

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

Customize this table

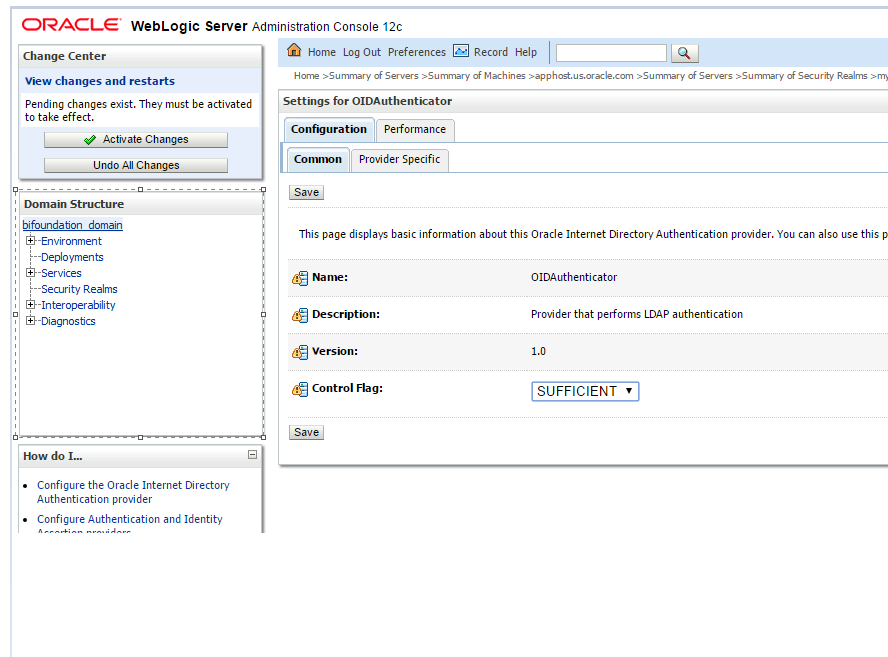
Authentication Providers

New Delete Reorder Showing 1 to 4 of 4 Providers

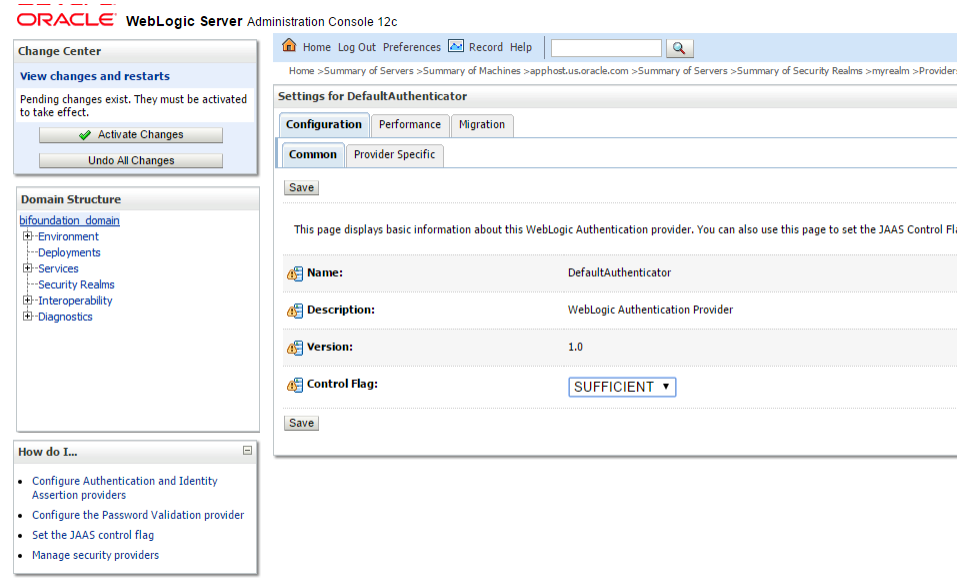
<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
<input type="checkbox"/>	OIDAuthenticator	Provider that performs LDAP authentication	1.0

New Delete Reorder Showing 1 to 4 of 4 Providers

- All the providers are displayed. Click **OIDAuthenticator**. Settings of **OIDAuthenticator** are displayed.



8. Set the Control Flag field to SUFFICIENT and click **Save**.
9. From the Providers tab, click on DefaultAuthenticator -> Configuration tab -> Common tab. Update the Control Flag to SUFFICIENT.
10. Click **Save**.



11. From the Providers tab, click the "OIDAuthenticator" (you just created), in the configuration -> Provider Specific tab enter your LDAP connection details:
The values shown below are examples only. You should match the entries to your OID.
 - Host: <oidhost>
 - Port: <oidport>

- Principal: cn=orcladmin
- Credential: <password>
- Confirm Credential: <password>
- User Base DN: cn=users,dc=us,dc=oracle,dc=com
- Check 'Retrieve credentials as principal.'

The screenshot shows the Oracle WebLogic Server Administration Console. The left sidebar contains the 'Change Center' with options to view changes and restarts, and a 'Domain Structure' tree. The main area displays the 'Settings for OIDAuthenticator' configuration page. The 'Configuration' tab is active, showing the 'Provider Specific' section. The configuration includes fields for Host (idmhost.us.oracle.com), Port (3060), Principal (cn=orcladmin), Credential (masked), Confirm Credential (masked), SSL Enabled (unchecked), User Base DN (cn=Users,dc=us,dc=oracle,dc=com), All Users Filter ((&(cn=*)(objectclass=person))), and User From Name Filter ((&(cn=%u)(objectclass=persc))).

12. Modify the following:

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

The screenshot shows the 'Groups' configuration page in the Oracle WebLogic Server Administration Console. The configuration includes fields for Group Base DN (cn=groups,dc=us,dc=oracle,dc=com), All Groups Filter ((&(cn=*)(objectclass=groupc)), Group From Name Filter ((&(cn=%g)(objectclass=grouc)), Group Search Scope (subtree), Group Membership Searching (unlimited), and Max Group Membership Search Level (0). There is also an 'Ignore Duplicate Membership' checkbox.

13. Check Propagate Cause For Login Exception

☒ Propagate Cause For Login Exception

☒ Cache Enabled

Cache Size:

Cache TTL:

GUID Attribute:

14. Click **Save**.

15. Click the **Providers** tab.

The screenshot shows the Oracle WebLogic Server Administration Console. On the left, the 'Change Center' panel shows 'View changes and restarts' with buttons for 'Activate Changes' and 'Undo All Changes'. Below it is the 'Domain Structure' tree with 'bifoundation_domain' selected. The main area shows the 'Providers' tab for 'myrealm'. It includes a 'Customize this table' link and a table of 'Authentication Providers'.

Name	Description	Version
DefaultAuthenticator	WebLogic Authentication Provider	1.0
DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0
OIDAuthenticator	Provider that performs LDAP authentication	1.0

16. Click **Reorder**.

17. Move **OIDAuthenticator** to the top of the providers list

The screenshot shows the 'Reorder Authentication Providers' dialog box. It contains a list of 'Available' providers: 'OIDAuthenticator' (selected), 'Trust Service Identity Asser', 'DefaultAuthenticator', and 'DefaultIdentityAsserter'. Arrows on the right allow moving providers up or down. The dialog also has 'OK' and 'Cancel' buttons.

18. Click OK.

19. Once your changes are saved, click **Activate Changes**.

Click the Lock & Edit button to modify, add or delete items in this domain.

Lock & Edit
Release Configuration

Domain Structure

- bifoundation_domain
 - Environment
 - Deployments
 - Services
 - Security Realms
 - Interoperability
 - Diagnostics

How do I...

- Configure Authentication and Identity Assertion providers
- Configure the Password Validation provider
- Manage security providers
- Set the JAAS control flag

System Status

Health of Running Servers

Failed (0)

Home > apphost.us.oracle.com > Summary of Servers > Summary of Security Realms > myrealm > Providers > OIDAuthenticator > Providers > DefaultAuthenticator > Providers > Providers

Messages

✓ All changes have been activated. However 2 items must be restarted for the changes to take effect.

Settings for myrealm

Configuration Users and Groups Roles and Policies Credential Mappings **Providers** Migration

Authentication Password Validation Authorization Adjudication Role Mapping Auditing Credential Mapping

Certification Path Keystores

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

Customize this table

Authentication Providers

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

New Delete Reorder Showing 1 to 4 of 4 Previous Next

<input type="checkbox"/>	Name	Description	Version
<input type="checkbox"/>	OIDAuthenticator	Provider that performs LDAP authentication	1.0
<input type="checkbox"/>	DefaultAuthenticator	WebLogic Authentication Provider	1.0
<input type="checkbox"/>	DefaultIdentityAsserter	WebLogic Identity Assertion provider	1.0

New Delete Reorder Showing 1 to 4 of 4 Previous Next

20. Shutdown all servers and restart the admin server using startWebLogic.sh script.

Load LDIF Files in LDAP

The OID (Oracle Internet Directory) must be set up in order to perform the configuration of OID Authenticator in Oracle BI EE WebLogic Domain.

There are two ldifs which need to be loaded in OID.

- BI_Group.ldif
- BI_User.ldif

Note: The ldif files are updated in [Appendix: BI User and Group LDIF Entries](#).

The steps given below can be used to import the Groups and Users into the LDAP using the LDIF files.

Note: If you are using the above LDIF files to set up the users and groups, you must update the 'BI_User.ldif' LDIF file with your password for the 'userpassword' attribute for all the users mentioned in the RESA-oid-create-user.ldif LDIF file. The changes must be done before importing the users LDIF file 'BI_User.ldif' into the LDAP. Once the users are imported into the LDAP, remove the 'userpassword' attribute value from the LDIF file. Refer to the *Oracle Internet Directory Administration Guide* for OID password policies for setting up passwords.

User DN and Group DN values (example:dc=us,dc=oracle,dc=com) may need to be updated based on the DN values in your OID.

Once the LDIF files are updated for your configuration, the LDIF files can be loaded into LDAP using the ldapadd tool that is included in the OID installation. LDIF files can also be imported in other ways like ODSM.

For example to load BI_Group.ldif using ldapadd (this is done on the OID host)

```
export ORACLE_HOME=/u00/webadmin/products/wls_idm/ORACLE_IDM (this is the ORACLE_HOME of your OID install)
```

```
export PATH=$ORACLE_HOME/bin:$PATH
```

```
$ORACLE_HOME/bin/ldapadd -v -c -h <OID_HOST> -p 3060 -w <ORCLADMIN  
PASSWORD> -D "cn=orcladmin" -f BI_Group.ldif
```

The same can be done to BI_User.ldif

Configure Oracle Single Sign-On

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

Create the SSO provider in the Oracle Analytics Domain

1. Log into the WebLogic console.
2. Navigate to: security realms -> myrealm (default realm) -> providers.
3. Start a Lock and Edit session.
4. Click **New provider**.
5. Set the provider name (Default: OAMIdentityAsserter).
6. Click **Ok**.
7. Open the new provider configuration.
8. Under Common, set the Control Flag to SUFFICIENT.
9. On the provider list, click **Reorder**.
10. Move the OAMIdentityAsserter to the top of the list, or above the DefaultAuthenticator.
11. Click **Ok**.
12. Click **Activate Changes**.
13. Shutdown the domain.
14. Start the admin and managed servers for the domain.

Configure RPD and Set up the Database Connection

In Oracle Analytic Server 5.5 RPD, Catalog and Security model metadata of a Service Instance can be migrated through Oracle Business Intelligence application archive (BAR) file. Refer "Managing Metadata and Working with Service Instances" chapter of the *Fusion Middleware System Administrator's Guide for Oracle Business intelligence Enterprise Edition* for additional details.

Note: The screen illustrations in the following steps are only examples. The screens that appear depend on the setup of your system.

A BAR file is a compressed archive file that contains a cohesive set of BI metadata artifacts (data model, content model, and authorization model). The Operational Insights Bar file packaged in the installer and will be available under `rpdcatalog-bar/Operational_Insights.bar`.

Bar file administration can be done at a command line through the WebLogic Scripting Tool (WLST).

1. Navigate to `/u01/domains/wls_oas/OASDomain/bitools/bin/` to invoke WLST command line as shown below.
For Example:

```
/u01/domains/wls_oas/OASDomain/bitools/bin/  
u01/domains/wls_oas/OASDomain/bitools/bin/> ./wlst.sh Initializing WebLogic  
Scripting Tool (WLST)... Welcome to WebLogic Server Administration Scripting Shell  
Type help () for help on available commands wls:/offline>
```
2. To view all the service instances in a domain use the WLST command

```
listBIServiceInstances: wls:/offline> listBIServiceInstances('/u01/domains/  
wls_oas/OASDomain ')  
oracle.bi.servicelcm.spi.PluginFinder createLoader INFO: Found servicelcm  
plugin jar:
```

Import BAR file

Import RPD, catalog, security model using BAR file. Options are available to import all three or just specific components.

Perform the following to import the `Operational_Insights.bar` file without security model:

Getting command parameters

```
domains/bi/bitools/bin/importarchive.sh -h
```

USAGE : <service instance key> <location of bar file to import> [nodatamodel]
[nocontent] [noauthorization] [nodatasets] [nosearch] [noaction]
[encryptionpassword=<encryption password for connections>]

nodatamodel	: Do not import RPD metadata content
nocontent	: Do not import WEBCAT metadata content
noauthorization	: Do not import JAZN metadata content
nodatasets	: Do not import DSS metadata content
nosearch	: Do not import Search metadata content
noaction	: Do not import Action metadata content
encryptionpassword	: Encryption password for connections if any

For Example:

```
./importarchive.sh ssi Operational_Insights.bar encryptionpassword=Admin123
```

```
importarchive.sh '/u00/webadmin/config/domains/wls_obiee/Bifoundation_domain'  
, 'ssi', '/u00/webadmin/media/rpd/Operational_Insights.bar'  
, true, true, false, 'Admin123'
```

Starting Import Service Instance

....

....

Finished Import Service Instance

- **OAS_DOMAIN_HOME:** Oracle Analytics Server Domain home
- **ServiceInstanceKey:** Service instance key name which it will be imported
- **BAR_FILE_LOCATION:** The Bar file full path and name
- **Whether to import RPD:** If RPD file need to be imported from BAR file. The default value is true, change to false if not needed
- **Whether to import WebCat:** If Web Catalog need to be imported from BAR file. The default value is true, change to false if not needed
- **Whether to import Security Model:** If security model need to be imported from BAR file. The default value is true, change to false if not needed
- **RPD_Password:** This is the password used to encrypt the database connection credentials in the RPD

Updating Connection pool for RPD

Uploaded RPD through BAR file migration can be found in the below directory
/bidata/service_instances/ssi/metadata/datamodel/customizations.

Verify the existence of “tnsnames.ora” file under / config/fmwconfig/bienv/core directory and the file has an entry of the database used by Operational Insights

For Example:

```
<DB_SID> = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp) (host =  
<RMS_DB_HOST>) (Port = 1521)))) (CONNECT_DATA = (SERVICE_NAME = <DB_SID>)))
```

Modify connection pool of RPD according to the environment.

There are two methods for updating connection pool.

1. Download rpd and update variables by obiee client tool and again upload rpd.
 - a. Download RPD file using datamodel.sh script available in
<OAS_DOMAIN_HOME>/bitools/bin directory

Download RPD:

OAS Domain tool

/u00/webadmin/config/domains/wls_obiee/Bifoundation_domain/bitools/bin/

Command:

```
./datamodel.sh downloadrpd -O /<RPD  
PATH>/<RPD_file_name_to_download.rpd> -U <weblogic user> -p  
<Weblogic Passwd> -ssi <service_instance>
```

```
-O filename of the downloaded RPD file  
-SI the OBIEE service instance, e.g. ssi  
-U the weblogic administrator user-id  
-P the weblogic administrator password
```

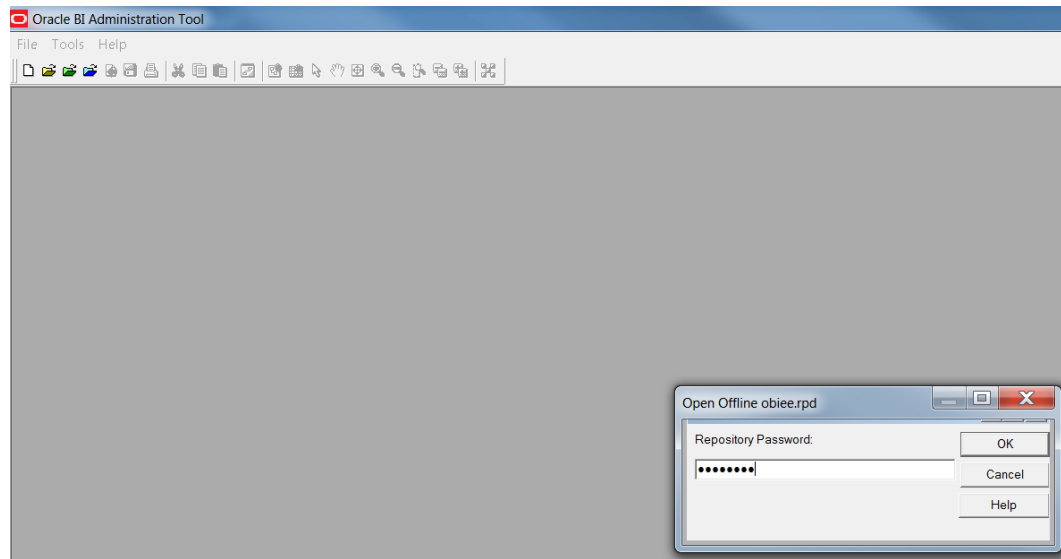
Example:

```
datamodel.sh downloadrpd -O Operational_Insights.rpd -SI ssi -U weblogic - P  
<Password>
```

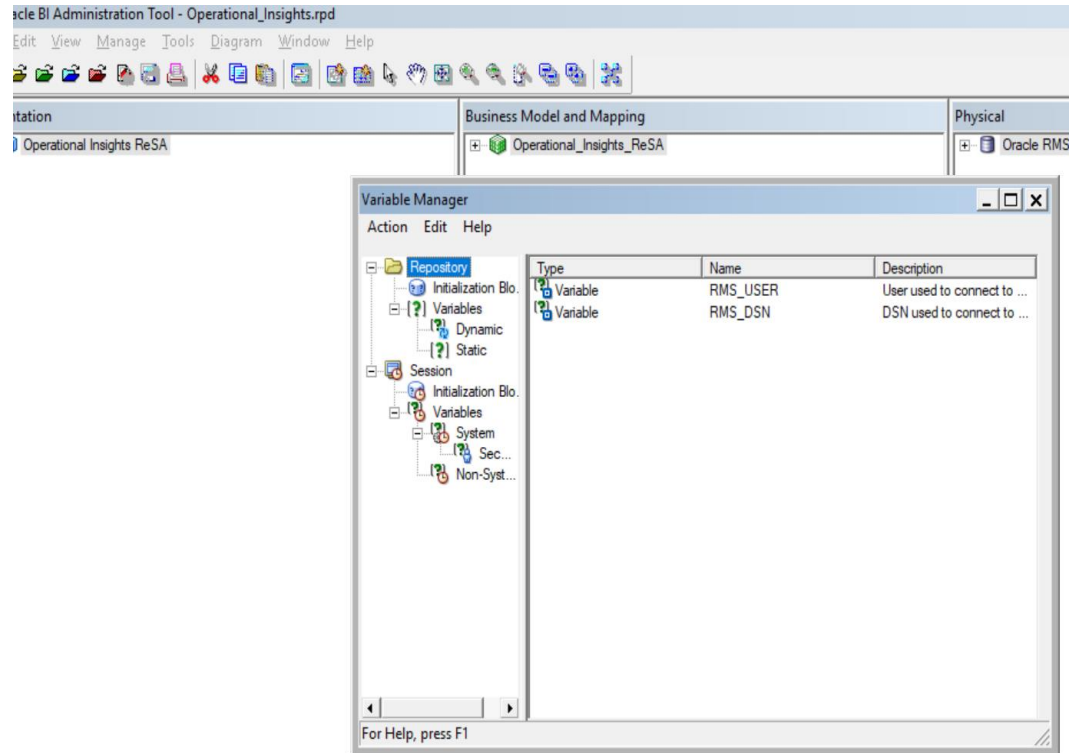
- b. Copy the Operational_Insights.rpd file and open the rpd file in 12c OAS Client tool and make changes to the db variables. The Oracle OA Client tool can be downloaded from

Oracle Analytics Client Tools 5.5.0

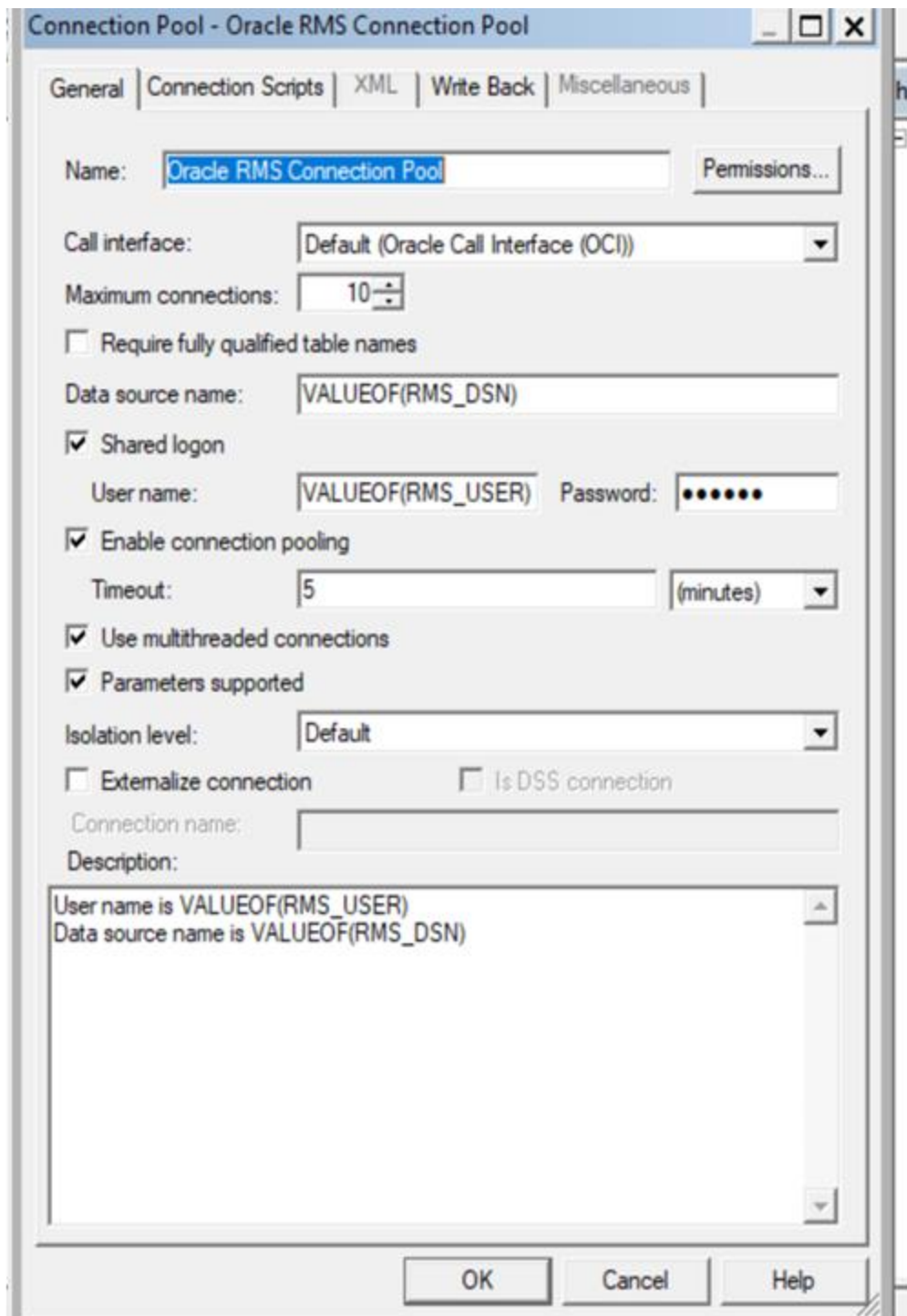
<https://www.oracle.com/solutions/business-analytics/analytics-server/analytics-server.html>



- i. When prompted for the password, provide RPD password
- ii. When the rpd is opened, from the menu, go to Manage > Variables.
- iii. Provide password: Admin123



- iv. Under Repository Static variables, Double-click on RMS_USER to edit with main RMS schema username (for example, RMS01) and RMS_DSN with Data Source Name of the RMS Database.
- v. In the Physical Layer, open the Connection Pool (Oracle RMS Connection Pool) under "Oracle RMS OLTP" and update the password for the RMS User. The following is a sample of the Oracle RMS Connection Pool screen.



- vi. Follow the same steps for Oracle Data RMS Repository Initblocks Connection Pool.
- vii. Save the Operational_Insights.rpd file.
- viii. Test the database connection by right-clicking on any of the tables in the Physical Layer, and select Update Row Count. The number of rows will be shown when that table is highlighted if the database connection is successful.

-
- c. Upload the Operational_Insights.rpd back to the OBIEE Domain under the destination environment.

```
<OAS_DOMAIN_HOME>/bitools/bin/datamodel.sh uploadrpd -I Operational_Insights.rpd -SI ssi -U
<weblogic> -P <WLS_password>
```

Example: ./datamodel.sh uploadrpd -I Operational_Insights.rpd -SI ssi -U weblogic -P <Password>

- d. RPD will have been updated in
<OAS_DOMAIN_HOME>/bdata/service_instances/ssi/metadata/datamodel/
customizations.

Note: When making any changes to the repository, do it in the offline mode and before saving the changes perform a global consistency check. The global consistency check should not show any errors. Out of the box Operational Insight repository will have some warnings when a Global Consistency Check is done. These warnings do not affect Operational Insight functionality in any way and these are been thoroughly verified.

2. Create a connect pool file and update directly to existing rpd.
 - a. Create ConnectionPool.json file from the Oracle BI EE Domain
 - b. Navigate to /<ORACLE_OAS_HOME>/bitools/bin
 - c. Execute following command to generate connection pool content for ConnectionPool.json file

```
./datamodel.sh listConnectionpool -SI ssi -U <WLS_Admin_UserName> -P
<WLS_Admin_Password>
```

Save the json out result

```
nohup ./datamodel.sh listConnectionpool -SI ssi -U weblogic -P <Password> >
ConnectionPool.json&
```

Modify the json file with DB details

/u00/webadmin/config/domains/wls_obiee_oi/Bifoundation_domain/bitools/bin>

```
./datamodel.sh listConnectionpool -SI ssi -U weblogic -P <Password>
{
  "Title": "List Connection Pools",
  "Conn-Pool-Info": [
    {
      "uid": "00000001-3216-14ed-806e-0a0a0a0000",
      "connPool": "Oracle RMS Connection Pool",
      "parentName": "\"Oracle RMS OLTP\"",
      "user": "VALUEOF(RMS_USER)",
      "password": "<RMS_SCHEMA_PASSWORD>",
      "dataSource": "VALUEOF(RMS_DSN)",
      "appServerName": "Null"
    },
    {
      "uid": "80000000-2a48-14f1-8029-0a0a0a0000",
      "connPool": "Oracle Data RMS Repository Initblocks Connection
Pool",
      "parentName": "\"Oracle RMS OLTP\"",
      "user": "VALUEOF(RMS_USER)",
      "password": "<RMS_SCHEMA_PASSWORD>",
      "dataSource": "VALUEOF(RMS_DSN)",
      "appServerName": "<Replace Me>"
    }
  ]
}
```



```

    },
    ],
    "Variables-In-Conn-Pool": [
    {
    "uid": "0023844e-0bd7-0000-714b-e31d00000000",
    "variable": "RMS_USER",
    "value": "'<RMS_SCHEMA_NAME>'"
    },
    {
    "uid": "0023844f-0bd7-0000-714b-e31d00000000",
    "variable": "RMS_DSN",
    "value": "'<RMS_DATABASE_NAME>'"
    }
    ]
  }
}

```

Run the command for json file for update connection pool.

```

./datamodel.sh updateConnectionpool -C ConnectionPool.json -SI ssi -U weblogic
-P <Password>

```

- d. Copy the above command output and save in ConnectionPool.json file
- e. Modify environment variables like RMS Schema username, password and RMS Database Name according to environment and Save the file
- f. Once after update, run following command. /bitools/bin/datamodel.sh
updateConnectionpool -C ConnectionPool.json -SI \$SSI -U -P Service Instance: ssi
Operation successful. Connection pool update completed successfully.

- g. Restart the OBIEE services.
cd <OAS_DOMAIN_HOME>/bitools/bin
./stop.sh
./start.sh
./status.sh

Configure Oracle Retail Operational Insights Roles and Application Roles

Migrating Application Roles

The Operational application roles are archived in a Jar file (OI_WebCatalog_RPD_Migration.jar) and packaged along with the Operational Insights installer in rpd-catalog-bar directory.

1. Extract the Operational insights package and migrate the jar file to get the require application roles.

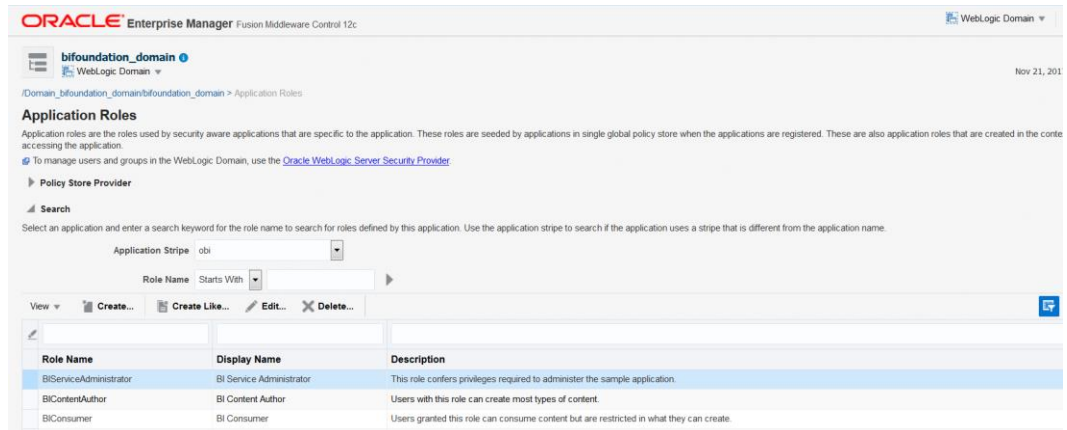
Navigate to <OAS_DOMAIN_HOME>/bitools/bin
./migration-tool.sh in <OI_WebCatalog_RPD_Migration.jar> ssi

Configure Users & Groups through EM Application Roles

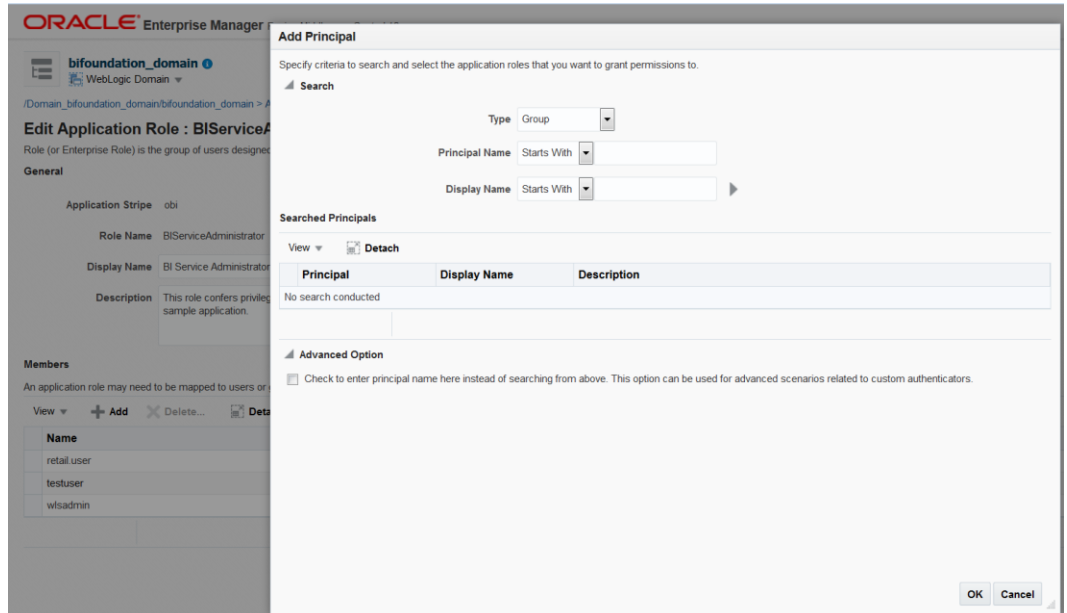
1. Login to OAS_DOMAIN EM console

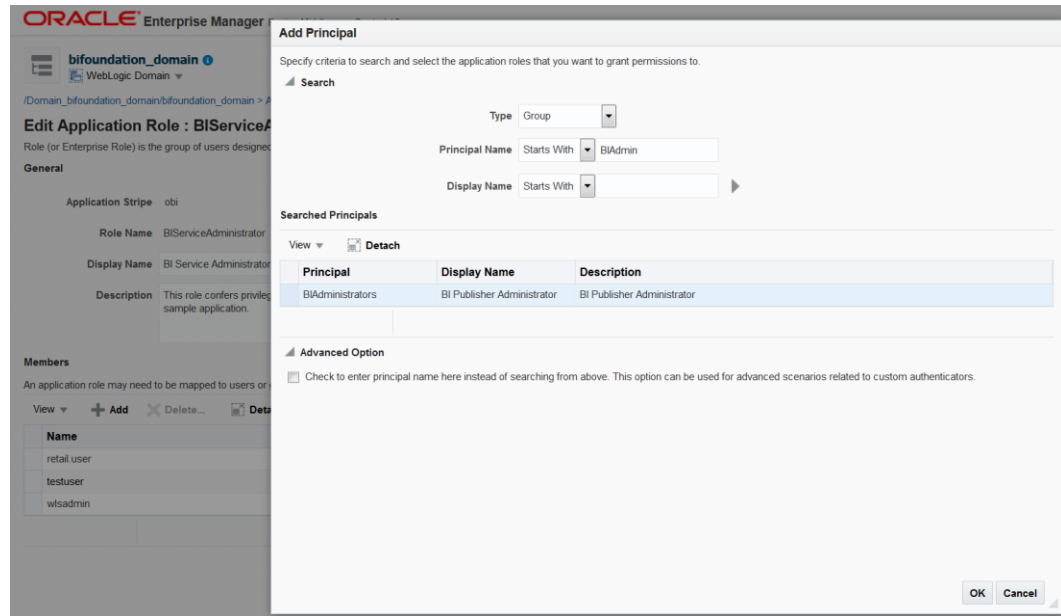


2. Click on WebLogic Domain and navigate to Security→Application Roles



3. Select BIServiceAdministrator role and click on **Edit**
4. Modify the type as Group and search for BIAdministrators group which was added/configured during "Load LDIF Files in LDAP" section.





BIAdministrators groups has been added to BIServiceAdmin Application role.

Now Users configured/setup under BIAdministrators group (LDAP) can access Operational insights application catalog and Dashboards.

Similarly add users/groups under BIContentAuthor and BIConsumer roles to get content and consumer access.

For more details refer “Managing Application Roles and Application Policies Using Fusion Middleware Control”

<https://docs.oracle.com/middleware/12212/biee/BIESC/GUID-7204D273-79EE-4A1A-BFCD-CF4C137328FE.htm#GUID-C5C45BBF-9271-4263-B7DB-C49D2EB18057>.

Language Selection with SSO

See the "Enabling SSO Authentication" chapter in the Oracle BI EE Security Guide for more information about configuration changes.

Operational Insights dashboards and reports display the same language as ReSA/REIM/Alloc by accepting the Lang parameter from the Respective system.

Operational Insights Configuration

- Operating System
RPD_post_install.txt which contain password to protect Operational Insights OBIEE code should be owned by Operational Insight UNIX user and installed with 600 permission. Password in Oracle BI EE should be changed after installation is done.
- Oracle BI EE Server
Operational Insights Oracle BI EE metadata files (rpd, catalog, and translation) should be owned by Operational Insights system administrator and installed with 750 permissions.

Infrastructure/Middleware

- Jdbc connection

Oracle database access through Oracle BI EE can be secured by using a Jdbc connection. The Jdbc connection setup is provided in rpd file. User needs to provide database login credential in the rpd file. The database login credential is stored securely through Oracle BI EE.

Operational Insights Security Role

Operational Insights provides role based security in the current release. The access permission of Operational Insights logical tables for each security role has been defined in Operational Insights rpd file. Within these roles, the user has the privilege to access every subject area of Operational Insights. It is designed for client's testing, developing, or similar non-business activities. Due to the extent of access associated with this role, it should be used cautiously. See the Oracle Retail Merchandising Security Guide for additional information on the Operational Insights security role.

Export BAR file

In Oracle BI EE 12c RPD, catalog and security model can be exported from any environment or within environment and import to another environment through BAR file.

1. Navigate to <OBIEE_ORACLE_HOME>/oracle_common/common/bin to invoke WLST command line as shown below.

For Example:

```
/u00/webadmin/products/wls_obiee/oracle_common/common/bin> ./wlst.sh
Initializing WebLogic Scripting Tool (WLST)...
Welcome to WebLogic Server Administration Scripting Shell
Type help () for help on available commands
wls:/offline>
exportServiceInstance('<OBIEE_DOMAIN_HOME>','<ServiceInstanceKey>','<Working
Directory>','<Export Directory>')
```

For Example:

```
exportServiceInstance('/u00/webadmin/config/domains/wls_obiee/Bifoundation_dom
ain','ssi',' /u01/workDir','/u01/exportDir')
OBIEE_DOMAIN_HOME: Oracle BI EE Domain home
ServiceInstanceKey: Service instance key name which needs to be exported
Work directory: e.g. /u01/workDir
Export directory: e.g. /u01/exportDir
```

Other unused optional parameters like Catalog Runtime info and include credentials can be used based on requirements.

Post Installation Tasks and Configuration

The Oracle BI EE environment has to be configured for enabling Operational Insights. Please follow the steps to configure the Oracle BI EE environment for Operational Insights and restart Oracle BI EE component processes.

Enable the Oracle BI EE Content to be Displayed in IFrame

The Oracle BI EE content is not allowed to be displayed in IFrame by default. Please enable the Oracle BI EE content to be displayed in IFrame using the following step.

Take a backup of the 'instanceconfig.xml' file in the following location

<OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/OBIPS

Add the following under the <Security></Security> section in the instanceconfig.xml file.

```
<InIFrameRenderingMode>allow</InIFrameRenderingMode>
```

Note: The <InIFrameRenderingMode> tag has to be inside the Security section.

Otherwise, you could encounter an issue with the Presentation Server failing to start.

Configure Charts /Charts/to use HTML5

In order to enable charts to use HTML5 instead of Flash, please modify instanceconfig.xml file at the following location

<OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/OBIPS

Add below tags under <views> </views>

```
<Charts>
  <DefaultWebImageType>html5</DefaultWebImageType>
  <MaxVisibleColumns>2000</MaxVisibleColumns>
  <MaxVisiblePages>1000</MaxVisiblePages>
  <MaxVisibleRows>2000</MaxVisibleRows>
  <MaxVisibleSections>25</MaxVisibleSections>
</Charts>
```

Enable EVALUATE Function in Oracle BI EE

In order to enable the Evaluate function in OBIEE, follow the step below.

Edit the NQSConfig.INI file, located at

<OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/OBIS

This is what you will see by default in the config file

```
# EVALUATE_SUPPORT_LEVEL:
# 1: evaluate is supported for users with manageRepositories permssion
# 2: evaluate is supported for any user.
# other: evaluate is not supported if the value is anything else.

EVALUATE_SUPPORT_LEVEL = 0;
```

Change the parameter EVALUATE_SUPPORT_LEVEL to 2 as follows.

```
# EVALUATE_SUPPORT_LEVEL:
```

```
# 1: evaluate is supported for users with manageRepositories permssion
# 2: evaluate is supported for any user.
# other: evaluate is not supported if the value is anything else.
```

```
EVALUATE_SUPPORT_LEVEL = 2;
```

Restart Oracle BI EE component processes by running stop and start scripts in <OBIEE_DOMAIN_HOME>/bitools/bin directory.

```
./stop.sh
```

```
./start.sh
```

Error: for Iframe is not allowed to display the Reports

Following file need to make entry as Add the tag:

```
<property name="X_FRAME_OPTIONS" value="false"/>
./config/fmwconfig/biconfig/bipublisher/Admin/Configuration/xmlp-server-
config.xml
```

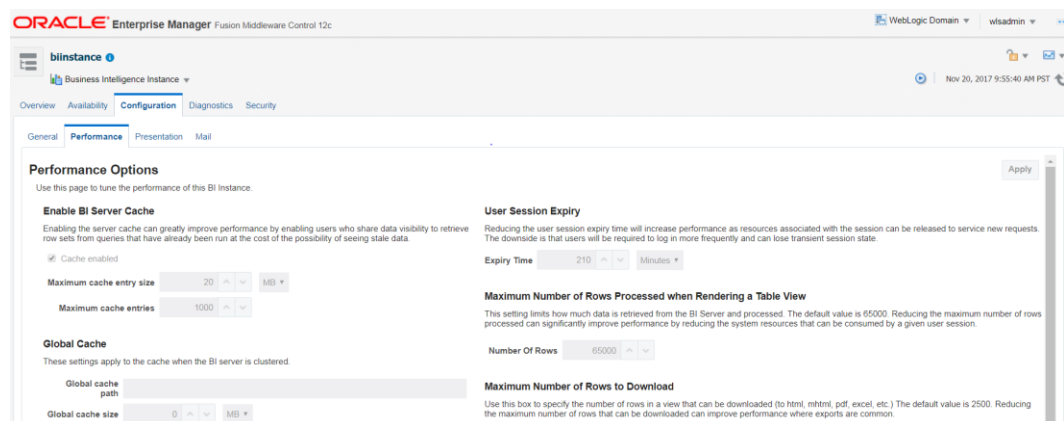
Modified the file in the below location

ActionFrameworkConfig.xml

Disable Cache in Oracle BI EE

The Oracle BI EE cache needs to be disabled to ensure that any saved changes on the Oracle Retail Application are reflected immediately in the Operational Insights reports which are embedded in the Oracle Retail Application screens. To disable cache in Oracle BI EE follow the steps below.

1. Log in to the WebLogic Enterprise Manager (EM) via web browser with the URL as http://<OBIEE_HOST>:<OBIEE_ADMIN_PORT>/em. Log in with the username and password created during Oracle BI EE installation.
2. Go to Business Intelligence > biinstance > Configuration > Performance as shown in the following screen.



3. Click on 'Lock and Edit Configuration'.
4. Uncheck the 'Cache enabled' checkbox as shown above. Click on Apply button on the top right of the page and then click on Activate Changes.

-
5. Navigate to the path
<OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/OBIPS
 6. Take a backup of the 'instanceconfig.xml' file and add the below mention code in between the <ServerInstance> </ServerInstance> tag of the instanceconfig.xml file.

```
<Cache>
<Query>
<MaxEntries>100</MaxEntries>
<MaxExpireMinutes>1</MaxExpireMinutes>
<MinExpireMinutes>1</MinExpireMinutes>
<MinUserExpireMinutes>1</MinUserExpireMinutes>
</Query>
</Cache>
```

Enable the ADF Contextual Event Action in Oracle BI EE

The ADF Contextual event action is not enabled by default in the Oracle BI EE installation. It has to be manually enabled. Edit the following file in your Oracle BI EE installation <OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/OBIPS /instanceconfig.xml

In file instanceconfig.xml add a new ActionLinks attribute between the <ServerInstance> </ServerInstance> tag of the instanceconfig.xml file as follows:

```
<ActionLinks><EnableADFContextualEvent>true</EnableADFContextualEvent></ActionLinks>
```

Once the above files added/modified, Restart Oracle BI EE component processes by running stop script and then start script in <OBIEE_DOMAIN_HOME>/bitools/bin directory.

```
./stop.sh
./start.sh
```

Single Sign-On Configuration for Oracle BI EE

When the Oracle BI EE is configured to use Single Sign-On using the Oracle Access Manager and the Oracle Web Tier then the following steps should be followed

Redirect of analytics to the WebLogic Server

If the analytics directory has been configured on the Oracle HTTP server 12c to be redirected to the WebLogic server

1. Change to the directory
<OHS_DOMAIN_HOME>/config/fmwconfig/components/OHS/ohs1
For Example:
/scratch/u00/webadmin/config/domains/wls_ohs_12c/OHSDomain/config/fmwconfig/components/OHS/ohs1
2. This directory has a file called mod_wl_ohs.conf.
3. Edit the mod_wl_ohs.conf file, /analytics context root is configured to be redirected to the WebLogic Server.

```
<Location /analytics>
    SetHandler weblogic-handler
```

```

WebLogicHost obiee_host
WeblogicPort obiee_port
</Location>

```

Verify the Static Resources using the Oracle Web Tier

Clear your browser cache. Verify that you can access the following URLs using the Oracle HTTP Server and port. If the Oracle HTTP server has not been changed during installation then the default port is 7777

http://<WEBTIER_HOST>:<WEB_TIER_PORT>/analytics

Configure for In-Context launches of RMS forms

Step 1:

Add the below configuration in ActionFrameworkConfig.xml file located at
<OBIEE_DOMAIN_HOME>/config/fmwconfig/biconfig/actions

```

<aliases>
  <location-alias>
    <alias>rmshost</alias>
    <actual>http://<RMS_HOST>:<Port></actual>
  </location-alias>
</aliases>

```

```

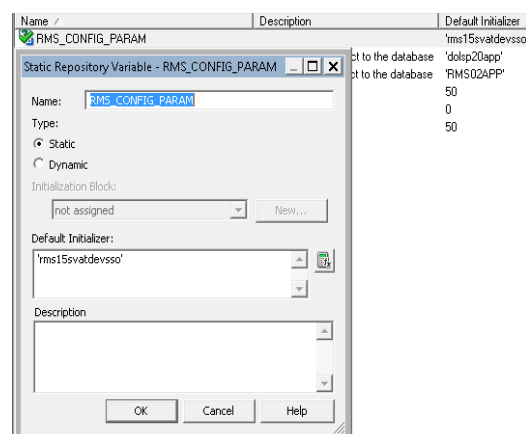
<?xml version="1.0" encoding="UTF-8"?>
<obi-action-config xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="afconfig.xsd">
  <aliases>
    <location-alias>
      <alias>rmshost</alias>
      <actual>http://<RMS_HOST>:<SSO_PORT></actual>
    </location-alias>
  </aliases>

```

Note: There would already be a <aliases \> and that should be replaced with the above 6 lines of code.

Step 2:

1. Change the value of Rpd Variable.
2. Open Rpd go to Manage -> Variable -> Repository -> Statics
3. And change the value of Repository variable: RMS_CONFIG_PARAM



Note: If RMS URL is as below:

`http://<RMS_HOST>:<PORT>/forms/frmservlet?config=<RMS15SSO>`

Then the value of “RMS_CONFIG_PARAM” variable will be “RMS15SSO”

Restart Oracle BI EE

After the above steps are completed, restart the entire Oracle BI EE domain and monitor the logs for any errors.

Validation

Oracle BI EE Analytics should be able to login with RESA/REIM/ALLOC application user and able to view dashboard as well.

Troubleshooting

If any login issue after BAR file migration (RPD and Catalog deployments) or Oracle BI EE presentation services is going to shutdown/failed state then please verify respective instance logs and check accordingly.

Data Migration

ReIM includes a data conversion script that allows you to move old EDI data (reject to table) to the new injector table structure from 14.1.1 to 15.0. This new script and database package includes logic to move data from the old IM_EDI_REJECT% table to the new IM_INJECTOR% tables so that the user can continue working on any documents that were rejected to table before the upgrade.

The script is available in the same directory as other ReIM batch scripts.

Usage

```
dataConversionEDIUpgrade <db_connect_string> <doc_create_username> <default_loc>
<default_dept> <default_class> <include_date_for_doc_dup_check[Y or N]>
<include_year_for_doc_dup_check[Y or N]> <doc_hdr_qty_req[Y or N]> errpath
```

Parameters

db_connect_string	Database connect String
doc_create_username	The batch username (will be used as create_id if at all any document passes validation)
default_loc	edi.default.location from reim.properties
default_dept	edi.default.department from reim.properties
default_class	edi.default.class from reim.properties
include_date_for_doc_dup_check[Y or N]	INCLUDE_DOC_DATE_FOR_DUPLICATE_DOC_CHECK from reim.properties (Y N)
include_year_for_doc_dup_check[Y or N]	INCLUDE_DOC_YEAR_FOR_DUPLICATE_DOC_CHECK from reim.properties (Y N)
doc_hdr_qty_req[Y or N]	document.header.quantity.required from reim.properties (Y N)
errpath	Error File directory

Error and Restart

The script would create errors in the error path if there were any. The user can rerun the script after correcting the reason for failure.

Locking

If the run is successful, the script creates a lock file which would prevent the user from running the upgrade script again. The user can delete the lock file if they need to override and rerun the script for any reason. (Not recommended, since all the documents which got uploaded to IM% tables from previous runs would get rejected as DUPLICATES)

Since this is a data conversion mechanism, it does not perform a reject to file. Users need to go through the errors in IM_INJECT_DOC_ERROR table to check if there are any documents that were earlier part of IM EDI_REJECT% tables and have now been classified as reject to file. (FIXABLE = 'N' in IM_INJECT_DOC_ERROR)

Patching Procedures

Oracle Retail Patching Process

The patching process for many Oracle Retail products has been substantially revised from prior releases. Automated tools are available to reduce the amount of manual steps when applying patches. To support and complement this automation, more information about the environment is now tracked and retained between patches. This information is used to allow subsequent patches to identify and skip changes which have already been made to the environment. For example, the patching process uses a database manifest table to skip database change scripts which have already been executed.

The enhanced product patching process incorporates the following:

Utilities to automate the application of Oracle Retail patches to environments.

Unified patches so that a single patch can be applied against Database, Forms, Java applications, Batch, etc. installations.

Database and Environment manifests track versions of files at a module level.

Centralized configuration distinguishes installation types (Database, Forms, Java, Batch, etc.).

Patch inventory tracks the patches applied to an environment.

These enhancements make installing and updating Oracle Retail product installations easier and reduce opportunities for mistakes. Some of these changes add additional considerations to patching and maintaining Oracle Retail product environments. Additional details on these considerations are found in later sections.

Supported Products and Technologies

With version 15.0, several products and technologies are supported by the enhanced patching process. The utilities, processes and procedures described here are supported with the following products and listed technologies:

Product	Supported Technology
Oracle Retail Merchandising System (RMS)	<ul style="list-style-type: none"> ▪ Database scripts ▪ Batch scripts ▪ RETL scripts ▪ Data Conversion Scripts ▪ Forms ▪ BI Publisher Reports
Oracle Retail Warehouse Management System (RWMS)	<ul style="list-style-type: none"> ▪ Database scripts ▪ Batch scripts ▪ Forms ▪ BI Publisher Reports

Product	Supported Technology
Oracle Retail Price Management (RPM)	<ul style="list-style-type: none"> Database scripts (included with RMS) Java Application Batch scripts
Oracle Retail Invoice Matching (ReIM)	<ul style="list-style-type: none"> Database scripts (included with RMS) Java Application Batch scripts
Oracle Retail Allocation	<ul style="list-style-type: none"> Database scripts (included with RMS) Java Application Batch scripts
Oracle Retail Sales Audit (ReSA)	<ul style="list-style-type: none"> Database scripts (included with RMS) Java Application
Oracle Retail Insights (RI) Previously called Oracle Retail Analytics (RA)	<ul style="list-style-type: none"> Database scripts
Oracle Retail Advanced Science Engine (ORASE)	<ul style="list-style-type: none"> Database scripts Batch scripts
Oracle Retail Data Extractor (RDE)	<ul style="list-style-type: none"> Database scripts
Oracle Retail Application Admin Console (ORAAC). Previously called Oracle Retail Application Security Role Manager (RASRM)	<ul style="list-style-type: none"> Java Application

Patch Concepts

During the lifecycle of an Oracle Retail environment, patches are applied to maintain your system. This maintenance may be necessary to resolve a specific issue, add new functionality, update to the latest patch level, add support for new technologies, or other reasons.

A patch refers to a collection of files to apply to an environment. Patches could be cumulative, such as the 15.0.3 release, or incremental, such as a hot fix for just a few modules. Patches may contain updates for some or all components of a product installation including database, application code, forms, and batch. In a distributed architecture the same patch may need to be applied to multiple systems in order to patch all of the components. For example, if a patch contains both database and application changes, the patch would need to be applied to both the database server and the application server.

The top-level directory for the installation of an Oracle Retail product is referred to as the RETAIL_HOME. Underneath RETAIL_HOME are all of the files related to that product installation, as well as configuration and metadata necessary for the Oracle Retail Patch Assistant to maintain those files. In some cases the runtime application files also exist under RETAIL_HOME. For example, the compiled RMS forms, compiled RMS batch files, or Java Application batch scripts.

Patching Utility Overview

Patches are applied and tracked using utilities that are specifically designed for this purpose. The primary utility is described briefly below and additional information is available in later sections.

Oracle Retail Patch Assistant (ORPatch)

ORPatch is the utility used to apply patches to an Oracle Retail product installation. It is used in the background by the installer when creating a new installation or applying a cumulative patch. It is used directly to apply an incremental patch to an environment.

Oracle Retail Merge Patch (ORMerge)

ORMerge is a utility to allow multiple patches to be combined into a single patch. Applying patches individually may require some steps to be repeated. Merging multiple patches together allows these steps to be run only once. For example, applying several incremental patches to database packages will recompile invalid objects with each patch. Merging the patches into a single patch before applying them will allow invalid objects to be recompiled only once.

Oracle Retail Compile Patch (ORCompile)

ORCompile is a utility to compile components of Oracle Retail products outside of a patch. It allows RMS Forms, RMS Batch, and RWMS Forms to be fully recompiled even if no patch has been applied. It also contains functionality to recompile invalid database objects in product schemas.

Oracle Retail Deploy Patch (ORDeploy)

ORDeploy is a utility to deploy components of Oracle Retail Java products outside of a patch. It allows RPM, ReIM, Allocation and ReSA java applications to be redeployed to WebLogic even if a patch has not been applied. It contains functionality to optionally include or not include Java customizations when redeploying.

Changes with 15.0

Some products and technologies are supported by the enhanced patching process for the first time in 15.0. In those cases all of the content in this chapter is new with 15.0.

Renamed Products

For the 15.0 release several products using Orpatch have been renamed. Oracle Retail Analytics (RA) is renamed to Oracle Retail Insights (RI) and Oracle Retail Application Security Role Manager (RASRM) is renamed to Oracle Retail Application Admin Console (ORAAC). The old product names are still used in the underlying Orpatch code, the Orpatch Action names, the Orpatch env_info.cfg, and the Orpatch wallet paths. Documentation for these products will refer to the new names.

Patching Considerations

Patch Types

Oracle Retail produces two types of patches for their products: cumulative and incremental.

Cumulative Patches

A cumulative patch includes all of the files necessary to patch an environment to a specific level or build a new environment at that level. Examples of cumulative patches would be 15.0.1, 15.0.2, and so on. Cumulative patches come with a standard Oracle Retail installer and so can be applied to an environment with the installer rather than with ORPatch or other utilities.

Incremental Patches

An incremental patch includes only selected files necessary to address a specific issue or add a feature. Examples of incremental patches would be a hot fix for a specific defect. Incremental patches do not include an installer and must be applied with ORPatch.

Incremental Patch Structure

An Oracle Retail incremental patch generally contains several files and one or more subdirectories. The subdirectories contain the contents of the patch, while the individual files contain information about the patch and metadata necessary for patching utilities to correctly apply the patch. The most important files in the top-level directory are the README.txt, the manifest files.

README File

The README.txt file contains information about the incremental patch and how to apply it. This may include manual steps that are necessary before, after or while applying the patch. It will also contain instructions on applying the patch with ORPatch.

Manifest Files

Each patch contains manifest files which contain metadata about the contents of a patch and are used by ORPatch to determine the actions necessary to apply a patch. Patches should generally be run against all installations a product in an environment, and ORPatch will only apply the changes from the patch that are relevant to that installation.

Note: Cumulative patches use a different patch structure because they include a full installer which will run ORPatch automatically.

Version Tracking

The patching infrastructure for 15.0 tracks version information for all files involved with a product installation. The RETAIL_HOME contains files which track the revision of all files within the RETAIL_HOME including batch, forms, database, Java archives and other files. In addition, records of database scripts that have been applied to the product database objects are kept within each database schema.

Apply all Patches with Installer or ORPatch

In order to ensure that environment metadata is accurate all patches must be applied to the Oracle Retail product installation using patching utilities. For cumulative patches this is done automatically by the installer. For incremental patches ORPatch must be used directly. This is especially important if database changes are being applied, in order to ensure that the database-related metadata is kept up-to-date.

Environment Configuration

A configuration file in \$RETAIL_HOME/orpatch/config/env_info.cfg is used to define the details of a specific Oracle Retail environment. This file defines:

The location of critical infrastructure components such as the ORACLE_HOME on a database or middleware server.

The location of Oracle Wallets to support connecting to the database users.

The type of file processing which is relevant to a particular host. For example, if this is a host where database work should be done, or a host where batch compilation should be done, a host where Java applications should be deployed, etc. This allows a single database, forms and batch patch to be run against all types of hosts, applying only the relevant pieces on each server.

Other configuration necessary to determine proper behavior in an environment.

Retained Installation Files

The RETAIL_HOME location of an Oracle Retail product installation contains all of the files associated with that installation. This can include database scripts, Java files, Forms, Batch, RETL and Data Conversion files as with previous versions and also includes all database scripts. This allows objects to be reloaded during patching, including any necessary dependencies.

Reloading Content

In order to ensure that database contents and generated files exactly match patched versions, when applying cumulative patches some content is regenerated even if it does not appear to have changed.

On a cumulative patch this includes:

All re-runnable database content will be reloaded

- Packages and Procedures
- Database Types (excluding RIB objects)
- Control scripts
- Triggers
- Webservice jars and packages
- Form Elements

All RMS and RWMS forms files will be recompiled

All RMS batch files will be recompiled

When applying incremental patches, only changed files will be reloaded. However this does not apply to RMS batch, which is fully recompiled with any change.

Java Hotfixes and Cumulative Patches

When applying cumulative patches to Java applications components with ORPatch, all hotfixes related to base product ear files included with the patch will be rolled back. This increases the likelihood of a successful deployment because hotfixes may not be compatible with updated product ear files, or may already be included with the ear. Before applying a cumulative patch to Java applications, check the patch documentation to determine which hotfixes are not included in the ear. Then work with Oracle Support to obtain compatible versions of the fixes for the updated ear version. In some cases this may be the same hotfix, in which case it can be re-applied to the environment. In other cases a new hotfix may be required.

Backups

Before applying a patch to an environment, it is extremely important to take a full backup of both the RETAIL_HOME file system and the Oracle Retail database. Although ORPatch makes backups of files modified during patching, any database changes cannot be reversed. If a patch fails which contains database changes, and cannot be completed, the environment must be restored from backup.

Disk Space

When patches are applied to an environment, the old version of files which are updated or deleted are backed up to \$RETAIL_HOME/backups/backup-`<timestamp>`. When applying large patches, ensure there is sufficient disk space on the system where you unzip the patch or the patching process may fail. Up to twice as much disk space as the unzipped patch may be required during patching.

In addition to backups of source files, the existing compiled RMS or RWMS Forms and RMS Batch files are saved before recompilation. These backups may be created during patches:

Batch 'lib' directory in \$RETAIL_HOME/oracle/lib/bin-`<timestamp>`

Batch 'proc' directory in \$RETAIL_HOME/oracle/proc/bin-`<timestamp>`

Forms 'toolset' directory in \$RETAIL_HOME/base/toolset/bin-`<timestamp>`

Forms 'forms' directory in \$RETAIL_HOME/base/forms/bin-`<timestamp>`

Periodically both types of backup files can be removed to preserve disk space.

Patching Operations

Running ORPatch

ORPatch is used to apply patches to an Oracle Retail product installation. When applying a patch which includes an installer, ORPatch does not need to be executed manually as the installer will run it automatically as part of the installation process. When applying a patch that does not include an installer, ORPatch is run directly.

ORPatch performs the tasks necessary to apply the patch:

- Inspects the patch metadata to determine the patch contents and patch type.

- Reads the environment configuration file to determine which product components exist in this installation.

- Assembles a list of patch actions which will be run on this host to process the patch.

- Executes pre-checks to validate that all patch actions have the necessary configuration to proceed.

- Compares version numbers of files from the patch against the files in the environment.

- Backs up files which will be updated.

- Copies updated files into the installation.

- Loads updated files into database schemas, if applicable.

- Recompiles RMS batch, if applicable.

- Recompiles RMS forms, if applicable.

- Recompiles RWMS forms, if applicable.

- Constructs updated Java archives and deploys them to WebLogic, if applicable

- Updates Java batch files and libraries, if applicable

- Records the patch in the patch inventory.

If a patch does not contain updated files for the database or system, no action may be taken. If a previously failed ORPatch session is discovered, it will be restarted.

Preparing for Patching

Before applying a patch to your system, it is important to properly prepare the environment.

Single Patching Session

It is extremely important that only a single ORPatch session is active against a product installation at a time. If multiple patches need to be applied, you can optionally merge them into a single patch and apply one patch to the environment. Never apply multiple patches at the same time.

Shutdown Applications

If a patch updates database objects, it is important that all applications are shutdown to ensure no database objects are locked or in use. This is especially important when applying changes to Oracle Retail Integration Bus (RIB) objects as types in use will not be correctly replaced, leading to "ORA-21700: object does not exist or marked for delete" errors when restarting the RIB.

Backup Environment

Before applying a patch to an environment, it is important to take a full backup of both the RETAIL_HOME file system and the retail database. Although ORPatch makes backups of files modified during patching, any database changes cannot be reversed. If a patch which contains database changes fails and cannot be completed, the environment must be restored from backup.

Log Files

When applying a patch, ORPatch will create a number of log files which contain important information about the actions taken during a patch and may contain more information in the event of problems. Log files are created in the \$RETAIL_HOME/orpatch/logs directory. Logs should always be reviewed after a patch is applied.

After a patch session the log directory will contain at a minimum an ORPatch log file and may also contain other logs depending on the actions taken. The following table describes logs that may exist.

Log File	Used For
orpatch-<date>-<time>.log	Primary ORPatch log file
detail_logs/dbsql_<component>/invalids/*	Details on the errors causing a database object to be invalid
detail_logs/analyze/details	Detail logs of files that will be created/updated/removed when a patch is applied
detail_logs/compare/details	Detail logs of the differences between two sets of environment metadata
orpatch_forms_<pid>_child_<num>.log	Temporary logs from a child process spawned to compile forms in parallel. After the child process completes, the contents are append to the primary orpatch log file
detail_logs/forms/rms_frm_toolset/*	Detail logs of the compilation of each RMS Toolset file
detail_logs/forms/rms_frm_forms/*	Detail logs of the compilation of each RMS Forms file
detail_logs/rmsbatch/lib/*	Detail logs of the compilation of RMS Batch libraries
detail_logs/rmsbatch/proc/*	Detail logs of the compilation of RMS Batch programs
detail_logs/dbsql_rms/rms_db_ws_consumer_jars/*	Detail logs of the loadjava command to install RMS WebService Consumer objects
detail_logs/dbsql_rms/rms_db_ws_consumer_libs/*	Detail logs of the loadjava command to install RMS WebService Consumer libraries

Log File	Used For
detail_logs/forms/rwms_frm_forms/*	Detail logs of the compilation of each RWMS Forms file
detail_logs/dbsql_rwms/rwms_db_sp_jars/*	Detail logs of the loadjava command to install RWMS SP jars
detail_logs/javaapp_<product>/deploy/*	Detail logs of the deploy of a Java product

Unzip Patch Files

Before executing ORPatch, the patch files must be unzipped into a directory. This directory will be passed to ORPatch as the “-s <source directory>” argument on the command-line when applying or analyzing a patch.

Location of ORPatch

The ORPatch script will be located in \$RETAIL_HOME/orpatch/bin.

Command Line Arguments

ORPatch behavior is controlled by several command-line arguments. These arguments may be actions or options. Command and option names can be specified in upper or lower case, and will be converted to upper-case automatically. Arguments to options, for example the source directory patch, will not be modified.

ORPatch command-line actions:

Action	Description
apply	Tells ORPatch to apply a patch, requires the -s option Example: orpatch apply -s \$RETAIL_HOME/stage/patch123456
analyze	Tells ORPatch to analyze a patch, requires the -s option Example: orpatch analyze -s \$RETAIL_HOME/stage/patch123456
lsinventory	Tells ORPatch to list the inventory of patches that have been applied to this installation
exportmetadata	Tells ORPatch to extract all metadata information from the environment and create a \$RETAIL_HOME/support directory to contain it. Requires the -expname option.
diffmetadata	Tells ORPatch to compare all metadata from the current environment with metadata exported from some other environment. Requires the -expname and -srcname options.
revert	Tells ORPatch to revert the files related to a patch, requires the -s option Example: orpatch revert -s \$RETAIL_HOME/backups/backup-09302013-153010

Note: An action is required and only one action can be specified at a time.

ORPatch command-line arguments:

Argument	Valid For Actions	Description
-s <source dir>	apply analyze	Specifies where to find the top-level directory of the patch to apply or analyze. The source directory should contain the manifest.csv and patch_info.cfg files.
-new	apply	Forces ORPatch to not attempt to restart a failed ORPatch session
-expname	exportmetadata diffmetadata lsinventory	Defines the top-level name to be used for the export or comparison of environment metadata. When used with lsinventory, it allows an exported inventory to be printed.
-srcname	diffmetadata	Defines the 'name' to use when referring to the current environment during metadata comparisons.
-dbmodules	diffmetadata	When comparing metadata at a module-level, compare the dbmanifest information rather than the environment manifest. This method of comparing metadata is less accurate as it does not include non-database files.
-jarmodules	analyze diffmetadata	When used with analyze, requests a full comparison of the metadata of Java archives included in the patch versus the metadata of the Java archives in the environment. This behavior is automatically enabled when Java customizations are detected in the environment. Analyzing the contents of Java archives allows for detailed investigation of the potential impacts of installing a new Java ear to an environment with customizations. When used with diffmetadata, causes metadata to be compared using jarmanifest information rather than the environment manifest. This provides more detailed information on the exact differences of the content of Java archives, but does not include non-Java files.
-selfonly	apply analyze	Only apply or analyze changes in a patch that relate to orpatch itself. This is useful for applying updates to orpatch without applying the entire patch to an environment.
-s <backup dir>	revert	Specifies the backup from a patch that should be reverted to the environment. This restores only the files modified during the patch, the database must be restored separately or the environment will be out-of-sync and likely unusable.

Analyzing the Impact of a Patch

In some cases, it may be desirable to see a list of the files that will be updated by a patch, particularly if files in the environment have been customized. ORPatch has an 'analyze' mode that will evaluate all files in the patch against the environment and report on the files that will be updated based on the patch.

To run ORPatch in analyze mode, include 'analyze' on the command line. It performs the following actions:

Identifies files in the environment which the patch would remove.

Compares version numbers of files in the patch to version numbers of files in the environment.

Prints a summary of the number of files which would be created, updated or removed.

Prints an additional list of any files that would be updated which are registered as being customized.

Prints an additional list of any files which are in the environment and newer than the files included in the patch. These files are considered possible conflicts as the modules in the patch may not be compatible with the newer versions already installed. If you choose to apply the patch the newer versions of modules in the environment will NOT be overwritten.

If a Java custom file tree is detected, prints a detailed analysis of the modules within Java ear files that differ from the current ear file on the system.

Saves details of the files that will be impacted in
\$RETAIL_HOME/orpatch/logs/detail_logs/analyze/details.

This list of files can then be used to assess the impact of a patch on your environment.

To analyze a patch, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.
3. Set the PATH environment variable to include the orpatch/bin directory
4. Set the JAVA_HOME environment variable if the patch contains Java application files.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```

```
export JAVA_HOME=/u00/oretail/java_jdk
```

Note: If the JAVA_HOME environment variable is not specified, the value from
\$RETAIL_HOME/orpatch/config/env_info.cfg will be used.

5. Create a staging directory to contain the patch, if it does not already exist.
6. Download the patch to the staging directory and unzip it.
7. Execute orpatch to analyze the patch.
8. Repeat the patch analysis on all servers with installations for this product environment.
9. Evaluate the list(s) of impacted files.

```
mkdir -p $RETAIL_HOME/stage
```

```
orphatch analyze -s $RETAIL_HOME/stage/patch123456
```

For more information on registering and analyzing customizations, please see the Customization section later in this document.

Applying a Patch

Once the system is prepared for patching, ORPatch can be executed to apply the patch to the environment. The patch may need to be applied to multiple systems if it updates components that are installed on distributed servers.

To apply a patch, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```

3. Set the PATH environment variable to include the orpatch/bin directory
4. Set the DISPLAY environment variable if the patch contains Forms.

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```

```
export DISPLAY=localhost:10.0
```

Note: If the DISPLAY environment variable is not specified, the value from RETAIL_HOME/orpatch/config/env_info.cfg will be used.

5. Set the JAVA_HOME environment variable if the patch contains Java application files.

```
export JAVA_HOME=/u00/oretail/java_jdk
```

Note: If the JAVA_HOME environment variable is not specified, the value from RETAIL_HOME/orpatch/config/env_info.cfg will be used.

6. Create a staging directory to contain the patch, if it does not already exist.
7. Download the patch to the staging directory and unzip it.
8. Review the README.txt included with the patch. If manual steps are specified in the patch, execute those steps at the appropriate time.
9. Shutdown applications.
10. Execute ORPatch to apply the patch.
11. After ORPatch completes, review the log files in \$RETAIL_HOME/orpatch/logs.
12. Repeat the patch application on all servers with installations for this product environment.
13. Restart applications.

```
mkdir -p $RETAIL_HOME/stage
```

```
orpatch apply -s $RETAIL_HOME/stage/patch123456
```

Restarting ORPatch

If ORPatch is interrupted while applying a patch, or exits with an error, it saves a record of completed work in a restart state file in \$RETAIL_HOME/orpatch/logs. Investigate and resolve the problem that caused the failure, then restart ORPatch.

By default when ORPatch is started again, it will restart the patch process close to where it left off. If the patch process should **not** be restarted, add '-new' to the command-line of ORPatch.

Please note that starting a new patch session without completing the prior patch may have serious impacts that result in a patch not being applied correctly. For example, if a patch contains database updates and batch file changes and ORPatch is aborted during the load of database objects, abandoning the patch session will leave batch without the latest changes compiled in the installation.

Listing the Patch Inventory

After a patch is successfully applied by ORPatch the patch inventory in \$RETAIL_HOME/orpatch/inventory is updated with a record that the patch was applied. This inventory contains a record of the patches applied, the dates they were applied, the patch type and products impacted.

To list the patch inventory, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```

3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```

4. Execute orpatch to list the inventory.

```
orpatch lsinventory
```

Exporting Environment Metadata

ORPatch functionality is driven based on additional metadata that is stored in the environment to define what version of files are applied to the environment, and which database scripts have been applied to database schemas. This environment metadata is used to analyze the impact of patches to environments and controls what actions are taken during a patch. The metadata is stored in several locations depending on the type of information it tracks and in some cases it may be desirable to extract the metadata for analysis outside of ORPatch. For example, Oracle Support could ask for the metadata to be uploaded to assist them in triaging an application problem.

ORPatch provides a capability to export all of the metadata in an environment into a single directory and to automatically create a zip file of that content for upload or transfer to another system. The exact metadata collected from the environment depends on the products installed in the RETAIL_HOME.

ORPatch metadata exported:

Installed Product Component	Exported Metadata	Description
Any	orpatch/config/env_info.cfg orpatch/config/custom_hooks.cfg ORPatch inventory files	ORPatch configuration and settings
Any	All env_manifest.csv and deleted_env_manifest.csv files	Environment manifest files detailing product files installed, versions, customized flags and which patch provided the file
Database Schemas	DBMANIFEST table contents	Database manifest information detailing which database scripts were run, what version and when they were executed
Java Applications	All files from javaapp_<product>/config except jar files	Environment-specific product configuration files generated during installation

Installed Product Component	Exported Metadata	Description
Java Applications	Combined export of all META-INF/env_manifest.csv files from all product ear files	Jar manifest information detailing files, versions, customized flags and which patch provided the file
Java Applications	orpatch/config/javaapp_<product>/ant.deploy.properties	Environment properties file created during product installation and used during application deployment
Java Applications	<weblogic_home>/server/lib/weblogic.policy	WebLogic server java security manager policy file
RMS Batch	orpatch/config/rmsbatch_profile	Batch compilation shell profile
RMS Forms	orpatch/config/rmsforms_profile	Forms compilation shell profile
RWMS Forms	orpatch/cofngi/rwsnforms_profile	Forms compilation shell profile

Exports of environment metadata are always done to the \$RETAIL_HOME/support directory. When exporting metadata, you must specify the -exname argument and define the name that should be given to the export. The name is used for the directory within \$RETAIL_HOME/support and for the name of the zip file.

To extract an environment's metadata, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```
4. Execute orpatch to export the metadata.

```
orpatch exportmetadata -exname test_env
```

This example would export all metadata from the environment to the \$RETAIL_HOME/support/test_env directory. A zip file of the metadata would be created in \$RETAIL_HOME/support/test_env.zip.

Note: The \$RETAIL_HOME/support/<name> directory should be empty or not exist prior to running exportmetadata in order to ensure accurate results.

Comparing Environment Metadata

Once metadata has been exported from an environment, it can be used to compare the environment manifest metadata of two environments. ORPatch provides a capability to compare metadata of the current environment with the exported metadata of another environment. Note that even though there are many types of metadata exported by ORPatch, only environment manifest metadata is evaluated during comparisons. Metadata comparison happens in four phases: product comparison, patch comparison, ORPatch action comparison, and module-level comparison.

Product comparison compares the products installed in one environment with the products installed in another environment. Patch comparison compares the patches applied in one environment with the patches applied in another environment, for common products. This provides the most summarized view of how environments

differ. Patches which only apply to products on one environment are not included in the comparison.

Since each patch may impact many files, the comparison then moves on to more detailed analysis. The third phase of comparison is to compare the enabled ORPatch actions between environments. These actions roughly correspond to the installed 'components' of a product. For example, one environment may have database and forms components installed while another has only forms. Action comparison identifies components that are different between environments. The final phase of comparison is at the module level for actions that are common between environments. Modules which exist only on one environment, or exist on both environments with different revisions, or which are flagged as customized are reported during the comparison.

Differences between environment metadata are reported in a summarized fashion during the ORPatch execution. Details of the comparison results are saved in `$RETAIL_HOME/orphatch/logs/detail_logs/compare/details`. One CSV file is created for each phase of comparison: `product_details.csv`, `patch_details.csv`, `action_details.csv` and `module_details.csv`.

In order to be compared by ORPatch, exported metadata must be placed in the `$RETAIL_HOME/support` directory. The metadata should exist in the same structure that it was originally exported in. For example, if the metadata was exported to `$RETAIL_HOME/support/test_env` on another system, it should be placed in `$RETAIL_HOME/support/test_env` on this system.

When reporting differences between two environments, ORPatch uses names to refer to the environments. These names are defined as part of the `diffmetadata` command. The `-expname` parameter, which defines the directory containing the metadata, is also used as the name when referring to the exported metadata. The `-srcname` parameter defines the name to use when referring to the current environment. As an example, if you had exported the 'test' environment's metadata and copied it to the 'dev' environment's `$RETAIL_HOME/support/test_env` directory, you could run "`orphatch diffmetadata -expname test_env -srcname dev_env`". The detail and summary output would then refer to things that exist on dev but not test, revisions in the test environment versus revisions in the dev environment, etc.

ORPatch will automatically export the environment's current metadata to `$RETAIL_HOME/support/compare` prior to starting the metadata comparison.

To compare two environment's metadata, perform the following steps:

1. Export the metadata from another environment using `orphatch exportmetadata`.
2. Transfer the metadata zip from the other system to `$RETAIL_HOME/support`.
3. Log in as the UNIX user that owns the product installation.
4. Set the `RETAIL_HOME` environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/dev
```

5. Set the `PATH` environment variable to include the `orphatch/bin` directory

```
export PATH=$RETAIL_HOME/orphatch/bin:$PATH
```

6. Unzip the metadata zip file.

```
unzip test_env.zip
```

7. Execute `orphatch` to compare the metadata

```
orphatch diffmetadata -expname test_env -srcname dev_env
```

This example would compare the current environment against the metadata extracted in `$RETAIL_HOME/support/test_env` directory.

Note: The \$RETAIL_HOME/support/compare directory will be automatically removed before environment metadata is exported at the start of the comparison.

Reverting a Patch

In general it is best to either completely apply a patch, or restore the entire environment from the backup taken before starting the patch. It is important to test patches in test or staging environments before applying to production. In the event of problems, Oracle Retail recommends restoring the environment from backup if a patch is not successful.

Note: Reverting patches in an integrated environment can be extremely complex and there is no fully automated way to revert all changes made by a patch. Restoring the environment from a backup is the recommended method to remove patches.

It is, however, possible to revert small patches using the backups taken by ORPatch during a patch. This will restore only the files modified, and it is still necessary to restore the database if any changes were made to it.

Note: Reverting a patch reverts only the files modified by the patch, and does not modify the database, or recompile forms or batch files after the change.

When multiple patches have been applied to an environment, reverting any patches other than the most recently applied patch is strongly discouraged as this will lead to incompatible or inconsistent versions of modules applied to the environment. If multiple patches are going to be applied sequentially it is recommended to first merge the patches into a single patch that can be applied or reverted in a single operation.

To revert a patch, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.
`export RETAIL_HOME=/u00/oretail/15.0/tst`
3. Set the PATH environment variable to include the orpatch/bin directory
`export PATH=$RETAIL_HOME/orpatch/bin:$PATH`
4. Identify the backup directory in \$RETAIL_HOME/backups that contains the backup from the patch you want to restore.
 - The backup directory will contain a patch_info.cfg file which contains the name of the patch the backup is from.
 - It is possible to have two directories for the same patch, if ORPatch was updated during the patch. It is not possible to revert the updates to ORPatch. Select the backup directory that does not contain orpatch files.
 - If it is not clear which backup directory to use, restore the environment from backup
5. Execute orpatch to revert the environment using the contents of the backup directory
`orphatch revert -s $RETAIL_HOME/backups/backup-11232013-152059`
6. Restore the database from backup if the patch made database changes
7. Use the orcompile script to recompile forms if the patch included RMS or RWMS forms files

```
orcompile -a RMS -t FORMS
orcompile -a RWMS -t FORMS
```

8. Use the orcompile script to recompile batch if the patch included RMS batch files

```
orcompile -a RMS -t BATCH
```

9. Use the ordeploy script to redeploy the appropriate Java applications if the patch included Java files

```
ordeploy -a RPM -t JAVA
ordeploy -a REIM -t JAVA
ordeploy -a ALLOC -t JAVA
ordeploy -a RESA -t JAVA
```

Merging Patches

When patches are applied individually some ORPatch tasks such as compiling forms and batch files or deploying Java archives are performed separately for each patch. This can be time-consuming. An alternative is to use the ORMerge utility to combine several patches into a single patch, reducing application downtime by eliminating tasks that would otherwise be performed multiple times. Patches merged with ORMerge are applied with ORPatch after the merge patch is created.

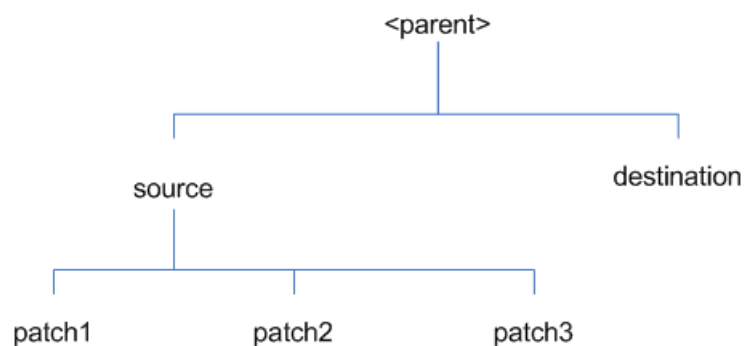
Source and Destination Directories

ORMerge uses source and destination areas in order to merge patch files. The source area is a single directory that contains the extracted patches to merge. The destination area is the location where the merged patch will be created. If a file exists in one or more source patches, only the highest revision will be copied to the merged patch.

The source and destination directories should exist under the same parent directory. That is, both the source and destination directories should be subdirectories of a single top-level directory.

The source directory must have all patches to be merged as immediate child directories. For example if three patches need to be merged the directory structure would look like this:

Source and Destination Directory Example



In the example above, the manifest.csv and patch_info.cfg files for each patch to be merged must exist in source/patch1, source/patch2, and source/patch3.

ORMerge Command-line Arguments

Argument	Required	Description
-s	Yes	Path to source directory containing patches to merge
-d	Yes	Path to destination directory that will contain merged patch
-name	No	The name to give the merged patch. If not specified, a name will be generated. When the merged patch is applied to a system, this name will appear in the Oracle Retail patch inventory.
-inplace	No	Used only when applying a patch to installation files prior to the first installation. See "Patching prior to the first install" in the Troubleshooting section later, for more information.

Running the ORMerge Utility

To merge patches, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```
4. Create a staging directory to contain the patches.

```
mkdir -p $RETAIL_HOME/stage/merge/src
```
5. Download the patches to the staging directory and unzip them so that each patch is in a separate subdirectory.
6. Review the README.txt included with each patch to identify additional manual steps that may be required. If manual steps are specified in any patch, execute them at the appropriate time when applying the merged patch.
7. Create a destination directory to contain the merged patches.

```
mkdir -p $RETAIL_HOME/stage/merge/dest
```
8. Execute ORMerge to merge the patches.

```
ormerge -s $RETAIL_HOME/stage/merge/src -d $RETAIL_HOME/stage/merge/dest -name merged_patch
```

The merged patch can now be applied as a single patch to the product installation using ORPatch.

Compiling Application Components

In some cases it may be desirable to recompile RMS Forms, RWMS Forms or RMS Batch outside of a product patch. The ORCompile utility is designed to make this easy and remove the need to manually execute 'make' or 'frmcmp' commands which can be error-prone. ORCompile leverages ORPatch functions to ensure that it compiles forms and batch exactly the same way as ORPatch. In addition ORCompile offers an option to compile invalid database objects using ORPatch logic.

ORCompile takes two required command line arguments each of which take an option. Arguments and options can be specified in upper or lower case.

ORCompile Command Line Arguments

Argument	Description
-a <app>	The application to compile.
-t <type>	The type of application objects to compile

ORCompile Argument Options

Application	Type	Description
RMS	BATCH	Compile RMS Batch programs
RMS	FORMS	Compile RMS Forms
RWMS	FORMS	Compile RWMS Forms
RMS	DB	Compile invalid database objects in the primary RMS schema
RMS	DB-ASYNC	Compile invalid database objects in the RMS_ASYNC_USER schema
ALLOC	DB-ALC	Compile invalid database objects in the Allocations user schema
ALLOC	DB-RMS	Compile invalid database objects in the RMS schema
REIM	DB	Compile invalid database objects in the RMS schema
RME	DB	Compile invalid database objects in the RME schema
ASO	DB	Compile invalid database objects in the ASO schema
RI	DB-DM	Compile invalid database objects in the RI DM schema
RI	DB-RIBATCH	Compile invalid database objects in the RI batch schema
RI	DB-RMSBATCH	Compile invalid database objects in the RI RMS batch schema
RI	DB-FEDM	Compile invalid database objects in the RI front-end schema
RDE	DB-DM	Compile invalid database objects in the RDE DM schema
RDE	DB-RDEBATCH	Compile invalid database objects in the RDE batch schema
RDE	DB-RMSBATCH	Compile invalid database objects in the RDE RMS batch schema

Note: Compiling RMS type DB, ReIM type DB, and Allocation type DB-RMS, are all identical as they attempt to compile all invalid objects residing in the RMS schema.

Running the ORCompile utility

To compile files, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orphatch/bin:$PATH
```

4. Execute orcompile to compile the desired type of files.

```
orcompile -a <app> -t <type>
```

ORCompile Examples

Compile RMS Batch.

```
orcompile -a RMS -t BATCH
```

Compile RWMS Forms.

```
orcompile -a RWMS -t FORMS
```

Compile invalid objects in the RA DM schema.

```
orcompile -a RI -t DB-DM
```

Compile invalid objects in the RMS owning schema.

```
orcompile -a RMS -t DB
```

Deploying Application Components

In some cases it may be desirable to redeploy Java applications outside of a product patch. For example, when troubleshooting a problem, or verifying the operation of the application with different WebLogic settings. Another situation might include wanting to deploy the application using the same settings, but without customizations to isolate behavior that could be related to customized functionality.

The ordeploy utility is designed to make this easy and remove the need to re-execute the entire product installer when no configuration needs to change. ORDeploy leverages Oracle Retail Patch Assistant functions to ensure that it deploys applications exactly the same way as ORPatch. In addition ORDeploy offers an option to include or not include custom Java files, to ease troubleshooting.

ORDeploy takes two required command line arguments each of which take an option. Arguments and options can be specified in upper or lower case.

ORDeploy Command Line Arguments

Argument	Description
-a <app>	The application to deploy.
-t <type>	The type of application objects to deploy

ORDeploy Argument Options

Application	Type	Description
ALLOC	JAVA	Deploy the Allocations Java application and Java batch files, including any custom Java files.
ALLOC	JAVANOCUSTOM	Deploy the Allocations Java application and Java batch files, NOT including any custom Java files.
REIM	JAVA	Deploy the REIM Java application and Java batch files, including any custom Java files.
REIM	JAVANOCUSTOM	Deploy the REIM Java application and Java batch files, NOT including any custom Java files.

Application	Type	Description
RESA	JAVA	Deploy the RESA Java application, including any custom Java files.
RESA	JAVANOCUSTOM	Deploy the RESA Java application, NOT including any custom Java files.
RPM	JAVA	Deploy the RPM Java application and Java batch files, including any custom Java files.
RPM	JAVANOCUSTOM	Deploy the RPM Java application and Java batch files, NOT including any custom Java files.

Running the ORDeploy utility

To deploy Java applications, perform the following steps:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orphatch/bin:$PATH
```
4. Execute ORDeploy to deploy the desired Java application.

```
ordeploy -a <app> -t <type>
```

ORDeploy Examples

Deploy RPM.

```
ordeploy -a RPM -t JAVA
```

Deploy ReIM without including Java customizations.

```
ordeploy -a REIM -t JAVANOCUSTOM
```

Maintenance Considerations

The additional information stored within the RETAIL_HOME and within database schemas adds some considerations when performing maintenance on your environment.

Database Password Changes

Oracle wallets are used to protect the password credentials for connecting to database schemas. This includes all database schemas used during an install. If the password for any of these users is changed the wallet's entry must be updated.

The wallet location is configurable but by default is in the following locations:

Location	Installation Type
\$RETAIL_HOME/orphatch/rms_wallet	RMS Database RMS Batch
\$RETAIL_HOME/orphatch/rms_wallet_app	RMS Forms
\$RETAIL_HOME/orphatch/rwms_wallet	RWMS Database
\$RETAIL_HOME/orphatch/rwms_wallet_app	RWMS Forms
\$RETAIL_HOME/orphatch/oraso_wallet	ASO Database

Location	Installation Type
\$RETAIL_HOME/orpatch/orme_wallet	RME Database
\$RETAIL_HOME/orpatch/ra_wallet	RI (Previously RA) Database
\$RETAIL_HOME/orpatch/rde_wallet	RDE Database

The wallet alias for each schema will be <username>_<dbname>. Standard mkstore commands can be used to update the password.

For example:

```
mkstore -wrl $RETAIL_HOME/orpatch/rms_wallet -modifyCredential rms_rmsdb rms01
rmspassword
```

This command will update the password for the RMS01 user to 'rmspassword' in the alias 'rms_rmsdb'.

The Oracle wallets are required to be present when executing ORPatch. Removing them will prevent you from being able to run ORPatch successfully. In addition the Oracle wallet location is referenced in the RMS batch.profile, and in the default RMS and RWMS Forms URL configuration, so removing them will require reconfiguration of batch and forms. If batch and forms were reconfigured after installation to use other wallet files, it is possible to backup and remove the wallets, then restore them when running ORPatch.

WebLogic Password Changes

Java wallets are used to protect the password credentials used when deploying Java products. This includes the WebLogic administrator credentials, LDAP connection credentials, batch user credentials and any other credentials used during an install. If the password for any of these users is changed the wallet's entry must be updated, or the Java product installation can be run again.

The wallet location is in the following locations:

Location	Installation Type
\$RETAIL_HOME/orpatch/config/javapp_rpm	RPM Java
\$RETAIL_HOME/orpatch/config/javapp_reim	ReIM Java
\$RETAIL_HOME/orpatch/config/javapp_alloc	Allocation Java
\$RETAIL_HOME/orpatch/config/javapp_resa	RESA Java
\$RETAIL_HOME/orpatch/config/javaapp_rasrm	ORAAC (Previously RASRM) Java

The wallet aliases will be stored in the retail_installer partition. The names of the aliases will vary depending on what was entered during initial product installation.

The dump_credentials.sh script can be used to list the aliases in the wallet.

For example:

```
cd $RETAIL_HOME/orpatch/deploy/retail-public-security-api/bin
./dump_credentials.sh $RETAIL_HOME/orpatch/config/javapp_alloc
```

```
Application level key partition name:retail_installer
```

```
User Name Alias:dsallocAlias User Name:rms0lapp
```

```
User Name Alias:BATCH-ALIAS User Name:<SYSTEM_ADMINISTRATOR>
```

```
User Name Alias:wlsAlias User Name:<weblogic>
```

The easiest way to update the credential information is to re-run the Java product installer. If you need to manually update the password for a credential, the `save_credential.sh` script can be used.

For example:

```
cd $RETAIL_HOME/orpatch/deploy/retail-public-security-api/bin
./save_credential.sh -l $RETAIL_HOME/orpatch/config/javapp_alloc -p
retail_installer -a wlsAlias -u weblogic
```

This command will prompt for the new password twice and update the alias `wlsAlias`, username `weblogic` with the new password.

Infrastructure Directory Changes

The `RETAIL_HOME/orpatch/config/env_info.cfg` file contains the path to the database `ORACLE_HOME` on database or RMS Batch installations, to the WebLogic Forms and Reports `ORACLE_HOME` and `ORACLE_INSTANCE` on RMS or RWMS Forms installations, and to the `WEBLOGIC_DOMAIN_HOME`, `WL_HOME` and `MW_HOME` on Java product installations. If these paths change, the related configuration variables in the `env_info.cfg` file must be updated.

DBManifest Table

The table `dbmanifest` within Oracle Retail database schemas is used to track the database scripts which have been applied to the schema. It is critical not to drop or truncate this table. Without it, `ORPatch` will attempt to re-run scripts against the database which have already been applied which can destroy a working environment. Similarly, if copying a schema from one database to another database, ensure that the `dbmanifest` table is preserved during the copy.

RETAIL_HOME relationship to Database and Application Server

The `RETAIL_HOME` associated with an Oracle Retail product installation is critical due to the additional metadata and historical information contained within it. If a database or application installation is moved or copied, the `RETAIL_HOME` related to it should be copied or moved at the same time.

Jar Signing Configuration Maintenance

The RPM product installation includes an option to configure a code signing certificate so that jar files modified during installation or patching are automatically re-signed. This configuration is optional, but recommended. If it is configured, the code signing keystore is copied during installation to `$RETAIL_HOME/orpatch/config/jarsign/orpkeystore.jks`. The keystore password and private key password are stored in a Java wallet in the `$RETAIL_HOME/orpatch/config/jarsign` directory. The credentials are stored in a wallet partition called `orpatch`:

Alias	Username	Description
storepass	discard	Password for the keystore
keypass	discard	Password for the private key

The keystore file and passwords can be updated using the product installer. This is the recommended way to update the signing configuration.

If only the credentials need to be updated, the `sign_jar.sh` script can be used.

5. Log in as the UNIX user that owns the product installation.
6. Set the `RETAIL_HOME` environment variable to the top-level directory of your installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
7. Change directories to the location of `sign_jar.sh`

```
cd $RETAIL_HOME/orpatch/deploy/bin
```
8. Execute `sign_jar.sh`

```
sign_jar.sh changepwd
```
9. When prompted, enter the new keystore password
10. When prompted, enter the new private key password

Customization

Patching Considerations with Customized Files and Objects

In general, the additional capabilities provided by the ORPatch should make it easier to evaluate the potential impacts of patches to your customizations of Oracle Retail products. However, the additional metadata maintained by the Oracle Retail patching utilities does add some considerations when making customizations.

General Guidelines

It is always preferred to customize applications by extension rather than by direct modification. For example, adding new database objects and forms rather than modifying existing Oracle Retail objects and forms. You can also leverage built-in extension points such as User Defined Attributes, the Custom Flexible Attribute Solution, or seeded customization points in ADF Applications.

It is strongly discouraged to directly modify Oracle Retail database objects, especially tables, as your changes may be lost during patching or may conflict with future updates. When adding or modifying database objects, Oracle Retail recommends that all objects be added with scripts to ensure that they can be rebuilt if necessary after a patch.

Custom Database Objects

When you create new database objects, Oracle Retail recommends placing them in an Oracle database schema specifically for your customizations. You must use synonyms and grants to allow the Oracle Retail product schema owner and other users to access your objects, and use synonyms and grants to allow your customizations to access Oracle Retail objects. A separate schema will ensure that your customizations are segregated from base Oracle Retail code.

ORPatch expects that there will be no invalid objects in the database schemas it manages after a patch is applied. For this reason adding extra objects to the product schema could result in failures to apply patches as changes to base objects may cause custom objects to go invalid until they are updated. In this situation, manually update the custom objects so that they compile, and restart the patch.

Custom Forms

When creating new custom forms, Oracle Retail recommends placing them in a separate directory specifically for your customizations. This directory should be added to the FORMS_PATH of your RMS or RWMS Forms URL configuration to allow the forms to be found by the Forms Server. This will ensure that your customizations are segregated from base Oracle Retail code. If you choose to place customizations in the Forms bin directory, then your custom forms will need to be recopied each time Forms are fully recompiled.

ADF Application Customization

Oracle Retail ADF-based applications such as Allocation and ReSA can be customized using a process called 'seeded customization'. The customization process involves using JDeveloper in Customizer mode to create changes to product configurations, and then building a MAR archive containing the changes. The generated MAR is deployed to the MDS repository used by the application and applied to the application at runtime. These types of customizations are handled outside of ORPatch and are not reported during patch analysis or tracked by the custom file registration utility. More information can be found in the respective product customization guides.

Custom Compiled Java Code

When customizing Oracle Retail Java-based products such as RPM and ReIM via product source code, ORPatch supports automatically adding compiled customizations into the application ear file prior to deployment. This allows customizations to be applied to the application without directly modifying the base product ear, enabling customizations and defect hotfixes to co-exist when they do not change the same file or a dependent file. See the later “Custom Compiled Java Code” section for additional information and considerations.

Analyze Patches when Customizations are Present

Whenever you have customized a product by directly modifying Oracle Retail files or database objects, it is important to ensure you analyze each the files that will be updated by a patch before applying the patch. This will allow you to identify any customized files which may be overwritten by the patch and either merge your customization with the new version of the file, or re-apply the customization after applying the patch.

Manifest Updates

If you choose to customize Oracle Retail files directly, it is extremely important **not** to update the revision number contained in the env_manifest.csv. This could cause future updates to the file to be skipped, invalidating later patch applications as only a partial patch would be applied. The customized revision number for modified files will need to be tracked separately.

Registering Customized Files

The ORPatch contains utilities and functionality to allow tracking of files that have been customized through direct modification. This process is referred to as ‘registering’ a customized file. Registration only works for files which are shipped by Oracle Retail. It is not possible to register new files created in the environment as part of extensions or customizations.

When patches are analyzed with ORPatch, special reporting is provided if any registered files would be updated or deleted by the patch. Customized files impacted by the patch are listed at the end of the analysis report from ORPatch. The detail files generated during the analyze will contain a column called ‘customized’ which will have a Y for any files which were registered as customized. This allows easier identification of customizations which will be overwritten by a patch.

All files delivered by Oracle Retail are considered ‘base’ and so when they are applied to an environment any registrations of those files as customized will revert back to un-customized. **Each time a patch overwrites customized files, you must re-register the files as customized once you have applied customizations.**

To register customized files, use the \$RETAIL_HOME/orpatch/bin/orcustomreg script.

The orcustomreg script operates in one of two modes: registration and list.

Registration mode registers or unregisters one or more files as customized.

List mode lists all files in the environment that are registered as customized.

Command Line Arguments for Registration Mode

Argument	Description
-f <file>	Adds <file> to the list of files that will be registered. Can be specified more than once.

Argument	Description
-bulk <file>	Specifies a file to read, containing one filename per line. All filenames listed inside <file> will be registered.
-register	Files specified with -f or -bulk will be registered as 'customized'
-unregister	Files specified with -f or -bulk will be registered as 'base'

Notes:

- At least one of -f or -bulk is required.
- If neither -register nor -unregister is specified, the default is '-register'.
- File names specified with -f must either be fully-qualified or be relative to RETAIL_HOME. The same is true for filenames specified within a -bulk file.

Command Line arguments for list mode

Argument	Description
-list	List all files in the environment registered as customized

Running the orcustomreg Script

Perform the following procedure to run the orcustomreg script:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```
3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orphatch/bin:$PATH
```
4. Execute orcustomreg script to register the desired file(s).

```
orcustomreg -register -f <file>
```

Examples of using the orcustomreg Script

Register \$RETAIL_HOME/dbsql_rms/Cross_Pillar/control_scripts/source/oga.sql as customized.

```
orcustomreg -f dbsql_rms/Cross_Pillar/control_scripts/source/oga.sql
```

Unregister customizations for

\$RETAIL_HOME/dbsql_rwms/Triggers/Source/TR_WAVE.trg

```
orcustomreg -unregister -f $RETAIL_HOME/dbsql_rwms/Triggers/Source/TR_WAVE.trg
```

Bulk register several files as customized.

```
echo "$RETAIL_HOME/oracle/proc/src/mrt.pc" > custom.txt
echo "$RETAIL_HOME/oracle/proc/src/saldly.pc" >> custom.txt
echo "$RETAIL_HOME/oracle/proc/src/ccprg.pc" >> custom.txt
orcustomreg -bulk custom.txt
```

List all files registered as customized.

```
orcustomreg -list
```

Custom Compiled Java Code

When customizing Oracle Retail Java-based products such as RPM and ReIM via product source code, ORPatch supports automatically adding compiled customizations into the application ear file prior to deployment. This allows customizations to be applied to the application without directly modifying the base product ear, enabling customizations and defect hotfixes to co-exist when they do not change the same file or a dependent file.

This functionality is enabled by creating a directory called `$RETAIL_HOME/javaapp_<app>/custom`, where `<app>` is the application the customizations apply to. Files stored within this directory will be combined with the base product ear files before the application is deployed to WebLogic. ORPatch will attempt to consider customizations stored within the 'custom' directory during patch analysis by triggering more detailed ear file change analysis to assist with identifying which customizations might be impacted by changes in the patches.

Note: It is not possible, nor necessary, to register compiled Java customizations with the `orcustomreg` tool.

As with other customization techniques for other technologies, Oracle Retail recommends making Java customizations in new files as much as possible, versus overwriting base product or configuration files. In the past it was necessary to build complete replacement product ear files, but this method of customization is no longer required nor recommended. Replacement ear and jar files will not contain the META-INF/env_manifest.csv files which are required in order to be able to apply incremental patches. Instead, compile the specific Java classes being customized and place them along with any custom configuration files in `$RETAIL_HOME/javaapp_<app>/custom`.

Building Deployable ear files

When constructing the product ear file to deploy to WebLogic, ORPatch applies changes to the ear file in a specific order, with files from later steps overwriting files in earlier steps. The resulting ear is stored in `$RETAIL_HOME/javaapp_<app>/deploy`, and then deployed to WebLogic.

Sequence for ORPatch Java Product ear file updates

Order	File Type	Location
1	Base product ear	<code>\$RETAIL_HOME/javaapp_<app>/base</code>
2	Updated configuration files	<code>\$RETAIL_HOME/javaapp_<app>/config</code>
3	Oracle Retail-supplied hotfixes	<code>\$RETAIL_HOME/javaapp_<app>/internal</code>
4	Compiled customizations	<code>\$RETAIL_HOME/javaapp_<app>/custom</code>

Merging Custom Files

When merging files from the custom directory with the product ear, ORPatch uses the directory path of the files within custom to calculate where the file should be stored within the ear. This allows arbitrary nesting of files, even when placing files within jars stored in jars, stored within the ear. The following examples below use RPM, but apply to adding compiled customizations to any Java-based product.

Custom directory location and product ear location Examples

File path within javaapp_<app>/custom/	Final Ear File Location
rpm.ear/company/ui/MyCustom.class	In rpm.ear: /company/ui/MyCustom.class
rpm.ear/rpm.jar/company/bc/MyCustom2.class	In rpm.ear: In rpm.jar: /company/bc/MyCustom2.class
rpm.ear/lib/ourcustomlibs.jar	In rpm.ear /lib/ourcustomlibs.jar
rpm.ear/WebLaunchServlet.war/lib/ rpm.jar/company/bc/MyCustom2.class	In rpm.ear: In WebLaunchServlet.war: In lib/rpm.jar: /company/bc/MyCustom2.class

Analyzing patches when customizations are present

When analyzing a patch which contains a base product ear and the custom directory contains files, ORPatch will automatically trigger a more detailed analysis of the changes coming in a patch. This includes calculating what files inside the product ear have been added, removed or updated and which files appear to be customized based on the contents of the 'custom' directory. The detailed results of the ear file comparison during patch analysis will be saved in javaapp_<app>_archive_compare_details.csv. Any custom files which appeared to be impacted by the patch are saved in javapp_<app>_archive_custom_impacts.csv. Both files will be in the \$RETAIL_HOME/orpatch/logs/detail_logs/analyze/details directory.

Note: This detailed analysis is not available when analyzing individual hotfixes, so special care must be taken when applying hotfixes to a customized product installation, to ensure there are no conflicts between customizations and hotfix changes.

Customizations and cumulative patches

By default, when applying a cumulative patch, ORPatch will not include customizations in the deployed product ear, even if they are present in the appropriate directory. This allows verification that the application is functioning properly using base code, before applying customizations. After verifying the initial deployment, use ORDeploy with the "-t JAVA" option to construct and deploy the product ear including customizations.

If customizations need to be removed outside of a patch, use ORDeploy with the "-t JAVANOCUSTOM" option to create and deploy an ear containing only Oracle Retail code. To force ORPatch to include customizations in the deployed ear even when applying a cumulative patch, set JAVAAPP_<app>_INCLUDE_CUSTOM=Y in the \$RETAIL_HOME/orpatch/config/env_info.cfg file.

Changing configuration files

It is possible to directly change product configuration files in \$RETAIL_HOME/javaapp_<app>/config. These updates can be deployed to the environment using the ORDeploy utility. However, the 'config' directory is completely

recreated each time the product installer is used. This means that modifications will be lost and must be manually reapplied after each installer run. It is recommended to make configuration changes via the installer where possible, and retain the `ant.install.properties` file for use in later installer sessions.

Extending Oracle Retail Patch Assistant with Custom Hooks

The default ORPatch actions and processing logic is sufficient to install and patch the base Oracle Retail product code. However there may be situations where custom processing is desired during patching activities such as executing a shell script prior to the start of patching, or running a SQL script at the end of the patch.

ORPatch supports extensions in the form of custom hooks. These hooks allow external scripts to be run at specific points during ORPatch processing.

ORPatch Processing

Action

ORPatch supports a variety of 'actions' which define the steps necessary to apply updates to a particular area of the Oracle Retail application. Each action is generally specific to updates to a single technology or logical component of the environment. For example, one action might handle making updates to the RMS database schema, while a separate action is responsible for compiling RWMS forms, and a different action deploys the RPM Java application. These actions are enabled and disabled within the environment configuration file, allowing ORPatch to determine what types of changes to apply to each product installation.

ORPatch Actions

Order	Action Name	Description
1	DBSQL_RMS	Loads RMS and RPM database objects into the primary RMS schema
2	DBSQL_RMSASYNC	Loads database objects into the RMS_ASYNC_USER schema
3	DBSQL_RAF	Loads Retail Application Framework database objects into the RMS schema
4	DBSQL_REIM	Loads ReIM database objects into the RMS schema
5	DBSQL_ALCRMS	Loads Allocation database objects into the RMS schema
6	DBSQL_ALLOC	Loads Allocation database objects into the Allocation user schema
7	DBSQL_RMSDEMO	Used to create demo data in the RMS schema if demo data was selected during initial installation
8	DBSQL_RMSDAS	Loads database objects into the RMS Data Access Schema
9	RMSBATCH	Compiles RMS Batch
10	ORAFORMS_RMS	Compiles RMS Forms, copies RMS reports to \$RETAIL_HOME
11	RMSRETLSCRIPTS	Copies Oracle Retail Extract and Load scripts for RMS
12	RMSDCSCRIPTS	Copies Oracle Retail Merchandising System data conversion scripts

Order	Action Name	Description
13	DBSQL_RWMS	Loads database objects into the primary RWMS schema
14	DBSQL_RWMSADF	Loads database objects into the RWMS ADF user schema
15	DBSQL_RWMSUSER	Loads database objects into the RWMS user schema
16	ORAFORMS_RWMS	Compiles RWMS Forms, copies RWMS batch scripts and reports to \$RETAIL_HOME
17	JAVAAPP_RPM	Deploys the RPM Java application and batch scripts
18	JAVAAPP_REIM	Deploys the REIM Java application and batch scripts
19	JAVAAPP_ALLOC	Deploys the Allocation Java application and batch scripts
20	JAVAAPP_RESA	Deploys the ReSA Java application
21	JAVAAPP_RASRM	Deploys the ORAAC (previously called RASRM) Java application
22	DBSQL_RARMSBATCH	Loads database objects into the RMS Batch schema for RI (previously called RA)
23	DBSQL_RADM	Loads database objects into the RI (previously called RA) Data Mart schema
24	DBSQL_RAFEDM	Loads database objects into the RI (previously called RA) Front-end schema
25	DBSQL_RABATCH	Loads database objects into the RI (previously called RA) Batch schema
26	DBSQL_RDERMSBATCH	Loads database objects into the RMS Batch schema for RDE
27	DBSQL_RDEDM	Loads database objects into the RDE Data Mart schema
28	DBSQL_RDEBATCH	Loads database objects into the RDE Batch schema
29	DBSQL_RASECORE	Loads core database objects into the ORASE schema
30	DBSQL_RASEASO	Loads ASO database objects into the ORASE schema
31	DBSQL_RASECDT	Loads CDT database objects into the ORASE schema
32	DBSQL_RASECIS	Loads CIS database objects into the ORASE schema
33	DBSQL_RASEDT	Loads DT database objects into the ORASE schema
34	DBSQL_RASEMBA	Loads MBA database objects into the ORASE schema
35	RASECOREBATCH	Copies ORASE core batch scripts and libraries
36	RASEASOBATCH	Copies ORASE ASO batch scripts and libraries
37	RASECDTBATCH	Copies ORASE CDT batch scripts and libraries
38	RASECISBATCH	Copies ORASE CIS batch scripts and libraries
39	RASEDTBATCH	Copies ORASE DT batch scripts and libraries
40	RASEMBABATCH	Copies ORASE MBA batch scripts and libraries

Phase

ORPatch processes patches in phases. Each action relevant to a patch and host is provided an opportunity to process the patch for each phase. The standard phases which allow hooks are:

Restart Phase Number	Phase Name	Description
N/A	PRECHECK	Actions verify that their configuration appears complete and correct. This phase and the associated hooks will be run every time orpatch is executed, even if processing will be restarted in a later phase.
10	PREACTION	Actions do processing prior to when files are copied to the environment. Files are deleted during this phase.
20	COPYPATCH	Actions copy files included in a patch into the destination environment and the environment manifest is updated.
30	PATCHACTION	Actions take the more detailed steps necessary to apply the new files to the environment. For database actions in particular, this is the phase when new and updated sql files are loaded into the database.
40	POSTACTION	Actions do processing after files have been copied and PatchActions are completed. The Forms actions, for example, use this phase to compile the forms files as this must happen after database packages are loaded.
50	CLEANUP	Actions do any additional processing. Currently no actions implement activities in this phase.

Configuring Custom Hooks

Custom hooks are configured in a configuration file `RETAIL_HOME/orpatch/config/custom_hooks.cfg`. The configuration file is a simple text file where blank lines and lines starting with `#` are ignored and all other lines should define a custom hook.

To define a custom hook, a line is added to the file in the form:

```
<hook name>=<fully qualified script>
```

The hook name must be in upper case and is in the form:

```
<action name>_<phase name>_<sequence>
```

The action name is any action name understood by ORPatch. The phase name is one of the five phase names from the table above. The sequence is either 'START' or 'END'. Hooks defined with a sequence of 'START' are run before the action's phase is invoked. Hooks defined with a sequence of 'END' are run after the action's phase is invoked.

Multiple scripts can be associated with a single hook by separating the script names with a comma. If a hook name appears in the configuration file multiple times only the last entry will be used.

The script defined as a custom hook must be an executable shell script that does not take any arguments or inputs. The only environment variable that is guaranteed to be passed to the custom hook is `RETAIL_HOME`. The script must return 0 on success and non-zero on failure.

If an action is a DBSQL action (i.e. has a name like `DBSQL_`), the custom hook can optionally be a .sql file. In this case the SQL script will be run against the database schema that the DBSQL action normally executes against. The SQL script must not

generate any ORA- or SP2- errors on success. In order to be treated as a database script, the extension of the file defined as the custom hook must be .sql in lower-case. Any other extension will be treated as if it is a shell script. If you have database scripts with different extensions, they must be renamed or wrapped in a .sql script.

When using the PRECHECK phase and START sequence, please note that the custom hook will be executed prior to any verification of the configuration. Invalid configuration, such as invalid database username/password or a non-existent ORACLE_HOME, may cause the custom hook to fail depending on the actions it tries to take. However in these cases, the normal orpatch PRECHECK activities would likely have failed as well. All that is lost is the additional context that orpatch would have provided about what was incorrect about the configuration.

Restarting with Custom Hooks

If a custom hook fails, for example a shell script hook returns non-zero or a sql script generates an ORA- error in its output, the custom hook will be treated as failing. A failing custom hook causes ORPatch to immediately stop the patching session.

When ORPatch is restarted it always restarts with the same phase and action, including any START sequence custom hooks. If the START sequence custom hook fails, the action's phase is never executed. With an END sequence custom hook, the action's phase is re-executed when ORPatch is restarted and then the custom hook is re-executed.

When an action's phase is costly, for example the DBSQL_RMS action which does a lot of work, this can mean a lot of duplicate processing.

For this reason it is preferred to use START sequence custom hooks whenever possible. If necessary, use a START sequence hook on a later phase or a later action, rather than an END sequence custom hook.

Patch-level Custom Hooks

In addition to action-specific hooks, there are two patch-level hook points available.

These hooks allow scripts to be run before any patching activities start and after all patching activities are completed. The hooks are defined in the same configuration file, with a special hook name.

To run a script before patching, define:

```
ORPATCH_PATCH_START=<fully qualified script>
```

To run a script after patching, define:

```
ORPATCH_PATCH_END=<fully qualified script>
```

These hooks only support executing shell scripts, database scripts must be wrapped in a shell script. It is also important to note that these hooks are run on every execution of ORPatch to apply a patch, even when restarting a patch application. If the START sequence patch-level hook returns a failure, patching is aborted. If the END sequence patch-level hook returns a failure, it is logged but ignored as all patching activities have already completed.

Please note that the ORPATCH_PATCH_START hook is executed prior to any verification of the configuration. Invalid configuration may cause the custom hook to fail depending on the actions it tries to take. However in these cases, the normal ORPatchactivities would likely fail as well.

Example Custom Hook Definitions

A shell script that is executed prior to the Pre-Action phase of RMS Batch:

```
RMSBATCH_PREACTION_START=/u00/oretail/prepare_custom_header.sh
```

A shell script that is executed after RETL script files are copied into the RETAIL_HOME:

```
RETLSCRIPTS_COPYPATCH_END=/u00/oretail/copy_custom_files.sh
```

A SQL script that is executed against the RWMS owning schema at the start of the Clean-up Phase:

```
DBSQL_RWMS_CLEANUP_START=/dba/sql/recompile_synonyms.sql
```

Troubleshooting Patching

There is not a general method for determining the cause of a patching failure. It is important to ensure that patches are thoroughly tested in a test or staging system several times prior to attempting to apply the patch to a production system, particularly if the patch is a large cumulative patch. After the test application is successful, apply the patch to the production system.

ORPatch Log Files

ORPatch records extensive information about the activities during a patch to the log files in `RETAIL_HOME/orphatch/logs`. This includes a summary of the actions that are planned for a patch, information about all files that were updated by the patch, and detailed information about subsequent processing of those files. The ORPatch log files also contain timestamps to assist in correlating log entries with other logs.

Even more detailed logs are available in `RETAIL_HOME/orphatch/logs/detail_logs` for some activities such as forms compilation, invalid database object errors, and output from custom hooks. If the standard ORPatch log information is not sufficient, it might be helpful to check the detailed log if it exists.

Restarting ORPatch

The restart mechanism in ORPatch is designed to be safe in nearly any situation. In some cases to ensure this, a portion of work may be redone. If the failure was caused by an intermittent issue that has been resolved, restarting ORPatch may be sufficient to allow the patch to proceed.

Manual DBManifest Updates

A possible cause for database change script failures is that a database change was already made manually to the database. In this event, you may need to update the dbmanifest table to record that a specific script does not need to be run. Before doing this, it is extremely important to ensure that all statements contained in the script have been completed.

Use the `$RETAIL_HOME/orphatch/bin/ordbmreg` script to register database scripts in the dbmanifest table.

Command Line Arguments for ordbmreg

Argument	Description
-f <file>	Adds <file> to the list of files that will be registered. Can be specified more than once.
-bulk <file>	Specifies a file to read, containing one filename per line. All filenames listed inside <file> will be registered.
-register	Files specified with -f or -bulk will be registered in the dbmanifest table
-unregister	Files specified with -f or -bulk will be removed from the dbmanifest table

Notes:

- At least one of -f or -bulk is required.
 - If neither -register nor -unregister is specified, the default is '-register'.
 - File names specified with -f must either be fully-qualified or be relative to RETAIL_HOME. The same is true for filenames specified within a -bulk file.
 - Registering a file in the dbmanifest table will cause it to be completely skipped. Before doing so, ensure that all commands contained in it have been completed.
 - Removing a file from the dbmanifest table will cause it to be run again. This will fail if the commands in the script cannot be re-run. For example if they create a table that already exists.
-

Running the ordbmreg Script

Perform the following procedure to run the ordbmreg script:

1. Log in as the UNIX user that owns the product installation.
2. Set the RETAIL_HOME environment variable to the top-level directory of your product installation.

```
export RETAIL_HOME=/u00/oretail/15.0/tst
```

3. Set the PATH environment variable to include the orpatch/bin directory

```
export PATH=$RETAIL_HOME/orpatch/bin:$PATH
```

4. Execute ordbmreg script to register the desired file(s).

```
ordbmreg -register -f <file>
```

Examples of using the ordbmreg Script

Register

\$RETAIL_HOME/dbsql_rms/Cross_Pillar/db_change_scripts/source/000593_system_options.sql with the dbmanifest table.

```
ordbmreg -f
dbsql_rms/Cross_Pillar/db_change_scripts/source/000593_system_options.sql
```

Remove the dbmanifest row for

\$RETAIL_HOME/dbsql_radm/ra_db/radm/database_change_scripts/000035_s12733240_w_party_per_d.sql.

```
ordbmreg -unregister -f
$RETAIL_HOME/dbsql_radm/ra_db/radm/database_change_scripts/000035_s12733240_w_party_per_d.sql
```

Bulk register several files in the dbmanifest table.

```
echo "$RETAIL_HOME/dbsql_rwms/DBC/Source/000294_container.sql" > dbcs.txt
echo "$RETAIL_HOME/dbsql_rwms/DBC/Source/000457_drop_object.sql" >> dbcs.txt
ordbmreg -bulk dbcs.txt
```

Restarting after registration

Once the row has been added to the dbmanifest table, restart ORPatch and the script will be skipped. If the file is not skipped there are several possibilities:

The script registered is not the failing script.

The file type is not a type that is filtered by the dbmanifest. The only file types that skip files listed in the dbmanifest are:

- Initial install DDL Files
- Installation scripts that cannot be rerun
- Database Change Scripts

Manual Restart State File Updates

Oracle Retail strongly discourages manually updating the ORPatch restart state files.

Updating the file improperly could cause necessary steps in the patching process to be skipped or patches to be incorrectly recorded as applied.

DISPLAY Settings When Compiling Forms

When compiling RMS or RWMS forms, it is necessary to have a valid X-Windows Display. ORPatch allows this setting to come from one of two places:

DISPLAY environment variable set before executing ORPatch

or

DISPLAY setting in RETAIL_HOME/orpatch/config/env_info.cfg

The DISPLAY variable in the environment overrides the env_info.cfg, if both are set. The destination X-Windows display must be accessible to the user running ORPatch, and for best compilation performance it should be on the network 'close' to the server where RMS Forms are installed and compiled. Using a local display or VNC display is preferred. Compiling forms across a Wide-Area Network will greatly increase the time required to apply patches to environments.

JAVA_HOME Setting

When working with Java application jar, ear or war files, it is necessary to have a valid JAVA_HOME setting. ORPatch allows this setting to come from one of two places:

JAVA_HOME environment variable set before executing ORPatch

or

JAVA_HOME setting in RETAIL_HOME/orpatch/config/env_info.cfg

The JAVA_HOME variable in the environment overrides the env_info.cfg, if both are set. The specified Java home location must be accessible to the user running ORPatch and be a full Java Development Kit (JDK) installation. The JAVA_HOME must contain the jar utility and if automatic Jar file signing is configured, must also contain the keytool and jarsigner utilities.

Patching Prior to First Install

In some situations, it may be necessary to apply a patch to product installation files before the initial install. For example, if there is a defect with a script that would be run during the install and prevent proper installation. In this rare situation, it may be necessary to apply a patch to the installation files prior to starting installation.

Note: These steps should only be undertaken at the direction of Oracle Support.

Perform the following steps to patch installation files prior to starting an installation. The steps assume an RMS installation, but apply to any product supported by ORPatch:

1. Unzip the installation files to a staging area.

Note: The following steps assume the files are in
/media/oretail15.0

2. Locate the patch_info.cfg within the product media. The directory it resides in will be used for later steps.

```
find /media/oretail15.0/rms/installer -name patch_info.cfg
```

Output Example:

/media/oretail15.0/rms/installer/mom15/patch_info.cfg

3. Get the PATCH_NAME for the standard product installation. The patch name to use in subsequent steps will be the portion following the "=" sign.

```
grep "PATCH_NAME=" /media/oretail15.0/rms/installer/mom15/patch_info.cfg
```

Output Example:

PATCH_NAME=MOM_15_0_0_0

4. Create a directory that will contain the patch that must be applied, next to the directory with the product installation files.

Note: The following steps assume this directory is in
/media/patch.

5. Unzip the patch into the directory created in step 2.

Note: This should place the patch contents in
/media/patch/<patch num>.

6. Export RETAIL_HOME to point within the installation staging area.

```
export RETAIL_HOME=/media/oretail15.0/rms/installer/mom15/Build
```

7. Create a logs directory within the installation staging area

```
mkdir $RETAIL_HOME/orpatch/logs
```

8. Ensure the ORMerge shell script is executable.

```
chmod u+x $RETAIL_HOME/orpatch/bin/ormerge
```

9. Run ORMerge to apply the patch to the installation media, using a -name argument that is the same as what was found in step 3.

```
$RETAIL_HOME/orpatch/bin/ormerge -s /media/patch -d  
/media/oretail15.0/rms/installer/mom15 -name MOM_15_0_0_0 -inplace
```

Note: The -inplace argument is critical to ensure that the
patching replaces files in the mom15 directory.

10. Unset the RETAIL_HOME environment variable.

```
unset RETAIL_HOME
```

At this point, the installation files will have been updated with the newer versions of files contained within the patch. Log files for the merge will be in
/media/oretail15.0/rms/installer/mom15/Build/orpatch/logs.

Providing Metadata to Oracle Support

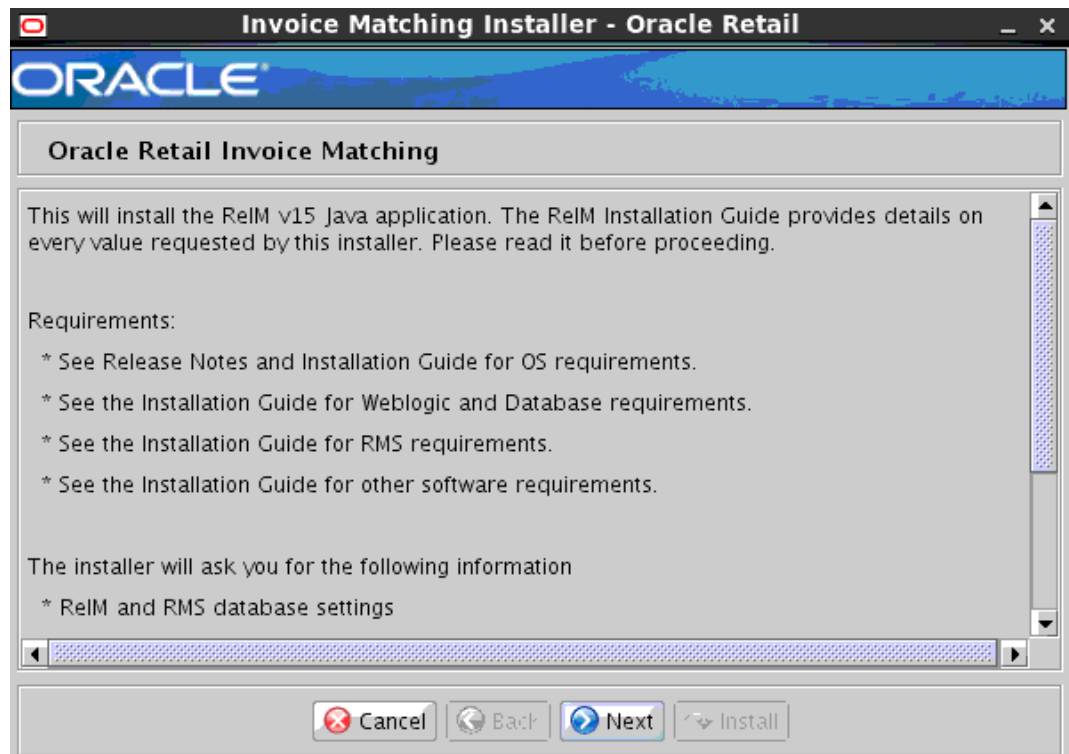
In some situations, it may be necessary to provide details of the metadata from an environment to Oracle support in order to assist with investigating a patching or application problem. ORPatch provides built-in functionality through the 'exportmetadata' action to extract and consolidate metadata information for uploading to

Oracle Support or for external analysis. For more information, see the ORPatch 'Exporting Environment Metadata' section.

Appendix: ReIM Application Installer Screens

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

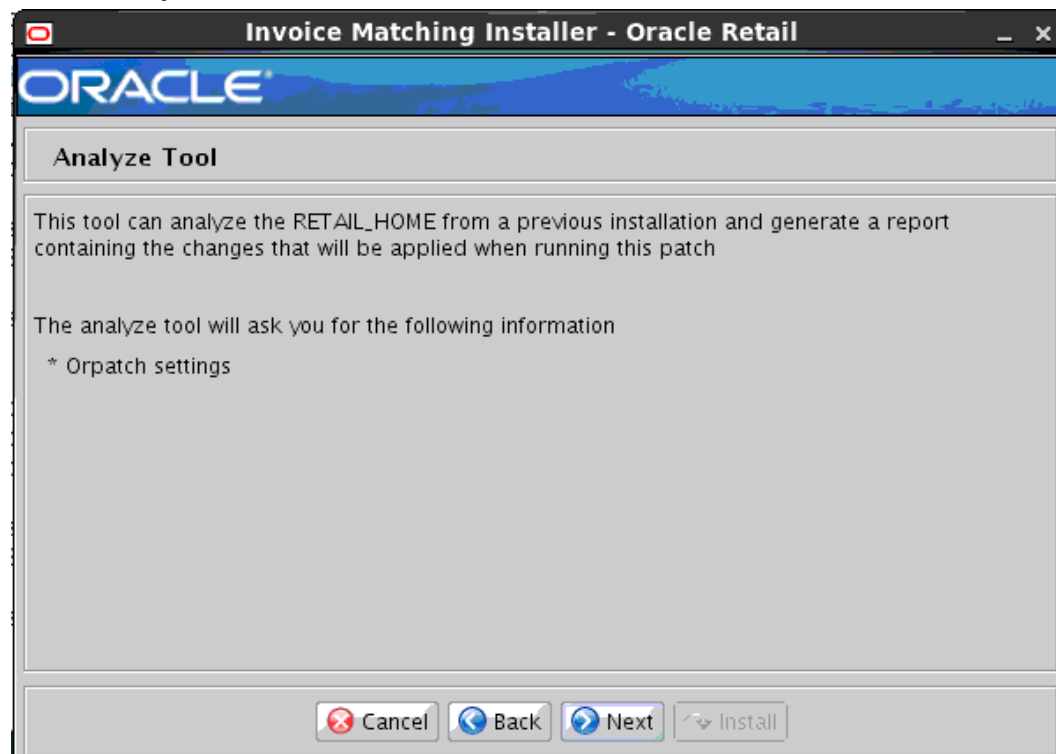
Screen: Startup



Analyze Tool

The following screens will only appear if the variable ORPATCH_ANALYZE has been set to True in the environment.

Screen: Analyze Tool



Screen: RETAIL_HOME to Analyze

Invoice Matching Installer - Oracle Retail

ORACLE

RETAIL_HOME to Analyze

Please enter a RETAIL_HOME path from a pre-existing installation that you would like to analyze.

RETAIL_HOME

/path/to/retail_home

Select Folder

Note: If you proceed to run the analyze tool, Orpatch will be updated in the RETAIL_HOME you have selected with the latest Orpatch files from this patch. Only generic Orpatch files will be updated, no product patches will be applied.

Cancel

Back

Next

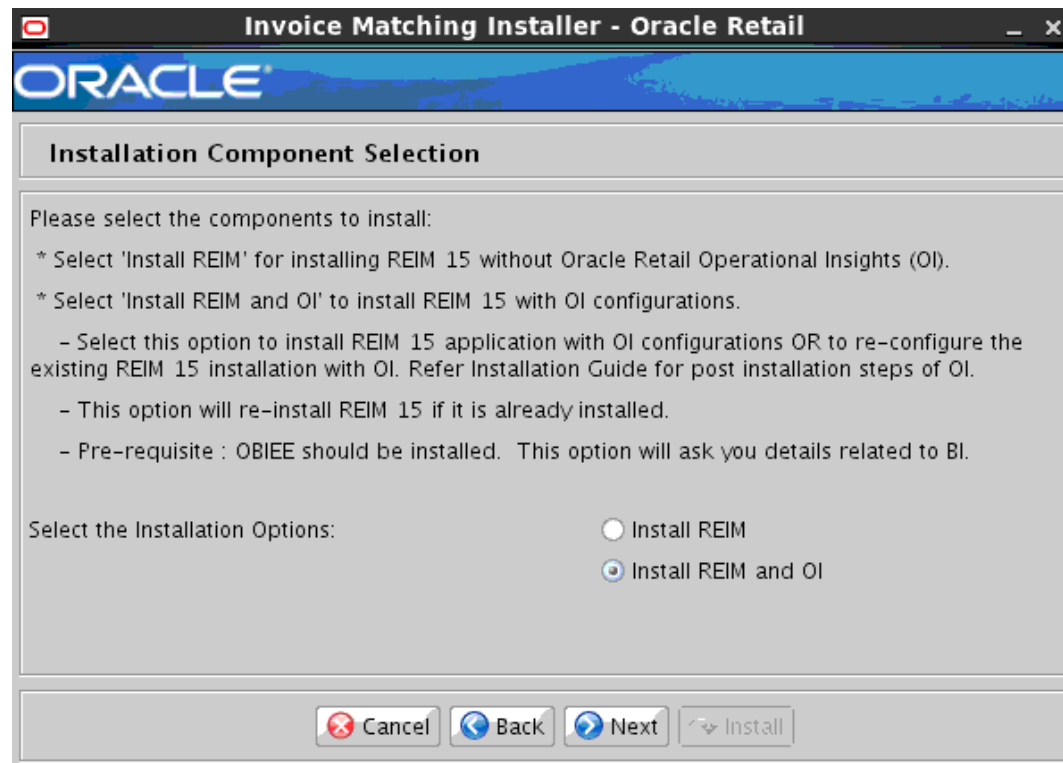
Install

Field Title	RETAIL_HOME to Analyze
Field Description	The pre-existing RETAIL_HOME location created and used during REIM installation. This location should contain directories with your installed files as well as the “orpatch” directory.
Example	/path/to/retail_home
Note	The Orpatch files in this RETAIL_HOME may need to be updated in order to be able to run the analysis. The Analyze tool will take care of this automatically.

Application Installer

The following screens will only appear if the variable ORPATCH_ANALYZE has not been set in the environment.

Screen: Installation Component Selection



Field Title	Installation Component Selection
Field Description	Selecting 'Install REIM' will install REIM 15.0.3 without Operational Insights (OI). 'Install REIM and OI' will install REIM along with OI configurations or reconfigure the existing REIM 15.0.3 installation. Note that selecting the second option will require OBIEE details to be entered in the further stages of the installation.

Screen: ReIM Application RETAIL_HOME

Invoice Matching Installer - Oracle Retail

ORACLE

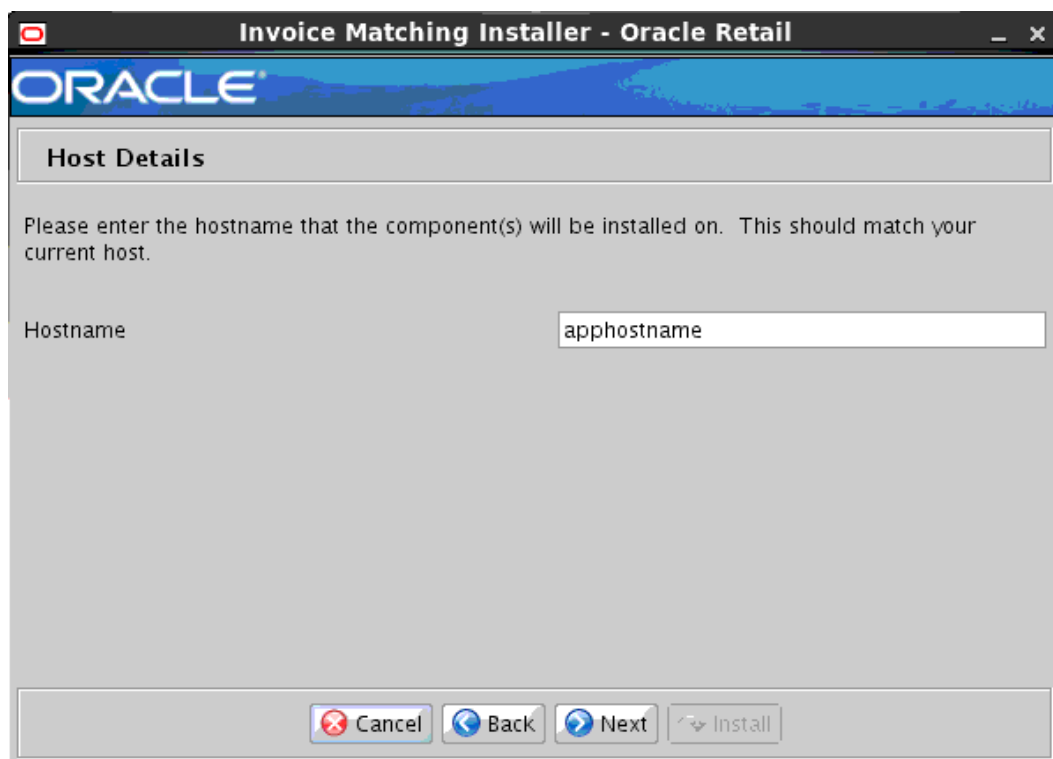
ReIM Application RETAIL_HOME

Please enter the directory where the ReIM application files and batch scripts will be installed. Please keep track of this directory, it should remain in place after installation and will be used to apply future patches.

ReIM Application RETAIL_HOME

Field Title	ReIM Application RETAIL_HOME
Field Description	Retail Home is used to keep Orpatch related files, batches etc. by default. Please keep track of this directory, it should remain in place after installation and will be used to apply future patches.
Examples	/path/to/reim_retail_home

Screen: Host Details



Invoice Matching Installer - Oracle Retail

ORACLE

Host Details

Please enter the hostname that the component(s) will be installed on. This should match your current host.

Hostname

Field Title	Hostname
Field Description	Provide the hostname where the Retail Home will be installed. This shall match your Application Server hostname.
Examples	apphostname

Screen: Security Details

Invoice Matching Installer - Oracle Retail

ORACLE

Security Details

Provide security details for the REIM application

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

Enable SSL for REIM?

☒ Yes
☐ No

Cancel Back Next Install

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

Screen: JDBC Security Details

Invoice Matching Installer - Oracle Retail

ORACLE

JDBC Security Details

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

Enable Secure JDBC connection

☒ Yes
☐ No

Cancel Back Next Install

Field Title	Enable Secure JDBC connection
Field Description	Select Yes to create secured data sources in WebLogic, otherwise choose No. A secure data base connection must already be set up if you want to create a secure data source.

Screen: Data Source Details

Invoice Matching Installer - Oracle Retail

ORACLE

Data Source Details

Provide the details for the Invoice Matching data source

ReIM/RMS JDBC URL

ReIM/RMS schema user

ReIM/RMS schema password

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

RMS schema owner

REIM schema user alias

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

Field Title	ReIM/RMS JDBC URL
Field Description	URL used by the ReIM application to access the ReIM/RMS database schema. See Appendix: URL Reference for expected syntax.
Examples	For Non Secure JDBC Connection: jdbc:oracle:thin:@hostname:1521/dbname For Secure JDBC Connection: jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=tcps)(HOST=dbhostname)(PORT=2484)))(CONNECT_DATA=(SERVICE_NAME=mydb)))

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

Field Title	ReIM/RMS schema password
Field Description	Password for the RMS database user entered above to access the ReIM tables.

Field Title	RMS schema owner
Field Description	Database user which owns the RMS and ReIM tables. This usually has the same value as the ReIM/RMS schema field above.
Example	rms01

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

Screen: Secure Data Source Details

Secure Data Source Details

Provide the details for the REIM secure data source

Identity Keystore: /home/sample.keystore

Identity Keystore Type: JKS

Identity Keystore Passphrase:

Identity truststore: /home/test.keystore

Identity truststore Type: JKS

Identity truststore Passphrase:

Buttons: Cancel, Back, Next, Install

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

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

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

Field Title	Identity Keystore Passphrase
Field Description	The password to access the keystore mentioned above.

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

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

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

Screen: Application Deployment Details

Invoice Matching Installer - Oracle Retail

ORACLE

Application Deployment Details

The default values shown below are examples

ReIM app deployment name

Enter the REIM weblogic managed server or cluster.

ReIM server/cluster

Field Title	ReIM app deployment name
Field Description	Name by which this ReIM application is identified in the application server.
Example	reim15

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

Screen: WebLogic Administrative User

Weblogic Administrative User

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

Hostname:

Weblogic admin port:

Weblogic admin user:

Weblogic admin password:

Weblogic admin alias:

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

Buttons: Cancel, Back, Next, Install

Field Title	Hostname
Field Description	The hostname of the server where the WebLogic server is installed.
Example	Hostname

Field Title	WebLogic admin port
Field Description	This is the port of Administration Console.
Example	23002

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

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

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

Screen: Webservice Account Validation Details

Invoice Matching Installer - Oracle Retail

ORACLE

Webservice Account Validation Details

Provide the details for the Invoice Matching Webservice Account Validation URL

Please provide Account Validation Web Service URL

Should Account Validation Web Service invocation be done with credentials?

☒ Yes
☐ No

Field Title	Account Validation Web Service URL
Field Description	The URL for validating Web service accounts. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.
Example	https://hostname:18008/fin-GIAccountValidation-AppServiceDecorator/ProxyService/GIAccountValidationAppServiceProxy?wsdl

Field Title	Should Account Validation Web Service invocation be done with credentials?
Field Description	If the webservices entered in the above screen have security validation, choose Yes. Choosing Yes will navigate you to the screen asking for Webservice Account Validation Credentials. Choosing No will skip the Webservice Account Validation Credentials screen

Screen: Webservice Account Validation Credentials

Invoice Matching Installer - Oracle Retail

ORACLE®

Webservice Account Validation Credentials

Provide the credentials for the Invoice Matching Webservice Account Validation.

Webservice Account Validation user

retail.user

Webservice Account Validation password

.....

Webservice Account Validation user alias

WAV -alias

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

Cancel

Back

Next

Install

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

Field Title	Webservice Account Validation user
Field Description	Enter the username for validating the Web service.
Example	retail.user

Field Title	Webservice Account Validation Password
Field Description	The password of the above username which is used to validate the Web service.

Field Title	Webservice Account Validation Alias
Field Description	The alias for the Web service account user name.
Example	WAV-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: Enable Account Validation Drill Forward Credentials

Invoice Matching Installer - Oracle Retail

ORACLE®

Enable Account Validation Drill Forward Credentials

Provide the details for the Invoice Matching Webservice Account Validation Drill Forward Credentials for REIM

Please provide Drill Forward Web Service URL

https://hostname:18008

Should Drill Forward Web Service invocation be done with credentials?

☒ Yes

☐ No

Cancel

Back

Next

Install

Field Title	Drill Forward Web Service URL
Field Description	The Web service drilling forward URL used for the ReIM application. This information is from the financial application to which you are integrating (for example, Oracle E-Business Suite). Leave this field blank if there is no integration with a financial application.
Example	https://hostname:18008/fin-DrillBackForwardUrl-AppServiceDecorator/ProxyService/DrillBackForwardUrlAppServiceProxy?wsdl

Field Title	Drill Forward Web Service Invocation be done with credentials?
Field Description	<div>If the Drill Forward Web Service URL entered in the above screen have security validation, choose Yes.</div> <div>Choosing Yes will navigate you to the screen asking for Drill Forward Web Service URL validation credentials. Choosing No will skip the Drill Forward Web Service URL Validation Credentials screen</div>

Screen: Webservice Account Validation Drill Forward Credentials

Invoice Matching Installer - Oracle Retail

ORACLE

Webservice Account Validation Drill Forward Credentials

Provide the details for the Invoice Matching Drill Forward URL.

WAV Drill Forward user: retail.user

WAV Drill Forward password:

WAV Drill Forward user alias: WAVD-alias

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

Buttons: Cancel, Back, Next, Install

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

Field Title	Webservice Account Validation Drill Forward user
Field Description	Enter the username for validating the Web service Drill Forward
Example	retail.user

Field Title	Webservice Account Validation Drill Forward Password
Field Description	The password of the above username which is used to validate the Web service Account Validation Drill Forward.

Field Title	Webservice Account Validation Drill Forward user alias
Field Description	The alias for the Web service account drill forward user name.
Example	WAVD-alias
Note	This alias must be unique. Do not use the same value for any other alias fields in the installer. If the same alias is used, entries in the wallet can override each other and cause problems with the application.

Screen: Batch User Credentials

Batch User Credentials

Provide the credentials for the Batch User

Batch user: ADMIN

Batch User password:

Batch user alias: batch-alias

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

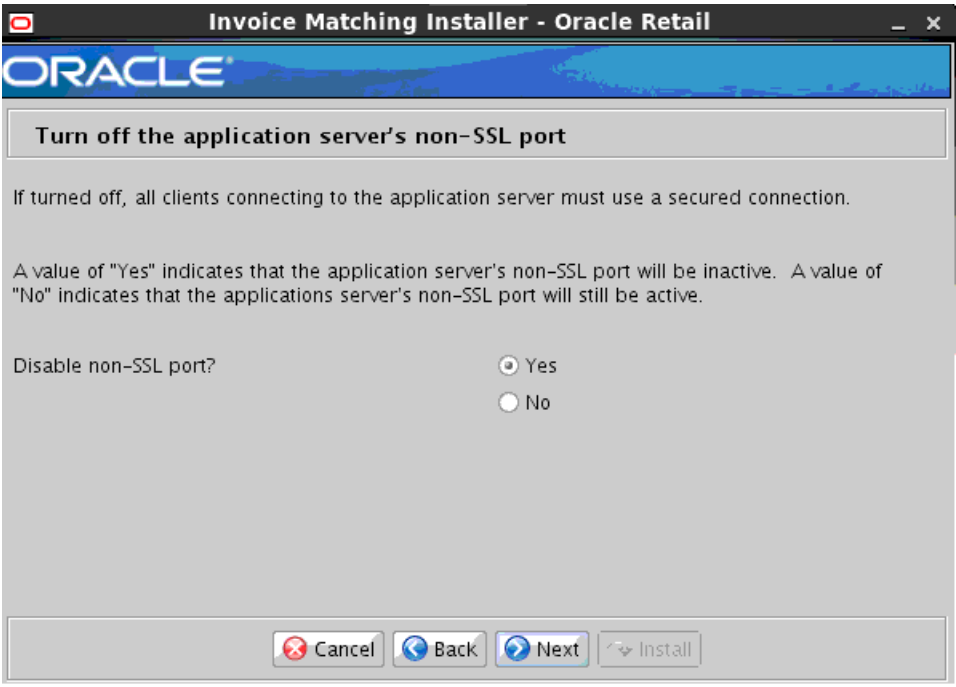
Buttons: Cancel, Back, Next, Install

Field Title	Batch User
Field Description	This shall be a valid user that can login into the application.
Example	REIM_ADMIN

Field Title	Batch User Password
Field Description	The password of the user that can login into the application.

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

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



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

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

Screen: OHS Web Tier

The screenshot shows a window titled "Invoice Matching Installer - Oracle Retail". Inside, there's a header with the "ORACLE" logo. Below it, the title "OHS Web Tier" is displayed. The main text asks: "Are you running an OHS web tier for use in Oracle Single Sign-On and/or a Clustered Environment?". There are two radio buttons: "Yes" (unselected) and "No" (selected). At the bottom, there are four buttons: "Cancel" (with a red X icon), "Back" (with a left arrow icon), "Next" (with a right arrow icon), and "Install" (with a downward arrow icon).

Field Title	Are you running OHS Web Tier for use in Oracle Single Sign-on?
Field Description	Selecting the option 'Yes' will configure all the application URLs delivered by this installer with the OHS webtier hostname and port that will be entered in the next screen. Selecting option 'No' will result in application URLs having default ports.

Screen: OHS Web Tier Details

This screen appears only if you have selected Yes in the previous screen.

Invoice Matching Installer - Oracle Retail

ORACLE

OHS Web Tier Details

Please enter the OHS web tier details.

OHS web tier connection protocol ☐ http ☒ https

OHS web tier host

OHS web tier port

Field Title	OHS web Tier connection protocol
Field Description	Connection protocol for OHS web tier – http or https

Field Title	OHS web tier host
Field Description	Host name for OHS web tier
Example	ohshostname

Field Title	OHS web tier port
Field Description	Port number for OHS web tier
Example	7002

Screen: OBIEE Details

This screen will appear only if you have selected the option 'Install REIM and OI' in the 'Installation Component Selection' screen.

Field Title	OBIEE connection protocol
Field Description	Connection protocol used while connecting to OBIEE - http or https

Field Title	OBIEE Hostname
Field Description	OBIEE Hostname where you have installed/planning to install the Operational Insights Dashboards.
Example	obieehostname

Field Title	OBIEE Managed Server Port
Field Description	The port of the Oracle BI EE installation
Example	7333

Field Title	OBIEE SSO Port
Field Description	The SSO port where OBIEE is configured, if SSO is enabled. If you are not using SSO, leave the field blank.
Example	7780

Field Title	OBIEE Impersonate User Name
Field Description	The username that has been configured on the Oracle BI EE with the impersonate permissions.
Example	BIImpersonateUser

Field Title	OBIEE Impersonate User Alias
Field Description	An alias for the OBIEE Impersonate User
Example	ImpersonateUserAlias

Field Title	OBIEE Impersonate User Password
Field Description	The password associated with the username that has been configured on the Oracle BI EE with the impersonate permissions.

Field Title	OBIEE Static Resources Location
Field Description	<p>The path of the location where the static resources are available.</p> <p>For non-SSO environments use the following URL.</p> <p><a href="http://<obiee_host>:<obiee_port>/analytics">http://<obiee_host>:<obiee_port>/analytics</p> <p>For SSO environments, use the host and port of the Oracle Web Tier.</p> <p><a href="http://<web_tier_host>:<web_tier_port>">http://<web_tier_host>:<web_tier_port></p>
Example	http://obieehostname:7333/analytics

Screen: Installation Summary

Invoice Matching Installer - Oracle Retail

ORACLE

Installation Summary

Summary of Installation

App Name	reim15
Context Root	reim
Weblogic Managed Server/Cluster	reim-server
App Server Host	hostname
Weblogic Admin Port	23002
Weblogic Admin User	weblogic
Weblogic Admin Alias	weblogic-alias

Cancel Back Next Install

Appendix: Installer Silent Mode

Once you have a managed server that is configured and started, you can run the REIM application installer. This installer configures and deploys the REIM application.

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`, `JAVA_HOME`, and `WEBLOGIC_DOMAIN_HOME` environment variables. `ORACLE_HOME` should point to your WebLogic installation. `JAVA_HOME` should point to the Java JDK 1.7+. This is typically the same JDK which is being used by the WebLogic domain where Application is getting installed. `WEBLOGIC_DOMAIN_HOME` should point to the full path of the domain into which REIM will be installed.
3. If a secured datasource is going to be configured you also need to set “ANT_OPTS” so the installer can access the key and trust store that is used for the datasource security:

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

An example of this would be:

```
export ANT_OPTS="-
Djavax.net.ssl.keyStore/u00/webadmin/product/identity.keystore -
Djavax.net.ssl.keyStoreType=jks -Djavax.net.ssl.keyStorePassword=retail123 -
Djavax.net.ssl.trustStore/u00/webadmin/product/identity.truststore -
Djavax.net.ssl.trustStoreType=jks -
Djavax.net.ssl.trustStorePassword=retail123"
```

- 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.
- Edit the `ant.install.properties` file and correct any invalid settings that may have caused the installer to fail in its previous run.

Note: The password properties need to be copied over from the `ant.install.properties.sample` to the `ant.install.properties` file in this case and update with the values.

- If the application needs to be installed in silent mode copy the `ant.install.properties.sample` to `ant.install.properties`. Provide values for each property including the passwords
- Run the installation command “`./install.sh silent`”. This launches the installer in silent mode. A detailed installation log file is created (`reiminstall.<timestamp>.log`).
- Remove the values for password once the installation is completed successfully.

Appendix: Single Sign-On for WebLogic

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

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

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

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

What Do I Need for Single Sign-On?

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

- An Oracle Internet Directory (OID) LDAP server, used to store user, role, security, and other information. OID uses an Oracle database as the back-end storage of this information.
- An Oracle Access Manager (OAM) 12c server and administrative console for implementing and configuring policies for single sign-on.
- A Policy Enforcement Agent such as Oracle Access Manager 12c Agent (WebGate), used to authenticate the user and create the Single Sign-On cookies.
- Oracle Directory Services Manager (ODSM) application in OIM12c, used to administer users and group information. This information may also be loaded or modified via standard LDAP Data Interchange Format (LDIF) scripts.
- Additional administrative scripts for configuring the OAM system and registering HTTP servers.

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

Can Oracle Access Manager Work with Other SSO Implementations?

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

Oracle Single Sign-on Terms and Definitions

The following terms apply to single sign-on.

Authentication

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

Dynamically Protected URLs

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

Oracle Identity Management (OIM) and Oracle Access Manager (OAM) for 12c

Oracle Identity Management (OIM) 12c includes Oracle Internet Directory and ODSM. Oracle Access Manager (OAM) 12c should be used for SSO using WebGate. Oracle Forms 12c contains Oracle HTTP server and other Retail Applications will use Oracle WebTier 12c for HTTP Server.

MOD_WEBLOGIC

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

Oracle Access Manager Agent (WebGate)

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

Oracle Internet Directory

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

Partner Application

A partner application is an application that delegates authentication to the Oracle Identity Management Infrastructure. One such partner application is the Oracle HTTP Server (OHS) supplied with Oracle Forms Server or WebTier12c Server if using other Retail Applications other than Oracle Forms Applications.

All partner applications must be registered with Oracle Access Manager (OAM)12c. An output product of this registration is a configuration file the partner application uses to verify a user has been previously authenticated.

Statically Protected URLs

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

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

What Single Sign-On is not

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

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

How Oracle Single Sign-On Works

Oracle Access Manager involves several different components. These are:

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

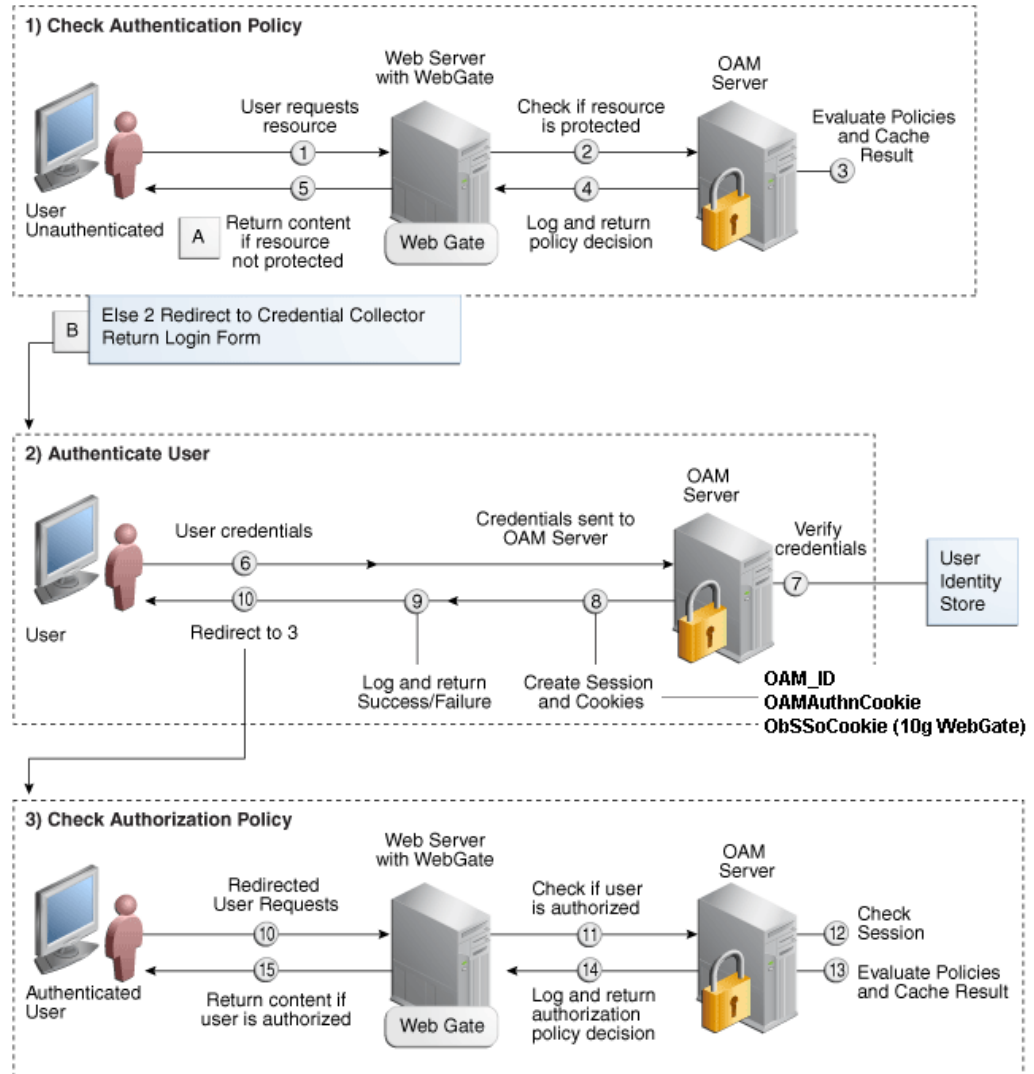
About SSO Login Processing with OAM Agents

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

15. WebGate responds as follows:

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

SSO Login Processing with OAM Agents



Installation Overview

Installing an Oracle Retail supported Single Sign-On installation using OAM12c 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. The ODSM application can be used for user and realm management within OID.
2. Oracle Access Manager 12c has to be installed and configured.
3. Additional midtier instances (such as Oracle Forms) for Oracle Retail applications based on Oracle Forms technologies (such as RMS). These instances must be registered with the OAM installed in step 2.
4. Additional application servers to deploy other Oracle Retail applications and performing application specific initialization and deployment activities must be registered with OAM installed in step 2.

Infrastructure Installation and Configuration

The Infrastructure installation for Oracle Access Manager (OAM) is dependent on the environment and requirements for its use. Deploying Oracle Access Manager (OAM) to be used in a test environment does not have the same availability requirements as for a production environment. Similarly, the Oracle Internet Directory (OID) LDAP server can be deployed in a variety of different configurations. See the *Oracle Identity Management Installation Guide12c*.

OID User Data

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

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

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

User Management

User Management consists of displaying, creating, updating or removing user information. There are many methods of managing an LDAP directory including LDIF scripts or Oracle Directory Services Manager (ODSM) available for OID12c.

ODSM

Oracle Directory Services Manager (ODSM) is a Web-based application used in OID12c is designed for both administrators and users which enables you to configure the structure of the directory, define objects in the directory, add and configure users, groups, and other entries. ODSM is the interface you use to manage entries, schema, security, adapters, extensions, and other directory features.

LDIF Scripts

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

User Data Synchronization

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

Appendix: URL Reference

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

JDBC URL for a Database

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

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

<sid>: system identifier for the database

Example: jdbc:oracle:oci:@mysid

Thin Client Syntax: jdbc:oracle:thin:@<host>:<port>/servicename<host>: hostname of the database server

<port>: database listener port

< servicename>: Service Name for the database

Example: jdbc:oracle:thin:@myhost:1521/servicename

Appendix: BI User and Group LDIF Entries

BI_User.ldif Entries

```
dn: cn=BISystemUser,cn=Users,dc=us,dc=oracle,dc=com
orclsamaccountname: BUYER
givenname: BISystemUser
sn: BISystemUser
userpassword: welcome1
mail: BISystemUser@rgbu.generated.oracle.com
displayname: BISystemUser
uid: BISystemUser
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orclUser
objectclass: orclUserV2
objectclass: orclIDXPerson
orclpassword: <your password here>
orclactivestartdate: 20140821000000z
cn: BISystemUser
description: A user for the 'Buyer' role.
```

```
dn: cn=BIImpersonateUser,cn=Users,dc=us,dc=oracle,dc=com
orclsamaccountname: BUYER
givenname: BIImpersonateUser
sn: BIImpersonateUser
userpassword: welcome1
mail: BIImpersonateUser@rgbu.generated.oracle.com
displayname: BIImpersonateUser
uid: BIImpersonateUser
objectclass: inetOrgPerson
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: orclUser
objectclass: orclUserV2
objectclass: orclIDXPerson
orclpassword: <your password here>
orclactivestartdate: 20140821000000z
cn: BIImpersonateUser
description: A user for the 'Buyer' role.
```

Note: Change the userpassword with your password before loading the ldif into the LDAP.

BI_Group.Idifs Entries

```
dn: cn=BIAdministrators,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
description: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
uniquemember: cn=resa_admin,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=reim_admin,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=allocation_admin,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
cn: BIAdministrators
```

```
dn: cn=BIAuthors,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
description: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
uniquemember: cn=resa_su,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
cn: BIAuthors
```

```
dn: cn=BIConsumers,cn=groups,dc=us,dc=oracle,dc=com
uniquemember: cn=bisystemuser,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=orcladmin
uniquemember: cn=resa_su,cn=users,dc=us,dc=oracle,dc=com
uniquemember: cn=retail.user,cn=users,dc=us,dc=oracle,dc=com
orclnormdn: cn=biconsumers,cn=groups,dc=us,dc=oracle,dc=com
displayname: OBIEE Users
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
modifytimestamp: 20140925090248z
modifiersname: cn=orcladmin
cn: BIConsumers
creatorsname: cn=orcladmin
createtimestamp: 20140822142024z
description: OBIEE Users
```

Appendix: Common Installation Errors

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

ConcurrentModificationException in Installer GUI

Symptom

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

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

Solution

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

Warning: Could not find X Input Context

Symptom

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

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

Solution

This message is harmless and can be ignored.

GUI screens fail to open when running Installer

Symptom

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

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

Solution

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

Hostname Verification Error when SSL is used

Symptom:

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

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

Solution:

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

Appendix: Setting Up Password Stores with wallets/credential stores

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

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

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

About Database Password Stores and Oracle Wallet

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

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

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

```
sqlplus /@db_username
```

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

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

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

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

Setting Up Password Stores for Database User Accounts

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

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

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

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

1. Create a wallet using the following command:

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

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

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

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

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

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

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

3. Repeat Step 2 for all the database user accounts.
4. Update the `sqlnet.ora` file to include the following statements:

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

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

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


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

Setting up Wallets for Database User Accounts

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

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

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

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

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

```
cd /projects/rms15/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/rms15/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/12.1.0.2/network/admin/tnsnames.ora
```

Examples for a NON pluggable db:

```
dvols29_rms01user =
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
(host = xxxxxx.us.oracle.com) (Port = 1521)))
(CONNECT_DATA = (SID = <sid_name> (GLOBAL_NAME = <sid_name>))))
```

```
dvols29_rms01user.world =
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
(host = xxxxxx.us.oracle.com) (Port = 1521)))
(CONNECT_DATA = (SID = <sid_name>) (GLOBAL_NAME = <sid_name>)))
```

Examples for a pluggable db:

```
dvols29_rms01user =
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
(host = xxxxxx.us.oracle.com) (Port = 1521)))
(CONNECT_DATA = (SERVICE_NAME = <pluggable db name>)))
```

```
dvols29_rms01user.world =
(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = tcp)
(host = xxxxxx.us.oracle.com) (Port = 1521)))
(CONNECT_DATA = (SERVICE_NAME = <pluggable db name>)))
```

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/rms15/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/rms15/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 12
```

```
Connected to:
Oracle Database 12g
```

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

Running batch programs or shell scripts would be similar:

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

Set the UP unix variable to help with some compiles :

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

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

Additional Database Wallet Commands

The following is a list of additional database wallet commands.

Delete a credential on wallet

```
mkstore -wrl . -deleteCredential dvols29_rms01user
```

Change the password for a credential on wallet

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

List the wallet credential entries

```
mkstore -wrl . -list
```

This command returns values such as the following.

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

View the details of a wallet entry

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

Returns the value of the entry:

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

Returns the value of the entry:

```
rms01user
```

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

Returns the value of the entry:

```
Passwd
```

Setting up RETL Wallets

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

cwallet.sso

jazn-data.xml

jps-config.xml

README.txt

To set up RETL wallets, perform the following steps:

1. Set the following environment variables:
 - ORACLE_SID=<retaildb>
 - RFX_HOME=/u00/rfx/rfx-13
 - RFX_TMP=/u00/rfx/rfx-13/tmp
 - JAVA_HOME=/usr/jdk1.6.0_12.64bit
 - LD_LIBRARY_PATH=\$ORACLE_HOME
 - PATH=\$RFX_HOME/bin:\$JAVA_HOME/bin:\$PATH
2. Change directory to \$RFX_HOME/bin.
3. Run setup-security-credential.sh.
 - Enter 1 to add a new database credential.
 - Enter the dbuseralias. For example, retl_java_rms01user.
 - Enter the database user name. For example, rms01user.
 - Enter the database password.
 - Re-enter the database password.
 - Enter D to exit the setup script.

4. Update your RETL environment variable script to reflect the names of both the Oracle Networking wallet and the Java wallet.

For example, to configure RETLforRPAS, modify the following entries in `$RETAIL_HOME/RETLforRPAS/rfx/etc/rmse_rpas_config.env`.

- The RETL_WALLET_ALIAS should point to the Java wallet entry:
 - `export RETL_WALLET_ALIAS="retl_java_rms01user"`
 - The ORACLE_WALLET_ALIAS should point to the Oracle network wallet entry:
 - `export ORACLE_WALLET_ALIAS="dvols29_rms01user"`
 - The SQLPLUS_LOGON should use the ORACLE_WALLET_ALIAS:
 - `export SQLPLUS_LOGON="/@${ORACLE_WALLET_ALIAS}"`
5. To change a password later, run `setup-security-credential.sh`.
 - Enter 2 to update a database credential.
 - Select the credential to update.
 - Enter the database user to update or change.
 - Enter the password of the database user.
 - Re-enter the password.

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

For Java applications, consider the following:

For database user accounts, ensure that you set up the same alias names between the password stores (database wallet and Java wallet). You can provide the alias name during the installer process.

Document all aliases that you have set up. During the application installation, you must enter the alias names for the application installer to connect to the database and application server.

Passwords are not used to update entries in Java wallets. Entries in Java wallets are stored in partitions, or application-level keys. In each retail application that has been installed, the wallet is located in

`<WEBLOGIC_DOMAIN_HOME>/retail/<appname>/config` Example:
`/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15/config`

Application installers should create the Java wallets for you, but it is good to know how this works for future use and understanding.

Scripts are located in `<WEBLOGIC_DOMAIN_HOME>/retail/<appname>/retail-public-security-api/bin` for administering wallet entries.

Example:

`/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/retail-public-security-api/bin`

In this directory is a script to help you update each alias entry without having to remember the wallet details. For example, if you set the RPM database alias to `rms01user`, you will find a script called `update-RMS01USER.sh`.

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

Two main scripts are related to this script in the folder for more generic wallet operations: `dump_credentials.sh` and `save_credential.sh`.

If you have not installed the application yet, you can unzip the application zip file and view these scripts in `<app>/application/retail-public-security-api/bin`.

Example:

```
/u00/webadmin/reim15/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:

```
/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15/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.
/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15/retail-public-
security-api/bin>
```

dump_credentials.sh

dump_credentials.sh is used to retrieve information from wallet. For each entry found in the wallet, the wallet partition, the alias, and the user name are displayed.

Note that the password is not displayed. If the value of an entry is uncertain, run save_credential.sh to resave the entry with a known password.

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

Example:

```
dump_credentials.sh location:
/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15/config
```

Retail Public Security API Utility

```
=====
Below are the credentials found in the wallet at the
location/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15/
config
=====
```

```
Application level key partition name:reim15
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:rms15mock
User Name Alias:REIMBAT-ALIAS User Name:reimbat
```

save_credential.sh

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

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

Example:

```
/u00/webadmin/mock15_testing/reim15/application/retail-public-security-api/bin>
save_credential.sh -l wallet_test -a myalias -p mypartition -u myuser
```

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

Enter password:

Verify password:

Note: -p in the above command is for partition name. You must specify the proper partition name used in application code for each Java application.

save_credential.sh and dump_credentials.sh scripts are the same for all applications. If using save_credential.sh to add a wallet entry or to update a wallet entry, bounce the application/managed server so that your changes are visible to the application. Also, save a backup copy of your cwallet.sso file in a location outside of the deployment path, because redeployment or reinstallation of the application will wipe the wallet entries you made after installation of the application. To restore your wallet entries after a redeployment/reinstallation, copy the backed up cwallet.sso file over the cwallet.sso file. Then bounce the application/managed server.

Usage

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

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

How does the Wallet Relate to the Application?

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

Reim.properties code sample:

```
datasource.url=jdbc:oracle:thin:@xxxxxxx.us.oracle.com:1521/pkols07
datasource.schema.owner=rms15mock
datasource.credential.alias=RMS-ALIAS
# =====
# ossa related Configuration
#
# These settings are for ossa configuration to store credentials.
# =====

csm.wallet.path=/u00/webadmin/config/domains/wls_retail/REIMDomain/retail/reim15co
nfig
csm.wallet.partition.name=reim15
```

How does the Wallet Relate to Java Batch Program use?

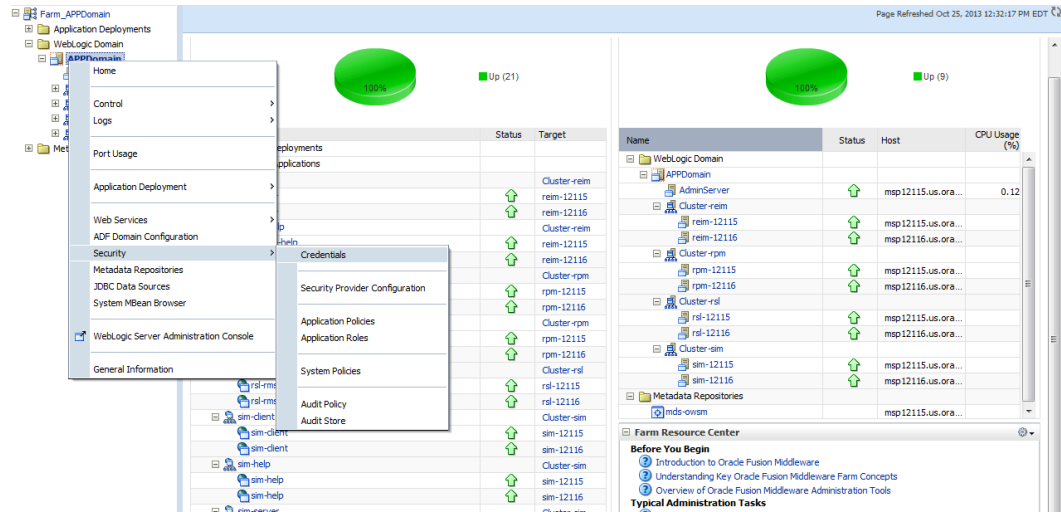
Some of the ORACLE Retail Java batch applications have an alias to use when running Java batch programs. For example, alias REIMBAT-ALIAS maps through the wallet to dbuser RMS01APP, already on the database. To run a ReIM batch program the format would be: reimbatchpgmname REIMBAT-ALIAS <other arguments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

Database Credential Store Administration

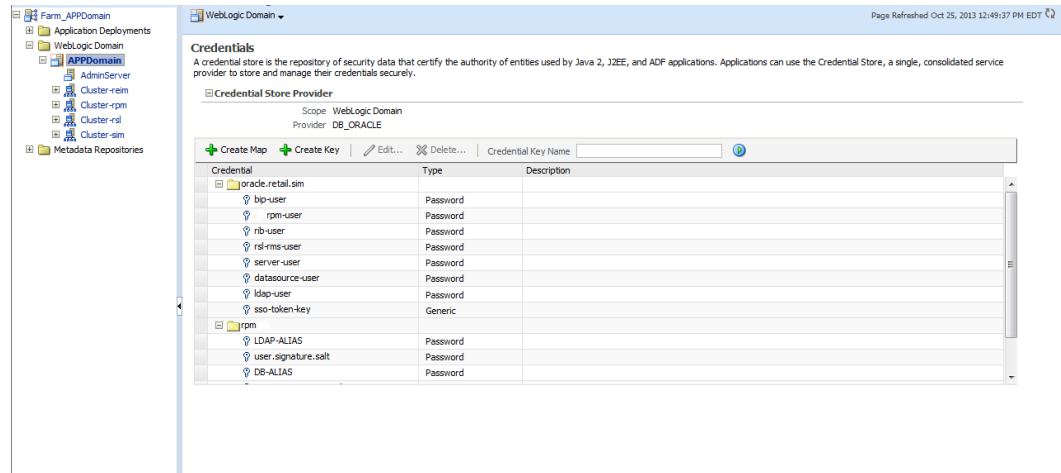
The following section describes a domain level database credential store. This is used in RPM login processing, SIM login processing, RWMS login processing, RESA login processing and Allocation login processing and policy information for application permission. Setting up the database credential store is addressed in the RPM, SIM, RESA, RWMS, and Alloc 15.0 install guides.

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

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

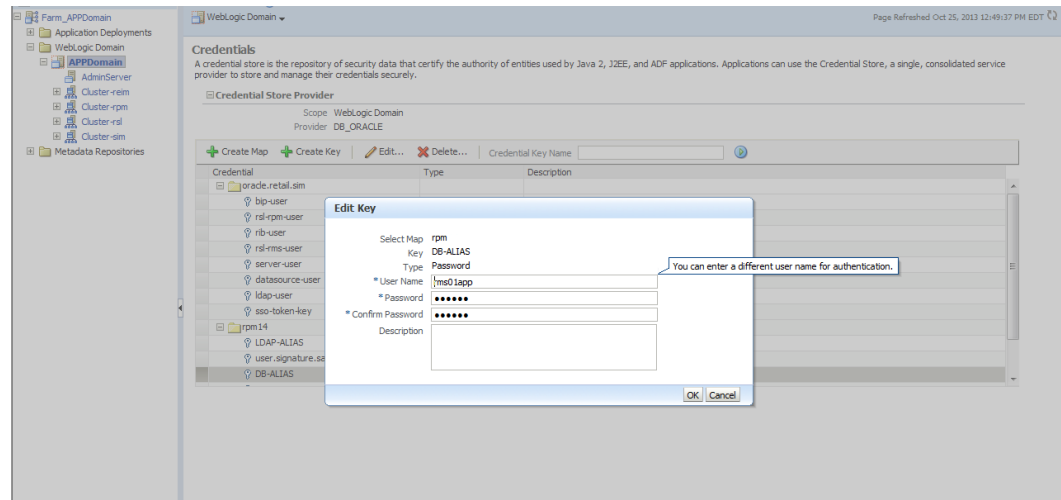


2. Click on Credentials and you will get a screen similar to the following. The following screen is expanded to make it make more sense. From here you can administer credentials.



The Create Map add above is to create a new map with keys under it. A map would usually be an application such as rpm15. The keys will usually represent alias to various users (database user, WebLogic user, LDAP user, etc). The application installer should add the maps so you should not often have to add a map.

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



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

Managing Credentials with WSLT/OPSS Scripts

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

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

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

WLST scripts can be run in interactive mode or in script mode. In interactive mode, you enter the script at a command-line prompt and view the response immediately after. In

script mode, you write scripts in a text file (with a py file name extension) and run it without requiring input, much like the directives in a shell script.

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

```
/u00/webadmin/product/wls_apps/oracle_common/bin> ./orapki wallet display -  
wallet  
/u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmw  
config
```

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

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

Requested Certificates:

User Certificates:

Oracle Secret Store entries:

```
rpm@#3#@DB-ALIAS  
rpm@#3#@LDAP-ALIAS  
rpm@#3#@RETAIL.USER  
rpm@#3#@user.signature.salt  
rpm@#3#@user.signature.secretkey  
rpm@#3#@WEBLOGIC-ALIAS  
rpm@#3#@WLS-ALIAS
```

Trusted Certificates:

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

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

```
listCred  
updateCred  
createCred  
deleteCred  
modifyBootStrapCredential  
addBootStrapCredential
```

listCred

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

Script Mode Syntax

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

Interactive Mode Syntax

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

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

`map` specifies a map name (folder).

`key` specifies a key name.

Examples of Use:

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

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

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

```
/u00/webadmin/product/wls_apps/oracle_common/common/bin>
sh wlst.sh
```

```
Initializing WebLogic Scripting Tool (WLS)...
```

```
Welcome to WebLogic Server Administration Scripting Shell
```

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

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

```
[Name : rms01app, Description : null, expiry Date : null]
PASSWORD:retail
*The above means for map rpm15 in APPDomain, alias DB-ALIAS points to database
user rms01app with a password of retail
```

updateCred

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

Interactive Mode Syntax

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

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

`map` specifies a map name (folder) in the credential store.

`key` specifies a key name.

`user` specifies the credential user name.

`password` specifies the credential password.

`desc` specifies a string describing the credential.

Example of Use:

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

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

createCred

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

Interactive Mode Syntax

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

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

`map` specifies the map name (folder) of the credential.

`key` specifies the key name of the credential.

`user` specifies the credential user name.

`password` specifies the credential password.

`desc` specifies a string describing the credential.

Example of Use:

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

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

deleteCred

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

Script Mode Syntax

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

Interactive Mode Syntax

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

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

`map` specifies a map name (folder).

`key` specifies a key name.

Example of Use:

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

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

modifyBootstrapCredential

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

This script is available in interactive mode only.

Interactive Mode Syntax

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

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

`jpsConfigFile` specifies the location of the file `jps-config.xml` relative to the location where the script is run. Example location:
`/u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmw
config`. Example location of the bootstrap wallet is
`/u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmw
config/bootstrap`

`username` specifies the distinguished name of the user in the LDAP store.

`password` specifies the password of the user.

Example of Use:

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

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

Any output regarding the audit service can be disregarded.

addBootStrapCredential

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

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

This script is available in interactive mode only.

Interactive Mode Syntax

```
addBootStrapCredential(jpsConfigFile="pathName", map="mapName", key="keyName",  
username="usrName", password="usrPass")
```

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

`jpsConfigFile` specifies the location of the file `jps-config.xml` relative to the location where the script is run. Example location:
`/u00/webadmin/product/wls_apps/user_projects/domains/APPDomain/config/fmw
config`

`map` specifies the map of the credential to add.

`key` specifies the key of the credential to add.

`username` specifies the name of the user in the credential to add.

`password` specifies the password of the user in the credential to add.

Example of Use:

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

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

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

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RMS batch	DB	<RMS batch install dir (RETAIL_HOME)>/.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 batch plsql and sqlldr	DB	<RPM batch install dir>/.wallet	n/a	<rms schema owner alias>	<rms schema owner>	Execute batch	Manual	rms-alias	RPM plsql and sqlldr batches
RWMS auto-login	JAVA	<forms install dir>/base/.javawallet							
			<RWMS Installation name>	<RWMS database user alias>	<RWMS schema owner>	RWMS forms app to avoid dblogin screen	Installer	rwms15inst	
			<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
			aip	<AIP weblogic user alias>	<AIP weblogic user name>	App use	Installer	aip-weblogic-alias	
			aip	<AIP database schema user alias>	<AIP database schema user name>	App use	Installer	aip01user-alias	
			aip	<rib-aip weblogic user alias>	<rib-aip weblogic user name>	App use	Installer	rib-aip-weblogic-alias	
RPM app	DB credential store		Map=rpm or what you called the app at install time.	Many for app use					<weblogic domain home>/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.
RPM app	JAVA	<weblogic domain home>/retail/<deployed rpm app name>/config							Each alias must be unique
			rpm	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	rpm-weblogic-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			rpm	<rpm batch user name> is the alias. Yes, here alias name = user name	<rpm batch user name>	App, batch use	Installer	RETAIL.USER	
	JAVA	<retail_home>/orpatch/config/javaapp_rpm							Each alias must be unique
			retail_installer	<rpm weblogic user alias>	<rpm weblogic user name>	App use	Installer	weblogic-alias	
			retail_installer	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			retail_installer	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbat-alias	
			retail_installer	<LDAP-ALIAS>	cn=rpm.admin,cn=Users,dc=us,dc=oracle,dc=com	LDAP user use	Installer	LDAP_ALIAS	
ReIM app	JAVA	<weblogic domain home>/retail/<deployed reim app name>/config							Each alias must be unique
			<installed app name, ex: reim>	<reim weblogic user alias>	<reim weblogic user name>	App use	Installer	weblogic-alias	
			<installed app name, ex: reim>	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			<installed app name, ex: reim>	<reim webservice validation user alias>	<reim webservice validation user name>	App use	Installer	reimwebser vice-alias	
			<installed app name, ex: reim>	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbat-alias	
			<installed app name, ex: reim>	<LDAP-ALIAS>	cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com	LDAP user use	Installer	LDAP_ALIAS	
	JAVA	<retail_home>/orpatch/conf/javaapp_reim							Each alias must be unique
			retail_installer	<reim weblogic user alias>	<reim weblogic user name>	App use	Installer	weblogic-alias	
			retail_installer	<rms shema user alias>	<rms shema user name>	App, batch use	Installer	rms01user-alias	
			retail_installer	<reim webservice validation user alias>	<reim webservice validation user name>	App use	Installer	reimwebser vice-alias	
			retail_installer	<reim batch user alias>	<reim batch user name>	App, batch use	Installer	reimbat-alias	
			retail_installer	<LDAP-ALIAS>	cn=REIM.ADMIN,cn=Users,dc=us,dc=oracle,dc=com	LDAP user use	Installer	LDAP_ALIAS	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
RESA app	DB credential store		Map=resaor what you called the app at install time	Many for login and policies					<weblogic domain home>/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file. The bootstrap directory under this directory has bootstrap cwallet.sso file.
RESA app	JAVA	<weblogic domain home>/retail/<deployed resa app name>/config							Each alias must be unique
			<installed app name>	<resa weblogic user alias>	<resa weblogic user name>	App use	Installer	wlsalias	
			<installed app name>	<resa schema db user alias>	<rmsdb shema user name>	App use	Installer	Resadb-alias	
			<installed app name>	<resa schema user alias>	<rmsdb shema user name>>	App use	Installer	resa-alias	
	JAVA	<retail_home>/orpatch/conf/javaapp_resa							Each alias must be unique

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
			retail_installer	<resa weblogic user alias>	<resa weblogic user name>	App use	Installer	wlsalias	
			retail_installer	<resa schema db user alias>	<rmsdb shema user name>	App use	Installer	Resadb-alias	
	JAVA	<retail_ home>/orpatch/config/javaapp_rasrm							Each alias must be unique
			retail_installer	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	
Alloc app	DB credential store		Map=alloc or what you called the app at install time	Many for login and policies					<weblogic domain home>/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file. The bootstrap directory under this directory has bootstrap cwallet.sso file.
Alloc app	JAVA	<weblogic domain home>/retail/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 schema user alias>	<rms schema user name>	App use	Installer	dsallocAlias	
			<installed app name>	<alloc batch user alias>	<SYSTEM_ADMINISTRATOR>	Batch use	Installer	alloc14	
	JAVA	<retail_home>/orpatch/config/javaapp_alloc							Each alias must be unique
			retail_installer	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	
			retail_installer	<rms schema user alias>	<rms schema user name>	App use	Installer	dsallocAlias	
			retail_installer	<alloc batch user alias>	<SYSTEM_ADMINISTRATOR>	Batch use	Installer	alloc14	
	JAVA	<retail_home>/orpatch/config/javaapp_rasrm							Each alias must be unique
			retail_installer	<alloc weblogic user alias>	<alloc weblogic user name>	App use	Installer	weblogic-alias	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
SIM app	DB credential store		Map=oracle.retail.sim	Aliases required for SIM app use					<weblogic domain home>/config/fmwc onfig/jps-config.xml has info on the credential store. This directory also has the domain cwallet.sso file.
	JAVA	<weblogic domain home>/retail/<deployed sim app name>/batch/resources/conf	oracle.retail.sim	<sim batch user alias>	<sim batch user name>	App use	Installer	BATCH-ALIAS	
	JAVA	<weblogic domain home>/retail/<deployed sim app name>/wireless/resources/conf	oracle.retail.sim	<sim wireless user alias>	<sim wireless user name>	App use	Installer	WIRELESS-ALIAS	
RETL	JAVA	<RETL home>/etc/security	n/a	<target application user alias>	<target application db userid>	App use	Manual	retl_java_rms01user	User may vary depending on RETL flow's target application
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	

Retail app	Wallet type	Wallet loc	Wallet partition	Alias name	User name	Use	Create by	Alias Example	Notes
WebLogic			rib-<app>-app-server-instance	<rib-app weblogic user alias>	<rib-app weblogic user name>	Integration use	Installer	weblogic-alias	
Admin GUI			rib-<app>#web-app-user-alias	<rib-app admin gui user alias>	<rib-app admin gui user name>	Integration use	Installer	admin-gui-alias	
Application			rib-<app>#user-alias	<app weblogic user alias>	<app weblogic user name>	Integration use	Installer	app-user-alias	Valid only for aip, rpm, sim
DB			rib-<app>#app-db-user-alias	<rib-app database schema user alias>	<rib-app database schema user name>	Integration use	Installer	db-user-alias	Valid only for rfm, rms, rwms, tafr
Error Hospital			rib-<app>#hosp-user-alias	<rib-app error hospital database schema user alias>	<rib-app error hospital database schema user name>	Integration use	Installer	hosp-user-alias	
RFI	Java	<RFI-HOME>/retail-financial-integration-solution/service-based-integration/conf/security							
			<installed app name>	rfiAppServerAdminServerUserAlias	<rfi weblogic user name>	App use	Installer	rfiAppServerAdminServerUserAlias	
			<installed app name>	rfiAdminUiUserAlias	<ORFI admin user>	App use	Installer	rfiAdminUiUserAlias	
			<installed app name>	rfiDataSourceUserAlias	<ORFI schema user name>	App use	Installer	rfiDataSourceUserAlias	

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

Appendix: Installation Order

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

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

Enterprise Installation Order

1. Oracle Retail Merchandising System (RMS), Oracle Retail Trade Management (RTM)
2. Oracle Retail Sales Audit (ReSA)
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)
8. Oracle Retail Allocation
9. Oracle Retail Mobile Merchandising (ORMM)
10. Oracle Retail Xstore Office
11. Oracle Retail Xstore Point-of-Service, including Xstore Point-of-Service for Grocery, and including Xstore Mobile
12. Oracle Retail Xstore Environment
13. Oracle Retail EFTLink
14. Oracle Retail Store Inventory Management (SIM), including Mobile SIM
15. Oracle Retail Predictive Application Server (RPAS)
16. Oracle Retail Batch Script Architecture (BSA)
17. Oracle Retail Demand Forecasting (RDF)
18. Oracle Retail Category Management Planning and Optimization/Macro Space Optimization (CMPO/MSO)
19. Oracle Retail Replenishment Optimization (RO)
20. Oracle Retail Analytic Parameter Calculator Replenishment Optimization (APC RO)
21. Oracle Retail Regular Price Optimization (RPO)
22. Oracle Retail Merchandise Financial Planning (MFP)
23. Oracle Retail Size Profile Optimization (SPO)
24. Oracle Retail Assortment Planning (AP)
25. Oracle Retail Item Planning (IP)
26. Oracle Retail Item Planning Configured for COE (IP COE)
27. Oracle Retail Advanced Inventory Planning (AIP)
28. Oracle Retail Integration Bus (RIB)
29. Oracle Retail Services Backbone (RSB)

-
- 30.** Oracle Retail Financial Integration (ORFI)
 - 31.** Oracle Retail Data Extractor for Merchandising
 - 32.** Oracle Retail Clearance Optimization Engine (COE)
 - 33.** Oracle Retail Analytic Parameter Calculator for Regular Price Optimization (APC-RPO)
 - 34.** Oracle Retail Insights, including Retail Merchandising Insights (previously Retail Merchandising Analytics) and Retail Customer Insights (previously Retail Customer Analytics)